

Український державний університет залізничного транспорту

Кафедра економіки та управління виробничим і комерційним бізнесом

ФОРМУВАННЯ ЦИФРОВОЇ СТІЙКОСТІ ПІДПРИЄМСТВ ЗАЛІЗНИЧНОГО
ТРАНСПОРТУ В УМОВАХ ЗАГОСТРЕННЯ КІБЕРЗАГРОЗ

Пояснювальна записка і розрахунки
до кваліфікаційної роботи

МРЕ.011.02.06 ПЗ

Розробив: студент 2 курсу, групи 214-П-324
спеціальності 076 «Підприємництво та торгівля»
(роботу виконано самостійно, відповідно до
принципів академічної доброчесності)



(підпис)

Сергій ПОГРЕБНЯК

Керівник: доцент, д-р екон. наук
Ганна ОБРУЧ

Рецензент: канд. екон. наук
Олена СЕМЕНЦОВА

Український державний університет залізничного транспорту

Факультет економічний

Кафедра економіки та управління виробничим і комерційним бізнесом

Рівень вищої освіти: магістр

Спеціальність: 076 «Підприємництво та торгівля»

Освітня програма: «Підприємництво»

ЗАТВЕРДЖУЮ

Завідувач кафедри,
професор, д-р екон. наук



Володимир ДИКАНЬ

«____» _____ 2026 р.

ЗАВДАННЯ НА КВАЛІФІКАЦІЙНУ РОБОТУ Погребняку Сергію Романовичу

1 Тема «Формування цифрової стійкості підприємств залізничного транспорту в умовах загострення кіберзагроз»

керівник Обруч Ганна Володимирівна, д-р екон. наук, доцент

затверджені розпорядженням по економічному факультету

від «27» лютого 2025 року № 70/25

2 Строк подання студентом закінченої роботи «06» січня 2026 року

3 Вихідні дані: Статистичні дані про діяльність ПрАТ «Київ-Дніпровське міжгалузеве підприємство промислового залізничного транспорту»

Фінансово-економічна звітність ПрАТ «Київ-Дніпровське міжгалузеве підприємство промислового залізничного транспорту»

Науково-методична література

Періодичні видання

4 Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити):

1 Теоретико-методологічні аспекти формування цифрової стійкості підприємств

2 Техніко-економічний аналіз діяльності ПрАТ «Київ – Дніпровське міжгалузеве підприємство промислового залізничного транспорту»

3 Практичні рекомендації щодо забезпечення цифрової стійкості підприємств промислового залізничного транспорту

5 Перелік графічного матеріалу

1 Мета, завдання, об'єкт, предмет та новизна дослідження

2 Глобальні витрати та масштаби кіберзлочинності, її наслідки кібератак у розрізі галузей

3 Перелік кіберризиків, які здійснюють найбільший вплив на бізнес-суб'єкти в контексті геополітичної напруженості. Історичний контекст найвідоміших кіберзлочинів

4 SWOT-аналіз українського ринку кібербезпеки

5 Види стійкості підприємства. Порівняльна характеристика цифрової безпеки та стійкості. Компоненти цифрової стійкості

6 Концепція забезпечення цифрової стійкості підприємства

7 – 8 Аналіз показників діяльності ПрАТ «Київ-Дніпровське міжгалузеве підприємство промислового залізничного транспорту»

9 Моделі компетенцій персоналу у сфері кібербезпеки. Рекомендації для підвищення компетентності працівників підприємства промислового залізничного транспорту у сфері кібербезпеки

10 Стратегія та інструменти забезпечення цифрової стійкості підприємства промислового залізничного транспорту

11 Орієнтовний річний план заходів із формування культури кібергігієни на промисловому підприємстві залізничного транспорту. Очікувані переваги впровадження цифрового застосунку для формування кібергігієни

12 Орієнтовні витрати на розроблення цифрового застосунку. Ефективність реалізації запропонованих заходів

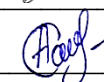
6 Консультанти окремих розділів

Розділ	Прізвище, ініціали, посада та науковий ступінь консультанта	Підпис, дата	
		завдання видав	завдання прийняв

7 Дата видачі завдання «24» лютого 2025 року.

КАЛЕНДАРНИЙ ПЛАН

Назва етапів	Строк виконання етапів	Примітка
1 Теоретико-методологічні аспекти формування цифрової стійкості підприємств	21.05.2025	виконано
2 Техніко-економічний аналіз діяльності ПрАТ «Київ – Дніпровське міжгалузеве підприємство промислового залізничного транспорту»	31.10.2025	виконано
3 Практичні рекомендації щодо забезпечення цифрової стійкості підприємств промислового залізничного транспорту	27.11.2025	виконано
Висновки	22.12.2025	виконано
Графічна частина	31.12.2025	виконано

Студент  Сергій ПОГРЕБНЯК
Керівник  Ганна ОБРУЧ

Зміст

Вступ	6
1 Теоретико-методологічні аспекти формування цифрової стійкості підприємств	10
1.1 Посилення кіберзагроз для суб'єктів підприємництва в умовах цифровізації	10
1.2 Еволюція поняття цифрової стійкості підприємств	25
1.3 Формування концепції забезпечення цифрової стійкості підприємств	32
Висновки до розділу 1	37
2 Техніко-економічний аналіз діяльності ПрАТ «Київ – Дніпровське міжгалузеве підприємство промислового залізничного транспорту»	40
2.1 Загальна характеристика діяльності підприємства	40
2.2 Аналіз обсягів діяльності підприємства	42
2.3 Аналіз стану основних засобів підприємства	43
2.4 Аналіз ефективності використання трудових ресурсів підприємства	51
2.5 Аналіз операційних витрат діяльності підприємства	55
2.6 Аналіз фінансових результатів діяльності підприємства	60
2.7 Аналіз інвестиційної політики підприємства	63
Висновки до розділу 2	65
3 Практичні рекомендації щодо забезпечення цифрової стійкості підприємств промислового залізничного транспорту	69
3.1 Роль людського фактору у забезпечення цифрової стійкості підприємств промислового залізничного транспорту	69
3.2 Розроблення комплексної стратегії цифрової стійкості підприємства промислового залізничного транспорту	80

					МРЕ.011.02.06 ПЗ				
Змн.	Арк.	№ докум.	Підпис	Дата					
Розроб.		Погребняк			Формування цифрової стійкості підприємств залізничного транспорту в умовах загострення кіберзагроз		Літ.	Арк.	Аркуші
Перевір.		Обруч						4	119
Реценз.		Семенцова					УкрДУЗТ		
Н. Контр.		Назаренко							
Затверд.		Дикань							

3.3 Формування культури кібергігієни на промисловому підприємстві залізничного транспорту	94
Висновки до розділу 3	103
Висновки	107
Список використаних джерел	111

					МРЕ.011.02.06 ПЗ	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		5

Вступ

Актуальність теми. В умовах масштабної та прискореної цифровізації транспортні підприємства, у т. ч. і залізничного транспорту, активно впроваджують автоматизовані системи управління рухом, GPS-моніторинг, IoT-пристрої та електронний документообіг. Це підвищує ефективність роботи та конкурентоспроможність, але при цьому робить їх більш вразливими до кіберзагроз. Зростання кількості атак на критичну інфраструктуру у світі підтверджує необхідність формування цифрової стійкості, яка дозволяє не лише запобігати інцидентам, а й швидко відновлюватися після них.

Особливу актуальність тема набуває через те, що кіберінциденти у транспортній сфері можуть мати не лише фінансові наслідки, а й безпосередньо впливати на безпеку руху, зупинку перевезень та довіру клієнтів і партнерів. Тому підприємства залізничного транспорту мають переходити від базових заходів захисту до комплексних стратегій цифрової стійкості, що включають такі інноваційні технології як штучний інтелект для аналізу аномалій, блокчейн для захисту даних та сучасні системи управління інцидентами.

Таким чином, дослідження проблеми формування цифрової стійкості підприємств промислового залізничного транспорту є надзвичайно актуальним, оскільки спрямоване на забезпечення безперервності транспортних процесів, зниження ризиків кіберінцидентів та підвищення конкурентоспроможності галузі в умовах глобальної цифрової трансформації та загострення кіберзагроз.

Зв'язок роботи з науковими програмами, темами. Кваліфікаційна робота виконувалася у рамках і за тематикою наукових досліджень, що проводяться на кафедрі «Економіка та управління виробничим і комерційним бізнесом» Українського державного університету залізничного транспорту.

Метою кваліфікаційної роботи є удосконалення теоретичних аспектів і розроблення практичних рекомендацій щодо формування цифрової стійкості підприємств промислового залізничного транспорту в умовах кіберзагроз.

Для досягнення поставленої мети необхідно вирішити наступні **завдання**:

- 1) проаналізувати процеси та масштаби посилення кіберзагроз для суб'єктів підприємництва в умовах цифровізації;
- 2) розглянути еволюцію поняття цифрової стійкості підприємств;
- 3) сформуванати концепцію забезпечення цифрової стійкості підприємств;
- 4) проаналізувати діяльність ПрАТ «Київ-Дніпровське міжгалузеве підприємство промислового залізничного транспорту», з'ясувати основні проблеми і визначити резерви підвищення ефективності функціонування;
- 5) дослідити роль людського фактору у забезпечення цифрової стійкості підприємств промислового залізничного транспорту;
- 6) розробити комплексну стратегію цифрової стійкості підприємства промислового залізничного транспорту;
- 7) сформуванати програму підтримки культури кібергігієни на підприємстві промислового залізничного транспорту і технологічне забезпечення її реалізації;
- 8) розрахувати економічну ефективність розроблення та застосування цифрового застосунку формування і підтримки культури кібергігієни.

Об'єктом дослідження є процес забезпечення цифрової стійкості підприємств промислового залізничного транспорту.

Предметом дослідження є теоретико-методологічні основи, методичні та прикладні положення забезпечення цифрової стійкості підприємств промислового залізничного транспорту в умовах кіберзагроз.

Інформаційною основою роботи є дослідження вітчизняних та закордонних вчених у сфері забезпечення цифрової безпеки та стійкості суб'єктів економічної діяльності, у тому числі підприємств промислового залізничного транспорту, статистична та довідкова інформація, періодичні видання та відомості з мережі Інтернет, які містяться у джерелах [1 – 78], наведених у списку використаних джерел, а також інформація, отримана в результаті консультування з керівником роботи, науковими, науково-педагогічними працівниками та іншими особами, яка є неопублікованими

авторськими напрацюваннями (найсучасніша інформація дослідницького, інноваційного характеру), дозволена для використання автору роботи виключно при виконанні тільки цієї кваліфікаційної роботи.

Методи дослідження. Для досягнення поставленої мети та вирішення відповідних завдань у кваліфікаційній роботі використані такі загальнонаукові та спеціальні методи: порівняльний аналіз і графічний метод – використано для визначення та відображення тенденцій розвитку ПрАТ «Київ – Дніпровське міжгалузеве підприємство промислового залізничного транспорту»; систематизація і класифікація – для деталізації наслідків кібератак у розрізі галузей економіки, розкриття ключових етапів розвитку кіберзагроз, класифікації кіберзагроз підприємств, визначення компонентів цифрової стійкості, розкриття матриці компетенцій за ролями для підприємства промислового залізничного транспорту у сфері кібербезпеки; морфологічного аналізу – для удосконалення змісту поняття «цифрова стійкість підприємства промислового залізничного транспорту»; системний підхід – для розроблення концепції та стратегії забезпечення цифрової стійкості підприємства промислового залізничного транспорту.

Наукова новизна полягає у розробленні концепції забезпечення цифрової стійкості підприємств, що розкриває принципи, напрями, завдання та інструменти, які дозволяють інтегрувати цифрові технології у бізнес-процеси, формувати гнучкі управлінські стратегії, забезпечувати кібербезпеку та ефективне використання інформаційних ресурсів.

Практична значущість кваліфікаційної роботи полягає в розробленні стратегії забезпечення цифрової стійкості підприємства промислового залізничного транспорту і обґрунтуванні доцільності впровадження цифрового застосунку формування та підтримки культури кібергігієни.

Результатами роботи є розроблення та обґрунтування підходів до забезпечення цифрової стійкості підприємств промислового залізничного транспорту і формуванні практичних пропозицій щодо впровадження цифрового застосунку формування та підтримки культури кібергігієни.

Апробація результатів роботи. Основні положення і результати кваліфікаційної роботи доповідалися на міжнародній науково-практичній конференції «Економіко-правове та фінансово-облікове забезпечення сталого розвитку : сучасні виклики та тренди» Харківського національного університету внутрішніх справ (21 листопада 2025 р., м. Вінниця).

Публікації. За темою роботи опубліковано 1 статтю у науковому журналі «Інвестиції: практика та досвід» (у співавторстві).

Структура і обсяг роботи. Кваліфікаційна робота складається з вступу, трьох розділів, висновків, списку використаних джерел.

Перший розділ присвячено теоретичним питанням, пов'язаним із формуванням цифрової стійкості підприємств, а саме аналізу процесів та масштабів посилення кіберзагроз для суб'єктів підприємництва в умовах цифровізації, розгляду еволюції поняття цифрової стійкості підприємств і формуванню концепції забезпечення цифрової стійкості підприємств.

У другому розділі наведено характеристику діяльності ПрАТ «Київ – Дніпровське міжгалузеве підприємство промислового залізничного транспорту», проаналізовано обсягові показники роботи, стан та ефективність використання основних засобів, ефективність використання трудових ресурсів, операційні витрати та фінансові результати, капітальні інвестиції.

Третій розділ роботи присвячено формуванню практичних рекомендацій щодо забезпечення цифрової стійкості підприємств промислового залізничного транспорту, зокрема дослідженню ролі людського фактору у забезпеченні цифрової стійкості підприємства, розробленню комплексної стратегії цифрової стійкості підприємства промислового залізничного транспорту, формуванню програми підтримки культури кібергігієни на підприємстві промислового залізничного транспорту і технологічному забезпеченню її реалізації, оцінюванню економічної ефективності розроблення та застосування цифрового застосунку формування і підтримки культури кібергігієни.

1 Теоретико-методологічні аспекти формування цифрової стійкості підприємств

1.1 Посилення кіберзагроз для суб'єктів підприємництва в умовах цифровізації

У сучасних умовах цифрової трансформації суб'єкти економічної діяльності дедалі більше залежать від інформаційних технологій, автоматизованих систем управління та електронних сервісів. З одного боку, це спрощує та прискорює виконання різних операцій та бізнес-процесів, а, з іншого, це посилює вразливість підприємств до кіберзагроз, які постійно ускладнюються, набуваючи нових масштабів та форм.

Як свідчать аналітичні дослідження щороку фіксується збільшення випадків несанкціонованого доступу, вірусних атак та DDoS-нападів. У 2024 році глобальні економічні втрати від них оцінювалися у понад 9 трлн дол., а у 2025 році прогнозуються вже на рівні 10,5 трлн дол. (рисунок 1.1). При таких річних витратах світ витрачає приблизно 333 тис. дол. на хвилину на кіберзлочинність. При цьому значна кількість злочинів залишаються незареєстрованими. В останньому звіті ФБР за 2024 рік було нараховано 859,5 тис. скарг на інтернет-злочини та збитки на суму понад 16 млрд дол., що на 33% більше порівняно з попереднім роком. Це свідчить про швидке зростання кількості атак. На практиці, у 2023 році кібератака вражала підприємства або окремих осіб приблизно кожні 39 секунд. За даними APWG було зафіксовано понад 1,0 млн фішингових інцидентів. Кіберзлочинність зараз за масштабами конкурує з організованою злочинністю або навіть перевершує її. Gartner та WEF визначають її як головний глобальний ризик. ФБР зазначає, що навіть за активних зусиль щодо порушення роботи, таких як блокування LockBit, втрати все одно зростають. Trend Micro зафіксувала 161 млрд заблокованих загроз у 2023 році, що підкреслює обсяг та автоматизацію сучасних атак. Цей глобальний

сплеск є причиною того, що відстеження статистики є критично важливим [8, 9].

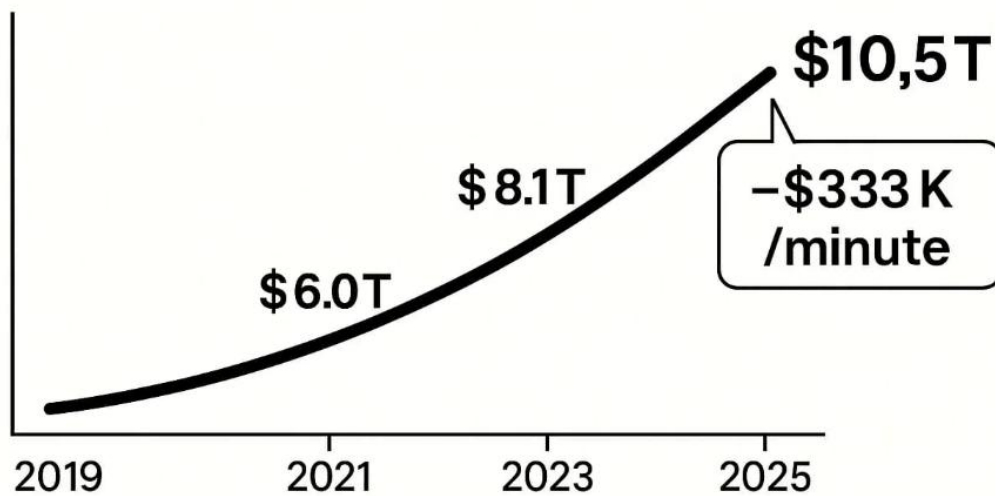


Рисунок 1.1 – Глобальні витрати та масштаби кіберзлочинності [9]

Кількість атак зросла на 25% у країнах НАТО у першому півріччі 2025 року порівняно з 2024 роком. Вартість хакерських атак до 2031 року може досягнути 12,2 трлн дол., щорічно зростаючи на 2,5 %. У дослідженні Cybersecurity Ventures зазначено, що «якби кіберзлочинність вимірювалася як країна, то вона була б третьою за величиною економікою світу після США та Китаю». Збитки, пов'язані з кіберзлочинністю, включають пошкодження та знищення даних, викрадення коштів, втрату продуктивності, крадіжку інтелектуальної власності, персональних та фінансових даних, розкрадання, шахрайство, порушення нормального ведення бізнесу після атаки, судово-медичні розслідування, відновлення та видалення зламаних даних і систем, репутаційну шкоду, судові витрати та, ймовірно, штрафи регуляторних органів, а також інші фактори [8, 9].

Серед найпопулярніших типів кіберзлочинних атак протягом 2024-2025 рр. слід відзначити такі (рисунок 1.2) [9]:

1) фішинг та спуфінг. Звіт ФБР за 2024 рік показує, що фішинг/спуфінг є категорією номер 1 серед зареєстрованих кіберзлочинів. Жертви отримували шахрайські електронні листи чи текстові повідомлення, що імітували довірені джерела. APWG зафіксувала 1003924 фішингових атак у першому кварталі 2025 року, що є найвищим показником з кінця 2023 року, причому 30,9% з них

були спрямовані на фінансовий/платіжний сектори. Приблизно третина зареєстрованих атак є фішинговими. Електронні листи, створені штучним інтелектом, текстові повідомлення, що розсилаються через фальшиві повідомлення, голосовий фішинг сприяють посиленню таких викликів;

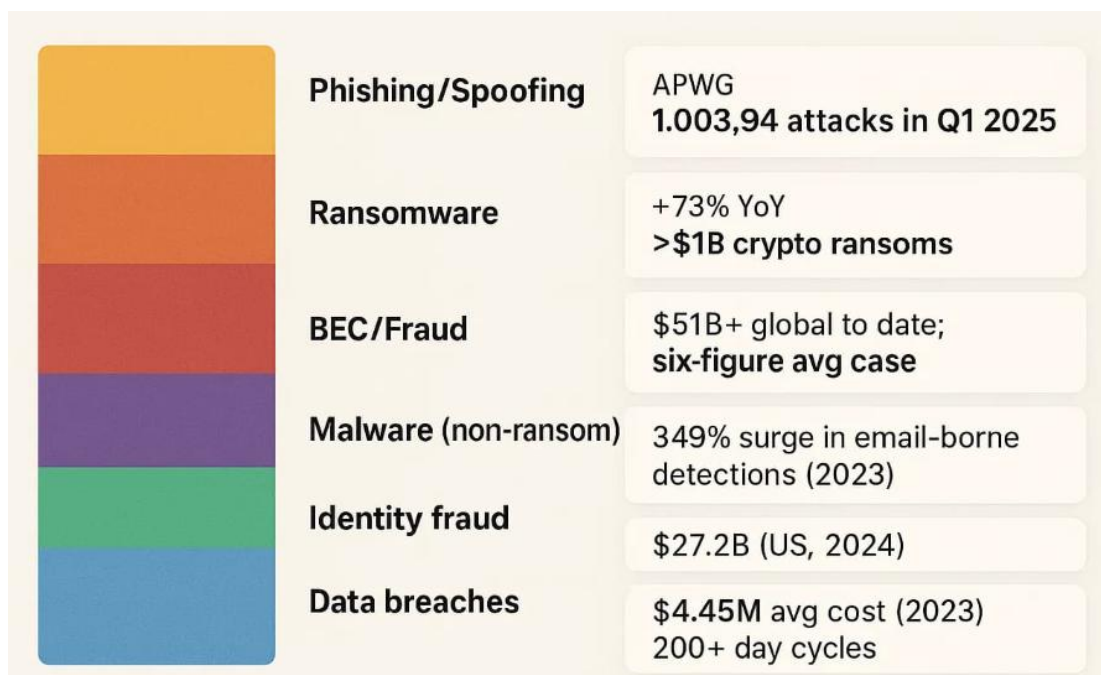


Рисунок 1.2 – Найпопулярніші типи кіберзлочинних атак протягом 2024-2025 рр. [9]

2) програми-вимагачі. Глобальні інциденти програм-вимагачів зросли на 73% у 2024 р. порівняно з 2023 р. Спеціальна група з питань програм-вимагачів зареєструвала 6670 атак програм-вимагачів у світі, жертвами яких стали 2800 у США. WatchGuard також повідомив про 95% зростання частоти атак програм-вимагачів у 2023 році. Зловмисники часто націлюються на великих суб'єктів, лікарні, комунальні підприємства, банки, вимагаючи величезні виплати. Програми-вимагачі зараз є найпоширенішою загрозою для критичної інфраструктури. Витрати в криптовалюті перевищили 1 млрд дол. у 2023 році за рахунок того, що шахрайські схеми було удосконалено;

3) компрометація ділової електронної пошти Business Email Compromise (BEC) та шахрайство. Зловмисники підробляють керівників або постачальників,

щоб обманом змусити фінансовий чи HR-персонал переказати гроші. Дані ФБР неодноразово показували, що втрати ВЕС оцінюються в десятки мільярдів. Аналіз показав, що глобальні втрати ВЕС на сьогоднішній день перевищують 51 млрд дол. Звіти IC3 у США виділяють ВЕС як найдорожчий тип шахрайства. Минулого року IC3 зазнала втрат у розмірі 6,5 млрд дол. через шахрайство з інвестиціями в криптовалюту. На практиці ВЕС та пов'язане з ним шахрайство в часто лідирують за кількістю та обсягом збитків;

4) шкідливе програмне забезпечення. Традиційні шкідливі програми такі як трояни, викрадачі інформації та боти залишаються дуже поширеними. Trend Micro повідомила про блокування 161 млрд інцидентів у 2023 році, що майже вдвічі більше, ніж п'ять років тому. У 2023 році спостерігалось 349 % зростання випадків застосування шкідливого програмного забезпечення в електронній пошті, тобто зловмисники все частіше надсилають шкідливі вкладення, а не просто посилення. Особливо поширилися банківські трояни та викрадачі облікових даних. Хоча багато атак шкідливого програмного забезпечення є поширеними, злочинці впроваджують й нові рішення;

5) крадіжка особистих даних / шахрайство. Масові витоки даних та фішинг сприяють шахрайству з використанням особистих даних, що коштує жертвам величезних витрат. Згідно з Javelin Strategy Allstate, споживачі США втратили 27,2 млрд дол. через шахрайство з використанням особистих даних у 2024 році, що на 19% більше, ніж у 2023 році, і набагато більше, якщо врахувати пов'язані з цим фінансові втрати. У світовому масштабі ця цифра ще вища, оскільки викрадені особисті дані призводять до захоплення облікових записів, кредитного шахрайства, створення штучних ідентифікаторів тощо. Програми-вимагачі та шкідливі програми часто створюють великі кеші особистих даних, тому злочини проти особистих даних є наслідком зростання кіберзлочинності;

6) витоки даних. Звіт Verizon DBIR за 2023 рік зафіксував 16312 інцидентів безпеки та 5199 підтверджених порушень у світі. Гучні порушення, такі як MOVEit 2023, додали тисячі додаткових жертв та десятки мільйонів викрадених записів. IBM виявила, що середні світові витрати на витік даних зараз становлять

4,45 млн дол., що вказує на 15-ти відсоткове зростання за три роки. Витоки в охороні здоров'я оцінюють у середньому у 10,93 млн дол., фінанси – 5,9 млн дол. Виявлення таких порушень займає більше часу, часто понад 200 днів, що призводить до збільшення витрат.

При цьому певні галузі постійно зазнають надмірних атак та збитків. По-перше, одним із секторів, що найбільше страждає від кібератак є охорона здоров'я. Організації охорони здоров'я зберігають величезні персональні дані та повинні працювати цілодобово, що робить їх основними цілями. Звіт IBM за 2023 рік показав, що середні витрати на порушення безпеки в охороні здоров'я склали 10,93 млн дол., що є найвищим показником серед усіх секторів. Лікарні, страхові компанії та клініки зіткнулися з поширеними блокуваннями медичних записів та крадіжками даних через програми-вимагачі. Загалом, атаки на охорону здоров'я продовжують і надалі зростати. По-друге, фінанси та банківська справа. Зловмисники використовують системи онлайн-банкінгу та фінансового персоналу. У 2023 році IBM оцінила збитки від порушення безпеки фінансового сектору в 5,9 млн дол., поступаючись лише охороні здоров'я. У цьому секторі постійно фішингують клієнтів для отримання кредитних даних на рахунки та вилучення кредитних карток співробітників. Наприклад, у першому кварталі 2025 року 30,9% усіх фішингових атак були спрямовані на платіжну та фінансову галузь. Банки та фінтех-компанії також стикаються з важкими атаками з використанням шкідливого програмного забезпечення та викраденням облікових даних. Крадіжка даних з банків та криптоплатформ часто викликає втрати на сотні мільйонів. Банківські послуги Trend Micro найбільше постраждали від програм-вимагачів у 2023 році [9]. По-третє, уряд та критична інфраструктура в результаті посилення геополітичної нестабільності. Урядові установи, комунальні послуги та інфраструктура в таких сферах, як енергетика, водопостачання, транспорт тощо, стикаються з частими кампаніями, від хактивізму до шпигунства, що спонсорується державою. CSIS повідомила про 138-те відсоткове зростання кібератак на урядові установи Індії у 2019-2023 рр. NCSC Великої Британії також відзначила трикратне зростання значних кібератак

у 2024 р. порівняно з 2023 р. Навіть якщо прямі втрати є непрямими, витрати на відновлення та проблеми національної безпеки роблять ці витрати значними.

Наслідки кібератак на різні галузі подано в таблиці 1.1.

Таблиця 1.1 – Наслідки кібератак у розрізі галузей економіки

Галузь	2023 р.	2024 р.	2025 р. (прогноз)	Основні наслідки
Фінансовий сектор	Масові атаки на банки та платіжні системи	Зростання атак на крипто-валютні біржі та мобільний банкінг	Збільшення атак на фінтех-сервіси, шахрайство з AI	Витік даних клієнтів, фінансові втрати, падіння довіри
Енергетика	Атаки на SCADA-системи	Збільшення атак на електромережі та нафтогазові компанії	Ціле-спрямовані атаки на «зелену енергетику» і LNG-термінали	Зупинка виробництва, перебої з постачанням
Транспорт і логістика	Атаки на авіаційні та морські системи	NotPetya паралізував Maersk (приклад для галузі)	Зростання атак на залізничні та автомобільні системи	Затримки перевезень, економічні втрати
Охорона здоров'я	WannaCry паралізував лікарні у Британії	Збільшення атак на медичні бази даних	Використання AI для атак на медичні IoT-пристрої	Загроза життю пацієнтів, витік медичних даних
Державний сектор	Зростання атак на урядові портали	Масові атаки на реєстри та виборчі системи	Збільшення атак на критичну інфраструктуру та оборонні системи	Порушення роботи державних послуг, шпигунство
ІТ та телекомунікації	Атаки на постачальницькі ланцюги (SolarWinds)	Збільшення атак на хмарні сервіси	Масові DDoS-атаки на операторів зв'язку	Перебої у зв'язку, компрометація даних

Отже, крім сфера охорони здоров'я, яка стає все більш вразливою через цифровізацію та використання IoT пристроїв, фінансового сектору та державних установ, які залишаються найбільш атакованими через високу цінність даних, критичної інфраструктури, зокрема енергетику та транспорт, атаки на яку мають глобальні економічні наслідки, піддаються впливу кіберзагроз ІТ та телекомунікації, що є ключовими точками входу для атак на інші галузі.

При цьому слід відзначити регіональну нерівномірність у готовності країн до реагування на серйозні кіберінциденти, спрямовані на критичну інфраструктуру, що було визначено на основі опитувань (рисунок 1.3). Лише 15 % респондентів у Європі та Північній Америці не впевнені у здатності країни реагувати на великі кіберінциденти, спрямовані на критичну інфраструктуру. В Африці ця частка зростає до 36 %, а в Латинській Америці – до 42 % [10].

