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 УПРАВЛІННЯ КІБЕРБЕЗПЕКОЮ ПІДПРИЄМСТВА ЗА ДОМЕНАМИ БЕЗПЕКИ В УМОВАХ ГІБРИДНОЇ ВІЙНИ”

на здобуття освітнього ступеня бакалавра
зі спеціальності 125 Кібербезпека
освітньої програми Управління інформаційною та кібернетичною безпекою

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

_____ Валерія НЕНЬКО
(підпис) *Ім’я, ПРІЗВИЩЕ здобувача*

Виконала: здобувачка вищої освіти гр. УБД-41
Валерія НЕНЬКО
Ім’я, ПРІЗВИЩЕ

Керівник: Тетяна КАПЕЛЮШНА
д.е.н., доцент Ім’я, ПРІЗВИЩЕ

Рецензент: Галина ГАЙДУР
д.т.н., професор Ім’я, ПРІЗВИЩЕ

Київ 2026

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

Кафедра управління кібербезпекою та захистом інформації

Ступінь вищої освіти бакалавр

Спеціальність 125 Кібербезпека

Освітня програма Управління інформаційною та кібернетичною безпекою

ЗАТВЕРДЖУЮ
Завідувач кафедрою УКБЗІ
_____Світлана ЛЕГОМІНОВА
“____” _____ 2026 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Ненько Валерії Романівні
(прізвище, ім’я, по батькові здобувача)

1. Тема кваліфікаційної роботи “Система управління кібербезпекою підприємства за доменами безпеки в умовах гібридної війни”,
керівник кваліфікаційної роботи Тетяна КАПЕЛЮШНА, д.е.н., доцент,
(ПРІЗВИЩЕ, Ім’я, науковий ступінь, вчене звання)
затверджені наказом Державного університету інформаційно-комунікаційних технологій від “20“ лютого 2026 р. №51

2. Строк подання кваліфікаційної роботи “20” травня 2026 р.

3. Вихідні дані до кваліфікаційної роботи: *нормативно-правове забезпечення з питань кібербезпеки та захисту інформації, наукова та технічна література, аналітичні звіти сучасних кіберзагроз, матеріали щодо гібридної війни та кіберінцидентів, а також інформація про політики безпеки підприємств.*

4. Перелік питань, які мають бути розроблені:

4.1 Визначити суть гібридних загроз та розглянути концепцію доменів безпеки, оцінити роль у побудові захисту підприємства.
4.2. Проаналізувати стан кібербезпеки підприємства та вплив гібридних атак на діяльність підприємства.
4.3. Спроєктувати систему управління кібербезпекою за доменами безпеки та змоделювати параметри стійкості системи для забезпечення кіберстійкості підприємства в умовах гібридної війни

5. Перелік ілюстративного матеріалу: *презентація PowerPoint*

6. Дата видачі завдання “05“ березня 2026 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назви етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1.	Визначення об’єкту, предмету, мети та завдань дослідження.	18.03.2026	
2.	Збір та аналіз наукової літератури, нормативної бази та стандартів з кібербезпеки.	30.03.2026	
3.	Виклад основних положень та теоретичних засад управління кібербезпекою в умовах гібридних загроз	08.04.2026	
4.	Аналіз загроз та оцінка стану кібербезпеки підприємства в умовах гібридної війни	15.04.2026	
5.	Проєктування та імітаційне моделювання системи управління кібербезпекою підприємства за доменами безпеки в умовах гібридної війни	22.04.2026	
6.	Формулювання висновків за результатами дослідження.	29.04.2026	
7.	Оформлення кваліфікаційної роботи.	06.05.2026	
8.	Оформлення презентації.	11.05.2026	
9.	Отримання рецензії на роботу.	08.06.2026	
10.	Захист в ЕК.	09.06.2026	

Здобувач вищої освіти _____ Валерія НЕНЬКО
(підпис) *(Ім’я, ПРІЗВИЩЕ)*

Керівник кваліфікаційної роботи _____ Тетяна КАПЕЛЮШНА
(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 бакалавра

Направляється здобувачка Ненько В.Р до захисту кваліфікаційної роботи
(прізвище та ініціали)
за спеціальністю 125 Кібербезпека
(код, найменування спеціальності)
освітньої програми Управління інформаційною та кібернетичною безпекою
(назва)
на тему: "Система управління кібербезпекою підприємства за доменами безпеки в умовах гібридної війни".

Кваліфікаційна робота і рецензія додаються.

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

Висновок керівника кваліфікаційної роботи

Здобувачка НЕНЬКО Валерія продемонструвала самостійність у виконанні та глибоке розуміння предметної області. До переваг роботи слід віднести: системний підхід до аналізу: авторка логічно перейшла від теоретичного обґрунтування концепції доменів безпеки (Розділ 1) до практичної оцінки стану захищеності (Розділ 2).

Слід відмітити практичну значущість третього розділу, зокрема розробку архітектури системи управління кібербезпекою та прикладний характер підрозділу 3.3, де здобувачка успішно розробила та застосувала імітаційну модель BIA CRS для розрахунку параметрів стійкості інфраструктури, що є складним завданням для бакалаврського рівня.

Все це дозволяє оцінити кваліфікаційну роботу здобувачки НЕНЬКО Валерії на оцінку "відмінно" та присвоїти їй кваліфікацію бакалавра з кібербезпеки за освітньою програмою Управління інформаційною та кібернетичною безпекою.

Керівник кваліфікаційної роботи _____ Тетяна КАПЕЛЮШНА
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

"___"_____2026 року

Висновок кафедри про кваліфікаційну роботу

Кваліфікаційна робота розглянута. Здобувачка НЕНЬКО В.Р допускається до захисту даної роботи в Екзаменаційній комісії.

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

ВІДГУК РЕЦЕНЗЕНТА
на кваліфікаційну бакалаврську роботу

здобувачки вищої освіти НЕНЬКО Валерії
на тему: "Система управління кібербезпекою підприємства за доменами безпеки в умовах гібридної війни"

Актуальність. Забезпечення кіберстійкості організацій під час гібридних конфліктів є одним із пріоритетних завдань сучасної галузі інформаційної безпеки. Робота НЕНЬКО Валерії присвячена розв'язанню важливої науково-практичної проблеми - структуруванню системи захисту за доменами безпеки та розрахунку параметрів стійкості. Враховуючи постійну трансформацію векторів атак, підхід авторки, що базується на імітаційному моделюванні впливу на бізнес-процеси (BIA), є сучасним, затребуваним та актуальним.

Позитивні сторони. Кваліфікаційна робота характеризується логічною структурою та ґрунтовністю дослідження. Серед сильних сторін варто виділити:

1. Детальний аналіз актуальних гібридних кіберзагроз та оцінку їхнього впливу на безперервність бізнес-процесів (Розділ 2).
2. Запропоновану архітектуру управління кібербезпекою (підрозділ 3.1), яка враховує розподіл за доменами безпеки, що дозволяє оптимізувати ресурси підприємства.
3. Розробку імітаційної моделі BIA CRS (підрозділ 3.3). Авторка продемонструвала вміння застосовувати математичний та аналітичний апарат для розрахунку RTO/RPO та інших критичних параметрів в умовах нестандартних (гібридних) загроз.

Недоліки.

1. Запропоновані у підрозділі 3.2 правила щодо забезпечення кіберстійкості частково носять узагальнений характер і могли б бути більш специфіковані під конкретну галузь (наприклад, критичну інфраструктуру).

2. Імітаційна модель BIA CRS виграла б, якби у роботі було наведено результати її тестування на більшій кількості різних сценаріїв гібридних атак.

Втім, ці зауваження мають характер побажань і не впливають на достовірність та обґрунтованість отриманих результатів.

Висновок: Кваліфікаційна робота виконана на належному науково-методичному рівні і заслуговує оцінки "відмінно", а здобувачка НЕНЬКО Валерія заслуговує присвоєння кваліфікації бакалавра з кібербезпеки за освітньою програмою Управління інформаційною та кібернетичною безпекою.

Рецензент:
д.т.н., професор,
завідувач кафедри
Систем та технологій
кібербезпеки

_____
підпис

Галина ГАЙДУР
Ім'я, ПРІЗВИЩЕ

РЕФЕРАТ

Кваліфікаційна робота присвячена дослідженню системи управління кібербезпекою підприємства за доменами безпеки в умовах гібридної війни. Робота складається зі вступу, трьох розділів, висновків і списку використаних джерел.

Текстова частина кваліфікаційної роботи на здобуття освітнього ступеня бакалавра містить 79 сторінок, 12 рисунків, 10 таблиць, 40 використаних джерел.

Метою роботи є розробка системи управління кібербезпекою за доменами безпеки та створення імітаційної моделі аналізу впливу на безперервність роботи підприємства для оцінки її параметрів в умовах гібридних загроз.

Об'єктом дослідження є процес управління інформаційною та кібернетичною безпекою підприємства в умовах гібридної війни.

Предметом дослідження є система управління кібербезпекою за доменами безпеки та моделювання параметрів її стійкості (RTO/RPO).

Методи дослідження. У роботі використано методи системного та порівняльного аналізу, класифікації, моделювання, експертного оцінювання, а також ризик-орієнтований підхід до управління кібербезпекою.

Короткий зміст роботи. Розглянуто засади управління кібербезпекою, гібридні загрози та концепцію доменів безпеки. Проведено аналіз актуальних кіберзагроз для підприємств енергетичного сектору та здійснено оцінювання рівня кіберризиків за доменами безпеки. Розроблено систему управління кібербезпекою підприємства та рекомендації щодо підвищення кіберстійкості.

Галузь застосування. Результати роботи можуть бути використані під час побудови та вдосконалення систем управління кібербезпекою та забезпечення безперервності бізнес-процесів в умовах гібридних загроз на підприємствах критичної інфраструктури енергетичного сектору.

Апробація результатів кваліфікаційної роботи відбулася на Всеукраїнській науково-практичній конференції “Стратегії кіберстійкості: управління ризиками та безперервність бізнесу” 25 лютого 2026 року.

КЛЮЧОВІ СЛОВА: КІБЕРБЕЗПЕКА, ГІБРИДНІ ЗАГРОЗИ, ДОМЕНИ БЕЗПЕКИ, УПРАВЛІННЯ КІБЕРБЕЗПЕКОЮ, КІБЕРСТІЙКІСТЬ, КРИТИЧНА ІНФРАСТРУКТУРА.

ABSTRACT

The qualification work is devoted to the study of an enterprise cybersecurity management system based on security domains under conditions of hybrid warfare.

The thesis consists of an introduction, three chapters, conclusions, and a list of references.

The qualification thesis for obtaining the Bachelor's degree contains 79 pages, 12 figures, 10 tables, and 40 references.

The purpose of the study is to develop a cybersecurity management system based on security domains, taking into account hybrid threats.

The object of the study is the process of cybersecurity management of a critical infrastructure enterprise in the energy sector of Ukraine under conditions of hybrid warfare.

The subject of the study is the domain-based approach to enterprise cybersecurity management under conditions of hybrid threats.

Research methods. The study applies methods of system and comparative analysis, classification, modeling, expert assessment, as well as a risk-oriented approach to cybersecurity management.

Brief content of the thesis. The thesis examines the foundations of cybersecurity management, hybrid threats, and the concept of security domains. An analysis of current cyber threats to energy sector enterprises was carried out, and cybersecurity risks were assessed according to security domains. An enterprise cybersecurity management system and recommendations for improving cyber resilience were developed.

Field of application. The results of the study may be used in the development and improvement of cybersecurity management systems and ensuring business continuity under conditions of hybrid threats at critical infrastructure enterprises in the energy sector.

KEYWORDS: CYBERSECURITY, HYBRID THREATS, SECURITY DOMAINS, CYBERSECURITY MANAGEMENT, CYBER RESILIENCE.

ЗМІСТ

Стор.

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ І СКОРОЧЕНЬ

APT	Advanced Persistent Threat (цілеспрямована тривала атака)
АСУ ТП	Автоматизовані системи управління технологічними процесами
BIA	Business Impact Analysis (аналіз впливу на бізнес)
CERT-UA	Урядова команда реагування на комп’ютерні надзвичайні події України
DDoS	Distributed Denial of Service (розподілена атака відмови в обслуговуванні)
DLP	Data Loss Prevention
GRC	Governance, Risk and Compliance
IAM	Identity & Access Management
IT	Information Technology
MITM	Man-in-the-Middle
MFA	Multi-Factor Authentication
OT	Operational Technology
SCADA	Supervisory Control and Data Acquisition
СУКБ	Система управління кібербезпекою
SIEM	Security Information and Event Management
SOC	Security Operations Center (центр моніторингу безпеки)
UEBA	User and Entity Behavior Analytics
ОКІ	Об’єкт критичної інфраструктури

ВСТУП

Актуальність теми. Повномасштабна збройна агресія російської федерації проти України остаточно закріпила статус кіберпростору як п’ятого домену ведення бойових дій, нарівні із суходолом, морем, повітрям та космосом. Нинішня війна стирає традиційні межі між фронтом і тилом, переносячи значну частину протистояння у цифровий простір. Інформаційні системи держави та бізнесу стають об’єктами безперервного кібернетичного тиску, що перетворює підприємства на важливі цілі для противника. У цих умовах оборона корпоративних мереж виходить за рамки збереження комерційної інформації та набуває стратегічного значення, оскільки стабільність роботи бізнесу є ключовим чинником економічної стійкості країни.

Концепція гібридних війн визначає поточну війну як комбінацію різних видів військових і невійськових засобів, які використовуються для досягнення стратегічних цілей. Ці засоби поєднують традиційні військові операції з нетрадиційними методами, зокрема інформаційно-психологічними операціями (ІПсО), кібератаками, економічним тиском, шпигунством, соціальною інженерією та асиметричними методами впливу. Іншими словами — це прагнення не знищити мільйони людей, а залякати й деморалізувати їх. Завдяки швидкості поширення інформації світом вона перетворилася не лише на товар, а й на зброю [1].

За даними аналітичних звітів Державної служби спеціального зв’язку та захисту інформації України, у 2024–2025 роках спостерігається зміна характеру кібероперацій — від масових деструктивних атак до більш складних цілеспрямованих кампаній, спрямованих на отримання доступу до інформаційних систем, викрадення даних та тривале приховане перебування в мережах організацій [2]. Особливу активність демонструють організовані кіберугруповання, пов’язані з державою-агресором, які здійснюють атаки на фінансовий сектор, логістичні компанії, енергетичну інфраструктуру та ІТ-

постачальників. Використання вразливостей нульового дня та легітимних інструментів адміністрування значно ускладнює виявлення таких атак традиційними засобами протидії.

У зв’язку з цим актуальним є впровадження системного підходу до реалізації безпеки цифрового середовища, який дозволяє враховувати комплексний характер новітніх загроз. Одним із таких підходів є концепція доменів безпеки, що передбачає структуризацію системи захисту за функціональними напрямами. До таких доменів належать управління ризиками, безпека активів, мережева безпека, управління доступом, безпека програмного забезпечення, моніторинг та реагування на інциденти, комплаєнс і навчання персоналу.

Застосування доменного підходу дозволяє систематизувати заходи кібербезпеки, чітко розподілити обов'язки та створити багаторівневу захисну архітектуру. Оскільки компрометація окремого домену не руйнує загальну систему захисту, такий розподіл є важливим для підвищення кіберстійкості підприємства. Це зумовлює необхідність розробки ефективної системи управління кібербезпекою на основі доменів безпеки, адаптованої до викликів сучасної гібридної війни.

Метою роботи є розробка системи управління кібербезпекою підприємства критичної інфраструктури енергетичного сектору за доменами безпеки з урахуванням гібридних загроз та формування практичних рекомендацій щодо підвищення кіберстійкості.

Об’єктом дослідження є процес управління кібербезпекою підприємства критичної інфраструктури енергетичного сектору України в умовах гібридної війни.

Предметом дослідження є доменний підхід до управління кібербезпекою підприємства в умовах гібридних загроз.

Наукові завдання:

1. Розкрити сутність та класифікацію гібридних загроз у кіберпросторі.

2. Проаналізувати концепцію доменів безпеки та їх роль у побудові системи управління кібербезпекою підприємства.
3. Розглянути міжнародні стандарти та нормативні підходи як підґрунтя для управління доменами безпеки.
4. Провести аналіз основних кіберризиків для типового підприємства критичної інфраструктури енергетичного сектору України.
5. Розробити структуру системи управління кібербезпекою (СУКБ) за доменами для умовного підприємства.
6. Надати практичні рекомендації щодо автоматизації процесів моніторингу та реагування в межах визначених доменів.

Методи дослідження. У роботі використано методи системного та порівняльного аналізу, класифікації, моделювання, узагальнення експертного оцінювання, а також ризик-орієнтований та доменний підходи до управління кібербезпекою.

Практичне значення одержаних результатів полягає у можливості застосування запропонованого підходу під час побудови системи управління кібербезпекою на підприємствах життєво важливої інфраструктури, зокрема енергетичного сектору. Запропоновані рішення можуть бути використані для підвищення рівня захисту інформаційних систем, забезпечення стійкості бізнес-процесів та покращення реагування на кіберзагрози в умовах гібридної війни.

Апробація результатів кваліфікаційної роботи відбулася на Всеукраїнській науково-практичній конференції “Стратегії кіберстійкості: управління ризиками та безперервність бізнесу” 25 лютого 2026 року.

Розділ 1 ТЕОРЕТИЧНІ ЗАСАДИ УПРАВЛІННЯ КІБЕРБЕЗПЕКОЮ В УМОВАХ ГІБРИДНИХ ЗАГРОЗ

1.1. Сутність та класифікація гібридних загроз у кіберпросторі

Розвиток цифрових технологій та масштабна цифровізація суспільства суттєво трансформували характер сучасних конфліктів, у яких кіберпростір відіграє роль одного з ключових складових протиборства. У таких умовах інформаційні системи державних установ і стратегічних підприємств дедалі частіше стають цілями кібератак, інформаційного тиску та спроб несанкціонованого втручання.

У науковій літературі відсутнє єдине універсальне визначення гібридних загроз, однак більшість дослідників розглядають їх як поєднання військових, інформаційних, кібернетичних, економічних, політичних та психологічних методів впливу, які використовуються для досягнення стратегічних цілей без прямого застосування традиційної військової сили. Також вони зазначають, що інформаційна сфера є ключовим елементом протистояння, де відбувається маніпуляція суспільною свідомістю, дезінформація та інформаційний тиск.

Особливістю таких загроз є поєднання технічних і нетехнічних інструментів впливу. На відміну від традиційних цифрових атак, які переважно спрямовані на отримання фінансової вигоди або викрадення даних, скоординовані загрози мають більш широкий та стратегічний характер. Їх метою є дестабілізація функціонування держави, порушення роботи енергетичної інфраструктури, створення паніки серед населення, зниження довіри до державних інституцій та порушення безперервності бізнес-процесів.

Ще видатний китайський стратег і мислитель Сунь-Цзи у своєму трактаті «Мистецтво війни» зазначав: «Здобути сто перемог у ста битвах – це не вершина військового мистецтва. Повалити ворога без бою – ось вершина» [7]. Це положення відображає модернізований підхід до ведення гібридної війни, в основі якого лежить комплексне використання різних методів дестабілізації

замість відкритого силового протистояння. Така синергія методів дозволяє агресору досягати стратегічних цілей, розмиваючи межу між станом війни та миру, зокрема дестабілізація держави, порушення роботи ключового середовища, тиск на суспільну свідомість та підрив систем державного управління [8].

