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 кіберстійкістю підприємства в умовах гібридних загроз”

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

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

_____ Данило Шевчук

(підпис) *Ім’я, ПРІЗВИЩЕ здобувача*

Виконав: Здобувач вищої освіти гр. УБДМ-61
Данило Шевчук-Нагорний

Керівник:
д-р іст. н., професор Євгенія ІВАНЧЕНКО

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

Київ 2025

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

Навчально-науковий інститут кібербезпеки та захисту інформації

Кафедра Управління кібербезпекою та захистом інформації
Ступінь вищої освіти магістр
Спеціальність 125 Кібербезпека та захист інформації
Освітньо-професійна програма Управління інформаційною та кібернетичною безпекою

ЗАТВЕРДЖУЮ
Завідувач кафедрою УКБЗІ
_____ Світлана ЛЕГОМІНОВА
“____” _____ 2025 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Студенту Шевчук-Нагорному Данилу Кириловичу
(прізвище, ім’я, по батькові здобувача)

1. Тема кваліфікаційної роботи: “Система управління кіберстійкістю підприємства в умовах гібридних загроз”

керівник кваліфікаційної роботи Євгенія ІВАНЧЕНКО., д-р.іст.н., професор
(Ім’я, ПРІЗВИЩЕ, науковий ступінь, вчене звання)

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

2. Строк подання кваліфікаційної роботи “11” грудня 2025 р.
3. Вихідні дані до кваліфікаційної роботи:.
4. Перелік питань, які потрібно розробити:
   1..
   2..
   3..
5. Перелік ілюстративного матеріалу: *презентація*
6. Дата видачі завдання “02” жовтня 2025 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назви етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1.	Визначення об’єкту, предмету, мети та завдань дослідження.	10.10.2025	
2.	Збір та аналіз літератури.	23.10.2025	
3.	Аналіз основних характеристик інформаційного протиборства.	27.10.2025	
4.	Дослідження особливостей управління інформаційною безпекою підприємствав умовах інформаційного протиборства.	10.11.2025	
5.	Визначення напрямів та методів забезпечення інформаційної безпеки підприємства у процесі інформаційного протиборства.	15.11.2025	
6.	Формулювання висновків за результатами дослідження.	22.11.2025	
7.	Оформлення роботи.	04.12.2025	
8.	Оформлення презентації.	14.12.2025	
9.	Отримання рецензії на роботу.	18.12.2025	
10.	Захист в ЕК.	__.01.2026	

Здобувач вищої освіти _____ Данило Шевчук-Нагорний

(підпис) *(Ім’я, ПРІЗВИЩЕ)*

Керівник кваліфікаційної роботи _____ Євгенія ІВАНЧЕНКО

(підпис) *(Ім’я, ПРІЗВИЩЕ)*

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

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

Направляється здобувач Шевчук-Нагорний Д.К.. до захисту кваліфікаційної роботи
(прізвище та ініціали)
за спеціальністю 125 Кібербезпека та захист інформації
(код, найменування спеціальності)
Освітньо-професійної програми Управління інформаційною та кібернетичною безпекою
(назва)

на тему: "Технологія створення системи управління інформаційною безпекою в організації"
Кваліфікаційна робота і рецензія додаються.

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

Висновок керівника кваліфікаційної роботи

Здобувач у кваліфікаційній роботі проаналізував теоретичні аспекти технологій введення в оману, вивчив методи та засоби технологій введення в оману, а також дослідив практичне застосування технологій введення в оману для кібербезпеки підприємства.

Студент показав високу теоретичну і практичну підготовку, володіння науково-дослідницькими методами, вміння самостійно знаходити шляхи вирішення проблеми дослідження. Результати дослідження апробовані на конференції "Стратегії кіберстійкості: управління ризиками та безперервність бізнесу" 28 лютого 2024 року.

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

Керівник кваліфікаційної роботи _____ Євгенія ІВАНЧЕНКО
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

" " 2025 року

Висновок кафедри про кваліфікаційну роботу

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

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

ВІДГУК РЕЦЕНЗЕНТА
на кваліфікаційну магістерську роботу

здобувачки вищої освіти
на тему “ Система управління кіберстійкістю підприємства в умовах гібридних загроз.”

Актуальність Як свідчать реалії, різноманітні засоби інформаційного впливу зараз активно застосовуються конкуруючими фірмами та корпораціями в ринковій боротьбі. Тому важливим завданням сучасного підприємства є його захист від негативного інформаційного впливу, запобігання і протидія загрозам, що виникають внаслідок застосування засобів інформаційного протиборства. З огляду на зазначене дослідження проблем забезпечення інформаційної безпеки підприємства в умовах інформаційного протиборства є актуальним науковим завданням.

Позитивні сторони

1. У роботі досліджено засади забезпечення інформаційної безпекипідприємства в умовах інформаційного протиборства та проведено аналіз його основних характеристик. Визначено особливості управління інформаційною безпекою підприємства в умовах інформаційного протиборства, представлено схему актуальних загроз інформаційній безпеці підприємства з урахуванням зазначеної специфіки.
2. Кваліфікаційна робота оформлена відповідно до вимог. Виклад матеріалу здійснено відповідно до плану, зроблено логічні висновки. Ключові положення роботи представлено у вигляді рисунків. Автор опрацювала значну джерельну базу: близько 50 публікацій та електронних джерел, в тому числі англомовних.
3. За результатами дослідження запропоновано рекомендації щодо забезпечення інформаційної безпеки підприємства в умовах інформаційного протиборства.

Недоліки

1. Доцільно було б приділити більше уваги вивченню і класифікації методів протидії загрозам інформаційного протиборства, а також особливостям їх використання у вітчизняних реаліях.

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

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

Рецензент: завідувач кафедри
Систем та технологій кібербезпеки
д-р техн. н., професор _____ Галина ГАЙДУР

РЕФЕРАТ

Текстова частина кваліфікаційної роботи на здобуття освітнього ступеня магістра: 90 стор., 14 рис., 6 табл., 71 джерело.

Метою роботи є дослідження теоретичних та прикладних засад формування і функціонування системи управління кіберстійкістю підприємства в умовах гібридних загроз та розроблення практичних рекомендацій щодо підвищення її ефективності.

Об'єктом дослідження є система забезпечення кіберстійкості підприємства.

Предметом дослідження є процеси, методи та інструменти управління кіберстійкістю підприємства в умовах дії гібридних загроз.

Методи дослідження. Для досягнення поставленої мети та розв'язання завдань у роботі застосовано методи системного та структурно-функціонального аналізу для дослідження системи управління кіберстійкістю підприємства та взаємозв'язків між її елементами, методи аналізу й синтезу для узагальнення теоретичних підходів до визначення сутності кіберстійкості та гібридних загроз, методи ризик-менеджменту для оцінювання вразливостей і загроз кіберпростору підприємства, методи моделювання для розроблення концептуальної моделі системи управління кіберстійкістю, експертні методи для оцінювання ефективності запропонованих заходів, а також методи порівняльного аналізу для зіставлення національних і міжнародних стандартів та практик забезпечення кіберстійкості організацій.

Короткий зміст роботи. У роботі проведено аналіз еволюції поняття кіберстійкості та її місця в системі інформаційної безпеки підприємства, досліджено природу та класифікацію гібридних загроз і їх вплив на діяльність сучасних організацій, розглянуто нормативно-правові та міжнародні стандарти у сфері забезпечення кіберстійкості. На основі аналізу стану системи інформаційної безпеки реального підприємства здійснено оцінювання рівня його кіберстійкості та вразливостей в умовах гібридних загроз, виявлено ключові ризики, інциденти та проблеми функціонування наявної системи управління. Запропоновано модель системи управління кіберстійкістю підприємства, обґрунтовано комплекс заходів і інструментів її підвищення, а також проведено оцінювання ефективності запропонованих рішень і прогноз результатів їх упровадження.

Галузь застосування. Результати дослідження та розроблені рекомендації можуть бути використані в практичній діяльності підприємств різних галузей економіки при формуванні та вдосконаленні систем управління кіберстійкістю, зокрема в умовах зростання інтенсивності гібридних загроз, а також у навчальному процесі під час підготовки фахівців у сфері кібербезпеки та інформаційних технологій.

КЛЮЧОВІ СЛОВА: КІБЕРСТІЙКІСТЬ ПІДПРИЄМСТВА, ГІБРИДНІ ЗАГРОЗИ, СИСТЕМА УПРАВЛІННЯ КІБЕРСТІЙКІСТЮ, КІБЕРБЕЗПЕКА, УПРАВЛІННЯ РИЗИКАМИ, БЕЗПЕРЕРВНІСТЬ БІЗНЕСУ, ІНЦИДЕНТИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ.

ABSTRACT

The text part of the qualification thesis for obtaining the Master's degree: 90 pages, 14 figures, 6 tables, 71 references.

The purpose of the thesis is to study the theoretical and applied foundations of the formation and functioning of an enterprise cyber resilience management system under hybrid threats and to develop practical recommendations for improving its effectiveness.

The object of the research is the system for ensuring the cyber resilience of an enterprise.

The subject of the research is the processes, methods, and tools for managing the cyber resilience of an enterprise under the impact of hybrid threats.

Research methods. To achieve the stated purpose and solve the research objectives, the study applies methods of systemic and structural-functional analysis to investigate the cyber resilience management system of the enterprise and the relationships between its elements; methods of analysis and synthesis to generalize theoretical approaches to defining the essence of cyber resilience and hybrid threats; risk management methods to assess vulnerabilities and threats in the enterprise cyber environment; modeling methods to develop a conceptual model of the cyber resilience management system; expert methods to evaluate the effectiveness of the proposed measures; as well as comparative analysis methods to compare national and international standards and practices for ensuring organizational cyber resilience.

Brief content of the thesis. The study analyzes the evolution of the concept of cyber resilience and its place in the enterprise information security system, examines the nature and classification of hybrid threats and their impact on the activities of modern organizations, and considers the regulatory and international standards in the field of cyber resilience. Based on the analysis of the information security system of a real enterprise, the level of its cyber resilience and vulnerabilities under hybrid threats is assessed, and key risks, incidents, and

problems in the functioning of the existing management system are identified. A model of the enterprise cyber resilience management system is proposed, a set of measures and tools to enhance it is substantiated, and the effectiveness of the proposed solutions and the forecast of the results of their implementation are evaluated.

Field of application. The results of the research and the developed recommendations can be used in the practical activities of enterprises in various sectors of the economy when forming and improving cyber resilience management systems, particularly under conditions of increasing intensity of hybrid threats, as well as in the educational process for training specialists in the field of cybersecurity and information technologies.

KEYWORDS: ENTERPRISE CYBER RESILIENCE, HYBRID THREATS, CYBER RESILIENCE MANAGEMENT SYSTEM, CYBERSECURITY, RISK MANAGEMENT, BUSINESS CONTINUITY, INFORMATION SECURITY INCIDENTS.

ЗМІСТ

ВСТУП

У сучасних умовах цифрової трансформації економіки та суспільства діяльність підприємств дедалі більше залежить від інформаційних технологій, мережевих сервісів і цифрових платформ. Паралельно з цим зростає кількість та складність кіберзагроз, які дедалі частіше поєднуються з елементами інформаційно-психологічного впливу, економічного тиску, дезінформації та інших проявів так званих гібридних загроз. Для України, що перебуває в умовах воєнного протистояння, проблема кіберстійкості підприємств набуває особливої ваги, оскільки кіберпростір став повноцінним полем боротьби, а атаки на інформаційні ресурси можуть мати критичні наслідки для стабільності бізнесу, економічної безпеки та національної стійкості загалом.
Традиційні підходи до інформаційної та кібербезпеки, орієнтовані переважно на запобігання інцидентам, уже не відповідають сучасним умовам, коли повністю уникнути кібератак практично неможливо. У зв’язку з цим актуалізується концепція кіберстійкості, яка передбачає не лише захист, а й здатність підприємства своєчасно виявляти загрози, ефективно реагувати на інциденти, забезпечувати безперервність бізнес-процесів і швидке відновлення після порушень. Формування та впровадження системи управління кіберстійкістю стає стратегічним завданням для підприємств різних галузей, особливо в умовах гібридних загроз, що поєднують технічні, організаційні та соціальні аспекти впливу.

Актуальність теми дослідження зумовлена зростанням інтенсивності та різноманітності гібридних загроз у кіберпросторі, високим рівнем цифровізації бізнес-процесів, недостатньою зрілістю систем управління кіберстійкістю на вітчизняних підприємствах, а також потребою адаптації міжнародних стандартів і кращих практик до умов функціонування підприємств в Україні. Відсутність комплексного підходу до управління

кіберстійкістю призводить до фрагментарності заходів безпеки, зниження ефективності реагування на інциденти та значних економічних втрат. Тому розроблення науково обґрунтованих рішень щодо формування та удосконалення системи управління кіберстійкістю підприємства є своєчасним і практично значущим завданням.

Метою магістерської роботи є теоретичне обґрунтування та розроблення практичних рекомендацій щодо формування й удосконалення системи управління кіберстійкістю підприємства в умовах гібридних загроз.

Об'єктом дослідження є процеси забезпечення кіберстійкості діяльності підприємства в умовах гібридних загроз.

Предметом дослідження є методи, моделі та механізми управління кіберстійкістю підприємства.

Для досягнення поставленої мети в роботі передбачається розв'язання таких завдань:

– проаналізувати сутність і зміст поняття кіберстійкості підприємства та її місце в системі інформаційної безпеки;

– дослідити природу гібридних загроз і особливості їх впливу на функціонування підприємств;

– узагальнити нормативно-правові засади та міжнародні стандарти у сфері кіберстійкості;

– проаналізувати наявну систему управління кіберстійкістю на досліджуваному підприємстві;

– оцінити рівень кіберстійкості та визначити ключові вразливості й ризики;

– розробити модель системи управління кіберстійкістю підприємства в умовах гібридних загроз;

– обґрунтувати комплекс заходів щодо підвищення кіберстійкості підприємства;

– здійснити оцінювання ефективності запропонованих рішень та визначити очікувані результати їх упровадження.

Методи дослідження. У процесі виконання магістерської роботи використано сукупність загальнонаукових і спеціальних методів пізнання. Теоретичне узагальнення, аналіз і синтез застосовано для дослідження наукових підходів до визначення сутності кіберстійкості та гібридних загроз. Методи системного та структурно-функціонального аналізу дали змогу розглянути систему управління кіберстійкістю як цілісну сукупність взаємопов'язаних елементів. Порівняльний аналіз використано для зіставлення національних і міжнародних стандартів та практик у сфері кібербезпеки й кіберстійкості. Експертні оцінки та методи аналізу ризиків застосовано для виявлення вразливостей і загроз у діяльності підприємства. Економіко-статистичні методи використано для оброблення показників, що характеризують наслідки кіберінцидентів. Моделювання застосовано під час розроблення пропонованої системи управління кіберстійкістю. Графічні та табличні методи використано для наочного подання результатів дослідження.

РОЗДІЛ 1 ТЕОРЕТИЧНІ ОСНОВИ КІБЕРСТІЙКОСТІ ПІДПРИЄМСТВА В УМОВАХ ГІБРИДНИХ ЗАГРОЗ

1.1. Сутність та еволюція поняття кіберстійкості в системі інформаційної безпеки підприємства

Кіберстійкість у системі інформаційної безпеки підприємства варто розглядати як результат еволюції поглядів на те, що саме означає «бути захищеним» у цифровому середовищі. Якщо класичне уявлення про інформаційну безпеку тривалий час концентрувалося на запобіганні порушенням та мінімізації ймовірності інциденту, то сучасна логіка кіберстійкості виходить із реалістичного припущення: інцидент не є винятком, він є неминучою подією в життєвому циклі організації. Саме тому кіберстійкість не протиставляє себе інформаційній безпеці, а розширює її зміст, зміщуючи акцент із «захистити будь-якою ціною» до «витримати удар, зберегти керованість, відновитися і навчитися на події».

Сутність кіберстійкості проявляється у здатності підприємства зберігати функціональність ключових бізнес-процесів навіть тоді, коли відбувається кібератака, внутрішня помилка, технічна відмова або зовнішній гібридний вплив. Це поняття охоплює не лише технічний аспект захисту мережі, серверів або робочих станцій, а й організаційну зрілість управління: наявність політик, процедур, ролей і відповідальностей, готовність персоналу діяти за сценаріями, ефективну взаємодію з підрядниками, провайдерами та державними структурами, а також здатність до швидкої переорієнтації на альтернативні канали, резервні контури, ручні процедури або тимчасові рішення. У цьому сенсі кіберстійкість безпосередньо пов’язана з безперервністю бізнесу, кризовим управлінням і загальною стійкістю підприємства як соціально-економічної системи.

Важливо підкреслити, що інформаційна безпека історично виростала з потреби забезпечувати конфіденційність, цілісність та доступність даних. Ця класична триада, відома як CIA, довгий час була рамкою, у якій будувалися політики доступу, системи контролю, антивірусний захист, шифрування та резервне копіювання. Проте у міру того, як цифрові технології почали прямо визначати здатність підприємства виробляти продукт, надавати послугу і отримувати дохід, стало очевидно, що недостатньо лише «захищати дані». Потрібно забезпечувати стійкість процесів, сервісів і взаємодій, які спираються на ці дані. Так відбулося розширення фокусу: від охорони інформаційного ресурсу до забезпечення життєздатності всієї цифрової екосистеми підприємства.

