

Український державний університет залізничного транспорту

Кафедра економіки та управління виробничим і комерційним бізнесом

АНТИКРИЗОВЕ УПРАВЛІННЯ ПІДПРИЄМСТВАМИ ЗАЛІЗНИЧНОГО
ТРАНСПОРТУ

Пояснювальна записка і розрахунки
до кваліфікаційної роботи

МРЕ.129.02.06 ПЗ

Розробив: студент 2 курсу, групи 213-ЕП-322
спеціальності 051 Економіка»
(роботу виконано самостійно, відповідно до
принципів академічної доброчесності)

_____ Едуард КРІЩИН
(підпис)

Керівник: професор, д-р екон. наук
Володимир ДИКАНЬ

Рецензент: доцент, канд. екон. наук
Олена СЕМЕНЦОВА

2024

Український державний університет залізничного транспорту

Факультет економічний

Кафедра економіки та управління виробничим і комерційним бізнесом

Рівень вищої освіти: магістр

Спеціальність: 051 «Економіка»

Освітня програма: «Економіка підприємства»

ЗАТВЕРДЖУЮ

Завідувач кафедри,
професор, д-р екон. наук

_____ Володимир ДИКАНЬ

« ____ » _____ 2024 р.

ЗАВДАННЯ НА КВАЛІФІКАЦІЙНУ РОБОТУ Кріщину Едуарду Володимировичу

1 Тема «Антикризове управління підприємствами залізничного транспорту»

керівник Дикань Володимир Леонідович, д-р екон. наук, професор

затверджені розпорядженням по економічному факультету

від «23» жовтня 2023 року № 30/23

2 Строк подання студентом закінченої роботи «02» січня 2024 року

3 Вихідні дані: Статистична інформація про діяльність залізничного транспорту

Фінансова звітність залізничного транспорту

Науково-методична література

Періодичні видання

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

1 Концептуальні основи забезпечення безпеки підприємств транспорту в умовах цифровізації

2 Дослідження стану і тенденцій розвитку підприємств залізничного транспорту

3 Методологія та технологія антикризового управління на залізничному транспорті

5 Перелік графічного матеріалу

1 Мета, завдання, об'єкт та предмет кваліфікаційної роботи

2 Проблеми економічної безпеки цифрового суспільства

3 Показники обсягу перевезених вантажів

4 Показники кількості перевезених пасажирів АТ «Укрзалізниця»

5 Показники фонду оплати праці

6 Аналіз вартості та ступеня зносу основних фондів

7 Аналіз фінансових результатів діяльності підприємства

8 Показники фінансового стану АТ «Укрзалізниця»

9 Структура економічної безпеки на залізничному транспорті із позиції концепції економічної безпеки

10 Модель реалізації заходів щодо захисту підприємства в умовах цифровізації

11 Можливі успішні та невдалі результати антикризового управління

12 Адаптивна модель безпеки

13 Стратегічними напрямками діяльності ДП «Галузевий центр цифровізації та кібербезпеки»

6 Консультанти окремих розділів

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

7 Дата видачі завдання «02» жовтня 2023 року.

КАЛЕНДАРНИЙ ПЛАН

Назва етапів	Строк виконання етапів	Примітка
1 Концептуальні основи забезпечення безпеки підприємств транспорту в умовах цифровізації	22.10.2023	викон.
2 Дослідження стану і тенденцій розвитку підприємств залізничного транспорту	01.11.2023	викон.
3 Методологія та технологія антикризового управління на залізничному транспорті	15.11.2023	викон.
Висновки	11.12.2023	викон.
Графічна частина	26.12.2023	викон.

Студент _____ Едуард КРІЩИН

Керівник _____ Володимир ДИКАНЬ

Зміст

Вступ	6
1 Концептуальні основи забезпечення безпеки підприємств транспорту в умовах цифровізації	10
1.1 Розвиток транспортних систем у цифровій ері	10
1.2 Проблеми економічної безпеки цифрового суспільства в умовах глобалізації	21
1.3 Загрози інформаційної безпеки в епоху цифрової трансформації	37
1.4 Інформаційна безпека у логістиці та на транспорті	42
Висновки до розділу 1	49
2 Дослідження стану і тенденцій розвитку підприємств залізничного транспорту	52
2.1 Загальна характеристика АТ «Укрзалізниця»	52
2.2 Аналіз кількісних та якісних показників роботи компанії	53
2.3 Аналіз ефективності використання трудових ресурсів та рівня оплати праці АТ «Укрзалізниця»	58
2.4 Аналіз стану та ефективності використання основних фондів підприємства	64
2.5 Аналіз операційних витрат підприємства залізничного транспорту	67
2.6 Аналіз фінансових результатів і фінансового стану АТ «Укрзалізниця»	71
Висновки до розділу 2	75
3 Методологія та технологія антикризового управління на залізничному транспорті	78
3.1 Роль та місце залізничного транспорту в умовах забезпечення економічної безпеки	78

					<i>МРЕ.129.02.06 ПЗ</i>			
Змн.	Арк.	№ докум.	Підпис	Дата	Антикризове управління підприємствами залізничного транспорту	Літ.	Арк.	Аркуші
Розроб.		Кріцин						
Перевір.		Дикань					4	117
Рецензент						УкрДУЗТ		
Н. Контр.		Назаренко	<i>М.Г.Д.</i>	26.12.23				
Затверд.		Дикань						4

3.2 Технологічний процес антикризового управління в транспортно-логістичній системі на залізничному транспорті	83
3.3 Формування підходів антикризового управління підприємствами залізничного транспорту в умовах цифровізації	88
Висновки до розділу 3	103
Висновки	105
Список використаних джерел	109

					МРЕ.129.02.06 ПЗ	АФК.
Змн.	Арк.	№ докум.	Підпис	Дат		

Вступ

Актуальність теми. Проблеми забезпечення безпеки в умовах ускладнення соціальних, економічних, політичних процесів і явищ набувають дедалі більшої актуальності.

Різні напрямки сучасної діяльності є джерелами раніше невідомих викликів та погроз, що, відповідно, вимагає вироблення нових принципів їхньої мінімізації.

Досвід показує, що безпека є найважливішою умовою стабільності та досягнення результатів у розвитку окремих держав та суспільства в цілому. По суті, це набір економічних, політичних, правових інструментів, які сприяють захисту життєвоважливих економічних інтересів. У більш широкому розумінні безпека характеризує здатність інституційної системи захищати інтереси ключових суб'єктів економіки на основі національних та міжнародних правових норм при дотриманні та повазі національних та господарських традицій та цінностей.

Пріоритетним завданням забезпечення безпеки, особливо помітним в мінливих умовах сучасного глобального світу, є прогнозування викликів та загроз щодо реалізації яких необхідно готуватися вже сьогодні, а найважливішим глобальним викликом є загальна цифровізація.

Вже зараз цифрові технології займають істотне місце у розвитку науки, техніки та економіки у всьому світі. Їхню важливість як локомотива розвитку виразно видно на прикладі таких країн як США, Індія, Китай, Японія. Значна частина національного доходу цих країн забезпечується за рахунок продажу товарів та послуг, пов'язаних з цифровими технологіями. Ефективне керування даними як ключовим ресурсом цифрової економіки є запорукою успіху в будь-якого виді господарської діяльності, а монопольне володіння певними даними часто виявляється вирішальною перевагою у конкурентній боротьбі. Бо в сучасному світі основна діяльність економічних агентів часто пов'язана із застосуванням цифрових технологій, виконання операцій з різного роду даними,

знаходження в глобальному цифровому просторі, з одного боку, дає додаткові можливості для отримання економічного ефекту, з іншого боку, створює певні ризики для подальшого розвитку.

Глибокі зміни, викликані використанням цифрових технологій, значно розширили масштаби проблем при забезпеченні безпеки.