У нинішніх реаліях такі загрози активно використовуються у віртуальному середовищі. Особливої актуальності це питання набуло для України в умовах повномасштабної війни, коли ворожа активність у цифровому середовищі стала складовою частиною гібридного протистояння. Атаки на державні інформаційні ресурси, енергетику, телекомунікаційні та інфраструктурні об’єкти держави демонструють, що мережевий простір фактично став окремим доменом ведення нинішньої війни.

Таким чином, поняття «гібридні загрози» та «гібридні війни» є спорідненими. Їх характеристиками є діяльність державних і недержавних акторів, асиметричний фактор, нелінійність та багаторівневість атак, а також поєднання традиційних і нетрадиційних інструментів впливу.

До характерних ознак належать:

— Синергія, тобто одночасне використання технічних (DDoS-атаки, шкідливе програмне забезпечення) та нетехнічних (ІПСО, дезінформація, соціальна інженерія) засобів;

— Багаторівневість, прояв не лише на технічне середовище (мережі, сервери), але й на соціальні системи та поведінку користувачів;

— Анонімність та висока швидкість реалізації, що ускладнює ідентифікацію джерела атак та оперативне реагування;

— Створення хаосу та нестабільності, метою є дестабілізація ситуації в країні, підрив безпеки та вплив на прийняття рішень [21].

Важливою рисою є суттєве розширення поверхні атаки (attack surface) підприємства, тобто сукупності всіх можливих точок входу для зловмисника. Це зумовлено тим, що об'єктами компрометації стають не лише корпоративні

сервери, а й особисті пристрої працівників, віддалені робочі середовища та канали комунікації в месенджерах.

У кіберпросторі подібні механізми реалізуються через поєднання технічних атак із інформаційним та соціальним тиском. Наприклад, атака може розпочинатися з фішингової кампанії, продовжуватися проникненням у корпоративну мережу та завершуватися викраденням даних або порушенням діяльності інформаційних систем.

До домінуючих механізмів реалізації належать:

— Соціальна інженерія – психологічна маніпуляція користувачами з метою отримання доступу до конфіденційної інформації або порушення політик безпеки. Зокрема, використовується фішинг (phishing), що спрямований на викрадення облікових даних.

— Впровадження шкідливого програмного забезпечення – використання ransomware (вірусів-вимагачів), spyware (шпигунського програмного забезпечення), троянів та інших видів шкідливого коду для порушення роботи механізмів або отримання несанкціонованого доступу.

— Розподілені атаки на відмову в обслуговуванні (DDoS) – штучне створення надмірного навантаження на вебресурси та мережеві сервіси підприємства.

— Експлуатація вразливостей – використання недоліків програмного забезпечення, мережевих конфігурацій або застарілих систем для обходу засобів контролю безпеки.

Комплексне застосування зазначених механізмів суттєво ускладнює їх виявлення та значно підвищує ефективність атак.

Загрози гібридного характеру у цифровій сфері можуть відрізнятися за цілями, способами реалізації та напрямами здійснення атак. Їх узагальнену класифікацію наведено на рис. 1.1. [2,4,5].

Рис. 1.1. Узагальнена класифікація гібридних загроз у кіберпросторі

Джерело: складено автором за даними ENISA, MITRE ATT&CK, Держспецзв'язку України та наукових джерел [2, 4, 5]

Аналіз наведеної класифікації показує, що актуальні загрози мають комплексний характер та поєднують технічні, інформаційні й соціальні результати дій. Зокрема, відповідно до звітів ENISA та Держспецзв'язку України, спостерігається зростання кількості атак на ланцюги постачання (supply chain attacks), реалізація складних цілеспрямованих кампаній, а також атак із використанням автоматизованих інструментів для проведення фішингу та поширення дезінформації [2,4,5].

Тому загрози у кібернетичному середовищі є багатовекторним явищем, що може діяти як на інформаційні системи підприємства, так і на його персонал, бізнес-процеси та стратегічні об'єкти. Це обумовлює необхідність побудови комплексної моделі управління кібербезпекою за доменами безпеки.

Для даного дослідження особливий інтерес становлять сфери, які безпосередньо пов'язані з діяльністю комплексу енергетичного сектору, інформаційно-комунікаційними системами та створення умов для протидії

загрозам підприємства в умовах зростання кіберризиків. Тому вони представлені в табл. 1.1 [7].

Таблиця 1.1

Основні сфери реалізації гібридних загроз

Сфера	Характеристика
Інформаційна сфера	Використовується для поширення дезінформації, пропаганди, маніпулювання громадською думкою та створення соціальної напруги. Інструментами впливу є фейкові новини, інформаційно-психологічні операції та кіберпропаганда.
Кіберпростір	Охоплює інформаційні мережі та телекомунікації. Основними загрозами є ворожі дії у цифровому середовищі, шкідливе програмне забезпечення, несанкціонований доступ, кібершпигунство та порушення роботи мережевої структури.
Військова/оборонна сфера	Передбачає здійснення тиску на обороноздатність держави, військові системи управління та інформаційні ресурси. Ворожі дії у цій сфері можуть використовуватись для послаблення стійкості держави та створення умов для порушення національної безпеки.
Критична інфраструктура	Спрямована на порушення функціонування життєво важливих систем держави. Об’єктами атак виступають енергетика, транспорт, зв’язок, водопостачання та інші важливі об’єкти, порушення роботи яких може мати значний суспільний та економічний ефект.
Сфера державного управління	Спрямована на порушення стабільної роботи органів державної влади, державних інформаційних систем та електронних сервісів. Метою є дестабілізація управлінських процесів і зниження довіри до державних інституцій.
Соціально-психологічна	Спрямована на формування суспільних настроїв, формування паніки, страху та недовіри. Реалізується через інформаційні кампанії, психологічний тиск та маніпулювання суспільною свідомістю.
Енергетична інфраструктура	Провідними загрозами є атаки на OT-мережі, платформи диспетчеризації, SCADA-системи та об’єкти енергопостачання, що можуть призводити до фізичних наслідків та порушення енергозабезпечення.

Джерело: складено на основі [7]

Тому поточні загрози інформаційній безпеці здатні одночасно впливати на інформаційні, технічні, економічні та соціальні процеси. Для підприємств енергетичного сектору найбільшу небезпеку становлять атаки на інформаційно-

комунікаційні мережі, енергетичні об’єкти та цифрове середовище, оскільки їх компрометація може призвести до збоїв у роботі підприємства. За таких умов забезпечення кібербезпеки потребує застосування системного підходу, заснованого на розподілі функцій захисту за окремими доменами безпеки.

1.2. Концепція доменів безпеки та її роль у побудові комплексної системи захисту підприємства

У нинішніх реаліях кібератаки вважаються однією з головних складових гібридних конфліктів [9], що безпосередньо спрямовується на функціонування підприємств. У зв’язку з цим підвищення кіберстійкості організацій вимагає переходу від використання окремих засобів захисту до побудови цілісної системи управління кібербезпекою.

Нові загрози б'ють одночасно по технічному сектору, персоналу та організаційних ланках. Традиційні підходи до кіберзахисту, що базуються на застосуванні окремих технічних рішень (антивірусів, міжмережевих екранів), не забезпечують належного рівня контролю безпеки в таких умовах. Це призводить до фрагментарності архітектури безпеки, зниження ефективності виявлення загроз та ускладнення реагування на кіберінциденти.

Одним із найбільш ефективних підходів до структуризації моделі захисту цифрового середовища є концепція доменів безпеки. Домен безпеки — це логічно відокремлена сфера контролю, що об’єднує сукупність активів, процесів, технологій та людських ресурсів, спрямованих на вирішення окремого функціонального сегмента інформаційної мережі або бізнес-процесів підприємства із забезпечення конфіденційності, цілісності та доступності інформації. Доменна модель дозволяє структурувати складну систему кібербезпеки підприємства, розподіляючи відповідальність та ресурси відповідно до діяльності напрямків.

Концепція доменів безпеки (security domains) є основою архітектури корпоративної безпеки, яка дозволяє структурувати захист великих та складних

підприємств. Вона передбачає поділ IT-інфраструктури на логічні, функціональні або фізичні зони (домени) з різними рівнями довіри та правилами безпеки [11].

Використання доменного підходу дає можливість:

— системність управління кібербезпекою;

— розподіл функцій безпеки між окремими напрямами;

— інтеграцію технічних і організаційних заходів;

— підвищення рівня контролю та моніторингу загроз.

Актуальні підходи до інформаційної безпеки, відображені в міжнародних стандартах (ISO/IEC 27001 [13], NIST Cybersecurity Framework [15], NIST SP 800-53 [16], CIS Controls [17]), не визначають єдиного універсального переліку доменів безпеки, проте пропонують різні способи структуризації заходів захисту — через функції, контролі або процеси. Узагальнення цих підходів дозволяє сформувати інтегровану модель доменів кібербезпеки підприємства, яка поєднує стратегічний, технічний та операційний рівні протидії інформаційним загрозам.

Для прикладу візуалізації взаємозв’язків між доменами було обрано карту доменів кібербезпеки (Henry Jiang, 2021) [12], яка узагальнює актуальні практики побудови систем кіберзахисту. Водночас дана карта не є нормативним джерелом, а використовується як ілюстративна модель, що відображає логіку взаємодії основних напрямів інформаційного простору.

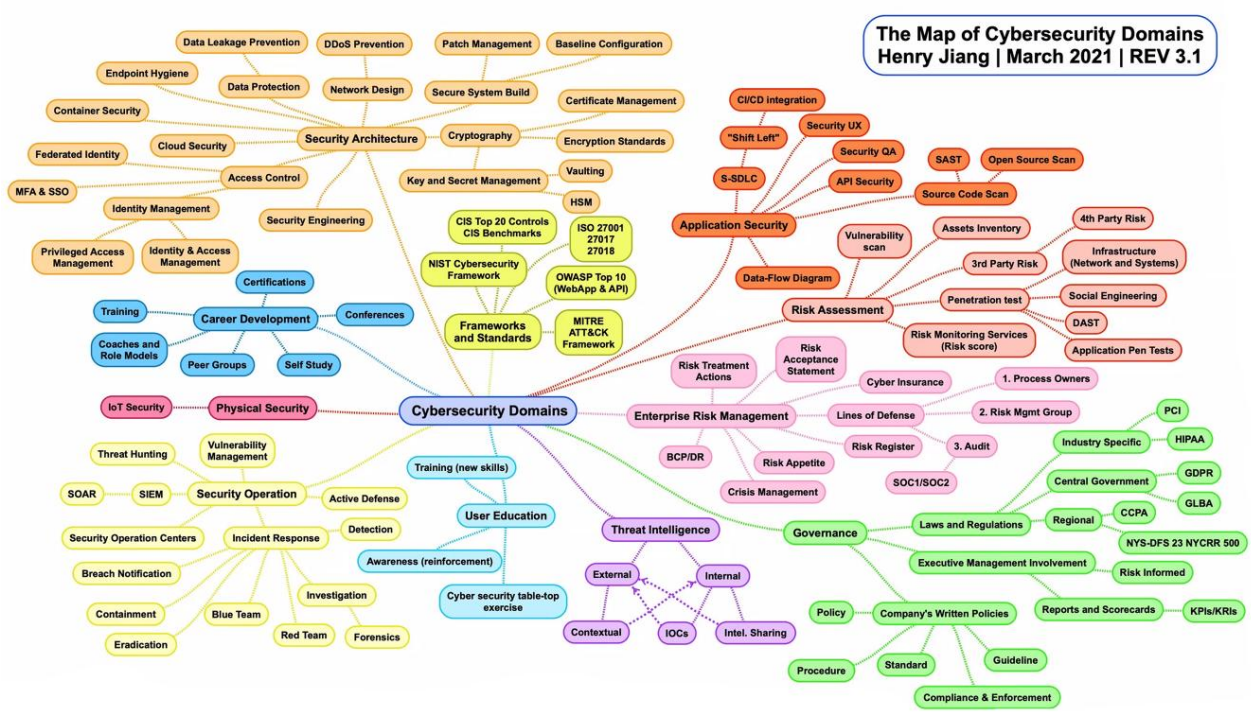

Рис. 1.2. Структура доменів кібербезпеки

Джерело: Henry Jiang. The Map of Cybersecurity Domains [12]

В межах даного дослідження для побудови моделі управління кібербезпекою підприємства виокремлено 10 ключових доменів, що формують фундамент кіберстійкості в умовах новітніх викликів безпеці. Запропонована структура базується на узагальненні підходів міжнародних стандартів ISO/IEC 27001:2022, NIST Cybersecurity Framework 2.0, NIST SP 800-53 та CIS Controls і адаптована до умов функціонування об’єктів критичної інфраструктури енергетичного сектору України [13, 15, 16, 17].

Виділення саме цих доменів обумовлено необхідністю охоплення всіх ключових складових системи управління кібербезпекою підприємства в умовах постійного зовнішнього тиску. Запропоновані домени охоплюють стратегічний, технічний, операційний та організаційний рівні захисту, а також враховують специфіку IT- та OT-середовищ, сучасні кіберзагрози, людський фактор і вимоги забезпечення безперервності бізнес-процесів [10, 11].

Сформована структура доменів дозволяє реалізувати комплексний багаторівневий підхід до управління кібербезпекою підприємства та забезпечити підвищення його кіберстійкості.

Ключові домени кібербезпеки підприємства:

1. Governance, Risk & Compliance (GRC) *(Управління, ризики та комплаєнс)*

Домен є стратегічною основою всієї інформаційної платформи підприємства. Він охоплює розробку політик інформаційної безпеки, управління ризиками, аудит та координацію відповідності нормативним вимогам і міжнародним стандартам.

У контексті воєнного конфлікту цей домен забезпечує прийняття управлінських рішень в умовах невизначеності, дозволяє оцінювати фактори загроз на активи та формувати пріоритети захисту.

2. Asset Management *(Управління активами)*

Передбачає ведення обліку, класифікації, ідентифікації та контролю інформаційних і технічних активів підприємства, включаючи обладнання, програмне забезпечення та дані, зокрема персональні дані користувачів, технічну інформацію та службову документацію.

Неможливо захистити те, чого не бачиш. Для підприємств енергетичної галузі особливе значення має своєчасне виявлення та класифікація життєво важливих активів, порушення роботи яких може призвести до збоїв у роботі технологічних систем, порушення безперервності бізнесу та суттєвих наслідків для енергозабезпечення регіону.

3. Security Architecture (*Архітектура безпеки*)

Домен визначає принципи побудови безпечної IT-інфраструктури, включаючи застосування моделей Zero Trust, сегментацію мережі, криптографічні механізми та інтеграцію засобів захисту.

Він забезпечує узгоджену взаємодію між усіма доменами безпеки та реалізацію багаторівневого захисту (defense in depth).

4. Identity & Access Management (IAM) (*Управління доступом*)

Головним завданням є контроль доступу до ресурсів підприємства та включає механізми автентифікації, авторизації, багатофакторної автентифікації (MFA) та управління привілейованими обліковими записами.

Він гарантує, що кожен працівник має доступ лише до тих активів, які потрібні йому для роботи.

5. Network & Infrastructure Security (*Мережева та інфраструктурна безпека*)

Спрямований на захист мережевого периметра та внутрішньої комунікаційної інфраструктури підприємства від несанкціонованого доступу, перехоплення трафіку та деструктивних технічних впливів.

У контексті енергетичної галузі цей домен є критично важливим, оскільки забезпечує сувору ізоляцію та логічну сегментацію корпоративної (IT) мережі від технологічного контуру АСУ ТП / SCADA (OT)

6. Data Security *(Безпека даних)*

Реалізуються заходи захисту інформації протягом усього її життєвого циклу, включаючи шифрування, резервне копіювання, контроль доступу та системи запобігання витоку даних (DLP).

Є одним із пріоритетних напрямів захисту типу ransomware та викрадення конфіденційної інформації.

7. Application Security & Supply Chain Security *(Безпека застосунків та ланцюга постачання)*

Охоплює організацію безпеки програмного забезпечення на етапах розробки та експлуатації, а також контроль сторонніх компонентів, API, вебзастосунків, хмарних сервісів і сторонніх програмних компонентів.

Особливого значення набуває контроль безпеки ланцюга постачання (supply chain).

8. Security Operations (Monitoring & Incident Response) *(Моніторинг та реагування на інциденти)*

Відповідає за безперервний моніторинг подій безпеки, виявлення та реагування на зловмисні події. Для реалізації функцій моніторингу

використовуються SIEM-системи, створення центрів моніторингу (SOC), аналіз журналів подій та автоматизація процесів реагування.

Включає процеси реагування на інциденти (Incident Response): виявлення, локалізацію, аналіз, усунення наслідків та відновлення архітектури.

9. Vulnerability Management (*Управління вразливостями*)

Домен охоплює процеси виявлення, оцінки та усунення вразливостей. Він включає контроль оновлень безпеки, сканування, оцінку ризиків та моніторинг потенційних слабких місць IT- та OT-інфраструктури.

Своєчасне управління вразливостями є важливим, оскільки зловмисники активно використовують невиправлені та zero-day вразливості для отримання доступу до об’єктів енергетичного сектору й порушення роботи технологічних процесів.

10. Human Factor, Awareness & Physical Security *(Людський фактор і фізична безпека)*

Об’єднує аспекти навчання персоналу, підвищення обізнаності щодо кіберзагроз та забезпечення фізичного середовища. Такі як проведення тренінгів, протидію соціальній інженерії, а також контроль доступу до приміщень, обладнання та інших об’єктів. У поточні ситуації людський фактор часто виступає основною точкою входу для атак.

Запропоновані домени охоплюють усі ключові напрями управління кібербезпекою підприємства та формують цілісну систему захисту в умовах гібридних загроз. Їх комплексна взаємодія забезпечує підвищення рівня кіберстійкості, безперервності бізнес-процесів та ефективності реагування на кіберінциденти. Узагальнену структуру взаємозв’язків між визначеними доменами безпеки представлено на рис. 1.3.