Еволюція поняття кіберстійкості тісно пов’язана зі змінами характеру загроз. На ранніх етапах інформатизації підприємства найчастіше стикалися з окремими вірусами, інцидентами несанкціонованого доступу або випадковими збоями. Поступово атаки стали цілеспрямованими і фінансово мотивованими: з’явилися професійні кіберзлочинні групи, експлуатація вразливостей, фішинг як інструмент соціальної інженерії, витоки даних як товар. Далі на перший план вийшли комплексні кампанії, коли технічна атака поєднується з дезінформацією, тиском на персонал, компрометацією постачальників або ланцюгів поставок, що особливо характерно для гібридних загроз. У таких умовах навіть підприємство з якісними засобами захисту може опинитися у ситуації, коли атака проходить «нижче порогу» традиційних систем контролю або реалізується через слабку ланку поза межами організації. Саме тоді критичною стає здатність підприємства не лише оборонятися, а й діяти під час порушення нормального режиму, швидко локалізувати наслідки і відновлювати керованість.

Кіберстійкість, на відміну від «статичної» безпеки, є динамічною характеристикою. Вона передбачає безперервний цикл підготовки та вдосконалення: підприємство формує профіль критичних активів, визначає

найбільш важливі бізнес-функції, оцінює допустимі межі простою, встановлює цільові показники відновлення, впроваджує резервування, сегментацію, моніторинг, процедури реагування, а після інцидентів проводить аналіз причин і оновлює контрольні заходи. Важливо, що кіберстійкість має «навчальний компонент»: організація підвищує власну здатність протистояти атакам через накопичення досвіду, тренування, моделювання інцидентів та відпрацювання планів реагування. Тобто це не одноразовий проєкт, а постійно діючий управлінський механізм.

У системі інформаційної безпеки підприємства кіберстійкість можна уявити як концептуальний «надбудовний» рівень, що інтегрує технічні заходи із корпоративним управлінням ризиками та безперервністю бізнесу. Технічні засоби, такі як контроль доступу, шифрування, багатофакторна автентифікація, системи виявлення вторгнень або резервне копіювання, залишаються важливими. Проте в рамках кіберстійкості вони отримують інше призначення: не лише запобігти проникненню, а й забезпечити швидке обмеження поширення атаки, збереження мінімально необхідних сервісів, можливість відновлення з гарантованою цілісністю та скорочення часу від простою до відновлення. Це змінює критерії ефективності безпеки: оцінюють не тільки кількість заблокованих атак, але й готовність підприємства працювати в умовах порушення нормального режиму, оперативність прийняття рішень, узгодженість дій, наявність комунікаційних каналів, контроль репутаційних наслідків та правові аспекти інциденту.

Окремо слід акцентувати, що кіберстійкість формується на перетині трьох площин: технологій, людей і процесів. Технології створюють інструменти захисту і відновлення, але без компетентного персоналу вони або неправильно налаштовуються, або не дають очікуваного ефекту. Люди, у свою чергу, потребують чітких процесів: хто приймає рішення під час інциденту, хто відповідає за ізоляцію сегмента, хто комунікує з клієнтами та партнерами, хто готує юридичні повідомлення, хто фіксує докази для розслідування.

Процеси повинні бути формалізованими і відпрацьованими, інакше підприємство в кризовий момент діятиме хаотично, що збільшує збитки. Власне, зріла кіберстійкість – це коли підприємство може діяти злагоджено під тиском часу, невизначеності та інформаційних маніпуляцій, що характерно для гібридних загроз.

Якщо узагальнити еволюційний шлях, то підприємства пройшли декілька логічних переходів. Спочатку безпека була переважно «периметровою», коли достатнім вважалися антивірус, фаєрвол і контроль доступу. Потім, з поширенням хмарних технологій, віддаленої роботи та мобільності, стало зрозуміло, що периметр розмитий, а загроза може бути як зовні, так і зсередини. Далі посилився управлінський підхід: з'явилися системи менеджменту інформаційної безпеки, аудити, політики, відповідність стандартам. І вже наступним кроком стала кіберстійкість як інтеграція безпеки з управлінням ризиками та безперервністю, де головним питанням є не «чи станеться інцидент», а «наскільки швидко і контрольовано ми зможемо повернутися до прийнятного рівня роботи». Саме ця логіка найбільш адекватна умовам гібридних загроз, коли атака може бути частиною більшого сценарію впливу, і підприємство має забезпечувати стійкість не тільки IT-ландшафту, а й управлінських і комунікаційних механізмів.

Таблиця 1.1

Еволюція підходів до забезпечення кіберстійкості підприємства

Етап розвитку	Період формування	Ключовий фокус	Основні характеристики підходу	Обмеження підходу
Периметрова інформаційна безпека	1990-ті – поч. 2000-х рр.	Захист від зовнішніх загроз	Орієнтація на антивірусний захист, міжмережеві екрани, контроль доступу; уявлення про	Недостатня увага до внутрішніх загроз, соціальної інженерії та складних атак

			чіткий «периметр» мережі підприємства	
Управління інформаційною безпекою	2000-ті рр.	Системність і стандартизація	Запровадження політик безпеки, процедур, аудитів; використання стандартів ISO/IEC 27001; управління ризиками	Формалізм та орієнтація на відповідність стандартам більше, ніж на реальні сценарії атак
Кібербезпека як технологічний захист	2010-ті рр.	Виявлення та реагування	Використання SIEM, IDS/IPS, SOC, моніторинг інцидентів у реальному часі, проактивне реагування	Зосередженість на IT-рівні без повної інтеграції з бізнес-процесами
Кіберстійкість	з кінця 2010-х рр. – дотепер	Стійкість і відновлення бізнесу	Інтеграція кібербезпеки, управління ризиками та безперервності бізнесу; готовність до неминучих інцидентів; швидке відновлення та адаптація	Високі вимоги до організаційної зрілості та ресурсів
Кіберстійкість в умовах гібридних загроз	2020-ті рр.	Комплексна стійкість до багатовимірного впливу	Урахування поєднання кібератак, дезінформації, тиску на персонал, атак на ланцюги	Складність прогнозування сценаріїв і необхідність міждисциплінарного підходу

			постачання; акцент на управлінські рішення та комунікації	

Наведена в таблиці 1.1 еволюція підходів до забезпечення кіберстійкості підприємства свідчить про поступовий перехід від вузького технічного розуміння безпеки до комплексної управлінської концепції, орієнтованої на забезпечення стійкості бізнесу в умовах постійних і багатовимірних загроз. Зміна акцентів з периметрового захисту на системне управління, а згодом на інтеграцію кібербезпеки з управлінням ризиками та безперервністю діяльності відображає зростаючу роль інформаційних технологій у формуванні конкурентоспроможності підприємств та їх економічної стабільності.

Аналіз етапів розвитку дозволяє зробити висновок, що сучасна кіберстійкість формується не як заперечення попередніх підходів, а як їх логічне узагальнення та розширення. Технічні засоби захисту, характерні для перших етапів, залишаються необхідною основою, однак у межах кіберстійкості вони розглядаються лише як один із елементів складної системи, що включає організаційні механізми, управлінські рішення, кадрову політику та корпоративну культуру безпеки. Водночас формалізовані системи менеджменту інформаційної безпеки набувають практичного змісту через орієнтацію не лише на відповідність стандартам, а й на реальні сценарії загроз та інцидентів.

Особливої актуальності концепція кіберстійкості набуває в умовах гібридних загроз, коли підприємство стикається не лише з технічними кібератаками, а й з інформаційно-психологічним впливом, маніпуляціями, спробами дестабілізації управлінських процесів, компрометацією ланцюгів постачання та тиском на персонал. За таких умов ефективність системи інформаційної безпеки визначається не тільки здатністю запобігати

інцидентам, а передусім можливістю підтримувати критично важливі функції, забезпечувати узгодженість дій підрозділів та оперативно відновлюватися після порушень. Це зумовлює необхідність інтеграції кіберстійкості в загальну систему стратегічного управління підприємством.

Кіберстійкість у сучасному розумінні постає як багатовимірна характеристика підприємства, що відображає його спроможність передбачати кіберзагрози, протидіяти їм, адаптуватися до змін середовища та відновлювати працездатність із мінімальними втратами для бізнесу, репутації та довіри стейкхолдерів. Вона поєднує технічні, організаційні та управлінські компоненти в єдину систему, орієнтовану на забезпечення сталого функціонування підприємства в умовах цифрової невизначеності.

Перехід до концепції кіберстійкості є об’єктивною відповіддю на ускладнення характеру загроз та зростання залежності підприємств від цифрової інфраструктури. Саме тому подальше дослідження має бути спрямоване на визначення особливостей формування та функціонування системи управління кіберстійкістю на конкретному підприємстві, а також на розроблення практичних рекомендацій щодо її удосконалення в умовах гібридних загроз.

1.2. Гібридні загрози: природа, класифікація та їх вплив на діяльність сучасних підприємств

Гібридні загрози в сучасному цифровому середовищі є однією з найскладніших і водночас найнебезпечніших форм впливу на діяльність підприємств, оскільки вони поєднують у собі різнорідні інструменти тиску, що діють синхронно та взаємопідсилюють один одного. Їх природа полягає у використанні не одного ізольованого каналу атаки, а комплексу технічних, інформаційних, економічних, соціальних і навіть правових засобів, спрямованих на досягнення стратегічної мети – дестабілізації діяльності організації, підриву її стійкості, репутації та здатності до ефективного

управління. На відміну від класичних кіберзагроз, які переважно мають чітко окреслений технічний характер, гібридні загрози формують багатовимірний простір протиборства, де кібератаки є лише одним із елементів загальної кампанії впливу.

Природа гібридних загроз зумовлена трансформацією сучасних конфліктів і конкурентної боротьби у бік так званих «сірих зон», у яких важко чітко ідентифікувати джерело атаки, відокремити злочинну активність від політичного чи економічного тиску та визначити момент переходу від нормального стану до кризового. Для підприємств це означає, що загроза може розгортатися поступово, маскуватися під легітимну діяльність, використовувати вразливості не лише в IT-інфраструктурі, а й у системі управління, корпоративній культурі, взаєминах із партнерами та клієнтами. Гібридний вплив часто має прихований характер, коли окремі інциденти здаються несуттєвими або випадковими, але в сукупності формують цілеспрямований сценарій дестабілізації.

У змістовному вимірі гібридні загрози охоплюють поєднання кібернетичних атак із інформаційно-психологічним впливом, маніпуляцією суспільною думкою, економічним тиском, використанням юридичних інструментів для блокування діяльності, а також залученням інсайдерів чи компрометацією персоналу. Кібератака в такому випадку може виконувати роль каталізатора, який відкриває доступ до даних або порушує роботу сервісів, після чого розгортається хвиля дезінформації, спрямована на дискредитацію підприємства, підрив довіри клієнтів та партнерів або створення панічних настроїв серед персоналу. Усе це формує комплексний тиск, який значно перевищує ефект від окремої технічної атаки.

Класифікація гібридних загроз у контексті діяльності підприємств ґрунтується на їх багатокомпонентній природі та способах впливу на організацію. За змістом впливу вони охоплюють кібернетичний вимір, пов’язаний із несанкціонованим доступом до інформаційних систем,

порушенням цілісності даних, блокуванням сервісів або компрометацією інфраструктури. Поряд із цим формується інформаційний вимір, який проявляється у поширенні неправдивих або маніпулятивних повідомлень про діяльність підприємства, його фінансовий стан, якість продукції чи етичність управління. Економічний вимір гібридних загроз реалізується через тиск на фінансові потоки, зрив контрактів, втручання в ланцюги постачання або створення штучних бар'єрів для доступу до ринків. Соціальний вимір пов'язаний із впливом на персонал, формуванням атмосфери недовіри, страху або демотивації, а правовий – із використанням судових процесів, скарг і регуляторних механізмів як інструменту тиску.

За джерелами походження гібридні загрози можуть формуватися як зовнішніми акторами, зокрема конкурентами, організованими кіберзлочинними угрупованнями або структурами, пов'язаними з іноземними державами, так і внутрішніми суб'єктами у вигляді незадоволених працівників, інсайдерів чи підрядників, які мають доступ до критичних ресурсів. Особливість гібридних сценаріїв полягає в тому, що внутрішні та зовнішні чинники часто поєднуються: зовнішній вплив підсилюється через використання внутрішніх слабких місць підприємства, людського фактору або прогалин в організації процесів.

За часовою динамікою гібридні загрози можуть реалізовуватися як у формі швидких кризових кампаній, спрямованих на досягнення ефекту за короткий період, так і у вигляді тривалого латентного впливу, коли атака розгортається поступово, непомітно накопичуючи критичні порушення в системі. У другому випадку підприємство може тривалий час не усвідомлювати масштабу проблеми, що суттєво ускладнює реагування і збільшує потенційні збитки.

Вплив гібридних загроз на діяльність сучасних підприємств має комплексний характер і виходить далеко за межі суто технічних наслідків. На операційному рівні вони можуть призводити до зупинки виробництва,

порушення логістики, недоступності ключових сервісів, втрати або спотворення даних, що безпосередньо відображається на здатності виконувати зобов'язання перед клієнтами та партнерами. Навіть короткочасні збої в цифрових системах здатні спричинити ланцюгову реакцію, коли порушення в одному підрозділі призводять до зупинки пов'язаних процесів у всій організації.

На економічному рівні наслідки гібридних загроз проявляються у прямих фінансових втратах, пов'язаних із простоєм, відновленням систем, виплатами компенсацій, штрафами та зростанням витрат на безпеку, а також у непрямих збитках, що виникають через втрату клієнтів, зниження ринкової вартості та погіршення інвестиційної привабливості. Особливо небезпечними є ситуації, коли гібридний вплив підриває довгострокові стратегічні позиції підприємства, обмежуючи його можливості для розвитку та інновацій.

Не менш значущим є репутаційний вплив гібридних загроз. У сучасному інформаційному просторі негативні повідомлення поширюються з високою швидкістю, і навіть тимчасовий інцидент може бути інтерпретований як ознака системної неспроможності або ненадійності підприємства. Втрата довіри клієнтів, партнерів і суспільства часто має довготривалі наслідки, подолання яких потребує значно більше ресурсів, ніж технічне відновлення систем. Для підприємств, що працюють у сферах із високими вимогами до надійності, таких як фінанси, енергетика, транспорт або охорона здоров'я, репутаційні ризики можуть мати критичний характер.

На управлінському рівні гібридні загрози створюють ситуацію постійної невизначеності, коли керівництво змушене приймати рішення в умовах дефіциту достовірної інформації, тиску часу та зовнішнього впливу. Це підвищує роль кризового менеджменту, внутрішніх комунікацій і здатності до швидкої координації дій між підрозділами. Неефективні управлінські рішення в умовах гібридної атаки можуть значно посилити негативні наслідки навіть за відносно обмеженого технічного інциденту.

Таблиця 1.2

Класифікація гібридних загроз та їх вплив на діяльність підприємства

Вид гібридної загрози	Зміст та характер впливу	Основні канали реалізації	Ключові наслідки для підприємства	Приклади прояву
Кібернетичні	Спрямовані на порушення роботи IT-інфраструктури, доступності сервісів і цілісності даних	Шкідливе ПЗ, фішинг, експлуатація вразливостей, DDoS-атаки	Зупинка процесів, втрата або спотворення даних, простій систем	Шифрування серверів, блокування сайту, компрометація облікових записів
Інформаційно-психологічні	Маніпулятивний вплив на репутацію та сприйняття діяльності підприємства	Соціальні мережі, ЗМІ, фейкові акаунти, витоки інформації	Втрата довіри клієнтів і партнерів, репутаційні збитки	Поширення фейкових новин про фінансові проблеми
Економічні	Створення фінансового та ринкового тиску на підприємство	Зрив контрактів, демпінг, атаки на ланцюги постачання	Фінансові втрати, зниження прибутковості	Блокування поставок через злам систем партнера
Соціальні	Вплив на персонал і внутрішній клімат організації	Соціальна інженерія, шантаж, компрометація працівників	Демотивація, плинність кадрів, витоки інформації	Фішинг-листи працівникам із вимогою розголошення даних
Правові	Використання юридичних механізмів як інструменту тиску	Судові позови, скарги регуляторам, блокування ліцензій	Штрафи, витрати на правовий захист, зупинка діяльності	Масові скарги після інформаційної кампанії
Комбіновані	Поєднання кількох видів впливу в єдиному сценарії	Кібератаки разом з дезінформацією та	Системна дестабілізація роботи підприємства	Кібератака з подальшою медіакампанією і зривом контрактів

		економічним тиском		

Важливим аспектом є також соціально-психологічний вплив гібридних загроз на персонал підприємства. Постійна напруга, страх перед витоками даних, відповідальністю за інциденти, можливістю скорочень або втрати стабільності формують стан хронічного стресу, що негативно позначається на продуктивності праці та лояльності працівників. У таких умовах людський фактор може стати як додатковим джерелом уразливості, так і ключовим ресурсом для подолання кризи, залежно від рівня підготовки та корпоративної культури.

Аналіз видів гібридних загроз свідчить про їхню здатність взаємно підсилювати одна одну. Кібернетичний інцидент, навіть обмежений за масштабами, може стати тригером для інформаційної кампанії, що дискредитує підприємство в очах клієнтів і партнерів, або для економічного тиску через зрив контрактів та порушення ланцюгів постачання. У таких умовах наслідки атаки значно перевищують прямі технічні збитки і трансформуються у довгострокові репутаційні та фінансові втрати. Це означає, що ефективна протидія гібридним загрозам неможлива в межах ізольованого підходу до кібербезпеки та потребує міждисциплінарної взаємодії різних функціональних підрозділів підприємства.

Важливою особливістю гібридних загроз є їхній латентний характер і складність своєчасної ідентифікації. На початкових етапах вплив може маскуватися під звичайні технічні збої, ринкові коливання або інформаційний шум, що ускладнює відокремлення цілеспрямованої атаки від випадкових подій. У результаті підприємство ризикує втратити час, необхідний для локалізації проблеми, а накопичення дрібних інцидентів поступово формує критичний рівень дестабілізації. Це підкреслює необхідність постійного

моніторингу не лише IT-середовища, а й зовнішнього інформаційного поля та внутрішнього стану організації.