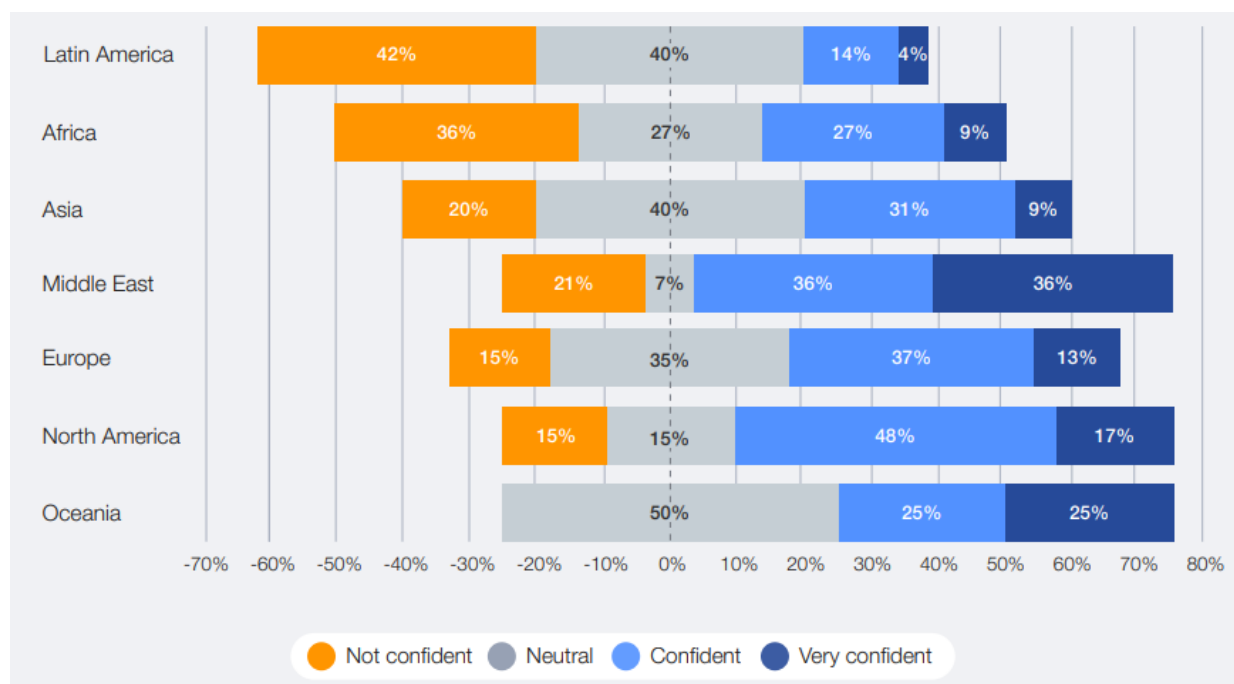


Рисунок 1.3 – Рівень готовності країн до реагування на серйозні кіберінциденти, спрямовані на критичну інфраструктуру (опитування) [10]

Вказують суб'єкти підприємництва і на кіберризики, які здійснюють найбільший вплив у контексті геополітичної напруженості (рисунок 1.4). Зокрема серед великих організацій 54 % визначили проблеми ланцюгів поставок

як найбільшу перешкоду для досягнення кіберстійкості. Зростаюча складність ланцюгів поставок у поєднанні з відсутністю прозорості та контролю за рівнями безпеки постачальників стала головним ризиком для кібербезпеки організацій. Ключові проблеми включають вразливості програмного забезпечення, внесені третіми сторонами, та поширення кібератак в екосистемі. Майже 60 % організацій заявляють, що геополітична напруженість вплинула на їхню стратегію кібербезпеки. Геополітичні потрясіння також вплинули на сприйняття ризиків, зокрема кожен третій керівник називає кібершпигунство та втрату конфіденційної інформації чи крадіжку інтелектуальної власності головною проблемою, тоді як 45% – стурбовані порушенням операцій та бізнес-процесів.

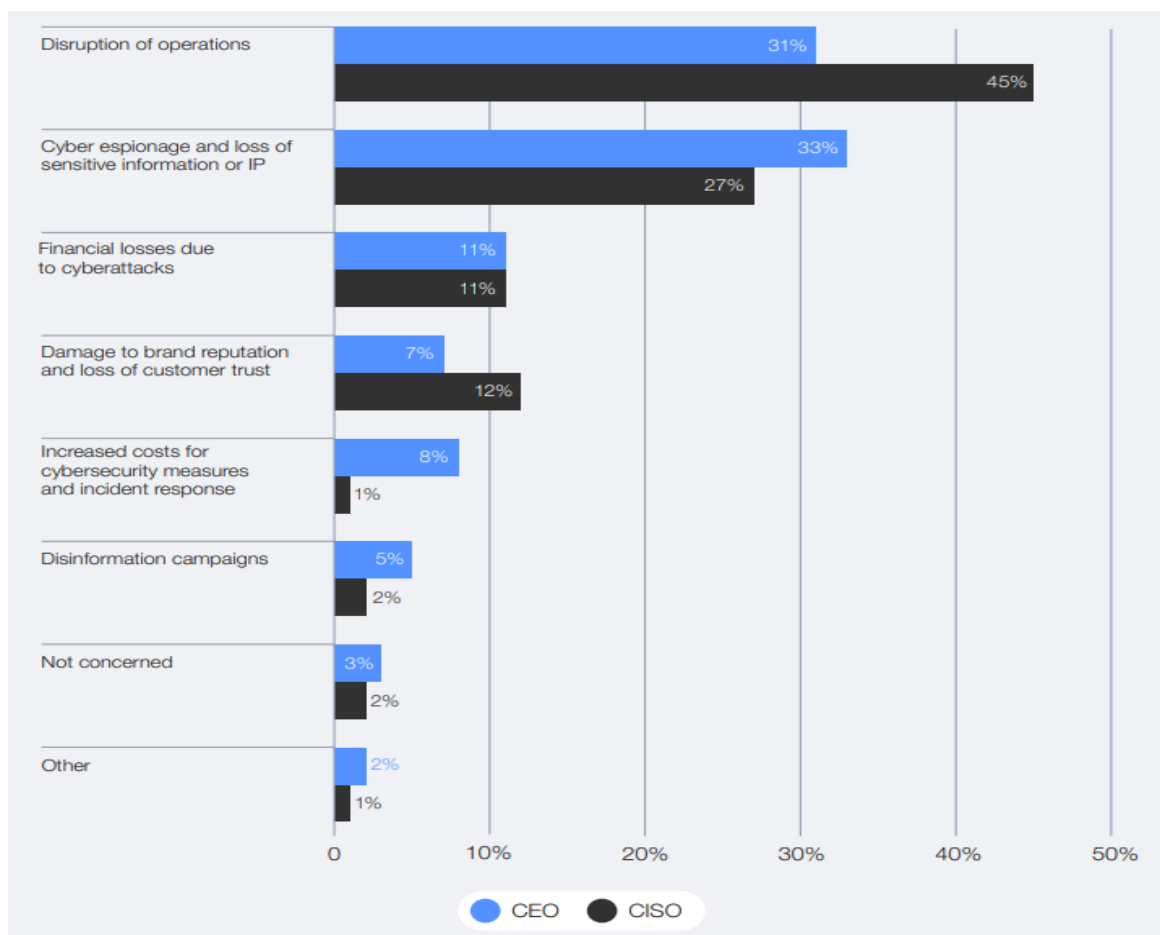


Рисунок 1.4 – Перелік кіберризиків, які здійснюють найбільший вплив на бізнес-суб’єкти в контексті геополітичної напруженості [10]

Зафіксовано і низку масштабних кібератак у світі та Україні, що

включають як класичні глобальні інциденти (WannaCry, NotPetya, Equifax), так і таргетовані атаки на критичну інфраструктуру України (державні реєстри, національна залізнична компанія, енергетичний сектор), серед яких:

- WannaCry (2017 р.) – глобальна атака з використанням шифрувальника, яка вразила понад 200 тис. комп'ютерів у 150 країнах. Постраждали лікарні у Великій Британії, компанії Renault, FedEx;

- NotPetya (2017 р.) – початково спрямована проти України, але швидко поширилася світом. Вразила Maersk, Merck, FedEx, спричинивши збитки понад 10 млрд дол.;

- Equifax (2017 р.) – витік даних 147 млн клієнтів у США через вразливість у веб-додатку. Збитки оцінюються у понад 4 млрд дол.;

- SolarWinds (2020 р.) – атака на постачальницький ланцюг, коли хакери зламали оновлення програмного забезпечення, що використовувалося урядовими та корпоративними структурами США;

- Colonial Pipeline (2021 р.) – атака на найбільший паливний трубопровід США, що призвела до зупинки постачання пального на кілька днів.

Цікавий підхід до розкриття історичної еволюції розвитку кіберзагроз подано в дослідженні [11] і відображено на рисунку 1.5.



Рисунок 1.5 – Історичний контекст найвідоміших кіберзлочинів [11]

Також, окрім NotPetya у 2017 р. Україна в роки війни продовжує потерпати від кібератак. Так, у 2024 р. відбулася масштабна кібератака на державні реєстри

України, яка паралізувала доступ до даних, у 2025 р. – атака на онлайн-системи Укрзалізниці, що призвела до тимчасової недоступності сервісу купівлі квитків, хоча рух поїздів не зупинився. Протягом 2022-2024 рр. було зафіксовано понад 4,8 тис. кіберінцидентів, спрямованих лише на критичну інфраструктуру. Як свідчить рисунок 1.6 значна кількість інцидентів у 2022 році була пов’язана з атаками на уряд та місцеві органами влади, сектор безпеки та оборони.

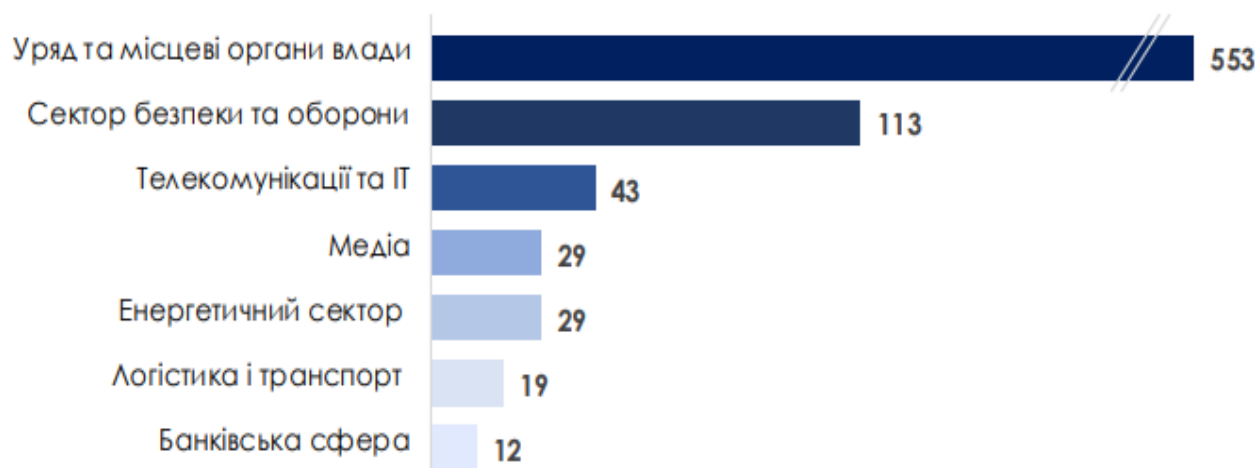


Рисунок 1.6 – Кількість інцидентів у 2022 році [11]

Отже, якщо світові атаки демонструють масштаби збитків та глобальний вплив (мільярди доларів, сотні тисяч постраждалих систем), то українські атаки часто мають геополітичний характер і спрямовані на критичну інфраструктуру. Нині в умовах розгортання повномасштабної війни на території держави Україна є однією з найбільш атакованих країн світу, що підтверджує необхідність розвитку цифрової стійкості та кібергігієни на рівні бізнес-суб’єктів.

Слід зазначити, що в умовах прискореного науково-технічного прогресу і розвитку технологій кіберзагроза та кібератаки значно еволюціонували від простих вірусів, таких як віруси й черв’яки, до багатовекторних кампаній, що поєднують технічні, організаційні та психологічні методи. Розвиток хмар, мобільності, IoT та промислових систем (OT/ICS) розширив поверхню атаки, а економізація злочину (кіберзлочин як сервіс) зробила атаки масштабнішими та доступнішими. У таких умовах для підприємств, особливо критичної

інфраструктури, важливо відстежувати ці зміни, щоб вчасно адаптуватися.

Ключовими етапи розвитку загроз є такі (рис. 1.7) [12-18]:

1) початковий етап (1980-2000 рр.):

- види атак – експериментальні віруси, черв'яки, дефейсинг сайтів;
- мотиви атак – цікавість, репутація хакера, локальні збитки;
- тип захисту – базові антивіруси, перші міжмережеві екрани;

	<i>початковий етап (1980-2000 рр.)</i>	<i>етап комерціалізації (1980-2000 рр.)</i>	<i>етап індустріалізації (2010-2017 рр.)</i>	<i>етап ransomware та гібридних атак (2017 р і до сьогодні)</i>
<i>Види атак</i>	експериментальні віруси, черв'яки, дефейсинг сайтів	фішинг, банківські трояни, ботнети	APT-кампанії, експлойти нульового дня, кібероперації проти організацій та держав	шифрувальники, подвійне вимагання (зашифрувати + злити дані), атаки на OT/ICS, постачальницькі ланцюги
<i>Мотиви атак</i>	цікавість, репутація хакера, локальні збитки	фінансова вигода, крадіжка даних і грошей	шпигунство, саботаж, стратегічний вплив	великі викупи, дестабілізація критичної інфраструктури
<i>Тип захисту</i>	базові антивіруси, перші міжмережеві екрани	IDS/IPS, сегментація мереж, перші стандарти ISMS	SOC, Threat Intelligence, багаторівневі контролю	Zero Trust, EDR/XDR, кіберстійкість, оркестрація реагування

Рисунок 1.7 – Ключові етапи розвитку кіберзагроз [12-18]

2) етап комерціалізації (1980-2000 рр.):

- види атак – фішинг, банківські трояни, ботнети;
- мотиви атак – фінансова вигода, крадіжка даних і грошей;
- тип захисту – IDS/IPS, сегментація мереж, перші стандарти ISMS;

3) етап індустріалізації (2010-2017 рр.):

- види атак – APT-кампанії, експлойти нульового дня, кібероперації проти організацій та держав;
- мотиви атак – шпигунство, саботаж, стратегічний вплив;
- тип захисту – SOC, Threat Intelligence, багаторівневі контролю;

4) етап ransomware та гібридних атак (2017 р і до сьогодні):

- види атак – шифрувальники, подвійне вимагання (зашифрувати та злити

дані), атаки на OT/ICS, постачальницькі ланцюги;

- мотиви атак – великі викупи, дестабілізація критичної інфраструктури;
- тип захисту – Zero Trust, EDR/XDR, кіберстійкість, оркестрація реагування.

Таке прискорення еволюції загроз зумовлено впливом такими факторами:

по-перше, розвиток хмарних технологій та мобільність і, як результат, розмиті периметри, складність контролю доступу. Це ставить перед підприємствами виклики ідентифікації, зокрема багатофакторної, керування привілеями (PAM);

по-друге, IoT та OT/ICS, нові вразливі протоколи й пристрої, довгий життєвий цикл обладнання. Це ставить перед підприємствами виклики сегментації OT, моніторингу аномалій, патч-менеджменту у промислових мережах;

по-третє, сервіси кіберзлочину (Crime-as-a-Service) і зниження «порогу входу» для атакувальників. Це ставить перед підприємствами виклики проактивної розвідки загроз, блокування інфраструктури злочинців;

по-четверте, людський фактор і соціальна інженерія, обхід технічних бар'єрів через користувача. Це ставить перед підприємствами виклики навчання, симуляції фішингу, політики мінімальних прав.

Якщо говорити про український ринок кібербезпеки, то для нього сьогодні характерні як сильні та слабкі сторони, так і можливості та загрози зовнішнього середовища, що відображено на рисунку 1.8.

Під впливом еволюції кіберзагроз змінюються і методи та форми захисту: від периметральної оборони до багаторівневого контролю (фаєрволи доповнюються сегментацією, IDS/IPS, проксі, WAF); від реактивності до проактивності (Threat Hunting, використання TI-даних, червоні команди); від довірчої моделі до підходу Zero Trust (перевірка кожної сесії та кожної дії, мікросегментація): від простого виявлення до виявлення та реагування (EDR/XDR, SOAR, автоматизоване реагування); від безпеки до кіберстійкості (планування безперервності, резервування, відновлення, тренування).

Сильні сторони ринку	Слабкі сторони ринку
Унікальний досвід протидії повномасштабній кібервійні: - масові кібератаки на мережі критичної інфраструктури, телекомунікації та фінансові установи з початку російського вторгнення призвели до підвищення обізнаності в загрозах; - унікальний досвід України в реальній кібервійні дає цінну інформацію, якою слід ділитися з іноземними партнерами	Відсутність систематичного фінансування: - несприятливий інвестиційний клімат ускладнюється воєнними ризиками та низькою обізнаністю у сфері кібербезпеки
Зміни в цифровому ландшафті: - тривала тенденція до цифровізації виконання функцій державного сектору, а також сервісів та бізнес-процесів приватного сектору, що призводить до постійної генерації попиту на продукти та послуги в сфері кібербезпеки	Фрагментація пропозиції на ринку: - нові стартапи у сфері кібербезпеки частіше уникають співпраці з колегами та не мають тенденції до об'єднання в універсальні кластери
Міжнародна матеріально-технічна допомога: - з початком повномасштабного вторгнення уряди іноземних держав підвищили свою зацікавленість у підтримці функціонування української кібербезпеки	Недовершене правове регулювання галузі: - імплементація кращих практик в систему національного законодавства в сфері кібербезпеки та захисту інформації залишається точковою, що також є стримуючим фактором розвитку загальної культури кібербезпеки як приватного, так і державного секторів; - вимоги кіберзахисту щодо державного сектору та критичної інфраструктури, які є основними споживачами продуктів та послуг, не повністю відповідають кращим практикам, а імплементація вимог є фрагментарною
Можливості розвитку ринку	Ризики для ринку
Диверсифікація ринку: - список сьогоденних викликів та інструментів реалізації кібербезпеки, як у світі, так і в Україні, не є остаточною і розширюється з розвитком цифрових технологій; - поступово в поняття "кібербезпека" інтегруються інформаційна і нарративна безпеки та OSINT-практики, що збільшує сектор діяльності	Нестача кадрів: - зручність роботи в аутсорсі на іноземні компанії, реалії воєнного часу та довготривалий відтік талантів за кордон – ключові причини нестачі кваліфікованих співробітників у вітчизняних компаніях; - актуальною залишається проблема підготовки спеціалістів. Якість вищої освіти часто не відповідає потребам та викликам сучасності
Перспектива збільшення попиту: - прогрес в цифровізації є серед основних викликів та мотивом зміни підходів до управління безпекою і заходів захисту; - євроінтеграційний процес передбачає поступове впровадження національних і галузевих практик безпеки, норм відповідності для цифрових продуктів і послуг, що призведе до широкого впровадження організаційно-технічних заходів безпеки	Небезпека кібератак з-за кордону: - на Україну в 2023 р. прийшла найбільша частина спонсорованих державами кібератак у Європі; - у час війни з Росією та політичного конфлікту з її союзниками (Іран та КНДР) завжди можливе збільшення кількості та різноманіття кібератак ззовні, особливо на критично важливі галузі економіки
Умови для впровадження нових рішень: - кіберзагрози воєнного часу та недовершена архітектура кібербезпеки України роблять місцеві ринки вдалими для тестування експериментальних рішень у цій сфері; - постачальники послуг з кібербезпеки мають можливість навчити свої продукти на унікальних даних та перевірити їх на стійкість перед найсучаснішими викликами	Залежність систем від забезпечення з-за кордону: - робота цифрових систем в Україні можлива завдяки присутності на ринку закордонних виробників та постачальників; - Український ринок має труднощі у виробництві hardware, що ставить його у вразливе положення

Рисунок 1.8 – SWOT-аналіз українського ринку кібербезпеки [11]

Важливо приділити увагу і класифікації кіберзагроз підприємств, які можна систематизувати за джерелом походження, способом реалізації та наслідками для бізнес-процесів [12-18]. Основні групи – це зовнішні атаки (хакери, державні актори), внутрішні загрози (помилки чи зловживання персоналу), технічні збої та комплексні гібридні атаки.

За джерелом походження можна виділити (таблиця 1.2) [12-18]:

- зовнішні загрози (атаки хакерських угруповань, державних структур, конкурентів);
- внутрішні загрози (недбалість співробітників, умисні дії інсайдерів, витік даних через персонал).

Таблиця 1.2 – Класифікація кіберзагроз підприємств [12-18]

Критерій	Тип загрози	Приклади
За джерелом походження	Зовнішні	Хакерські атаки, державні кібератаки, конкуренти
	Внутрішні	Недбалість персоналу, інсайдерські дії, витік даних через співробітників
За способом реалізації	Технічні	DDoS-атаки, віруси, трояни, атаки на SCADA-системи
	Соціальна інженерія	Фішинг, спуфінг, викрадення паролів через маніпуляції
	Фізичні	Несанкціонований доступ до серверів, викрадення носіїв інформації
За наслідками	Порушення конфіденційності	Витік персональних чи комерційних даних
	Порушення цілісності	Зміна або підробка даних (графіки руху, фінансові документи)
	Порушення доступності	Блокування роботи систем, зупинка виробничих процесів
	Комплексні	Масштабний параліч бізнес-процесів, фінансові втрати, репутаційні ризики

За способом реалізації можна виділити:

- технічні атаки (DDoS-атаки (перевантаження системи), віруси, трояни,

шкідливе програмне забезпечення, атаки на SCADA-системи та автоматизовані системи управління);

- соціальна інженерія (фішинг, спуфінг, маніпуляції з користувачами, викрадення паролів через психологічний тиск);

- фізичні загрози (несанкціонований доступ до серверів чи обладнання, викрадення носіїв інформації).

За об'єктом впливу можна виділити:

- на інформацію (крадіжка, модифікація, знищення даних);

- на інфраструктуру (атаки на сервери, мережі, системи управління критичною інфраструктурою);

- на користувачів (шахрайство, крадіжка особистих даних, фінансові махінації).

За наслідками можна виділити:

- порушення конфіденційності (витік комерційних або персональних даних);

- порушення цілісності (зміна або підробка даних (наприклад, графіків руху чи фінансових документів);

- порушення доступності (блокування роботи систем, зупинка виробничих процесів);

- комплексні наслідки (параліч бізнес-процесів, фінансові втрати, репутаційні ризики).

Якщо йде мова про підприємства критичної інфраструктури, то слід виділити особливості таких атак:

- по-перше, енергетика, транспорт, зв'язок, водопостачання – найбільш вразливі сфери, адже їхня робота забезпечує життєдіяльність держави;

- по-друге, гібридні атаки поєднують кіберзасоби з фізичними діями (наприклад, кібератака на диспетчерський центр та диверсія на об'єкті);

- по-третє, цілеспрямовані атаки часто мають політичний або військовий характер, особливо в умовах війни.

1.2 Еволюція поняття цифрової стійкості підприємств

У сучасних умовах цифрової трансформації транспортна галузь стає однією з ключових сфер, що залежить від стабільності та захищеності інформаційних систем. Підприємства залізничного транспорту належать до категорії критичної інфраструктури, адже їхня діяльність забезпечує безперервність логістичних процесів, функціонування промисловості та міжнародних торговельних зв'язків.

Загострення кіберзагроз, що проявляється у зростанні кількості атак на інформаційні системи, спробах несанкціонованого доступу до даних та блокуванні транспортних сервісів, створює реальні ризики для економічної стабільності підприємств. Будь-який інцидент у сфері цифрової безпеки може призвести до зупинки перевезень, зриву контрактів, фінансових втрат та втрати довіри клієнтів і партнерів.

Забезпечення цифрової безпеки є доцільним з декількох причин:

- економічна ефективність – інвестиції у безпеку значно менші за потенційні збитки від кібератак, кібератаки можуть призвести до зупинки перевезень, втрати контрактів, штрафів, захищені системи працюють стабільніше, менше простоїв;

- організаційна стабільність – захищені системи гарантують безперервність роботи та зменшують ризики простоїв, захист даних клієнтів і партнерів формує довіру та лояльність, відповідність стандартам ISO/IEC 27001, GDPR та іншим вимогам міжнародних ринків;

- стратегічна конкурентоспроможність – підприємства, що впроваджують сучасні стандарти безпеки, отримують перевагу на ринку та можливість інтеграції у міжнародні транспортні коридори, оскільки клієнти обирають компанії, які гарантують безпеку даних і сервісів;

- соціальна відповідальність – цифрова безпека сприяє захисту інтересів клієнтів, партнерів та держави.

Таким чином, цифрова безпека виступає не лише технічним інструментом, а й стратегічним чинником розвитку підприємств залізничного транспорту. Її забезпечення є обов'язковою умовою для підвищення ефективності бізнес-процесів, формування довіри клієнтів та партнерів, а також для стійкого розвитку у глобалізованому та конкурентному середовищі.

Загалом цифрову безпеку підприємства можна розглядати як комплекс організаційних, технічних та правових заходів, спрямованих на захист інформаційних ресурсів, бізнес-процесів та цифрових сервісів від внутрішніх і зовнішніх загроз, що забезпечує збереження конфіденційності даних, цілісність і достовірність інформації, доступність цифрових систем для користувачів, стійкість бізнесу до кіберризиків. Таке поняття включає багато складових.

Основними складовими цифрової безпеки підприємства є наступні [19-26].

1 Інформаційна безпека: захист баз даних, комерційної та фінансової інформації; використання шифрування, резервного копіювання, багаторівневого доступу.

2 Кібербезпека: захист корпоративних мереж, серверів та робочих станцій від атак; системи моніторингу, антивірусні рішення, міжмережеві екрани, реагування на інциденти.

3 Телекомунікаційна безпека: захист каналів зв'язку (інтернет, мобільні мережі, корпоративні VPN); використання захищених протоколів та систем виявлення вторгнень.

4 Технічна безпека обладнання: контроль доступу до комп'ютерів, серверів, IoT-пристроїв; захист від фізичного втручання та несанкціонованого використання.

5 Організаційна безпека: політики та регламенти цифрової безпеки; навчання персоналу правилам кібергігієни; відповідальність керівництва за дотримання стандартів.

6 Правова складова: дотримання законодавства у сфері захисту даних (GDPR, ISO/IEC 27001 тощо); юридичні механізми захисту комерційної та інтелектуальної власності.

7 Бізнес-орієнтована складова: використання цифрової безпеки як конкурентної переваги; формування довіри клієнтів і партнерів через гарантії захисту даних тощо.

Щодо цифрової стійкості, то дане поняття також знайшло відображення в наукових працях. Так, стійкість трактується як комплексне явище, що охоплює здатність підприємства зберігати конкурентні переваги, ефективно використовувати ресурси, впроваджувати інновації та дотримуватися принципів соціальної відповідальності. Ключовим фактором виступає швидка й результативна адаптація до змін, яка визначає рівень протидії зовнішнім викликам та забезпечує утримання стратегічних позицій [27]. У праці [28] зазначено, що в сучасних економічних умовах дослідження стійкості підприємств потребує комплексного аналізу, що враховує різні наукові концепції. Здатність компанії до довготривалого функціонування та адаптації в мінливому середовищі визначається не лише фінансовими результатами, а й ефективністю управлінських рішень, гнучкістю у взаємодії з інституційними структурами та рівнем технологічного розвитку. Кожен із підходів розкриває окремий вимір стійкості, проте, як зазначає автор, саме їх поєднання створює основу для тривалої стабільності та збереження конкурентних позицій. Вченим виділено фінансову, операційну, ринкову, організаційну, соціальну та екологічну стійкість. На рисунку 1.9 наведено даний перелік видів стійкості та розкрито визначення кожного з них. Однак, безпосередньо цифрову стійкість як окрему категорію автором не розглянуто. Хоча зазначено, що цифрова економіка, поряд із новими можливостями, формує для підприємств і нові виклики, здатних поставити під сумнів їхню стійкість. Також зазначено, що технологічна залежність, посилення кіберзагроз та потреба швидкої адаптації до мінливих ринкових умов вимагають розроблення стратегічних механізмів управління цифровими ризиками. Високий рівень цифрової зрілості забезпечує компаніям не лише ефективну реакцію на ці виклики, а й використання цифровізації як інструменту для посилення ринкових позицій, диверсифікації бізнес-моделей та підвищення результативності операційних процесів [28].



Рисунок 1.9 – Види стійкості підприємства [28]

В іншому дослідженні відзначено, що стійкість підприємств у цифровій економіці визначається як здатність господарюючих суб'єктів підтримувати ефективність діяльності, забезпечувати безперервність бізнес-процесів та адаптуватися до мінливого зовнішнього середовища завдяки впровадженню цифрових технологій, інноваційних управлінських рішень і стратегічному використанню даних. При цьому вона охоплює фінансовий, операційний, ринковий, організаційний, соціальний та екологічний виміри, формуючи багатогранну систему довготривалої конкурентоспроможності та розвитку підприємства. У сучасних умовах ключовими чинниками стійкості бізнесу стають цифрова зрілість, автоматизація процесів, кіберстійкість та ефективне управління інформаційними ресурсами, що визначають його позиції в умовах

глобальної цифрової трансформації [29].

Під стратегічною стійкістю в умовах цифрової економіки автори статті [30] пропонують розуміти здатність підприємства гнучко трансформувати стратегії, бізнес-процеси та організаційну структуру відповідно до динамічного цифрового середовища, забезпечуючи стабільну діяльність, сталий розвиток і конкурентоспроможність. Така стійкість проявляється у здатності компанії інтегрувати сучасні технології, оперативно реагувати на зміни попиту, технологічних тенденцій, економічних та регуляторних умов, а також у гарантуванні кібербезпеки, ефективному управлінні ресурсами й підтриманні довгострокового розвитку за умов нестабільності та непередбачуваних викликів.

У дослідженні [31] розглядається цифрова стійкість як риса фахівця. Авторами зазначено, що цифрова стійкість є складним і багатовимірним явищем, що потребує міждисциплінарного підходу та постійного оновлення знань і навичок. Вона має вирішальне значення для гарантування безперервності національної безпеки в умовах стрімкого розвитку технологій та появи нових форм загроз. У сучасних реаліях цифрова стійкість стає невід'ємним елементом професійної підготовки, особливо з огляду на виклики кіберзагроз та гібридної війни. Здатність ефективно протидіяти цим викликам є ключовою умовою збереження безпеки держави. Формування цифрової стійкості потребує тісної взаємодії між приватним технологічним сектором, що відповідає за створення інноваційних рішень, та державними інституціями, які ухвалюють стратегічні політичні рішення. Вивчення стратегічних комунікацій у процесі освіти допомагає майбутнім фахівцям усвідомити природу інформаційних загроз – пропаганди, дезінформації та маніпуляцій, що активно поширюються у кіберпросторі, та набути навичок їхнього виявлення й нейтралізації.

Доволі часто поняття цифрової безпеки та стійкості пов'язують з інформаційною або кібербезпекою. Так, у дослідженні [11] визначено кібербезпеку як процес, спрямований на забезпечення конфіденційності, цілісності та доступності інформаційних систем, мереж, програм і даних, що включає заходи з управління ідентифікацію, виявленням, захистом, реагуванням

та відновленням. Забезпечення такої безпеки в значній мірі залежить від якості кіберрішень, тобто продуктів або послуг, адаптованих до унікальних вимог організацій з урахуванням їх ландшафту ризиків і стратегій безпеки (рис. 1.10).



Рисунок 1.10 – Кіберрішення як базис забезпечення кібербезпеки [11]

Отже, порівнюючи цифрову безпеку та цифрову стійкість можна виділити як схожі, так і відмінні риси (таблиця 1.3).