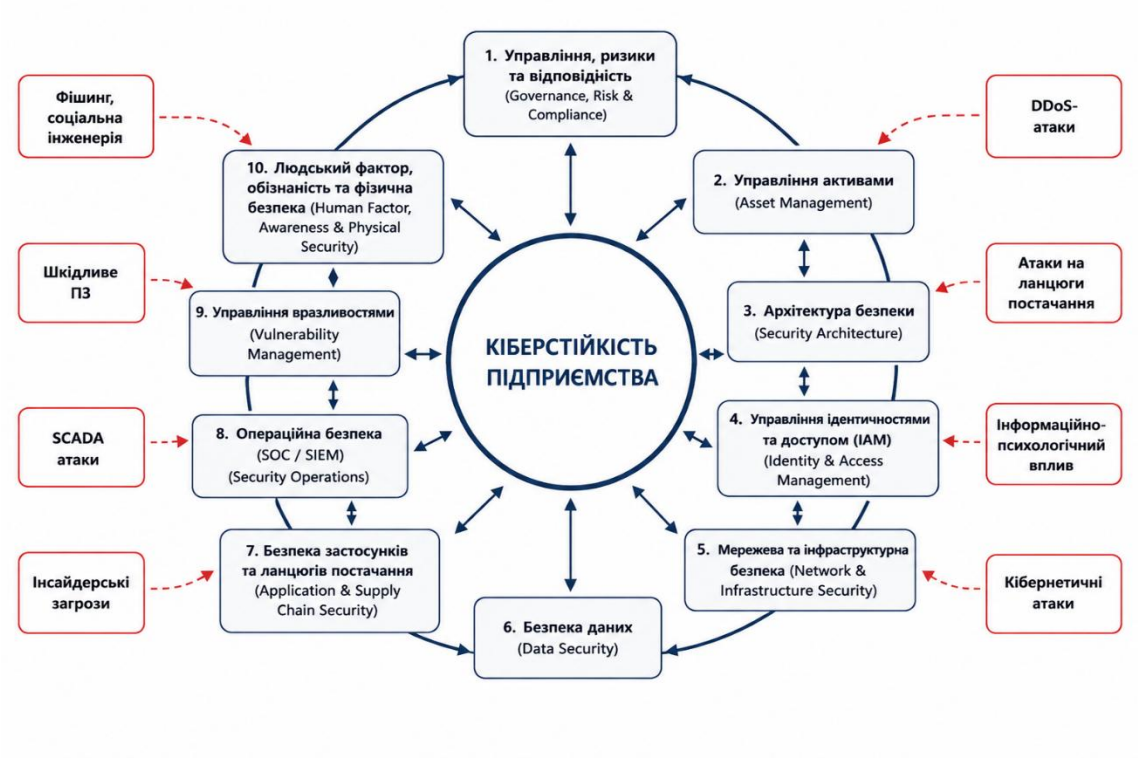

Рис. 1.3. Домени безпеки у системі управління кібербезпекою підприємства в гібридних умовах

Джерело: складено автором на основі визначених доменів

Роль доменів у побудові комплексної системи захисту

Розподіл системи кібербезпеки за доменами дозволяє реалізувати принцип багаторівневого підходу, який передбачає створення декількох рівнів безпеки. Запропонована структура забезпечує комплексний підхід до управління безпекою в інформаційному середовищі, сприяє ефективному розподілу функцій та протидії викликам безпеки. У разі компрометації одного з доменів інші продовжують забезпечувати захист структури, знижуючи загальну величину ризику.

Такий підхід дозволяє інтегрувати заходи у всі бізнес-процеси підприємства, що є доволі важливим в поточному протистоянні. У результаті формується структурована модель кіберзахисту, що сприяє ефективному розподілу функцій між окремими напрямами безпеки та підвищує загальну кіберстійкість підприємства.

Для стратегічного підприємства енергетичного сектору це має особливе значення, оскільки порушення роботи інформаційних, мережевих або технологічних систем може впливати на безперервність енергопостачання та стабільність функціонування підприємства. Саме тому доменний підхід формує основу для побудови ефективної моделі управління кібербезпекою.

1.3. Комплаєнс та стандартизація управління кібербезпекою в умовах гібридної війни

В умовах гібридної війни, коли ризики кіберпростору стають складнішими, багаторівневими та часто непередбачуваними, управління кібербезпекою без чіткої системи правил фактично неможливе. Саме тому особливого значення набуває комплаєнс — відповідність діяльності підприємства встановленим стандартам та нормативним вимогам.

Комплаєнс у сфері кібербезпеки слід розглядати не лише як виконання формальних вимог, а як механізм впорядкування процесів захисту та управління ризиками. Без єдиних підходів кожен підрозділ підприємства може діяти за власною логікою, що призводить до хаосу та втрати контролю над ситуацією.

Міжнародні стандарти як основа управління виконують роль фундаменту, на якому будується вся архітектура. Вони забезпечують узгодженість між різними доменами безпеки, про які йшлося у підрозділі 1.2, та дозволяють перетворити окремі заходи захисту на єдину, цілісну систему.

Для побудови ефективної моделі управління кібербезпекою підприємства доцільно використовувати не один стандарт, а їх поєднання, оскільки кожен із них виконує свою функцію.

Перш за все, варто виділити NIST Cybersecurity Framework (CSF) 2.0 [15], який задає загальну логіку управління кібербезпекою. Його структура базується на ключових функціях — управління, ідентифікація, захист, виявлення,

реагування та відновлення. Такий підхід дозволяє охопити всі етапи роботи з ризиками та фактично відображає життєвий цикл безпеки.

Не менш важливим є стандарт ISO/IEC 27001:2022 [13], який визначає вимоги до системи управління інформаційною безпекою. Його особливістю є орієнтація на організаційний рівень — політики, процедури, аудит і управління ризиками. Водночас оновлена версія стандарту вже враховує нинішні виклики, зокрема хмарні середовища та аналіз загроз.

Якщо попередні стандарти більше відповідають на питання “що потрібно робити”, то CIS Controls [18] надає практичну відповідь “як це реалізувати”. Це набір конкретних заходів, які дозволяють суттєво зменшити ризик реалізації найпоширеніших атак.

Додатково, стандарт NIST SP 800-53 [16] забезпечує глибоку деталізацію технічних і організаційних контролів, тоді як звіти ENISA Threat Landscape [4] дозволяють адаптувати ці контролі до актуальних загроз, що є особливо важливим для підприємств, які працюють в умовах кризової ситуації.

Таким чином, міжнародні стандарти формують комплексну опору управління кібербезпекою — від стратегічного рівня до практичної реалізації заходів охорони інформації.

Поряд із міжнародними стандартами підприємства повинні враховувати вимоги національного законодавства, що регулює цю сферу.

Ключовим документом є Закон України «Про основні засади забезпечення кібербезпеки України» [19], який визначає загальні принципи захисту кіберпростору та відповідальність суб’єктів інформаційного середовища.

Окреме значення мають вимоги Держспецзв’язку [20], особливо для підприємств, що належать до об’єктів державної інфраструктури. Вони встановлюють обов’язкові правила організації захисту інформаційних систем і доповнюють міжнародні стандарти з урахуванням національних особливостей.

Ефективна структура кібербезпеки повинна поєднувати як міжнародні підходи, так і вимоги державного регулювання. Взаємозв’язок між актуальними

загрозами, міжнародними стандартами, нормативно-правовими вимогами та доменами кібербезпеки підприємства наведено на рис. 1.4

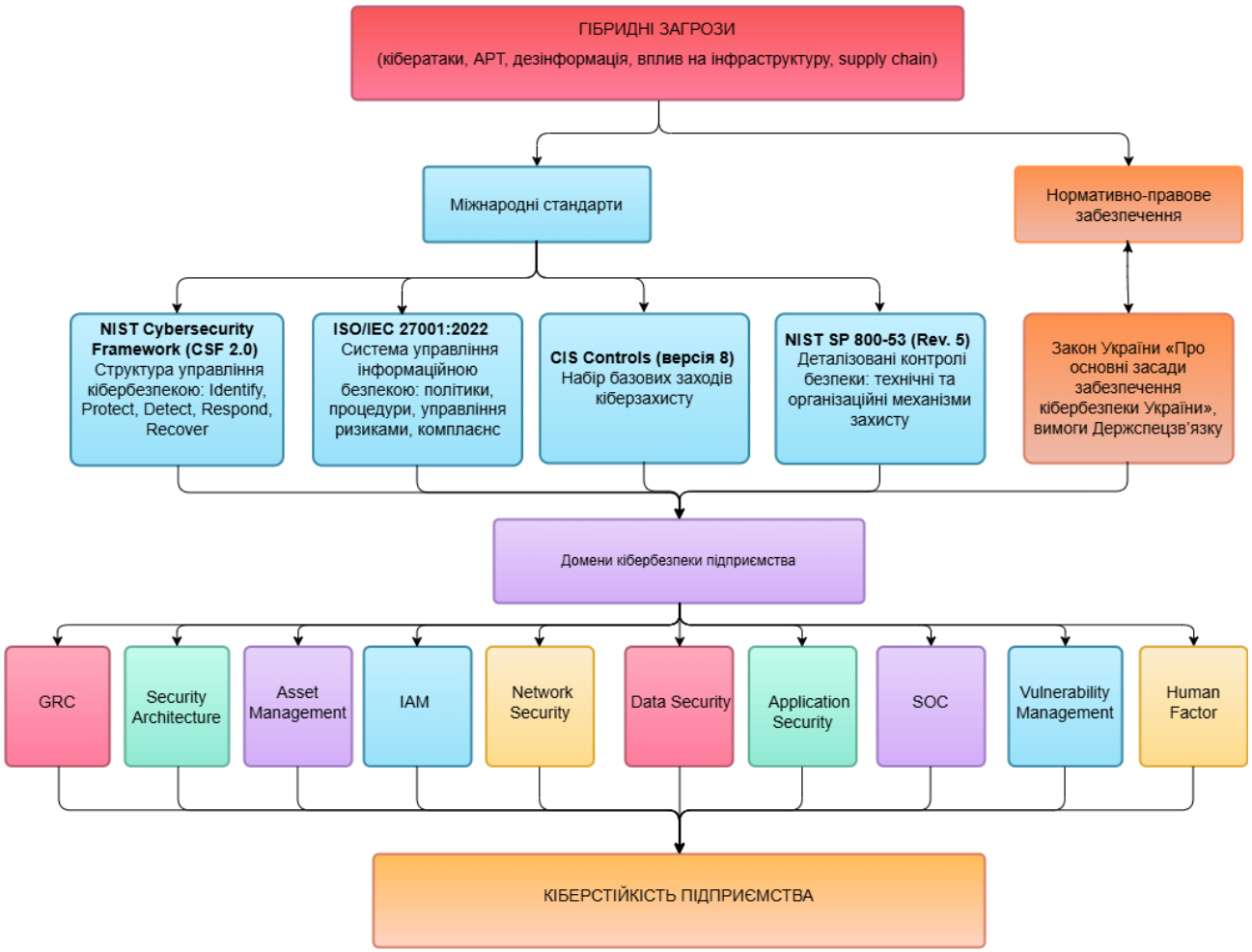

Рис. 1.4. Взаємозв'язок гібридних загроз, стандартів та доменів кібербезпеки підприємства

Джерело: складено автором на основі міжнародних стандартів кібербезпеки [13, 15, 16, 18]

Зв'язок стандартів з доменами безпеки. Систему кібербезпеки підприємства доцільно структурувати за доменами. Водночас жоден із міжнародних стандартів не задає жорсткого переліку таких доменів. Однак саме стандарти створюють базу для їх формування. Наприклад:

— функції NIST CSF можуть бути безпосередньо відображені у відповідних доменах;

— контролі ISO/IEC 27001 охоплюють управління доступом, безпеку мереж, захист даних та інші ключові напрями [13];

— CIS Controls дозволяє деталізувати практичну реалізацію заходів у кожному домені [18].

Гібридна війна встановлює нові правила: сьогодні міжнародні стандарти — це лише база, яка потребує адаптації до реальних бойових умов у інфопросторі. Для енергетичного сектору замало просто виконувати формальні інструкції. Важливо навчитися бачити атаку ще на підході, тримати під повним контролем кожен сегмент мережі та, що найголовніше, швидко відновлювати роботу усіх компонентів у разі порушення їх діяльності.

Саме тому стратегія захисту неможлива без постійного моніторингу подій безпеки, аналізу актуальних загроз та своєчасного управління вразливостями. Безпека має стати не окремим додатком, а частиною підприємства — коли кожен бізнес-процес заздалегідь готується до роботи в передбачуваних умовах. Тільки такий комплексний підхід робить енергосистему справді стійкою та здатною витримати тиск гібридної агресії.

Отже, міжнародні стандарти та нормативно-правові вимоги формують головні засади для побудови системи управління кібербезпекою підприємства. Їх поєднання з доменним підходом дозволяє структуровано організувати процеси контролю безпеки, адаптувати заходи безпеки до умов війни та підвищити кіберстійкість підприємства.

На основі розглянутих стандартів, доменів безпеки та сучасних підходів до управління кіберризиками у наступному розділі буде проведено аналіз актуальних гібридних загроз і оцінку стану кібербезпеки підприємства енергетичного сектору.

Висновки до розділу 1

У першому розділі кваліфікаційної роботи досліджено теоретико-методологічні засади управління кібербезпекою підприємства в умовах

гібридних загроз. Встановлено, що сучасні гібридні загрози поєднують технічні кібератаки, інформаційно-психологічний вплив, соціальну інженерію та інші інструменти дестабілізації. Їх основною метою є порушення стабільності функціонування критичної інфраструктури, зниження рівня довіри до державних інституцій та створення кризових ситуацій в умовах війни.

У результаті аналізу встановлено, що традиційні підходи до кіберзахисту, засновані виключно на використанні окремих технічних засобів захисту, є недостатньо ефективними для протидії складним багаторівневим атакам [36]. Це обумовлює необхідність переходу до комплексної системи управління кібербезпекою, побудованої за доменним принципом. Доменний підхід дозволяє структуровано організувати процеси захисту, розподілити функції безпеки між окремими напрямами та реалізувати багаторівневу модель кіберзахисту підприємства.

Також ефективність системи кібербезпеки залежить не лише від технічних засобів захисту, а й від узгодженості управлінських процесів, постійного моніторингу подій безпеки, своєчасного управління вразливостями та готовності підприємства до реагування на інциденти. Комплексний підхід дозволяє підвищити рівень кіберстійкості підприємства та забезпечити безперервність його функціонування навіть в умовах підвищеного зовнішнього тиску.

Для підприємств енергетичного сектору питання забезпечення кіберстійкості мають особливе значення, оскільки компрометація інформаційних, мережевих або технологічних систем може призвести до порушення безперервності енергопостачання та негативних наслідків для критичної інфраструктури держави. Отримані результати формують теоретичну основу для подальшого аналізу актуальних кіберзагроз та оцінювання рівня кіберризиків підприємства у другому розділі роботи.

Розділ 2 АНАЛІЗ ЗАГРОЗ ТА ОЦІНКА СТАНУ КІБЕРБЕЗПЕКИ ПІДПРИЄМСТВ В УМОВАХ ГІБРИДНОЇ ВІЙНИ

2.1. Моніторинг та аналіз актуальних гібридних кіберзагроз підприємства

Упродовж наступних років кібератаки стали більш скоординованими та цілеспрямованим безпосередньо на об’єкти критичної інфраструктури [38].

Якщо у 2018–2019 рр. переважали фішингові кампанії, спроби кібершпигунства та пошук вразливостей у корпоративних мережах енергетичних підприємств, то вже у 2020 році спостерігалося суттєве зростання кількості атак через масовий перехід на віддалені формати роботи та збільшення кількості сервісів дистанційного доступу.

У 2021 році кіберактивність щодо енергетичного сектору України переважно мала локальний та розвідувальний характер для підготовки до подальших масштабних операцій. Упродовж року було офіційно зафіксовано лише 2 масштабні DDoS-атаки на енергетичну інфраструктуру, хоча загальна кількість кіберінцидентів та спроб втручань залишалася значною.

Після початку повномасштабної війни у 2022 році інтенсивність кібератак різко зросла. За словами заступника міністра енергетики України Фаріда Сафарова, лише за перші 47 днів війни було зафіксовано понад 200 тисяч випадків негативної кібернетичної активності щодо енергетичної інфраструктури, а також близько 50 спроб DDoS-атак на енергетичний сектор [37].

У 2023 році було зафіксовано близько 55 атак на енергооб’єкти України. У 2024 році енергетичний сектор продовжив залишатися однією з ключових цілей кібератак — кількість зафіксованих інцидентів зросла до 127 [39]. Водночас за даними CERT-UA, у 2025 році кількість кіберінцидентів в енергетичній галузі становила вже 279 випадків, що підтверджує подальше зростання активності зловмисників [40].

Для візуалізації зміни інтенсивності кібератак на енергетичний сектор України на рис. 2.1 представлено динаміку розвитку кіберзагроз у 2021–2025 рр.

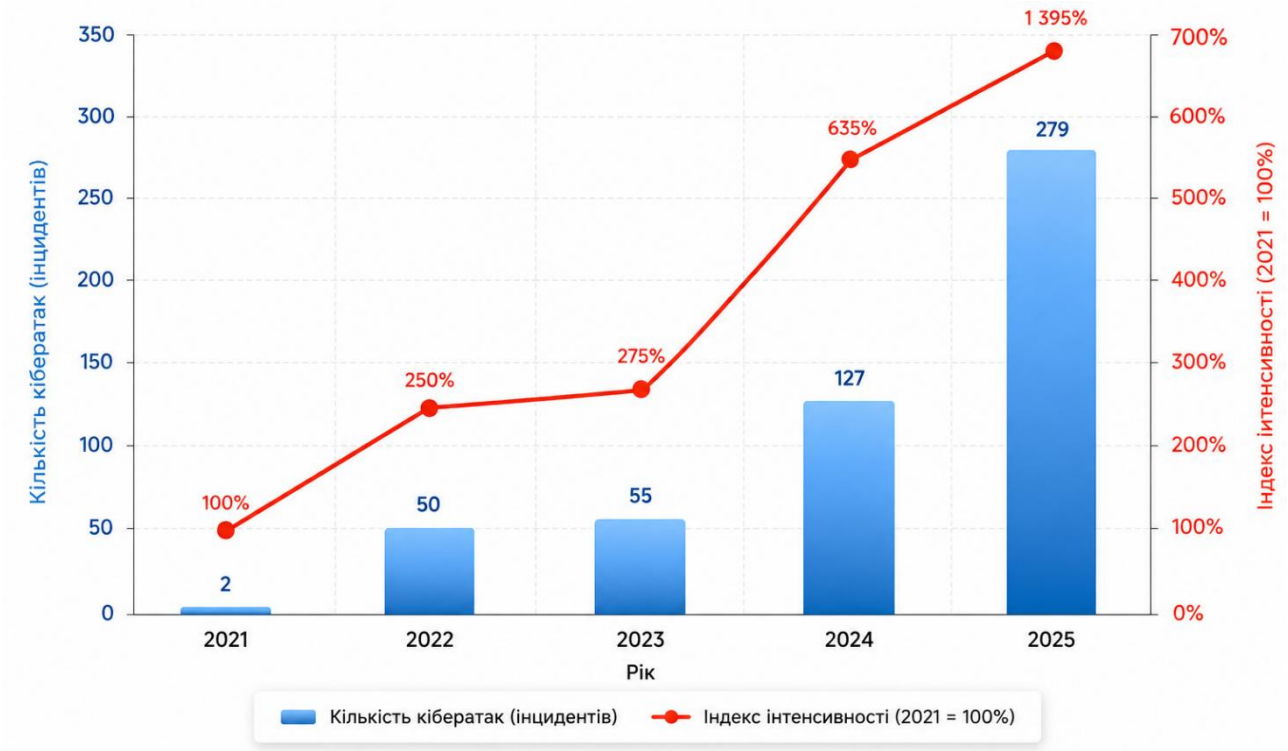

Рис. 2.1. Аналіз динаміки кібератак на енергетичний сектор України за 2021–2025 рр.