З огляду на комплексний характер гібридних загроз, зростає роль людського та управлінського факторів у системі забезпечення кіберстійкості. Навіть за наявності сучасних технічних засобів захисту вирішальним може стати рівень підготовки персоналу, чіткість процедур реагування та здатність керівництва до швидкого прийняття рішень в умовах невизначеності. Помилки в комунікації, несвоєчасне інформування або суперечливі управлінські дії здатні суттєво посилити негативний ефект гібридного впливу, тоді як злагодженість і прозорість дій сприяють зменшенню втрат і відновленню довіри стейкхолдерів.

Результати класифікації гібридних загроз і аналіз їхнього впливу на діяльність підприємства підтверджують, що сучасне середовище безпеки характеризується високим рівнем складності, динамічності та невизначеності. У цих умовах підприємство має орієнтуватися не лише на мінімізацію ймовірності окремих інцидентів, а на формування здатності витримувати багатовекторний тиск, зберігати керованість і забезпечувати відновлення ключових функцій. Саме це зумовлює необхідність переходу до системного управління кіберстійкістю як інтегрованої складової загальної системи менеджменту підприємства.

1.3. Нормативно-правові та міжнародні стандарти забезпечення кіберстійкості організацій

Нормативно-правове та стандартне забезпечення кіберстійкості організацій формується на перетині двох площин: національного регулювання, яке встановлює обов’язкові правила та відповідальність, і міжнародних стандартів та рамкових підходів, які задають «мову» управління ризиками, інцидентами й безперервністю бізнесу. Для підприємства це

означає, що кіберстійкість не може будуватися виключно як технічний набір засобів захисту, адже значна частина вимог стосується управління, ролей, процесів, доказовості контролів, реагування на інциденти, захисту персональних даних і забезпечення стійкості критичних функцій.

У вітчизняному правовому полі базовою опорою є Закон України «Про основні засади забезпечення кібербезпеки України», який визначає організаційні та правові засади функціонування системи кібербезпеки, ролі суб'єктів у цій сфері та загальну рамку державної політики у протидії кіберзагрозам. Для підприємств практичне значення цього закону полягає в тому, що він закладає логіку взаємодії з державними інституціями, визначає важливість побудови організаційних механізмів захисту, а також підкреслює, що кібербезпека є системною функцією, а не разовим технічним проєктом.
Другою ключовою складовою є Закон України «Про захист інформації в інформаційно-комунікаційних системах», який регулює відносини у сфері захисту інформації в ІКС та задає нормативну основу для встановлення вимог до захисту інформаційних ресурсів і процедур в організаціях. Його актуальність для теми кіберстійкості полягає в тому, що він фіксує обов'язковість організаційних і технічних заходів захисту інформації, тобто формує мінімальний «гігієнічний» рівень, від якого вже будується зріліша модель кіберстійкості (із реагуванням, відновленням і безперервністю).

Окремий блок правових вимог пов'язаний із персональними даними. Закон України «Про захист персональних даних» встановлює правила обробки персональних даних і спрямований на захист прав і свобод людини під час такої обробки; для підприємств це прямо трансформується у вимоги до політик доступу, контролю обробки, інцидент-менеджменту щодо витоків та дисципліни роботи з даними клієнтів і працівників. У контексті кіберстійкості важливо, що витік персональних даних зазвичай запускає одразу кілька типів наслідків: технічні (локалізація інциденту), правові (виконання вимог

законодавства) та репутаційні (довіра клієнтів), а отже вимоги до захисту персональних даних органічно «вшиваються» у комплексну модель стійкості. Для підприємств, які належать або дотичні до критичної інфраструктури, суттєвого значення набуває Закон України «Про критичну інфраструктуру», який окреслює засади функціонування та захисту критичної інфраструктури й прямо вказує на важливість кіберзахисту/кібербезпеки об’єктів цієї сфери. Практична «прикладна» площина деталізується урядовими актами, зокрема Загальними вимогами до кіберзахисту об’єктів критичної інфраструктури (у профільних оглядах держорганів вони прив’язуються до постанови КМУ № 519 від 19.06.2019). Для підприємства це означає перехід від загальних декларацій до конкретизації: які класи систем мають бути захищені, як організовується реагування, як здійснюється контроль виконання вимог та взаємодія у випадку інцидентів.

Паралельно із національним регулюванням підприємства орієнтуються на міжнародні стандарти, які дозволяють побудувати керовану систему кіберстійкості, що є зрозумілою для партнерів, аудиторів, інвесторів і регуляторів у різних юрисдикціях. Центральне місце займає ISO/IEC 27001:2022 як стандарт вимог до системи менеджменту інформаційної безпеки (ISMS): він задає логіку управління ризиками, політик, ролей, контролю, вимірюваності та безперервного поліпшення, тобто переводить безпеку з «набору інструментів» у формат управлінського циклу. Водночас ISO/IEC 27002:2022 надає деталізований «каталог» і практичні настанови щодо контролів (від доступу й криптографії до реагування на інциденти), що дозволяє організації обґрунтовано наповнювати систему управління безпекою конкретними заходами й узгоджувати їх із ризиками. У контексті кіберстійкості ці стандарти важливі тим, що допомагають формалізувати керованість: визначити, які активи критичні, які ризики прийнятні, які контролі впроваджуються і як перевіряється їх ефективність.

Оскільки кіберстійкість виходить за межі запобігання інцидентам і фокусується на здатності підтримувати критичні функції та відновлюватися, значну роль відіграють стандарти безперервності бізнесу. ISO 22301:2019 визначає вимоги до системи менеджменту безперервності бізнесу (BCMS) і фактично «підключає» кіберінциденти до загальної логіки стійкості організації: оцінювання впливу на бізнес, планування відновлення, узгодження ролей, випробування планів і вдосконалення після кризових подій. У практиці підприємства саме зв'язка ISO/IEC 27001 (керування безпекою та ризиками) і ISO 22301 (керування безперервністю) формує міцну основу кіберстійкості, коли захист і відновлення розглядаються як дві частини єдиного управлінського механізму.

Для операційної зрілості кіберстійкості критично важливими є стандартизовані підходи до реагування на інциденти та управління контролями. У цьому контексті широко застосовуються публікації NIST, які практично описують процеси і надають універсальну «сітку координат» для оцінки рівня зрілості. NIST Cybersecurity Framework 2.0 (опублікований 26 лютого 2024 року) прямо позиціонується як інструмент, що допомагає організаціям розуміти, оцінювати, пріоритезувати та комунікувати кіберризики, а також вибудовувати управління ними на рівні організації. Для інцидент-менеджменту NIST підтримує спеціалізовані керівництва; при цьому важливо враховувати актуальність версій: NIST SP 800-61 Rev.2 у 2025 році був архівований (withdrawn), а оновлена редакція Rev.3 доступна як актуальніша база для організації реагування. Для побудови «контрольного каркасу» організації часто використовують NIST SP 800-53 Rev.5 як каталог контрольних заходів безпеки та приватності, який допомагає структурувати вимоги і підбирати контролі під профіль ризиків і середовище загроз.

Окремо варто враховувати європейський регуляторний контур, що безпосередньо впливає на підприємства, які працюють із контрагентами в ЄС, входять до ланцюгів постачання або мають компанії/філії в європейській

юрисдикції. Директива NIS2 вводить посилені вимоги до кіберризик-менеджменту, звітності про інциденти та нагляду/відповідальності для ширшого кола секторів і суб'єктів у ЄС, що фактично підвищує «планку очікувань» до кіберстійкості навіть для компаній поза ЄС через вимоги ланцюгів постачання. Для фінансового сектору ЄС діє DORA (Regulation (EU) 2022/2554), який застосовується з 17 січня 2025 року і фокусується на цифровій операційній стійкості, включно з управлінням ІКТ-ризиками, інцидентами та ризиками третіх сторін, що особливо релевантно темі кіберстійкості підприємств, які залежать від провайдерів і хмарних сервісів.

Таблиця 1.3

Нормативно-правові та міжнародні стандарти забезпечення кіберстійкості організацій

Нормативний акт / стандарт	Рівень застосування	Сфера регулювання	Ключова спрямованість вимог	Значення для кіберстійкості підприємства
Закон України «Про основні засади забезпечення кібербезпеки України»	Національний	Кібербезпека держави та суб'єктів господарювання	Визначення принципів, суб'єктів і завдань у сфері кібербезпеки	Формує організаційну основу побудови системи кіберзахисту та взаємодії з державними структурами
Закон України «Про захист інформації в інформаційно-комунікаційних системах»	Національний	Захист інформації в ІКС	Встановлення вимог до організаційних і технічних заходів захисту	Забезпечує базовий рівень інформаційної безпеки як фундамент кіберстійкості
Закон України «Про захист	Національний	Обробка та захист	Регламентація прав суб'єктів даних і	Інтегрує правові, технічні та

персональних даних»		персональних даних	обов’язків володільців	організаційні аспекти захисту даних у систему кіберстійкості
Закон України «Про критичну інфраструктуру» та підзаконні акти	Національний	Захист об’єктів критичної інфраструктури	Вимоги до стійкості та безпеки критичних систем	Орієнтує підприємства на пріоритетний захист критичних функцій і безперервність діяльності
ISO/IEC 27001:2022	Міжнародний	Система менеджменту інформаційної безпеки	Управління ризиками, політики, контроль та постійне вдосконалення	Створює управлінський каркас для системного забезпечення кіберстійкості
ISO/IEC 27002:2022	Міжнародний	Контролі інформаційної безпеки	Рекомендації щодо впровадження організаційних і технічних заходів захисту	Надає практичний інструментарій для наповнення системи кіберстійкості
ISO 22301:2019	Міжнародний	Безперервність бізнесу	Планування відновлення та управління кризами	Забезпечує зв’язок кіберінцидентів із відновленням бізнес-процесів
NIST Cybersecurity Framework 2.0	Міжнародний (де-факто)	Управління кіберризиками	Ідентифікація, захист, виявлення, реагування, відновлення та управління	Формує практичну модель побудови та оцінювання

				кіберстійкості
NIST SP 800-53 Rev.5	Міжнародний (де-факто)	Контролі безпеки та приватності	Каталог технічних і організаційних заходів безпеки	Допомагає структурувати систему контролів відповідно до профілю ризиків
Директива ЄС NIS2 та Регламент DORA	Регіональний (ЄС)	Кібер- та цифрова операційна стійкість	Посилені вимоги до управління ризиками, інцидентами та відповідальності	Визначає підвищені очікування до кіберстійкості підприємств у ланцюгах постачання ЄС

У підсумку нормативно-правові акти України задають обов’язкові рамки відповідальності та мінімальні вимоги до захисту інформації, персональних даних і (за потреби) критичної інфраструктури, тоді як міжнародні стандарти та рамкові підходи на кшталт ISO/IEC 27001–27002, ISO 22301 і NIST CSF дозволяють побудувати керовану, вимірювану та відтворювану систему кіберстійкості, яка витримує аудит, масштабування і підвищує довіру партнерів. Саме поєднання правових вимог із стандартами управління створює практичну основу для формування корпоративної системи управління кіберстійкістю в умовах гібридних загроз: підприємство не лише «виконує закон», а й отримує цілісну модель управління ризиками, реагуванням та відновленням, яка підтримує безперервність бізнесу і конкурентоспроможність.

Узагальнення, наведене в таблиці 1.3, засвідчує, що нормативно-правове та стандартне забезпечення кіберстійкості організацій формується як багаторівнева система, у якій національні правові акти визначають обов’язкові рамки відповідальності та мінімальні вимоги до захисту інформаційних

ресурсів, тоді як міжнародні стандарти задають методологію управління ризиками, інцидентами та безперервністю бізнесу. Таке поєднання дозволяє підприємствам не лише виконувати законодавчі вимоги, а й вибудовувати внутрішню систему управління кіберстійкістю відповідно до кращих світових практик.

Аналіз змісту стандартів свідчить, що ключовим є їхній управлінський характер. ISO/IEC 27001 орієнтує організацію на побудову циклічної моделі управління інформаційною безпекою, у межах якої ризики ідентифікуються, оцінюються та обробляються на постійній основі, а ефективність заходів контролю регулярно переглядається. У поєднанні з рекомендаціями ISO/IEC 27002 це створює структурований інструментарій, який дозволяє підприємству адаптувати заходи захисту до власного профілю загроз і ресурсних можливостей. Водночас ISO 22301 розширює цей підхід, інтегруючи кіберінциденти в загальну систему забезпечення безперервності бізнесу та відновлення критичних процесів після кризових подій, що є сутнісною характеристикою кіберстійкості.

Міжнародні рамкові підходи NIST, зокрема Cybersecurity Framework, доповнюють стандарти ISO практичною логікою побудови процесів і взаємозв’язків між ними, що полегшує впровадження системи управління кіберстійкістю в організаціях із різним рівнем зрілості. Їхня цінність полягає у можливості оцінювання поточного стану, визначення цільового профілю та планування поетапного розвитку спроможностей, що особливо важливо для підприємств, які лише розпочинають системне впровадження управління кіберризиками.

Суттєвого значення набуває також європейський регуляторний контур, сформований директивою NIS2 та регламентом DORA, які фактично підвищують вимоги до кібер- та цифрової операційної стійкості організацій, що залучені до ланцюгів постачання Європейського Союзу або співпрацюють із європейськими партнерами. Навіть для підприємств, що формально не

підпадають під дію цих актів, вони стають орієнтиром очікуваного рівня зрілості системи управління кіберстійкістю, оскільки партнери дедалі частіше вимагають підтвердження відповідності таким підходам у межах договірних відносин.

Узгодження національних правових вимог із міжнародними стандартами дозволяє підприємству сформувати цілісну систему управління кіберстійкістю, у якій правові норми визначають межі допустимого та відповідальність, а стандарти надають інструменти практичної реалізації цих вимог у вигляді політик, процедур, процесів і контрольних заходів. У такій системі кіберстійкість перестає бути ізольованою функцією служби IT або безпеки і трансформується в складову корпоративного управління, що інтегрується в стратегічне планування, управління ризиками та систему внутрішнього контролю підприємства.

РОЗДІЛ 2 АНАЛІЗ СТАНУ ТА ПРОБЛЕМ УПРАВЛІННЯ КІБЕРСТІЙКІСТЮ НА ПІДПРИЄМСТВІ

2.1. Характеристика підприємства та організація системи інформаційної безпеки

Для проведення аналізу стану управління кіберстійкістю доцільно обрати підприємство, яке одночасно є технологічно складним, суспільно значущим і має реальні прецеденти впливу гібридних загроз. Таким підприємством є **Kyivstar (ПрАТ «Київстар»)** — найбільший оператор електронних комунікацій в Україні, що надає послуги мобільного зв'язку та фіксованого доступу до інтернету для масового та корпоративного сегментів. Масштаб діяльності компанії підтверджується кількістю абонентів: за даними публічної звітності/профілю для інвесторів, станом на кінець 2024 року Kyivstar обслуговував понад **23 млн мобільних** та понад **1,1 млн фіксованих широкосмугових** абонентів, що робить його інфраструктуру однією з найкритичніших для цифрової стійкості країни. Додатково офіційна довідка компанії вказує на порівнянні показники на 2025 рік і підкреслює фокус на розвитку фіксованої мережі та технологій доступу (зокрема FTTB/GPON), що демонструє високу залежність бізнесу від безперебійної роботи мережі та IT-систем.

Специфіка Kyivstar полягає в тому, що він функціонує як **оператор критично важливих цифрових сервісів**, у яких відмова або деградація доступності має прямий ефект на економіку, державні та муніципальні сервіси, екстрені комунікації, а також на діяльність мільйонів користувачів і тисяч бізнес-клієнтів. Технологічний контур підприємства включає мобільну радіомережу та транспортну мережу передачі даних, ядро мобільної мережі, системи керування мережею, білінгові платформи та CRM, інфраструктуру

обслуговування клієнтів, корпоративні IT-сервіси, а також цифрові B2B-продукти. Це важливо для теми кіберстійкості, адже для оператора такого класу цільовим об’єктом захисту є не лише дані, а насамперед **безперервність надання послуг** і збереження керованості мережі в умовах атак і криз.

Останніми роками Kyivstar розширює цифрову складову бізнесу та пропонує підприємствам інструменти роботи з даними та хмарні сервіси, що додатково підвищує вимоги до інформаційної безпеки. Зокрема, компанія розвиває рішення на кшталт **Data platform (DWH)** для консолідації та аналітики даних бізнес-клієнтів, що означає роботу з великими масивами інформації, інтеграцію різних джерел та підвищену увагу до контролю доступу, журналювання і захисту від витоків. Також публічно комунікується розвиток **Kyivstar Cloud** як інфраструктурного сервісу для організацій, де типовими сценаріями є розміщення CRM/ERP, віртуальних машин, віддалених робочих середовищ, резервного копіювання та гібридних моделей із інтеграцією з глобальними хмарними платформами.

Усе це означає, що інформаційна безпека у Kyivstar має охоплювати як телеком-інфраструктуру, так і класичні IT/хмарні контури, а отже організація системи ІБ неминуче є багаторівневою.

Організація системи інформаційної безпеки на підприємствах такого типу зазвичай спирається на поєднання управлінського рівня та операційного рівня. На управлінському рівні формуються політики та правила, визначається модель відповідальності, порядок класифікації активів і даних, принципи доступу, вимоги до постачальників і підрядників, а також вимоги до реагування на інциденти. На операційному рівні реалізуються технологічні та процедурні механізми, що забезпечують моніторинг, виявлення атак, локалізацію наслідків і відновлення сервісів. Для Kyivstar така модель є критичною, оскільки одночасно необхідно підтримувати високий рівень доступності мережі та протистояти інтенсивному тиску з боку противника в умовах війни.

Практичну значущість питання організації інформаційної безпеки у Kyivstar підтверджує реальний досвід масштабного кібервпливу. У пресрелізі материнської групи VEON зазначено, що **12 грудня 2023 року** мережа Kyivstar зазнала однієї з найбільших кібератак у глобальному телеком-секторі, що призвело до недоступності комунікаційних сервісів для абонентів і вимагало поетапного відновлення послуг.