Таблиця 1.3 – Порівняльна характеристика цифрової безпеки та стійкості

Критерій	Цифрова безпека	Цифрова стійкість
Сутність	Система заходів для захисту даних, мереж та систем від кіберзагроз	Здатність підприємства адаптуватися, протидіяти та швидко відновлюватися після атак
Основна мета	Запобігання інцидентам та мінімізація ризиків	Забезпечення безперервності бізнес-процесів навіть після інциденту
Фокус	Технічні та організаційні заходи захисту	Поєднання захисту, відновлення та адаптації
Інструменти	Антивіруси, фаєрволи, системи контролю доступу, шифрування	Планування безперервності, резервні системи, кризові протоколи, адаптивні політики
Часовий вимір	Орієнтація на теперішнє: запобігти атаці зараз	Орієнтація на майбутнє: як швидко відновитися після атаки
Роль персоналу	Виконання правил безпеки, дотримання політик	Активна участь у тренінгах, кризових симуляціях, формування культури стійкості
Результат	Захищеність даних і систем	Стабільність бізнесу та довгострокова конкурентоспроможність

Отже, цифрова стійкість підприємства – це здатність підприємства адаптуватися до цифрових загроз, протидіяти їм та швидко відновлюватися після інцидентів, зберігаючи безперервність ключових процесів. Це є доволі комплексною категорією, що включає такі складові (таблиця 1.4):

Таблиця 1.4 – Компоненти цифрової стійкості

Компонент	Сутність	Приклади заходів
Технічна стійкість	Захист інфраструктури та даних	Резервне копіювання, мікросегментація мереж, EDR/XDR, SIEM, шифрування, Zero Trust
Організаційна стійкість	Політики та процеси управління	План реагування на інциденти, Business Continuity Plan, кризові комунікації, аудит безпеки
Людська стійкість	Культура та поведінка персоналу	Навчання кібергігієні, симуляції фішингових атак, мотивація співробітників, контроль доступу
Правова та регуляторна стійкість	Відповідність законам і стандартам	Дотримання ISO/IEC 27001, GDPR, національних законів України, галузевих вимог
Економічна стійкість	Управління фінансовими ризиками	Інвестиції у безпеку, оцінка вартості простоїв, планування бюджету, страхування кіберризиків
Адаптивність та інноваційність	Гнучкість та розвиток	Використання AI для виявлення загроз, блокчейн для захисту даних, оновлення політик, аналіз інцидентів

по-перше, технічна стійкість: резервне копіювання та відновлення даних (Backup & Recovery); мікросегментація мереж та багаторівневий захист; використання сучасних технологій (EDR/XDR, SIEM, SOAR, Zero Trust); захист хмарних сервісів та IoT-пристроїв;

по-друге, організаційна стійкість: політики реагування на інциденти (Incident Response Plans); планування безперервності бізнесу (Business Continuity

Plan); кризові комунікації та координація між відділами; аудит та регулярне тестування систем безпеки;

по-третє, людська стійкість: навчання персоналу кібергігієні; симуляції атак (наприклад, фішингові тренінги); формування культури відповідальності за безпеку; зниження ризику інсайдерських загроз через мотивацію та контроль;

по-четверте, правова та регуляторна стійкість: відповідність міжнародним стандартам (ISO/IEC 27001, NIST, GDPR); дотримання національних законів (Закон України «Про кібербезпеку», «Про захист персональних даних»); врахування галузевих вимог (фінанси, енергетика, транспорт);

по-п'яте, економічна стійкість: інвестиції у безпеку як стратегічний актив; оцінка фінансових ризиків від кібератак; планування бюджету на превентивні заходи; врахування вартості простоїв та репутаційних втрат;

по-шосте, адаптивність та інноваційність: використання штучного інтелекту для виявлення загроз; інтеграція блокчейну для захисту даних; гнучке оновлення політик безпеки відповідно до нових викликів; постійне вдосконалення системи на основі аналізу інцидентів.

Цифрова стійкість складається з технічних, організаційних, людських, правових, економічних та інноваційних компонентів і саме їх взаємодія формує комплексну систему, яка дозволяє підприємству не лише захищатися, а й виживати та розвиватися в умовах постійних цифрових загроз.

1.3 Формування концепції забезпечення цифрової стійкості підприємств

Розроблення концепції забезпечення цифрової стійкості підприємств передбачає створення системного підходу, що поєднує технологічні інновації, кібербезпеку, гнучке управління та стратегічне використання даних. Така концепція дозволяє підприємствам не лише протистояти сучасним викликам цифрової економіки, а й використовувати цифровізацію як основу для сталого

розвитку та посилення конкурентних позицій. Це вказує на той факт, що цифрова стійкість є не просто технічним інструментом, а стратегічним фактором конкурентоспроможності підприємства, забезпечуючи стабільність бізнес-процесів, формуючи довіру клієнтів і партнерів, відкриваючи доступ до міжнародних ринків та підвищуючи репутацію компанії (таблиця 1.5).

Таблиця 1.5 – Роль цифрової безпеки у формуванні конкурентоспроможності підприємств

Роль цифрової безпеки	Конкретні конкурентні переваги	Приклади застосування
Захист даних та інтелектуальної власності	Збереження унікальних технологій, комерційної інформації, клієнтських баз	Шифрування контрактів, захист баз даних
Формування довіри клієнтів і партнерів	Підвищення лояльності, залучення нових клієнтів	Сертифікація ISO/IEC 27001, гарантії безпеки онлайн-сервісів
Безперервність бізнес-процесів	Мінімізація простоїв, стабільність роботи	Системи резервного копіювання, моніторинг інцидентів
Відповідність міжнародним стандартам	Доступ до глобальних ринків, інтеграція у міжнародні ланцюги постачання	GDPR-сумісність, аудит безпеки
Імідж сучасного підприємства	Підвищення репутації, позиціонування як інноваційного лідера	Використання AI-систем для аналізу загроз
Економічна ефективність	Зниження витрат на ліквідацію наслідків атак	Превентивні заходи дешевші за відновлення після інцидентів

Представлена таблиця демонструє, що цифрова стійкість є багатовимірним інструментом, який одночасно виконує функцію захисту та створює стратегічні переваги для бізнесу. Вона забезпечує збереження даних і технологій, формує довіру клієнтів та партнерів, гарантує безперервність бізнес-процесів і відкриває доступ до міжнародних ринків завдяки відповідності стандартам. Таким чином,

цифрова стійкість перетворюється з витратної статті на інвестицію у розвиток підприємства, що підвищує його репутацію, економічну ефективність та стійкість у конкурентному середовищі.

Можна говорити про те, що цифрова стійкість об'єднує кібербезпеку, управління ризиками та бізнес-стійкість. З огляду на це серед ключових принципів забезпечення цифрової стійкості можна виділити такі (рисунок 1.11):

- системність – інтеграція цифрових технологій у всі бізнес-процеси;
- адаптивність – здатність швидко реагувати на зміни ринку та технологій;
- безперервність – гарантування стабільності бізнес-процесів навіть в умовах криз;
- інноваційність – постійне впровадження нових технологічних рішень;
- безпечність – пріоритет кіберзахисту та управління ризиками;
- відповідальність – врахування соціальних та екологічних аспектів цифрової трансформації.

Основними напрямми забезпечення цифрової стійкості підприємства можна виділити наступні.

Технологічний – впровадження сучасних ІТ-рішень, автоматизація та цифровізація процесів.

Організаційний – формування гнучкої структури управління та корпоративної культури цифрової стійкості.

Фінансовий – інвестування в цифрові інновації та кібербезпеку.

Соціальний – розвиток цифрових компетенцій персоналу, навчання та підвищення кваліфікації.

Екологічний та етичний – використання цифрових технологій для сталого розвитку та прозорості бізнесу.

Доцільно в рамках кожного напрямку виділити завдання та інструменти.

У рамках технологічного напрямку можна виділити такі головні завдання як впровадження сучасних ІТ-рішень та автоматизація бізнес-процесів, забезпечення кіберзахисту та безперервності роботи систем, інтеграція інноваційних технологій (AI, IoT, блокчейн). Інструменти технологічного

напрямку є: ERP та CRM-системи; хмарні платформи та сервіси; системи кіберзахисту (SIEM, SOC, IDS/IPS); Big Data та аналітичні платформи.



Рисунок 1.11 – Концепція забезпечення цифрової стійкості підприємства

Завданнями організаційного забезпечення цифрової стійкості є:

- формування гнучкої організаційної структури;
- розроблення політик цифрової трансформації та кібербезпеки;
- створення корпоративної культури цифрової стійкості.

Для реалізації перелічених завдань доцільно застосувати такі інструменти: регламенти та стандарти управління ризиками; системи управління якістю (ISO 27001, ISO 22301); внутрішні комунікаційні платформи; Agile та DevOps-практики тощо.

Завданнями фінансового забезпечення цифрової стійкості є:

- інвестування у цифрові технології та інновації;
- формування бюджету на кібербезпеку;
- оцінка економічної ефективності цифрових рішень.

Для реалізації перелічених завдань доцільно застосувати такі інструменти: фінансове моделювання та прогнозування; системи управління витратами та інвестиціями; ROI-аналіз цифрових проєктів; інструменти фінансової аналітики (BI-системи) тощо.

Завданнями соціального забезпечення цифрової стійкості є:

- підвищення цифрової грамотності та компетенцій персоналу;
- формування навичок роботи з новими технологіями;
- забезпечення культури кібербезпеки серед співробітників.

Для реалізації перелічених завдань доцільно застосувати такі інструменти: програми навчання та сертифікації (Coursera, Udemu, корпоративні тренінги); внутрішні освітні платформи; симуляції та тренінги з кіберзахисту; HR-аналітика для оцінки цифрових навичок тощо.

Завданнями екологічного та етичного забезпечення цифрової стійкості є:

- використання цифрових технологій для сталого розвитку;
- забезпечення прозорості бізнес-процесів;
- дотримання етичних норм у використанні даних.

Для реалізації перелічених завдань доцільно застосувати такі інструменти: ESG-звітування та цифрові системи моніторингу; інструменти контролю викидів

та енергоефективності; політики захисту персональних даних (GDPR); блокчейн для прозорості ланцюгів постачання тощо.

Таким чином, завдання та інструменти організаційного, фінансового, соціального, екологічного та етичного забезпечення взаємодоповнюють одне одного, формуючи комплексну систему цифрової стійкості підприємства в умовах постійних загроз. Це перетворює цифрову стійкість на стратегічний актив, що забезпечує конкурентоспроможність і довгострокову стабільність.

Висновки до розділу 1

Виявлено, що в сучасних умовах цифрової трансформації суб'єкти економічної діяльності дедалі більше залежать від інформаційних технологій, автоматизованих систем управління та електронних сервісів. З одного боку, це спрощує та прискорює виконання різних операцій та бізнес-процесів, а, з іншого, це посилює вразливість підприємств до кіберзагроз, які постійно ускладнюються, набуваючи нових масштабів та форм.

Досліджено аналітичні дослідження щодо кіберзагроз як на світовому, так і національному рівнях, і встановлено, що щороку фіксується збільшення випадків несанкціонованого доступу, вірусних атак та DDoS-нападів. У 2024 році глобальні економічні втрати від них оцінювалися у понад 9 трлн дол., а у 2025 році прогнозуються вже на рівні 10,5 трлн дол. При таких річних витратах світ витрачає приблизно 333 тис. дол. на хвилину на кіберзлочинність. Розглянуто найпопулярніші типи кіберзлочинних атак протягом 2024-2025 рр., серед яких: фішинг та спуфінг; програми-вимагачі; компрометація ділової електронної пошти; шкідливе програмне забезпечення; крадіжка особистих даних / шахрайство; витоки даних. Проаналізовано наслідки кібератак у розрізі галузей економіки. По-перше, одним із секторів, що найбільше страждає від кібератак є охорона здоров'я. Організації охорони здоров'я зберігають величезні

персональні дані та повинні працювати цілодобово, що робить їх основними цілями. Лікарні, страхові компанії та клініки зіткнулися з поширеними блокуваннями медичних записів та крадіжками даних через програми-вимагачі. Загалом, атаки на охорону здоров'я продовжують і надалі зростати. По-друге, фінанси та банківська справа. Зловмисники використовують системи онлайн-банкінгу та фінансового персоналу. По-третє, уряд та критична інфраструктура в результаті посилення геополітичної нестабільності. Урядові установи, комунальні послуги та інфраструктура в таких сферах, як енергетика, водопостачання, транспорт тощо, стикаються з частими кампаніями, від хактивізму до шпигунства, що спонсорується державою.

Виділено ключові етапи розвитку кіберзагроз: початковий етап (1980-2000 рр.); етап комерціалізації (1980-2000 рр.); етап індустріалізації (2010-2017 рр.); етап ransomware та гібридних атак (2017 р і до сьогодні). Особливостями сучасного етапу є: види атак – шифрувальники, подвійне вимагання (зашифрувати та злити дані), атаки на OT/ICS, постачальницькі ланцюги; мотиви атак – великі викупи, дестабілізація критичної інфраструктури; тип захисту – Zero Trust, EDR/XDR, кіберстійкість, оркестрація реагування.

Вивчено еволюцію понять стійкості, цифрової та кібербезпеки і цифрової стійкості підприємств. Наведено порівняльну характеристику цифрової безпеки та стійкості. Запропоновано цифрову стійкість підприємства розглядати як здатність підприємства адаптуватися до цифрових загроз, протидіяти їм та швидко відновлюватися після інцидентів, зберігаючи безперервність ключових процесів. Серед компонентів цифрової стійкості підприємства виділено технічну, організаційну, людську, правову та регуляторну, економічну, адаптивну та інноваційну стійкість.

Зазначено, що розроблення концепції забезпечення цифрової стійкості підприємств передбачає створення системного підходу, що поєднує технологічні інновації, кібербезпеку, гнучке управління та стратегічне використання даних. Така концепція дозволяє підприємствам не лише протистояти сучасним викликам цифрової економіки, а й використовувати цифровізацію як основу для

сталого розвитку та посилення конкурентних позицій. Це вказує на той факт, що цифрова стійкість є не просто технічним інструментом, а стратегічним фактором конкурентоспроможності підприємства, забезпечуючи стабільність бізнес-процесів, формуючи довіру клієнтів і партнерів, відкриваючи доступ до міжнародних ринків та підвищуючи репутацію компанії. Сформовано концепцію забезпечення цифрової стійкості підприємств, що розкриває принципи, напрями, завдання та інструменти, які дозволяють інтегрувати цифрові технології у бізнес-процеси, формувати гнучкі управлінські стратегії, забезпечувати кібербезпеку та ефективне використання інформаційних ресурсів. Реалізація цієї концепції спрямована на підвищення рівня адаптивності підприємств до зовнішніх викликів, збереження конкурентних позицій на ринку та створення умов для довгострокового сталого розвитку в умовах глобальної цифрової трансформації.

2 Техніко-економічний аналіз діяльності ПрАТ «Київ – Дніпровське міжгалузеве підприємство промислового залізничного транспорту»

2.1 Загальна характеристика діяльності підприємства

Приватне акціонерне товариство Київ – Дніпровське міжгалузеве підприємство промислового залізничного транспорту (ПрАТ «Київ – Дніпровське МППЗТ») є підприємством, що забезпечує взаємодію з магістральним залізничним транспортом загального користування через окремі регіональні філії Укрзалізниці та має примикання до її станцій.

Метою діяльності є отримання прибутку на комерційній основі за рахунок ринкової діяльності і забезпечення на цій основі соціально-економічних потреб суспільства та зростання добробуту працівників Товариства та його акціонерів.

Основними напрямками діяльності товариства є перевезення вантажів, експлуатація та обслуговування інфраструктури.

Компанія надає комплекс транспортних послуг, зокрема [32]:

- перевезення вантажів від станцій примикання до місць навантаження та вивантаження;
- виконання маневрових операцій;
- навантажувально-розвантажувальні роботи;
- будівництво та модернізацію колійного господарства;
- метрологічні та інші послуги, пов'язані з організацією вантажних перевезень залізничним транспортом.

Більше детально перелік послуг наведено в статусі підприємства [33].

На ринку промислових перевезень ПрАТ «Київ – Дніпровське МППЗТ» посідає друге місце після Укрзалізниці, утримуючи частку близько 10 %. Підприємство включено до Переліку об'єктів державної власності, що мають стратегічне значення для економіки та безпеки України (затверджено постановою Кабінету Міністрів України від 04.03.2015 р. № 83) [6].

До складу товариства входить 30 відокремлених структурних підрозділів (філій) та Київ-Дніпровський виробничий підрозділ, створені в процесі реорганізації відповідно до наказів Міністерства транспорту України від 25.01.2001 р. № 35 та Міністерства транспорту та зв'язку України від 26.04.2006 р. № 396 [32]. Через тимчасову окупацію частини територій (Донецької та Луганської областей, АР Крим та м. Севастополя) контроль над чотирма філіями втрачено.

Станом на 2024 рік у складі ПрАТ «Київ – Дніпровське МППЗТ» функціонує 27 філій: Барська, Бердянська, Бродецька, Енергодарська, Житомирська, Зеленодольська, Ізмаїльська, Кам'янець-Подільська, Київ-Деміївська, Київ-Оболонська, Кіровоградська, Подільська, Лубенська, Констянтинівська, Миронівська, Новокаховська, Одеська, Ольшанська, Полтавська, Прилуцька, Сумська, Тернопільська, Трипільська, Харківська, Херсонська, Черкаська та Київ-Дніпровський виробничий підрозділ [32].

Загальну структуру підприємств подано на рисунку 2.1.



Рисунок 2.1 – Загальна структура ПрАТ «Київ – Дніпровське МППЗТ» станом на 2024 р. [32]

Філії товариства здійснюють повну фінансово-господарську діяльність у 17 областях України та місті Києві, співпрацюють з усіма залізницями Укрзалізниці та мають примикання до 49 станцій залізничного транспорту загального користування.

2.2 Аналіз обсягів діяльності підприємства

Підприємство надає комплекс транспортних послуг щодо перевезення вантажів від станцій примикання до місць навантаження та вивантаження, виконання маневрових операцій, навантажувально-розвантажувальних робіт, будівництва та модернізації колійного господарства, метрологічних та інших послуг, пов'язаних з організацією вантажних перевезень залізничним транспортом. Проаналізуємо обсяги діяльності підприємства (таблиця 2.1).

Таблиця 2.1 – Аналіз обсягів роботи підприємства [32, 34-38]

Показник	2020	2021	2022	2023	2024
Перевезення вантажів, тис. т	21679,0	21306,3	9212,0	10104,0	9737,0
<i>абсолютне відхилення, тис. т</i>	-	-372,7	-12094,3	892,0	-367,0
<i>відносне відхилення, %</i>	-	98,3	43,2	109,7	96,4

Аналіз динаміки обсягів роботи підприємства вказує на нестабільність обсягів перевезень вантажів (рисунок 2.2). Зокрема у 2020 р. перевезено 21679,0 тис. т вантажів, у 2021 р. – 21306,3 тис. т вантажів, що на 372,7 тис. т або 1,7 % менше, у 2022 р. – 9212,0 тис. т вантажів, що на 12094,3 тис. т або 56,8 % менше (найбільш суттєве скорочення за аналізований період), у 2023 р. – 10104,0 тис. т вантажів, що на 892,0 тис. т або 9,7 % більше, у 2024 р. – 9737,0 тис. т вантажів, що на 367,0 тис. т або 3,6 % менше.

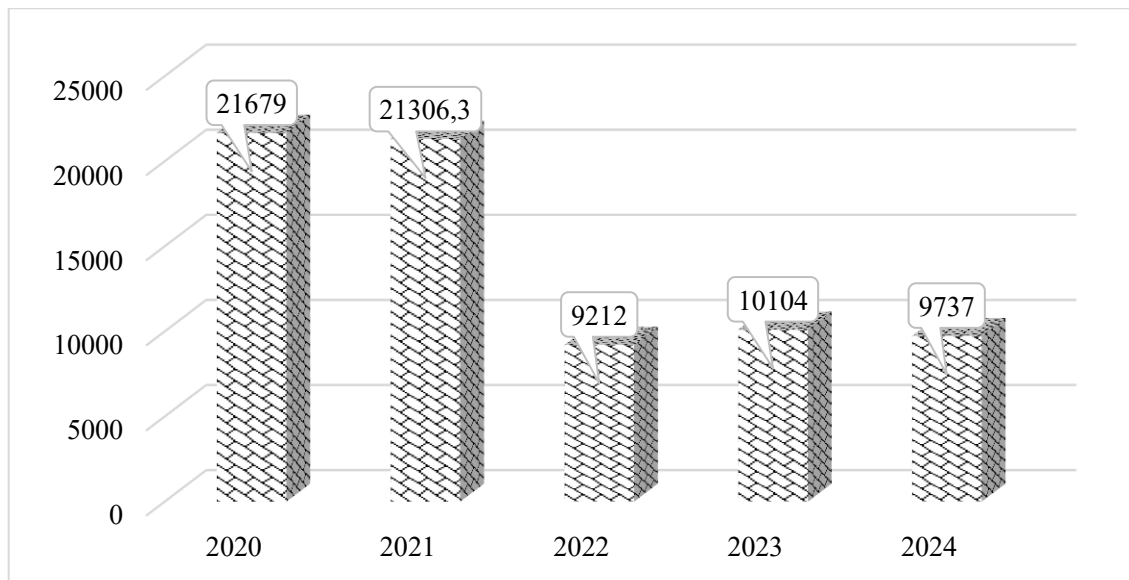


Рисунок 2.2 – Динаміка обсягів перевезень вантажів за 2020-2024 рр., тис. т

Варто зазначити, що причинами скорочення обсягів роботи підприємства у 2024 році стали зменшення кількості замовників послуг, вихід з ладу Трипільської ТЕС, зменшення об'ємів перевезення зернових, будівельних вантажів та паливномастильних матеріалів. Тобто вплив негативних наслідків військових дій продовжує бути суттєвим і дестабілізує роботу підприємства.

Серед інших послуг, які надаються підприємством, слід відзначити: відстій вагонів, користування під'їзними залізничними коліями, маневрова робота.

2.3 Аналіз стану основних засобів підприємства

Сьогодні основні фонди є ключовим елементом та базисом функціонування будь-якого підприємства, забезпечуючи матеріальну основу виробничого процесу, визначаючи його масштаби та технологічний рівень. Саме від стану будівель, споруд, обладнання та транспортних засобів залежить ефективність господарської діяльності та конкурентоспроможність компанії.

Аналіз стану основних засобів дозволяє оцінити рівень їх фізичного та морального зносу, своєчасно виявити потребу у ремонті, модернізації чи заміні.

Це дає можливість уникнути простоїв, зменшити витрати на аварійні ремонти та забезпечити безперервність виробничого процесу [39].

З фінансової точки зору, основні фонди становлять значну частину активів підприємства. Їхня вартість та амортизація впливають на собівартість продукції чи послуг, формування прибутку та інвестиційні рішення. Тому аналіз їхнього стану є важливим інструментом для планування витрат, визначення потреби у капіталовкладеннях та оптимізації фінансової стратегії.

Не менш важливим є аспект безпеки. Використання застарілого чи несправного обладнання може призвести до виробничих ризиків, аварій та штрафних санкцій. Регулярний аналіз стану основних засобів допомагає підтримувати належний рівень охорони праці та екологічної безпеки. Особливо важливим аспект безпеки є для підприємств промислового залізничного транспорту, адже їх діяльність пов'язана з перевезенням великих обсягів вантажів, використанням складної техніки та експлуатацією розгалуженої інфраструктури. Будь-які технічні несправності чи зношеність основних фондів можуть призвести не лише до економічних втрат, але й до аварійних ситуацій, що становлять загрозу для життя та здоров'я працівників, а також для навколишнього середовища. Регулярний аналіз стану основних засобів у цьому секторі дозволяє своєчасно виявляти критичні проблеми, планувати ремонти та модернізацію, а також забезпечувати безперервність транспортного процесу. Це особливо актуально для залізничних підприємств, які виконують стратегічні завдання з перевезення промислових вантажів та підтримують економічну стабільність країни. Крім того, належний контроль за технічним станом обладнання та інфраструктури сприяє дотриманню вимог охорони праці та техніки безпеки. Це знижує ризики виробничого травматизму, підвищує рівень довіри з боку партнерів і замовників та забезпечує відповідність міжнародним стандартам транспортної галузі [40-42].

Таким чином, для підприємств промислового залізничного транспорту аналіз стану основних засобів є не лише економічною необхідністю, а й ключовим чинником безпеки, що визначає стабільність та ефективність їхньої

роботи.

Відповідно до статутних завдань майновий стан ПрАТ «Київ – Дніпровське МППЗТ» являє собою комплекс будівель, споруд, пристроїв, обладнання та рухомого складу промислового залізничного транспорту. Загальна довжина залізничних колій складає 954,9 км, з них: знаходяться на тимчасово окупованих територіях філій – 242,8 км, експлуатується – 445,6 км, виведені з експлуатації – 266,5 км. Крім того, на балансі підприємства нараховується 2389 стрілочних переводів, 38 мостів, 200 переїздів загального користування [32].

Локомотивний парк підприємства нараховує 168 одиниць тепловозів, з яких 28 одиниць залишилися на тимчасово окупованій території Автономної Республіки Крим та 17 одиниць з 24 лютого 2022 року перебувають на територіях, на яких ведуться (велися) бойові дії або тимчасово окупованих рф. На даний час експлуатаційний локомотивний парк складається з 119 тепловозів, з яких 78 тепловозів в роботі, 41 тепловоз знаходиться в ремонті, очікуванні ремонту або потребують списання. Власний вагонний парк вантажних вагонів нараховує 435 одиниць, з них 177 одиниць – вагони-думпкари, 31 – хопер-дозатор, 16 – напіввагони, службових вагонів – 5; для власних потреб – 84, під списання – 122 (у тому числі 18 вагонів залишилися на тимчасово окупованій території Автономної Республіки Крим та 28 на територіях, на яких ведуться (велися) бойові дії або тимчасово окупованих рф) [32].

Для виконання вантажно-розвантажувальних та складських робіт Товариство має 63 крани на залізничному ходу, козлові крани, розвантажувачі, екскаватори; автомобільні та електронавантажувачі, бульдозери та іншу техніку. У зв'язку з військовою агресією російської федерації на території України, що розпочалась 24 лютого 2022 року, частина філій Товариства наразі знаходиться на тимчасово окупованих рф територіях (Бердянська, Енергодарська, Миронівська, Новокаховська, Херсонська), частина – де ведуться активні бойові дії або у прифронтовій зоні. Внаслідок військової агресії рф та введення воєнного стану на території України з 24.02.2022 року відбулося призупинення або скорочення обсягів діяльності більшості підприємств, яким Товариство надає

послуги з перевезення вантажів.

Наразі філії Товариства, які знаходяться на підконтрольних територіях України, здійснюють господарську діяльність з низькою завантаженістю виробничих потужностей. Водночас філії, які знаходяться на тимчасово окупованих рф територіях, у районах ведення активних бойових дій або в прифронтовій зоні – не здійснюють перевезення вантажів або здійснюють частково. З огляду на тривалий характер та непередбачуваність війни, оцінити повний спектр економічних наслідків наразі складно. Станом на кінець 2024 року ключові активи Товариства не зазнали пошкоджень і продовжують функціонувати у штатному режимі. Операційна діяльність Товариства забезпечується в повному обсязі [32].

Проаналізуємо динаміку вартості та ступеня зносу основних фондів підприємства (таблиця 2.2).

Таблиця 2.2 – Аналіз вартості та зносу основних фондів [32, 34-38]

Показник	2020	2021	2022	2023	2024
1	2	3	4	5	6
Первісна вартість основних фондів, тис. грн	1134763,0	1154617,0	1158831,0	1165063,0	12459674,0
<i>абсолютне відхилення, тис. грн</i>	-	19854,0	4214,0	6232,0	11294611,0
<i>відносне відхилення, %</i>	-	101,7	100,4	100,5	1069,4
Знос основних фондів, тис. грн	819963,0	844314,0	873227,0	920738,0	11047700,0
<i>абсолютне відхилення, тис. грн</i>	-	24351,0	28913,0	47511,0	10126962,0
<i>відносне відхилення, %</i>	-	103,0	103,4	105,4	1199,9
Залишкова вартість основних фондів, тис. грн	314800,0	310303,0	285604,0	244325,0	1411974,0

Продовження таблиці 2.2

1	2	3	4	5	6
<i>абсолютне відхилення, тис. грн</i>	-	-4497,0	-24699,0	-41279,0	1167649,0
<i>відносне відхилення, %</i>	-	98,6	92,0	85,5	577,9
Ступінь зносу основних фондів, %	72,3	73,1	75,4	79,0	88,7
<i>абсолютне відхилення, %</i>	-	0,8	2,3	3,6	9,7

Протягом 2020-2024 рр. спостерігається зростання вартості основних фондів: у 2020 р. їх первісна вартість склала 1134763,0 тис. грн, у 2021 р. – 1154617,0 тис. грн, що на 19854,0 тис. грн або 1,7 % більше, у 2022 р. – 1158831,0 тис. грн, що на 4214,0 тис. грн або 0,4 % більше, у 2023 р. – 1165063,0 тис. грн, що на 6232,0 тис. грн або 0,5 % більше, у 2024 р. – 12459674,0 тис. грн, що на 11294611,0 тис. грн або у 10,7 разів більше.

Збільшувалася і вартість зносу основних фондів: у 2020 р. вона склала 819963,0 тис. грн, у 2021 р. – 844314,0 тис. грн, що на 24351,0 тис. грн або 3,0 % більше, у 2022 р. – 873227,0 тис. грн, що на 28913,0 тис. грн або 3,4 % більше, у 2023 р. – 920738,0 тис. грн, що на 47511,0 тис. грн або 5,4 % більше, у 2024 р. – 11047700,0 тис. грн, що на 10126962,0 тис. грн або майже в 12 разів більше.

Залишкова вартість основних фондів підприємства у 2020 р. склала 314800,0 тис. грн, у 2021 р. – 310303,0 тис. грн, що на 4497,0 тис. грн або 1,4 % менше, у 2022 р. – 285604,0 тис. грн, що на 24699,0 тис. грн або 8,0 % менше, у 2023 р. – 244325,0 тис. грн, що на 41279,0 тис. грн або 14,5 % менше, у 2024 р. – 1411974,0 тис. грн, що на 1167649,0 тис. грн або в 5,8 разів більше.

Оскільки темпи зносу основних фондів перевищували темпи приросту їх первісної вартості, ступінь їхнього фізичного зношення на підприємстві зростав: у 2020 р. значення показника зносу склало склав 72,3 %, у 2021 р. – 73,1 %, що на 0,8 % більше, у 2022 р. – 75,4 %, що на 2,3 % більше, у 2023р. – 79,0 %, що на

3,6 % більше, у 2024 р. – 88,7 %, що на 9,7 % більше. У 2024 р. зафіксовано найвищий рівень зносу основних фондів підприємства за аналізований період – 88,7 %. Загалом рівень зносу на критичному рівні – не менше 70 %.

Динаміка вартості та ступеня зносу основних фондів підприємства наведена на рисунку 2.3.