Джерело: складено автором за даними Forbes Ukraine, CERT-UA та Держспецзв'язку України [37, 38, 39, 40, 20]

Щоб оцінити реальні масштаби загрози, варто простежити, як змінювалися кількість та внутрішня логіка цих атак впродовж останніх років. Це дає змогу чітко побачити різницю між періодом відносного спокою та фазою повномасштабного протистояння.

Таким чином, характер кібератак на енергетичний сектор України впродовж останніх років суттєво змінився. Якщо раніше переважали переважно окремі фішингові кампанії та спроби кібершпигунства, то після 2022 року атаки стали більш масштабними, системними та спрямованими безпосередньо на порушення роботи об'єктів критичної інфраструктури.

Підприємства енергетичного сектору, як об’єкти критичної інфраструктури (ОКІ), є пріоритетними цілями в умовах нестабільного безпекового середовища. Перехід енергетичної галузі до цифрових та екологічних рішень супроводжується зростанням кіберризиків. Енергетичні компанії дедалі більше залежать від цифрових технологій та сторонніх сервісів, а зловмисники використовують складність взаємопов’язаних компонентів для прихованого переміщення між сегментами архітектури та реалізації атак.

У межах дослідження розглядається узагальнена модель енергетичного підприємства України. З огляду на вимоги інформаційної безпеки та обмеження щодо розголошення критичної інформації в умовах воєнного стану, об’єкт представлений без деталізації конкретних систем.

Особливістю підприємств енергетичного сектору є поєднання технологічного сегмента OT (Operational Technology), який керує фізичними процесами виробництва (передачі та розподілу електроенергії) з традиційною IT-інфраструктурою (офісні мережі, бухгалтерія).

До складу типової моделі такого підприємства входять корпоративні мережі, серверне та мережеве обладнання, бази даних, телекомунікаційні, автоматизовані системи керування технологічними процесами (АСУ ТП/SCADA), механізми моніторингу та диспетчеризації.

Об’єкти захисту для підприємства:

— користувачі та облікові записи;

— персональні, службові, комерційні та технічні дані;

— серверне, мережеве та фізичне середовище;

— бази даних та програмне забезпечення;

— канали передачі даних і телекомунікаційні системи;

— автоматизовані системи управління технологічними процесами (АСУ ТП/SCADA);

— бізнес-процеси та механізми реалізації безперервності діяльності підприємства.

Зазначені об’єкти виступають основними цілями сучасних гібридних кіберзагроз для підприємств енергетичного сектору. З огляду на специфіку функціонування підприємства та характер гібридних конфліктів, найбільш актуальними є загрози, здатні одночасно впливати на інформаційні системи, мережеву інфраструктуру, персонал і технологічні процеси підприємства.

Нижче наведено табл. 2.1. узагальнення основних типів таких загроз:

Таблиця 2.1

Актуальні гібридні кіберзагрози для підприємства енергетичного сектору

Тип загрози	Мета	Об’єкт впливу	Можливі наслідки
Фішингові атаки	Компрометація облікових записів	Персонал підприємства	Несанкціонований доступ до систем
Ransomware/Wiper	Блокування або знищення даних	Сервери, бази даних	Зупинка бізнес-процесів
DDoS-атаки	Недоступність сервісів	Мережеві ресурси	Недоступність інформаційних середовищ
MITM-атаки	Перехоплення або підміна даних	Канали передачі даних	Компрометація конфіденційної інформації
Supply Chain Attacks	Компрометація через постачальників	ПЗ та підрядники	Порушення цілісності інфраструктури
Атаки на SCADA/АСУ ТП	Збій роботи технологічних систем	OT-інфраструктура	Порушення енергопостачання
Використання вразливостей нульового дня (Zero-Day)	Експлуатація невідомих вразливостей	Сервери, ПЗ	Компрометація та приховане проникнення в мережу
Координовані атаки (Kinetic-Cyber)	Синхронізуються з ракетними ударами	Системи захисту	Блокування відновлювальних робіт
Інформаційно-психологічні операції (ІПСО)	Створення паніки та дестабілізації	Персонал, інформаційні ресурси	Зниження довіри до енергетичного сектору

Продовження таблиці 2.1

Тип загрози	Мета	Об’єкт впливу	Можливі наслідки
Фізичний вплив на інфраструктуру	Виведення з ладу критичних елементів енергосистеми	Підстанції, серверні приміщення, обладнання	Пошкодження або зупинка енергетичних процесів

Джерело: складено на основі аналітичних звітів [2, 4, 25]

Одним із найбільш відомих прикладів скоординованих атак на енергетичний сектор України стали атаки угруповання Sandworm із використанням ШПЗ Industroyer та Industroyer2, спрямованого на ураження енергетичного комплексу та структур керування технологічними процесами [23, 25].

Особливістю таких операцій є їх тривалий та прихований характер. Зловмисники можуть протягом тривалого часу перебувати у внутрішній мережі підприємства, здійснюючи розвідку IT- та OT-середовища, аналіз архітектури мережі й підготовку до активної фази атаки.

Для закріплення та прихованого переміщення мережею використовуються PowerShell-скрипти, механізми групових політик (GPO), SSH-тунелі та інші легітимні інструменти адміністрування [23, 24]. Це дозволяє зловмисникам обходити традиційні засоби захисту, ускладнювати виявлення шкідливої активності та створювати умови для одночасного впливу на серверне, мережеве й технологічне середовище підприємства.

Важливим елементом формування цифрової стійкості ОКІ є постійний моніторинг, що охоплює не лише події інформаційної безпеки, а й загальний технічний стан IT- та OT-інфраструктури. Це дозволяє вчасно виявляти аномальну поведінку, контролювати привілейований доступ та реагувати на приховані загрози [24].

На досліджуваному підприємстві моніторинг інфраструктури реалізується переважно на базовому рівні та спрямований на контроль

доступності серверів, мережевого обладнання і окремих сервісів. Для цього можуть використовуватись системи моніторингу, які дозволяють централізовано контролювати працездатність серверів, інфраструктури та отримувати повідомлення про критичні збої.

Водночас наявний підхід орієнтований переважно на технічний контроль працездатності систем і не забезпечує повноцінного аналізу подій кібербезпеки, поведінкових аномалій користувачів та кореляції подій між IT- і OT-сегментами.

Енергетичний сектор залишається головним фронтом сучасного протистояння, де кібератаки стають дедалі складнішими та синхронізованими з фізичним чинником. Це вимагає від підприємства переходу до проактивного моніторингу та побудови ешелонованого захисту, оцінку якого ми проведемо в наступному підрозділі через аналіз ризиків за доменами безпеки.

2.2. Оцінка управління кібербезпекою за доменами безпеки

Для комплексного аналізу стану кібербезпеки енергетичного сектору доцільно використовувати доменний підхід, який дозволяє оцінювати параметри захищеності окремих напрямів функціонування підприємства. Цей підхід реалізує можливість виявлення найбільш вразливих елементів інформаційної структури та визначення пріоритетних ризиків.

Аналіз проводиться на основі рекомендацій міжнародних стандартів та фреймворків у сфері кібербезпеки, а також підходів до оцінки кіберстійкості CRR (Cyber Resilience Review) і CRI (Cyber Risk Index).

Оцінка доменів безпеки дозволяє визначити стан готовності підприємства до загроз інформаційним системам, виявити найбільш вразливі елементи архітектури захисту та встановити пріоритетні напрями посилення стійкості в умовах кризової ситуації.

Узагальнений аналіз доменів безпеки, головних векторів атак та пов’язаних із ними ризиків і вразливостей наведено в табл. 2.2.

Таблиця 2.2.

Аналіз доменів безпеки, векторів гібридних атак та вразливостей підприємства

Код	Домен безпеки	Інструменти та вектори гібридних атак	Ризики, проблеми та вразливості підприємства
R1	Governance, Risk & Compliance (GRC)	Нормативний тиск, атаки на процеси прийняття рішень, дезінформаційний вплив	Формальний підхід до управління ризиками, слабка адаптація політик безпеки нових викликів, неактуальні сценарії реагування
R2	Asset Management	Використання необлікованих активів, підключення несанкціонованих пристроїв, розвідка	Часткова інвентаризація активів, складність виявлення несанкціонованих пристроїв та застарілих компонентів системи
R3	Security Architecture	Атаки на взаємодію IT та OT середовищ, експлуатація архітектурних недоліків	Неповна сегментація мереж, слабкі архітектурні бар'єри між корпоративним та технологічним середовищами, MFA
R4	Identity & Access Management (IAM)	Фішинг, brute force-атаки, викрадення облікових даних	Компрометація облікових записів, слабкі парольні політики, відсутність MFA, надлишкові права доступу
R5	Network & Infrastructure Security	DDoS-атаки, MITM-атаки, мережева розвідка, сканування та експлуатація вразливостей мережевих протоколів	Недостатній контроль мережевого трафіку, відсутність ефективної сегментації мережі, ризик компрометації мережевої структури, недостатній захист OT-мереж
R6	Data Security	Впровадження програм-вимагачів (Ransomware), викрадення даних (data exfiltration), несанкціонований доступ	Ризик витоку та втрати важливої та конфіденційної інформації, недостатній захист резервних копій
R7	Application Security & Supply Chain Security	Exploitation вразливостей ПЗ, supply chain attacks, компрометація сторонніх компонентів, атаки на API та вебзастосунки	Використання вразливого або неперевіреного стороннього ПЗ, недостатній контроль оновлень

Продовження таблиці 2.2.

Код	Домен безпеки	Інструменти та вектори гібридних атак	Ризики, проблеми та вразливості підприємства
R8	Security Operations (Monitoring & Incident Response)	Приховане перебування APT-груп у мережі, обходи SIEM-систем, приховування або модифікація журналів подій	Відсутність централізованого моніторингу подій (SOC/SIEM), складність оперативного виявлення інцидентів, недостатня швидкість реагування
R9	Vulnerability Management	Експлуатація вразливостей нульового дня (Zero-day), атаки через невиправлені вразливості, компрометація через помилки конфігурації	Несвоєчасне оновлення систем, використання застарілого ПЗ, недостатній контроль процесів patch management, відсутність регулярного тестування на проникнення (pentest)
R10	Human Factor, Awareness & Physical Security	Фішинг, соціальна інженерія, insider threats, психологічні маніпуляції в межах ІПсО, несанкціонований фізичний доступ	Недостатній рівень кібергігієни персоналу, внутрішні загрози, слабкий контроль фізичного доступу, відсутність регулярних тренінгів та кібернавчань.

Джерело: складено на основі аналітичних звітів [2, 4, 25]

Проведений аналіз доменів безпеки показав, що найбільш вразливими для підприємства є напрями, пов’язані з управлінням доступом, мережевою безпекою, моніторингом подій та людським фактором. Особливу небезпеку становить взаємодія IT- та OT-середовищ, оскільки компрометація корпоративної інфраструктури може створити передумови для подальших наслідків на технологічний сегмент підприємства.

Для визначення рівня вразливості виявлених загроз проведено кількісне та якісне оцінювання ризиків інформаційної безпеки за кожним доменом безпеки.

Методологія кількісної та якісної оцінки ризиків

Оцінювання здійснюється відповідно до підходів стандартів ISO/IEC 27005 [6] та NIST SP 800-30 [32], згідно з якими рівень ризику визначається як добуток ймовірності реалізації загрози на ступінь її впливу на підприємство.

У межах роботи використовується класична модель «ймовірність – вплив» (Probability × Impact), відповідно до якої рівень ризику визначається за формулою [6, 32]:

$$R = P \cdot I \tag{2.1}$$

де R — рівень ризику;

P — ймовірність реалізації загрози;

I — вплив загрози на підприємство.

Для проведення оцінки використано адаптовану п’ятибальну шкалу, сформовану на базі міжнародних підходів. Зазначені стандарти визначають загальні принципи управління ризиками інформаційної безпеки, однак не встановлюють єдиної обов’язкової шкали оцінювання. У зв’язку з цим критерії оцінювання були адаптовані відповідно до специфіки підприємства та рівня важливості інформаційних активів.

Таблиця 2.3

Шкала оцінювання ймовірності реалізації загрози (P)

Значення	Характеристика
1	Малоймовірно
2	Низька ймовірність
3	Середня ймовірність
4	Висока ймовірність
5	Дуже висока ймовірність

Таблиця 2.4

Шкала оцінювання впливу загрози (I)

Значення	Характеристика
1	Незначний вплив
2	Низький вплив
3	Середній вплив
4	Високий вплив
5	Критичний вплив

Таблиця 2.5

Інтерпретація рівня кіберризику

Значення *R*	Рівень ризику
1-5	Низький
6-10	Середній
11-15	Значний
16-19	Високий
20-25	Критичний

Значення показника «Ймовірність» визначалося з урахуванням частоти реалізації відповідних типів атак, їх актуальності для енергетичного сектору та доступності механізмів реалізації загроз. Показник «Вплив» оцінювався за можливими наслідками для інформаційних систем, OT-сегмента, цілісності даних і стабільності роботи підприємства.

Для наочного представлення результатів оцінювання у табл. 2.6. наведено матрицю ризиків 5×5 для визначення рівня ризику за кожним сценарієм. Рівень ризику визначається як результат множення показників «Ймовірність» та «Вплив», встановлених на етапі аналізу ризиків [31, 36].

Таблиця 2.6

Матриця ризиків 5x5 для визначення рівня кіберризику

Критичний (5)	Середній (5)	Значний (10)	Високий (15)	Критичний (20)	Критичний (25)
Високий (4)	Низький (4)	Середній (8)	Значний (12)	Високий (16)	Критичний (20)
Середній (3)	Низький (3)	Середній (6)	Середній (9)	Значний (12)	Високий (15)
Низький (2)	Низький (2)	Низький (4)	Середній (6)	Середній (8)	Значний (10)
Незначний (1)	Низький (1)	Низький (2)	Низький (3)	Низький (4)	Середній (5)
	Малоймовірно (1)	Низька ймовірність (2)	Середня ймовірність (3)	Висока ймовірність (4)	Дуже висока ймовірність (5)

Для забезпечення обґрунтованості оцінювання рівня кіберризиків було використано метод якісного оцінювання ризиків (qualitative risk assessment) відповідно до рекомендацій ISO/IEC 27005 та NIST SP 800-30 [6, 32]. Формування значень показників «Ймовірність» (P) та «Вплив» (I) здійснювалось методом експертного оцінювання на основі аналізу сучасних кіберзагроз для енергетичного сектору, рекомендацій міжнародних стандартів, актуальних сценаріїв реалізації гібридних кіберзагроз в умовах воєнного стану, аналітичних матеріалів CERT-UA, ENISA та Держспецзв'язку України [4, 20, 25, 40].

Підхід до оцінювання критичності доменів безпеки також ґрунтується на положеннях Постанови Кабінету Міністрів України №518 від 19.06.2019 р. [3]. Результати кількісної та якісної оцінки кіберризиків за доменами безпеки наведено в табл. 2.7.

Таблиця 2.7

Матриця оцінки кіберризиків підприємства

Код	P	I	$R = P \times I$	Рівень ризику
R1	3	3	9	Середній
R2	3	4	12	Значний
R3	4	5	20	Критичний
R4	5	4	20	Критичний
R5	5	5	25	Критичний
R6	4	4	16	Високий
R7	4	4	16	Високий
R8	4	5	20	Критичний
R9	4	4	16	Високий
R10	4	4	16	Високий

Джерело: складено автором на основі експертного оцінювання, рекомендацій ISO/IEC 27005, NIST SP 800-30 та аналізу актуальних кіберзагроз [4, 6, 20, 25, 32, 40]

Для більш наочного представлення результатів оцінювання ризиків інформаційної безпеки за доменами безпеки підприємства побудовано радарну діаграму рис. 2.2, яка відображає рівень ризику для кожного домену комплексу управління кібербезпекою.

Отримані результати дозволяють визначити найбільш вразливі напрями підтримання безпеки та встановити пріоритетні області підвищення кіберстійкості підприємства в умовах військово-політичної нестабільності.

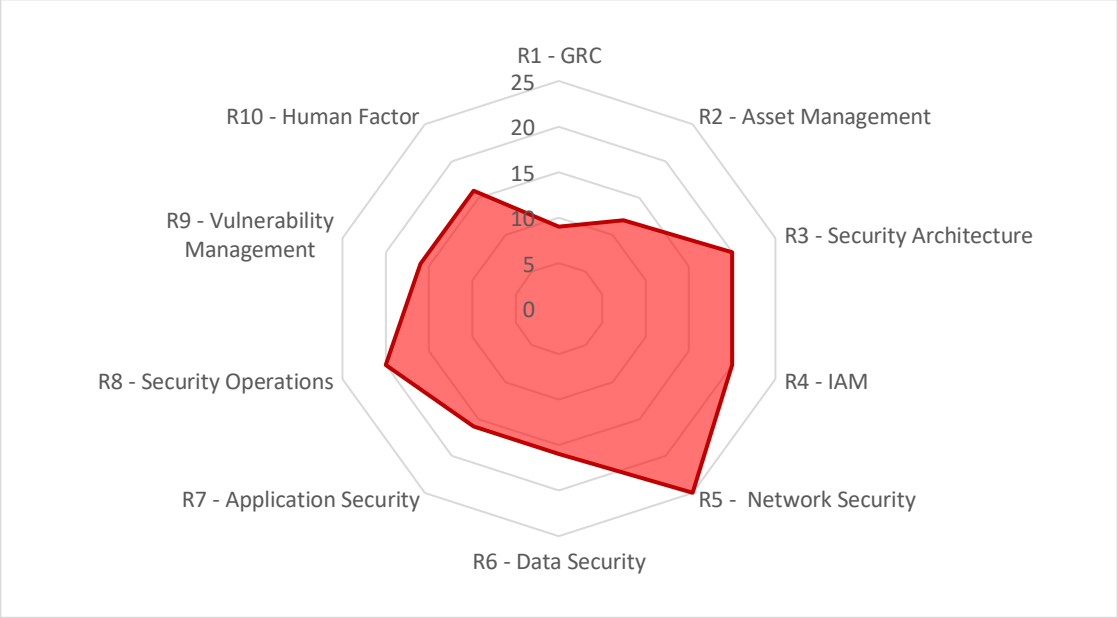

Рис. 2.2. Рівень кіберризиків за доменами безпеки управління кібербезпекою підприємства

Результати оцінювання демонструють, що найбільш критичними для підприємства є домени Security Architecture, Identity & Access Management (IAM), Network & Infrastructure Security та Security Operations (SOC). Саме ці напрями безпосередньо впливають на захищеність технологічного сегмента OT, стабільність функціонування мережевої інфраструктури та своєчасне виявлення кібератак.

Найвищий рівень ризику отримав домен Network & Infrastructure Security, оскільки компрометація мережевої інфраструктури або SCADA-систем може призвести до порушення технологічних процесів та зупинки енергопостачання.

Критичними також визначено домени IAM та SOC, адже компрометація облікових записів і відсутність належного моніторингу суттєво підвищують ризик прихованого проникнення зловмисників у внутрішню мережу підприємства.

Високий рівень ризику отримали домени Data Security, Application Security & Supply Chain Security та Vulnerability Management, які забезпечують підтримання стійкості інформаційної інфраструктури та зниження рівня експлуатації вразливостей.