Взаємодія влади, бізнесу, громадських організацій у питаннях цифрової безпеки відіграє ключову роль у підтримці умов для зміцнення основ спільної діяльності у такій ситуації. Незважаючи на значну увагу до проблем розвитку цифрової економіки серед безлічі експертів, питання впливу цифрових технологій на безпеку розроблено досить слабо.

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.

Мета кваліфікаційної роботи полягає у розробці методології забезпечення безпеки підприємств залізничного транспорту в умовах цифровізації, які є зв'язковою ланкою у забезпеченні ефективного функціонування економіки країни.

Для досягнення поставленої мети потрібно вирішення наступних взаємозалежних **завдань**:

- дослідити особливості функціонування підприємств транспорту в умовах цифровізації;
- розкрити проблеми безпеки цифрового суспільства в умовах глобалізації;
- проаналізувати сучасний стан і проблеми функціонування вітчизняних підприємств залізничного транспорту ;
- обґрунтувати чинники антикризового управління підприємствами залізничного транспорту;
- розкрити суть забезпечення безпеки підприємств залізничного транспорту в умовах цифровізації;
- запропонувати підходи щодо забезпечення кібербезпеки на

підприємствах залізничного транспорту.

Об'єктом дослідження кваліфікаційної роботи є процес цифрового розвитку підприємств залізничного транспорту.

Предметом дослідження є теоретико-методологічні засади, методичні підходи та практичні рекомендації щодо забезпечення безпеки підприємств залізничного транспорту в умовах цифровізації

Інформаційною основою роботи є теоретичні та практичні напрацювання вітчизняних та закордонних вчених щодо забезпечення безпеки в умовах цифровізації, а також проблеми розвитку підприємств залізничного транспорту в умовах цифрової трансформації економіки, матеріали та рекомендації науково-практичних конференцій та семінарів, інформаційно-довідкова, навчально-методична література, матеріали періодичних видань, а також відомості із мережі Інтернет, які містяться у джерелах [1-84] 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: розрахунково-аналітичний, аналізу та синтезу, класифікації, узагальнення та конкретизація визначень, а також порівняльний аналіз і графічний.

Наукова новизна: запропоновано концептуальні положення забезпечення безпеки підприємств залізничного транспорту в умовах цифровізації, з урахуванням змін та вимог інформатизації економіки.

Практична значущість кваліфікаційної роботи полягає в тому, що розроблені методичні рекомендації дозволять підвищити цифрову безпеку підприємств залізничного транспорту

Результатами роботи автора є формування пропозицій щодо забезпечення

безпеки підприємств залізничного транспорту в умовах цифровізації.

Публікації. За темою роботи опубліковано статтю у збірнику наукових праць «Вісник економіки транспорту і промисловості» загальним обсягом 16 сторінок (у співавторстві).

Апробація результатів роботи. Основні положення і результати кваліфікаційної роботи доповідалися на 83-й студентській науково-технічній конференції СНТК Українського державного університету залізничного транспорту (12-14 грудня 2023 р., м. Харків).

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

У першому розділі досліджено концептуальні основи забезпечення безпеки підприємств транспорту в умовах цифровізації, виокремлено проблеми забезпечення безпеки цифрового суспільства в умовах глобалізації, окреслено проблематику інформаційної безпеки у логістиці та на транспорті в умовах цифровізації економіки.

У другому розділі проведено оцінювання рівня розвитку АТ «Укрзалізниця», результати якого дозволили дійти висновку про поступову втрату підприємствами галузі стабілізаційних здатностей і обмеженість наявних можливостей щодо ефективного розвитку підприємств залізничного транспорту

У третьому розділі розглянуто особливості реалізації заходів щодо захисту підприємства в умовах цифровізації та обґрунтовано технологічний процес антикризового управління в транспортно-логістичній системі, також сформовано підходи антикризового управління підприємствами залізничного транспорту в умовах цифровізації.

1 Концептуальні основи забезпечення безпеки підприємств транспорту в умовах цифровізації

1.1 Розвиток транспортних систем у цифровій ері

Процеси цифрової трансформації глобальної та національної економік стають однією з актуальних тем сучасних досліджень, а термін «цифрова економіка» - або, на професійному сленгу, «цифрономіка», все більше знаходить застосування в лексиконі учасників підприємницького ринку.

Цифрова трансформація передбачає об'єднання всіх складових цифрового світу, а використання цифрових даних стає ключовим фактором виробництва, що дозволяє створювати нові моделі ведення бізнесу, забезпечуючи серйозні конкурентні переваги компаніям, як на регіональних, і на глобальних ринках.

Інтелектуальне перевезення як інноваційний продукт цифрової логістики дозволяє створити інноваційні комплексні транспортні послуги в залежності від потреб клієнта, що постійно змінюються. Спираючись не тільки на виробничу потребу, а й з метою підвищення якості сервісу та зменшення витрат за участю різних перевізників при здійсненні різних перевезень потрібна масштабна інтеграція інтелектуальних комунікаційних технологій між користувачем, транспортним засобом, інфраструктурою тощо.

Цифровий розвиток транспорту – невід'ємний компонент успішного переходу до розвитку транспортних систем до цифрового порядку. Створення єдиних цифрових платформ, використання нових ІТ-технологій, введення в експлуатацію безпілотних транспортних засобів (БТС) – це лише деякі способи цифрового розвитку сфери.

У цифровій трансформації логістики вантажних перевезень ключову роль відіграють інтегровані інформаційні цифрові платформи (ІЦП). Ці платформи об'єднують учасників ланцюжки створення вартості, канали збуту, споживачів та окремі галузі економіки. Для підвищення продуктивності використовують

локальні ІЦП у транспорті та логістиці. З їх допомогою планують перевезення, організовують взаємодію різного виду транспорту, обробляють вантажі на складах, що суттєво скорочує тимчасові та фінансові витрати транспортних компаній та їх клієнтів. Застосування комплексних ІЦП широко використовується логістичними посередниками, які виконують сервісні функції та керують окремими компетенціями виробничих компаній. Поєднуючи бізнес-процеси клієнтів, логістичні посередники з'єднують виробників із споживачами, забезпечують доставку сировини, готової продукції, комплектуючих, керують складськими запасами, проводять розрахунки та надають інші послуги. Тому логічний сектор стає потужним драйвером розвитку та підвищення конкурентоспроможності від ділових компаній та цілих галузей на глобальному ринку у цифрову епоху [21].

Що стосується глобальних ІЦП, можна навести яскравий приклад їх розвитку: за дорученнями Кабінету Міністрів України було запроваджено експериментальний проєкту щодо забезпечення впровадження замовлення бланків дозволів на поїздку по територіях іноземних держав при виконанні перевезень вантажів автомобільним транспортом у міжнародному сполученні в електронній формі через Транспортний портал електронних послуг, який об'єднує електронні сервіси у всіх сферах транспортної галузі в одну розумну систему [76].

Реалізація даного проєкту вирішить наявні проблеми у транспортному комплексі, дозволить ефективніше керувати транспортним розвитком, не допустить появи несправностей. Введення єдиних цифрових платформ зробить крок назустріч інтеграції видів транспорту в єдину мережу, шляхом утворення єдиної інформаційної бази. Така інтеграція дозволить максимально ефективно використовувати внутрішні ресурси, знизить витрати перевезень, встановить єдині стандарти на якість перевезення, безпеку, тарифи.

Ще одним зразком продукту цифровізації служить Інтернет речей (ІоТ), що поєднує навколишні об'єкти в єдину комп'ютерну мережу. Наочним прикладом використання ІоТ можна розглядати порт Гамбург. Завдяки впровадженням

технологіям у порту Гамбург, другим за обсягом вантажоперевезень у Європі, на 15% скоротилося навантаження на транспортні потоки та на 75% зменшилися операційні витрати.

У Гамбурзі використовується своя локальна інформаційна система, що реалізує принципи механізму "Єдиного вікна". Ядро DAKOSY – центральна база даних, що дозволяє обробляти і накопичувати інформацію, яка надходить від усіх сторін-учасників. Для зручної взаємодії DAKOSY пропонує всім транспортним компаніям інтерфейси електронного обміну даними EDI (Electronic Data Interchan).