Публічні повідомлення також свідчать, що компанія протягом повномасштабної війни витримувала численні атаки різної тактики, включно з DDoS та спробами проникнення, а інцидент 2023 року став якісно іншим за масштабом і наміром порушити роботу інфраструктури. Сам факт такого інциденту є ключовим для розділу 2, оскільки дозволяє аналізувати не теоретичну «готовність», а реальні проблеми, залежності та вузькі місця системи управління кіберстійкістю.

У таких умовах інформаційна безпека Kyivstar закономірно має орієнтуватися на підтримання керованості в кризі, а не лише на профілактику. Це означає, що поряд із класичними заходами захисту периметра та кінцевих точок критичними стають сегментація середовищ, резервування, контроль привілеїв, постійний моніторинг подій безпеки та механізми аварійного відновлення. Для телеком-оператора центральним об’єктом захисту виступає **віртуалізована та програмно-керована інфраструктура**, оскільки саме вона визначає, наскільки швидко можна відновити надання послуг після руйнівної атаки. Із цього випливає, що системи управління конфігураціями, резервне копіювання критичних компонентів, відпрацьовані процедури відновлення та кризові комунікації стають елементами не «додатковими», а базовими для управління кіберстійкістю.

Крім того, для підприємства масштабу Kyivstar важливим компонентом організації ІБ є управління ризиками третіх сторін і ланцюгів постачання. Значна частина функціонування мережі й ІТ-ландшафту залежить від постачальників обладнання, програмних платформ, сервісних підрядників та

хмарних інтеграцій, а отже вимоги до безпеки повинні формалізуватися не лише внутрішніми політиками, але й контрактними умовами, аудитами та контролем доступів підрядників. Це безпосередньо корелює з характером гібридних загроз, де атака може реалізовуватися через суміжні організації або через компрометацію облікових записів і процесів підтримки.

Таблиця 2.1

Загальна характеристика ПрАТ «Київстар» та організація системи інформаційної безпеки

Показник	Характеристика
Повна назва підприємства	Приватне акціонерне товариство «Київстар»
Сфера діяльності	Надання послуг мобільного зв’язку, фіксованого інтернету, передачі даних, цифрових і хмарних сервісів для фізичних та юридичних осіб
Роль у національній економіці	Найбільший оператор електронних комунікацій в Україні, об’єкт критичної інфраструктури, що забезпечує зв’язок для населення, бізнесу та державних структур
Масштаб діяльності	Понад 23 млн абонентів мобільного зв’язку та понад 1 млн користувачів фіксованого інтернету, розгалужена мережа по всій території України
Ключові цифрові активи	Мобільна та транспортна мережі, ядро мережі, білінгові системи, CRM, дата-центри, хмарна інфраструктура, платформи аналітики даних
Тип ІТ-інфраструктури	Розподілена, багаторівнева, з елементами віртуалізації, використанням приватних і гібридних хмарних рішень
Критичні бізнес-процеси	Забезпечення безперервного зв’язку, обробка абонентських даних, білінг, підтримка клієнтів, управління мережею
Організація управління ІБ	Централізована система з виділеним підрозділом інформаційної та кібербезпеки, інтегрована в загальну систему корпоративного управління
Нормативна основа ІБ	Дотримання законодавства України у сфері кібербезпеки, захисту інформації та

	персональних даних, орієнтація на міжнародні стандарти ISO/IEC 27001
Основні функції системи ІБ	Захист інформаційних ресурсів, моніторинг подій безпеки, реагування на інциденти, забезпечення відновлення сервісів
Технічні засоби ІБ	Системи контролю доступу, сегментація мережі, засоби виявлення атак, антивірусний захист, резервне копіювання, журналювання подій
Управління інцидентами	Наявність процедур реагування, кризових команд, взаємодії з державними структурами та поетапного відновлення сервісів
Робота з персоналом	Навчання з кібергігієни, регламентація доступів, визначення відповідальності за дотримання політик безпеки
Управління ризиками	Ідентифікація критичних активів, оцінка загроз, урахування ризиків третіх сторін і постачальників
Орієнтація на кіберстійкість	Забезпечення не лише захисту, а й здатності підтримувати роботу мережі та швидко відновлюватися після інцидентів
Актуальні виклики	Масштабні кібератаки, гібридні загрози, висока залежність від безперервності цифрових сервісів, складність інфраструктури

Аналіз організації управління інформаційною безпекою на підприємстві свідчить про її інтеграцію в загальну систему корпоративного управління. Це означає, що питання безпеки не обмежуються виключно технічним рівнем ІТ-підрозділів, а розглядаються як елемент стратегічного управління ризиками, що впливає на якість послуг, репутацію компанії та довіру абонентів і партнерів. Такий підхід відповідає сучасним концепціям кіберстійкості, відповідно до яких відповідальність за безпеку розподіляється між керівництвом, профільними підрозділами та персоналом підприємства.

З огляду на характер діяльності ПрАТ «Київстар», система інформаційної безпеки має охоплювати одночасно телекомунікаційний

контур і корпоративні ІТ-системи. Це зумовлює необхідність узгодження вимог безпеки для різних типів активів, починаючи від елементів ядра мобільної мережі та систем управління мережею і завершуючи білінговими платформами, клієнтськими базами даних та хмарними сервісами для бізнес-користувачів. У таких умовах особливого значення набуває сегментація інфраструктури, розмежування доступів і формалізація процедур взаємодії між підрозділами, що дозволяє зменшити ймовірність каскадного поширення інцидентів.

Важливим аспектом організації інформаційної безпеки є орієнтація на управління інцидентами та відновлення сервісів. Досвід масштабних кібератак, яких зазнав оператор у період воєнних дій, продемонстрував, що навіть за наявності розвинених засобів захисту повністю уникнути інцидентів неможливо. У цьому контексті здатність підприємства швидко локалізувати порушення, забезпечити альтернативні канали функціонування та поетапно відновити роботу мережі стає визначальною характеристикою його кіберстійкості. Саме тому організаційні процедури реагування, кризові комунікації та резервування ресурсів мають не менше значення, ніж технічні засоби захисту.

Не менш суттєвим є людський фактор у системі інформаційної безпеки. Для підприємства з великою кількістю працівників і розгалуженою структурою доступів ризики, пов’язані з помилками персоналу, соціальною інженерією або зловживанням привілеями, залишаються одними з найбільш значущих. Тому навчання з кібергігієни, формування культури безпеки та чітке визначення відповідальності за дотримання політик є важливою складовою організації системи ІБ, що безпосередньо впливає на рівень загальної кіберстійкості підприємства.

2.2. Оцінювання рівня кіберстійкості та вразливостей підприємства в умовах гібридних загроз

Оцінювання рівня кіберстійкості підприємства в умовах гібридних загроз доцільно здійснювати не як перевірку окремих технічних засобів захисту, а як аналіз здатності організації зберігати керованість і безперервність критичних функцій під час цілеспрямованого багатовекторного впливу. У випадку ПрАТ «Київстар» така оцінка має враховувати специфіку оператора електронних комунікацій, де головною цінністю є не тільки конфіденційність даних, а насамперед доступність сервісів і відновлюваність мережі, оскільки порушення зв'язку трансформується у суспільно значущі наслідки та економічні втрати. Реальний контекст воєнного часу робить оцінювання ще більш прикладним, адже гібридні загрози для телеком-оператора включають одночасно руйнівні кібератаки, інформаційні кампанії, тиск на ланцюги постачання і вплив на енергетичну стійкість інфраструктури.

Методологічно оцінювання кіберстійкості є логічним здійснювати через призму управлінського циклу «підготовленість – протидія – відновлення – адаптація», який добре корелює з міжнародними рамками на кшталт NIST CSF, де критичною ознакою зрілості є наявність і узгодженість процесів ідентифікації ризиків, захисту, виявлення інцидентів, реагування та відновлення. Саме в такому підході кіберстійкість вимірюється не фактом наявності окремих контролів, а спроможністю підприємства підтримувати ключові послуги в умовах атаки, локалізувати збиток, зберігати мінімально необхідний рівень сервісу та відновлюватися із прийнятними показниками часу й якості.

Оцінюючи підготовленість Київстару, слід виходити з того, що компанія має розгалужену критичну інфраструктуру і, відповідно, об'єктивно повинна мати кризові процедури та плани безперервності. Важливо, що у публічній звітності материнської групи VEON прямо зазначається застосування кризового управління та планів безперервності під час інциденту, а також взаємодія з українськими правоохоронними органами в межах розслідування

події, що свідчить про наявність інституційної основи управління кіберінцидентами та кризами на рівні підприємства. Водночас сама природа інциденту грудня 2023 року вказує, що загрози для оператора перебувають на рівні «високої складності» й можуть бути не просто спрямовані на викрадення даних, а мати руйнівну мету знищення або виведення з ладу ключових компонентів інфраструктури, що суттєво підвищує вимоги до сегментації, резервування, контролю привілеїв і відновлюваності.

Ключовою подією для оцінювання кіберстійкості є масштабна кібератака 12 грудня 2023 року, яку VEON/Київстар характеризували як одну з найбільших для телеком-ринку, а її наслідком стала недоступність сервісів для абонентів і необхідність поетапного відновлення. Для аналізу кіберстійкості важливими є не тільки факт атаки, а її параметри: Reuters з посиланням на українського посадовця (кібернапрям СБУ) повідомляв, що зловмисники могли перебувати в системі щонайменше з травня 2023 року, а атака мала руйнівний характер і зачепила «core» (ядро) інфраструктури. Такий сценарій означає, що противник (а у публічних оцінках фігурує підозра на російський слід і конкретні пов’язані структури) міг мати час для розвідки, закріплення та підготовки синхронного удару по критичних вузлах, що є типовою ознакою гібридного підходу, коли кіберкомпонент є частиною ширшої кампанії дестабілізації.

З позиції показників відновлення, які є центральними для кіберстійкості, важливо, що повідомлення Reuters від 19 грудня 2023 року вказують на відновлення всіх типів сервісів приблизно за тиждень після атаки. Це демонструє наявність реальної спроможності до відновлення, однак одночасно підкреслює критичність навіть короткострокової деградації, адже збої зв’язку впливають на життєво важливі сервіси для населення та бізнесу. Додатково гуманітарні повідомлення ООН у дні інциденту відзначали вплив атаки на доступ мільйонів людей до важливих сервісів, що підкреслює ширину

суспільних наслідків і посилює вимогу до кіберстійкості саме як до здатності зберігати доступність.

Фінансовий вимір є ще одним маркером рівня стійкості та масштабу наслідків. Reuters повідомляв, що Київстар виділив близько 90 млн доларів на подолання наслідків атаки та посилення захисту, а також що інцидент негативно вплинув на показники зростання. Окремо Reuters оцінював, що атака могла коштувати материнській компанії майже 100 млн доларів у продажах, що вказує на високу економічну ціну порушення доступності та підтверджує, що для телеком-оператора кіберстійкість прямо пов’язана з фінансовою стійкістю. У термінах управління ризиками це означає, що навіть при наявності здатності до відновлення організація зазнала суттєвих втрат, а отже подальша еволюція системи управління кіберстійкістю має бути спрямована на зменшення ймовірності «руйнівних» сценаріїв і скорочення часу/масштабу деградації сервісів.

Оцінюючи вразливості Київстару в умовах гібридних загроз, доцільно розглядати їх як системні «точки напруги», що виникають на стику технологій, процесів і людського фактора. По-перше, сам факт тривалого перебування противника в середовищі (як це описано у публічних оцінках) свідчить про потенційну вразливість у частині раннього виявлення та протидії прихованому доступу, що може бути пов’язано з компрометацією облікових записів, недосконалим контролем привілейованого доступу або недостатньою «видимістю» подій у критичних сегментах. Для кіберстійкості це означає, що виявлення повинно бути максимально наближене до критичних компонентів, а моніторинг має забезпечувати кореляцію подій не тільки в корпоративних ІТ-системах, а й у мережевому та телеком-контурі, де наслідки атак можуть бути руйнівними.

По-друге, руйнівний характер атаки, що спрямовується на порушення працездатності ядра та ключових систем, підсилює важливість сегментації, принципу мінімальних привілеїв і стійкості механізмів резервного

копіювання. У контексті гібридних загроз особливо небезпечною є ситуація, коли резервні копії або інструменти відновлення можуть бути знищені чи скомпрометовані разом із основним середовищем. Це створює потребу в таких архітектурних рішеннях, які забезпечують «роз'єднання» зон довіри, наявність незмінних (immutable) резервних копій, а також відпрацьованих сценаріїв відновлення, які реально тестуються і не залишаються формальними документами.

По-третє, для телеком-оператора суттєвою вразливістю є залежність від постачальників, підрядників і ланцюгів постачання. Гібридні загрози часто реалізуються через суміжні організації, компрометацію сервісних доступів або використання оновлень/інтеграцій як каналу проникнення. Для Київстару, який підтримує масштабну інфраструктуру і розвиває хмарні та дата-продукти, значущими стають вимоги до безпеки third-party доступу та контроль безпеки інтеграцій, адже будь-який слабкий елемент у ланцюгу може стати точкою входу для атаки з подальшим рухом до критичних компонентів. По-четверте, гібридні загрози для підприємства такого профілю включають не лише «чисто кібер» вплив, а й енергетичний та фізичний вимір. Показово, що у 2025 році Reuters описував, як Київстар посилює стійкість мережі через резервні джерела живлення і розгортання генераторів у відповідь на удари по енергосистемі, тобто компанія змушена враховувати, що доступність сервісів визначається не лише кіберзахистом, але й стійкістю до відключень електроенергії. Це підкреслює інтегрований характер кіберстійкості в умовах війни: навіть ідеально захищена цифрова інфраструктура втрачає сенс без енергетичної підтримки, а отже система управління кіберстійкістю має включати управління фізичною стійкістю критичних вузлів, пріоритезацію живлення і планування роботи під час деградації інфраструктури.

По-п'яте, інформаційно-психологічний компонент гібридних загроз підсилює вразливість у сфері комунікацій і довіри. Масштабні збої зв'язку часто супроводжуються дезінформацією, маніпуляціями та панічними

повідомленнями, що можуть посилювати репутаційні втрати й впливати на поведінку абонентів та партнерів. У таких умовах кіберстійкість включає спроможність до кризових комунікацій, узгодженого інформування та підтримання довіри, оскільки відновлення сервісів без відновлення довіри не забезпечує повноцінного відновлення бізнес-функцій.

Таблиця 2.2

Оцінювання рівня кіберстійкості та ключових вразливостей ПрАТ «Київстар» в умовах гібридних загроз

Компонент кіберстійкості	Характеристика поточного стану	Прояв стійкості	Виявлені вразливості та проблеми
Ідентифікація активів і ризиків	Критичні мережеві та ІТ-активи визначені, здійснюється класифікація даних і сервісів	Усвідомлення пріоритетності ядра мережі та ключових бізнес-систем	Складність повної інвентаризації через масштаб і динамічність інфраструктури
Захист інфраструктури	Застосування сегментації мережі, контролю доступу та багаторівневих засобів захисту	Наявність розвинених технічних контролів безпеки	Ризики компрометації привілейованих облікових записів і складність керування доступами
Виявлення інцидентів	Функціонування систем моніторингу та аналізу подій безпеки	Здатність фіксувати масові атаки та аномалії	Ймовірність пізнього виявлення прихованої присутності зловмисника
Реагування на атаки	Наявні процедури реагування та кризові команди,	Мобілізація ресурсів під час масштабної атаки 2023 року	Високе навантаження на персонал у кризових умовах

	взаємодія з держорганами		
Відновлення сервісів	Реалізовані механізми поетапного відновлення мережі та сервісів	Відновлення основних послуг упродовж приблизно тижня після інциденту	Значний простій для критичних сервісів і висока вартість відновлення
Безперервність бізнесу	Орієнтація на підтримання мінімально необхідного рівня сервісів	Наявність резервних сценаріїв функціонування мережі	Залежність від енергетичної та фізичної інфраструктури
Резервне копіювання	Використання резервного копіювання для критичних систем	Можливість відновлення даних після руйнівних впливів	Ризик компрометації або знищення резервів при глибокому проникненні
Людський фактор	Проводяться навчання з кібергігієни та регламентація доступів	Підвищення обізнаності персоналу з питань безпеки	Соціальна інженерія та помилки персоналу залишаються суттєвим ризиком
Постачальники та підрядники	Контроль доступів третіх сторін і інтеграцій	Урахування ризиків ланцюгів постачання	Потенційні вразливості через суміжні організації
Кризові комунікації	Функціонують канали інформування абонентів і партнерів	Можливість офіційних повідомлень під час інцидентів	Репутаційні ризики та вплив дезінформації
Загальний рівень кіберстійкості	Сформована система управління з орієнтацією на відновлення	Спроможність відновлювати роботу після масштабних атак	Вразливість до довготривалих прихованих і руйнівних сценаріїв

Оцінювання рівня кіберстійкості Київстару в умовах гібридних загроз показує наявність суттєвої спроможності до відновлення після руйнівних інцидентів, що підтверджується відносно швидким поверненням сервісів після атаки грудня 2023 року, але водночас виявляє критичні зони ризику, пов’язані з тривалою прихованою присутністю противника, потенційними прогалинами раннього виявлення, високою «вартістю» деградації доступності, залежністю від постачальників та енергетичної інфраструктури. Сукупно це означає, що для підвищення кіберстійкості пріоритетом стає посилення управління ризиками на рівні архітектури і процесів, підвищення якості виявлення і контролю привілеїв, забезпечення відновлюваності через стійкі резервні механізми, а також інтеграція кіберзахисту з безперервністю бізнесу та фізичною стійкістю мережі, що логічно веде до наступного підрозділу — аналізу ризиків, інцидентів і проблем функціонування наявної системи управління кіберстійкістю.