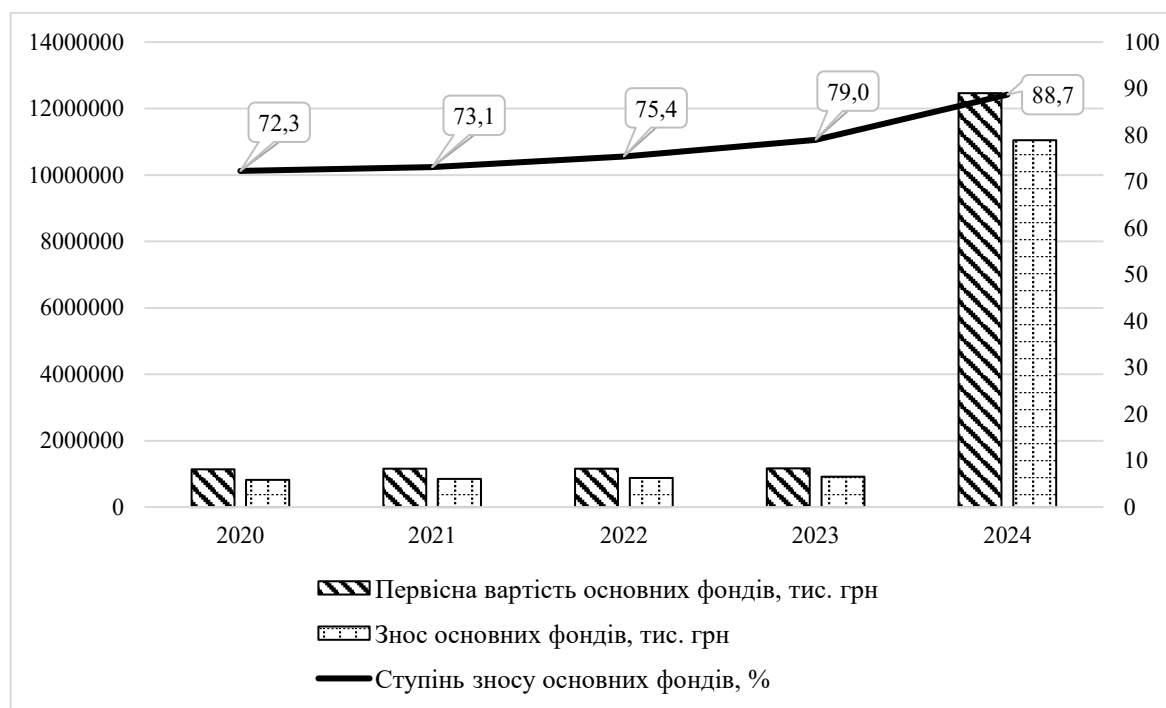


Рисунок 2.3 – Динаміка вартості та рівня зносу основних фондів підприємства за період 2020-2024 рр.

Збільшення витрат на амортизацію відбулося в результаті проведеної дооцінки активів до справедливої їх вартості станом на 31 грудня 2023 року. Дооцінка активів до справедливої їх вартості була проведена Товариством із залученням професійних незалежних оцінювачів станом на 31 грудня 2023 року з відображенням по бухгалтерському обліку у 2024 році. Приводом для переоцінки стала істотна відмінність залишкової вартості об'єктів необоротних активів від їх справедливої (ринкової) вартості.

Слід відзначити і зміни в вартості та структурі основних засобів за рахунок придбання, модернізації та ремонту. Зокрема у 2020 р. відбулося придбання основних засобів на суму 4392,0 тис. грн, модернізація основних засобів

(тепловозів) – 1689,0 тис. грн, капітальний ремонт основних засобів (тепловозів 5 од., вагонів 27 од., виробничого приміщення) – 31091,0 тис. грн. У 2021 р. відбулося придбання основних засобів на суму 1503,0 тис. грн, модернізація основних засобів (встановлення додаткового обладнання на тепловози, залізнична колія (стрілочні переводи), системи опалення в виробничих приміщеннях) – 3992,0 тис. грн, капітальний ремонт основних засобів (вагони, тепловози залізнична переїзди, будівлі та споруди) – 19897,0 тис. грн. У 2022 р. відбулося придбання основних засобів (виробниче обладнання: колійний інструмент, дизель генератори) – 120,0 тис. грн, капітальний ремонт основних засобів (тепловоз, вагони, залізничні колії, стрілочні переводи) – 5250,0 тис. грн. У 2023 році відбулося придбання основних засобів (виробниче обладнання: колійний інструмент, дизель генератори) – 4811,0 тис. грн, модернізація основних засобів (будівлі та споруди (стрілочні пости), модернізація тепловозів) – 2188,0 тис. грн, капітальний ремонт основних засобів (тепловоз, 2 вагони думпкари) – 959,0 тис. грн. Фінансування придбання основних засобів та їх модернізація і ремонт відбувалася за рахунок власних коштів підприємства.

Важливим етапом аналізу основних фондів виступає дослідження змін показників фондівіддачі, фондомісткості та фондоозброєності. Фондовіддача визначається як співвідношення вартості виготовленої продукції у грошовому вимірі до середньорічної вартості основних виробничих фондів. Цей показник відображає ефективність використання засобів праці та демонструє, який обсяг продукції отримують на кожну одиницю основних фондів. Протилежним до нього є показник фондомісткості, що дозволяє встановити, яка вартість основних засобів припадає на одну гривню виробленої продукції, та характеризує рівень забезпеченості підприємства виробничими ресурсами. Фондоозброєність праці визначається як співвідношення вартості основних засобів до кількості працівників підприємства.

Аналіз показників ефективності використання основних засобів підприємства подано в таблиці 2.3 і на рисунку 2.4.

Таблиця 2.3 – Аналіз показників ефективності використання основних засобів підприємства

Показник	2020	2021	2022	2023	2024
Фондовіддача, грн/грн	2,36	2,48	1,62	2,57	0,46
<i>абсолютне відхилення, грн/грн</i>	-	0,12	-0,86	0,95	-2,11
<i>відносне відхилення, %</i>	-	105,1	65,3	158,6	17,9
Фондомісткість, грн/грн	0,42	0,40	0,62	0,39	2,19
<i>абсолютне відхилення, грн/грн</i>	-	-0,02	0,22	-0,23	1,80
<i>відносне відхилення, %</i>	-	95,2	155,0	62,9	561,5
Фондоозброєність, тис. грн/ос.	175,38	163,23	178,17	186,79	1110,92
<i>абсолютне відхилення, грн/ос.</i>	-	-12,15	14,94	8,62	924,13
<i>відносне відхилення, %</i>	-	93,1	109,2	104,8	594,7

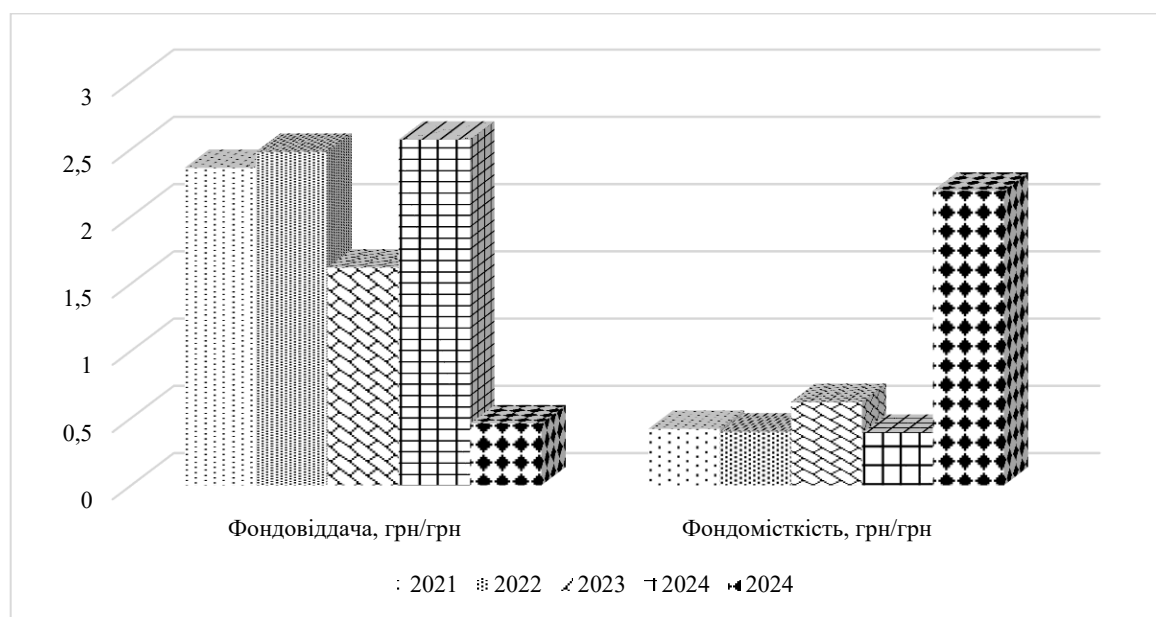


Рисунок 2.3 – Динаміка фондовіддачі та фондомісткості, грн/грн

Динаміка показників оцінювання ефективності використання основних фондів була наступною. Фондовіддача основних фондів у 2020 р. склала 2,36 грн/грн, у 2021 р. – 2,48 грн/грн, що на 0,12 грн/грн або 5,1 % більше, у 2022 р. – 1,62 грн/грн, що на 0,86 грн/грн або 34,7 % менше, у 2023 р. – 2,57 грн/грн, що на 0,95 грн/грн або 58,6 % більше, у 2024 р. – 0,46 грн/грн, що

на 2,11 грн/грн або 82,1 % менше. Погіршення фондівдачі основних фондів зумовлено зниженням обсягів роботи підприємства, а у 2024 році ще додатково переоцінкою основних фондів підприємства.

Нестабільність характерна і для фондомісткості основних фондів, значення якої у 2020 р. склала 0,42 грн/грн, у 2021 р. – 0,40 грн/грн, що на 0,02 грн/грн або 4,8 % менше, у 2022 р. – 0,62 грн/грн, що на 0,22 грн/грн або 55,0 % більше, у 2023 р. – 0,39 грн/грн, що на 0,23 грн/грн або 37,1 % менше, у 2024 р. – 2,19 грн/грн, що на 1,80 грн/грн або в 5,6 разів більше.

Фондоозброєність працівників у 2020 р. склала 175,38 тис. грн/ос., у 2021 р. – 163,23 тис. грн/ос., що на 12,15 тис. грн/ос. або 6,9 % менше, у 2022 р. – 178,17 тис. грн/ос., що на 14,94 тис. грн/ос. або 9,2 % більше, у 2023 р. – 186,79 тис. грн/ос., що на 8,62 тис. грн/ос. або 4,8 % більше, у 2024 р. – 1110,92 тис. грн/ос., що на 924,13 тис. грн/ос. або майже в 6 разів більше.

2.4 Аналіз ефективності використання трудових ресурсів підприємства

Важливою складовою комплексного аналізу діяльності підприємства є вивчення руху та ефективності використання трудових ресурсів. Належне забезпечення підприємства робочою силою та високий рівень продуктивності праці відіграють ключову роль у зростанні виробничих обсягів. Основні завдання аналізу трудових ресурсів полягають у: оцінці використання персоналу, робочого часу та продуктивності праці; визначенні чинників та кількісному вимірюванні їхнього впливу на зміну показників праці; пошуку резервів для більш раціонального й результативного застосування трудових ресурсів [44].

Аналіз починається з оцінки забезпеченості підприємства персоналом за чисельністю, структурою, рівнем кваліфікації та культурно-освітнім рівнем, а також з вивчення руху робочої сили з метою виявлення внутрішніх резервів її економного використання [45]. Важливо враховувати співвідношення основних

і допоміжних працівників, частку управлінського персоналу, а також вікові та кваліфікаційні характеристики колективу. Такий підхід дозволяє визначити, чи оптимально сформований кадровий склад і чи відповідає потребам виробництва.

Не менш значущим є дослідження рівня кваліфікації та професійного розвитку працівників. Рівень освіти, наявність програм підвищення кваліфікації, витрати на навчання персоналу та їхній вплив на продуктивність праці дають змогу оцінити потенціал колективу та можливості його подальшого розвитку.

Важливим напрямом аналізу виступає використання робочого часу. У даному напрямі розглядаються коефіцієнти його ефективності, втрати через прогули, простої чи лікарняні, а також використання понаднормових годин. Такий аналіз допомагає виявити резерви для зменшення непродуктивних витрат часу та підвищення результативності праці.

Узагальненим показником результативності та ефективності праці виступає продуктивність, яка відображає обсяг виробленої продукції чи наданих послуг на одиницю витрат праці. Рівень продуктивності визначається за прямими та зворотними показниками. До прямих належать виробіток продукції та показник продуктивності праці, який може вимірюватися у натуральних, вартісних або нормативних одиницях. Зворотним показником є трудомісткість – планова, фактична та нормативна [43]. Порівняння продуктивності з середньогалузевими значеннями дозволяє оцінити конкурентоспроможність підприємства та визначити фактори, що стримують її зростання.

Окремо аналізується ефективність використання фонду оплати праці. Тут важливо зіставити темпи зростання заробітної плати з темпами зростання продуктивності, дослідити структуру фонду (основна, додаткова заробітна плата, премії), а також оцінити мотиваційну систему підприємства. Це дає змогу визначити, чи стимулює система оплати праці підвищення результативності.

Не можна оминати увагою питання плинності кадрів та стабільності колективу. Вивчення коефіцієнтів обороту кадрів, причин звільнень та їхнього впливу на витрати підприємства дозволяє оцінити кадрову політику та розробити заходи для утримання кваліфікованих працівників.

Завершальним етапом аналізу є визначення резервів підвищення ефективності використання трудових ресурсів. Це може включати оптимізацію чисельності персоналу, впровадження нових технологій, автоматизацію процесів, поліпшення умов праці та розвиток корпоративної культури.

Проведемо аналіз чисельності працівників підприємства, фонду оплати праці та продуктивності праці (таблиця 2.4). Щодо чисельності працівників, то варто вказати на негативну тенденцію скорочення персоналу. Так, у 2020 р. середньооблікова чисельність працівників склала 1795 осіб, у 2021 р. – 1901 осіб, що на 106 осіб або 5,9 % більше, у 2022 р. – 1603 осіб, що на 298 осіб або 15,7 % менше, у 2023 р. – 1308 осіб, що на 295 осіб або 18,4 % менше, у 2024 р. – 1271 особа, що на 37 осіб або 2,8 % менше. Розмір фонду оплати праці загалом збільшувався, лише у 2022 р. зафіксовано негативну зміну. У 2020 р. фонд оплати праці склав 278459,1 тис. грн, у 2021 р. – 314883,0 тис. грн, що на 36423,9 тис. грн або 13,1 % більше, у 2022 р. – 194663,0 тис. грн, що на 120220,0 тис. грн або 38,2 % менше, у 2023 р. – 246265,0 тис. грн, що на 51602,0 тис. грн або 26,5 % більше, у 2024 р. – 280913,0 тис. грн, що на 34648,0 тис. грн або 14,1 % більше.

Таблиця 2.4 – Аналіз показників використання трудових ресурсів

Показник	2020	2021	2022	2023	2024
Середньооблікова чисельність працівників, осіб	1795	1901	1603	1308	1271
<i>абсолютне відхилення, осіб</i>	-	106	-298	-295	-37
<i>відносне відхилення, %</i>	-	105,9	84,3	81,6	97,2
Фонд оплати праці, тис. грн	278459,1	314883,0	194663,0	246265,0	280913,0
<i>абсолютне відхилення, тис. грн</i>	-	36423,9	-120220,0	51602,0	34648,0
<i>відносне відхилення, %</i>	-	113,1	61,8	126,5	114,1
Продуктивність праці, тис. грн/ос.	413,7	405,4	288,4	479,7	508,2
<i>абсолютне відхилення, тис. грн/ос.</i>	-	-8,3	-117,0	191,3	28,5
<i>відносне відхилення, %</i>	-	98,0	71,1	166,3	105,9

Розглянемо і динаміку продуктивності праці: у 2020 р. показник склав 413,7 тис. грн/ос., у 2021 р. – 405,4 тис. грн/ос., що на 8,3 тис. грн/ос. або 2,0 % менше, у 2022 р. – 288,4 тис. грн, що на 117,0 тис. грн/ос. або 28,9 % менше, у 2023 р. – 479,7 тис. грн, що на 191,3 тис. грн/ос. або 66,3 % більше, у 2024 р. – 508,2 тис. грн, що на 28,5 тис. грн/ос. або 5,9 % більше.

Важливим етапом оцінки ефективності використання трудових ресурсів є аналіз співвідношення динаміки продуктивності праці та фонду оплати праці, що дозволяє визначити, чи забезпечується випереджальне зростання продуктивності порівняно з витратами на заробітну плату.

Відповідний порівняльний аналіз подано на рисунку 2.5.

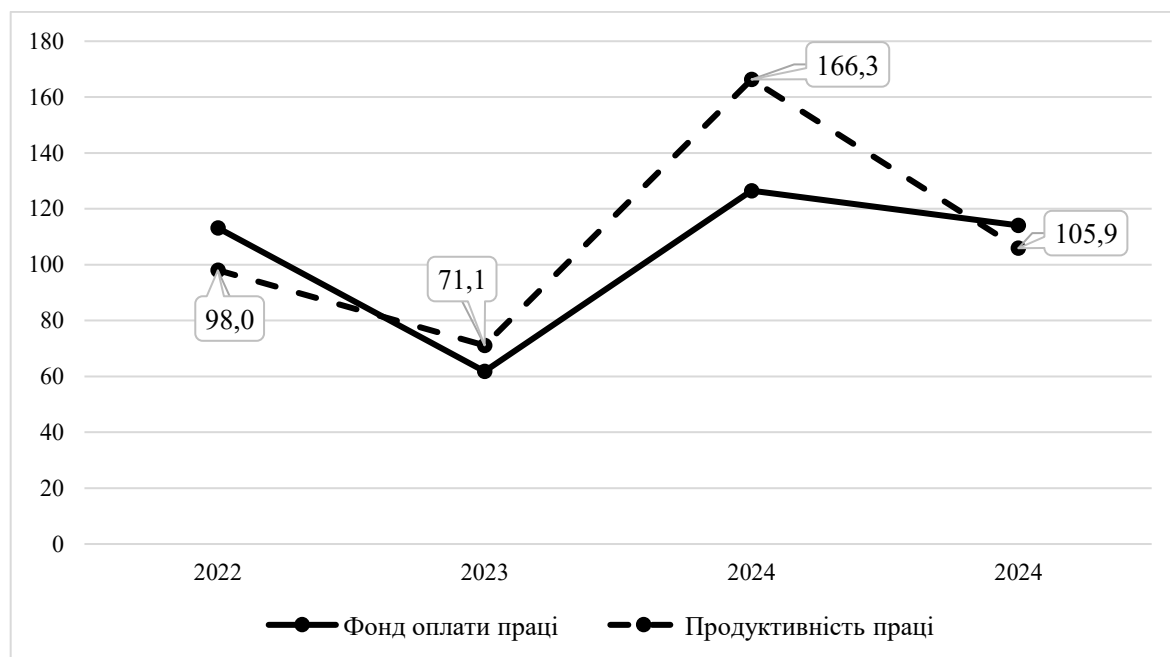


Рисунок 2.5 – Порівняльний аналіз динаміки темпу росту продуктивності праці та темпу росту фонду оплати праці

Наведені на рисунку 2.5 вказують загалом на позитивну тенденцію перевищення темпу росту продуктивності праці над темпом росту фонду оплати праці, зокрема у 2021 р. – на 9,3 %, у 2022 р. – на 39,8 %. У 2020 р. та 2024 р. спостерігається негативна динаміка щодо перевищення темпу росту фонду оплати праці над темпом росту продуктивності праці – на 15,1 % та 8,2 %.

2.5 Аналіз операційних витрат діяльності підприємства

Одним із ключових показників діяльності підприємства є рівень виробничих витрат, тому їх аналіз набуває особливого значення у випадку, коли суб'єкт господарювання прагне підвищити конкурентоспроможність та забезпечити незалежність власного виробництва. Витрати у виробничому процесі відображають такі характеристики, як ефективність роботи, раціональність використання матеріалів та обладнання, рівень застосування енергії й трудових ресурсів, що безпосередньо впливають на результати діяльності підприємства. Облік витрат виконує низку важливих функцій: здійснює загальний контроль виробничого процесу, визначає загальну собівартість продукції та її одиничну вартість, а також забезпечує контроль кінцевих результатів. Детальний аналіз виробничих витрат дозволяє виявити недоліки в системі обліку, визначити напрями вдосконалення та запобігти можливим проблемам у майбутньому. Без застосування аналітичних процедур неможливо об'єктивно оцінити ефективність діяльності підприємства, адже зниження витрат не завжди свідчить про зростання продуктивності, так само як їх збільшення не обов'язково означає погіршення результатів роботи [46].

Аналіз витрат діяльності підприємств залізничного транспорту спрямований на виявлення причин перевитрат та пошук можливостей скорочення витрат основної діяльності, зокрема експлуатаційних та інших, як у масштабах всієї залізниці, так і окремих її підприємств. Головною метою такого аналізу є визначення резервів для зниження собівартості перевезень. Джерелами інформації виступають форма № 2 «Звіт про фінансові результати» з відповідними додатками та форма № 17 «Витрати за основними видами економічної діяльності, видами робіт допоміжної діяльності, економічними елементами та статтями витрат за фактичними показниками», яка містить деталізовані дані щодо експлуатаційних витрат підприємства [40].

Залізничний транспорт має специфічні особливості, які відображаються в

обліковій діяльності. Управління здійснюється за територіальним принципом (до складу Укрзалізниці входять шість залізниць як юридичні особи з власними рахунками та обліком) і функціональним принципом – через вертикаль від центрального рівня до окремих напрямів господарства. У структурі залізниць діють підрозділи (станції, вокзали, депо, дистанції колії та зв'язку), що беруть участь у перевезеннях, але не мають статусу юридичних осіб [47].

Аналіз операційних витрат підприємства доцільно розпочати з аналізу динаміки витрат, а саме матеріальних витрат, витрат на паливо та енергію, на оплату праці, відрахувань на соціальні заходи, амортизації, інших витрат.

Аналіз перелічених елементів витрат подано в таблиці 2.5 та рисунку 2.6.

Таблиця 2.5 – Аналіз операційних витрат підприємства

Показник	2020	2021	2022	2023	2024
1	2	3	4	5	6
Матеріальні витрати, тис. грн	233928,0	220142,0	131770,0	215160,0	198982,0
<i>абсолютне відхилення, тис. грн</i>	-	-13786,0	-88372,0	83390,0	-16178,0
<i>відносне відхилення, %</i>	-	94,1	59,9	163,3	92,5
Витрати на оплату праці, тис. грн	278298,0	314883,0	194663,0	246265,0	280913,0
<i>абсолютне відхилення, тис. грн</i>	-	36585,0	-120220,0	51602,0	34648,0
<i>відносне відхилення, %</i>	-	113,1	61,8	126,5	114,1
Відрахування на соціальні заходи, тис. грн	61610,0	69896,0	44782,0	53616,0	60837,0
<i>абсолютне відхилення, тис. грн</i>	-	8286,0	-25114,0	8834,0	7221,0
<i>відносне відхилення, %</i>	-	113,4	64,1	119,7	113,5
Амортизація, тис. грн	34343,0	33523,0	30355,0	28315,0	148167,0

Продовження таблиці 2.5

1	2	3	4	5	6
абсолютне відхилення, тис. грн	-	-820,0	-3168,0	-2040,0	119852,0
відносне відхилення, %	-	97,6	90,5	93,3	523,3
Інші операційні витрати, тис. грн	95786,0	94455,0	52529,0	79241,0	61853,0
абсолютне відхилення, тис. грн	-	-1331,0	-41926,0	26712,0	-17388,0
відносне відхилення, %	-	98,6	55,6	150,9	78,1
Разом операційні витрати, тис. грн	703965,0	732899,0	454099,0	622597,0	750752,0
абсолютне відхилення, тис. грн	-	28934,0	-278800,0	168498,0	128155,0
відносне відхилення, %	-	104,1	62,0	137,1	120,6

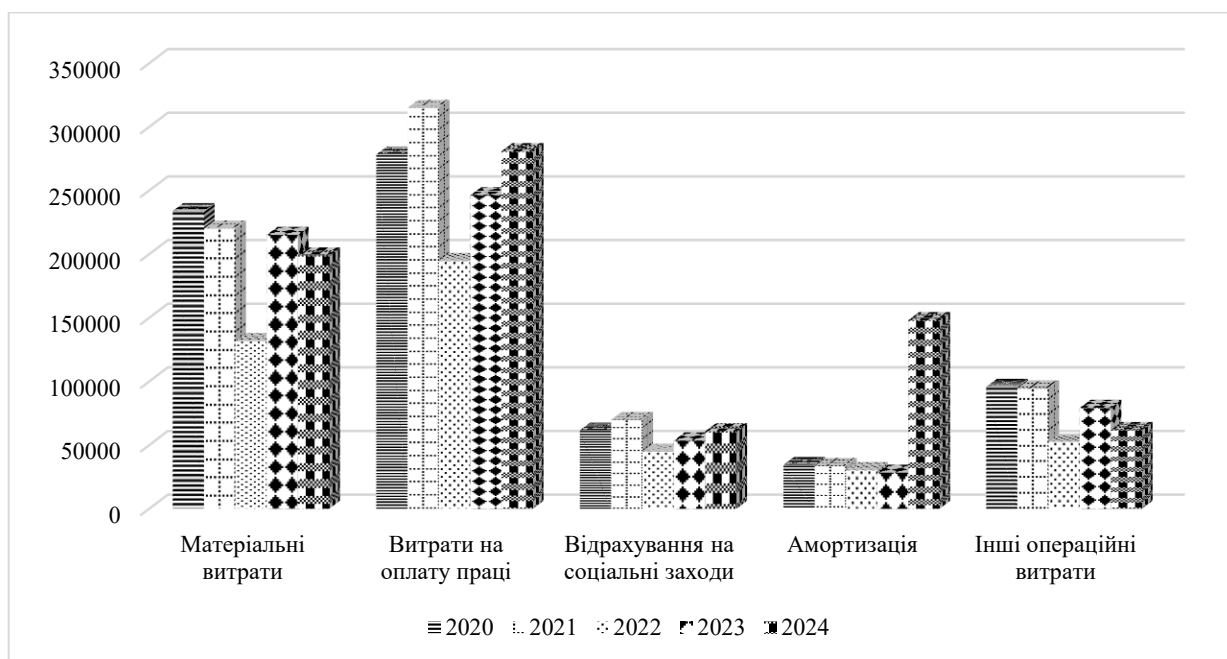


Рисунок 2.6 – Динаміка операційних витрат підприємства, тис. грн

Аналіз операційних витрат діяльності підприємства дозволяє дійти наступних висновків. У 2020 р. операційні витрати склали 703965,0 тис. грн, у 2021 р. – 732899,0 тис. грн, що на 28934,0 тис. грн або 4,1 % більше, у 2022 р. –

454099,0 тис. грн, що на 278800,0 тис. грн або 38,0 % менше, у 2023 р. – 622597,0 тис. грн, що на 168498,0 тис. грн або 37,1 % більше, у 2024 р. – 750752,0 тис. грн, що на 128155,0 тис. грн або 20,6 % більше.

Розглянемо і в розрізі складових операційних витрат.

Матеріальні витрати у 2020 р. склали 233928,0 тис. грн, у 2021 р. – 220142,0 тис. грн, що на 13786,0 тис. грн або 5,9 % менше, у 2022 р. – 131770,0 тис. грн, що на 88372,0 тис. грн або 40,1 % менше, у 2023 р. – 215160,0 тис. грн, що на 83390,0 тис. грн або 63,3 % більше, у 2024 р. – 198982,0 тис. грн, що на 16178,0 тис. грн або 7,5 % менше.

Витрати на оплату праці у 2020 р. склали 278298,0 тис. грн, у 2021 р. – 314883,0 тис. грн, що на 36585,0 тис. грн або 13,1 % більше, у 2022 р. – 194663,0 тис. грн, що на 120220,0 тис. грн або 32,2 % менше, у 2023 р. – 246265,0 тис. грн, що на 51602,0 тис. грн або 26,5 % більше, у 2024 р. – 280913,0 тис. грн, що на 34648,0 тис. грн або 14,1 % більше.

Відрахування на соціальні заходи у 2020 р. склали 61610,0 тис. грн, у 2021 р. – 69896,0 тис. грн, що на 8286,0 тис. грн або 13,4 % більше, у 2022 р. – 44782,0 тис. грн, що на 25114,0 тис. грн або 35,9 % менше, у 2023 р. – 53616,0 тис. грн, що на 8834,0 тис. грн або 19,7 % більше, у 2024 р. – 60837,0 тис. грн, що на 7221,0 тис. грн або 13,5 % більше.

Амортизаційні відрахування у 2020 р. склали 34343,0 тис. грн, у 2021 р. – 33523,0 тис. грн, що на 820,0 тис. грн або 2,4 % менше, у 2022 р. – 30355,0 тис. грн, що на 3168,0 тис. грн або 9,5 % менше, у 2023 р. – 28315,0 тис. грн, що на 2040,0 тис. грн або 6,7 % більше, у 2024 р. – 148167,0 тис. грн, що на 119852,0 тис. грн або в 5,2 рази більше.

Інші операційні витрати у 2020 р. склали 95786,0 тис. грн, у 2021 р. – 94455,0 тис. грн, що на 1331,0 тис. грн або 1,4 % менше, у 2022 р. – 52529,0 тис. грн, що на 41926,0 тис. грн або 44,4 % менше, у 2023 р. – 79241,0 тис. грн, що на 26712,0 тис. грн або 50,9 % більше, у 2024 р. – 61853,0 тис. грн, що на 17388,0 тис. грн або 21,9 % більше.

Дослідження структури операційних витрат дає змогу визначити складові,

що займають найбільшу частку у їх загальному обсязі (рисунк 2.7).

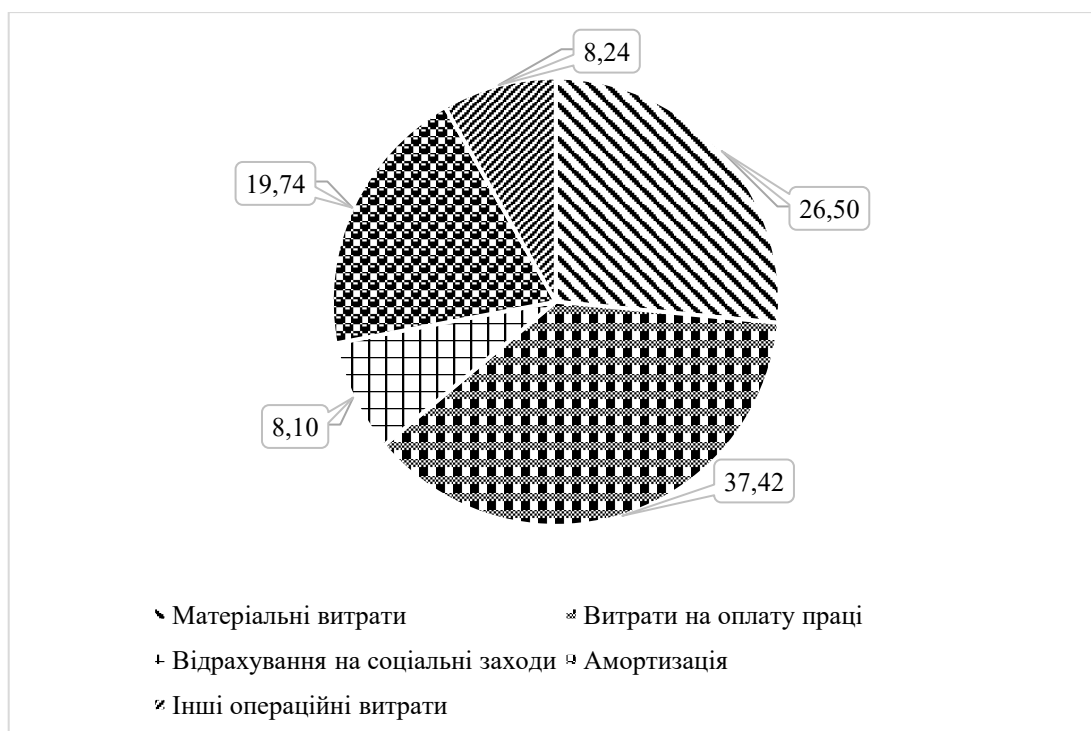


Рисунок 2.7 – Структура операційних витрат за елементами за 2024 р., %

Так, у 2024 році найбільшу частку в операційних витратах займають витрати на оплату праці – 37,42 %, що свідчить про високу трудомісткість діяльності та значну роль людського ресурсу у виробничому процесі. Другим за величиною елементом є матеріальні витрати – 26,50 %, які відображають витрати на сировину, паливно-мастильні матеріали, запасні частини та інші ресурси, необхідні для забезпечення роботи підприємства. Вагому частку становить амортизація – 19,74 %, що зумовлено потребою у відновленні та підтриманні основних засобів у належному стані. Відрахування на соціальні заходи складають 8,10 %, демонструючи виконання підприємством соціальних зобов’язань перед працівниками. Інші операційні витрати формують 8,24 %, охоплюючи витрати на комунальні послуги, охорону праці, навчання персоналу та інші супутні витрати. Таким чином, структура операційних витрат у 2024 році показує домінування витрат на оплату праці та матеріальних витрат, що визначає основні напрями впливу на собівартість продукції та послуг підприємства.