HABIS є експлуатаційною інформаційною системою для портової залізниці. GEGIS – інформаційна система, яка дозволяє передавати інформацію по небезпечним вантажам у порту Гамбург. Пересування небезпечних вантажів фіксуються EDI за допомогою GEGIS. Повідомлення EDI показує точну інформацію про час і місцезнаходження вантажу, EDI використовують для складання точної картини поточного стану.

ZAPP – система електронного моніторингу експортної митниці у безпаперовому порту. Система забезпечує всім учасникам експортного процесу електронний зв'язок з митницею через систему DAKOSY. В даний час DAKOSY застосовують не лише у порту Гамбурга, а й у портах від Роттердама до Антверпена.

Ще одним елементом цифровізації логістики вантажних перевезень є БТС. Завдяки БТС може бути повністю автоматизована робота морських портів, терміналів, складів та інших інфраструктурних об'єктів. Багато контейнерних терміналів портів світу функціонують без безпосередньої участі людини. Прикладом використання безпілотних транспортних засобів є автоматизований контейнерний термінал у Роттердам. Контейнери від місця складування до судна перевозяться на AGV (automated guided vehicle) – автоматично керований візок. AGV забезпечений всіма необхідними системами і елементами безпеки, який може експлуатуватися на шкідливих або небезпечних виробництвах, місцях скупчення людей та інших AGV, що рухаються. Допоміжні крани, які дістають

контейнери з майданчика зберігання і вантажать на візки, теж автоматизовано.

Говорячи про розвиток цифрових технологій на залізниці, то масштабною ініціативою у сфері залізничного транспорту є європейська програма Shift2Rail, що координується Європейським залізничним агентством, спрямована на прискорення процесів розроблення і впровадження інноваційних технічних рішень у залізничній галузі, зокрема розвитку європейської системи управління рухом поїздів ETCS. Серед таких технічних новацій слід відзначити автоматичне зчеплення вагонів, рухливі блок-ділянки магістральних залізниць, інтелектуальні вантажні термінали, пристрої для виявлення перешкод тощо. Також до переліку тематичних напрямів входять розроблення альтернативних систем тяги, новації в системі управління рухом поїздів, вимоги до вантажних поїздів майбутнього, зокрема безпілотного управління.

На національному рівні країнами також взято вектор на цифровізацію залізниць і започатковано реалізацію програмних ініціатив щодо впровадження цифрових рішень в усі сегменти їхньої діяльності. Відтак програма Smart Rail 4.0 з'явилася у Швейцарії на початку 2017 р. з ініціативи федеральних залізниць Schweizerische Bundesbahnen і в подальшому завдяки залученню до її реалізації приватних операторів ринку залізничних перевезень набула загальногалузевого масштабу. Необхідність її розроблення зумовлена тим, що термін експлуатації багатьох систем, пов'язаних із забезпеченням безпеки і управлінням рухом поїздів (у т. ч. систем централізації, підлогового обладнання, цифрового радіозв'язку GSM-R), скоро завершується. З огляду на це програмою Smart Rail 4.0 передбачається об'єднання в єдину відкриту архітектуру всіх релевантних проривних технологій: європейська система управління рухом поїздів ECTS 2 рівня та вище; безпечна ідентифікація місцезнаходження поїзда бортовими пристроями; радіозв'язок нового покоління FRMCS, автоматичний перерахунок оперативного графіка руху поїздів; автоведення тощо. Зокрема одна з шести підпрограм галузевої програми має назву ECTS Stellwerk / ECTS Interlocking і передбачає створення системи мікропроцесорної централізації нового покоління, що дозволить скоротити до 70 % інвестиційні витрати системи централізації та

блокування і управління рухом поїздів. Загалом впровадження вказаної програми дозволить підвищити економічну ефективність і продуктивність залізниць.

Починаючи з січня 2019 р. Schweizerische Bundesbahnen реалізується практична ініціатива щодо впровадження інтелектуальної системи управління споживачами електроенергії, що відключає частину з них на короткий час (максимум 40 с) у разі пікових навантажень, що виникають при одночасному русі великої кількості поїздів. До таких споживачів належать системи опалення в поїздах і пристрої обігріву стрілок. До 2023 р. Schweizerische Bundesbahnen має намір оснастити необхідним обладнанням весь парк пасажирського рухомого складу і всі пристрої обігріву стрілок. Очікується, що в результаті пікові навантаження можуть бути знижені на 70 МВт. Також вивчається можливість інтелектуального управління тяговими двигунами електровозів і електропоїздів з метою короточасного зниження їхньої потужності в періоди пікового навантаження без порушення графіка руху. Впровадження такого роду цифрових технологій дозволить уникнути значних витрат на нарощування потужності залізничної енергосистеми.

Програма «Цифрові залізниці Німеччини» (Digitale Schiene Deutschland) була представлена у 2018 р., і саме цю країну вважають піонером у напрямі цифровізації залізниці, що пов'язано з упровадженням цифрових рішень ще задовго до прийняття програми в рамках загальної стратегії розвитку Deutsche 93 Bahn. Особлива роль у забезпеченні ефективного впровадження цифрових рішень у галузі належить європейській системі управління рухом поїздів (ETCS) і системам мікропроцесорної централізації. Deutsche Bahn зазначено, що впровадження цифрових технологій на всій мережі дозволить збільшити її пропускну спроможність на 20 % протягом наступних 10-15 років, а також ввести в обіг тисячі додаткових поїздів і взагалі підвищити рівень автоматизації роботи залізничного транспорту.

Загалом планується розгортання цифрових технологій на 80 % мережі залізниць Німеччини до 2030 р. Зокрема в першу чергу мають бути обладнані ділянки транс'європейських коридорів TEN-T, розташовані на території

Німеччини. Так, до 2022 р. передбачено обладнати системою ETCS близько 2500 км ділянок у межах коридорів TEN-T. Щодо мікропроцесорної централізації, то слід вказати, що заплановано впровадження так званих цифрових систем централізації, відмінність яких від традиційних полягає в тому, що команди управління будуть надходити не в аналоговому, а цифровому вигляді. Це дозволить збільшити радіус дії системи централізації, стандартизувати її компоненти і спростити технічне обслуговування.

Крім того, Deutsche Bahn має намір створити окрему компанію для управління цифровізацією залізничної мережі Німеччини, так звану Digital Rail Germany, що відповідатиме безпосередньо за планування та впровадження цифрових технологій у цій сфері, включаючи системи цифрової централізації, колійні та бортові компоненти системи управління і контролю за рухом поїздів ETCS. За оцінками залізничної компанії, впровадження цих технологій дозволить приблизно на третину збільшити пропускну спроможність мережі.

При цьому урядом Німеччини надається значна фінансова підтримка реалізації реформ у сфері залізничного транспорту. Зокрема на 2020 р. Deutsche Bahn заплановано інвестиції в обсязі 12,2 млрд євро, що на 1,5 млрд євро перевищує загальний розмір коштів, виділених у 2019 р. Їх передбачається спрямувати на оновлення 1800 км колій і понад 1900 стрілочних переводів, а також реконструкцію 160 мостів і модернізацію 800 станцій.

У свою чергу в рамках програми з захисту клімату Klimaschutzprogramm 2030 урядом виділено 94 додатково 11 млрд євро на розвиток залізничного транспорту країни протягом 10 років. Ці кошти будуть спрямовані виключно на реалізацію інфраструктурних заходів у галузі з метою досягнення сталого розвитку залізничного транспорту і впровадження цифрових технологій. Перший пакет охоплює заходи щодо підвищення надійності роботи мережі та включає інвестиції в системи централізації, усунення вузьких місць, перехід на тактовий графік руху пасажирських поїздів далекого сполучення, електрифікацію вантажних ліній, створення інфраструктури для альтернативних систем тяги, розвиток мультимодальних терміналів і т. п. Другий пакет включає додаткове

фінансування початкового етапу розгортання на мережі залізниці європейської системи управління рухом поїздів ETCS і цифрових систем централізації, а також впровадження інших цифрових технологій. Третій пакет передбачає фінансування різних заходів з оновлення вокзалів, а четвертий спрямований на підвищення якості транспортних послуг і пропускної здатності мережі.