Домени Governance, Risk & Compliance (GRC), Asset Management та Human Factor, Awareness & Physical Security отримали середній рівень ризику, оскільки виконують переважно організаційну та підтримуючу функцію. Їх компрометація не призводить до миттєвого збою роботи технологічного сегмента, однак може створювати передумови для реалізації складних кібератак.

Отримані результати дозволяють визначити домени, які потребують першочергового вдосконалення організаційних і технічних заходів безпеки. Сформований профіль кіберризиків є опорою для подальшого проєктування комплексної моделі управління кібербезпекою підприємства.

2.3. Аналіз впливу гібридних атак на безперервність бізнес-процесів підприємства

Енергетичні підприємства є одними з найбільш стратегічно важливих об’єктів для держави, тому кібератаки на такі системи можуть мати наслідки не лише для окремого підприємства, а й для стабільності енергосистеми загалом. Поєднання кібернетичного, фізичного та інформаційно-психологічного тиску створює додаткові ризики для безперервності технологічних процесів, стабільності енергопостачання та оперативного реагування на інциденти.

Результати оцінювання кіберризиків, наведені у підрозділі 2.2, показали, що найбільш критичними для досліджуваного підприємства є домени

мережевої безпеки, управління доступом, архітектури безпеки та моніторингу інцидентів. Саме порушення функціонування цих доменів безпосередньо впливає на допустимий час простою інформаційних і технологічних систем підприємства.

Для оцінювання можливих наслідків таких порушень використано методологію Business Impact Analysis (BIA) відповідно до вимог ISO 22301:2019 [33]. Даний підхід дозволяє визначити критичність бізнес-процесів, оцінити допустимий час їх простою та встановити цільові показники відновлення інформаційних і технологічних систем після інцидентів.

Для кількісної оцінки параметрів безперервності бізнес-процесів енергетичного підприємства в умовах гібридної війни розраховано цільовий час відновлення (RTO) та цільову точку відновлення (RPO). Розрахунок базується на введенні Коефіцієнта гібридної загрози (K_m), який враховує синергетичний ефект від одночасних кібератак (наприклад, із застосуванням деструктивного ПЗ типу Wiper) та кінетичних ударів по об’єктах критичної інфраструктури.

У звичайних умовах підприємства керуються стандартними міжнародними практиками ISO 22301:2019, ISO/IEC 27031:2025 (Cybersecurity - Information and communication technology readiness for business continuity) [33, 26]. Проте реалії гібридної війни вимагають суттєвого скорочення часових меж відновлення для забезпечення життєздатності енергосистеми.

Нижче наведено зведену таблицю розрахунків та порівняння отриманих результатів із загальноприйнятими нормативними значеннями.

Таблиця 2.8

Аналіз впливу на безперервність бізнес-процесів (BIA) за доменами безпеки

Код	Домен	Норматив RTO	Фактично RTO	Норматив RPO	Фактично RPO	Δ - різниця між факт. І норматив., год
R1	GRC	24 год.	16 год.	24 год.	16 год.	8 год.

Продовження таблиці 2.8

Код	Домен	Норматив RTO	Фактично RTO	Норматив RPO	Фактично RPO	Δ - різниця між факт. І норматив., год
R2	Asset Management	6 год.	4 год.	12 год.	8 год.	2 год.
R3	Security Architecture	3 год.	2 год.	2 год.	1 год.	1 год.
R4	IAM	0,5 год.	0,33 год.	0,3 год.	0,17год.	0,17 год.
R5	Network Security	2 год.	1,33 год.	4 год.	2,67 год.	0, 67 год.
R6	Data Security	4, 0 год.	2,67 год.	1,0 год.	0,67 год.	1,33 год.
R7	Application Security	24 год.	16 год.	12 год.	8 год.	8 год.
R8	Security Operations	1,5 год.	1 год.	0,1 год.	0,05 год.	0,5 год.
R9	Vulnerability Management	24 год.	16 год.	24 год.	16 год.	8 год.
R10	Human Factor	3 год.	2 год.	4 год.	2,67 год.	1 год.

Джерело: складено автором на основі положень [26, 33]

Аналіз отриманих результатів демонструє, що в умовах гібридної війни допустимі часові межі відновлення інформаційних і технологічних систем суттєво скорочуються порівняно зі стандартними нормативними значеннями. Найбільше стиснення часових вікон спостерігається у доменах Identity & Access Management (IAM), Security Operations та Network Security, оскільки їх функціонування безпосередньо впливає на доступність систем керування, мережевої інфраструктури та засобів моніторингу безпеки.

Отримані значення RTO та RPO підтверджують, що в умовах підвищеного рівня гібридних загроз підприємство потребує більш швидкого відновлення критичних сервісів, ніж це передбачено класичними підходами мирного часу. Особливо це стосується систем диспетчеризації, моніторингу мережевої активності та механізмів контролю доступу, порушення роботи яких може спричинити каскадне поширення інциденту на суміжні елементи інфраструктури.

Таким чином, результати BIA свідчать про необхідність впровадження адаптивної системи управління кібербезпекою, здатної забезпечити безперервність функціонування підприємства навіть в умовах комплексного поєднання кібернетичних і фізичних деструктивних впливів.

Операційні, фінансові та каскадні наслідки для бізнес-процесів підприємства

Дестабілізаційні чинники на такі підприємства можуть спрямовуватись одночасно на корпоративну IT-інфраструктуру, технологічний сегмент (OT) та невід'ємні бізнес-процеси. У більшості випадків наслідки однієї атаки не обмежуються окремою системою, а поступово поширюються на інші елементи архітектури, створюючи так званий «каскадний ефект» [34].

Порушення диспетчеризації та технологічного управління Одним із найбільш небезпечних наслідків є компрометація корпоративної мережі з подальшим поширенням атаки на технологічний сегмент підприємства. Подібні дії призводять до аварійних відключень споживачів, технологічних пошкоджень дорогого силового обладнання (трансформаторів) та тривалих локальних блекаутів.

Параліч корпоративної діяльності та фінансові збитки

Використання програм-вимагачів (Ransomware) чи шкідливого ПЗ для знищення даних (Wipers) призводить до повної втрати доступності IT-систем. Зупинка ERP-систем, електронного документообігу та внутрішніх інформаційних ресурсів суттєво ускладнює координацію роботи між підрозділами підприємства. У результаті виникає «каскадний ефект», коли

порушення функціонування одного життєво важливого активу поступово впливає на фінансову діяльність, логістику, диспетчеризацію та аварійно-відновлювальні процеси підприємства.

Уразливість IT- та OT-середовищ

На основі положень міжнародного стандарту IEC 62443 [35] більшість операційних ризиків підприємства зумовлена архітектурними недоліками. Відсутність сегментації мереж дозволяє зловмисникам здійснювати горизонтальне переміщення (lateral movement) від компрометованого IT-сегмента (наприклад, через фішинг) безпосередньо до контурів управління SCADA. Ситуацію погіршує брак систем класу SIEM та постійного аналізу мережевої активності, через що складні цілеспрямовані загрози (APT) можуть залишатися непоміченими протягом тижнів.

Масштабування наслідків до державного рівня

Енергетична компанія є невід'ємним елементом Об'єднаної енергетичної системи (ОЕС) України, тому локальні інциденти швидко трансформуються у загрози національній безпеці:

— Регіональні блекаути, скоординовані атаки на об’єкти енергетичної інфраструктури здатні порушувати баланс в ОЕС та створювати ризик масштабних регіональних блекаутів.

— Порушення роботи важливих сервісі, тривале припинення електропостачання має негативний ефект на транспортну структуру, системи зв’язку, водопостачання, медичні заклади та інші.

— Економічні втрати та зупинка промислових споживачів знижує обсяги виробництва та податкових надходжень до державного бюджету в умовах воєнного стану.

— Інформаційно-психологічний тиск, кібератаки синхронізуються із дезінформацією для провокування паніки серед населення та підриву довіри до державних органів та стратегічних підприємств.

Таким чином, наслідки гібридних атак виходять за межі окремого підприємства та можуть впливати на функціонування критичної

інфраструктури держави. Це обумовлює необхідність впровадження адаптивної системи управління кібербезпекою для забезпечення безперервності бізнес-процесів і підвищення кіберстійкості підприємства.

Висновки до розділу 2

Проведений аналіз показав, що за останні роки характер кібератак на енергетичний сектор України суттєво змінився — від окремих фішингових кампаній та спроб кібершпигунства до масштабних скоординованих атак на об’єкти критичної інфраструктури. Особливу небезпеку становлять атаки, які поєднуються з фізичним впливом на енергетичні об’єкти та спрямовані на порушення стабільності функціонування IT- і OT-середовищ підприємства.

Оцінка стану кібербезпеки за доменами безпеки дозволила визначити найбільш критичні напрями для підприємства. Найвищий рівень ризику отримали мережева та інфраструктурна безпека, архітектура захисту, управління доступом і моніторинг інцидентів. Встановлено, що недостатня сегментація між корпоративним та технологічним середовищами, відсутність повноцінного моніторингу подій безпеки та слабкий контроль доступу створюють умови для поширення атак усередині інфраструктури.

Дослідження впливу гібридних атак підтвердило, що кіберінциденти можуть спричиняти каскадні наслідки для технологічних процесів, диспетчеризації та стабільності енергопостачання. Отримані результати дозволили сформувати профіль кіберризиків підприємства та визначити пріоритетні напрями посилення захисту, що стало основою для розроблення системи управління кібербезпекою у третьому розділі роботи.

Розділ 3 ПРОЄКТУВАННЯ ТА ІМІТАЦІЙНЕ МОДЕЛЮВАННЯ СИСТЕМИ УПРАВЛІННЯ КІБЕРБЕЗПЕКОЮ ПІДПРИЄМСТВА ЗА ДОМЕНАМИ БЕЗПЕКИ В УМОВАХ ГІБРИДНОЇ ВІЙНИ

3.1. Архітектура системи управління кібербезпекою підприємства за доменами безпеки в умовах гібридної війни

Підприємства енергетичного сектору України постійно перебувають під впливом складних кіберзагроз, спрямованих на ускладнення функціонування роботи критичної інфраструктури. Проведений у другому розділі аналіз показав, що найбільш критичними ризиками для підприємства залишаються компрометація облікових записів, недостатня сегментація мережі, наявність вразливостей у мережевій інфраструктурі, недостатній рівень моніторингу подій безпеки та людський фактор. Тому успішна атака на один із сегментів може призвести до каскадного поширення інциденту та порушення безперервності бізнес-процесів.

Основою запропонованої системи управління кібербезпекою є доменний підхід, який передбачає розподіл механізмів захисту за окремими функціональними напрямами безпеки. Такий підхід дозволяє комплексно охопити процеси управління ризиками, контролю доступу, моніторингу подій безпеки, захисту мережевої інфраструктури, даних та технологічних систем підприємства.

Система управління кібербезпекою включає десять взаємопов’язаних доменів безпеки: GRC, Asset Management, Security Architecture, IAM, Network Security, Data Security, Application Security, Security Operations, Vulnerability Management, а також Human Factor. Кожен із доменів виконує окремі функції захисту та взаємодіє з іншими компонентами системи, формуючи єдину багаторівневу архітектуру кіберзахисту.

Важливим компонентом системи управління кібербезпекою є забезпечення відповідності нормативно-правовим вимогам та міжнародним стандартам у сфері захисту об’єктів критичної інфраструктури.

Формування системи управління кібербезпекою здійснюється з урахуванням вимог Закону України «Про критичну інфраструктуру», нормативних документів Держспецзв’язку та сучасних міжнародних стандартів у сфері кібербезпеки [22, 20]. Особлива увага приділяється впровадженню підходів безперервного моніторингу та підвищення кіберстійкості об’єктів критичної інфраструктури відповідно до рекомендацій ISO/IEC 27001, ISO/IEC 27005, IEC 62443 та NIST Cybersecurity Framework [13, 6, 35, 15].

Використання зазначених нормативних документів та стандартів дозволяє забезпечити комплексний підхід до управління кіберризиками, підвищити рівень кіберстійкості підприємства та адаптувати механізми захисту до сучасних гібридних загроз.

Запропонована система управління кібербезпекою функціонує відповідно до циклу PDCA (Plan–Do–Check–Act) [14], який забезпечує безперервне вдосконалення процесів кіберзахисту та адаптацію системи до змінного ландшафту кіберзагроз.

Використання даного підходу дозволяє систематизувати управління кіберризиками, забезпечити контроль ефективності впроваджених механізмів захисту та своєчасно адаптувати систему безпеки до нових гібридних загроз.

На етапі Plan (планування) здійснюється оцінювання кіберризиків, визначення критичних активів підприємства, формування політик безпеки та процедур реагування на інциденти. Особлива увага приділяється процесам управління ризиками, комплаєнсу та класифікації інформаційних активів.

Етап Do (впровадження) передбачає реалізацію організаційних і технічних механізмів захисту, зокрема сегментацію IT/OT-середовищ, впровадження MFA, PAM, SIEM, IDS/IPS, резервного копіювання та інших компонентів доменної моделі кіберзахисту.

На етапі Check (контроль) здійснюється постійний моніторинг подій безпеки, аналіз журналів подій, контроль вразливостей та аудит ефективності засобів захисту. Основними компонентами цього рівня виступають SOC, SIEM та механізми централізованого моніторингу.

Етап Act (удосконалення) орієнтований на аналіз інцидентів, оновлення політик безпеки, усунення вразливостей, вдосконалення сценаріїв реагування та проведення навчання персоналу. Реалізація даного етапу сприяє підтриманню кіберстійкості підприємства та забезпечує адаптацію до змінних загроз.

На рисунку 3.1 представлено цикл функціонування запропонованої системи управління кібербезпекою відповідно до моделі PDCA [14].

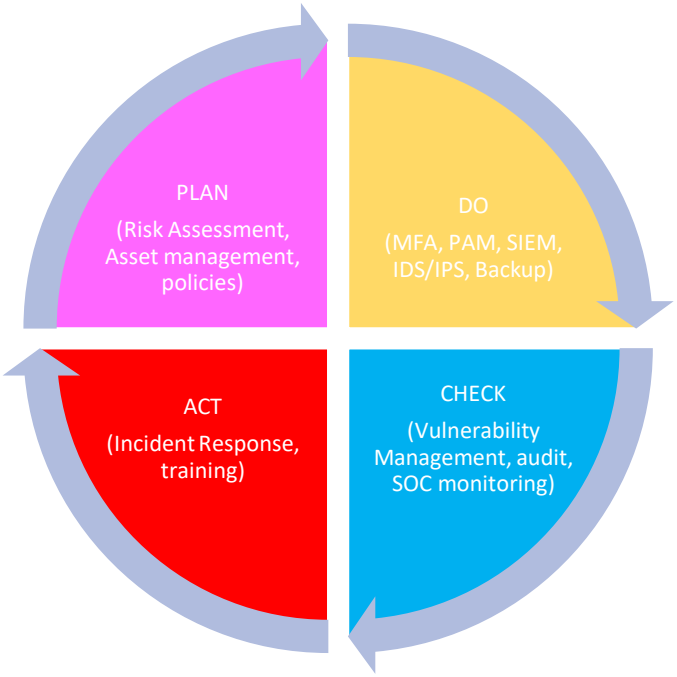

Рис. 3.1. Цикл функціонування системи управління кібербезпекою PDCA

Джерело: розроблено автором на основі циклу Демінга (PDCA) та ISO/IEC 27001:2022 [13, 14]

Архітектура системи управління кібербезпекою побудована за принципом багаторівневого захисту (Defense in Depth), рекомендованого міжнародними стандартами NIST SP 800-53 та IEC 62443 для захисту критичної інфраструктури [16, 35]. Такий підхід обумовлений специфікою

функціонування об’єктів критичної інфраструктури, високим рівнем сучасних гібридних загроз та він дозволяє мінімізувати ризик каскадного поширення інцидентів та підвищити рівень кіберстійкості в умовах гібридних загроз.

У межах архітектури системи управління кібербезпекою кожен домен виконує окремі функції захисту та взаємодіє з іншими компонентами системи, формуючи єдине середовище кіберзахисту. Основні механізми та функції доменів безпеки наведено на рис. 3.2.

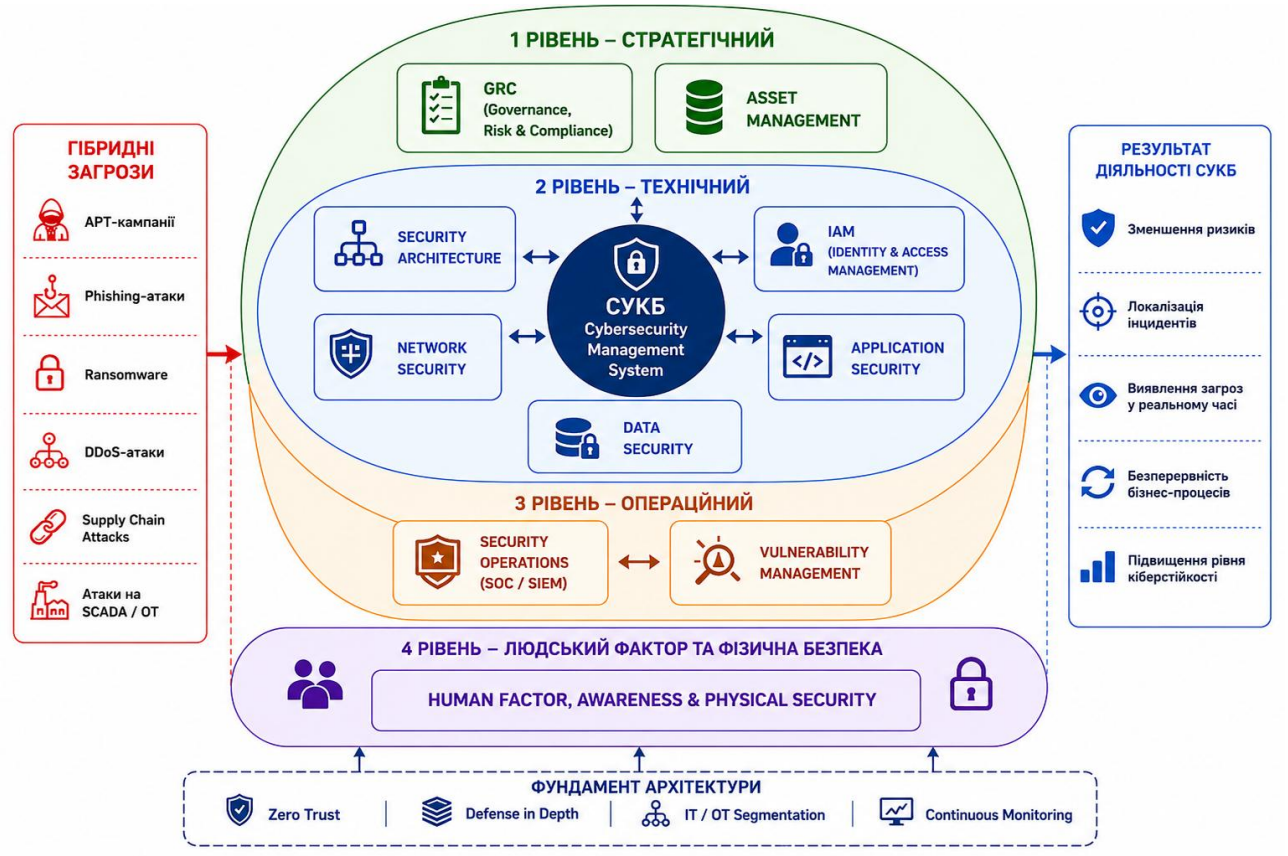

Рис. 3.2. Архітектура системи управління кібербезпекою підприємства за доменами безпеки

Нижче наведено детальний опис кожного домену безпеки відповідно до встановленої функціональної структури управління та протидії гібридним загрозам.