2.6 Аналіз фінансових результатів діяльності підприємства

Фінальним етапом аналізу діяльності підприємства є дослідження його фінансових результатів та фінансового стану, від правильності проведення якого залежить подальша ефективність роботи. Організація такого аналізу передбачає дотримання певних вимог: він має ґрунтуватися на сучасних наукових досягненнях і практичному досвіді, враховувати дію економічних законів у межах підприємства та здійснюватися за науково обґрунтованими методиками.

Основними завданнями аналізу фінансових результатів є: оцінка можливостей отримання прибутку з урахуванням ресурсного потенціалу та ринкової кон'юнктури; систематичний контроль за процесом формування прибутку та його динамікою; визначення впливу зовнішніх і внутрішніх чинників на фінансові показники та оцінка якості прибутку; пошук резервів для збільшення його обсягу та підвищення рівня рентабельності; аналіз ефективності використання можливостей зростання прибутковості; розробка рекомендацій щодо вдосконалення системи управління прибутком [48].

Аналіз фінансових результатів діяльності підприємства, а саме чистого доходу, собівартості, валового прибутку (збитку), фінансового результату від операційної діяльності, чистого фінансового результату подано в таблиці 2.6.

Щодо динаміки чистого доходу від реалізації продукції (товарів, робіт, послуг), то у 2020 р. його значення склало 742598,0 тис. грн, у 2021 р. – 770641,0 тис. грн, що на 28043,0 тис. грн або 3,8 % більше, у 2022 р. – 462287,0 тис. грн, що на 308354,0 тис. грн або 40,0 % менше, у 2023 р. – 627465,0 тис. грн, що на 165178,0 тис. грн або 35,7 % більше, у 2024 р. – 645910,0 тис. грн, що на 18445,0 тис. грн або 2,9 % більше.

Собівартість реалізованої продукції у 2020 р. склала 610289,0 тис. грн, у 2021 р. – 629113,0 тис. грн, що на 18824,0 тис. грн або 3,1 % більше, у 2022 р. – 389327,0 тис. грн, що на 239786,0 тис. грн або 38,1 % менше, у 2023 р. – 522933,0 тис. грн, що на 133606,0 тис. грн або 34,3 % більше, у 2024 р. –

642989,0 тис. грн, що на 120056,0 тис. грн або 23,0 % більше.

Таблиця 2.6 – Аналіз фінансових результатів діяльності підприємства

Показники	2020	2021	2022	2023	2024
1	2	3	4	5	6
Чистий дохід від реалізації продукції (товарів, робіт, послуг), тис. грн	742598,0	770641,0	462287,0	627465,0	645910,0
<i>абсолютне відхилення, тис. грн</i>	-	28043,0	-308354,0	165178,0	18445,0
<i>відносне відхилення, %</i>	-	103,8	60,0	135,7	102,9
Собівартість реалізованої продукції (товарів, робіт, послуг), тис. грн	610289,0	629113,0	389327,0	522933,0	642989,0
<i>абсолютне відхилення, тис. грн</i>	-	18824,0	-239786,0	133606,0	120056,0
<i>відносне відхилення, %</i>	-	103,1	61,9	134,3	123,0
Валовий прибуток (збиток), тис. грн	132309,0	141528,0	72960,0	104532,0	2921,0
<i>абсолютне відхилення, тис. грн</i>	-	9219,0	-68568,0	31572,0	-101611,0
<i>відносне відхилення, %</i>	-	107,0	51,6	143,3	2,8
Фінансовий результат від операційної діяльності, тис. грн	52005,0	52321,0	4090,0	8620,0	(143469,0)
<i>абсолютне відхилення, тис. грн</i>	-	316,0	-48231,0	4530,0	-152089,0
<i>відносне відхилення, %</i>	-	100,6	7,8	210,8	-
Чистий фінансовий результат: прибуток (збиток), тис. грн	41471,0	37844,0	8641,0	7990,0	(121966,0)

Продовження таблиці 2.6

1	2	3	4	5	6
<i>абсолютне відхилення, тис. грн</i>	-	-3627,0	-29203,0	-651,0	-129956,0
<i>відносне відхилення, %</i>	-	91,3	22,8	92,5	-

Динаміку показників, які відображають фінансові результати діяльності аналізованого підприємства, наведено на рисунку 2.8.

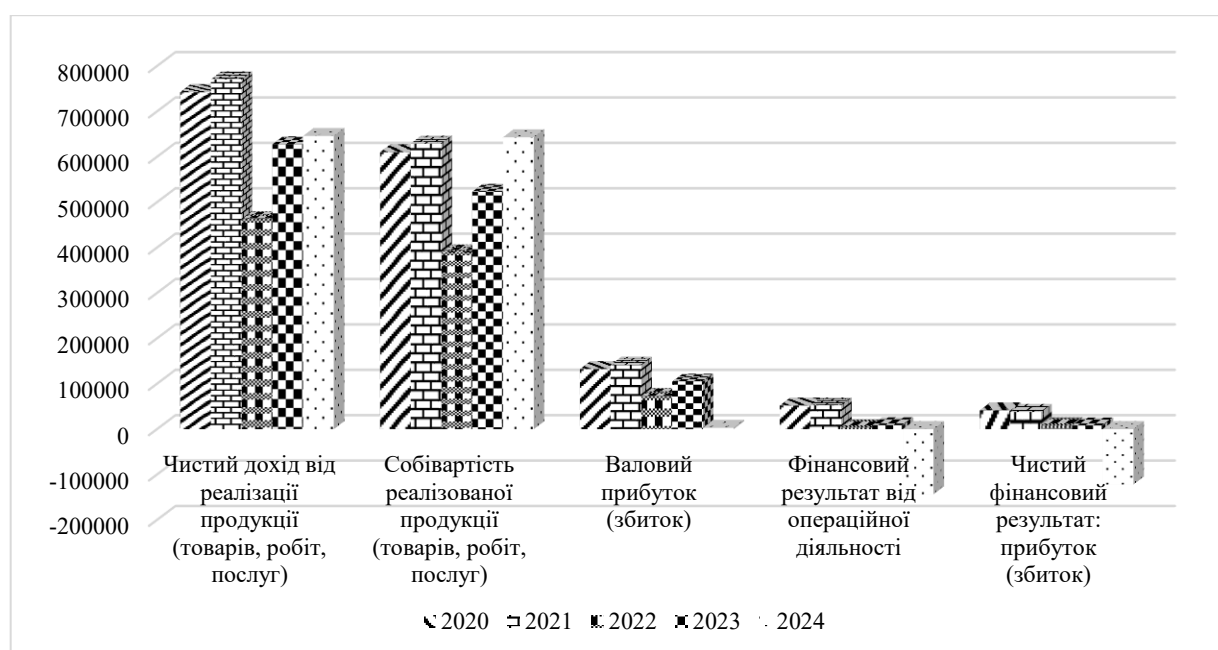


Рисунок 2.8 – Динаміка показників, що характеризують фінансові результати діяльності підприємства, тис. грн

Фінансовим результатом від операційної діяльності у 2020 р. був прибуток у розмірі 52005,0 тис. грн, у 2021 р. – 52321,0 тис. грн, що на 316,0 тис. грн або 0,6 % більше, у 2022 р. – 4090,0 тис. грн, що на 48231,0 тис. грн або 92,2 % менше, у 2023 р. – 8620,0 тис. грн, що на 4530,0 тис. грн або 110,8 % більше. Збитковим став 2024 р. – 143469,0 тис. грн, що на 152089,0 тис. грн менше.

Щодо чистого фінансового результату, то протягом 2020-2023 рр. підприємство здійснювало прибуткову діяльність: у 2020 р. прибуток склав 41471,0 тис. грн, у 2021 р. – 37844,0 тис. грн, що на 3627,0 тис. грн або 8,7 %

менше, у 2022 р. – 8641,0 тис. грн, що на 29203,0 тис. грн або 77,2 % менше, у 2023 р. – 7990,0 тис. грн, що на 651,0 тис. грн або 7,5 % менше. При цьому 2024 р. став збитковим – 121966,0 тис. грн, що на 129956,0 тис. грн менше.

2.7 Аналіз інвестиційної політики підприємства

ПрАТ «Київ-Дніпровське МППЗТ» приділяє значну увагу реалізації інвестиційної політики. Серед ключових стратегічних завдань розвитку підприємства визначено: нарощування обсягів вантажоперевезень, підвищення ефективності роботи, модернізацію та оновлення рухомого складу, створення безпечних і здорових умов праці, розвиток кадрового потенціалу, скорочення витрат на землю та впровадження цифрових технологій.

Для досягнення цих цілей компанія здійснює інвестиційну діяльність з основним акцентом на модернізації та оновленні основних фондів, що забезпечує економічну результативність. Важливим напрямом є вдосконалення системи ремонтного обслуговування шляхом залучення спеціалізованих організацій із багаторічним досвідом, власною матеріально-технічною базою та кваліфікованим персоналом для виконання капітальних і поточних ремонтів. Додаткові доходи планується отримувати завдяки відновленню технічних характеристик вагонного парку та його використанню. Також підприємство застосовує гнучкі механізми ціноутворення та вдосконалює технологію взаємодії з магістральним залізничним транспортом і споживачами послуг.

Аналіз капітальних інвестицій підприємства наведено у таблиці 2.7.

Загалом у 2020 р. капітальні інвестиції склали 31509,0 тис. грн, у 2021 р. – 20696,0 тис. грн, що на 10813,0 тис. грн або 34,3 % менше, у 2022 р. – 5063,0 тис. грн, що на 15633,0 тис. грн або 75,5 % менше, у 2023 р. – 10803,0 тис. грн, що на 5740,0 тис. грн або 113,4 % більше, у 2024 р. – 54553,0 тис. грн, що на 43750,0 тис. грн або в 5,1 рази більше. Тобто в останні роки спостерігається нестабільний

характер реалізації інвестиційної діяльності підприємством.

Таблиця 2.7 – Аналіз капітальних інвестицій підприємства

Показники	2020	2021	2022	2023	2024
Капітальні інвестиції, тис. грн, у т. ч.:	31509,0	20696,0	5063,0	10803,0	54553,0
<i>абсолютне відхилення, тис. грн</i>	-	-10813,0	-15633,0	5740,0	43750,0
<i>відносне відхилення, %</i>	-	65,7	24,5	213,4	505,0
Придбання (виготовлення) основних засобів, тис. грн	28844,0	16238,0	2363,0	9257,0	41773,0
<i>абсолютне відхилення, тис. грн</i>	-	-12606,0	-13875,0	6894,0	32516,0
<i>відносне відхилення, %</i>	-	56,3	14,6	391,7	451,3
Придбання (виготовлення) інших необоротних матеріальних активів, тис. грн	1110,0	2357,0	216,0	1546,0	4662,0
<i>абсолютне відхилення, тис. грн</i>	-	1247,0	-2141,0	1330,0	3116,0
<i>відносне відхилення, %</i>	-	212,3	9,2	715,7	301,6
Придбання (створення) нематеріальних активів, тис. грн	1432,0	2101,0	2484,0	-	3417,0
<i>абсолютне відхилення, тис. грн</i>	-	669,0	383,0	-2484,0	3417,0
<i>відносне відхилення, %</i>	-	146,7	118,2	-	-
Капітальне будівництво, тис. грн	123,0	-	-	-	4701,0
<i>абсолютне відхилення, тис. грн</i>	-	-123,0	-	-	4701,0
<i>відносне відхилення, %</i>	-	-	-	-	-

Витрати на придбання (виготовлення) основних засобів у 2020 р. склали 28844,0 тис. грн, у 2021 р. – 16238,0 тис. грн, що на 12606,0 тис. грн або 43,7 % менше, у 2022 р. – 2363,0 тис. грн, що на 13875,0 тис. грн або 85,4 % менше, у

2023 р. – 9257,0 тис. грн, що на 6894,0 тис. грн або 3,9 разів більше, у 2024 р. – 41773,0 тис. грн, що на 32516,0 тис. грн або 4,5 разів більше.

Витрати на придбання (виготовлення) інших необоротних матеріальних активів у 2020 р. склали 1110,0 тис. грн, у 2021 р. – 2357,0 тис. грн, що на 1247,0 тис. грн або в 112,3 % більше, у 2022 р. – 216,0 тис. грн, що на 2141,0 тис. грн або 90,8 % менше, у 2023 р. – 1546,0 тис. грн, що на 1330,0 тис. грн або в 7,2 рази більше, у 2024 р. – 4662,0 тис. грн, що на 3116,0 тис. грн або 3,1 рази більше.

Витрати на придбання (створення) нематеріальних активів у 2020 р. склали 1432,0 тис. грн, у 2021 р. – 2101,0 тис. грн, що на 609,0 тис. грн або на 46,7 % більше, у 2022 р. – 2484,0 тис. грн, що на 383,0 тис. грн або на 18,2 % більше, у 2023 р. не відбувалося придбання (створення) нематеріальних активів, у 2024 р. – 3417,0 тис. грн, що на 3417,0 тис. грн більше.

Витрати на капітальне будівництво були здійснені лише у 2020 р. і 2024 р. і склали 123,0 та 4701,0 тис. грн відповідно.

Подальші плани підприємства містять завдання щодо покращення інвестиційної політики і реалізації запланованих проєктів, спрямованих на підвищення конкурентоспроможності та стійкого розвитку.

Висновки до розділу 2

Проаналізовано діяльність приватного акціонерного товариства Київ – Дніпровське міжгалузеве підприємство промислового залізничного транспорту (ПрАТ «Київ – Дніпровське МППЗТ») – підприємства, що забезпечує взаємодію з магістральним залізничним транспортом загального користування через окремі регіональні філії Укрзалізниці та має примикання до її станцій. Метою діяльності підприємства є отримання прибутку на комерційній основі за рахунок ринкової діяльності і забезпечення на цій основі соціально-економічних потреб

суспільства та зростання добробуту працівників Товариства та його акціонерів.

Підприємство надає комплекс транспортних послуг щодо перевезення вантажів від станцій примикання до місць навантаження та вивантаження, виконання маневрових операцій, навантажувально-розвантажувальних робіт, будівництва та модернізації колійного господарства, метрологічних та інших послуг, пов'язаних з організацією вантажних перевезень залізничним транспортом. Аналіз динаміки обсягів роботи підприємства вказує на нестабільність обсягів перевезень вантажів. Зокрема у 2020 р. перевезено 21679,0 тис. т вантажів, у 2021 р. – 21306,3 тис. т вантажів, що на 372,7 тис. т або 1,7 % менше, у 2022 р. – 9212,0 тис. т вантажів, що на 12094,3 тис. т або 56,8 % менше (найбільш суттєве скорочення за аналізований період), у 2023 р. – 10104,0 тис. т вантажів, що на 892,0 тис. т або 9,7 % більше, у 2024 р. – 9737,0 тис. т вантажів, що на 367,0 тис. т або 3,6 % менше.

Щодо основних фондів підприємства, то експлуатаційний локомотивний парк складається з 119 тепловозів, з яких 78 тепловозів в роботі, 41 тепловоз знаходиться в ремонті, очікуванні ремонту або потребують списання. Власний вагонний парк вантажних вагонів нараховує 435 одиниць, з них 177 одиниць – вагони-думпкари, 31 – хопер-дозатор, 16 – напіввагони, службових вагонів – 5; для власних потреб – 84, під списання – 122. Для виконання вантажно-розвантажувальних та складських робіт Товариство має 63 крани на залізничному ходу, козлові крани, розвантажувачі, екскаватори; автомобільні та електронавантажувачі, бульдозери та іншу техніку.

Протягом 2020-2024 рр. спостерігається зростання вартості основних фондів: у 2020 р. їх первісна вартість склала 1134763,0 тис. грн, у 2021 р. – 1154617,0 тис. грн, що на 19854,0 тис. грн або 1,7 % більше, у 2022 р. – 1158831,0 тис. грн, що на 4214,0 тис. грн або 0,4 % більше, у 2023 р. – 1165063,0 тис. грн, що на 6232,0 тис. грн або 0,5 % більше, у 2024 р. – 12459674,0 тис. грн, що на 11294611,0 тис. грн або у 10,7 разів більше.

Оскільки темпи зносу основних фондів перевищували темпи приросту їх первісної вартості, ступінь їхнього фізичного зношення на підприємстві зростає:

у 2020 р. значення показника зносу склало склав 72,3 %, у 2021 р. – 73,1 %, що на 0,8 % більше, у 2022 р. – 75,4 %, що на 2,3 % більше, у 2023р. – 79,0 %, що на 3,6 % більше, у 2024 р. – 88,7 %, що на 9,7 % більше. У 2024 р. зафіксовано найвищий рівень зносу основних фондів підприємства за аналізований період – 88,7 %. Загалом рівень зносу на критичному рівні – не менше 70 %.

Динаміка показників оцінювання ефективності використання основних фондів була наступною. Фондовіддача основних фондів у 2020 р. склала 2,36 грн/грн, у 2021 р. – 2,48 грн/грн, що на 0,12 грн/грн або 5,1 % більше, у 2022 р. – 1,62 грн/грн, що на 0,86 грн/грн або 34,7 % менше, у 2023 р. – 2,57 грн/грн, що на 0,95 грн/грн або 58,6 % більше, у 2024 р. – 0,46 грн/грн, що на 2,11 грн/грн або 82,1 % менше. Погіршення фондовіддачі основних фондів зумовлено зниженням обсягів роботи підприємства, а у 2024 році ще додатково переоцінкою основних фондів підприємства.

Щодо чисельності працівників, то варто вказати на негативну тенденцію скорочення персоналу. У 2020 р. середньооблікова чисельність працівників склала 1795 осіб, у 2021 р. – 1901 осіб, що на 106 осіб або 5,9 % більше, у 2022 р. – 1603 осіб, що на 298 осіб або 15,7 % менше, у 2023 р. – 1308 осіб, що на 295 осіб або 18,4 % менше, у 2024 р. – 1271 особа, що на 37 осіб або 2,8 % менше. Розмір фонду оплати праці загалом збільшувався, лише у 2022 р. зафіксовано негативну зміну. У 2020 р. фонд оплати праці склав 278459,1 тис. грн, у 2021 р. – 314883,0 тис. грн, що на 36423,9 тис. грн або 13,1 % більше, у 2022 р. – 194663,0 тис. грн, що на 120220,0 тис. грн або 38,2 % менше, у 2023 р. – 246265,0 тис. грн, що на 51602,0 тис. грн або 26,5 % більше, у 2024 р. – 280913,0 тис. грн, що на 34648,0 тис. грн або 14,1 % більше.

Аналіз операційних витрат діяльності підприємства дозволяє дійти наступних висновків. У 2020 р. операційні витрати склали 703965,0 тис. грн, у 2021 р. – 732899,0 тис. грн, що на 28934,0 тис. грн або 4,1 % більше, у 2022 р. – 454099,0 тис. грн, що на 278800,0 тис. грн або 38,0 % менше, у 2023 р. – 622597,0 тис. грн, що на 168498,0 тис. грн або 37,1 % більше, у 2024 р. – 750752,0 тис. грн, що на 128155,0 тис. грн або 20,6 % більше.

Так, у 2024 році найбільшу частку в операційних витратах займають витрати на оплату праці – 37,42 %, що свідчить про високу трудомісткість діяльності та значну роль людського ресурсу у виробничому процесі. Другим за величиною елементом є матеріальні витрати – 26,50 %, які відображають витрати на сировину, паливно-мастильні матеріали, запасні частини та інші ресурси, необхідні для забезпечення роботи підприємства. Вагому частку становить амортизація – 19,74 %, що зумовлено потребою у відновленні та підтриманні основних засобів у належному стані.

Щодо динаміки чистого доходу від реалізації продукції (товарів, робіт, послуг), то у 2020 р. його значення склало 742598,0 тис. грн, у 2021 р. – 770641,0 тис. грн, що на 28043,0 тис. грн або 3,8 % більше, у 2022 р. – 462287,0 тис. грн, що на 308354,0 тис. грн або 40,0 % менше, у 2023 р. – 627465,0 тис. грн, що на 165178,0 тис. грн або 35,7 % більше, у 2024 р. – 645910,0 тис. грн, що на 18445,0 тис. грн або 2,9 % більше. Щодо чистого фінансового результату, то протягом 2020-2023 рр. підприємство здійснювало прибуткову діяльність: у 2020 р. прибуток склав 41471,0 тис. грн, у 2021 р. – 37844,0 тис. грн, що на 3627,0 тис. грн або 8,7 % менше, у 2022 р. – 8641,0 тис. грн, що на 29203,0 тис. грн або 77,2 % менше, у 2023 р. – 7990,0 тис. грн, що на 651,0 тис. грн або 7,5 % менше. При цьому 2024 р. став збитковим – 121966,0 тис. грн, що на 129956,0 тис. грн менше.

Загалом у 2020 р. капітальні інвестиції склали 31509,0 тис. грн, у 2021 р. – 20696,0 тис. грн, що на 10813,0 тис. грн або 34,3 % менше, у 2022 р. – 5063,0 тис. грн, що на 15633,0 тис. грн або 75,5 % менше, у 2023 р. – 10803,0 тис. грн, що на 5740,0 тис. грн або 113,4 % більше, у 2024 р. – 54553,0 тис. грн, що на 43750,0 тис. грн або в 5,1 рази більше. Тобто в останні роки спостерігається нестабільний характер реалізації інвестиційної діяльності підприємством.

Загалом можна зробити висновок про нестабільний характер діяльності аналізованого підприємства, на що вказує низка показників, і вплив низки негативних факторів на стабільність його функціонування.

3 Практичні рекомендації щодо забезпечення цифрової стійкості підприємств промислового залізничного транспорту

3.1 Роль людського фактору у забезпечення цифрової стійкості підприємств промислового залізничного транспорту

У сучасних умовах цифровізації та зростання кількості кіберінцидентів особливого значення набуває дослідження кіберзагроз підприємств критичної інфраструктури та оцінювання їх цифрової стійкості. Ключові загрози цифровій стійкості підприємства промислового залізничного транспорту включають кібернапади на ІТ-системи, людський фактор, технічні збої та зовнішні ризики, що можуть паралізувати роботу критичної інфраструктури. Людський фактор є однією з найслабших ланок у системі цифрової безпеки та стійкості підприємства. Оскільки навіть найдосконаліші технології не гарантують захисту, якщо співробітники не дотримуються правил або навмисно порушують їх.

Кібернапади на інформаційні системи передбачають атаки на системи управління рухом поїздів, диспетчерські центри та бази даних, використання шкідливого програмного забезпечення (віруси, трояни, ransomware), DDoS-атаки, що можуть призвести до зупинки сервісів, диспетчерських систем та хаосу у графіку руху. Технічні та інфраструктурні ризики виникають у результаті використання застарілого обладнання та програмного забезпечення, що не відповідає сучасним стандартам безпеки, відсутності резервних систем або слабкої системи відновлення після інцидентів, вразливості у системах автоматизації та телекомунікацій. Можуть виникати і зовнішні фактори: геополітичні ризики та цілеспрямовані атаки на критичну інфраструктуру держави; порушення постачання енергії чи інтернет-зв'язку, що впливають на цифрові системи; використання підприємства як «точки входу» для атак на ширшу транспортну мережу. Серед основних проявів людського фактору в цифровій безпеці та стійкості слід відзначити:

по-перше, помилки та недбалість, що передбачає використання слабких паролів, відкриття фішингових листів, зберігання конфіденційних даних у незахищених місцях. Так, співробітник міг відкрити лист із вкладенням і результатом стала компрометація всієї мережі;

по-друге, інсайдерські загрози, що включають навмисні дії співробітників (крадіжка даних, саботаж), використання службових прав для несанкціонованого доступу. Зокрема працівник міг продати базу клієнтів конкурентам;

по-третє, низька обізнаність, а саме відсутність знань про сучасні загрози, недостатня культура кібергігієни. Так, залишений незахищений ноутбук призвів до витоку конфіденційної інформації.

При вивченні впливу людського фактору в забезпеченні цифрової стійкості підприємства промислового залізничного транспорту слід враховувати і те, що в здійсненні перевезень і виконанні інших ключових завдань приймає участь експлуатаційний персонал (машиністи, диспетчери, ремонтні бригади), який має доступ до критичних систем управління рухом та їх дії напряду впливають на безпеку перевезень, IT-фахівці та інженери відповідають за підтримку цифрової інфраструктури, тому їхня компетентність у сфері кіберзахисту є вирішальною, менеджмент формує політику безпеки та інвестиційні пріоритети, що визначають рівень цифрової стійкості підприємства.

Як зазначено в дослідженні [49] хоча цифрова стійкість і відноситься до більш технічної сфери, але вона глибоко орієнтована на людину. Стійка система може відновитися після кібератаки, але саме люди, які стоять за системою, їхнє навчання, спосіб мислення та рішення, формують основу цієї стійкості. Зокрема автором вказано, що важливою є роль керівництва у підтримці стійкості. Керівники повинні підкреслювати її важливість, виділяти необхідні ресурси та просувати бачення стійкої організації, оскільки вони відповідають за створення середовища, де стійкість розглядається не лише як технічне рішення, а й як бізнес-імператив. Їхня проактивна участь демонструє відданість і заохочує організацію наслідувати цей приклад. Також, слід враховувати, що цифровий ландшафт швидко розвивається, що вимагає постійного навчання. Працівники

всіх рівнів повинні володіти навичками та знаннями для розпізнавання, повідомлення та реагування на потенційні загрози. Регулярні навчальні сесії, семінари та навчання можуть гарантувати, що персонал завжди буде на крок попереду, готовий до вирішення викликів. Вказано в дослідженні і про важливість залученості та відповідальності співробітників. Окрім обов'язкових навчальних сесій необхідно приділяти вагому увагу формуванню почуття відповідальності серед співробітників. Коли люди усвідомлюють, що відіграють важливу роль у підтримці цифрової стійкості компанії, вони з більшою ймовірністю будуть уважними, проактивними та залученими. Відкриті канали комунікації, де співробітники можуть повідомляти про вразливості або пропонувати покращення, можуть ще більше зміцнити захист. Культура, яка цінує адаптивність, постійне вдосконалення та колективну відповідальність, може значно підвищити рівень стійкості організації. Децентралізоване прийняття рішень, підкріплене навчанням та розумінням цифрових цілей бізнесу, може призвести до швидшого та ефективного реагування на загрози [49].

Отже, цифрова стійкість підприємства залізничного транспорту залежить від комплексного захисту – технічного, організаційного та кадрового. Технології можуть лише частково компенсувати ризики, але навчання, культура та мотивація персоналу є вирішальними для формування стійкої системи захисту.

Варто вказати, що керівництву компанії повинні зробити кілька наступних ключових кроків для побудови цифрової стійкості [50].

1 Важливо підвищити обізнаність ради директорів та керівництва. Хоча члени правління та керівники вищої ланки не мають бути технічними експертами в кібер- або цифровій сферах, але вони повинні мати глибоке розуміння принципів кібербезпеки, а також впливу та ризиків цифрових технологій. Це дозволить їм приймати обґрунтовані стратегічні рішення щодо підвищення цифрової стійкості.

2 Необхідно розглядати проекти з цифрової стійкості як один із ключових стратегічних інвестиційних пріоритетів. Важливо позиціонувати цифрову стійкість як стратегічний бізнес-імператив, щоб ресурси ефективно

розподілялися на впровадження передових технологій та навчання співробітників. Складні рішення щодо стратегічних компромісів у ресурсах та інвестиціях повинні прийматися на рівні ради директорів.

3 Варто побудувати сильне корпоративне управління. Важливо встановити політики та структури управління, щоб компанія могла дотримуватися законів про захист даних, галузевих стандартів та міжнародних норм у всіх географічних регіонах та юрисдикціях, де вона працює. Це допоможе уникнути юридичних санкцій або навіть кримінальної недбалості, особливо в юрисдикціях із суворішими законами.

4 Сприяти розвитку культури цифрової стійкості, підкреслюючи її важливість у всіх аспектах бізнесу, від розроблення продукту до практики співробітників. Жодна окрема людина чи команда не відповідає за розбудову цифрової стійкості, оскільки це вимагає залучення всіх співробітників. Мета полягає в тому, щоб розвивати в усіх співробітників установку на постійне врахування кібер- або цифрових ризиків у роботі.

5 Оцінка та управління кібер- та цифровими ризиками. Важливо оцінювати та керувати ризиками, пов'язаними з цифровою трансформацією та загрозами кібербезпеці, включаючи ті, що стосуються ланцюга поставок та третіх сторін. Ризики необхідно кількісно оцінити, щоб ефективно оцінити вплив інцидентів на бізнес з точки зору репутаційної, фінансової, юридичної та операційної шкоди. Рада директорів та керівництво повинні визначити поріг ризику компанії та встановити заходи щодо передачі, пом'якшення, уникнення та прийняття ризиків.

Отже, ключовим елементом забезпечення цифрової стійкості є персонал та рівень його компетентності, що підтверджує багато досліджень [49-57]. Рівень знань і навичок співробітників у сфері кібербезпеки прямо впливає на здатність підприємства протидіяти загрозам. Це проявляється у кількох вимірах:

1) технічна грамотність – вміння працювати з корпоративними системами без створення вразливостей, знання базових принципів кібергігієни (складні паролі, багатофакторна автентифікація, безпечне використання електронної

пошти), розуміння ризиків, пов'язаних із використанням зовнішніх носіїв та підключенням до незахищених мереж;

2) оперативна готовність – здатність швидко реагувати на підозрілі дії чи інциденти, вміння повідомляти про кіберінциденти відповідним службам без зволікань, навички роботи в умовах кризових ситуацій, коли цифрові системи можуть бути частково недоступні;

3) аналітичні навички – розпізнавання ознак фішингових атак, соціальної інженерії чи підроблених повідомлень, вміння оцінювати ризики при використанні нових програмних продуктів чи сервісів, здатність критично мислити щодо інформаційних потоків і перевіряти їхню достовірність;

4) культура безпеки – усвідомлення, що кожен працівник є «ланкою» у системі кіберзахисту, дотримання внутрішніх політик безпеки та процедур доступу, відповідальність за власні дії у цифровому середовищі.

При цьому слід звернути увагу і на моделі компетенцій персоналу у сфері кібербезпеки, яку можна використати для оцінювання цифрової стійкості підприємства промислового залізничного транспорту (таблиця 3.1).