У 2018 р. стратегія Digital Railway для Network Rail також з'явилася і у Великобританії. Вона містить рекомендації щодо впровадження безпаперових технологій, рішень для підвищення пропускної спроможності в умовах пікового завантаження за рахунок пошуку можливостей виділення додаткових ниток графіка і комбінованого використання локомотивної сигналізації, рішень для поліпшення можливостей транспортних сполучень, а також переходу на широкосмуговий зв'язок 4-го покоління LTE. Згодом у 2019 р. Network Rail оприлюднено довгостроковий план переходу до цифрових систем сигналізації, в основі якого знаходяться положення вказаної стратегії. На першому етапі він передбачає оснащення бортовими пристроями ETCS більше 4000 од. рухомого складу і оновлення систем сигналізації на 30,6 тис. км залізничних колій, що пов'язано з необхідністю заміни в найближчі 15 років 2/3 систем сигналізації. Надалі довгостроковий план передбачає поступовий перехід до цифрових систем сигналізації протягом 30 років починаючи з 2024 р [82].

Впровадження цифрових систем сигналізації означає відмову від значної частини існуючого нині обладнання і прискорене переоснащення тягових одиниць бортовими пристроями, розрахованими на управління рухом поїздів радіоканалом. Очікується, що економічний ефект від переходу до таких систем за 30-річний період складе від 7 млрд до 18 млрд фунтів стерлінгів. Також важливою подією для Великобританії в напрямі цифровізації залізниці стало відкриття іспанською компанією CAF цифрового підприємства з виробництва рухомого складу в м. Ньюпорт (Уельс) у лютому 2020 р., що є одним із ключових інфраструктурних елементів повномасштабної цифровізації залізниці в країні. Цей пілотний проєкт має на меті відпрацювання концепції широкого застосування цифрових технологій в організації виробництва. Вартість проєкту склала 40 млн

євро, з яких 30 млн євро інвестовано компанією CAF, а також отримано грант уряду Уельсу. На першому етапі роботи підприємства у виробничих процесах задіяно близько 200 співробітників, чисельність яких у подальшому збільшиться до 300 осіб. Запуск такого підприємства в Ньюпорті дозволить CAF виконати укладені з британськими операторами контракти на загальну суму близько 2,5 млрд євро.

Програма впровадження цифрових систем управління рухом поїздів у Норвегії є однією з найбільш масштабних і передбачає повну заміну пристроїв сигналізації, централізації та блокування на всій мережі Bane NOR протяжністю 4200 км з 350 станціями до 2034 р. Передбачається, що Норвегія стане першою у світі країною, управління рухом поїздів на всій залізничній мережі якої буде здійснюватися з одного дата-центру, що реалізовуватиме функції розпорядчого поста централізації. У 2018 р. Bane NOR підписала контракти на впровадження підлогового обладнання пристроїв централізації і ETCS з компанією Siemens, бортового обладнання ETCS з компанією Alstom і системи автоматизації диспетчерського управління з компанією Thales. На замовлення Bane NOR для управління цим проєктом створення лабораторії для тестування ETCS, що здійснюватиме компанія ProRail – оператор інфраструктури залізниць Нідерландів [81].

Також у сфері управління вантажними перевезеннями започатковано ініціативу щодо впровадження цифрових платформ їх організації. Зокрема німецькою лізинговою компанією VTG, що має у своєму розпорядженні найбільший у Європі парк рухомого складу, оголошено про намір створення нової цифрової платформи traigo. Ця платформа складе основу цифрової інфраструктури організації перевезень вантажів залізничним транспортом. Після її запуску клієнти отримають доступ до даних контрактної документації та інформації про орендовані вагони в реальному часі. Надалі платформа дозволить перевести всі сервіси в цифровий формат, включаючи подачу заявок на вагони в режимі онлайн і планування технічного обслуговування і ремонту рухомого складу. Крім того, VTG, використовуючи можливості цифрових технологій та

інтелектуальне моделювання, планує надавати клієнтам нові послуги, зокрема прогнозувати час прибуття всіх залізничних вантажних відправлень. При цьому сфера дії traigo не обмежується тільки клієнтами компанії: до співпраці запрошуються всі підприємства залізничної галузі, що мають відношення до цифровізації управління вантажними перевезеннями. Офіційний запуск платформи планується на другий квартал 2020 р. Компанія має намір до кінця 2020 р. завершити обладнання парку вантажних вагонів телематичними пристроями і бортовими датчиками інтернету речей [78].

Як приклад формування цифрових платформ у сфері організації залізничних перевезень слід навести й іспанську компанію CAF, якою розроблено багатоцільову цифрову платформу LeadMind для якісної організації пасажирських перевезень. Оператор інфраструктури залізниць Великобританії Network Rail у свою чергу переходить на нову цифрову корпоративну платформу, використання якої забезпечить технологічну гнучкість і сумісність існуючої інфраструктури і нових цифрових рішень у залізничній галузі. У свою чергу оператор VTG Rail Europe також підписав контракт зі швейцарською компанією Nexxiot, що займається прикладною цифровізацією у сфері логістичних послуг, на оснащення до весни 2020 р. його контейнерного парку датчиками інтернету речей Globehopper. Їх використання дозволить повномасштабно контролювати розташування і переміщення устаткування всіма видами транспорту, завдяки чому оператор отримає можливість точніше прогнозувати перевезення і пропонувати клієнтам більш прозорі послуги.

Разом з обладнанням IoT компанія Nexxiot пропонує програмні рішення для аналізу отриманої інформації і пропонує комплексну аналітичну платформу на основі «хмарних» технологій. Інтегральне рішення, що розробляється у співпраці з VTG, дасть можливість, починаючи з 2020 р., вводити інформацію з датчиків безпосередньо в корпоративну систему компанії. Наразі Nexxiot обладнала датчиками близько 50 тис. транспортних об'єктів, включаючи вантажні вагони і танк-контейнери, і щомісяця їх кількість збільшується на 3-4 тис. од.

Важлива увага реалізації цифрових ініціатив приділяється і країнами

Центральної Азії. Зокрема стратегія «Цифрова залізниця» 2018- 2022 рр. поетапно реалізується в Казахстані. Вказаною ініціативою передбачено цифровізацію бізнес-моделі компанії і впровадження нових технологій в усі ключові операційні сегменти: вантажні і пасажирські перевезення, інфраструктура і транспортна логістика. Зокрема серед проєктів цифровізації у сфері пасажирських перевезень, які вже реалізовано, слід вказати на систему продажів електронних квитків. Також заплановано впровадження систем динамічного управління тарифами і зверненнями клієнтів 24/7. На об'єктах залізничної інфраструктури у свою чергу реалізуються проєкти з упровадження цифрової діагностики колій, центру управління рухом поїздів, цифрових сервісів на 17 вокзалах. У вантажному русі здійснюється впровадження та експлуатація автоматизованих систем, спрямованих на оперативне управління перевезеннями, інтегровану обробку маршрутів, планування і прогнозування руху поїздовагонопотоків, контроль споживання дизельного палива та електроенергії локомотивами тощо. Найбільш успішною у вантажному господарстві є автоматизована система управління «Договірна та комерційна робота», що функціонує за принципом «єдиного електронного вікна» при плануванні, організації і здійсненні перевезень, електронної оплати послуг, пов'язаних з перевезенням вантажів. Крім того, процеси цифровізації поширюються і на корпоративний центр, до діяльності якого заплановано впровадження інтегрованої системи планування з елементом machine learning. Її використання дозволить здійснювати оптимальний розподіл ресурсів, приймати ефективні рішення при експлуатаційному, комерційному та інвестиційному плануванні.