2.3. Аналіз ризиків, інцидентів та проблем функціонування наявної системи управління кіберстійкістю

Аналіз ризиків, інцидентів та проблем функціонування системи управління кіберстійкістю підприємства доцільно проводити як комплексне дослідження взаємозв’язку між загрозами, критичними активами, організаційними процесами та фактичними подіями безпеки. Для ПрАТ «Київстар» така логіка є особливо релевантною, оскільки компанія не лише працює з масовою абонентською базою і критичними сервісами зв’язку, а й функціонує в умовах гібридного протистояння, де кіберінциденти можуть мати руйнівну мету, синхронізуватися з інформаційними операціями та накладатися на фізичні фактори воєнного часу. У цьому контексті кіберстійкість проявляється не у «відсутності інцидентів», а у здатності

виявляти ризики на ранніх стадіях, обмежувати масштаб порушень, зберігати керованість та відновлювати сервіси із прийнятними втратами.

Вихідним пунктом аналізу ризиків є ідентифікація того, що для оператора зв'язку найбільш критичними є ризики, які впливають на доступність мережі та сервісів, а вже потім — ризики порушення конфіденційності чи цілісності даних. Це пояснюється тим, що навіть короткострокова втрата доступності для мільйонів користувачів одразу породжує ланцюгові наслідки для економіки, державних та муніципальних сервісів, екстрених комунікацій і репутації компанії. Саме тому в системі управління кіберстійкістю Київстару ризики повинні оцінюватися з урахуванням бізнес-впливу на критичні функції, а критерії пріоритизації мають базуватися на показниках безперервності: допустимий час простою, швидкість відновлення, мінімально прийнятний рівень сервісу та здатність працювати в деградованому режимі.

Ключовою емпіричною основою для аналізу інцидентів є масштабна кібератака 12 грудня 2023 року, яка спричинила значні збої мобільного та інтернет-зв'язку й вимагала поетапного відновлення. У публічних повідомленнях материнської групи VEON подія характеризувалася як одна з найбільших атак на телеком-оператора, а також підтверджувалася реалізація кризового управління і планів безперервності та взаємодія з державними органами. Додатково Reuters із посиланням на представника СБУ повідомляв, що зловмисники могли перебувати у системах щонайменше з травня 2023 року, а сам удар мав руйнівний характер і був націлений на критичні компоненти, що з позиції ризик-менеджменту свідчить про сценарій довготривалої прихованої присутності та підготовленої деструктивної операції. Така подія є характерним прикладом гібридної загрози, оскільки вона спрямована не лише на цифрові активи компанії, а й на дестабілізацію комунікаційного середовища країни в цілому.

З аналізу цього інциденту випливають три важливі управлінські висновки щодо ризиків. Перший полягає в тому, що найбільш небезпечними є не «швидкі» атаки, а кампанії, які забезпечують противнику час для розвідки, поступового розширення доступів і підготовки синхронного удару по критичних вузлах. У таких сценаріях традиційна модель безпеки, побудована на блокуванні відомих загроз і реагуванні на очевидні аномалії, може бути недостатньою, адже противник діє обережно, використовуючи легітимні інструменти адміністрування, компрометовані облікові записи або ланцюги постачання. Для системи управління кіберстійкістю це означає, що центральним ризиком стає «невидимість» атаки на ранніх стадіях і недостатня здатність до виявлення прихованої присутності. Показником проблеми у такому випадку є тривалий dwell time — час перебування зловмисника в системі до моменту виявлення, який прямо корелює з масштабом потенційної шкоди.

Другий висновок стосується архітектурних ризиків. Якщо атакуючий здатен досягти критичних компонентів інфраструктури, зокрема вузлів, що визначають функціонування ядра мережі та керування сервісами, то наслідком стає не просто витік інформації, а системна відмова сервісів. Такий ризик підсилює важливість сегментації, принципу «нульової довіри» для адміністративних доступів, розмежування середовищ експлуатації та управління, а також особливого захисту привілейованих облікових записів. Практична проблема полягає в тому, що в телеком-оператора з великою кількістю технологічних доменів і постійними змінами конфігурацій забезпечення єдиного стандарту сегментації і контролю доступів є складним завданням, а отже виникають «сірі зони», які можуть бути використані для латерального переміщення.

Третій висновок пов’язаний із ризиками відновлення. Навіть якщо організація здатна відновити роботу, саме відновлення може бути дорогим, тривалим і супроводжуватися деградацією якості сервісу, що завдає

фінансових та репутаційних втрат. Reuters повідомляв, що компанія виділила близько 90 млн доларів на подолання наслідків атаки і посилення захисту, що демонструє масштабність післяінцидентних витрат та економічну ціну порушення кіберстійкості. Сам факт значних витрат свідчить, що у системі управління кіберстійкістю існували проблеми, які дозволили інциденту досягти рівня, коли відновлення потребує надзвичайних ресурсів. Для оцінки кіберстійкості це означає, що важливо аналізувати не лише «чи відновилися», а «якою ціною» і «наскільки оптимальним було відновлення» з точки зору заздалегідь визначених показників.

Окремим пластом аналізу є ризики, пов’язані з третім сторонами та інтеграціями. У сучасному телеком-бізнесі значна частина технологічної екосистеми формується на базі постачальників обладнання, програмних платформ і сервісних підрядників, а також інтеграцій із зовнішніми партнерами і хмарними середовищами. За умов гібридних загроз це створює проблему розширеного периметра: навіть якщо внутрішні процеси безпеки є відносно зрілими, слабке місце може виникати в суміжній організації, через канали сервісного доступу або через компрометацію облікових записів постачальника. Для Київстару ця проблема посилюється тим, що компанія розвиває цифрові B2B-напрями, хмарні сервіси та продукти роботи з даними, де число інтеграцій і точок взаємодії різко зростає, а разом із ним зростає ймовірність інцидентів, пов’язаних із неправильними налаштуваннями доступів, ключів, токенів або взаємодією API.

У контексті інцидентів і проблем функціонування системи управління кіберстійкістю важливим є також інформаційно-психологічний вимір. Масштабна відмова зв’язку, як правило, супроводжується хвилею чуток, спробами інформаційної дестабілізації та підривом довіри, а отже кризове управління має включати не лише технічне відновлення, а й керування комунікаціями зі стейкхолдерами. У випадку оператора зв’язку ключовим стає завдання підтримання прозорого інформування абонентів і партнерів про стан

сервісів та хід відновлення, оскільки інформаційний вакуум заповнюється дезінформацією, що здатна примножити репутаційні втрати. В управлінській площині це означає, що система кіберстійкості повинна включати узгоджені протоколи кризових повідомлень, визначені ролі спікерів і механізми підтвердження достовірності інформації.

Ще однією групою проблем функціонування кіберстійкості є залежність від фізичних факторів, передусім від енергопостачання та доступності об'єктів інфраструктури. Для телеком-оператора війна створює ситуацію, коли кіберінциденти можуть накладатися на відключення електроенергії, руйнування або обмеження доступу до вузлів мережі. Це формує комбінований ризик, коли навіть ефективна робота кіберзахисту не гарантує доступності сервісів, якщо відсутнє резервне живлення, логістика підтримки та можливість оперативного відновлення фізичних компонентів. З управлінського боку це перетворює кіберстійкість у «цифрово-фізичну» стійкість, де планування аварійного живлення, розміщення генераторів, паливна логістика та пріоритезація критичних вузлів стають частиною загальної моделі управління безперервністю.

Таблиця 2.3

Основні ризики, інциденти та проблеми функціонування системи управління кіберстійкістю ПрАТ «Київстар»

Категорія	Зміст та прояв	Потенційні наслідки для підприємства	Виявлені проблеми управління
Прихована присутність зловмисника	Можливість тривалого перебування атакуючого в системі без явних ознак компрометації	Підготовка руйнівних сценаріїв, компрометація критичних компонентів інфраструктури	Недостатня ефективність раннього виявлення та кореляції подій безпеки
Руйнівні атаки на ядро мережі	Цілеспрямований вплив на core-	Масові збої сервісів і втрата	Складність сегментації та

	інфраструктуру та системи керування мережею	доступності зв’язку для абонентів	ізоляції критичних вузлів у масштабній архітектурі
Компрометація привілейованих доступів	Захоплення адміністраторських облікових записів через фішинг або витоки	Повний контроль над системами, латеральний рух у мережі	Обмежена керованість привілеями та потреба в посиленому PAM
Інцидент масштабної кібератаки 2023 року	Руйнівний вплив на частину інфраструктури та зупинка сервісів	Простої, фінансові втрати, репутаційний удар	Недостатня стійкість до сценаріїв руйнівного характеру
Деградація доступності сервісів	Висока залежність бізнесу від безперервної роботи мережі	Масовий вплив на клієнтів і втрати доходів	Потреба в оптимізації показників часу відновлення
Ризики ланцюгів постачання	Компрометація через підрядників або партнерські доступи	Проникнення у внутрішні системи через суміжні організації	Недостатній контроль безпеки третіх сторін та інтеграцій
Компрометація резервних копій	Одночасний вплив на основні системи і резерви	Неможливість швидкого відновлення після атаки	Потреба в ізольованих та незмінних резервних копіях
Інформаційно-психологічний вплив	Дезінформація та паніка під час інцидентів	Втрата довіри абонентів і партнерів	Недостатня формалізація кризових комунікацій
Фізичні та енергетичні ризики	Відключення електроенергії та ураження об’єктів інфраструктури	Додаткові збої сервісів незалежно від кіберзахисту	Залежність кіберстійкості від фізичної стійкості об’єктів
Організаційні ризики	Високе навантаження на команди в кризових умовах	Помилки реагування та зниження ефективності відновлення	Потреба в масштабуванні й автоматизації процесів

Економічні наслідки інцидентів	Значні витрати на відновлення та модернізацію	Зниження фінансової стійкості підприємства	Недостатня інтеграція кіберризиків у фінансове планування
Загальний стан кіберстійкості	Спроможність до відновлення після масштабних інцидентів	Повернення сервісів у прийнятні строки	Переважна орієнтація на реагування, а не на попередження

Аналіз ризиків і інцидентів у Київстарі демонструє, що наявна система управління кіберстійкістю має ознаки розвиненості в частині кризового реагування та відновлення, оскільки підприємство змогло повернути сервіси після масштабної атаки, однак водночас виявляє проблемні зони, пов’язані з раннім виявленням прихованих атак, складністю керування привілейованими доступами та сегментацією у масштабній інфраструктурі, високою вартістю простою та відновлення, а також розширенням периметра за рахунок третіх сторін, інтеграцій і фізичних залежностей. У термінах управління це означає, що подальше підвищення кіберстійкості повинно бути спрямоване на посилення превентивної керованості та зменшення масштабу руйнівних сценаріїв через підвищення «видимості» подій, підсилення контролю привілеїв, забезпечення ізольованих і перевірених механізмів відновлення, а також інтеграцію кіберризик-менеджменту з безперервністю бізнесу та управлінням залежностями від зовнішнього середовища. Саме ці результати створюють підґрунтя для переходу до третього розділу, у якому мають бути запропоновані практичні напрями вдосконалення системи управління кіберстійкістю підприємства в умовах гібридних загроз, із визначенням конкретних організаційних і технологічних заходів та очікуваних ефектів.

Узагальнення, наведене в таблиці 2.3, дозволяє розглядати ризики та проблеми функціонування системи управління кіберстійкістю ПрАТ «Київстар» як взаємопов’язаний комплекс технічних, організаційних та

зовнішніх чинників, що формують середовище підвищеної невизначеності для підприємства. Домінування сценаріїв руйнівного характеру, спрямованих на доступність сервісів і керованість інфраструктури, свідчить про те, що кіберстійкість оператора визначається не стільки рівнем ізольованого захисту окремих компонентів, скільки спроможністю всієї системи управління координувати дії в умовах багатовекторного тиску.

Аналіз інцидентів показує, що найбільш критичними для підприємства є ті події, які поєднують тривалу приховану фазу з подальшим синхронним руйнівним впливом на ключові вузли мережі. Такий характер атак виявляє проблему обмеженої «видимості» подій безпеки на ранніх етапах і свідчить про необхідність підсилення спроможностей до глибинного моніторингу, поведінкової аналітики та кореляції подій у різних доменах інфраструктури. У контексті управління це означає, що система має еволюціонувати від реактивної моделі, орієнтованої на очевидні інциденти, до проактивної, спрямованої на виявлення слабких сигналів і аномалій, які можуть передувати масштабним атакам.

Виявлені ризики у сфері керування привілейованими доступами та сегментації інфраструктури свідчать про складність підтримання принципів мінімальних привілеїв і ізоляції у великомасштабному, динамічному середовищі. Для оператора зв’язку, де кількість технологічних доменів і інтеграцій є значною, навіть незначні прогалини у контролі доступів можуть призводити до можливості латерального переміщення зловмисника та ескалації привілеїв. З управлінської точки зору це формує потребу в централізованих механізмах контролю, стандартизації процесів доступу та постійному перегляді ролей і повноважень відповідно до змін в архітектурі.

Не менш показовими є ризики, пов’язані з відновленням після інцидентів. Незважаючи на наявність механізмів резервування та поетапного відновлення, значна вартість простою та відновлювальних робіт демонструє, що поточні показники часу і якості відновлення залишаються критичними для фінансової

та репутаційної стійкості підприємства. Це свідчить про необхідність переходу від формального планування відновлення до систематичного тестування сценаріїв, оцінювання реальних можливостей резервних механізмів та інтеграції показників відновлюваності у систему управління ефективністю бізнес-процесів.

Окремий вимір проблем стосується залежності кіберстійкості від зовнішніх чинників, зокрема від постачальників і фізичної інфраструктури. Умови гібридних загроз демонструють, що навіть високий рівень внутрішнього кіберзахисту може бути нівельований через компрометацію суміжних організацій або через відключення енергопостачання, що безпосередньо впливає на доступність сервісів. Це означає, що система управління кіберстійкістю має розширюватися за межі власної IT- та телеком-інфраструктури і включати управління ризиками ланцюгів постачання та фізичної стійкості критичних об’єктів як рівноправні складові загальної моделі безперервності.

Аналіз інформаційно-психологічного виміру інцидентів підкреслює, що для оператора зв’язку кіберінцидент швидко трансформується у кризу довіри. Втрата або деградація сервісів супроводжується інформаційним тиском, дезінформацією та панічними настроями, що можуть посилювати негативний ефект від технічних збоїв. У такому контексті проблеми функціонування системи кіберстійкості полягають не лише у швидкості технічного відновлення, а й у здатності організації забезпечити узгоджені кризові комунікації, підтримати прозорість і керованість інформаційного поля, що є критично важливим для збереження репутації.

Узагальнюючи результати аналізу, можна стверджувати, що наявна система управління кіберстійкістю ПрАТ «Київстар» демонструє реальну спроможність до відновлення після масштабних інцидентів, однак водночас характеризується низкою системних проблем, пов’язаних із раннім виявленням прихованих загроз, керуванням привілейованими доступами,

високою вартістю деградації сервісів, залежністю від зовнішніх і фізичних чинників та недостатньою інтеграцією кіберризиків у загальне управління бізнесом. Саме ці проблеми формують поле для подальших удосконалень і визначають напрями розвитку системи управління кіберстійкістю.

РОЗДІЛ 3 УДОСКОНАЛЕННЯ СИСТЕМИ УПРАВЛІННЯ КІБЕРСТІЙКІСТЮ ПІДПРИЄМСТВА

3.1. Розроблення моделі системи управління кіберстійкістю в умовах гібридних загроз

Розроблення моделі системи управління кіберстійкістю в умовах гібридних загроз має ґрунтуватися на результатах аналізу, проведеного у попередньому розділі, який виявив як наявні спроможності підприємства до відновлення після масштабних інцидентів, так і системні проблеми, пов’язані з раннім виявленням прихованих атак, складністю керування доступами, залежністю від зовнішніх чинників та високою вартістю деградації сервісів. У цьому контексті модель управління кіберстійкістю повинна орієнтуватися не лише на підвищення рівня захищеності, а передусім на формування здатності організації підтримувати керованість і безперервність критичних функцій під час багатовекторного впливу та швидко адаптуватися до змін середовища загроз.

Концептуально запропонована модель розглядає кіберстійкість як інтегровану властивість підприємства, що формується на перетині управлінського, процесного, технологічного та людського рівнів. На управлінському рівні модель передбачає закріплення кіберстійкості як одного з пріоритетів корпоративного управління та ризик-менеджменту, коли відповідальність за неї покладається не лише на підрозділи ІТ чи безпеки, а й на вищий менеджмент, який визначає політику, допустимий рівень ризику та ресурсне забезпечення. У такій логіці кіберстійкість інтегрується в систему стратегічного планування, а її показники стають складовою оцінювання ефективності управлінських рішень.

Процесний вимір моделі базується на безперервному циклі управління, який охоплює ідентифікацію критичних активів і процесів, оцінювання ризиків, упровадження заходів захисту, моніторинг подій, реагування на інциденти, відновлення та подальшу адаптацію. Важливо, що цей цикл у запропонованій моделі не є лінійним, а має характер постійного зворотного зв'язку, коли кожен інцидент або відхилення розглядається як джерело знань для коригування архітектури, процедур і пріоритетів. Саме така динаміка дозволяє системі еволюціонувати відповідно до змін у середовищі гібридних загроз.

Технологічна складова моделі спрямована на створення архітектури, здатної протистояти як масовим, так і прихованим атакам, і водночас забезпечувати відновлюваність. У межах моделі передбачається поєднання принципів сегментації, нульової довіри, централізованого керування ідентичностями та доступами, глибинного моніторингу подій і поведінкової аналітики. Окремий акцент робиться на архітектурі резервування та відновлення, яка має забезпечувати ізольованість і незмінність резервних копій, можливість швидкого розгортання критичних сервісів у альтернативному середовищі та регулярне тестування сценаріїв відновлення. У такій моделі технології розглядаються не як набір розрізнених засобів, а як взаємопов'язана система, підпорядкована єдиній меті збереження доступності та керованості.