1. Governance, Risk & Compliance (GRC) (Управління, ризики та комплаєнс)

Перекриває відсутність централізованого стратегічного планування, а також невідповідність внутрішніх нормативних актів вимогам законодавства України у сфері захисту критичної інфраструктури під час воєнного стану,

нормативно-правовий хаос, комбінований адміністративно-інформаційний тиск ворога.

Комплекс заходів:

— Впровадження динамічного управління ризиками в умовах невизначеності, перехід від статичного оцінювання ризиків до безперервного моделювання загроз (Continuous Threat Modeling) на основі підходів ISO/IEC 27005 та Risk IT (ISACA) [6, 36]. Сценарії ризиків включають комбіновані удари (кібератака на підстанцію одночасно з ракетним обстрілом). Проведення регулярних внутрішніх аудитів.

— Розробка та адаптація планів BCP/DRP (Бізнес-безперервність та аварійне відновлення) [33]. Створення інструкцій для персоналу щодо переходу диспетчерських пунктів у повністю автономний (ізольований) режим роботи у разі компрометації корпоративного сегмента.

— Забезпечення повної відповідності вимогам закону України «Про критичну інфраструктуру» [22], Держспецзв'язку [20], нормативно-правовим актам та впровадження найкращих світових практик серії ISO/IEC 27001 [13], IEC 62443 та NIST Cybersecurity Framework [35, 15] як методологічна основа управління ризиками та організації процесів кіберзахисту.

Який результат для підприємства: Формується централізована модель управління кібербезпекою, що дозволяє швидко ухвалювати управлінські рішення, координувати дії під час кризових ситуацій та розподіляти ресурси відповідно до пріоритетів ризиків.

З ким взаємодіє: Усі домени безпеки, керівництво підприємства, SOC, юридичний відділ, державні регулятори (ДССЗЗІ, Кіберполіція, Міненерго), CERT-UA.

2. Asset Management (Управління активами)

Закриває такі цільові загрози як розвідка зловмисників через відкриті незахищені ресурси підприємства, використання несанкціонованого або застарілого програмного забезпечення (Shadow IT/Shadow OT), підключення

несанкціонованих пристроїв та використання необлікованих систем, відсутність чіткої класифікації критичності обладнання для бізнес-процесів. Комплекс заходів:

— Автоматизована інвентаризація IT та OT середовищ. Впровадження спеціалізованих систем класу пасивного моніторингу *Passive Network Monitoring* для OT-сегмента, які дозволяють ідентифікувати промислові активи без ризику порушення їхньої роботи активним скануванням.

— Активне сканування (Active Asset Discovery). Застосовується виключно в IT-сегменті (офісна мережа, сервери корпоративних сервісів) за допомогою сканерів уразливостей.

— Контроль підключення зовнішніх пристроїв. Впровадження технології контролю мережевого доступу NAC (Network Access Control). Будь-який новий пристрій при спробі підключення до порту комутатора або Wi-Fi мережі автоматично поміщається в карантинну VLAN. На рівні кінцевих точок (Endpoint) силами рішень класу *EDR/XDR* блокується використання сторонніх USB-пристроїв.

Який результат для підприємства: Підприємство отримує повну карту цифрової інфраструктури та розуміння критичних вузлів, що дозволяє швидше локалізувати атаки та мінімізувати площу компрометації. Суттєве зменшення поверхні атаки (Attack Surface Reduction), що ускладнює реалізацію прихованого проникнення та горизонтального поширення атак у мережі підприємства.

Взаємодіє з IT-департаментом, інженерами АСУ ТП, SOC, а також доменами Security Architecture та Vulnerability Management.

3. Security Architecture (Архітектура безпеки)

Домен спрямований на усунення хаотичної побудови мережевої інфраструктури, відсутності меж безпеки між корпоративним (IT) та технологічним (OT/SCADA) сегментами, а також використання незахищених протоколів зв’язку. Які гібридні загрози перекриває: каскадне поширення шкідливого ПЗ з офісних комп'ютерів безпосередньо до систем управління

турбінами чи підстанціями (SCADA), поширення ransomware між сегментами, MITM-атаки, атаки Sandworm/Industroyer-подібного типу.

Які механізми впроваджуються:

— Розподіл інфраструктури на ізольовані зони безпеки відповідно до стандарту IEC 62443 [35]. Обов'язкове створення демілітаризованої зони (DMZ) між корпоративною мережею (IT) та технологічною мережею (OT/SCADA).

— Впровадження засобів криптографічного захисту каналів зв'язку, алгоритмів шифрування для диспетчерського зв'язку та передачі технологічних даних.

— Багаторівневий захист (Defense in Depth) [15, 16], архітектура проєктується таким чином, щоб зловмиснику для досягнення деструктивної мети необхідно було подолати серію незалежних бар'єрів захисту.

Який результат для підприємства: Створення стійкого цифрового каркаса підприємства, де компрометація одного сегмента чи комп'ютера не призводить до зупинки чи зламу всієї технологічної системи енергооб'єкта. Навіть в умовах активної фази кібератаки підприємство зберігає спроможність здійснювати критичні функції — диспетчеризацію, контроль частоти та потужності в енергомережі, запобігаючи системним блекаутам.

Взаємодіє з мережевими інженерами, архітекторами IT-систем, підрядниками з інтеграції ПЗ, а також доменами Network & Infrastructure Security, Identity & Access Management (IAM), Security Operations (SOC) та Vulnerability Management.

4. Identity & Access Management (IAM) (Управління доступом)

Яку проблему закриває: Слабкий контроль доступу, використання однакових паролів, надлишкові привілеї користувачів, відсутність контролю за діями адміністраторів та сторонніх інженерів, які обслуговують промислове обладнання.

Які гібридні загрози перекриває: Фішинг, компрометація облікових записів адміністраторів та диспетчерів, несанкціонований доступ.

Несанкціонований доступ до диспетчерських пультів з використанням скомпрометованих (вкрадених) облікових даних, атаки типу "man-in-the-middle" (перехоплення сесій), внутрішні диверсії з боку завербованого або ображеного персоналу.

Які механізми впроваджуються:

— Обов'язкове впровадження MFA для всіх без винятку корпоративних облікових записів, а також для віддалених підключень інженерів. Пріоритет надається апаратним ключам захисту (YubiKey), стійким до фішингу через перехоплення сесій.

— Впровадження PAM-систем (Privileged Access Management), усі дії адміністраторів IT-систем та інженерів АСУ ТП повинні здійснюватися виключно через PAM-шлюз із обов’язковим записом сесій, контролем введених команд та автоматичною ротацією паролів.

— Рольове управління доступом RBAC (Role-Based Access Control). Права чітко розділяються по наданим повноваженням і ролям.

— Журналювання та аудит дій користувачів. Логи з контролерів домену, PAM-систем, операційних систем та SCADA-середовища передаються до централізованого сховища журналів подій (SIEM). Це забезпечує можливість виявлення аномальної активності та захист журналів від несанкціонованої модифікації [29].

Який результат для підприємства: Повний контроль над тим, хто, коли і з якою метою отримав доступ до будь-якого ресурсу підприємства; унеможливлення використання чужих чи підроблених облікових записів. Значно знижується ризик несанкціонованого доступу до SCADA, серверів та корпоративних систем навіть у випадку компрометації пароля. Рольова модель та PAM-контроль обмежують можливості зловмисного інсайдера завдати миттєвої масштабної шкоди критичним процесам.

З ким взаємодіє: Відділ кадрів (HR), Security Operations (SOC), служба безпеки підприємства, адміністратори систем, кінцеві користувачі та інші домени.

5. Network & Infrastructure Security (Мережева та інфраструктурна безпека)

Спрямований на захист мережевої інфраструктури підприємства від перехоплення мережевого трафіку, зовнішнього втручання в роботу мережевого обладнання, DDoS-атак, діяльності хакерських APT-угруповань та несанкціонованого проникнення до SCADA-сегмента через незахищені мережеві порти.

Комплекс заходів:

— Встановлення міжмережевих екранів нового покоління (NGFW) з розгортання систем виявлення та запобігання вторгненням (IDS/IPS).

— Анти-DDoS рішення, підключення зовнішніх хмарних та операторських сервісів очищення трафіку для захисту публічних сервісів та каналів зв'язку ОКІ. Використання захищених VPN-каналів для віддаленого доступу до корпоративного та технологічного середовища.

Який результат для підприємства: Надійно захищений цифровий периметр та внутрішній мережевий простір підприємства, що забезпечує своєчасне виявлення, локалізацію та блокування мережевих атак ще на етапі їх реалізації.

З ким взаємодіє: Системні та мережеві адміністратори, провайдери зв'язку, домени IAM, Security Architecture та Security Operations (SOC).

6. Data Security (Безпека даних)

Яку проблему закриває: Зберігання конфіденційної інформації (схем мереж, паролів, персональних даних) без шифрування, відсутність резервування та неконтрольоване копіювання інформації на зовнішні носії.

Які гібридні загрози перекриває: шифрування та знищення даних вірусами-вимагачами (Ransomware) або деструктивними програмами-вайперами (Wipers), злиття службової інформації та карт критичних об'єктів для планування ракетно-дронових ударів.

Комплекс заходів:

— Реалізація стратегії резервного копіювання «3-2-1», що передбачає зберігання трьох копій даних на двох різних типах носіїв, одна з яких розміщується в ізольованому автономному сховищі.

— Впровадження систем запобігання витокам інформації DLP (Data Loss Prevention): Контроль та блокування спроб вивантаження критичної документації за межі захищеного контуру підприємства.

— Шифрування даних, застосування алгоритмів *AES-256* для баз даних SCADA.

Який результат для підприємства: Гарантія цілісності та доступності критично важливої інформації. Підприємство зберігає можливість швидкого відновлення критичних даних навіть після масштабної деструктивної атаки без втрати керованості технологічними процесами.

З ким взаємодіє: IT-департамент, фінансовий відділ, служба безпеки підприємства, а також домени Asset Management, Application Security & Supply Chain Security та Security Operations (SOC).

7. Application Security & Supply Chain Security (Безпека застосунків та ланцюга постачання)

Які проблеми закриває: Використання програмного забезпечення із прихованими вразливостями, неконтрольоване оновлення систем, надлишкові доступи зовнішніх вендорів і підрядників до внутрішніх мереж.

Які гібридні загрози перекриває: Атаки через ланцюг постачання (Supply Chain Attacks), впровадження шкідливих оновлень, компрометація систем через вразливості нульового дня (Zero-Day).

Які механізми впроваджуються:

— Обов’язкова верифікація та тестування оновлень у закритій пісочниці (Sandbox) перед розгортанням у продуктивному середовищі.

— Аналіз складу стороннього програмного коду (Software Bill of Materials — SBOM), а також проведення аудиту постачальників та підрядників щодо відповідності вимогам кібербезпеки.

Який результат для підприємства: Мінімізація ризику імпорту кіберзагроз ззовні разом із купованим програмним забезпеченням; повний контроль над діями та оновленнями від сторонніх розробників.

З ким взаємодіє: Відділ закупівель, зовнішні розробники та постачальники, системні інтегратори, домен Vulnerability Management.

8. Security Operations (Monitoring & Incident Response) (Моніторинг та реагування на інциденти)

Яку проблему закриває: Пізнє виявлення кібератак (коли зловмисник місяцями перебуває в мережі), відсутність централізованого моніторингу та автоматизованого реагування. Домен також перекриває складні багатовекторні APT-атаки, які маскуються під легітимну діяльність користувачів, а також тривалі приховані кібератаки, спрямовані на шпигунство або підготовку до диверсійних дій.

Які механізми впроваджуються:

— Створення SOC (Security Operations Center) та забезпечення цілодобового моніторингу подій безпеки.

— Впровадження SIEM та SOAR систем для збору та кореляції логів, а також використання підходів UEBA/UBA (User and Entity Behavior Analytics) для виявлення аномальної поведінки користувачів та прихованої активності зловмисників у мережі [27, 28].

— Розробка сценаріїв реагування на інциденти (Playbooks).

— Кіберрозвідка (Cyber Threat Intelligence), інтеграція актуальних загроз від державних органів та міжнародних партнерів для проактивного пошуку слідів шкідливого ПЗ (Threat Hunting).

— Для підвищення ефективності моніторингу та реагування на кіберінциденти можуть застосовуватися підходи MITRE ATT&CK Framework для класифікації тактик і технік зловмисників [5].

Який результат для підприємства: Скорочення часу виявлення атаки з місяців до кількох хвилин, наявність оперативної групи реагування на кіберінциденти.

З ким взаємодіє: Усі технічні підрозділи підприємства, чергові диспетчери енергомереж, CERT-UA та всі домени.

9. Vulnerability Management (Управління вразливостями)

Яку проблему закриває: Несвоєчасне встановлення оновлень безпеки на серверах та робочих станціях, наявність невиправлених вразливостей у ПЗ та ОС, хаотичний процес патчингу. Які гібридні загрози перекриває: Автоматизований злам систем хакерськими сканерами та ботнетами, експлуатація відомих критичних уразливостей для отримання повних прав адміністратора в мережі підприємства.

Які механізми впроваджуються:

— Ризик-орієнтований підхід, пріоритезація закриття вразливостей на основі метрик CVSS v3 та реальної наявності експлойтів

— Регулярне автоматизоване сканування інфраструктури сканерами вразливостей, розробка та впровадження процесу управління патчами (Patch Management).

Який результат для підприємства: Постійне підтримання цифрової гігієни інфраструктури, усунення технічних можливостей для легкого проникнення зловмисників у системи підприємства.

З ким взаємодіє: Системні адміністратори, домени Asset Management, SOC, Application Security та Network Security.

10. Human Factor, Awareness & Physical Security (Людський фактор і фізична безпека)

Яку проблему закриває: Низький рівень кіберграмотності працівників (відкриття підозрілих листів, підключення невідомих флешок), вразливість до маніпуляцій, а також ризик фізичного проникнення сторонніх осіб до серверних кімнат чи на територію об'єкта, людські помилки, які можуть призвести до катастрофічних наслідків

Які гібридні загрози перекриває: Цільовий фішинг, атаки із застосуванням соціальної інженерії та ворожих ІПсО, фізичні диверсії на

території підприємства (закладка апаратних шпигунських пристроїв), виведення з ладу ліній живлення.

Які механізми впроваджуються:

— Проведення навчання усього персоналу щодо кібергігієни, підвищення навичок кіберфахівців енергетичної галузі у сфері кібербезпеки, проходження симуляцій фішингових атак для перевірки пильності співробітників [30].

— Інтеграція систем відеонагляду, СКУД (систем контролю управління доступом) та охоронної сигналізації підстанцій з моніторингом SOC. Спроба несанкціонованого фізичного доступу до критичних приміщень або зон обмеженого доступу повинна генерувати інцидент у SIEM.

— Протидія ІПСО та інсайдерським загрозам.

— Психологічна підтримка та інструктаж персоналу щодо виявлення дезінформації під час кризових ситуацій.

Який результат для підприємства: Формування кіберстійкого колективу, надійний захист матеріальних та цифрових ресурсів від фізичного викрадення чи знищення.

З ким взаємодіє: Департамент управління персоналом (HR), служба фізичної охорони підприємства, SOC, IAM, керівництво підприємства та всі працівники підприємства без винятку.

Запропонована система управління кібербезпекою за доменами безпеки формує комплексну багаторівневу модель захисту, у якій усі механізми безпеки функціонують як єдина взаємопов’язана система це дозволяє підприємству енергетичного сектору ефективно протидіяти сучасним кіберзагрозам та підвищувати кіберстійкість об’єктів критичної інфраструктури.

3.2. Правила та рекомендації щодо забезпечення кіберстійкості підприємства за доменами безпеки в умовах гібридної війни

Для забезпечення практичного функціонування розробленої системи управління кібербезпекою (СУКБ) має бути впроваджено чіткий комплекс експлуатаційних правил, організаційних регламентів та інженерних рекомендацій. Вони структуровані за чотирма функціональними блоками та координуються з відповідними доменами безпеки (R1–R10).

Кіберстійкість підприємства безпосередньо залежить від операційного дотримання встановлених процедур та підтримання захисту в життєздатному стані на всіх рівнях управління.

Для об’єкта критичної інфраструктури важливим є не лише впровадження засобів захисту, а й постійне підтримання їх працездатності, контроль процедур безпеки та готовність персоналу до реагування на інциденти.

1. Організаційно-управлінські правила та комплаєнс (Домени: R1, R2):

— Регламент оцінювання ризиків (ISO 22301 / ISO/IEC 27005): аналіз ландшафту загроз проводиться щомісячно або за директивами Держспецзв’язку та CERT-UA. Загострення воєнної обстановки автоматично запускає позапланову перевірку планів безперервності бізнесу (BCP) та аварійного відновлення (DRP) з обов'язковим оперативним обміном індикаторами компрометації (IoC).

— Контроль активів: введення в експлуатацію будь-якого обладнання чи ПЗ дозволяється виключно після внесення його конфігурацій до бази даних CMDB та погодження зі службою кібербезпеки.

2. Технічні інженерні регламенти захисту інфраструктури (Домени: R3, R4, R5, R6, R7):

— Слід дотримуватися правила «Нульової довіри» (Zero Trust): обов'язковий глибокий аналіз пакетів (DPI) через NGFW на межі IT/OT сегментів. Передача незахищених промислових протоколів здійснюється суворо через IPsec-тунелі.

— Управління доступом (IAM/PAM): постійні канали дистанційного доступу заборонені. Підключення зовнішніх інженерів активується диспетчером АСУ ТП лише на час робіт через шлюз PAM із записом сесій, а вхід до критичних систем вимагає багатофакторної автентифікації (MFA) за апаратними токенами.

— Протидія Ransomware: резервне копіювання баз даних SCADA та конфігурацій систем захисту виконується за схемою: повний бекап — щотижнево, інкрементний — кожні 12 годин.

3. Операційні рекомендації з моніторингу та управління вразливостями (Домени: R8, R9):

— Правила реагування на інциденти в умовах комбінованих атак (Kinetic-Cyber): У разі оголошення повітряної тривоги або початку фізичного обстрілу об'єкта енергетики, чергова зміна SOC та диспетчери АСУ ТП діють за спеціальним сценарієм (Playbook): перевірка працездатності резервних каналів зв'язку, фіксація поточних станів конфігурацій та переведення систем логування в режим підвищеної чутливості для виявлення супутніх кібератак.

— Впровадження підходу безперервного моніторингу (Continuous Monitoring): Забезпечується цілодобовий збір, агрегація та аналіз журналів подій від міжмережевих екранів, систем автентифікації, кінцевих точок та технологічного обладнання в єдиній системі керування подіями безпеки (SIEM) у межах операційного центру безпеки (SOC).