Спільною ініціативою в напрямі цифрової трансформації транспортно-логістичної діяльності є розроблення єдиної екосистеми цифрових транспортних коридорів, що передбачає впровадження нових цифрових митних, логістичних, страхових і фінансових сервісів, а також доопрацювання та інтеграцію до загальної екосистеми вже існуючих. Екосистема має охопити сервіси для розрахунку маршрутів, електронні подорожні листи та міжнародні транспортні накладні, електронні протоколи результатів перевірки органами внутрішніх справ

тощо [77].

В Україні історично склалося так, що у сфері залізничного транспорту функціонує лише одна компанія – державний монополіст АТ «Укрзалізниця», який здійснює як перевізну, так й інфраструктурну діяльність. На тлі незавершеності організаційних перетворень і поглиблення системної кризи в галузі суттєво відчувається цифровий розрив між національною залізницею і залізничними компаніями світу, що виник у результаті відсутності цифрового бачення АТ «Укрзалізниця» і тривалого ігнорування потреби впровадження технологічних інновацій. Наразі залізничні компанії в усьому світі вже впровадили широкий спектр нових послуг і додатків з використанням цифрових технологій як для надання більшої кількості інформаційних і розважальних послуг, так і для поліпшення моніторингу активів та автоматизації операцій. Зміни, викликані цифровізацією в залізничному транспорті, сприймаються багатьма зацікавленими сторонами як можливість – завдяки перевагам, що вона може запропонувати, – але також і як проблема. Дійсно, цифровізація потребує зміни мислення і бізнес-моделей, значних фінансових вкладень і стратегії боротьби з кіберзагрозами. Проте вирішення цих проблем дозволить залізничній компанії завдяки цифровізації підвищити її ефективність і забезпечити конкурентоспроможність на ринку.

Наразі перевезення неможливі без комп'ютерної інтеграції всіх задіяних суб'єктів, які забезпечують зовнішньоекономічні зв'язки. Однак, враховуючи незаперечні переваги, впровадження інформаційних технологій має і свої недоліки. Нові технології створюють серйозні виклики на ринку праці. Масштабні скорочення персоналу очікуються у зв'язку з використанням БТС для перевезення вантажів та пасажирів. Ще одна проблема – це дефіцит управлінських кадрів у сфері інформаційних технологій. Вирішити цю проблему можна тільки шляхом загального перенавчання управлінського персоналу.

1.2 Проблеми економічної безпеки цифрового суспільства в умовах глобалізації

Суттєві зміни у соціально-економічних відносинах, способах виробництва, перехід до постіндустріального устрою супроводжуються цілим набором особливостей, характерних для цифрової економіки та виявляються у наступних моментах [54]:

- наявність інтелектуальних активів, які використовуються для підвищення економічної ефективності (найважливіша умова розвитку). В даний час найбільш привабливими для інвесторів є компанії, що володіють значним обсягом інтелектуальних ресурсів. Яскравими прикладами тут є представники інтернет економіки, такі як Facebook, Uber, Airbnb, які, по суті, не маючи фізичних активів, являють собою цифрові платформи та обганяють за своєю капіталізацією багатьох промислових гігантів;

- збільшення значущості даних в економічній діяльності. Істотна частина економічної діяльності пов'язана з послугами, що мають відношення до інтелектуальної власності, баз даних, програмних продуктів. Однією з тенденцій у галузі управління даними, що заслуговує на особливу увагу є «хмарні» технології. Такі технології - це модель, яка забезпечує доступ до необхідних послуг з управління даними у гнучкому, масштабованому варіанті. Оскільки «хмарні» технології трансформують обчислення на послугу, компаніям не потрібно здійснювати серйозних капіталовкладень для закупівлі обчислювальних потужностей. «Хмарні» технології надають можливості з використання програмного забезпечення, обчислювальних потужностей, зберігання даних. Важливим фактором при використанні «хмарних» технологій є прагнення заощадити на послугах. Підприємства, які використовують у своїй діяльності хмарні технології, скорочують витрати на створення та підтримку власної цифрової інфраструктури. При цьому економічна ефективність використання «хмарних» технологій залежить від рівня розвитку цифрової інфраструктури

підприємства. Для підприємств з розвинутою інфраструктурою «хмарні» технології — це спосіб збільшити швидкість надання послуг та зробити послуги більш гнучкими. Основними перевагами використання «хмарних» технологій є їх висока продуктивність і доступність, еластична масштабованість і швидке розгортання. Разом з тим використання «хмарних» технологій супроводжується певними проблемами та складнощами. Головна проблема — забезпечення безпеки даних. Використання цифрових технологій сприяє підвищенню продуктивності праці. Однак їх активне впровадження підприємствами стримується недостатньою поінформованістю про потенційні вигоди, а також інвестиційними та впроваджувальними витратами. Важливу роль у стимулюванні використання цифрових технологій можуть відіграти державні органи, заохочуючи підприємства використовувати сучасні цифрові технології для підвищення ефективності діяльності;

- основною організаційною структурою стає мережа, а не ієрархія. Гібридні форми організації більш пристосовані до швидких змін на ринку, що позначається на їх ефективності. Багато великих організації з жорсткою ієрархічною структурою адаптуються до нових реалій, знижуючи кількість рівнів ієрархії, розмиваючи межі підрозділів і віддаючи непрофільні напрямки діяльності на аутсорсинг. Країни з економікою, що розвивається, перебувають у процесі переходу до нового типу господарювання, вирішуючи питання про підвищення своєї конкурентоспроможності. Одним із методів подолання відставання від провідних економічних країн є активне використання нових мережових форм взаємодії економічних суб'єктів. Створення сприятливих умов функціонування мережових структур є важливим принципом розвитку сучасної економіки. Конкурентоспроможність сучасних економік базується на мережовій взаємодії підприємств і організацій, що виробляють, розповсюджують і використовують спільні ресурси. Її інтерактивний характер припускає, що інноваційні ідеї генеруються на всіх стадіях виробничого циклу. Існують численні горизонтальні зв'язки, в інноваційний процес залучаються фахівці різних професій та кваліфікацій. Можна стверджувати, що епоха щодо ізольованих і

замкнутих виробництв відходить у минуле. Все більшого значення набувають взаємозв'язки з постачальниками, споживачами, і навіть конкурентами, не кажучи про установи на науково-дослідний характер. Тому промислова політика повинна фокусуватися не на окремих підприємствах і секторах, а сприяти розвитку мережових структур;

- основним інструментом пошуку інформації та зв'язку є інтернет. Розвиток широкосмугового інтернету, мобільного інтернету, інтернет-додатків і гаджетів докорінно змінило способи комунікації в суспільстві. Використання веб-сайтів, цифрових платформ, месенджерів набагато більш ефективне, ніж використання раніше визнаних засобів комунікації;

- обмін даними носить глобальний характер. Економічні агенти, які не мають доступу до глобальної мережі передачі даних, ринків і технологій інших країн, які намагаються функціонувати лише на обмежених локальних ринках, у результаті залишаються в тісних рамках і поступаються у глобальній боротьбі;

- основним підходом до управління є самоорганізація. Економіка, заснована на децентралізації та глобалізації, є прекрасною основою для формування мережових структур за принципом «знизу вгору» та переходом бюрократичних структур до більш гнучких та ефективних форм. Іншими важливими прикладами процесів самоорганізації є краудсорсинг, краудфандинг та «дольова економіка».

За останні кілька років у розвинених країн з'явилися нові моделі економічних відносин, узагальнено та іменовані економікою спільного користування (sharing economy).

Такі моделі дозволяють здійснювати більше ефективного використання товарів тривалого користування. Декілька факторів стали каталізатором появи таких моделей: по всебічне проникнення інтернету та використання мобільних пристроїв, розповсюдження соціальних мереж, використання геолокаційних даних у реальному часі, які дозволяють оптимізувати процеси використання благ, використання рейтингів та оцінок для контролю якості продавців та покупців.