Людський вимір моделі полягає у формуванні культури кіберстійкості, де кожен працівник усвідомлює свою роль у забезпеченні безпеки та безперервності. Запропонована модель виходить із того, що навіть найсучасніші технології не можуть гарантувати стійкість без належного рівня підготовки персоналу, чітко визначених ролей у кризових ситуаціях і здатності до міжфункціональної взаємодії. Тому модель передбачає систематичне навчання, тренування сценаріїв реагування, розвиток навичок прийняття

рішень в умовах невизначеності та підтримку внутрішніх комунікацій між підрозділами.

Особливістю моделі управління кіберстійкістю в умовах гібридних загроз є врахування зовнішнього контуру, до якого належать постачальники, партнери, державні органи та фізична інфраструктура. У запропонованій моделі кіберстійкість підприємства розглядається як частина ширшої екосистеми, де слабка ланка в ланцюгу постачання або порушення енергетичної стійкості можуть нівелювати внутрішні заходи захисту. Відповідно, модель передбачає інтеграцію управління ризиками третіх сторін, вимог до їхньої безпеки, регулярних аудитів та узгоджених планів взаємодії у кризових ситуаціях.

Важливим елементом запропонованої моделі є орієнтація на показники результативності, що характеризують саме кіберстійкість, а не лише рівень захищеності. У центрі уваги опиняються такі характеристики, як здатність підтримувати мінімально необхідний рівень сервісів під час інциденту, час виявлення і локалізації атаки, швидкість відновлення критичних функцій та ступінь збереження довіри стейкхолдерів. Інтеграція цих показників у систему управління дозволяє перейти від формального виконання вимог до реального вимірювання спроможності організації протистояти гібридним загрозам.

Запропонована модель системи управління кіберстійкістю в умовах гібридних загроз є комплексною, динамічною та інтегрованою у загальну систему управління підприємством. Вона поєднує управлінські механізми, процеси, технологічні рішення та людський потенціал у єдину логіку, спрямовану на збереження керованості й безперервності критичних функцій за умов невизначеності та багатовекторного тиску. Реалізація такої моделі створює передумови для підвищення здатності підприємства не лише протистояти окремим кібератакам, а й адаптуватися до системних змін у середовищі гібридних загроз, що в подальшому має бути конкретизовано через розроблення практичних механізмів і інструментів її впровадження.

Рис. 3.1. Модель системи управління кіберстійкістю

Узагальнення, представлене в таблиці та на схемі моделі системи управління кіберстійкістю, дозволяє розглядати запропонований підхід як цілісну багаторівневу конструкцію, у якій усі елементи перебувають у постійній взаємодії та формують єдине середовище прийняття управлінських рішень. Модель відображає логіку переходу від стратегічного бачення кіберстійкості до її практичної реалізації через процеси, технології та людський потенціал, що забезпечує системність і узгодженість дій підприємства в умовах гібридних загроз.

Інтерпретація схеми свідчить, що управлінський рівень відіграє визначальну роль у формуванні політики кіберстійкості та інтеграції її цілей у загальну систему корпоративного управління. Саме на цьому рівні задаються допустимі межі ризику, визначаються пріоритети захисту критичних функцій і забезпечується ресурсна підтримка всієї системи. У межах запропонованої моделі управлінські рішення мають не лише регламентуючий, а й адаптивний

характер, оскільки вони повинні регулярно переглядатися з урахуванням змін у середовищі загроз і результатів аналізу інцидентів.

Процесний рівень, відображений у моделі, демонструє циклічність управління кіберстійкістю, де оцінювання ризиків, моніторинг, реагування, відновлення та адаптація утворюють безперервний контур удосконалення. Така логіка дозволяє трансформувати кожен інцидент або відхилення від нормального режиму в джерело управлінських знань, що забезпечує еволюцію системи та зменшення ймовірності повторення подібних сценаріїв у майбутньому. У контексті гібридних загроз це набуває особливого значення, оскільки характер атак постійно змінюється і вимагає гнучкості процесів.

Технологічний рівень у моделі виступає інструментальною основою реалізації управлінських і процесних рішень. Його інтерпретація свідчить, що технології в межах моделі не розглядаються ізольовано, а формують узгоджену архітектуру, орієнтовану на забезпечення доступності, керованості та відновлюваності критичних сервісів. Саме взаємодія засобів моніторингу, контролю доступів, сегментації та резервування створює технічні передумови для реалізації принципів кіберстійкості, закладених у моделі.

Людський рівень, відображений у схемі, підкреслює, що кіберстійкість неможлива без сформованої культури безпеки та готовності персоналу діяти в умовах кризових ситуацій. Інтерпретація цього елементу моделі показує, що роль працівників виходить за межі формального виконання інструкцій і передбачає активну участь у виявленні загроз, підтриманні стійкості процесів і прийнятті рішень у ситуаціях невизначеності. У такий спосіб людський фактор стає не джерелом ризику, а ключовим ресурсом підвищення адаптивності системи.

Важливою особливістю запропонованої моделі є врахування зовнішнього середовища та гібридних загроз як постійного фону функціонування системи управління. Інтерпретація схеми демонструє, що модель не є замкненою, а передбачає взаємодію з партнерами,

постачальниками, державними структурами та фізичною інфраструктурою, що дозволяє розширити межі кіберстійкості за межі власних інформаційних ресурсів підприємства. Такий підхід забезпечує комплексність і відповідає сучасному розумінню кіберстійкості як властивості всієї екосистеми.

Узагальнюючи, можна стверджувати, що подана в таблиці та на схемі модель відображає інтегроване бачення системи управління кіберстійкістю, у якій стратегічні рішення, процеси, технології та людський потенціал об’єднані спільною метою забезпечення керованості й безперервності діяльності підприємства в умовах гібридних загроз. Запропонована інтерпретація моделі створює підґрунтя для подальшої конкретизації її елементів і переходу до наступного підрозділу, присвяченого розробленню практичних механізмів і інструментів упровадження цієї моделі на підприємстві, а також оцінюванню очікуваних результатів від її реалізації.

3.2. Обґрунтування заходів та інструментів підвищення кіберстійкості підприємства

Обґрунтування заходів та інструментів підвищення кіберстійкості підприємства має спиратися на розуміння того, що в умовах гібридних загроз жоден окремий технічний або організаційний захід не здатний забезпечити необхідний рівень стійкості. Кіберстійкість формується як системна властивість, яка виникає внаслідок узгодженого поєднання управлінських рішень, процесів, технологій та людського потенціалу, спрямованих на збереження керованості та безперервності критичних функцій навіть за умови успішної реалізації атак. Тому обґрунтування запропонованих заходів полягає не лише у виборі ефективних інструментів, а й у доведенні їхньої відповідності виявленим у попередньому розділі проблемам і ризикам.

Вихідною позицією є необхідність зміщення акценту з переважно реактивної моделі безпеки до проактивної та адаптивної. Аналіз інцидентів

показав, що найбільш небезпечними для підприємства є довготривалі приховані атаки, які залишаються непоміченими до моменту синхронного руйнівного впливу. У цьому контексті ключового значення набуває впровадження інструментів, здатних забезпечити глибоку спостережуваність середовища та раннє виявлення аномалій. Йдеться не просто про фіксацію окремих подій, а про формування цілісної картини поведінки користувачів, сервісів і мережевих сегментів у часі, що дозволяє виявляти відхилення, характерні для прихованої присутності зловмисника. Обґрунтування таких інструментів полягає в тому, що вони безпосередньо зменшують ризик тривалого dwell time і, відповідно, масштаб потенційних наслідків атаки.

Не менш важливим є підсилення контролю доступів і управління привілейованими обліковими записами, оскільки саме компрометація адміністраторських прав у попередньому аналізі була визначена як один із найбільш критичних сценаріїв. У межах запропонованих заходів обґрунтовується необхідність централізації управління ідентичностями, жорсткої прив’язки доступів до ролей і завдань, а також постійного перегляду повноважень у динамічному середовищі. Такий підхід дозволяє мінімізувати поверхню атаки та зменшити ймовірність ескалації привілеїв у разі компрометації окремих облікових даних. Інструменти керування доступами в цьому контексті виступають не як формальні засоби контролю, а як фундамент архітектури нульової довіри, що відповідає вимогам функціонування в умовах гібридних загроз.

З огляду на домінування ризиків, пов’язаних із доступністю сервісів, особливе обґрунтування отримують заходи, спрямовані на підвищення відновлюваності та стійкості архітектури. Йдеться про створення таких технічних і організаційних умов, за яких навіть успішна атака не призводить до тривалої зупинки критичних функцій. Це означає необхідність розвитку резервних середовищ, ізольованих і незмінних копій даних, а також сценаріїв швидкого розгортання сервісів у деградованому або альтернативному режимі.

Обґрунтування цих інструментів ґрунтується на тому, що в умовах гібридних загроз неможливо повністю усунути ймовірність інциденту, проте можна істотно зменшити його вплив на бізнес за рахунок скорочення часу відновлення і збереження мінімально необхідного рівня сервісів.

Окремий блок заходів спрямований на інтеграцію управління кіберризиками у загальну систему корпоративного ризик-менеджменту. У попередньому аналізі було встановлено, що значні фінансові та репутаційні наслідки інцидентів свідчать про потребу в тіснішому зв’язку між кіберстійкістю та стратегічними управлінськими рішеннями. Обґрунтування таких заходів полягає в тому, що кіберризики мають розглядатися на рівні керівництва нарівні з фінансовими, операційними та стратегічними ризиками, а відповідні інструменти оцінювання повинні дозволяти співвідносити витрати на захист із потенційними втратами від інцидентів. Це створює передумови для більш обґрунтованого розподілу ресурсів і підвищення відповідальності управлінців за рівень кіберстійкості.

Важливою складовою обґрунтування є розвиток механізмів управління безперервністю та кризового реагування. Аналіз показав, що навіть за наявності технічних засобів захисту саме якість координації дій у кризовій ситуації значною мірою визначає швидкість відновлення та масштаби втрат. Тому доцільність упровадження чітко регламентованих процедур реагування, регулярних тренувань і моделювання кризових сценаріїв обґрунтовується необхідністю забезпечити готовність персоналу до дій в умовах невизначеності та дефіциту часу. Такі інструменти формують організаційну спроможність діяти злагоджено, що є ключовою ознакою кіберстійкої організації.

З урахуванням розширеного периметра загроз особливе обґрунтування отримують заходи з управління ризиками третіх сторін і ланцюгів постачання. У сучасних умовах підприємство не може вважатися кіберстійким, якщо його партнери та підрядники залишаються слабкою ланкою. Тому інструменти

оцінювання зрілості безпеки постачальників, формування вимог до їхніх практик і узгодження сценаріїв взаємодії під час інцидентів є логічним продовженням запропонованої моделі. Їхня доцільність обґрунтовується тим, що вони дозволяють зменшити ймовірність проникнення через суміжні організації та підвищують узгодженість дій у кризових ситуаціях.

Не менш вагомим є обґрунтування заходів, спрямованих на розвиток людського потенціалу та культури кіберстійкості. Аналіз показав, що соціальна інженерія та помилки персоналу залишаються суттєвим джерелом ризику, а водночас саме люди є основним ресурсом адаптації системи до нових загроз. У цьому контексті інструменти навчання, підвищення обізнаності, формування навичок прийняття рішень у кризових умовах та розвитку міжфункціональної взаємодії обґрунтовуються як необхідна умова перетворення людського фактору з джерела вразливості на фактор стійкості.
Запропоновані заходи та інструменти підвищення кіберстійкості підприємства обґрунтовуються їхньою відповідністю виявленим ризикам і проблемам, а також їхньою здатністю забезпечити перехід від фрагментарної системи захисту до інтегрованої, адаптивної та орієнтованої на безперервність моделі управління. Їх реалізація дозволяє не лише зменшити ймовірність і масштаб кібератак, а й підвищити спроможність підприємства зберігати керованість і довіру стейкхолдерів у найскладніших умовах гібридних загроз, що створює підґрунтя для подальшого оцінювання ефективності запропонованих рішень і формування практичних рекомендацій щодо їх упровадження.

Таблиця 3.1

Заходи та інструменти підвищення кіберстійкості підприємства в умовах гібридних загроз

Напрям підвищення кіберстійкості	Заходи та інструменти	Обґрунтування впровадження	Очікуваний ефект для підприємства

Раннє виявлення атак	Централізований моніторинг подій, кореляція та поведінкова аналітика	Зменшує ризик тривалої прихованої присутності зловмисника та дозволяє своєчасно фіксувати аномалії	Скорочення часу виявлення інцидентів і зниження масштабу потенційних наслідків
Контроль ідентичностей і доступів	Централізоване управління обліковими записами та привілейованими доступами	Мінімізує ризики компрометації адміністраторських прав і латерального руху	Підвищення керованості доступів і зменшення ймовірності повного захоплення систем
Сегментація інфраструктури	Архітектурний поділ середовищ із контрольованими точками доступу	Обмежує поширення атаки у разі компрометації окремого вузла	Локалізація інцидентів і збереження працездатності критичних сервісів
Відновлюваність систем	Ізольовані резервні копії та альтернативні середовища розгортання сервісів	Забезпечує відновлення після руйнівних атак і знищення даних	Скорочення часу відновлення та мінімізація простоїв бізнес-процесів
Безперервність діяльності	Сценарії деградованої роботи та кризового управління	Дозволяє підтримувати мінімально необхідний рівень сервісів під час інцидентів	Збереження доступності критичних функцій і довіри клієнтів
Корпоративне управління ризиками	Інтеграція кіберризиків у систему загального ризик-менеджменту	Забезпечує ухвалення рішень з урахуванням реальних кіберзагроз	Оптимізація розподілу ресурсів і підвищення відповідальності керівництва
Ризики третіх сторін	Оцінювання безпеки постачальників і контроль інтеграцій	Зменшує ймовірність проникнення через суміжні організації	Підвищення стійкості всієї екосистеми підприємства
Культура кіберстійкості	Навчання персоналу та тренування кризових сценаріїв	Перетворює людський фактор з джерела ризику на фактор стійкості	Зменшення впливу соціальної інженерії та помилок персоналу
Кризові комунікації	Процедури інформування стейкхолдерів під час інцидентів	Дозволяє протидіяти дезінформації та підтримувати довіру	Збереження репутації та керованості інформаційного поля
Оцінювання ефективності	Показники часу виявлення та	Забезпечує контроль	Безперервне вдосконалення системи управління

	відновлення, регулярний аналіз	реального рівня кіберстійкості	

Узагальнення заходів та інструментів, подане в таблиці 3.1, дозволяє розглядати запропонований комплекс рішень як взаємопов’язану систему, спрямовану на поетапне усунення виявлених у другому розділі ризиків і проблем функціонування системи управління кіберстійкістю. Представлені напрями не є ізольованими, а доповнюють один одного, формуючи цілісну архітектуру підвищення стійкості підприємства до гібридних загроз.

Інтерпретація таблиці свідчить, що ключовим вектором удосконалення є зміщення акценту з фрагментарного технічного захисту на формування інтегрованої моделі управління, у якій раннє виявлення атак, контроль доступів і сегментація інфраструктури виступають базовими умовами зменшення ймовірності розвитку прихованих та руйнівних сценаріїв. Їх поєднання забезпечує зростання «видимості» процесів у середовищі та зменшення поверхні атаки, що безпосередньо впливає на зниження ризику ескалації інцидентів до критичного рівня.

Не менш важливим є блок заходів, орієнтований на відновлюваність і безперервність діяльності. Як показав аналіз, навіть за умови успішного проникнення зловмисника саме здатність підприємства швидко відновити критичні сервіси та зберегти мінімально необхідний рівень функціонування визначає реальний рівень кіберстійкості. Заходи, спрямовані на розвиток резервних механізмів і сценаріїв деградованої роботи, дозволяють трансформувати кіберінцидент з катастрофічної події на керований кризовий процес із прогнозованими наслідками.

Інтеграція кіберризиків у систему корпоративного управління, відображена в таблиці, підкреслює необхідність залучення вищого керівництва до процесів формування кіберстійкості. Такий підхід дозволяє забезпечити узгодженість між стратегічними цілями підприємства та рівнем допустимого кіберризику, а також створює передумови для обґрунтованого

розподілу ресурсів на заходи захисту й відновлення. У результаті кіберстійкість перестає бути виключно технічною проблемою і набуває статусу управлінської категорії.

Окремий акцент у таблиці зроблено на управлінні ризиками третіх сторін і розвитку культури кіберстійкості, що відображає розуміння розширеного периметра сучасних загроз. В умовах гібридного протистояння вразливість може виникати не лише всередині підприємства, а й у суміжних організаціях або через людський фактор. Запропоновані заходи дозволяють зменшити цю залежність, формуючи більш стійку екосистему та підвищуючи рівень обізнаності й відповідальності персоналу.

Узагальнюючи, можна стверджувати, що комплекс заходів та інструментів, наведений у таблиці 3.1, створює практичну основу для реалізації запропонованої в попередньому підрозділі моделі системи управління кіберстійкістю. Їх впровадження забезпечує перехід від переважно реактивного реагування на інциденти до адаптивної, орієнтованої на безперервність моделі управління, здатної зменшувати як імовірність виникнення інцидентів, так і масштаб їх наслідків.