— Регламент безпечного усунення вразливостей (Патч-менеджмент): Забороняється проведення активного мережевого сканування в робочий час у технологічному сегменті, оскільки це може порушити стабільність промислових систем. Пошук уразливостей здійснюється виключно системами пасивного аналізу конфігурацій.

4. Управління людським фактором та фізичної безпеки (Домен: R10):

— Соціальна інженерія: персонал зобов'язаний повідомляти SOC про підозрілі контакти чи фішинг, в разі масових дезінформаційних кампаній у

медіапросторі персонал зобов'язаний керуватися внутрішніми захищеними каналами зв'язку та розпорядженнями диспетчерського центру.

— Фізико-кібернетичний контроль: дані СКУД та відеофіксації доступу до серверних шаф інтегруються з SIEM у реальному часі.

Впровадження запропонованих правил та рекомендації формують практичне підтримання кіберстійкості підприємства в умовах сучасних гібридних загроз.

Загальну архітектуру та взаємозв’язок розроблених експлуатаційних регламентів із доменами безпеки запропонованої СУКБ наочно представлено у вигляді структурованої схеми на рис. 3.3.

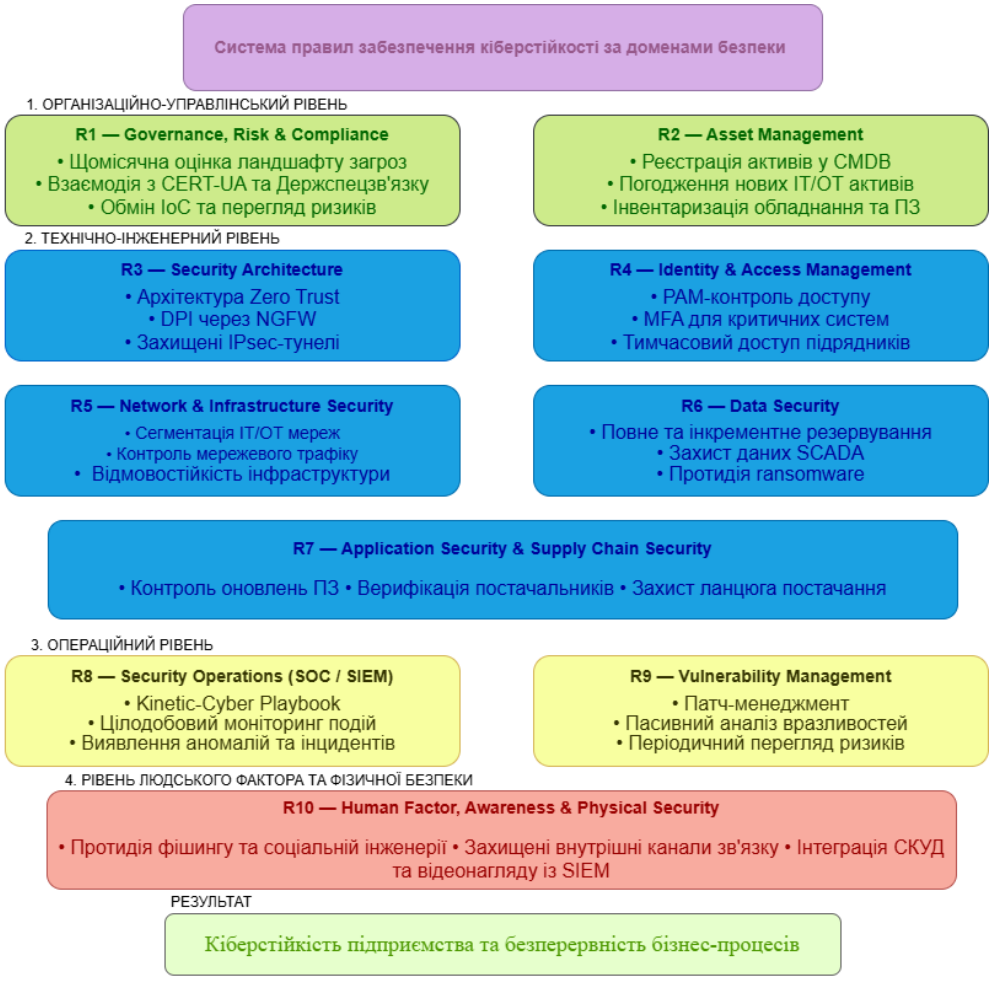

Рис. 3.3. Система правил щодо забезпечення кіберстійкості підприємства за доменами безпеки в умовах гібридної війни

3.3. Розробка імітаційної моделі BIA CRS та моделювання параметрів стійкості системи управління кібербезпекою підприємства за доменами безпеки в умовах гібридних загроз

Впровадження розробленої системи управління кібербезпекою (СУКБ) на підприємстві критичної інфраструктури енергетичного сектору України є ключовим етапом підвищення його загальної кіберстійкості. Перехід до доменної моделі дозволяє суттєво знизити рівень критичних ризиків (R1–R10), ідентифікованих у другому розділі дослідження, забезпечити проактивний контроль над активами, локалізувати інциденти та мінімізувати час відновлення систем.

На відміну від результатів BIA-аналізу, наведених у підрозділі 2.3, де оцінювання здійснювалося на рівні доменів безпеки, у даному розділі проведено деталізацію показників RTO та RPO для критичних активів підприємства енергетичного сектору. Такий підхід дозволяє врахувати різний ступінь впливу окремих активів на безперервність технологічних процесів та обґрунтувати пріоритетність заходів захисту в межах кожного домену.

Таблиця 3.1

Аналізу впливу на безперервність бізнес-процесів (BIA) за доменами безпеки

Домен безпеки і код	Критичні активи підприємства енергетики	Факт RTO (в умовах війни)	Норматив RTO (ISO 22301 / NIST)	Факт RPO (в умовах війни)	Норматив RPO (ISO 22301 / NIST)	Порівняльний статус та відхилення від нормативу
R1 Governance, Risk & Compliance (GRC)	Реєстри цифрових ризиків, плани BCP/DRP.	16 год	24 год	16 год	24 год	Резерв часу становить 8 год. Допустиме помірне відхилення, оскільки домен безпосередньо не впливає на миттєвий технологічний процес.
R2 Asset Management	Бази даних конфігурацій (CMDB), топологічні схеми мереж, реєстри IT/OT активів	4 год	6 год	8 год	12 год	Резерв часу становить 2 год. Вимагає високої оперативності для точної локалізації уражених вузлів під час аварії.

Продовження таблиці 3.1

Домен безпеки і код	Критичні активи підприємства енергетики	Факт RTO (в умовах війни)	Норматив RTO (ISO 22301 / NIST)	Факт RPO (в умовах війни)	Норматив RPO (ISO 22301 / NIST)	Порівняльний статус та відхилення від нормативу
R3 Security Architecture	Конфігурації Firewalls, криптографічні ключі, матриці зонування мереж	2 год	3 год	1 год	2 год	Стиснення на 33%. Швидке розгортання захищеного периметра критично для відновлення суміжних систем
R4 Identity & Access Management (IAM)	Каталоги Active Directory, бази даних MFA/2FA, системи привілейованого доступу (PAM)	15 хв	30 хв	5 хв	15 хв	Надкритичний стан. Скорочення часу відновлення вдвічі. Без IAM неможлива авторизація диспетчерів SCADA
R5 Network Security	Таблиці маршрутизації, конфігурації VPN-тунелів підстанцій, налаштування промислових IDS/IPS	1 год	2 год	2 год	4 год	Стиснення на 50%. Необхідно для оперативного перемикання на резервні канали зв'язку (наприклад, супутникові)
R6 Data Security	Комерційні бази, історична телеметрія процесів, масиви резервних копій	2,5 год	4 год	10 хв	1 год	Висока критичність даних. RPO мінімізовано майже до нуля для запобігання втрати фінансових транзакцій
R7 Application Security	Вихідний код внутрішнього ПЗ, профілі ризиків підрядників	16 год	24 год	8 год	12 год	Резерв часу становить 8 год. Допустиме відкладене відновлення, розробка не є процесом реального часу для постачання енергії
R8 Security Operations (SOC)	Логи SIEM/SOAR, телеметрія EDR/XDR, плани реагування (IRP), індикатори компрометації (IoC)	30 хв	1,5 год	1 хв	5 хв	Надкритичний стан. SOC має функціонувати безперервно. Втрата системних логів у перші хвилини атаки унеможливлює розслідування інциденту
R9 Vulnerability Management	Звіти сканування, графіки патч-менеджменту, ба контролерів	16 год	24 год	16 год	24 год	Стиснення на 33%. Патчинг в промислових мережах прив'язаний до регламентних технологічних вікон
R10 Human Factor & Physical Security	Бази даних СКУД, відеоархіви CCTV об'єктів генерації, матриці допусків персоналу	2 год	3 год	2 год	4 год	Комплексна взаємодія захисту. Необхідно для миттєвого забезпечення доступу аварійно-ремонтних бригад на фізичні об'єкти
Агрегований індекс стійкості	Порівняння з нормативними значеннями	Сер. від-ння RTO: -38%	Базовий нормативний рівень (100%)	Середнє відхилення RPO: -52%	Базовий нормативний рівень (100%)	Адаптивна готовність інфраструктури підвищена в 1,5–2 р. порівняно з мирним часом за рахунок стиснення часових вікон.

Порівняльний рядок чітко демонструє, що в умовах гібридної війни підтримання класичних таймінгів відновлення є недопустимим. Для надкритичних доменів (R4 та R8) розрахункові показники жорсткіші за світові стандарти мирного часу на 50–80%. Затримка у відновленні контролю доступу чи моніторингу загрожує каскадним колапсом усієї енергосистеми.

Раціональний розподіл ресурсів: Оскільки загальний ресурс служби безпеки обмежений, домени з низьким миттєвим операційним впливом (GRC, Supply Chain) функціонують із мінімальним стисненням, що дозволяє перенаправити сили на підтримку безперервної реплікації даних Data Security та миттєве відновлення мережевої інфраструктури.

Для моніторингу зміни параметрів безперервності бізнес-процесів залежно від рівня гібридної загрози розроблено імітаційну модель «BIA Cyber-Resilience Simulator».

Математична логіка (ядро моделі) написана мовою Python, яка є стандартом для наукового моделювання та аналізу даних. Нижче наведено Python-код (з використанням бібліотеки pandas), який реалізує алгоритм перерахунку нормативних показників RTO та RPO залежно від рівня гібридної загрози (K_m).

У цьому скрипті використовується лінійна залежність RTO / K_m.

Python-модель розрахунку показників стійкості інфраструктури K_m відображено та детально описано код моделі на рис. 3.4.

```python
import pandas as pd

# 1. Ініціалізація базових нормативних значень за ISO 22301 (в годинах)
# RTO_std: Нормативний цільовий час відновлення
# RPO_std: Нормативна цільова точка відновлення
data = {
    "Domain_Code": ["R1", "R2", "R3", "R4", "R5", "R6", "R7", "R8", "R9", "R10"],
    "Security_Domain": [
        "GRC", "Asset Management", "Architecture", "IAM",
        "Network", "Data Security", "Supply Chain",
        "Security Operations", "Vulnerability Mgt", "Physical Security"
    ],
    "RTO_std": [24.0, 6.0, 3.0, 0.5, 2.0, 4.0, 24.0, 1.5, 24.0, 3.0],
    "RPO_std": [24.0, 12.0, 2.0, 0.25, 4.0, 1.0, 12.0, 0.08, 24.0, 4.0]
}

df_baseline = pd.DataFrame(data)

def simulate_hybrid_threat_bia(df, threat_factor_km):
    """
    Моделювання показників BIA в умовах ескалації кібернетичних та кінетичних загроз.

    Параметри:
    df (DataFrame): Базовий набір нормативних даних.
    threat_factor_km (float): Коефіцієнт гібридної загрози (1.0 = норма, >1.0 = війна).

    Повертає:
    DataFrame: Розраховані показники зі стисненням часових вікон.
    """
    # Створення копії для збереження цілісності базових даних
    sim = df.copy()

    # Застосування математичної моделі адаптивного стиснення
    sim["RTO_war"] = sim["RTO_std"] / threat_factor_km
    sim["RPO_war"] = sim["RPO_std"] / threat_factor_km

    # Розрахунок дельти (наскільки скоротився час реагування порівняно з нормою)
    sim["RTO_Delta_(hrs)"] = sim["RTO_std"] - sim["RTO_war"]
    sim["RPO_Delta_(hrs)"] = sim["RPO_std"] - sim["RPO_war"]

    # Округлення результатів для аналітичного звіту (до 2 знаків після коми)
    sim = sim.round(2)

    return sim

# 2. Виконання моделювання для критичного рівня ескалації (Km = 1.8)
km_value = 1.8
results_df = simulate_hybrid_threat_bia(df_baseline, km_value)

# 3. Виведення результатів у консоль (може бути експортовано в Excel/CSV)
print(f"--- Аналіз впливу на бізнес (BIA) при рівні загрози Km = {km_value} ---\n")
print(results_df[["Domain_Code", "Security_Domain", "RTO_std", "RTO_war", "RPO_std", "RPO

# Розрахунок загального агрегованого індексу готовності інфраструктури (у %)
# Відображає, на скільки відсотків система має бути швидшою/ефективнішою за стандарт
average_rto_compression = (1 - (results_df["RTO_war"].mean() / results_df["RTO_std"].mean
print(f"\nАгрегований показник: Інфраструктура має відновлюватися на {average_rto_compression
```

Рис. 3.4. Python-модель розрахунку показників стійкості інфраструктури K_m

Модель дозволяє адаптивно змінювати коефіцієнт гібридної загрози (Km) у діапазоні від 0 до 2 та оцінювати вплив зміни інтенсивності кібератак і деструктивних факторів на показники RTO та RPO для кожного домену безпеки підприємства та представлена на рис. 3.5.

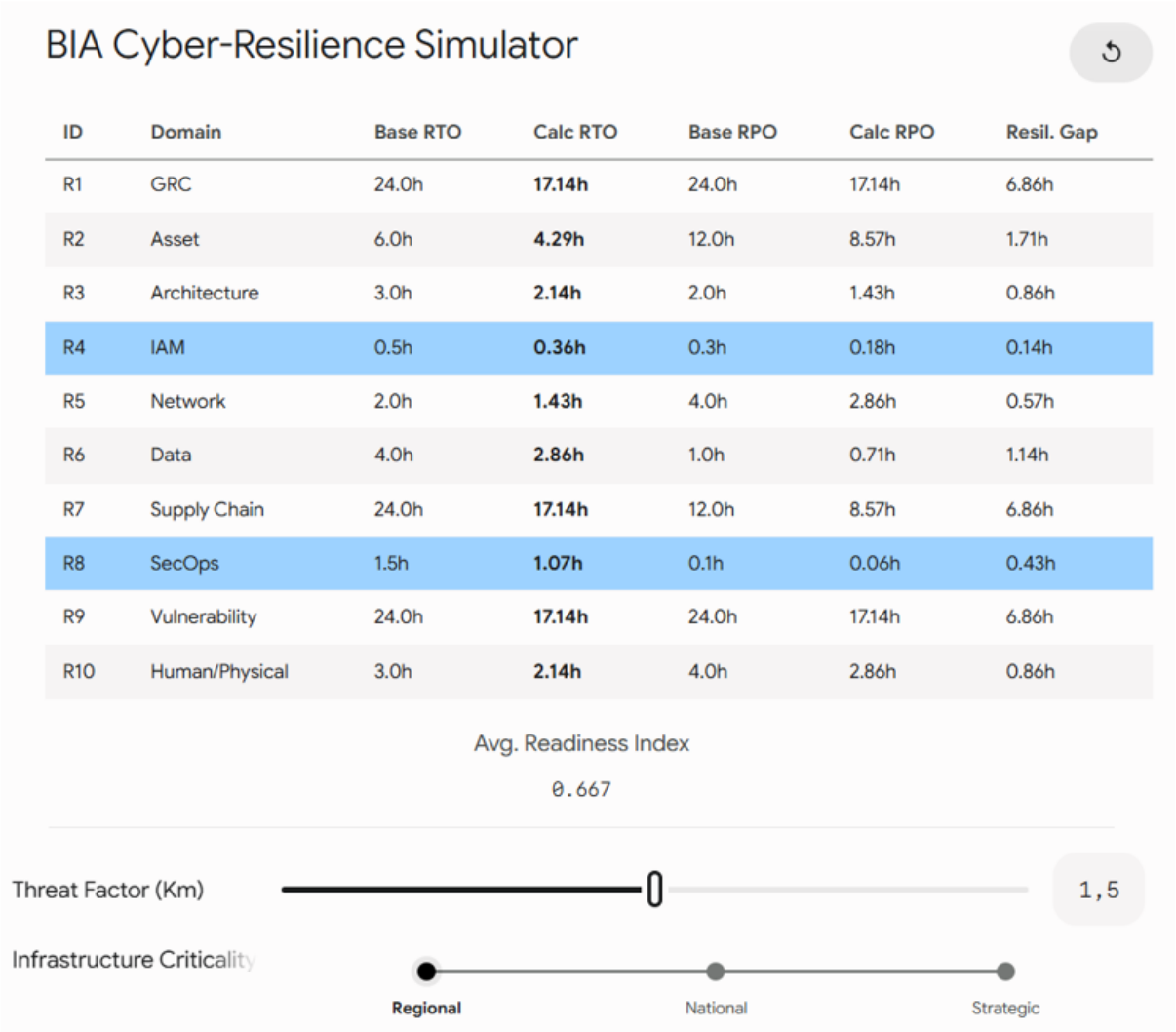

Рис. 3.5. Моделювання параметрів кіберстійкості підприємства залежно від коефіцієнта гібридної загрози (K_m 1,5)

Для оцінювання поведінки системи в умовах подальшого зростання рівня гібридних загроз проведено моделювання зі збільшеним значенням коефіцієнта гібридної загрози до Km = 1,8. Результати моделювання наведено на рис. 3.6.