Компанії економіки спільного споживання пропонують до використання платформи, що дозволяють формувати нові економічні відносини у сфері

нерухомості, транспортних засобів і т. д. (найчастіше товарів тривалого користування). Масштаби і швидкість, яких досягли компанії економіки спільного споживання за останній час, вражаючи (як приклади можна навести такі компанії, як Alibaba, Uber, Facebook, eBay, Amazon, чия ринкова капіталізація перевищує ВВП окремих країн). Більшість моделей економіки спільного споживання в даний час покладаються на саморегуляцію, використовуючи рейтинги та оцінки. Репутація — ключовий елемент економіки спільного споживання.

У той час як економіка спільного споживання приносить споживачам вигоду від великого розмаїття послуг та низьких цін, така модель не завжди узгоджується з чинним законодавством. Проблема полягає в тому, щоб гарантувати ефективний захист споживачів і виробників у новій економічній обстановці, сприяючи потенційним вигодам від економіки спільного споживання.

Розповсюдження цифрових технологій призвело до розвитку моделей у галузі виробництва продуктів та послуг, прикладами яких є краудсорсинг (crowdsourcing) та краудсординг (crowdfunding). Краудсорсинг є прикладом мобілізації ресурсів людей за допомогою цифрових технологій з метою вирішення завдань, що стоять перед бізнесом, державою та суспільством загалом. Компанії використовують дані практики для залучення капіталу та інших ресурсів. Краудсорсинг може застосовуватися в безлічі різних дій, включаючи розробку товарів, генерування ідей і рішень, у маркетингу та рекламних компаніях [72].

Краудфандінг використовується для створення платформ та моделей залучення коштів, включають кредитування (P2P-платформи), пожертвування чи інвестування для реалізації певних проєктів. Найбільш широко практика краудфандінгу поширена в США та країнах Європи. В останній час стає популярною модель крауд фандінгу, заснована на добровільних пожертвуваннях для реалізації перспективних проєктів. У такому разі фінансовий інтерес не є визначальним, що дозволяє новаторам не надавати першочергового значення повернення залучених коштів, а сконцентруватися на створенні якісного продукту. Прикладами краудфандінгових майданчиків є Kickstarter, IndieGoGo,

RocketHub та інші.

Рух у бік більш тісної взаємодії зі споживачем можна вважати відповідною реакцією компаній на зміни в бізнес-середовищі, підвищення рівня непередбачуваності ринків і зростання рівня ризиків.

За останнє десятиліття цифрові технології, включаючи інтернет, стали основою функціонування економіки, ключовим фактором розвитку у всіх її секторах [73].

Ефективне функціонування економіки стало залежним від цифрового середовища. При цьому все більше зростає число невизначеностей, властивих цифровому простору. Цифрові загрози стали масштабнішими, що найчастіше призводить до значних фінансовим, репутаційним, тимчасовим витрат. У звіті ВЕФ з глобальних ризиків (The Global Risks Report) такі загальні загрози, як кіберзлочинність і крадіжка даних розташовані на третьому та четвертому місці за значимістю.

Напрями, пов'язані з цифровими технологіями, так чи інакше позначені у планах розвитку більшості держав, які прагнуть вирішувати соціально-економічні проблеми і знижувати ризики цифровізації шляхом розробки та реалізації стратегій безпеки в цифровий простір.

Безпека цифрових систем є актуальною проблемою для економіки та суспільства загалом і одним із ключових та «наскрізних» напрямів управління цифровізацією та вимагає адекватних заходів захисту всіх учасників. У багатьох країнах стратегія цифрової безпеки приймається як цілісний документ, пов'язаний із забезпеченням національної безпеки. При цьому всі знають, що масштаби загроз і ризики виходять за межі окремих держав і стають світовими. Усвідомлення цього факту сприяло створенню рядом країн спеціалізованих організацій для координації мережевої та інформаційної безпеки на національному та міжнародному рівні. Типовими цілями стратегій із забезпечення безпеки у цифровому просторі є:

- виявлення кібератак і реагування на них;
- запобігання загрозам, підтримці та розробці надійних продуктів і послуг

для державних структур і суб'єктів економічної діяльності;

- підтримка державних установ та операторів інфраструктури;
- сприяння розвитку освіти в галузі цифрових технологій.

Крім того, у більшості країн створено національні програми захисту інфраструктури, які визначають технічні та функціональні критерії для цифрових технологій та сприяють ідентифікації щодо потенційно вразливих елементів на основі розробки правил та процедур забезпечення доступу до них. Наприклад, деякими країнами ОЕСР (Австрією, Бельгією, Португалією, Швецією, Чехією) були створені комп'ютерні групи реагування на надзвичайні ситуації (CERT) для більш ефективного обміну інформацією та розвитку співробітництва з організаціями приватного сектору, а також для координації цифрової взаємодії між країнами. Таким чином, загальновизнаними вважаються необхідність подальшого міжнародного співробітництва, реалізація конкретних оперативних ініціатив у сфері міжнародної та регіональної безпеки в цифровому середовищі, а також інші форми двостороннього та багатостороннього сприяння.

У розвинених країнах, як і раніше, пріоритетне заохочення подальшого розвитку інфраструктури широкосмужової мережі, оскільки доступність даного виду зв'язку вважається рушійною силою інновацій, зростання робочих місць у цифровій економіці. Це означає, що високоякісна інфраструктура повинна бути доступна для широкого загалу потенційних користувачів, щоб забезпечити розвиток таких сфер діяльності, як охорона здоров'я, освіта, фінанси. За останні кілька років були розроблені та впроваджені національні плани (як складові стратегій) щодо розвитку широкосмужового доступу, що передбачають розширення мереж та їх модернізацію для забезпечення більш високих швидкостей передачі даних для конкретних соціальних та економічних груп населення. Заходи щодо здійснення подібних стратегій варіюються від створення базової комунікаційної інфраструктури до розробки складних цифрових систем медичних записів. Такі країни, як Австралія, Канада та Естонія, впроваджують економічно ефективні рішення для віддалених та сільських районів за допомогою цифрових технологій для поліпшення якості наданих медичних послуг. У

багатьох випадках ініціативи в галузі електронної охорони здоров'я інтегруються з національними проєктами щодо розвитку цифрових технологій у державному секторі.

Організації державного сектора все частіше розвивають власні цифрові проєкти для досягнення цілей у множині галузей соціально-економічної діяльності, розглядаючи при цьому цифрові технології як основний драйвер перетворень і підвищення ефективності. Але не можна сказати, що подібні перетворення відбуваються легко або що цифрові технології є єдиним елементом, необхідним для досягнення еволюційних змін. Цифрові технології вже використовуються в багатьох державних організаціях, проте зараз необхідне розуміння того, як їх використання та розвиток цифрових проєктів підвищать ефективність діяльності таких структур [15].

Впровадження новітніх технологій та інформатизація на їх основі державного сектора є найважливішими моментами у створенні організаційно-технологічної бази для підвищення ефективності інформаційного обслуговування населення, діяльності системи органів державної влади та місцевого самоврядування, використання та розвитку загальнодержавної інформаційно-комунікаційної інфраструктури та системи інформаційних ресурсів. Сучасний інструментарій інформатизації державного сектора має забезпечити створення ефективної системи узгодження інтересів та дій в інформаційній сфері між федеральними та регіональними органами управління, формування системи нормативного правового забезпечення процесів інформатизації з урахуванням регіональної специфіки, оптимізацію рішення державних завдань, включаючи мінімізацію трансакційних витрат з інформатизації державного управління в масштабах регіонів та країни в цілому, постійний моніторинг розвитку регіональних складових національної інформаційно-комунікаційної інфраструктури та ринку інформаційної продукції та послуг. Використання цифрових технологій дозволяє істотно підвищити прозорість прийнятих рішень у галузі державного управління, знизити рівень корупції, підвищити довіру громадян за рахунок їх залучення у процес прийняття рішень.