Таблиця 3.1 – Моделі компетенцій персоналу у сфері кібербезпеки

Рівень	Характеристика знань і навичок	Приклади прояву
Базовий	Мінімальні знання про кібергігієну, дотримання простих правил безпеки	Використання складних паролів, уникання відкриття підозрілих листів
Середній	Розуміння основних кіберзагроз, здатність розпізнавати ризики	Виявлення фішингових повідомлень, повідомлення про інциденти керівництву
Просунутий	Глибокі технічні знання, здатність застосовувати інструменти захисту	Налаштування системи багатофакторної автентифікації, моніторинг мережових атак
Експертний	Стратегічне мислення, управління кіберризиками, розробка політик безпеки	Формування планів реагування на інциденти, керівництво командами з кіберзахисту

Якщо враховувати специфіку роботи підприємства промислового

залізничного транспорту, то таку матрицю компетенцій персоналу можна представити в розрізі ролей, які виконуються працівниками (рис. 3.1).

Роль працівника	Базові компетенції	Середні компетенції	Просунуті компетенції	Експертні компетенції
Диспетчер / оператор	Використання складних паролів, дотримання правил кібергігієни	Розпізнавання фішингових повідомлень, повідомлення про інциденти	Робота з системами моніторингу руху з урахуванням кіберризиків	Участь у розробці процедур реагування на інциденти
Інженер / ІТ-фахівець	Базові знання про захист даних та мереж	Налаштування антивірусних систем, резервне копіювання	Захист SCADA-систем, адміністрування мережевої безпеки	Розроблення політик кіберзахисту, управління інцидентами
Ремонтна бригада	Дотримання правил безпечного використання цифрових пристроїв	Усвідомлення ризиків при роботі з обладнанням	Використання захищених каналів зв'язку для технічних даних	Впровадження стандартів кібербезпеки у виробничі процеси
Керівництво / менеджмент	Розуміння важливості кібербезпеки	Контроль виконання базових політик безпеки	Планування інвестицій у цифрову стійкість	Формування стратегій кіберзахисту та управління ризиками

Рисунок 3.1 – Матриця компетенцій за ролями для підприємства промислового залізничного транспорту у сфері кібербезпеки

По-друге, слід звернути увагу на розвиток культури безпеки, що є не просто набором правил та інструкцій, а, насамперед, системою цінностей, переконань та поведінкових практик, які формують ставлення співробітників до цифрових ризиків. Така культура цифрової безпеки та стійкості визначає, наскільки працівники усвідомлюють їх роль у захисті інформаційних систем і наскільки відповідально діють у щоденній роботі. Тобто, працівники розуміють, що їхні дії можуть стати причиною кіберінциденту (усвідомленість), виконання політики безпеки для них не як формальність, а як частина робочої дисципліни (дотримання правил), кожен співробітник відчуває особисту причетність до

захисту підприємства (відповідальність), відкрито повідомляє про інциденти чи підозрілі дії без страху покарання (прозорість), проходить регулярні тренінги та практичні вправи, що закріплюють правильні звички (навчання).

Значна кількість досліджень присвячена саме інструментам формування та підтримки цифрової безпеки за рахунок розвитку кадрового потенціалу. Так, у дослідженні [63] йде мова про роль цифрових рішень у підтримці працівників у надзвичайних ситуаціях. Зокрема зазначено, що цифрові інструменти у сфері менеджменту відіграють ключову роль у розробці та реалізації планів дій на випадок надзвичайних ситуацій, а також у забезпеченні готовності персоналу оперативно реагувати на проблеми в екстрених умовах. Використання цифрових платформ дозволяє створювати та зберігати плани у електронному форматі, що значно спрощує доступ до необхідної документації та забезпечує можливість її оновлення в режимі реального часу. Електронні системи управління надають керівникам гнучкі можливості для редагування та коригування планів, враховуючи нові ризики та потенційні сценарії розвитку надзвичайних ситуацій. Цифрові технології також відкривають можливості для моделювання віртуальних сценаріїв навчання персоналу. Використання електронних тренажерів дозволяє працівникам занурюватися у максимально реалістичні умови та набувати практичних навичок реагування. Такі тренажери можуть охоплювати широкий спектр аспектів – від евакуації та надання першої допомоги до організації комунікації та відпрацювання стратегій поведінки.

Цифрові технології відіграють визначальну роль у процесі створення та управління резервними запасами й засобами захисту, що є ключовим елементом системи безпеки праці та готовності підприємств до надзвичайних ситуацій. Використання електронних платформ для управління запасами забезпечує автоматизацію процесів, дозволяє ефективно контролювати кількість і стан матеріальних ресурсів та своєчасно реагувати на їхнє зменшення. Системи автоматичного поповнення можуть бути налаштовані таким чином, щоб здійснювати замовлення необхідних матеріалів при досягненні критичного мінімуму, що гарантує постійну наявність засобів захисту та інших важливих

ресурсів. Цифрові системи моніторингу надають можливість відстежувати стан запасів у режимі реального часу, забезпечуючи керівництво оперативною інформацією для прийняття управлінських рішень. Аналітичні інструменти дозволяють визначати оптимальні рівні резервів та формувати стратегії їх ефективного використання, що мінімізує ризики дефіциту та надлишку. Крім того, цифрові платформи можуть застосовуватися для створення детальних планів екстреної готовності, які включають інвентаризацію запасів та засобів захисту. Електронні системи аудиту забезпечують регулярну перевірку стану резервів, їх відповідність стандартам безпеки та практичну дієвість, що підвищує рівень надійності та стійкості підприємства в умовах кризових викликів [63].

Цифрова компетентність фахівця, як зазначено в дослідженні – це складне, динамічне та інтегроване утворення особистості, яке відображає багаторівневу професійно-особистісну характеристику у сфері цифрових технологій та практичного досвіду їх застосування. Вона формується під впливом, з одного боку, потреб і вимог сучасного цифрового суспільства, а з іншого – появи цифрового освітнього простору, що трансформує навчально-виховну взаємодію між усіма його учасниками [64]. При цьому цифровий освітній простір вирізняється активним використанням мережі Інтернет, електронних систем зберігання та первинної систематизації даних, а також автоматизованих аналітичних платформ, побудованих на основі нейромереж і штучного інтелекту. Це створює умови для більш ефективного здійснення професійної діяльності, водночас висуваючи вимогу до постійного професійного саморозвитку та вдосконалення цифрових навичок [65].

У дослідженні [66] вченими розглядаються цифрові навички як комплекс умінь і компетенцій, що забезпечують впевнене, критичне та відповідальне використання інформаційно-комунікаційних технологій у процесі навчання, професійної діяльності та повсякденного життя в умовах цифрового суспільства. Вони формують основу цифрової грамотності особистості та визначають її здатність ефективно функціонувати в сучасному інформаційному середовищі. До складу цифрових навичок, на думку авторів, належать: інформаційна

грамотність – уміння знаходити, оцінювати та використовувати інформацію; медіаграмотність – здатність критично аналізувати медіаконтент та протидіяти дезінформації; опрацювання даних із використанням цифрових технологій – навички роботи з великими масивами даних, їх систематизації та аналізу; комунікація та співпраця – використання цифрових інструментів для ефективної взаємодії та командної роботи; створення цифрового контенту – уміння генерувати та розробляти матеріали, включаючи програмування та мультимедійні продукти; обізнаність у сфері інтелектуальної власності – розуміння правових аспектів використання та захисту цифрового контенту; вирішення проблем за допомогою цифрових технологій – застосування інноваційних інструментів для пошуку рішень у різних сферах діяльності; критичне мислення – здатність аналізувати інформацію, робити обґрунтовані висновки та приймати відповідальні рішення; інформаційна та кібербезпека – знання і навички захисту даних, особистої інформації та цифрових систем від загроз. Таким чином, як зазначають науковці, цифрові навички виступають базовим елементом професійної та особистісної компетентності, що забезпечує успішну інтеграцію людини у цифрове суспільство.

Отже, можна виділити наступні інструменти формування та підтримки цифрової безпеки, з акцентом на персоналі.

По-перше, програми мотивації, що включають: систему заохочень (бонуси чи відзнаки для працівників, які демонструють високий рівень дотримання політик безпеки); гейміфікація (внутрішні конкурси на найкращі практики кібергігієни (наприклад, «найскладніший пароль місяця»)); визнання на рівні колективу (публічне відзначення співробітників, які вчасно повідомили про інциденти чи уникнули ризиків).

По-друге, внутрішні комунікації, які передбачають: регулярні інформаційні бюлетені з прикладами актуальних кіберзагроз та порадами щодо їх уникнення; візуальні нагадування (плакати, інфографіки) у робочих приміщеннях про правила безпеки; кібербезпекові повідомлення у корпоративних месенджерах (короткі поради, що формують правильні звички).

По-третє, тренінги та навчання, що включають: обов'язкові курси з кібергігієни для всіх співробітників; симуляції атак (наприклад, фішингові кампанії) для перевірки готовності персоналу; рольові вправи (моделювання кризових ситуацій, де працівники відпрацьовують алгоритми реагування).

По-четверте, безпосередній приклад керівництва. Тобто лідери показують власну дисципліну у дотриманні правил безпеки, прозорість у прийнятті рішень щодо кіберзахисту, щоб працівники бачили важливість теми, проводять регулярні зустрічі з персоналом для обговорення ризиків та пропозицій щодо їх мінімізації.

По-п'яте, інтеграція у щоденну роботу шляхом автоматизованих нагадувань про зміну паролів чи оновлення програмного забезпечення, формування простих та зрозумілих інструкцій для кожної категорії працівників, включення безпеки у KPI (оцінка роботи з дотримання правил кіберзахисту).

Отже, культура безпеки формується не лише через навчання, а й через мотивацію, постійні нагадування та приклад керівництва. Це створює середовище, де кожен співробітник відчуває свою відповідальність за цифрову стійкість підприємства. Формування культури безпеки – це довгостроковий процес, який включає навчання, мотивацію, приклад керівництва та постійне нагадування про важливість цифрової стійкості. Вона знижує ймовірність випадкових помилок і недбалості, перетворюючи кожного співробітника на активного учасника системи кіберзахисту.

Для промислового залізничного транспорту формування культури цифрової безпеки сприяє зниженню ризику помилок диспетчерів та операторів, які працюють із критичними системами управління рухом, безпечній експлуатації обладнання ремонтними бригадами, що зменшує ймовірність інсайдерських загроз, підвищенню довіри клієнтів та партнерів, адже культура безпеки демонструє серйозне ставлення до захисту даних, стійкості до кризових ситуацій, персонал діє злагоджено та впевнено навіть під час кіберінцидентів.

Задля формування такої культури і формування відповідних навичок можна сформулювати практичні рекомендації для підвищення компетентності

різних груп працівників підприємства промислового залізничного транспорту у сфері кібербезпеки (рисунк 3.2):

– диспетчери та оператори – регулярні тренінги з кібергігієни (паролі, багатофакторна автентифікація, безпечна робота з електронною поштою), навчання розпізнаванню фішингових атак та соціальної інженерії, практичні заняття з реагування на інциденти у системах управління рухом;

Диспетчери та оператори	регулярні тренінги з кібергігієни (паролі, багатофакторна автентифікація, безпечна робота з електронною поштою)	навчання розпізнаванню фішингових атак та соціальної інженерії	практичні заняття з реагування на інциденти у системах управління рухом	
Інженери та IT-фахівці	курси з захисту SCADA-систем та промислових мереж; поглиблене навчання з адміністрування мережевої безпеки (firewall, IDS/IPS, VPN)	практика у створенні та тестуванні планів відновлення після інцидентів	участь у міжнародних сертифікаційних програмах	
Ремонтні бригади	ознайомлення з правилами безпечного використання цифрових пристроїв та мобільних додатків	навчання роботі з захищеними каналами зв'язку для передачі технічних даних	інструктаж щодо уникнення несанкціонованого підключення обладнання до корпоративних систем	
Керівництво та менеджмент	семінари з управління кіберризиками та стратегічного планування цифрової стійкості	ознайомлення з міжнародними стандартами	формування корпоративної культури безпеки через політики та мотиваційні програми	тренінги з прийняття рішень у кризових ситуаціях та інвестицій у кіберзахист

Рисунок 3.2 – Рекомендації для підвищення компетентності працівників підприємства промислового залізничного транспорту у сфері кібербезпеки

– інженери та IT-фахівці – курси з захисту SCADA-систем та промислових мереж; поглиблене навчання з адміністрування мережевої безпеки (firewall, IDS/IPS, VPN), практика у створенні та тестуванні планів відновлення після інцидентів, участь у міжнародних сертифікаційних програмах (наприклад, CEH, CISSP, CompTIA Security+);

– ремонтні бригади – ознайомлення з правилами безпечного використання

цифрових пристроїв та мобільних додатків, навчання роботі з захищеними каналами зв'язку для передачі технічних даних, інструктаж щодо уникнення несанкціонованого підключення обладнання до корпоративних систем;

– керівництво та менеджмент – семінари з управління кіберризиками та стратегічного планування цифрової стійкості, ознайомлення з міжнародними стандартами (ISO/IEC 27001, NIST Cybersecurity Framework), тренінги з прийняття рішень у кризових ситуаціях та інвестицій у кіберзахист, формування корпоративної культури безпеки через політики та мотиваційні програми.

Кожна група працівників має свою роль у забезпеченні цифрової стійкості: оператори – перша лінія захисту; IT-фахівці – технічний щит; ремонтні бригади – безпечна експлуатація обладнання; менеджмент – стратегічне бачення та інвестиції. Тому при забезпеченні цифрової безпеки та кіберстійкості необхідності приділяти увагу компетентностям всіх груп працівників.

3.2 Розроблення комплексної стратегії цифрової стійкості підприємства промислового залізничного транспорту

Розроблення комплексної стратегії цифрової стійкості підприємства загалом слід розпочинати з визначення ключових ризиків та можливостей у цифровому середовищі, аналізу поточного рівня цифрової зрілості підприємства та формування стратегічних цілей, спрямованих на забезпечення безперервності бізнес-процесів і захисту критично важливих даних.

Цифрова стійкість безпосередньо у сфері промислового залізничного транспорту означає здатність підприємства захищати критичні цифрові системи, адаптуватися до кіберзагроз та швидко відновлювати роботу після інцидентів, забезпечуючи безперервність перевезень і виробничих процесів.

Стратегія цифрової стійкості має будуватися на проактивному підході, який застосовують підприємства для пом'якшення впливу кіберзагроз та збоїв на

їх діяльність, дані та репутацію. Вона також включає впровадження комбінації технічних заходів контролю, навчання співробітників, планів реагування на інциденти та співпрацю з партнерами з кібербезпеки для зміцнення захисту та забезпечення безперервності бізнесу в умовах кібератак. Стратегія цифрової стійкості спрямована на побудову адаптивних та гнучких бізнес-процесів, які можуть ефективно протистояти кіберінцидентам та відновлюватися після них.

Ґрунтуючись на дослідженнях [67-74] можна виділити наступні умови та заходи для успішної реалізації стратегічних ініціатив з цифрової стійкості.

По-перше, одним із найефективніших способів підвищення цифрової стійкості є інвестування в навчання та освіту з кібербезпеки для співробітників. Необхідно забезпечити проведення регулярних навчальних сесій, спрямованих на ознайомлення персоналу з поширеними кіберзагрозами, фішинговими шахрайствами та найкращими практиками захисту даних. Надання співробітникам знань і навичок для виявлення та зменшення ризиків сприятиме формуванню культури обізнаності щодо кібербезпеки в усій організації.

По-друге, важливим є впровадження багаторівневих заходів безпеки. Надійна стратегія кібербезпеки повинна включати багаторівневі заходи захисту від різних типів кіберзагроз. Слід впроваджувати брандмауери, антивірусне програмне забезпечення, системи виявлення вторгнень та технології шифрування для захисту мережевої інфраструктури й конфіденційних даних. Крім того, необхідно розглянути можливість застосування багатофакторної автентифікації для додаткового рівня захисту облікових записів користувачів та запобігання несанкціонованому доступу.

По-третє, доцільно підтримувати актуальність програмного забезпечення та систем. Застаріле програмне забезпечення та системи часто є вразливими до кібератак через наявність відомих недоліків безпеки. Необхідно забезпечити регулярне оновлення всіх програмних додатків, операційних систем та мікропрограмного забезпечення останніми патчами й виправленнями. Слід встановити процес управління патчами для моніторингу оновлень та їх оперативного застосування, щоб мінімізувати ризик використання вразливостей

кіберзлочинцями.

По-четверте, слід звернути увагу на проведення регулярних аудитів безпеки та оцінок ризиків. Регулярні аудити безпеки та оцінки ризиків є важливими для виявлення слабких місць у бізнес-системах і процесах. Слід проводити комплексні оцінки для визначення потенційних прогалин у захисті, аналізу існуючих засобів контролю та встановлення пріоритетів щодо усунення недоліків. Завдяки проактивному управлінню ризиками цифрова стійкість підприємства може бути суттєво зміцнена, а ймовірність кібератак – зменшена.

По-п'яте, важливим є розроблення планів реагування на інциденти. Незважаючи на всі заходи щодо запобігання кібератакам, підприємство повинно бути готовим ефективно реагувати у випадку інциденту безпеки. Необхідно розробити плани реагування, які визначають ролі, обов'язки та процедури виявлення, стримування й пом'якшення кіберзагроз. Слід регулярно проводити навчальні тренування та симуляції для перевірки ефективності цих планів, щоб забезпечити готовність персоналу до реальних сценаріїв.

По-шосте, однією з ключових умов успішності заходів у сфері цифрової стійкості є сприяння співпраці з партнерами у сфері кібербезпеки. Співпраця з партнерами у сфері кібербезпеки, такими як постачальники керованих послуг безпеки (MSSP) або консультанти, може надати додаткову експертизу та ресурси для підвищення цифрової стійкості. Необхідно залучати авторитетні компанії для проведення оцінок безпеки, розроблення індивідуальних рішень та забезпечення постійної підтримки й моніторингу. Використання зовнішньої експертизи дозволяє зміцнити позиції підприємства в галузі кіберзахисту та випереджати нові загрози.

Зважаючи на комплексність поняття цифрової стійкості підприємства слід виділити її ключові компоненти з урахування специфіки галузі:

- 1) технічна стійкість – впровадження систем резервного копіювання даних; сегментація мереж; використання EDR/XDR для моніторингу станційних і диспетчерських систем;
- 2) організаційна стійкість – розроблення планів реагування на інциденти;

створення кризових протоколів для диспетчерських центрів; регулярні аудити безпеки;

3) людська стійкість – навчання персоналу кібергігієні; симуляції фішингових атак; тренінги для машиністів та диспетчерів щодо дій у разі кібератаки;

4) правова стійкість – дотримання національних законів («Про основні засади забезпечення кібербезпеки України», «Про захист персональних даних» тощо [3-5]); відповідність міжнародним стандартам ISO/IEC 27001;

5) економічна стійкість – планування бюджету на кіберзахист; оцінка вартості простоїв залізничних перевезень; страхування кіберризиків;

6) адаптивність та інноваційність – використання AI для моніторингу руху поїздів; блокчейн для захисту логістичних даних; гнучке оновлення політик безпеки тощо.

Для захисту цифрових активів і забезпечення цифрової безпеки підприємства науковцями запропоновано реалізовувати такі стратегії [74]:

- стратегія захисту даних – передбачає впровадження механізмів шифрування, регулярне створення резервних копій, а також використання інших технологій для збереження цілісності та конфіденційності інформації;

- стратегія кібербезпеки – базується на застосуванні сучасних систем захисту, антивірусного програмного забезпечення, а також постійному моніторингу та аналізі потенційних кіберзагроз;

- стратегія відновлення – включає розробку та тестування планів реагування на інциденти, впровадження рішень для швидкого відновлення даних і функціонування цифрової інфраструктури;

- стратегія нульової довіри – передбачає перехід до моделі безпеки, яка обмежує доступ до критично важливих застосунків, даних і внутрішнього середовища підприємства, незалежно від джерела запиту.

Наведені дослідження підкреслюють важливість забезпечення цифрової безпеки як на рівні окремої особистості, так і підприємства та держави. При цьому варто враховувати, що цифрова безпека ґрунтується на таких

фундаментальних принципах, які визначають якість захисту інформаційних систем, як [75]:

по-перше, конфіденційність, що означає здатність системи забезпечити доступ до інформації лише уповноваженим особам або процесам. Конфіденційність передбачає: захист персональних даних користувачів (наприклад, паспортні дані, медична інформація, фінансові реквізити); захист комерційної та службової інформації (бізнес-плани, внутрішні документи, технологічні розробки); використання шифрування, обмеження доступу, автентифікації та політик доступу (наприклад, система купівлі електронного квитку на залізниці повинна гарантувати, що дані пасажира не потраплять до сторонніх осіб;

по-друге, цілісність, яка передбачає, що дані залишаються точними, повними та незмінними без дозволу. Це важливо для запобігання несанкціонованому редагуванню або підробці інформації, виявлення змін у даних (наприклад, через контрольні суми або журнали змін), захисту баз даних, журналів подій, фінансових звітів. Наприклад, якщо особа, що здійснює протиправну діяльність у цифровому середовищі залізниці, зможе змінити розклад руху поїздів, система має зафіксувати, хто і коли вніс зміни;

по-третє, доступність, яка гарантує, що інформаційні ресурси та сервіси доступні користувачам у необхідний для них час. Це включає: захист від DDoS-атак, які можуть паралізувати роботу систем; резервне копіювання та аварійне відновлення; забезпечення стабільної роботи серверів, мереж і додатків. Тобто, наприклад, пасажир повинен мати змогу придбати квиток онлайн у будь-який час, без перебоїв у роботі сайту, незважаючи на кібератаки.

Для реалізації перелічених принципів цифрової безпеки на залізничному транспорті доцільно використовувати як технічні, так і організаційні та юридичні засоби та підходи. Серед технічних засобів ключовими є: антивірусне програмне забезпечення (виявляє та нейтралізує шкідливі програми); фаєрволи (мережеві екрани, які контролюють вхідний і вихідний трафік, блокуючи небезпечні запити); системи виявлення та запобігання вторгненням (IDS/IPS, що аналізують

поведінку в мережі та реагують на підозрілі дії); шифрування (забезпечує захист даних при передачі та зберіганні). Неможливо сформувати ефективну систему цифрової безпеки і без організаційних заходів, тобто управлінських та процедурних дій, які формують культуру безпеки: політики безпеки (внутрішні правила щодо доступу, зберігання та обробки даних); аудит безпеки (регулярна перевірка систем на відповідність стандартам і виявлення вразливостей); навчання персоналу (підвищення обізнаності працівників щодо кіберзагроз, фішингу, безпечного поводження з даними); план реагування на інциденти (алгоритм дій у разі порушення безпеки). Щодо юридичних аспектів цифрової безпеки, то вони регулюються законодавством і міжнародними стандартами: GDPR (регламент захисту персональних даних, що накладає обов'язки на організації щодо обробки даних в країнах ЄС); ISO/IEC 27001 (міжнародний стандарт управління інформаційною безпекою); українське законодавство (Закон України «Про захист персональних даних», нормативи Державної служби спеціального зв'язку та захисту інформації України, вимоги до критичної інфраструктури). Наприклад, АТ «Укрзалізниця» при обробці персональних даних пасажирів країн ЄС повинна дотримуватися вимог GDPR [76].

Отже, наразі цифрову безпеку можна розглядати як сукупність технологічних, організаційних та правових заходів, спрямованих на захист інформаційних систем, даних та об'єктів цифрової інфраструктури від несанкціонованого доступу, втрат, пошкоджень або зловмисного використання. Це охоплює захист персональних даних, конфіденційної інформації, цифрових пристроїв, мереж, програмного забезпечення та онлайн-сервісів. Тобто, на сучасному етапі встановити антивірусні програми чи системи захисту паролів вже недостатньо, цифрова безпека включає стратегії управління ризиками, реагування на інциденти, навчання користувачів, постійне вдосконалення захисних механізмів.

Значну роль у цифровій безпеці відіграє людський фактор, що зумовлено її значущістю у виконанні кожного процесу на підприємстві і забезпеченні його ефективного розвитку. Слід вказати і на те, що технічні засоби захисту часто

виявляються недостатніми без належної поведінки користувачів, оскільки саме люди (персонал та топ-менеджмент) приймають рішення, взаємодіють із системами, відкривають файли, переходять за посиланнями, і тим самим можуть як зміцнити, так і підірвати безпеку підприємства. Недостатня обізнаність щодо особливостей виникнення та протікання і масштабності наслідків кіберзагроз, нехтування правилами кібергігієни, використання слабких паролів або небезпечних пристроїв в цілому посилює вразливість підприємств, яку не завжди можна нейтралізувати технічними засобами. Тому ефективна система цифрової безпеки має включати не лише технології, а й культуру безпеки, навчання персоналу, тренінги, інтерактивні симуляції та інші заходи, що формують відповідальну поведінку в цифровому середовищі. Так, підприємства залізничного транспорту можуть щоквартально проводити навчання для персоналу щодо нових кіберзагроз, а також тестувати їх готовність через реалізацію інтерактивних симуляцій, зокрема щодо фішингових атак. Таке інвестування в обізнаність, навчання та створення культури безпеки підприємств галузі дозволить суттєво знизити ймовірність кіберінцидентів.

Зважаючи на зростаючу складність кіберзагроз та масштабність їх наслідків і еволюцію цифрових технологій, все більш активно використовуються проактивні, багаторівневі і адаптивні моделі захисту [75].

Одним із таких підходів є Zero Trust Architecture (принцип «нульової довіри»), який базується на припущенні, що жоден користувач, пристрій або система не повинні отримувати довіру за замовчуванням, навіть якщо знаходяться всередині корпоративної мережі. При цьому доступ має надаватися лише після ретельної перевірки ідентичності, контексту та рівня ризику. З огляду на це ключовими рисами такого підходу є: постійна верифікація користувачів і пристроїв; мінімізація прав доступу; сегментація мережі та контроль трафіку між зонами; моніторинг поведінки в реальному часі. Значним потенціалом володіє дана концепція і в аспекті застосування для підприємств залізничного транспорту, дозволяючи ізолювати системи управління рухом, обмежити доступ до SCADA-компонентів і зменшити ризик внутрішніх загроз.

Цікавою в контексті посилення цифрової безпеки підприємств залізничного транспорту є мультифакторна автентифікація (MFA), що передбачає підтвердження особи, вимагаючи щонайменше два незалежні фактори автентифікації з трьох можливих категорій: що користувач знає (пароль, PIN); що він має (смартфон, токен, смарт-карта), ким він є (біометричні дані: відбиток пальця, розпізнавання обличчя). Серед переваг такого підходу слід виділити значне зниження ризику компрометації облікових записів, ефективний захист від фішингу та крадіжки паролів, гнучкість у впровадженні. У контексті транспортної галузі MFA може бути критично важливою для захисту доступу до систем бронювання, диспетчерських панелей та внутрішніх порталів.

Бізнес-суб'єкти використовують і шифрування даних, перетворюючи їх у форму, недоступну для несанкціонованих осіб. У сучасних системах шифрування застосовується як на етапі зберігання, так і під час передачі. При цьому можуть застосовуватися різні типи шифрування: асиметричне (з відкритим ключем), яке використовується для захищеної передачі даних; симетричне, що ефективне для шифрування великих обсягів інформації; гібридне, яке передбачає поєднання симетричного та асиметричного шифрування; End-to-end (наскрізне або кінцеве), яке забезпечує, що лише відправник і отримувач мають доступ до вмісту повідомлення. Використання методу шифрування сприяє захисту персональних та фінансових даних, відповідає вимогам регуляторів (GDPR, ISO/IEC 27001, тощо), зменшує наслідки витоку даних. При цьому слід враховувати, що незважаючи на їх ефективність, вони не є абсолютно стійкими, їх можливо зламати за належної спрямованості та витрати ресурсів [71].

Із зростанням популярності хмарних технологій виникає потреба в специфічних підходах до захисту даних та сервісів у хмарі. Ключовими аспектами так званої «хмарної» безпеки є: контроль доступу до хмарних ресурсів; шифрування даних у хмарних сховищах; моніторинг активності та виявлення аномалій; резервне копіювання та відновлення після інцидентів; відповідність стандартам (SOC 2, ISO/IEC 27017, тощо). Однак, слід враховувати і певні виклики: розподілена відповідальність між провайдером і користувачем;

ризика неправильного налаштування доступу; потенційна залежність від сторонніх постачальників. Оскільки дедалі більше систем (аналітика трафіку, продаж квитків, відеоспостереження тощо) переміщуються в хмару для залізничного транспорту безпека таких середовищ є критично важливою.

Цікавим і перспективним для впровадження підходом до цифрової безпеки на підприємствах залізничного транспорту може стати вище розглянута концепція Zero Trust Architecture у поєднанні з цифровим моніторингом критичних об'єктів інфраструктури. Оскільки саме такий підхід дозволить врахувати специфіку залізничного транспорту, а саме: розгалуженість систем, мобільність об'єктів, високі вимоги до безперервності роботи і протидії сучасним кіберзагрозам. Реалізувати такий підхід у залізничній галузі можна шляхом ідентифікації користувачів і пристроїв через багатофакторну автентифікацію, сегментації мережі шляхом поділу на ізольовані зони (наприклад, системи управління рухом, білетні сервіси, внутрішній документообіг), контролю доступу на основі розподілу ролей (кожен співробітник має доступ лише до потрібних функцій), моніторингу та аналізу поведінки через виявлення аномалій у реальному часі.

Беручи до уваги той факт, що підприємства залізничного транспорту мають багато фізичних об'єктів (локомотиви, станції, депо), які можуть бути вразливими до атак через IoT-пристрої, SCADA-системи, слід посилити систему протидії кіберзагрозам цифровим моніторингом критичних об'єктів. Це можна практично втілити за рахунок встановлення цифрових сенсорів з захищеним каналом передачі даних, використання AI/ML для прогнозування інцидентів (перевантаження мережі чи спроби несанкціонованого доступу), інтеграції з підрозділом Держспецзв'язку CERT-UA для оперативного реагування на кіберінциденти. Також, можна застосовувати блокчейн-технології для захисту логістичних даних, резервні цифрові платформи для управління рухом у разі атаки. Для формування та розвитку культури цифрової стійкості доцільно впроваджувати гейміфікацію навчання з кібербезпеки для працівників.