3.3. Оцінювання ефективності запропонованих рішень та прогноз результатів їх впровадження

Оцінювання ефективності запропонованих рішень з підвищення кіберстійкості підприємства в умовах гібридних загроз має будуватися на принципі вимірюваності, порівнюваності та прив’язки до критичних бізнес-функцій. На відміну від класичного підходу до інформаційної безпеки, де результат часто ототожнюється з наявністю контролів або відповідністю стандартам, кіберстійкість потребує оцінювання здатності підприємства забезпечувати безперервність і керованість у ситуації, коли інцидент уже відбувся або перебуває у прихованій фазі. Тому ефективність запропонованих

рішень має визначатися не «кількістю встановлених засобів», а тим, наскільки покращуються показники раннього виявлення, локалізації, відновлення, стійкості до повторних атак і збереження довіри стейкхолдерів.

Базовою умовою коректного оцінювання є визначення вихідного рівня, тобто фіксація поточного стану системи управління кіберстійкістю до впровадження змін. Такий «нульовий зріз» має відображати як технічні характеристики (швидкість виявлення інцидентів, повнота журналювання, покриття моніторингом критичних сегментів), так і організаційні характеристики (узгодженість процедур реагування, готовність персоналу, рівень зрілості управління доступами, реалістичність планів безперервності). В умовах реального підприємства доцільно формувати цей зріз на основі аналізу інцидентів за останні періоди, результатів внутрішніх аудитів, журналів SOC/служби безпеки, звітів про тестування відновлення, а також на основі контрольних вправ із реагування та відновлення. Саме порівняння майбутніх результатів із зафіксованими вихідними значеннями дозволяє відокремити реальний ефект змін від випадкових коливань навантаження, сезонності або змін у профілі загроз.

Оскільки гібридні загрози мають багатовекторний характер, оцінювання ефективності має бути багатокритеріальним. У технічній площині ключовим показником стає зменшення часу до виявлення прихованих активностей і зменшення часу до локалізації інциденту. Якщо підприємство впроваджує централізовану кореляцію подій і поведінкову аналітику, ефект має проявлятися в тому, що нетипові дії облікових записів, аномальні переміщення між сегментами, спроби ескалації привілеїв або незвичні шаблони доступу до критичних ресурсів фіксуються швидше і з більшою достовірністю. Практична ефективність таких інструментів проявляється у зменшенні «сліпих зон» спостережуваності, коли атака може тривалий час залишатися непоміченою, а також у зростанні точності реагування, коли команди менше часу витрачають на хибні спрацювання та ручну верифікацію подій.

У площині управління доступами ефективність запропонованих рішень повинна проявлятися через зниження ризику компрометації привілейованих облікових записів і зменшення масштабу наслідків у випадку компрометації звичайного користувача. Після впровадження посиленого контролю привілеїв, централізованого управління ідентичностями та більш жорсткого розмежування ролей очікуваним результатом є обмеження можливостей латерального переміщення зловмисника, оскільки доступи стають короткочасними, контрольованими, прозорими для моніторингу та прив'язаними до конкретного завдання. У термінах кіберстійкості це означає, що навіть при успішній атаці на окремий обліковий запис противнику складніше масштабувати вплив до рівня, здатного паралізувати критичні сервіси.

Особливе місце в оцінюванні ефективності посідає відновлюваність, адже для підприємства, яке надає критичні послуги, саме час і якість відновлення визначають, чи інцидент перетворюється на керований кризовий випадок, чи на системну катастрофу. Якщо впроваджуються ізольовані резервні копії, альтернативні середовища розгортання, регулярні тести відновлення та сценарії деградованої роботи, ефективність має підтверджуватися скороченням часу відновлення критичних функцій і стабільністю результатів відновлення під час повторних тестів. Принциповим є не «разове успішне відновлення», а повторюваність і прогнозованість, коли підприємство може заздалегідь обґрунтувати, за який час буде відновлено конкретний сервіс і які ресурси для цього потрібні. У гібридних умовах додатковим критерієм стає здатність підтримувати мінімально необхідний рівень сервісів навіть при частковій недоступності окремих сегментів або при одночасному впливі кіберінциденту та зовнішніх факторів, таких як проблеми з енергопостачанням або доступом до об'єктів.

Організаційний компонент ефективності тісно пов'язаний із готовністю персоналу та узгодженістю взаємодії під час інциденту. Якщо запропоновані

рішення включають навчання, тренування сценаріїв і формалізацію кризових ролей, ефект має проявлятися у скороченні часу на прийняття рішень, зниженні кількості помилок у критичних діях, підвищенні узгодженості між технічними командами, керівництвом і комунікаційними підрозділами. Для кіберстійкості важливо, щоб реагування було не «героїчним» і залежним від окремих експертів, а системним, коли процедури та рольова модель дозволяють масштабувати реагування навіть у ситуації часткової недоступності людей, ресурсів або інструментів.

Окремо має оцінюватися ефективність управління ризиками третіх сторін, оскільки гібридні загрози часто реалізуються через суміжні організації. Після впровадження підходів до контролю доступів підрядників, вимог до безпеки постачальників і моніторингу інтеграцій очікуваним результатом є зменшення кількості інцидентів, пов’язаних із зовнішніми доступами, і зниження рівня невизначеності щодо того, які саме зв’язки і канали можуть бути використані для атаки. У практичному вимірі це означає, що підприємство отримує більшу керованість розширеного периметра і може включати постачальників у загальні сценарії реагування та відновлення.

Прогноз результатів впровадження запропонованих рішень доцільно формувати, виходячи з причинно-наслідкових зв’язків між заходами та очікуваними змінами показників. У короткостроковій перспективі найбільш помітним результатом зазвичай стає підвищення «видимості» подій безпеки та дисципліни доступів, оскільки ці зміни дають швидкий операційний ефект у вигляді більш раннього виявлення аномалій і зменшення кількості небезпечних конфігурацій. У середньостроковій перспективі очікується стабільне скорочення часу локалізації інцидентів і покращення повторюваності відновлення, адже регулярні тести та стандартизація процесів поступово зменшують залежність від ручних дій і імпровізації. У довгостроковій перспективі ключовим прогнозованим результатом є зниження масштабів і вартості наслідків руйнівних сценаріїв, оскільки

архітектурні зміни, культура кіберстійкості та інтеграція кіберризиків у корпоративне управління формують системну здатність підприємства не лише переживати інциденти, а й адаптуватися до нових форм гібридного впливу.

Фінальною ознакою ефективності запропонованих рішень є їхній вплив на сукупний профіль ризику підприємства, коли імовірність критичних інцидентів зменшується, а наслідки навіть успішних атак стають контрольованими й прогнозованими. Саме така зміна профілю означає перехід від «управління безпекою» до «управління кіберстійкістю», де підприємство здатне підтримувати критичні функції, зберігати керованість і довіру стейкхолдерів у складному середовищі гібридних загроз. У результаті впровадження моделі та комплексу заходів очікується підвищення готовності до прихованих атак, скорочення часу деградації сервісів у разі інцидентів, зниження економічних втрат і зміцнення репутаційної стійкості, що створює реальну конкурентну перевагу та підвищує загальну стійкість підприємства в умовах сучасних викликів.

Таблиця 3.2

Оцінювання ефективності запропонованих рішень та прогноз результатів їх упровадження

Напрям оцінювання	Показник ефективності	Поточний стан (до впровадження)	Очікуваний стан (після впровадження)	Спосіб оцінювання	Прогнозований результат
Раннє виявлення загроз	Час виявлення прихованих атак	Тривалий, можливе пізнє виявлення	Значно скорочений завдяки кореляції та аналітиці	Аналіз журналів інцидентів і звітів SOC	Зменшення масштабу наслідків атак
Локалізація інцидентів	Час до стримування інциденту	Залежить від ручних дій персоналу	Стабільно менший завдяки автоматизації	Порівняння результатів навчальни	Обмеження поширення атаки

				х сценаріїв	
Управління доступами	Інциденти з привілейованими обліковими записами	Існує високий ризик компрометації	Суттєве зниження завдяки централізованому контролю	Аудити доступів і журнали PAM	Зменшення ймовірності повного захоплення систем
Стійкість архітектури	Масштаб ураження при інциденті	Може охоплювати кілька сегментів	Локалізується в межах окремих зон	Аналіз тестових атак і сегментації	Збереження працездатності критичних сервісів
Відновлення сервісів	Час відновлення критичних функцій	Тривалий і нестабільний	Скорочений і прогнозований	Регулярні тести відновлення	Мінімізація простоїв бізнесу
Безперервність діяльності	Рівень доступності під час інциденту	Значна деградація сервісів	Підтримка мінімально необхідного рівня	Моніторинг SLA у кризових сценаріях	Збереження довіри клієнтів
Готовність персоналу	Час прийняття рішень у кризі	Залежить від досвіду окремих осіб	Скорочений завдяки тренуванням	Аналіз навчальних вправ	Підвищення керованості реагування
Культура кіберстійкості	Інциденти через людський фактор	Помітний вплив соціальної інженерії	Зниження кількості інцидентів	Фішинг-тести та опитування	Зменшення організаційних ризиків
Треті сторони	Інциденти через партнерські доступи	Недостатній контроль	Прозорий і контрольований доступ	Аудити постачальників	Зниження ризиків розширеного периметра
Фінансові наслідки	Витрати на подолання інцидентів	Високі й непередбачувані	Менші та прогнозовані	Порівняння витрат до і після	Підвищення економічної стійкості

Загальний рівень кіберстійкості	Сукупний профіль ризику	Високий ризик руйнівних сценаріїв	Контрольований і прийнятний	Комплексна оцінка зрілості	Підвищення адаптивності підприємства

Узагальнення, наведене в таблиці 3.2, дає змогу розглядати ефективність запропонованих рішень як комплексну характеристику, що формується на перетині технічних, організаційних та управлінських змін. Представлені показники відображають не лише потенціал зниження ймовірності інцидентів, а й спроможність підприємства контролювати їх перебіг і наслідки, що відповідає сучасному розумінню кіберстійкості як здатності функціонувати та відновлюватися в умовах постійного тиску гібридних загроз.

Інтерпретація результатів таблиці свідчить, що найбільш відчутний ефект очікується у сфері раннього виявлення та локалізації атак, де впровадження аналітики та централізованого моніторингу дозволяє скоротити часові інтервали між початком прихованої активності та управлінським реагуванням. Це створює передумови для переходу від реактивної моделі реагування до проактивної, коли інцидент ідентифікується ще до настання руйнівної фази, а масштаби потенційних втрат істотно зменшуються.

Не менш важливим є прогнозований вплив заходів на відновлюваність і безперервність діяльності. Очікуване скорочення часу відновлення критичних функцій і підвищення стабільності цього процесу свідчить про формування більш прогнозованої та керованої моделі подолання кризових ситуацій. У практичному вимірі це означає, що навіть за реалізації складних сценаріїв атаки підприємство здатне підтримувати мінімально необхідний рівень сервісів, що є критично важливим для збереження довіри клієнтів і партнерів.

Управлінський вимір ефективності проявляється через інтеграцію кіберризиків у загальну систему прийняття рішень, що, згідно з прогнозом, дозволить оптимізувати розподіл ресурсів і зменшити непрогнозовані

фінансові втрати. У цьому контексті кіберстійкість набуває статусу стратегічного активу, інвестиції в який розглядаються не як витрати, а як засіб забезпечення стабільності та конкурентоспроможності підприємства в умовах високої невизначеності.

Оцінювання готовності персоналу та розвитку культури кіберстійкості, відображене в таблиці, дозволяє прогнозувати підвищення керованості реагування та зменшення впливу людського фактору на виникнення інцидентів. З організаційної точки зору це означає поступове формування середовища, у якому співробітники діють узгоджено, спираючись на відпрацьовані сценарії, а не на інтуїцію чи імпровізацію, що особливо важливо в умовах дефіциту часу та ресурсів під час кризових ситуацій.

Прогнозовані результати у сфері управління третіх сторін і розширеного периметра свідчать про зменшення залежності підприємства від зовнішніх вразливостей та підвищення прозорості взаємодії з партнерами. Це дозволяє розглядати кіберстійкість не лише як внутрішню властивість організації, а як характеристику всієї екосистеми, у межах якої функціонує підприємство.

Узагальнюючи, можна стверджувати, що впровадження запропонованих рішень має призвести до поступового зниження сукупного профілю кіберризику та трансформації системи управління від орієнтації на реагування до орієнтації на адаптацію та безперервність. Очікується, що підприємство отримає здатність не лише швидше виявляти й локалізувати інциденти, а й передбачати потенційні сценарії, планувати ресурси для їх подолання та системно зменшувати наслідки навіть найскладніших гібридних впливів.

ВИСНОВКИ

У результаті виконання магістерської роботи, присвяченої дослідженню системи управління кіберстійкістю підприємства в умовах гібридних загроз, було комплексно проаналізовано теоретичні засади формування кіберстійкості, сучасні підходи до її управління та особливості функціонування організацій у середовищі багатовекторного впливу. Проведене дослідження підтвердило, що кіберстійкість на сучасному етапі розвитку цифрової економіки перестає бути суто технічною категорією і набуває характеру інтегрованої управлінської властивості підприємства, що поєднує здатність до запобігання, виявлення, реагування, відновлення та адаптації до загроз.

У ході роботи встановлено, що еволюція поняття кіберстійкості тісно пов’язана з трансформацією підходів до інформаційної безпеки, переходом від орієнтації на захист окремих ресурсів до забезпечення безперервності критичних бізнес-функцій. Аналіз природи гібридних загроз показав, що їхня особливість полягає у поєднанні кібернетичних, інформаційно-психологічних та фізичних впливів, що істотно ускладнює процес управління ризиками та потребує інтегрованого міждисциплінарного підходу. Розгляд нормативно-правових і міжнародних стандартів дозволив дійти висновку про необхідність адаптації загальновизнаних моделей і вимог до реалій функціонування підприємств в умовах підвищеної невизначеності та воєнних викликів.

На основі аналізу діяльності реального підприємства та оцінювання стану його системи інформаційної безпеки було виявлено, що, попри наявність розвинених технічних засобів захисту та спроможності до відновлення після масштабних інцидентів, система управління кіберстійкістю характеризується низкою проблем, пов’язаних із раннім виявленням прихованих атак, керуванням привілейованими доступами, складністю сегментації

великомасштабної інфраструктури, залежністю від третіх сторін і фізичних чинників, а також високою вартістю деградації сервісів. Це підтвердило доцільність переходу від фрагментарної моделі безпеки до цілісної системи управління кіберстійкістю, інтегрованої в загальне корпоративне управління.
У роботі розроблено модель системи управління кіберстійкістю підприємства в умовах гібридних загроз, яка базується на поєднанні управлінського, процесного, технологічного та людського вимірів і орієнтована на забезпечення керованості та безперервності критичних функцій. Запропонована модель дозволяє розглядати кіберстійкість як динамічну властивість організації, що формується в результаті безперервного циклу оцінювання ризиків, упровадження заходів, моніторингу, реагування, відновлення та адаптації. Її практична цінність полягає в можливості застосування як методологічної основи для побудови або трансформації систем управління на підприємствах різних галузей.

Обґрунтовані в роботі заходи та інструменти підвищення кіберстійкості спрямовані на усунення виявлених проблем і охоплюють напрями раннього виявлення загроз, контролю ідентичностей і доступів, сегментації інфраструктури, підвищення відновлюваності, управління безперервністю діяльності, інтеграції кіберризиків у корпоративне управління, розвитку культури кіберстійкості та управління ризиками третіх сторін. Оцінювання ефективності запропонованих рішень і прогноз результатів їх упровадження показали, що реалізація цих заходів здатна забезпечити скорочення часу виявлення і локалізації інцидентів, підвищення прогнозованості відновлення критичних сервісів, зменшення фінансових і репутаційних втрат та формування більш контрольованого профілю кіберризику підприємства.

Загалом результати дослідження підтверджують, що перехід до системного управління кіберстійкістю є необхідною умовою сталого розвитку підприємств у сучасному середовищі гібридних загроз. Запропоновані в роботі підходи та рішення мають як теоретичне значення для подальшого розвитку

наукових уявлень про кіберстійкість, так і практичну цінність для використання у діяльності підприємств, що прагнуть підвищити свою стійкість до складних багатовекторних викликів. Перспективи подальших досліджень пов’язані з розробленням методів кількісного вимірювання кіберстійкості, моделюванням сценаріїв гібридних загроз і створенням інструментів підтримки управлінських рішень у режимі реального часу, що дозволить ще більше підвищити адаптивність і надійність сучасних організацій.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection — Information security management systems — Requirements. Geneva : ISO, 2022.
2. ISO/IEC 27002:2022. Information security, cybersecurity and privacy protection — Information security controls. Geneva : ISO, 2022.
3. ISO/IEC 27005:2022. Information security risk management. Geneva : ISO, 2022.
4. ISO 22301:2019. Security and resilience — Business continuity management systems — Requirements. Geneva : ISO, 2019.
5. ISO 22316:2017. Security and resilience — Organizational resilience — Principles and attributes. Geneva : ISO, 2017.
6. NIST. Cybersecurity Framework 2.0. Gaithersburg : NIST, 2024. URL: https://www.nist.gov/cyberframework (дата звернення: 19.12.2025).
7. NIST SP 800-53 Rev. 5. Security and Privacy Controls for Information Systems and Organizations. Gaithersburg : NIST, 2020.
8. NIST SP 800-61 Rev. 2. Computer Security Incident Handling Guide. Gaithersburg : NIST, 2012.
9. NIST SP 800-92. Guide to Computer Security Log Management. Gaithersburg : NIST, 2006.
10. ENISA. Cybersecurity Resilience in the EU. Heraklion : ENISA, 2023. URL: https://www.enisa.europa.eu (дата звернення: 19.12.2025).
11. ENISA. Threat Landscape 2023. Heraklion : ENISA, 2023.
12. World Economic Forum. Global Cybersecurity Outlook 2024. Geneva : WEF, 2024.
13. Von Solms R., Van Niekerk J. From information security to cyber security. Computers & Security. 2013. Vol. 38. P. 97–102.