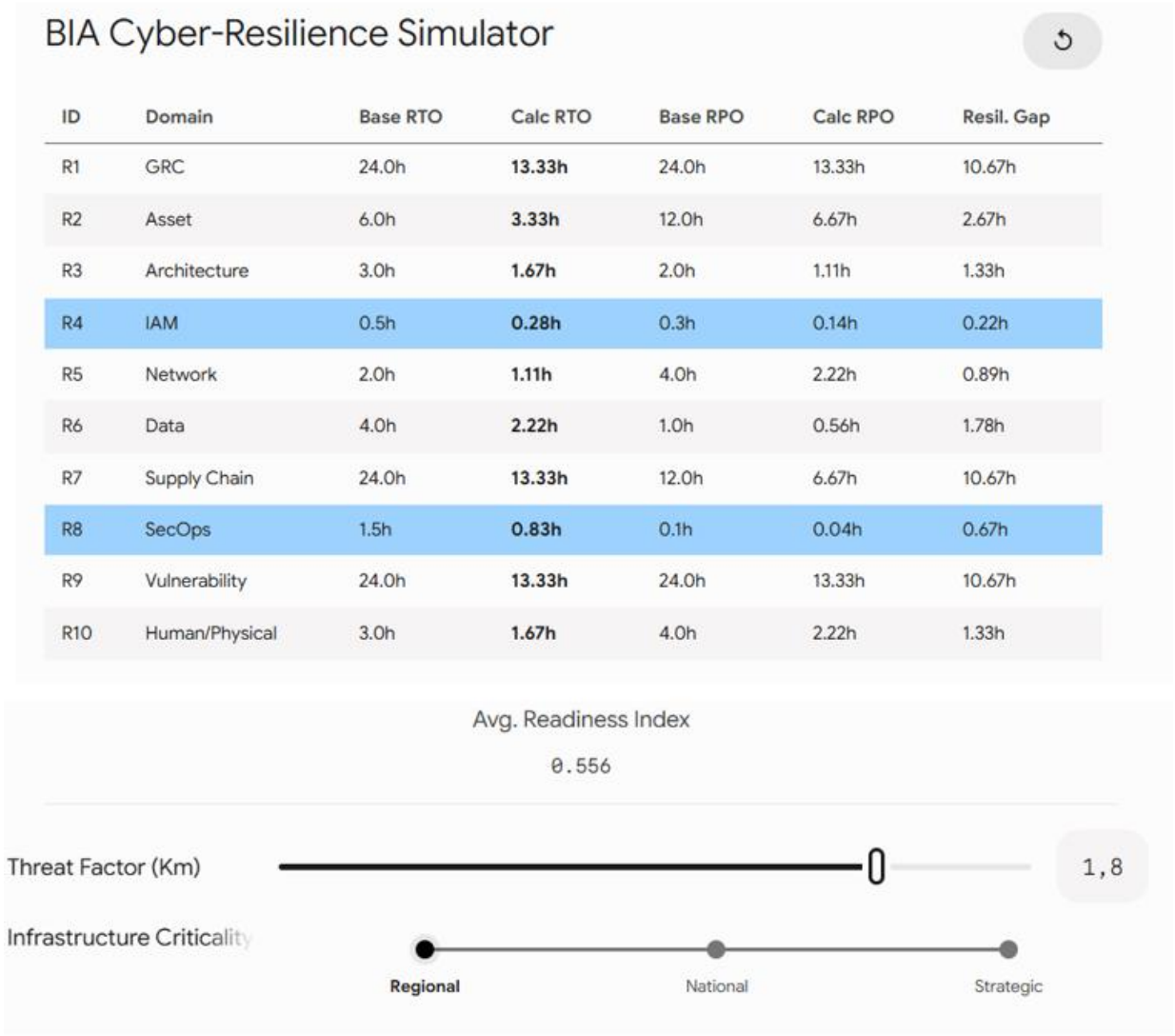

Рис. 3.6. Моделювання параметрів кіберстійкості підприємства залежно від коефіцієнта гібридної загрози (K_m 1,8)

Збільшення коефіцієнта гібридної загрози (K_m) з 1,5 до 1,8 відображає перехід від сценарію активного конфлікту до сценарію критичної ескалації та супроводжується подальшим скороченням допустимих часових меж відновлення критичних сервісів. На практиці для енергетичного підприємства це моделює ситуацію масованого кінетичного удару по критичних вузлах, який синхронізовано з деструктивними кібератаками (наприклад, масовим розгортанням wiper-програм у корпоративній та технологічній мережах).

Наближення K_m до значення 2,0 свідчить про необхідність переходу до більш автоматизованих та автономних механізмів забезпечення кіберстійкості підприємства.

Результати імітаційного моделювання демонструють, що впровадження запропонованої СУКБ дозволяє підприємству функціонувати в умовах підвищеного рівня гібридних загроз із більш прогнозованими параметрами відновлення критичних сервісів. Скорочення допустимих часових меж відновлення свідчить про підвищення готовності до реагування на кіберінциденти, зменшення потенційних втрат даних та зниження ризику поширення негативних наслідків між IT- та OT-сегментами. Отримані результати підтверджують доцільність використання доменного підходу як основи побудови системи управління кібербезпекою та створюють підґрунтя для оцінювання її впливу на загальний рівень кіберстійкості підприємства.

Підвищення кіберстійкості підприємства

Впровадження запропонованої системи управління кібербезпекою за доменами безпеки сприяє підвищенню загальної кіберстійкості підприємства. Зниження рівнів кіберризиків, скорочення показників RTO та RPO, а також посилення контролю над критичними активами забезпечують швидше виявлення, локалізацію та усунення наслідків кіберінцидентів. Це дозволяє підтримувати безперервність функціонування ключових бізнес-процесів навіть в умовах підвищеної інтенсивності гібридних загроз.

Переваги доменного підходу до побудови СУКБ

Запропонований доменний підхід забезпечує централізацію процесів управління кібербезпекою та інтеграцію всіх заходів захисту в єдину систему. Його використання дозволяє реалізувати багаторівневий захист, підвищити керованість безпекою, забезпечити гнучкість і масштабованість архітектури, а також мінімізувати ризики поширення інцидентів між IT- та OT-сегментами. У результаті формується цілісна система протидії кіберзагрозам, здатна підтримувати безперервність критичних процесів і підвищувати кіберстійкість підприємства в умовах гібридної війни.

Висновки до розділу 3

У третьому розділі розроблено систему управління кібербезпекою підприємства за доменами безпеки, яка охоплює стратегічний, технічний, операційний та організаційний рівні захисту. Запропонована модель побудована на основі десяти взаємопов’язаних доменів безпеки та спрямована на підвищення кіберстійкості підприємства енергетичного сектору в умовах гібридних загроз.

На основі результатів аналізу ризиків, проведеного у другому розділі, сформовано комплекс правил і рекомендацій щодо захисту IT- та OT-середовищ підприємства. Запропоновані заходи передбачають удосконалення управління доступом, мережевої сегментації, захисту даних, моніторингу подій безпеки, управління вразливостями та підготовки персоналу, що дозволяє знизити ймовірність успішної реалізації кібератак та мінімізувати їх наслідки.

Для обґрунтування доцільності впровадження запропонованої СУКБ проведено BIA-аналіз критичних активів підприємства та виконано імітаційне моделювання показників RTO і RPO залежно від рівня гібридної загрози. Результати моделювання показали скорочення часу відновлення критичних сервісів, зменшення потенційних втрат даних та підвищення готовності підприємства до реагування на інциденти.

Порівняльне оцінювання рівнів кіберризиків до та після впровадження СУКБ підтвердило прогнозоване зниження ризиків у всіх доменах безпеки. Отримані результати свідчать про доцільність використання доменного підходу як основи побудови системи управління кібербезпекою підприємств критичної інфраструктури та забезпечення їх безперервного функціонування в умовах гібридної війни.

ВИСНОВКИ

У кваліфікаційній роботі вирішено актуальне науково-практичне завдання щодо розробки системи управління кібербезпекою підприємства критичної інфраструктури енергетичного сектору України за доменами безпеки в умовах гібридної війни.

Досліджено теоретичні засади управління кібербезпекою в умовах гібридних загроз. Встановлено, що сучасні кібератаки мають комплексний характер та поєднують технічні, інформаційні й соціальні методи впливу. Це обумовлює необхідність застосування системного підходу до управління кібербезпекою та підвищення кіберстійкості підприємств.

Проаналізовано концепцію доменів безпеки та обґрунтовано доцільність її використання для побудови комплексної системи захисту. Визначено десять взаємопов’язаних доменів безпеки, які охоплюють стратегічний, технічний, операційний та організаційний рівні управління кібербезпекою підприємства.

Проведено аналіз актуальних гібридних загроз для підприємств енергетичного сектору України та виконано оцінювання кіберризиків за доменами безпеки. Встановлено, що найбільш критичними напрямами є мережева та інфраструктурна безпека, управління доступом, моніторинг подій безпеки та людський фактор. Також досліджено вплив гібридних атак на безперервність функціонування підприємства та визначено їх потенційні наслідки для критичної інфраструктури.

Розроблено систему управління кібербезпекою підприємства за доменами безпеки, яка об’єднує організаційні, технічні та операційні механізми захисту в єдину багаторівневу модель. Методологічною основою запропонованої системи стали вимоги міжнародних стандартів ISO/IEC 27001, ISO/IEC 27005, NIST Cybersecurity Framework та IEC 62443.

Сформовано практичні правила та рекомендації щодо забезпечення кіберстійкості підприємства в умовах гібридної війни. Запропоновані заходи охоплюють управління ризиками, захист мережевої інфраструктури, контроль

доступу, моніторинг подій безпеки, управління вразливостями та підвищення обізнаності персоналу. Для обґрунтування доцільності впровадження запропонованої СУКБ використано імітаційне моделювання коефіцієнтів впливу гібридних загроз на домени безпеки, результати якого підтвердили ефективність запропонованого підходу та його здатність підвищувати рівень кіберстійкості підприємства.

Практична цінність одержаних результатів полягає у можливості використання запропонованої доменної моделі під час побудови та вдосконалення систем управління кібербезпекою на підприємствах критичної інфраструктури, зокрема енергетичного сектору України, в умовах постійного впливу гібридних загроз.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Магда Є. Гібридна війна: питання і відповіді. MediaSapiens. 2015. URL: https://ms.detector.media/mediaanalitika/post/13805/2015-07-27-gibrydna-viyna-pytannya-i-vidpovidi/ (дата звернення: 28.04.2026).

2. Державна служба спеціального зв'язку та захисту інформації України. Кібероперації рф: нові цілі, інструменти та групи. Аналітика хакерських атак проти України за І півріччя 2024 року. URL: https://cip.gov.ua/ua/news/cyber-operations-rf-h1-2024-report (дата звернення: 01.05.2026).

3. Про затвердження Загальних вимог з кіберзахисту об'єктів критичної інфраструктури : Постанова Кабінету Міністрів України від 19.06.2019 № 518. База даних «Законодавство України». Верховна Рада України. URL: https://zakon.rada.gov.ua/go/518-2019-%D0%BF (дата звернення: 28.05.2026).

4. ENISA Threat Landscape 2025. European Union Agency for Cybersecurity. URL: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2025 (дата звернення: 01.05.2026)

5. MITRE ATT&CK Framework. MITRE Corporation. URL: https://attack.mitre.org/ (дата звернення: 01.05.2026)

6. ISO/IEC 27005:2022. Information security, cybersecurity and privacy protection — Guidance on managing information security risks. URL: https://www.iso.org/standard/80585.html (дата звернення: 01.05.2026)

7. Карпенко О. О., Осипова Є. Л. Гібридні загрози та комплексна безпека: навчальний посібник. Київ: ТОВ «ТРОПЕА», 2024. 76 с. URL: https://files.duit.edu.ua/uploads/%D0%A1%D0%B0%D0%B9%D1%82/3_%D0%9D%D0%90%D0%A3%D0%9A%D0%90/scientific-publications/monographs/varn-16-08-2024.pdf (дата звернення: 02.05.2026).

8. Гібридні загрози (Hybrid Threats). Глосарій проєкту WARN "Academic Response to Hybrid Threats". URL: https://warn-erasmus.eu/ua/glossary/gibridni-zagrozi/ (дата звернення: 02.05.2026).

9. Україна – ЄС – НАТО: співробітництво з протидії гібридним загрозам у кіберсфері. Центр глобалістики «Стратегія XXI». Київ, 2019. URL: https://www.kas.de/documents/270026/4625039/UA+Ukraine+-+EU+-+NATO+cooperation+to+counter+hybrid+threats+in+cyber+sphere.pdf (дата звернення: 02.05.2026).

10. Домени кібербезпеки: знайди свій улюблений. CyberSec. URL: https://cybersec.net.ua/statti/891-domeny-kiberbezpeky-znaidy-svii-uliublenyi.html (дата звернення: 03.05.2026).

11. Enterprise Security: How It Works and Why It Matters. CloudSEK. URL: https://www.cloudsek.com/knowledge-base/enterprise-security (дата звернення: 03.05.2026).

12. Jiang H. Cybersecurity Domains Map 3.0. LinkedIn, 2021. URL: http://linkedin.com/pulse/map-cybersecurity-domains-version-20-henry-jiang-ciso-cissp (дата звернення: 03.05.2026).

13. ISO/IEC 27001:2022. Information security management systems — Requirements. Geneva. URL: https://www.iso.org/standard/82875.html (дата звернення: 03.05.2026).

14. Цикл Демінга: як методологія PDCA допомагає при побудові бізнес-процесів. Nova Poshta Education. 2025. URL: https://online.novaposhta.education/blog/cikl-deminga-yak-metodologiya-pdca-dopomagae-pri-pobudovi-biznes-procesiv (дата звернення: 05.05.2026).

15. National Institute of Standards and Technology (NIST). Framework for Improving Critical Infrastructure Cybersecurity. Version 2.0. 2024. URL: https://www.nist.gov/cyberframework (дата звернення: 03.05.2026).

16. National Institute of Standards and Technology (NIST). NIST SP 800-53 Rev. 5. Security and Privacy Controls for Information Systems and Organizations. 2020. URL: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/f.SP.800-53r5.pdf (дата звернення: 03.05.2026).

17. Center for Internet Security (CIS). The 18 CIS Critical Security Controls. URL: https://www.cisecurity.org/controls/cis-controls-list (дата звернення: 03.05.2026).

18. Center for Internet Security (CIS). CIS Critical Security Controls v8. URL: https://www.cisecurity.org/controls/v8
(Дата звернення: 04.05.2026).

19. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.2017 № 2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19 (дата звернення: 04.05.2026).

20. Державна служба спеціального зв'язку та захисту інформації України. Захист критичної інфраструктури. URL: https://cip.gov.ua/ua/statics/zakhist-kritichnoyi-infrastrukturi (дата звернення: 04.05.2026).

21. Грищук Р. В., Жовноватюк Р. М., Носова Г. Д. Гібридні загрози у кіберпросторі: фактори впливу на природу виникнення. Сучасні інформаційні технології у сфері безпеки та оборони. 2019. URL: https://sit.nuou.org.ua/article/view/189097 (дата звернення: 12.05.2026).

22. Про критичну інфраструктуру : Закон України від 16.11.2021 № 1882-IX. URL: https://zakon.rada.gov.ua/laws/show/1882-20 (дата звернення: 04.05.2026).

23. CERT-UA. Кібератака групи Sandworm (UAC-0082) на об'єкти енергетики України з використанням шкідливих програм INDUSTROYER2 та CADDYWIPER (CERT-UA#4435). URL: https://cert.gov.ua/article/39518 (дата звернення: 14.05.2026).

24. Тімашов В. О., Адамович В. О. Організаційно-правове забезпечення енергетичної безпеки від кібератак та дронових небезпек України. Аналітично-порівняльне правознавство. 2025. DOI: https://doi.org/10.24144/2788-6018.2025.04.2.61 (дата звернення: 14.05.2026).

25. Держспецзв'язку України, CERT-UA. Russian Cyber Operations: Analytics for the H2 2024. URL:
https://cip.gov.ua/services/cm/api/attachment/download?id=68768 (дата звернення: 14.05.2026).

26. ISO/IEC 27031:2025. Cybersecurity — Information and communication technology readiness for business continuity. Geneva. URL: https://www.iso.org/standard/27031 (дата звернення: 29.05.2026).

27. CERT-UA. Cyber Threat Overview and Defense Strategies in 2025: CERT-UA's Experience. URL: https://cip.gov.ua/en/faqs/cyber-threat-overview-and-defense-strategies-in-2025-cert-ua-s-experience (дата звернення: 15.05.2026).

28. Протидія загрозам кібербезпеки для енергетичного сектору України. Modus X. URL: https://modusx.digital/uk-ua/blog/protidiya-zagrozam-kiberbezpeki-dlya-energetichnogo-sektoru-ukrayini (дата звернення: 15.05.2026).

29. Drahuntsov R., Symonov A., Potenko O., Dybach O., Zubok V. Моніторинг кібербезпеки під час знеструмлень: приклади використання для підвищення спостережуваності інфраструктури та потенційне значення для комбінованих подій на атомних електростанціях. Nuclear and Radiation Safety. 2025. № 3(107). DOI: https://doi.org/10.32918/nrs.2025.3(107).02 (дата звернення: 15.05.2026).

30. Міністерство енергетики України. Кібербезпека паливно-енергетичного комплексу України [Електронний ресурс]. URL: https://www.mev.gov.ua/storinka/kiberbezpeka (дата звернення: 15.05.2026).

31. Методика оцінювання ризиків кібербезпеки. Додаток 8 «Приклад оцінки ризиків кібербезпеки об'єктового рівня». URL: https://cip.gov.ua/services/cm/api/attachment/download?id=73336 (дата звернення: 18.05.2026).

32. National Institute of Standards and Technology. NIST SP 800-30 Rev. 1. Guide for Conducting Risk Assessments. URL: https://csrc.nist.gov/publications/detail/sp/800-30/rev-1/final (дата звернення: 18.05.2026).

33. ISO 22301:2019. Security and resilience — Business continuity management systems — Requirements. URL: https://www.iso.org/standard/75106.html (дата звернення: 18.05.2026).

34. TMS Outsource. Приклад плану забезпечення безперервності бізнесу. URL: https://tms.ua/blog/pryklad-planu-zabezpechennia-bezperervnosti-biznesu-velykyj-posibnyk/ (дата звернення: 18.05.2026).

35. IEC 62443. Industrial communication networks – Network and system security. URL: https://www.iec.ch/cyber-security (дата звернення: 18.05.2026).

36. ISACA. Risk IT Practitioner Guide. 2nd ed. Rolling Meadows : Information Systems Audit and Control Association, 2020. URL: https://www.isaca.org/ (дата звернення: 18.05.2026).

37. Енергореформа. Кількість кібератак на об'єкти енергетичної інфраструктури з початку війни збільшилася майже вдвічі. URL:https://reform.energy/news/kilkist-kiberatak-na-obekti-energetichnoi-infrastrukturi-z-pochatku-viyni-zbilshilasya-mayzhe-vdvichi-20140 (дата звернення: 21.05.2026).

38. Галкін А., Чайка О. Російські хакери координують дії з військовими та посилюють атаки напередодні зими: як Україна протистоїть кібератакам на енергосистему. Forbes Ukraine. 2023. URL: https://forbes.ua/company/rosiyski-khakeri-koordinuyut-dii-z-viyskovimi-ta-posilyuyut-ataki-naperedodni-zimi-yak-ukraina-protistoit-kiberatakam-na-energosistemu-08112023-17242 (дата звернення: 21.05.2026).

39. Куклінова Т. В. Інтелектуалізація кіберзахисту енергетичних підприємств: управлінський підхід. Безпека інформації та інфраструктури інформаційно-комунікаційних систем: міждисциплінарний підхід : монографія. Одеса : Видавничий дім «Гельветика», 2024. DOI: https://doi.org/10.36059/978-966-397-537-5 (дата звернення: 21.05.2026).

40. CERT-UA. CERT-UA у 2025 році опрацювала майже 6000 кіберінцидентів: кількість ворожих атак зросла на 37%. URL: https://cip.gov.ua/ua/news/cert-ua-u-2025-roci-opracyuvala-maizhe-6000-kiberincidentiv-kilkist-vorozhikh-atak-zrosla-na-37 (дата звернення: 21.05.2026).