Отже, можна виділити такі інструменти забезпечення цифрової стійкості

для промислового залізничного транспорту (таблиця 3.2):

Таблиця 3.2 – Інструменти забезпечення цифрової стійкості для промислового залізничного транспорту

Інструмент	Призначення	Особливості застосування у залізничному транспорті
SIEM (Security Information and Event Management)	Централізований збір та аналіз логів	Моніторинг диспетчерських центрів, серверів управління рухом поїздів, систем квиткового обліку
EDR/XDR (Endpoint/Extended Detection & Response)	Виявлення та реагування на загрози на робочих станціях і серверах	Захист комп'ютерів диспетчерів, серверів сигналізації та автоматизованих складів
Zero Trust-архітектура	Перевірка кожного доступу незалежно від статусу користувача	Контроль доступу до систем управління рухом та корпоративних баз даних
SOAR (Security Orchestration, Automation and Response)	Автоматизація реагування на інциденти	Автоматичне блокування акаунтів диспетчерів, ізоляція заражених сегментів мережі
Резервне копіювання та Disaster Recovery	Збереження та відновлення даних	Дублювання даних про рух поїздів, резервні сервери для диспетчерських центрів
UEBA (User and Entity Behavior Analytics)	Аналіз поведінки користувачів та систем	Контроль дій машиністів, диспетчерів та технічного персоналу для виявлення аномалій
Навчальні платформи з кібергігієни	Підвищення обізнаності персоналу	Регулярні тренінги для диспетчерів, машиністів, технічних працівників, симуляції фішингових атак

1) SIEM (Security Information and Event Management), призначені для централізованого збору та аналізу логів із різних систем. Особливістю застосування є моніторинг диспетчерських центрів, серверів управління рухом

поїздів, систем квиткового обліку. Перевагою такого інструменту є швидке виявлення аномалій у критичних процесах;

2) EDR/XDR (Endpoint/Extended Detection & Response), призначені для виявлення та реагування на загрози на робочих станціях і серверах. Особливістю застосування є захист комп'ютерів диспетчерів, серверів управління сигналізацією та автоматизованих систем складів. Перевагою такого рішення є локалізація атак до їх поширення на всю мережу;

3) Zero Trust-архітектура, призначена для перевірки кожного доступу незалежно від місця чи статусу користувача. Особливістю застосування є контроль доступу до систем управління рухом поїздів та корпоративних баз даних. Перевагою є мінімізація ризику інсайдерських загроз;

4) SOAR (Security Orchestration, Automation and Response), призначений для автоматизації реагування на інциденти. Особливістю застосування є автоматичне блокування акаунтів диспетчерів при підозрілих діях та ізоляція заражених сегментів мережі. Перевагою є висока швидкість реагування без участі людини;

5) системи резервного копіювання та Disaster Recovery, призначені для збереження даних та відновлення після інцидентів. Особливістю застосування є дублювання даних про рух поїздів та використання резервних серверів для диспетчерських центрів. Перевагою є забезпечення безперервності перевезень навіть після кібератаки;

6) UEBA (User and Entity Behavior Analytics), призначена для аналізу поведінки користувачів та систем з метою виявлення аномалій. Особливістю застосування є контроль дій машиністів, диспетчерів та технічного персоналу. Перевагою є можливість виявлення інсайдерських загроз та помилок персоналу;

7) кібергігієна та навчальні платформи, призначені для підвищення обізнаності персоналу. Особливістю застосування є регулярні тренінги для диспетчерів, машиністів та технічних працівників. Перевагою є формування культури відповідального ставлення до кібербезпеки.

Для підприємств промислового залізничного транспорту цифрова

стійкість забезпечується комплексним використанням інструментів, включно від SIEM та EDR/XDR до Zero Trust і SOAR. Оскільки особливістю галузі є критичність безперервності перевезень, тому ключовим стає резервування даних, автоматизація реагування та навчання персоналу.

Отже, на першому етапі розроблення та реалізації стратегії забезпечення цифрової стійкості підприємства промислового залізничного транспорту слід проаналізувати ризики шляхом ідентифікації критичних активів (системи управління рухом, диспетчерські центри, бази даних), оцінювання потенційних загроз (кібератаки, інсайдерські ризики, технічні збої), використання методик ISO 31000, NIST Risk Management Framework (рисунк 3.3).

На другому етапі йде вибір інструментів, а саме: SIEM для централізованого моніторингу; EDR/XDR для захисту робочих станцій і серверів; Zero Trust для контролю доступу; SOAR для автоматизації реагування; UEBA для аналізу поведінки персоналу; резервне копіювання та Disaster Recovery для безперервності перевезень.

Організаційні заходи є третім етапом, який включає розроблення планів реагування на інциденти (Incident Response Plan), планування безперервності бізнесу (Business Continuity Plan), впровадження кризових протоколів для диспетчерських центрів, регулярні аудити та тестування систем.

Четвертим етапом є навчання персоналу за рахунок проведення тренінгів з кібергігієни для диспетчерів, машиністів, технічних працівників, симуляцій фішингових атак, навчання діям у разі кібератаки чи збою систем, формування культури відповідальності за цифрову безпеку.

П'ятий етап – тестування та вдосконалення, що включає: проведення penetration-тестів для виявлення слабких місць; симуляції кризових ситуацій (tabletop exercises); оцінку ефективності інструментів та політик; внесення змін на основі результатів тестів.

Шостий етап – аудит та оцінка ефективності за рахунок використання KPI (RTO (Recovery Time Objective) – час відновлення після інциденту; RPO (Recovery Point Objective) – допустимий рівень втрати даних), оцінювання

кількості інцидентів та часу реагування, регулярних зовнішніх та внутрішніх аудитів, звітності перед керівництвом та державними органами.

Етап 1. Аналіз ризиків	Ідентифікація критичних активів (системи управління рухом, диспетчерські центри, бази даних). Оцінка потенційних загроз (кібератаки, інсайдерські ризики, технічні збої). Використання методик ISO 31000, NIST Risk Management Framework
Етап 2. Вибір інструментів	SIEM для централізованого моніторингу. EDR/XDR для захисту робочих станцій і серверів. Zero Trust для контролю доступу. SOAR для автоматизації реагування. UEBA для аналізу поведінки персоналу. Резервне копіювання та Disaster Recovery для безперервності перевезень
Етап 3. Організаційні заходи	Розроблення планів реагування на інциденти (Incident Response Plan). Планування безперервності бізнесу (Business Continuity Plan). Впровадження кризових протоколів для диспетчерських центрів, регулярні аудити та тестування систем
Етап 4. Навчання персоналу	Тренінги з кібергігієни для диспетчерів, машиністів, технічних працівників. Симуляції фішингових атак. Навчання діям у разі кібератаки чи збою систем. Формування культури відповідальності за цифрову безпеку
Етап 5. Тестування та вдосконалення	Проведення penetration-тестів для виявлення слабких місць. Симуляції кризових ситуацій (tabletop exercises). Оцінка ефективності інструментів та політик. Внесення змін на основі результатів тестів
Етап 6. Аудит та оцінка ефективності	Використання KPI: RTO (Recovery Time Objective) – час відновлення після інциденту; RPO (Recovery Point Objective) – допустимий рівень втрати даних; кількість інцидентів та час реагування. Регулярні зовнішні та внутрішні аудити. Звітність перед керівництвом та державними органами.

Базовий рівень (захист інфраструктури)		Операційний рівень (захист процесів)		HR-рівень (працівники)	
впровадження політики інформаційної безпеки для всіх працівників		резервне копіювання даних та план відновлення після інцидентів		навчання персоналу (тренінги з кібергігієни)	
використання антивірусних систем, фаєрволів та систем виявлення вторгнень		моніторинг ІТ інфраструктури в реальному часі		симуляції атак (перевірка готовності працівників реагувати на інциденти)	
сегментація мережі, тобто відокремлення критичних систем від офісних		управління доступом (багатофакторна автентифікація, рольові права доступу)		чіткі правила використання корпоративних пристроїв (USB носії, мобільні телефони)	
регулярне оновлення програмного забезпечення та патч менеджмент		аудит безпеки (регулярні перевірки систем та процесів)			

Інноваційний рівень (оцифрування процесів)	штучний інтелект для аналізу аномалій у поведінці систем	блокчейн рішень для захисту даних про вантажі та контракти	цифрові сертифікати та електронний документообіг для клієнтів	ІоТ моніторинг вагонів і локомотивів із захищеним каналом передачі даних
--	--	--	---	--

Рисунок 3.3 – Стратегія забезпечення цифрової стійкості підприємства промислового залізничного транспорту

Важливою складовою стратегії є формування багаторівневої системи, починаючи від базового і до інноваційного рівнів. Базовим рівнем є захист інфраструктури, що передбачає впровадження політики інформаційної безпеки для всіх працівників, використання антивірусних систем, фаєрволів та систем виявлення вторгнень (IDS/IPS), сегментацію мережі (відокремлення критичних систем (SCADA, управління рухом) від офісних), регулярне оновлення програмного забезпечення та патч менеджмент.

Операційний рівень – це захист процесів за рахунок резервного копіювання даних та плану відновлення після інцидентів (Disaster Recovery Plan), моніторингу IT інфраструктури в реальному часі (SIEM системи), управління доступом (багатофакторна автентифікація, рольові права доступу), аудит безпеки (регулярні перевірки систем та процесів).

HR-рівень (працівники), а саме: навчання персоналу (тренінги з кібергігієни (фішинг, соціальна інженерія)); симуляції атак (перевірка готовності працівників реагувати на інциденти); чіткі правила використання корпоративних пристроїв (USB носії, мобільні телефони).

Інноваційний рівень є забезпечуючим і включає оцифрування процесів шляхом використання штучного інтелекту для аналізу аномалій у поведінці систем, блокчейн рішень для захисту даних про вантажі та контракти, цифрових сертифікатів та електронного документообігу для клієнтів, IoT моніторинг вагонів і локомотивів із захищеним каналом передачі даних.

Щодо реалізації такої стратегії слід вказати, що почати слід з підготовки та аудиту (часовий вимір – 1-3 місяць), а саме провести аудит IT інфраструктури та виявити слабкі місця, розробити політику інформаційної безпеки (правила доступу, використання пристроїв, захист даних), сформувати команду з цифрової безпеки (HR, IT відділ, керівництво).

На другому етапі слід зосередитися на створенні базового рівня кіберзахисту (4-6 місяць). Необхідно встановити сучасні антивірусні системи, фаєрволи та IDS/IPS для виявлення вторгнень. Важливим завданням є проведення сегментації мережі, щоб критичні системи (SCADA, управління

рухом) були відокремлені від офісних. Також слід запровадити багатофакторну автентифікацію для доступу до корпоративних ресурсів та організувати резервне копіювання даних із планом відновлення після інцидентів.

На етапі операційної безпеки необхідно перейти до впровадження інструментів її забезпечення (7-12 місяць). Слід встановити SIEM систему для централізованого моніторингу подій та запустити план реагування на інциденти (Incident Response Plan). Важливо провести навчання персоналу з кібергігієни та організувати симуляції атак для перевірки готовності. Додатково слід забезпечити захист IoT-пристроїв, зокрема GPS-трекерів та датчиків вагонів.

Завершальний етап «Інноваційні рішення» передбачає інтеграцію сучасних технологій для підвищення цифрової стійкості (13-18 місяць). Необхідно використати AI-системи для аналізу аномалій у поведінці мережі, інтегрувати блокчейн-рішення для захисту даних про вантажі та контракти. Слід впровадити електронний документообіг та цифрові сертифікати для клієнтів, а також розробити мобільний додаток із безпечним каналом комунікації.

Відповідальними за реалізацію будуть як IT відділ (технічні рішення, моніторинг, так і керівництво (стратегія, бюджет, контроль), HR відділ (навчання персоналу), зовнішні консультанти (аудит і впровадження інноваційних рішень).

3.3 Формування культури кібергігієни на промисловому підприємстві залізничного транспорту

Важливою умовою успішної реалізації стратегії забезпечення цифрової стійкості промислового підприємств залізничного транспорту є формування культури кібергігієни, що має розпочинатися з визначення базових принципів безпечної роботи з цифровими системами, оцінки рівня обізнаності персоналу та розроблення внутрішніх політик, які регламентують використання інформаційних технологій у виробничих процесах. Якщо стратегія цифрової

стійкості описує комплекс заходів (технічних, організаційних, правових, економічних), то культура кібергігієни – це людський вимір стратегії, який забезпечує її практичну реалізацію. Вона може бути забезпечена за рахунок реалізації освітніх заходів (регулярні тренінги для диспетчерів, машиністів, технічних працівників; симуляції фішингових атак; курси з основ кібергігієни (паролі, MFA, безпечне використання пристроїв), впровадження політик мінімальних прав, контролю доступу до критичних систем, регулярних перевірок знань персоналу, формування корпоративної культури безпеки, мотивації співробітників дотримуватися правил, відкритої комунікації про інциденти без страху покарання тощо. З метою ефективної реалізації заходів слід розробити програму формування культури кібергігієни (рисунок 3.4). Це один із ключових елементів цифрової безпеки, адже навіть найсучасніші технології не будуть ефективними без правильної поведінки працівників.

Освітній компонент включає: регулярні тренінги та семінари для всіх працівників за тематикою фішингу, безпечного використання паролів, роботи з корпоративними пристроями, соціальної інженерії; мікро-навчання (короткі відео чи інструкції (5-10 хвилин) раз на місяць).

Практичні заходи включають: симуляції фішингових атак (перевірка готовності працівників розпізнавати небезпечні листи); вправи з реагування на інциденти: що робити, якщо виявлено підозрілий файл чи повідомлення; внутрішні конкурси: «Кращий кіберзахисник місяця» для мотивації.

Організаційна політика передбачає: впровадження політики паролів (мінімальна довжина, регулярна зміна, заборона використання однакових паролів); застосування правил використання USB-носіїв та мобільних пристроїв; впровадження чітких інструкцій для роботи з корпоративною поштою та документами.

Комунікація та культура включають: інформаційні кампанії (плакати, внутрішні розсилки, нагадування у корпоративних чатах); кібергігієна як частина корпоративної культури (включення теми безпеки у збори, наради, інструктажі); зворотний зв'язок (можливість повідомити про підозрілу

активність без страху покарання).

Формування культури кібергігієни – це довгостроковий захід, який поєднує навчання, практику та комунікацію, не потребуючи великих інвестицій, дає значний ефект у зниженні ризиків і підвищенні довіри клієнтів та партнерів.

У таблиці 3.3 подано орієнтовний річний план заходів із формування культури кібергігієни на промисловому підприємстві залізничного транспорту.

Таблиця 3.3 – Орієнтовний річний план заходів із формування культури кібергігієни на промисловому підприємстві залізничного транспорту

Період	Заходи	Результати
1	2	3
1-й квартал (січень-березень)		
Січень	стартова кампанія «Кібергігієна – наша безпека»	плакати, розсилки, інструктажі
Лютий	базовий тренінг для всіх працівників	паролі, фішинг, корпоративні пристрої
Березень	симуляція фішингової атаки та аналіз результатів	імітовані фішингові атаки, індивідуальні рекомендації
2-й квартал (квітень-червень)		
Квітень	відео уроки про безпечну роботу з поштою та файлами	короткі відео уроки (5 хв)
Травень	конкурс «Кращий кіберзахисник місяця» серед працівників	конкурс, подяки, подарунки
Червень	аудит використання USB носіїв та мобільних пристроїв, оновлення правил	практичні навички
3-й квартал (липень-вересень)		
Липень	тренінг для керівників підрозділів за тематикою: управління інцидентами, швидке реагування	знання
Серпень	симуляція атаки соціальної інженерії	дзвінки, повідомлення
Вересень	внутрішній семінар «Кібергігієна як частина корпоративної культури»	знання та практичні навички

Продовження таблиці 3.3

1	2	3
4-й квартал (жовтень-грудень)		
Жовтень	повторний тренінг для всіх працівників	оновлення знань, нові загрози
Листопад	інтеграція теми кібергігієни у щомісячні збори та інструктажі	оновлені правила
Грудень	підсумковий аудит та звіт про ефективність програми	кількість інцидентів, рівень обізнаності

Такий річний план дозволяє системно формувати культуру кібергігієни від базових знань до практичних навичок і корпоративної культури. Це сприятиме зменшенню кількості інцидентів, пов'язаних із людським фактором, підвищенню рівня обізнаності персоналу, формуванню стійкої корпоративної культури безпеки, де кожен працівник відчуває відповідальність.

Для ефективної реалізації таких заходів слід сформувати технічну можливість для їх впровадження, що може бути реалізовано в вигляді впровадження цифрового застосунку або програми для формування культури кібергігієни на промисловому підприємстві залізничного транспорту.

Такий цифровий застосунок повинен мати такі модулі:

- освітній модуль: короткі уроки та інтерактивні інструкції (5-10 хв); міні-тести після кожного уроку; сертифікати після завершення курсу;
- практичний модуль: симуляції фішингових атак (лист, SMS, дзвінок); вправи «знайди небезпечний елемент»; віртуальні тренажери реагування на інциденти;
- мотиваційний модуль: рейтинг працівників за рівнем кібергігієни; досягнення («Кіберзахисник місяця»); бонуси чи внутрішні нагороди;
- аналітичний модуль: звіти для керівництва (хто пройшов навчання, які теми засвоєні); індикатори «рівня кібергігієни» по підрозділах; виявлення слабких місць (наприклад, низькі результати у певному відділі) тощо.

Інтерфейс має бути простим та інтуїтивним (іконки, кольорові індикатори), доступна мобільна та веб-версія з будь-якого пристрою, інтегровані

push-нагадування («Зміни пароль», «Перевір пошту на фішинг») та чат-бот для швидких порад у реальному часі.

Розроблення цифрового застосунку для формування кібергігієни принесе підприємству відчутні економічні вигоди у вигляді зниження ризиків, оптимізації витрат та підвищення продуктивності (таблиця 3.4).

Таблиця 3.4 – Очікувані переваги впровадження цифрового застосунку для формування кібергігієни

Стаття витрат	Зміст	Очікуваний економічний ефект
Розроблення застосунку	Створення освітнього, практичного, мотиваційного та аналітичного модулів	Одноразові інвестиції, що забезпечують довгострокове використання; економія на зовнішніх тренінгах та консультаціях
Навчання персоналу	Проведення інтерактивних уроків, тестів, симуляцій	Зниження ймовірності успішних фішингових атак та інцидентів на 30-50%, економія коштів на відновлення
Підтримка та оновлення	Регулярне оновлення контенту, технічна підтримка	Постійна актуальність знань; зменшення витрат на ліквідацію наслідків нових загроз
Мотиваційні програми	Внутрішні бонуси, рейтинги, нагороди	Підвищення дисципліни та відповідальності персоналу; скорочення кількості помилок, що призводять до інцидентів
Аналітика та звітність	Звіти для керівництва, індикатори рівня кібергігієни	Оптимізація бюджету на кібербезпеку: інвестиції спрямовуються у слабкі місця, а не розпорошуються
Інтеграція у бізнес-процеси	Використання застосунку у щоденній роботі	Зменшення простоїв критичних систем; кожна година простою може коштувати десятки тисяч грн, що компенсується завдяки швидкому реагуванню

1 Зниження фінансових ризиків від кіберінцидентів: освітній модуль зменшує ймовірність успішних атак (фішинг, соціальна інженерія), що може зекономити підприємству значні кошти на відновлення після інцидентів. За оцінками міжнародних досліджень, середня вартість кіберінциденту для компанії середнього розміру може становити сотні тисяч доларів. Навчання персоналу дозволяє знизити ймовірність таких втрат на 30-50 %.

2 Оптимізація витрат на реагування та відновлення: практичний модуль (симуляції, тренажери) сформує навички швидкого реагування, що скорочує час простою систем. Кожна година простою критичних систем (наприклад, управління рухом чи логістика) може коштувати підприємству десятки тисяч гривень. Застосунок допомагає мінімізувати ці втрати.

3 Підвищення продуктивності та мотивації персоналу: мотиваційний модуль створює внутрішню конкуренцію та стимулює працівників дотримуватися правил кібергігієни. Це зменшує кількість помилок персоналу, які часто стають причиною інцидентів, і водночас підвищує загальну дисципліну та ефективність роботи.

4 Прозорість та управлінські переваги: аналітичний модуль забезпечує керівництво даними про рівень кібергігієни у різних підрозділах. Це дозволяє точково інвестувати у слабкі місця, а не витрачати ресурси на «загальні» заходи. Такий підхід оптимізує бюджет на кібербезпеку та підвищує рентабельність інвестицій.

5 Довгострокові економічні ефекти: формування культури кібергігієни знижує ризик штрафів та репутаційних втрат у випадку витоку даних. Підприємство отримує конкурентну перевагу, оскільки клієнти та партнери більше довіряють компанії, яка демонструє високий рівень цифрової стійкості. - Застосунок може масштабуватися на інші підрозділи чи дочірні компанії без значних додаткових витрат.

Отже, інвестиції у застосунок для формування кібергігієни є економічно доцільними, оскільки вони дозволяють зменшити прямі фінансові втрати від

кіберінцидентів, оптимізувати витрати на реагування, підвищити продуктивність персоналу та забезпечити довгострокову конкурентну перевагу підприємства.

Для повноцінного продукту (з усіма модулями: освітній, практичний, мотиваційний, аналітичний; мобільні додатки iOS/Android; інтеграція з корпоративними системами; масштабування на тисячі користувачів) витрати на розроблення складуть 1170,0 тис. грн (таблиця 3.6).

Таблиця 3.6 – Орієнтовні витрати на розроблення цифрового застосунку

Статті витрат	Значення, грн
1 Оплата праці команди розробки	720000
1.1 Backend-розробники (2 особи × 6 міс.)	240000
1.2 Frontend-розробники (2 особи × 6 міс.)	210000
1.3 UI/UX дизайнери (2 особи × 4 міс.)	80000
1.4 QA/тестувальники (2 особи × 4 міс.)	70000
1.5 DevOps/інженери інфраструктури	60000
1.6 Project Manager	60000
2 Інфраструктура (сервери, хмарні сервіси, ліцензії)	120000
3 Розроблення навчального контенту (курси, симуляції, тренажери)	150000
4 Маркетинг та впровадження	100000
5 Підтримка та оновлення (перший рік)	80000
Загалом витрати	1170000

Зважаючи на те, що кількість працівників склала 1271 особу (за даними 2024 р.), то впровадження такого цифрового продукту дозволить знизити ризик інцидентів та простоїв, економлячи від 100 до 250 грн/ос. на місяць (від 1,52 млн грн до 3,81 млн грн на рік залежно від сценарію).

У таблиці 3.7 наведено розрахунок економічного ефекту для трьох сценаріїв (песимістичний, базовий та оптимістичний).

Таблиця 3.7 – Ефективність реалізації запропонованих заходів (з урахуванням ставки дисконтування 20 % і витрат на обслуговування)

Показники	1 рік	2 рік	3 рік	4 рік	5 рік
Песимістичний сценарій					
Економія 100 грн/міс. – ефект з дисконтом, тис. грн	1520	1266	1055	880	733
Витрати з дисконтом (підтримка та обслуговування), тис. грн	1345	146	122	101	84
Чистий ефект, тис. грн	175	1120	933	779	649
Чистий ефект нарастаючим підсумком, тис. грн	175	1295	2228	3007	3656
Базовий сценарій					
Економія 150 грн/міс. – ефект з дисконтом, тис. грн	2290	1908	1590	1326	1103
Витрати з дисконтом (підтримка та обслуговування), тис. грн	1345	146	122	101	84
Чистий ефект, тис. грн	945	1762	1468	1225	1019
Чистий ефект нарастаючим підсумком, тис. грн	945	2707	4175	5400	6419
Оптимістичний сценарій					
Економія 250 грн/міс. – ефект з дисконтом, тис. грн	3813	3176	2645	2210	1838
Витрати з дисконтом (підтримка та обслуговування), тис. грн	1345	146	122	101	84
Чистий ефект, тис. грн	2468	3030	2523	2109	1754
Чистий ефект нарастаючим підсумком, тис. грн	2468	5498	8021	10130	11884

На рисунку 3.6 графічно відображено економічну ефективність проєкту.

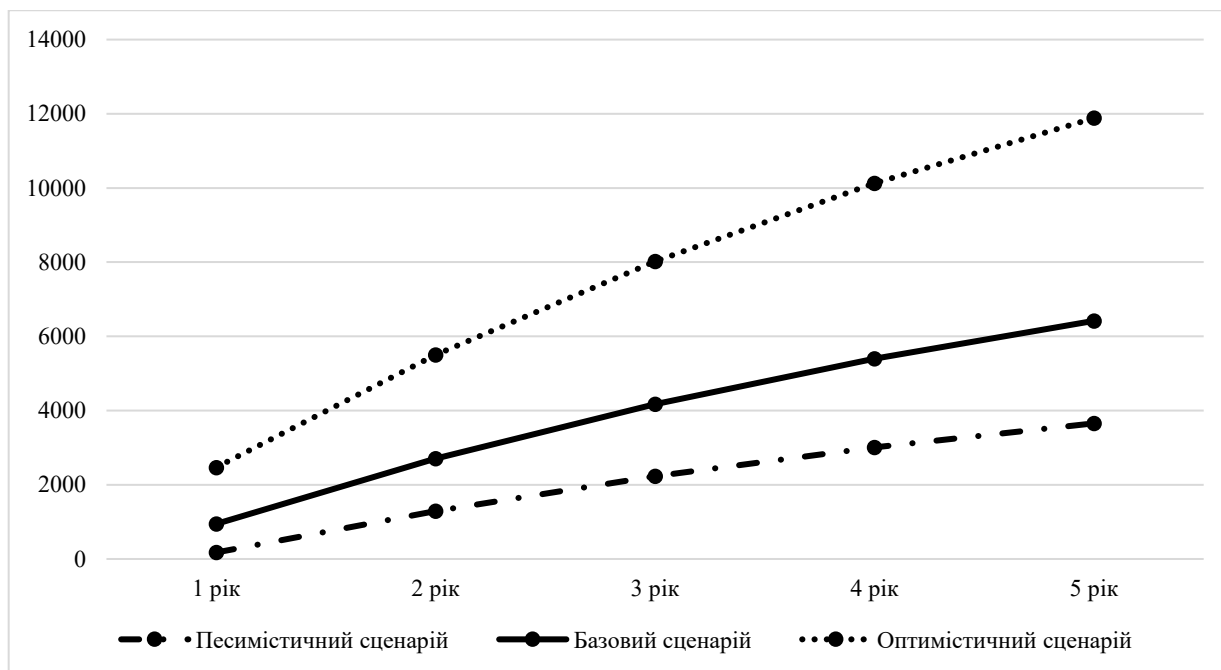


Рисунок 3.6 – Ефективність реалізації запропонованих заходів

Отже, окупність проекту спостерігається вже у перший рік у всіх трьох сценаріях. За умови економії 100 грн на працівника на місяць ефект є невеликим (близько 175 тис. грн) у перший рік, проте навіть цей варіант демонструє позитивний фінансовий результат. При економії 150 грн на працівника проект також виходить у плюс у перший рік, а вже у другому та третьому роках забезпечує значний приріст ефективності. Найбільш оптимістичний сценарій із економією 250 грн на працівника показує високу рентабельність із самого початку та формує максимальний довгостроковий ефект.

За п'ятирічний період чиста теперішня вартість становить приблизно 3,7 млн грн у песимістичному сценарії, 6,4 млн грн у базовому та 11,9 млн грн у оптимістичному. Це свідчить про те, що навіть за мінімальних припущень інвестиція у цифровий застосунок є економічно виправданою.

Витрати на щорічну підтримку та обслуговування помірно зменшують чистий ефект, однак не змінюють загального висновку: у всіх трьох сценаріях інвестиція залишається доцільною, а застосунок забезпечує стабільний економічний результат і довгострокову вигоду для підприємства.

Висновки до розділу 3

З'ясовано, що кібернапади на інформаційні системи передбачають атаки на системи управління рухом поїздів, диспетчерські центри та бази даних, використання шкідливого програмного забезпечення (віруси, трояни, ransomware), DDoS-атаки, що можуть призвести до зупинки сервісів, диспетчерських систем та хаосу у графіку руху. Технічні та інфраструктурні ризики виникають у результаті використання застарілого обладнання та програмного забезпечення, що не відповідає сучасним стандартам безпеки, відсутності резервних систем або слабкої системи відновлення після інцидентів, вразливості у системах автоматизації та телекомунікацій. Можуть виникати і зовнішні фактори: геополітичні ризики та цілеспрямовані атаки на критичну інфраструктуру держави; порушення постачання енергії чи інтернет-зв'язку, що впливають на цифрові системи; використання підприємства як «точки входу» для атак на ширшу транспортну мережу. Серед проявів людського фактору в цифровій безпеці та стійкості визначено: помилки та недбалість, що передбачає використання слабких паролів, відкриття фішингових листів, зберігання конфіденційних даних у незахищених місцях; інсайдерські загрози, що включають навмисні дії співробітників (крадіжка даних, саботаж), використання службових прав для несанкціонованого доступу; низька обізнаність, а саме відсутність знань про сучасні загрози, недостатня культура кібергігієни.

Розглянуто моделі компетенцій персоналу у сфері кібербезпеки за рівнями (базовий, середній, просунутий, експертний) і сформовано матрицю компетенцій за ролями для підприємства промислового залізничного транспорту у сфері кібербезпеки. Розроблено рекомендації для підвищення компетентності працівників підприємства промислового залізничного транспорту у сфері кібербезпеки у розрізі груп персоналу. Підкреслено, що кожна група працівників має свою роль у забезпеченні цифрової стійкості: оператори – перша лінія захисту; ІТ-фахівці – технічний щит; ремонтні бригади – безпечна експлуатація

обладнання; менеджмент – стратегічне бачення та інвестиції. Зазначено, що при забезпеченні цифрової безпеки та кіберстійкості необхідності приділяти увагу компетентностям всіх груп працівників.

Доведено доцільність розроблення комплексної стратегії цифрової стійкості підприємства промислового залізничного транспорту, що поетапно розкриває напрями, заходи та інструменти підтримки цифрової стійкості підприємств галузі. Визначено, що на першому етапі розроблення та реалізації стратегії забезпечення цифрової стійкості підприємства промислового залізничного транспорту слід проаналізувати ризики шляхом ідентифікації критичних активів, оцінювання потенційних загроз, використання методик ISO 31000, NIST Risk Management Framework. На другому етапі йде вибір інструментів. Організаційні заходи є третім етапом, який включає розроблення планів реагування на інциденти (Incident Response Plan), планування безперервності бізнесу (Business Continuity Plan), впровадження кризових протоколів для диспетчерських центрів, регулярні аудити та тестування систем. Четвертим етапом є навчання персоналу за рахунок проведення тренінгів з кібергігієни для диспетчерів, машиністів, технічних працівників, симуляцій фішингових атак, навчання діям у разі кібератаки чи збою систем, формування культури відповідальності за цифрову безпеку. П'ятий етап – тестування та вдосконалення, що включає: проведення penetration-тестів для виявлення слабких місць; симуляції кризових ситуацій (tabletop exercises); оцінку ефективності інструментів та політик; внесення змін на основі результатів тестів. Шостий етап – аудит та оцінка ефективності за рахунок використання KPI (RTO (Recovery Time Objective) – час відновлення після інциденту; RPO (Recovery Point Objective) – допустимий рівень втрати даних), оцінювання кількості інцидентів та часу реагування, регулярних зовнішніх та внутрішніх аудитів, звітності перед керівництвом та державними органами.

Визначено, що важливою складовою стратегії є формування багаторівневої системи, починаючи від базового і до інноваційного рівнів. Базовим рівнем є захист інфраструктури, що передбачає впровадження політики

інформаційної безпеки для всіх працівників, використання антивірусних систем, фаєрволів та систем виявлення вторгнень (IDS/IPS), сегментацію мережі (відокремлення критичних систем (SCADA, управління рухом) від офісних), регулярне оновлення програмного забезпечення та патч менеджмент. Операційний рівень – це захист процесів за рахунок резервного копіювання даних та плану відновлення після інцидентів (Disaster Recovery Plan), моніторингу ІТ інфраструктури в реальному часі (SIEM системи), управління доступом (багатофакторна автентифікація, рольові права доступу), аудит безпеки (регулярні перевірки систем та процесів). HR-рівень (працівники), а саме: навчання персоналу (тренінги з кібергігієни (фішинг, соціальна інженерія)); симуляції атак (перевірка готовності працівників реагувати на інциденти); чіткі правила використання корпоративних пристроїв (USB носії, мобільні телефони). Інноваційний рівень є забезпечуючим і включає оцифрування процесів шляхом використання штучного інтелекту для аналізу аномалій у поведінці систем, блокчейн рішень для захисту даних про вантажі та контракти, цифрових сертифікатів та електронного документообігу для клієнтів, IoT моніторинг вагонів і локомотивів із захищеним каналом передачі даних.