14. Linkov I., Trump B. The Science and Practice of Resilience. Cham : Springer, 2019. 358 p.
15. Hollnagel E., Woods D., Leveson N. Resilience Engineering: Concepts and Precepts. Aldershot : Ashgate, 2006. 397 p.
16. Kott A., Linkov I. Cyber Resilience of Systems and Networks. Cham : Springer, 2019. 312 p.
17. Bodeau D., Graubart R. Cyber Resiliency Engineering Framework. Bedford : MITRE, 2017.
18. MITRE. Cyber Resiliency Metrics Framework. Bedford : MITRE, 2021.
19. European Union. Directive (EU) 2022/2555 (NIS2 Directive). Brussels : EU, 2022.
20. European Union. Regulation (EU) 2019/881 (Cybersecurity Act). Brussels : EU, 2019.
21. Закон України «Про основні засади забезпечення кібербезпеки України». Відомості Верховної Ради України. 2017. № 45. Ст. 403.
22. Стратегія кібербезпеки України. Указ Президента України №447/2021 від 26.08.2021.
23. ДСТУ ISO/IEC 27001:2015. Інформаційні технології. Методи захисту. Київ : ДП «УкрНДНЦ», 2016.
24. ДСТУ ISO 22301:2015. Соціальна безпека. Управління безперервністю бізнесу. Київ : ДП «УкрНДНЦ», 2016.
25. Verizon. Data Breach Investigations Report 2024. New York : Verizon, 2024.
26. Mandiant. M-Trends 2024. Sunnyvale : Google Cloud, 2024.
27. Kaspersky. Cybersecurity and Cyber Resilience Report 2023. London : Kaspersky, 2023.
28. ISACA. State of Cybersecurity 2023. Schaumburg : ISACA, 2023.
29. Gartner. Top Trends in Cybersecurity 2024. Stamford : Gartner, 2024.
30. Symantec. Internet Security Threat Report 2023. Mountain View : Broadcom, 2023.

31. Sillaber C., Sauerwein C. Cybersecurity resilience: Definition and assessment. Computers & Security. 2021. Vol. 103.
32. Radanliev P. et al. Cyber risk management and resilience. Journal of Risk Research. 2020. Vol. 23(5). P. 567–586.
33. Tøndel I., Line M., Jaatun M. Information security incident management. Computers & Security. 2014. Vol. 45. P. 124–136.
34. Behl A., Behl K. Cybersecurity and Cyberwar: What Everyone Needs to Know. Oxford : Oxford University Press, 2017. 240 p.
35. Andress J., Winterfeld S. Cyber Warfare: Techniques, Tactics and Tools. Amsterdam : Elsevier, 2014. 320 p.
36. Conti G. Security Data Visualization. San Francisco : No Starch Press, 2016. 384 p.
37. Cherdantseva Y., Hilton J. A reference model of information assurance. Computers & Security. 2013. Vol. 32. P. 69–92.
38. Kolini F., Janczewski L. Cyber Resilience: A systematic literature review. Journal of Cyber Security Technology. 2022. Vol. 6(2). P. 65–88.
39. Microsoft. Digital Defense Report 2023. Redmond : Microsoft, 2023.
40. OECD. Digital Security Risk Management. Paris : OECD Publishing, 2020.
41. PwC. Global Digital Trust Insights 2024. London : PwC, 2024.
42. Accenture. State of Cyber Resilience 2023. Dublin : Accenture, 2023.
43. Cisco. Cybersecurity Readiness Index 2024. San Jose : Cisco, 2024.
44. IBM Security. Cost of a Data Breach Report 2024. Armonk : IBM, 2024.
45. UK NCSC. Cyber Resilience Framework. London : NCSC, 2023.
46. Australian Cyber Security Centre. Cyber Security Strategy 2023–2030. Canberra : ACSC, 2023.
47. National Academies of Sciences. Cyber Resilience: Concepts, Design and Measurement. Washington : NAP, 2022.
48. FEMA. National Cyber Incident Response Plan. Washington : DHS, 2016.

49. European Commission. Cybersecurity Strategy for the Digital Decade. Brussels : EC, 2020.
50. Shackleford D. The Cybersecurity Body of Knowledge. Hoboken : Wiley, 2021. 512 p.
51. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 № 2163-VIII // Відомості Верховної Ради України. – 2017. – № 45. – Ст. 403.
52. Стратегія кібербезпеки України : Указ Президента України від 26.08.2021 № 447/2021. – URL: https://www.president.gov.ua (дата звернення: 19.12.2025).
53. Про національну безпеку України : Закон України від 21.06.2018 № 2469-VIII // Відомості Верховної Ради України. – 2018. – № 31. – Ст. 241.
54. Про захист інформації в інформаційно-телекомунікаційних системах : Закон України від 05.07.1994 № 80/94-ВР // Відомості Верховної Ради України. – 1994. – № 31. – Ст. 286.
55. Про інформацію : Закон України від 02.10.1992 № 2657-XII // Відомості Верховної Ради України. – 1992. – № 48. – Ст. 650.
56. Про електронні комунікації : Закон України від 16.12.2020 № 1089-IX // Відомості Верховної Ради України. – 2021. – № 9. – Ст. 75.
57. ДСТУ ISO/IEC 27001:2015. Інформаційні технології. Методи захисту. Системи управління інформаційною безпекою. Вимоги. – Київ : ДП «УкрНДНЦ», 2016.
58. ДСТУ ISO 22301:2015. Соціальна безпека. Системи управління безперервністю бізнесу. Вимоги. – Київ : ДП «УкрНДНЦ», 2016.
59. ДСТУ ISO/IEC 27005:2015. Інформаційні технології. Методи захисту. Управління ризиками інформаційної безпеки. – Київ : ДП «УкрНДНЦ», 2016.
60. Бурячок В. Л., Толубко В. Б. Кібербезпека : підручник. – Київ : НАОУ, 2018. – 312 с.

61. Корченко О. Г., Казмірчук С. В. Інформаційна безпека держави : монографія. – Київ : Наук. думка, 2019. – 384 с.
62. Ліпкан В. А. Національна і міжнародна безпека у визначеннях та поняттях. – Київ : Текст, 2018. – 400 с.
63. Гнатюк С. О. Кібербезпека в умовах гібридних загроз // Захист інформації. – 2020. – Т. 22, № 4. – С. 250–259.
64. Мельник М. І., Шахов А. В. Управління ризиками інформаційної безпеки в організаціях // Інформаційна безпека. – 2021. – № 1. – С. 35–42.
65. Баранов О. А. Кібербезпека: правове забезпечення : монографія. – Київ : Юрінком Інтер, 2019. – 288 с.
66. Марущак А. І. Правові основи кібербезпеки України. – Київ : Алерта, 2020. – 256 с.
67. Конахович Г. Ф., Паціра Є. В. Основи захисту інформації. – Київ : КПІ ім. І. Сікорського, 2019. – 220 с.
68. Довгий С. О., Трофименко О. Г. Кіберпростір і національна безпека України. – Київ : Ін-т обдарованої дитини НАПН України, 2020. – 300 с.
69. Шпак Л. О. Кіберстійкість як новий вимір інформаційної безпеки // Наукові записки з інформаційної безпеки. – 2021. – № 2. – С. 48–55.
70. Руденко М. В. Управління інформаційною безпекою підприємства. – Харків : Форт, 2019. – 240 с.
71. Ткаченко В. І. Моделі та методи забезпечення кібербезпеки організацій // Системи управління, навігації та зв’язку. – 2020. – № 3. – С. 112–118.
72. Савченко О. М. Кіберризики у системі економічної безпеки підприємства // Економічна безпека. – 2021. – № 1. – С. 67–73.
73. Грищук Р. В. Основи кібербезпеки. – Житомир : ЖДТУ, 2018. – 196 с.
74. Козловський В. М. Інформаційна та кібербезпека: загрози і виклики // Вісник НТУУ «КПІ». – 2020. – № 2. – С. 25–31.

75. Ситник К. М. Стратегічне управління інформаційною безпекою. – Київ : КНЕУ, 2019. – 280 с.
76. Шевченко В. Л. Гібридні загрози у кіберпросторі // Стратегічні пріоритети. – 2021. – № 4. – С. 98–105.
77. Пилипчук В. Г. Інформаційна безпека: сучасні підходи. – Київ : Атіка, 2018. – 256 с.
78. Державна служба спеціального зв’язку та захисту інформації України. Щорічна доповідь про стан кібербезпеки України. – Київ, 2023.
79. Національний координаційний центр кібербезпеки. Аналітичний звіт за 2023 рік. – Київ, 2024.
80. РНБО України. Біла книга з питань кібербезпеки. – Київ, 2021.
81. Коваленко О. В. Організаційні аспекти управління кібербезпекою підприємств // Менеджмент та безпека. – 2020. – № 2. – С. 54–60.
82. Петренко С. А. Системи управління інформаційною безпекою. – Львів : Львівська політехніка, 2019. – 210 с.
83. Іванченко Є. А. Кіберзагрози та методи протидії. – Одеса : ОНУ, 2020. – 180 с.
84. Сопілко І. М. Правові засади забезпечення кібербезпеки в Україні // Юридична наука. – 2021. – № 3. – С. 40–46.
85. Кузьменко О. В. Кібербезпека як складова національної безпеки // Держава і право. – 2019. – Вип. 85. – С. 120–127.
86. Бондаренко Ю. Л. Управління інцидентами інформаційної безпеки. – Київ : Політехніка, 2020. – 200 с.
87. Федоренко В. Л. Кібербезпека в умовах цифрової трансформації. – Київ : Ліра-К, 2021. – 260 с.
88. Кравченко М. О. Інформаційні війни та кіберпростір // Політологічні студії. – 2020. – № 2. – С. 89–96.
89. Жуков С. А. Кіберстійкість організацій: теоретичні аспекти // Вісник ХНУРЕ. – 2022. – № 1. – С. 61–67.

90. Олійник О. В. Механізми забезпечення кібербезпеки підприємств // Економіка та держава. – 2021. – № 5. – С. 104–109.
91. Климчук М. М. Кіберризики в системі управління підприємством // Бізнес-інформ. – 2020. – № 10. – С. 221–226.
92. Романов О. В. Кіберзахист критичної інфраструктури України. – Київ : НІСД, 2021. – 180 с.
93. Тарасенко Н. О. Стійкість інформаційних систем до кіберзагроз // Сучасний захист інформації. – 2022. – № 1. – С. 33–39.
94. Гаврилюк Р. В. Кібербезпека бізнесу. – Київ : Освіта України, 2019. – 224 с.
95. Міщенко Д. А. Управління безперервністю діяльності підприємств. – Київ : КНЕУ, 2020. – 240 с.
96. Кучерявий О. П. Інформаційна безпека в корпоративних системах. – Харків : ХНЕУ, 2018. – 210 с.
97. Поліщук В. М. Системний підхід до кіберзахисту організацій // Вісник ЖДТУ. – 2021. – № 2. – С. 72–78.
98. Яремчук Ю. Є. Кіберзагрози та економічна безпека підприємства // Економіка і суспільство. – 2022. – № 36.
99. Кравчук О. С. Управління інформаційними ризиками. – Київ : Центр учбової літератури, 2019. – 256 с.
100. Сидоренко О. М. Кібербезпека та кіберстійкість: сучасні виклики // Науковий вісник НАДУ. – 2023. – № 1. – С. 95–102.

ДОДАТОК А

```
cyber_resilience_metrics.py
incident_id,detected_at,contained_at,recovered_at,severity,type,sla_hours
INC-001,2025-10-01 08:10,2025-10-01 10:05,2025-10-01 18:40,High,Ransomware,24
INC-002,2025-10-04 12:00,2025-10-04 12:50,2025-10-04 15:30,Medium,Phishing,8
"""
from __future__ import annotations
import argparse
from dataclasses import dataclass
from datetime import datetime
from pathlib import Path
from typing import Optional, List, Dict, Tuple
import pandas as pd
DT_FORMATS = [
    "%Y-%m-%d %H:%M:%S",
    "%Y-%m-%d %H:%M",
    "%d.%m.%Y %H:%M:%S",
    "%d.%m.%Y %H:%M",
]


def parse_dt(x: str) -> datetime:
    x = str(x).strip()
    for fmt in DT_FORMATS:
        try:
            return datetime.strptime(x, fmt)
```

```
        except ValueError:
            pass
    raise ValueError(f"Невідомий формат дати/часу: {x!r}. Підтримуються: {DT_FORMATS}")

def hours_between(a: datetime, b: datetime) -> float:
    return (b - a).total_seconds() / 3600.0

@dataclass
class Metrics:
    n: int
    mttd_h: float                  # Mean Time To Detect (тут: від detected_at до contained_at? зазвичай detect від start; але старту немає)
    mttc_h: float              # Mean Time To Contain (detected -> contained)
    mttr_h: float              # Mean Time To Recover (contained -> recovered)
    end_to_end_h: float        # Mean Time End-to-End (detected -> recovered)
    sla_breach_rate: float     # частка інцидентів із перевищенням SLA
    by_severity: Dict[str, int]
    by_type: Dict[str, int]

def compute_metrics(df: pd.DataFrame) -> Metrics:
    required = {"incident_id", "detected_at", "contained_at", "recovered_at", "severity", "type", "sla_hours"}
    missing = required - set(df.columns)
    if missing:
        raise ValueError(f"У CSV бракує колонок: {sorted(missing)}")

    # Парсимо дати
    for col in ["detected_at", "contained_at", "recovered_at"]:
```

```
        df[col] = df[col].apply(parse_dt)

    # Обчислюємо тривалості
    df["t_contain_h"] = df.apply(lambda r: hours_between(r["detected_at"], r["contained_at"]), axis=1)
    df["t_recover_h"] = df.apply(lambda r: hours_between(r["contained_at"], r["recovered_at"]), axis=1)
    df["t_end2end_h"] = df.apply(lambda r: hours_between(r["detected_at"], r["recovered_at"]), axis=1)

    # Перевірка SLA (за замовчуванням SLA застосуємо до end-to-end)
    df["sla_hours"] = pd.to_numeric(df["sla_hours"], errors="coerce")
    if df["sla_hours"].isna().any():
        raise ValueError("Колонка sla_hours має містити числові значення (години).")

    df["sla_breach"] = df["t_end2end_h"] > df["sla_hours"]

    n = len(df)
    mttc = float(df["t_contain_h"].mean()) if n else 0.0
    mttr = float(df["t_recover_h"].mean()) if n else 0.0
    end2end = float(df["t_end2end_h"].mean()) if n else 0.0

    # MTTD строго потребує "start_at". Якщо його немає, часто використовують proxy:
    # тут дамо MTTD як 0 або пояснення в роботі; але практично корисно:
    # можна інтерпретувати як "час від фіксації до первинної реакції" = MTTC.
    # Тому MTTD_h = MTTC_h (proxy).
    mttd_proxy = mttc
```

```
    by_sev = df["severity"].value_counts(dropna=False).to_dict()
    by_type = df["type"].value_counts(dropna=False).to_dict()
    breach_rate = float(df["sla_breach"].mean()) if n else 0.0

    return Metrics(
        n=n,
        mttd_h=mttd_proxy,
        mttc_h=mttc,
        mttr_h=mttr,
        end_to_end_h=end2end,
        sla_breach_rate=breach_rate,
        by_severity=by_sev,
        by_type=by_type,
    )

def format_report(m: Metrics) -> str:
    def pct(x: float) -> str:
        return f"{x*100:.1f}%"

    lines = []
    lines.append("ЗВІТ ПРО МЕТРИКИ КІБЕРСТІЙКОСТІ (за журналом інцидентів)")
    lines.append(f"Кількість інцидентів: {m.n}")
    lines.append("")
    lines.append("Часові метрики (середні значення, години):")
    lines.append(f"MTTD (proxy): {m.mttd_h:.2f} год")
    lines.append(f"MTTC (detected→contained): {m.mttc_h:.2f} год")
    lines.append(f"MTTR (contained→recovered): {m.mttr_h:.2f} год")
```

```
    lines.append(f"End-to-End (detected→recovered): {m.end_to_end_h:.2f} год")
    lines.append("")
    lines.append(f"Частка інцидентів із перевищенням SLA (end-to-end): {pct(m.sla_breach_rate)}")
    lines.append("")
    lines.append("Розподіл за критичністю (severity):")
    for k, v in m.by_severity.items():
        lines.append(f"  {k}: {v}")
    lines.append("")
    lines.append("Розподіл за типами інцидентів (type):")
    for k, v in m.by_type.items():
        lines.append(f"  {k}: {v}")

    lines.append("")
    lines.append("Примітка щодо MTTD:")
    lines.append("У класичному вигляді MTTD потребує часу початку атаки/відхилення (start_at).")
    lines.append("Якщо start_at не ведеться, допустимо використовувати proxy-метрику (час до стримування від моменту виявлення).")

    return "\n".join(lines)


def main():
    ap = argparse.ArgumentParser(description="Оцінювання метрик кіберстійкості з CSV інцидентів")
    ap.add_argument("--input", "-i", required=True, help="Шлях до CSV з інцидентами")
```

```
    ap.add_argument("--export-summary", "-o", default=None, help="Шлях для збереження summary CSV (опційно)")
    args = ap.parse_args()

    inp = Path(args.input)
    if not inp.exists():
        raise FileNotFoundError(f"Файл не знайдено: {inp}")

    df = pd.read_csv(inp)
    metrics = compute_metrics(df)
    print(format_report(metrics))

    if args.export_summary:
        out = Path(args.export_summary)
        summary = pd.DataFrame([{
            "n_incidents": metrics.n,
            "mttd_proxy_h": metrics.mttd_h,
            "mttc_h": metrics.mttc_h,
            "mttr_h": metrics.mttr_h,
            "end_to_end_h": metrics.end_to_end_h,
            "sla_breach_rate": metrics.sla_breach_rate,
        }])
        summary.to_csv(out, index=False, encoding="utf-8")
        print(f"\nSummary збережено у: {out}")


if __name__ == "__main__":
    main()
```