Розуміння того, що значне відставання в процесах цифровізації робить економіку неефективною, менш конкурентоспроможною, залежною від інших країн, що істотно знижує її економічну безпеку, змушує уряди країн приділяти питанням цифровізації значну увагу.

Суттєва увага до розвитку цифрової економіки у зв'язку приділяється і в нашій країні. Одним з основних етапів при русі в цьому напрямку стало прийняття таких значущих документів, як Закон України «Про стимулювання розвитку цифрової економіки в Україні» «Концепція розвитку цифрової економіки та суспільства України на 2018-2020 рр», «Стратегія Україна 2030Е» та ряду інших документів.

Зазначені стратегічні документи визначили напрями подальшого прогресивного розвитку інформаційного суспільства і створили умови для формування цифрової економіки, поклавши початок інтенсивному використанню державними організаціями, бізнесом і громадянами сучасних цифрових технологій.

Слабкими сторонами вітчизняних програм щодо розвитку власної цифрової економіки є відсутність аналізу поточного стану цифрової економіки, відсутність положень щодо створення структур, що відповідають за їхню реалізацію. Крім того, не позначені обсяги державної підтримки конкретних напрямів розвитку, не позначені конкурентні переваги вітчизняної цифрової економіки у глобальній системі [68].

Копіюючи досвід інших країн у розвитку цифрової економіки, наша країна ризикує стати залежною в галузі цифрових технологій. При сценарії вбудовування у глобальний цифровий простір Україні буде досить складно отримати суттєві конкурентні переваги і досягти високих результатів у соціально-економічному розвитку.

Сьогодні цифрова економіка спирається на складну екосистему взаємопов'язаних інформаційних та комунікаційних технологій, засновану на обробці «великих даних», забезпечуваних складним аналітичним інструментарієм. У такій багаторівневій взаємозалежній структурі існують

ризика, що є проблемою багатостороннього характеру. Те, що відбувається в малому бізнесі, може вплинути на великий бізнес і всіх учасників ланцюжка створення вартості. Правильне та зворотне: системний збій у цифровій системі країни поставить під загрозу існування окремих підприємств, банків, організацій державного сектора.

У цьому середовищі дані стали основним активом. Широке використання великих обсягів даних та аналітики для значного покращення або стимулювання розробки нових продуктів, процесів, організаційних методів та створення ринків стало основою для формування концепції «інновацій, заснованих на даних» («data-driven innovation, DDI»).

З одного боку, даний підхід дозволяє підвищити ефективність різних операцій, починаючи від оптимізації та реінжинірингу, поліпшення відносин з клієнтами та розвитку нових ринків і до вирішення більш глобальних соціальних та екологічних проблем. Ефективність розвитку в таких умовах безпосередньо залежить від відкритості і взаємопов'язаності. ти цифрового середовища, від здатності легко, гнучко і дешево переміщати дані серед потенційно необмеженого числа учасників.

З іншого боку, інтенсивний обмін та використання великих потоків даних знижують ступінь конфіденційності використовуваної інформації та сприяють створенню ряду цифрових небезпек. Ідея про те, що з міркувань безпеки система повинна залишатися закритою за умовчанням, відноситься до минулого, коли інформаційні технології не були розроблені для забезпечення ємності ринку, а їх внесок в економічний та соціальний прогрес менше залежав від вільного потоку даних. Закриття цих систем вже неможливо без підриву пов'язаних із цим економічних та соціальних ефектів і, внаслідок цього, призведе лише до ілюзії безпеки [16].

Інновації, засновані на даних, створюють нові проблеми в питаннях конфіденційності. Все більше невеликих і великих компаній, таких як інтернет-магазини, постачальники інтернет-послуг, банки та державні організації збирають величезну кількість персональних даних. Збираючи та аналізуючи великі обсяги

даних, компанії можуть прогнозувати сукупні тенденції, такі як коливання попиту, а також індивідуальні переваги клієнтів, а завдяки спостереженню за індивідуальною поведінкою, фірми вдосконалюють свої продукти та послуги. Однак ця здатність профілювати та відправляти цільові повідомлення та маркетингові пропозиції для окремих осіб також може мати несприятливі наслідки, адже споживачі можуть заперечувати проти того, щоб їх активність у мережі досліджувалась та аналізувалася [77].

Однією з найзначніших змін в онлайн і мобільному середовищі за останнє десятиліття стала поява соціальних мереж і різке збільшення контенту, створюваного користувачами. Широке впровадження цифрових технологій, у тому числі мобільних пристроїв і зростання соціальних мереж корінним чином змінили роль окремих користувачів. Самі користувачі створюють, публікують і обмінюються інформацією, використовуючи різні цифрові платформи, у тому числі соціальні мережі, сайти для обміну фотографіями, рейтингові системи, створюючи при цьому певні загрози особистої безпеки, оскільки в них часто відсутні механізми контролю над тим, що інші користувачі можуть робити з цим контентом. Це породжує складні питання про те, як держава має реагувати на нову роль громадян як творців та розповсюджувачів контенту та особистих даних.

В останні роки великі та малі організації зазнають більш частих і серйозних загроз у цифровому середовищі, що впливає на їхню економічну безпеку. З економічного погляду подібні загрози можуть впливати на репутацію організацій, фінансову складову, завдаючи шкоди їх конкурентоспроможності, підриваючи їх зусилля щодо інновацій та позиції на ринку. Такі погрози можуть порушити доступність, цілісність або конфіденційність інформаційних систем, на яких ґрунтується економічна діяльність.

В таблиці 1.1 систематизовано цифрові загрози та виклики, які суттєво впливають на економічну безпеку.

Таблиця 1.1 - Проблеми економічної безпеки цифрового суспільства [16, 54]

Тип проблем	Опис та приклади
Системні	Проблеми, що стосуються економіки або її значних частин (залежність від цифрових технологій інших держав, відсутність власної елементної бази, проблема «цифрової нерівності»)
Структурні	Структурні проблеми, викликані цифровізацією (наприклад, суттєві зміни на ринку праці та зростання безробіття).
Галузеві	Відсутність цифрових рішень для окремих галузей (наприклад, відсутність власної платіжної системи)
Діяльність окремих підприємств	Крадіжка корпоративних даних, промисловий шпигунство, хакерські атаки, недостатня забезпеченість цифровими технологіями, компетентними кадрами тощо.
Діяльність окремих громадян	Крадіжка, маніпулювання особистими даними.

Подані проблеми можуть бути розв'язані різними способами. Фундаментальною відповіддю на означені виклики цифрового суспільства стають зміни у структурі та підходах до управління економічними системами різного рівня. На перший план у таких змінах виходять горизонтальні команди, спрямовані на отримання результатів. Це вимагає переходу від замкнених, зайве бюрократизованих структур до відкритих організацій, що утворюють мережу. Такі організації є гібридними формами економічної діяльності з гнучкими зв'язками, які встановлюються та переглядаються за необхідністю.

Найважливішими питаннями у таких мережевих структурах стають питання про управління ресурсами в реальному часі та координації діяльності учасників мережі. У рамках розвитку «сегментованої економіки» даний підхід реалізується за рахунок цифрових платформ, за допомогою яких учасники можуть координуватися з метою більш ефективного використання ресурсів (наприклад,

спільне користування житлом, автомобілем тощо).

Подібні інструменти дозволяють ефективніше використовувати ресурси, підвищуючи їх доступність, знижуючи навантаження на навколишнє середовище. У рамках сучасних підприємств такі проблеми вирішуються інструментами цифрової економіки, таких як «хмарні» технології, ERP-систем та інших інструментів.

З розвитком мережових структур економіки стане помітним перетворення індустріальної економіки, створення гнучкої мережі нових структур та нових форм організацій виробничої та економічної діяльності.