Обґрунтовано доцільність формування культури кібергігієни на промисловому підприємстві залізничного транспорту, що може бути реалізовано в вигляді впровадження цифрового застосунку або програми для формування культури кібергігієни на промисловому підприємстві залізничного транспорту. Запропоновано розроблення цифрового застосунку, що буде включати такі модулі як: освітній модуль (короткі уроки та та інтерактивні інструкції (5-10 хв); міні-тести після кожного уроку; сертифікати після завершення курсу); практичний модуль (симуляції фішингових атак (лист, SMS, дзвінок); вправи «знайди небезпечний елемент»; віртуальні тренажери реагування на інциденти); мотиваційний модуль (рейтинг працівників за рівнем кібергігієни; досягнення («Кіберзахисник місяця»); бонуси чи внутрішні нагороди); аналітичний модуль (звіти для керівництва (хто пройшов навчання, які теми засвоєні); індикатори «рівня кібергігієни» по підрозділах; виявлення слабких місць (наприклад, низькі

результати у певному відділі)) тощо. Розраховано орієнтовні витрати на розроблення цифрового застосунку і ефективність його створення та впровадження. З'ясовано, що окупність проєкту спостерігається вже у перший рік у всіх трьох сценаріях (песимістичний, базовий та оптимістичний). За умови економії 100 грн на працівника на місяць ефект є невеликим (близько 175 тис. грн) у перший рік, проте навіть цей варіант демонструє позитивний фінансовий результат. При економії 150 грн на працівника проєкт також виходить у плюс у перший рік, а вже у другому та третьому роках забезпечує значний приріст ефективності. Найбільш оптимістичний сценарій із економією 250 грн на працівника показує високу рентабельність із самого початку та формує максимальний довгостроковий ефект. За п'ятирічний період чиста теперішня вартість становить приблизно 3,7 млн грн у песимістичному сценарії, 6,4 млн грн у базовому та 11,9 млн грн у оптимістичному. Це свідчить про те, що навіть за мінімальних припущень інвестиція у цифровий застосунок є економічно виправданою. Витрати на щорічну підтримку та обслуговування помірно зменшують чистий ефект, однак не змінюють загального висновку: у всіх трьох сценаріях інвестиція залишається доцільною, а застосунок забезпечує стабільний економічний результат і довгострокову вигоду для підприємства.

Висновки

Досліджено аналітичні звіти щодо кіберзагроз як на світовому, так і національному рівнях, і встановлено, що щороку фіксується збільшення випадків несанкціонованого доступу, вірусних атак та DDoS-нападів. У 2024 році глобальні економічні втрати від них оцінювалися у понад 9 трлн дол., а у 2025 році прогнозуються вже на рівні 10,5 трлн дол. При таких річних витратах світ витрачає приблизно 333 тис. дол. на хвилину на кіберзлочинність. Розглянуто найпопулярніші типи кіберзлочинних атак протягом 2024-2025 рр., серед яких: фішинг та спуфінг; програми-вимагачі; компрометація ділової електронної пошти; шкідливе програмне забезпечення; крадіжка особистих даних / шахрайство; витоки даних. Проаналізовано наслідки кібератак у розрізі галузей економіки. Виділено ключові етапи розвитку кіберзагроз: початковий етап (1980-2000 рр.); етап комерціалізації (1980-2000 рр.); етап індустріалізації (2010-2017 рр.); етап ransomware та гібридних атак (2017 р і до сьогодні). Особливостями сучасного етапу є: види атак – шифрувальники, подвійне вимагання (зашифрувати та злити дані), атаки на OT/ICS, постачальницькі ланцюги; мотиви атак – великі викупи, дестабілізація критичної інфраструктури; тип захисту – Zero Trust, EDR/XDR, кіберстійкість, оркестрація реагування.

Вивчено еволюцію понять стійкості, цифрової та кібербезпеки і цифрової стійкості підприємств. Наведено порівняльну характеристику цифрової безпеки та стійкості. Запропоновано цифрову стійкість підприємства розглядати як здатність підприємства адаптуватися до цифрових загроз, протидіяти їм та швидко відновлюватися після інцидентів, зберігаючи безперервність ключових процесів. Серед компонентів цифрової стійкості підприємства виділено технічну, організаційну, людську, правову та регуляторну, економічну, адаптивну та інноваційну стійкість. Сформовано концепцію забезпечення цифрової стійкості підприємств, що розкриває принципи, напрями, завдання та інструменти, які дозволяють інтегрувати цифрові технології у бізнес-процеси,

формувати гнучкі управлінські стратегії, забезпечувати кібербезпеку та ефективне використання інформаційних ресурсів. Реалізація цієї концепції спрямована на підвищення рівня адаптивності підприємств до зовнішніх викликів, збереження конкурентних позицій на ринку та створення умов для довгострокового сталого розвитку в умовах глобальної цифрової трансформації.

Проаналізовано діяльність приватного акціонерного товариства Київ – Дніпровське міжгалузеве підприємство промислового залізничного транспорту (ПрАТ «Київ – Дніпровське МППЗТ») – підприємства, що забезпечує взаємодію з магістральним залізничним транспортом загального користування через окремі регіональні філії Укрзалізниці та має примикання до її станцій. Аналіз динаміки обсягів роботи підприємства вказує на нестабільність обсягів перевезень вантажів. Зокрема у 2020 р. перевезено 21679,0 тис. т вантажів, у 2021 р. – 21306,3 тис. т вантажів, що на 372,7 тис. т або 1,7 % менше, у 2022 р. – 9212,0 тис. т вантажів, що на 12094,3 тис. т або 56,8 % менше (найбільш суттєве скорочення за аналізований період), у 2023 р. – 10104,0 тис. т вантажів, що на 892,0 тис. т або 9,7 % більше, у 2024 р. – 9737,0 тис. т вантажів, що на 367,0 тис. т або 3,6 % менше. Аналіз операційних витрат діяльності підприємства дозволяє дійти наступних висновків. У 2020 р. операційні витрати склали 703965,0 тис. грн, у 2021 р. – 732899,0 тис. грн, що на 28934,0 тис. грн або 4,1 % більше, у 2022 р. – 454099,0 тис. грн, що на 278800,0 тис. грн або 38,0 % менше, у 2023 р. – 622597,0 тис. грн, що на 168498,0 тис. грн або 37,1 % більше, у 2024 р. – 750752,0 тис. грн, що на 128155,0 тис. грн або 20,6 % більше. Так, у 2024 році найбільшу частку в операційних витратах займають витрати на оплату праці – 37,42 %. Другим за величиною елементом є матеріальні витрати – 26,50 %. Щодо чистого фінансового результату, то протягом 2020-2023 рр. підприємство здійснювало прибуткову діяльність: у 2020 р. прибуток склав 41471,0 тис. грн, у 2021 р. – 37844,0 тис. грн, що на 3627,0 тис. грн або 8,7 % менше, у 2022 р. – 8641,0 тис. грн, що на 29203,0 тис. грн або 77,2 % менше, у 2023 р. – 7990,0 тис. грн, що на 651,0 тис. грн або 7,5 % менше. При цьому 2024 р. став збитковим – 121966,0 тис. грн, що на 129956,0 тис. грн менше.

Розглянуто моделі компетенцій персоналу у сфері кібербезпеки за рівнями (базовий, середній, просунутий, експертний) і сформовано матрицю компетенцій за ролями для підприємства промислового залізничного транспорту у сфері кібербезпеки. Розроблено рекомендації для підвищення компетентності працівників підприємства промислового залізничного транспорту у сфері кібербезпеки у розрізі груп персоналу. Підкреслено, що кожна група працівників має свою роль у забезпеченні цифрової стійкості: оператори – перша лінія захисту; IT-фахівці – технічний щит; ремонтні бригади – безпечна експлуатація обладнання; менеджмент – стратегічне бачення та інвестиції. Зазначено, що при забезпеченні цифрової безпеки та кіберстійкості необхідності приділяти увагу компетентностям всіх груп працівників.

Доведено доцільність розроблення комплексної стратегії цифрової стійкості підприємства промислового залізничного транспорту, що поетапно розкриває напрями, заходи та інструменти підтримки цифрової стійкості підприємств галузі. Визначено, що на першому етапі розроблення та реалізації стратегії забезпечення цифрової стійкості підприємства промислового залізничного транспорту слід проаналізувати ризики шляхом ідентифікації критичних активів, оцінювання потенційних загроз, використання методик. На другому етапі йде вибір інструментів. Організаційні заходи є третім етапом, який включає розроблення планів реагування на інциденти, планування безперервності бізнесу, впровадження кризових протоколів для диспетчерських центрів, регулярні аудити та тестування систем. Четвертим етапом є навчання персоналу за рахунок проведення тренінгів з кібергігієни для диспетчерів, машиністів, технічних працівників, симуляцій фішингових атак, навчання діям у разі кібератаки чи збою систем, формування культури відповідальності за цифрову безпеку. П'ятий етап – тестування та вдосконалення, що включає: проведення penetration-тестів для виявлення слабких місць; симуляції кризових ситуацій; оцінку ефективності інструментів та політик; внесення змін на основі результатів тестів. Шостий етап – аудит та оцінка ефективності за рахунок

використання KPI, оцінювання кількості інцидентів та часу реагування, регулярних зовнішніх та внутрішніх аудитів, звітності.

Обґрунтовано доцільність формування культури кібергігієни на промисловому підприємстві залізничного транспорту, що може бути реалізовано в вигляді впровадження цифрового застосунку або програми для формування культури кібергігієни на промисловому підприємстві залізничного транспорту. Запропоновано розроблення цифрового застосунку, що буде включати освітній, практичний, мотиваційний та аналітичний модулі. Розраховано орієнтовні витрати на розроблення цифрового застосунку і ефективність його створення та впровадження. З'ясовано, що окупність проєкту спостерігається вже у перший рік у всіх трьох сценаріях (песимістичний, базовий та оптимістичний). За умови економії 100 грн на працівника на місяць ефект є невеликим (близько 175 тис. грн) у перший рік, проте навіть цей варіант демонструє позитивний фінансовий результат. При економії 150 грн на працівника проєкт також виходить у плюс у перший рік, а вже у другому та третьому роках забезпечує значний приріст ефективності. Найбільш оптимістичний сценарій із економією 250 грн на працівника показує високу рентабельність із самого початку та формує максимальний довгостроковий ефект. За п'ятирічний період чиста теперішня вартість становить приблизно 3,7 млн грн у песимістичному сценарії, 6,4 млн грн у базовому та 11,9 млн грн у оптимістичному. Це свідчить, що інвестиція у цифровий застосунок є економічно виправданою.

Список використаних джерел

1 Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.2017 р. № 2163-VIII. *Законодавство України : вебсайт*. URL: <https://zakon.rada.gov.ua/laws/show/2163-19#Text> (дата звернення: 02.11.2025).

2 Про захист персональних даних: Закон України від 01.06.2010 р. № 2297-VI. *Законодавство України : вебсайт*. URL: <https://zakon.rada.gov.ua/laws/show/2297-17#Text> (дата звернення: 02.11.2025).

3 Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України»: Указ Президента України від 26.08.2021 р. № 447/2021. *Законодавство України : вебсайт*. URL: <https://zakon.rada.gov.ua/laws/show/447/2021#n12> (дата звернення: 02.11.2025).

4 Про затвердження плану заходів на 2025 рік з реалізації Стратегії кібербезпеки України : Розпорядження Кабінету Міністрів України від 07.03.2025 р. № 204-р. *Законодавство України : вебсайт*. URL: <https://zakon.rada.gov.ua/laws/show/204-2025-%D1%80#Text> (дата звернення: 02.11.2025).

5 Про затвердження Методичних рекомендацій щодо реагування суб'єктами забезпечення кібербезпеки на різні види подій у кіберпросторі: Наказ Адміністрації державної служби спеціального зв'язку та захисту інформації України від 03.07.2023 р. № 570. *Законодавство України : вебсайт*. URL: <https://zakon.rada.gov.ua/rada/show/v0570519-23#Text> (дата звернення: 08.11.2025).

6 Про затвердження переліку об'єктів державної власності, що мають стратегічне значення для економіки і безпеки держави: Постанова Кабінету Міністрів України від 04.03.2015 р. № 83. *Законодавство України : вебсайт*. URL: <https://zakon.rada.gov.ua/laws/show/83-2015-%D0%BF#Text> (дата звернення: 08.11.2025).

7 Про реорганізацію державних міжгалузевих підприємств промислового залізничного транспорту: Наказ Міністерства транспорту України від 25.01.2001 р. № 35. *Законодавство України : вебсайт*. URL: <https://zakon.rada.gov.ua/rada/show/v0035361-01#Text> (дата звернення: 12.10.2025).

8 Cybercrime To Cost The World \$12.2 Trillion Annually By 2031. *Cybersecurityventures.com : website*. URL: <https://cybersecurityventures.com/official-cybercrime-report-2025/> (accessed: 03.11.2025).

9 The cost of cybercrime statistics is projected to be \$10.5 trillion annually by 2025. *Deepstrike.io : website*. URL: <https://deepstrike.io/blog/cybercrime-statistics-2025> (accessed: 03.11.2025).

10 Global Cybersecurity Outlook 2025. *Reports.weforum.org : website*. URL: https://reports.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2025.pdf (accessed: 05.11.2025).

11 Огляд ринку кібербезпеки в Україні. Січень 2025. *Itukraine.org.ua : вебсайт*. URL: <https://itukraine.org.ua/files/Ukraine-Cybersec-Market-Review.pdf> (дата звернення: 15.11.2025).

12 Кузьменко О. Ю., Маклюк О. В. Кібербезпека бізнесу під час війни. *Економіка та суспільство*. 2022. Вип. 44. URL: <https://economyandsociety.in.ua/index.php/journal/article/view/1790> (дата звернення: 05.11.2025).

13 Білявська Ю., Шестак Я. Кібербезпека та кібергігієна: нова ера цифрових технологій. *Товари і ринки*. 2022. № 3. С. 47-59.

14 Ескалація кіберзагроз національним інтересам України та правові аспекти кіберзахисту: монографія / О. Д. Довгань, І. М. Доронін; НАПрН України, НДІП. Київ : Видавничий дім «АртЕк», 2017. 107 с.

15 Діордіца І. Класифікація кіберзагроз та їх легітимація у нормативно-правових актах України. Підприємництво, господарство і право. 2017. № 10. С. 206-211.

16 Шматок О. С., Фіненко Ю. І., Єлізаров А. Б., Телющенко В. А.

Класифікація загроз і ризиків сучасних інфокомунікаційних систем. *Вісник Університету «Україна»*. 2019. № 2 (23). С. С. 221-229.

17 Муравський В., Починок Н., Фаріон В. Класифікація кіберризиків у бухгалтерському обліку. *Вісник Економіки*. 2021. № 2. С. 129-144.

18 Євсєєв С. П., Рзаєв Х. Н., Мамедова Т. А., Ромашенко Н. В. Класифікатор кіберзагроз інформаційних ресурсів автоматизованих банківських систем. *Кібербезпека: освіта, наука, техніка*. 2018. № 2 (2). URL: <https://scispace.com/pdf/klasifikator-kiberzagroz-informatsiinih-resursiv-4t574ptc3q.pdf> (дата звернення: 10.11.2025).

19 Петренко Л. Цифрова безпека в структурі цифрової компетентності майбутнього викладача педагогічного закладу вищої освіти: змістовий компонент. *Освіта дорослих: теорія, досвід, перспективи*. 2023. Вип. 23 (1). С. 98-109.

20 Ріль А. О., Талабко О. Ю., Тимкевич М. Б., Хімяк Я. Г., Горб'як А. В. Механізм забезпечення безпеки підприємства у цифровій взаємодії з контрагентами. *Наукові записки Львівського університету бізнесу та права. Серія економічна. Серія юридична*. 2023. Вип. 38. С. 454-460.

21 Ткаченко О., Ткаченко К. Кіберпростір і кібербезпека: проблеми, перспективи, технології. *Цифрова платформа: інформаційні технології в соціокультурній сфері*. 2018. Вип. 1. С. 75-86.

22 Передерій Т. Стратегія цифрової безпеки підприємства як драйвер цифрової трансформації економіки України. *Вісник економічної науки України*. 2019. № 2 (37). С. 201-204.

23 Аванесова Н. Е., Мордовцев О. С., Колодяжна Т. В. Формування механізму комплексного забезпечення цифрової безпеки промислового підприємства України. *Вісник НТУ «ХПІ» (економічні науки)*. 2020. Вип. 3. С. 9-14.

24 Краус К., Краус Н., Штепа О. Цифрова трансформація кібербезпеки на мікрорівні в умовах воєнного стану. *Innovation and Sustainability*. 2022. № 3. С. 26-37.

25 Касьянова Н. В., Біличенко М. М., Севериненко А. О. Моделювання

цифрової безпеки підприємства. *Modern Economics*. 2023. № 39. С. 54-61.

26 Обрамич О. С. Особливості формування цифрової безпеки на підприємстві. *Економіка та суспільство*. 2024. Вип. 68. URL: <https://doi.org/10.32782/2524-0072/2024-68-20> (дата звернення: 17.11.2025).

27 Жегус О., Пахуча Е., Петріянчук К., Шиян Д. Особливості формування маркетингової стійкості підприємства в умовах сучасних викликів. *Вісник Хмельницького національного університету. Серія: Економічні науки*. 2024. № 328 (2). С. 121-125.

28 Стецяк О. Б. Поняття та зміст стійкості підприємств у цифровій економіці. *Здобутки економіки: перспективи та інновації*. 2025. № 14. URL: <https://doi.org/10.5281/zenodo.14963146> (дата звернення: 16.11.2025).

29 Голобородько А. Стратегія фінансової стійкості підприємств в умовах цифровізації. *Сталий розвиток економіки*. 2025. № 1 (52). С. 173-179.

30 Островецький В. М., Качмарський І. В. Особливості стратегічної стійкості підприємств в умовах цифрової економіки. *Вісник Східноукраїнського національного університету імені Володимира Даля*. 2025. № 3 (289). С. 48-53.

31 Слюсар В., Яблонська Н., Зайко Л., Панченко Н. Формування цифрової стійкості у підготовці фахівців з національної безпеки та вчителів «Захисту України». *Society and Security*. 2024. № 2-3 (3). С. 106-111.

32 Звіт Ради директорів приватного акціонерного товариства «Київ-Дніпровське міжгалузеве підприємство промислового залізничного транспорту» за 2024 рік. *Mppzt.com.ua* : вебсайт. URL: https://mppzt.com.ua/wp-content/uploads/2025/10/zvit_rady_dyrectoriv_2024.pdf (дата звернення: 15.10.2025).

33 Статут приватного акціонерного товариства «Київ-Дніпровське міжгалузеве підприємство промислового залізничного транспорту». *Mppzt.com.ua* : вебсайт. URL: https://mppzt.com.ua/wp-content/uploads/2024/04/Statut_2023.pdf (дата звернення: 15.10.2025).

34 Фінансова звітність за рік, що закінчився 31 грудня 2020 року ПрАТ «Київ – Дніпровське МППЗТ» та звіт незалежного аудитора.

Mppzt.com.ua : вебсайт. URL: <https://mppzt.com.ua/wp-content/uploads/2023/04/Audytorskyj-zvit-za-2020-rik.pdf> (дата звернення: 15.10.2025).

35 Фінансова звітність за рік, що закінчився 31 грудня 2021 року ПрАТ «Київ – Дніпровське МППЗТ» та звіт незалежного аудитора. *Mppzt.com.ua* : вебсайт. URL: <https://mppzt.com.ua/wp-content/uploads/2023/11/Audytorskyj-zvit-2021.pdf> (дата звернення: 15.10.2025).

36 Фінансова звітність за рік, що закінчився 31 грудня 2022 року ПрАТ «Київ – Дніпровське МППЗТ» та звіт незалежного аудитора. *Mppzt.com.ua* : вебсайт. URL: <https://mppzt.com.ua/wp-content/uploads/2023/09/Fin-zvit-2022.pdf> (дата звернення: 15.10.2025).

37 Фінансова звітність за рік, що закінчився 31 грудня 2023 року ПрАТ «Київ – Дніпровське МППЗТ» та звіт незалежного аудитора. *Mppzt.com.ua* : вебсайт. URL: [https://mppzt.com.ua/wp-content/uploads/2024/08/finzvit2023%20kdzt%20\(1\).pdf](https://mppzt.com.ua/wp-content/uploads/2024/08/finzvit2023%20kdzt%20(1).pdf) (дата звернення: 15.10.2025).

38 Річний звіт Приватного акціонерного товариства «Київ-Дніпровське міжгалузеве підприємство промислового залізничного транспорту» за 2024 рік. *Mppzt.com.ua* : вебсайт. URL: https://mppzt.com.ua/wp-content/uploads/2025/09/richnyi_zvit_2024.pdf (дата звернення: 15.10.2025).

39 Дикань В. Л., Воловельська І. В., Каличева Н. Є. Економіка підприємства : конспект лекцій. Частина 3. Харків : УкрДУЗТ, 2021. 49 с.

40 Дикань В. Л., Компанієць В. В., Назаренко І. Л. Техніко-економічний аналіз діяльності підприємств залізничного транспорту : підручник. Харків : УкрДАЗТ, 2013. 655 с.

41 Дикань В. Л., Воловельська І. В., Каличева Н. Є. Економіка підприємства : конспект лекцій. Частина 1. Харків : УкрДУЗТ, 2021. 55 с.

42 Дикань В. Л., Воловельська І. В., Каличева Н. Є. Економіка підприємства : конспект лекцій. Частина 2. Харків : УкрДУЗТ, 2021. 45 с.

43 Дикань В. Л., Єлагін Ю. В., Сухорукова Т. Г. Економіка праці на підприємствах залізничного транспорту : підручник. Харків: УкрДАЗТ, 2011.

225 с.

44 Богацька Н. М., Гендега А. А. Фактори впливу на трудові ресурси підприємства. *Ukrlogos.in.ua : вебсайт*. URL: <https://www.ukrlogos.in.ua/10.11232-2663-4139.16.31.html> (дата звернення: 20.10.2025).

45 Кравченко М. А. Аналіз ефективності використання трудових ресурсів на підприємстві. *Ефективна економіка*. 2010. № 5. URL: <http://www.economy.nayka.com.ua/?op=1&z=219> (дата звернення: 21.10.2025).

46 Фокін О. К. Загальні положення аналізу витрат виробництва промислового підприємства. *Економічний простір*. 2019. № 148. С. 144-156.

47 Кірдіна О. Г., Орлова В. М., Гапусенко Ю. І. Удосконалення організації обліку та управління експлуатаційними витратами на підприємствах залізничного транспорту. *Вісник економіки транспорту і промисловості*. 2023. № 84. С. 47-54.

48 Горбунова О. А. Основні завдання аналізу фінансових результатів діяльності підприємства. *Dspace.puet.edu.ua : вебсайт*. URL: <http://dspace.puet.edu.ua/bitstream/123456789/2685/1/3.1.pdf> (дата звернення: 20.10.2025).

49 Adapting and Thriving: The Role of Digital Resilience in Business Success. *ctrl-Disrupt.nl : website*. URL: <https://ctrl-disrupt.nl/adapting-and-thriving-the-role-of-digital-resilience-in-business-success> (accessed: 03.12.2025).

50 How can enterprises build digital resilience for trust? *Ey.com : website*. URL: https://www.ey.com/en_id/insights/consulting/how-can-enterprises-build-digital-resilience-for-trust (accessed: 03.12.2025).

51 Обруч Г. В., Броварник М. М., Сидорець Д. П. Розвиток людського капіталу підприємств залізничного транспорту в умовах цифрових змін. *Вісник економіки транспорту і промисловості*. 2024. № 88. С. 47-55.

52 Обруч Г. В. Особливості управління персоналом залізничного транспорту в умовах цифровізації. *Бізнес-навігатор*. 2019. Вип. 6.1-1 (56). С. 99-105.

53 Жернова Є. В. Стратегія управління персоналом підприємства в

цифровій економіці. *Вісник економіки транспорту і промисловості*. 2024. № 86. С. 209-219.

54 Жернова Є. В. Концептуальні положення управління персоналом на підприємствах в умовах цифровізації економіки. *Вісник економіки транспорту і промисловості*. 2023. № 83. С. 212-221.

55 Дикань В. Л., Скрипінський О. Л., Шевченко В. В. Кадрове забезпечення процесів розвитку ресурсного потенціалу підприємств залізничного транспорту. *Вісник економіки транспорту і промисловості*. 2024. № 87. С. 9-19.

56 Дикань В. Л., Остапук Б. Б., Кас'ян С. Б. Управління людським капіталом як складовою ресурсного потенціалу підприємств. *Вісник економіки транспорту і промисловості*. 2024. № 88. С. 7-17.

57 Токмакова І. В., Корінь М. В., Полозов А. Є., Авагімова В. А. Кадрове забезпечення інноваційно-цифрової модернізації підприємств. *Вісник економіки транспорту і промисловості*. 2024. № 86. С. 276-286.

58 Каличева Н. Є., Обруч Г. В., Калашнік Д. М. Організаційно-економічні аспекти управління трудовим потенціалом малих підприємств. *Розвиток методів управління та господарювання на транспорті*. 2025. № 2 (91). С. 179-189.

59 Косінцева П. Ю. Забезпечення розвитку людського капіталу підприємств залізничного транспорту в умовах цифровізації : дис. ...д-ра філософії : 051 – Економіка; галузь знань 05 – Соціальні та поведінкові науки / Косінцева Поліна Юріївна. Харків, 2025. 310 с.

60 Гринько Т., Гвініашвілі Т., Каліберда М. Стратегічне управління підприємством в умовах цифрової економіки. *Економіка та суспільство*. 2023. Вип. 50. URL: <https://doi.org/10.32782/2524-0072/2023-50-71> (дата звернення: 21.11.2025).

61 Міщенко В. І. Забезпечення стійкості кадрового потенціалу підприємства в умовах цифровізації. *Економічний простір*. 2022. № 182. С. 93-100.

62 Власенко Т. А. Управління персоналом підприємства в умовах

цифрової економіки: чинники ефективності та особливості забезпечення. *Український журнал прикладної економіки та техніки*. 2024. Т. 9. № 3. С. 270-274.

63 Кубатко О. В., Калініченко Л. Л., Бурлакова І. М., Дудка М. А., Михайлов С. О. Цифрові трансформації в безпеці персоналу підприємств при надзвичайних ситуаціях. *Приазовський економічний вісник*. 2025. Вип. 1 (41) . URL: http://rev.kpu.zp.ua/journals/2025/1_41_ukr/9.pdf (дата звернення: 06.12.2025).

64 Опис цифрової компетентності педагогічного працівника : електронне наукове фахове видання «Відкрите освітнє е-середовище сучасного університету» / Н. Морзе та ін. URL: <https://doi.org/10.28925/2414-0325.2019s39> (дата звернення: 06.12.2025).

65 Городянська Л. В. Роль цифрової компетентності фахівця у сфері кібербезпеки в умовах воєнних загроз. Формування компетентностей обдарованої особистості в системі позашкільної та вищої освіти. 2023. № 1. С. 210-217.

66 Деркаченко Я. А., Дзюба Т. М. Забезпечення кіберстійкості України за сучасних умов: цифрові навички та компетентності. *Зв'язок*. 2021. № 3. С. 12-16.

67 Strengthening Your Business's Digital Resilience: Practical Strategies for Success. *Mindquest.io* : website. URL: <https://mindquest.io/en/blog/news/9562/strengthening-your-business8217s-digital-resilience-practical-strategies-for-success> (accessed: 03.12.2025).

68 10 Tips for Creating a Cyber Resilience Strategy. *Cybeready.com* : website. URL: <https://cybeready.com/creating-a-cyber-resilience-strategy/> (accessed: 10.12.2025).

69 Achieving Digital Resilience: Key Strategies for Modern Enterprises. *Tuxcare.com* : website. URL: <https://tuxcare.com/blog/digital-resilience/> (accessed: 10.12.2025).

70 How to Improve Your Digital Resilience. *Mightybytes.com* : website. URL: <https://www.mightybytes.com/insights/digital-resilience/> (accessed: 10.12.2025).

71 Strategies for digital resilience to navigate increasing uncertainty. *Strategyand.pwc.com* : website. URL: <https://www.strategyand.pwc.com/de/en/functions/digital/strategies-for-digital-resilience.html> (accessed: 15.12.2025).

72 What is digital resilience? Definition, strategy and use cases. *Techtarget.com* : website. URL: <https://www.techtarget.com/searchdatabackup/definition/What-is-digital-resilience> (accessed: 15.12.2025).

73 Building and Implementing Cyber Resilience Strategies. *Cacm.acm.org* : website. URL: <https://cacm.acm.org/blogcacm/building-and-implementing-cyber-resilience-strategies/> (accessed: 16.12.2025).

74 Шостак Л., Федонюк А., Помазун О. Кібербезпека в системі формування бізнес-моделі підприємства в умовах цифрової економіки. *Економіка та суспільство*. 2024. Вип. 64. URL: <https://economyandsociety.in.ua/index.php/journal/article/view/4240/4166> (дата звернення: 15.12.2025).

75 Обруч Г. В., Челомбітько М. Д., Погребняк С. Р. Забезпечення цифрової безпеки підприємств залізничного транспорту в умовах посилення кібератак. *Інвестиції: практика та досвід*. 2025. № 21. С. 109-114.

76 Obruch H. V., Chelombitko M. D., Pohrebniak S. R. The role of digital security in ensuring the stability of the activities of railway transport enterprises. *Економіко-правове та фінансово-облікове забезпечення сталого розвитку : сучасні виклики та тренди* : тези доп. Міжнар. наук.-практ. конф. (м. Вінниця, 21 листоп. 2025 р.). Вінниця : ХНУВС, 2025. С. 23-25.

77 Методичні вказівки до виконання кваліфікаційної роботи для здобувачів вищої освіти другого (магістерського) рівня спеціальності 076 «Підприємництво та торгівля» / укладачі : В. Л. Дикань, Н. Є. Каличева, І. Л. Назаренко. Харків : УкрДУЗТ, 2023. 62 с.

78 Студентська навчальна звітність. Текстова частина (пояснювальна записка). Загальні вимоги до побудови, викладення та оформлення: метод. посіб. з додержання вимог нормоконтролю у студент. навч. звітності / Козар Л. М. та ін.; за заг. ред. Л. М. Козара. Харків: УкрДУЗТ, 2018. 54 с.

АКТ

перевірки випускної кваліфікаційної роботи на наявність ознак академічного плагіату

Відповідно до даних сервісу Strikeplagiarism.com кваліфікаційна робота на тему: «Формування цифрової стійкості підприємств залізничного транспорту в умовах загострення кіберзагроз»
автора: ПОГРЕБНЯК Сергій Романович
(ІПБ автора повністю)

містить 1,72 % запозичень. Ознаки академічного плагіату – відсутні.

Перевірку виконала
професор кафедри економіки та управління
виробничим і комерційним бізнесом



(підпис)

Ганна ОБРУЧ

14.12.2025 р.