Економічні переваги мережових форм полягають у їх здатності до швидкої адаптації в умовах, що змінюються. Внаслідок того, що межі мережових форм організації зазвичай більш легко керовані, ніж межі ієрархій, легшими є модифікації композиції мережових організацій як реакція у відповідь на ці зміни.

Результатами такого розвитку стане збільшення числа дрібносерійних виробництв, індивідуальне виконання виробничих замовлень. Зміни торкнуться інших аспектів економіки, зокрема ринку праці. Вже зараз основними вимогами, що пред'являються роботодавцем до працівників, є вміння працювати в команді, робота в багатозадачному режимі, творчий підхід до вирішення завдань, високий ступінь адаптації в умовах, які швидко змінюються, що характерно для мережових організацій. В цілому ж відбуваються інтелектуалізація праці та капіталу, зростання інформаційної ємності сучасної економіки.

Основним інструментом моніторингу розвитку мережових явищ в економіці є індекс мережевої готовності (Network Readiness Index, NRI) — комплексний показник, запропонований Світовим економічним форумом та міжнародною школою бізнесу "INSEAD". В даний час даний індекс вважається найбільш повним і авторитетним джерелом міжнародної оцінки впливу факторів постіндустріального розвитку на конкурентоспроможність і добробут країн. Він використовується як засіб аналізу для побудови порівняльних рейтингів, що відображають рівень розвитку компонент мережної економіки, і включає наступні субіндекси [80]:

- розвиток навколишнього середовища;
- готовність суспільства до використання цифрових технологій;
- фактичне використання цифрових технологій основними економічними агентами;
- наслідки, що породжують в економіці та суспільстві цифрові технології.

Перші три субіндекси можна розглядати як драйвер, що визначає величину четвертого субіндексу, тобто вплив цифрових технологій на суспільство і економіку.

Для розвитку мережевої економіки потрібні, перш за все, відповідні ринкові умови, державне управління та нормативно-правова база, що утворюють навколишнє середовище. Оцінка ділового та інноваційного середовища визначає якість умов ведення бізнесу.

Готовність країни до мережевої економіки багато в чому залежить і від того, наскільки основні агенти економіки зацікавлені та підготовлені до використання мережевих технологій у своїй повсякденній діяльності. Вона оцінюється наявністю мережевої інфраструктури і доступом до цифрової інформації, вартістю підключення до мереж та рівнем конкуренції в даній галузі, здатністю суспільства до ефективного використання цифрових технологій завдяки наявності основних освітніх навичок.

Формування мережевого укладу, заснованого на високорозвиненій інформаційно управлінській інфраструктурі та ефективному використанні інтелектуального ресурсу, передбачає суттєву зміну всієї соціально-економічної системи суспільства та держави. Мережеві технології займають центральне місце в оновленні ключових сфер життєдіяльності суспільства: державного та муніципального управління, бізнесу, освіти, охорони здоров'я, культури, забезпечення безпеки, суспільного життя. Мережевий компонент економічних відносин забезпечує ефективність діяльності окремих економічних відносин агентів, дозволяє зменшити трансакційні витрати та налагодити мобільну організацію роботи. Можна сказати, що без рішення проблем їх ефективного широкомасштабного використання, без розвитку мережевої інфраструктури

сьогодні неможливо успішне вирішення жодного з пріоритетних завдань соціально-економічного розвитку.

Важливою зміною у підході до управління в сучасних умовах є принципово інше ставлення до людини та її участь у прийнятті рішень. З розвитком цифрової економіки найістотнішим чином змінюються місце і роль людини в умовах нового типу господарювання. Аналіз таких змін включає вивчення цілого комплексу взаємопов'язаних питань: зміна вимог до робочої сили, трансформація системи освіти та професійної підготовки, нові підходи до системи управління. Рівень знань, компетенцій та навичок населення в галузі цифрових технологій є важливим фактором поширення та розвитку цих тенденцій у різних сферах суспільного життя. Для аналізу цього фактора соціально-економічного розвитку застосовується категорія «людський капітал». У класичному трактуванні під людським капіталом розуміється сукупність знань, навичок і здібностей, якими володіє і користується людина у процесі праці і які впливають на її економічну продуктивність. В умовах формування цифрової економіки трактування цього поняття розширюється і найзначніша роль відводиться навичкам у галузі цифрових технологій. Підвищення якості людського капіталу, залучення все більшої кількості людей в освітні процеси, розвиток навичок та компетенцій у сфері цифрових технологій є базисом для формування цифрової економіки та ефективного використання цифрових технологій у різних галузях діяльності [13].

Зміни в попиті на навички представляють дві серйозні проблеми для системи освіти та підвищення кваліфікації. По-перше, незважаючи на визнання того, що попит та навички в майбутньому серйозно відрізнятимуться від сьогоднішніх, їх важко ідентифікувати і прогнозувати через швидкі технологічні зміни. Друга проблема полягає в адаптації системи розвитку до нових умов після того, як попит на навички зміниться.

Нині у низці країн розробляються стратегії розвитку навичок у сфері цифрових технологій, які допоможуть країнам у розвитку сильних сторін та пом'якшенні недоліків їх національних систем освіти. Подібні механізми

розвитку людського капіталу в умовах цифрової економіки, як правило, складаються з трьох компонентів:

- по-перше, це визначення базових навичок, необхідних у цифровій економіці;
- по-друге, прогнозування змін в економіці в цілому і на ринку праці та оцінка здібності системи освіти до адаптації в нових умовах;
- по-третє, використання цифрових технологій для покращення доступу та якості освіти, наприклад, через он-лайн-курси та інші способи отримання знань.

Визначальним фактором розвитку нового типу суспільства і притаманної йому економіки стає домінуюча роль висококваліфікованої творчої праці. Економічна ефективність в сучасних умовах визначається не стільки кількісними показниками чисельності персоналу, скільки наявністю фахівців, здатних створити новий продукт або запропонувати нову послугу, знайти новий спосіб організації виробництва, адекватно реагувати на мінливі ринкові умови. З'являються нові форми людської діяльності, динамічно формується людський капітал, який виражається в знаннях і навичках, що постійно оновлюються. Безперервне навчання та підвищення кваліфікації стають необхідною умовою розвитку сучасної економіки.

В даний час спостерігається тенденція в збільшенні середнього терміну освіти. Цьому сприяє той факт, що безперервне підвищення кваліфікації є запорукою суспільного успіху і стабільного доходу. Тому особливу увагу необхідно приділити підготовці кадрів у сфері інформаційних технологій, а також спеціалістів нових інформаційних професій. Це дозволить підвищити якість людського капіталу як окремих особистостей, так і колективів, а значить, і суспільства в цілому.

У таблиці 1.2 узагальнено принципи систем розвитку навичок в умовах інформатизації.

Таблиця 1.2 - Принципи побудови систем розвитку навичок за умов цифровізації

Принципи	Зміст
Раціональне використання ресурсів	Зважаючи на обмеженість ресурсів інвестиції у створення системи розвитку навичок повинні забезпечувати найбільші економічні та соціальні вигоди
Об'єднання короткострокових та довгострокових цілей розвитку	Ефективна система розвитку навичок необхідна для вирішення структурних навичок і циклічних завдань (таких як зростання безробіття, коли економіка скорочується, або брак кваліфікованих кадрів при економічному підйомі), а також для забезпечення довгострокового стратегічного планування з метою досягнення конкурентних переваг та підтримки структурних змін
Навчання протягом всього життя	Вивчаючи навички як інструмент, який потрібно відточувати протягом усього життя людини, стратегічний підхід дозволяє оцінювати вплив різних видів навчання - починаючи з раннього дитинства і закінчуючи неформальним навчанням з метою збалансування розподілу ресурсів для максимізації економічної та соціальної вигоди
Системність	Узгодження цілей у таких взаємопов'язаних галузях, як освіта, наука, технології та інновації, промисловість, зайнятість, економічний розвиток, міграція та фінанси сприяє виявленню компромісів, уникнення дублювання функцій
Вирівнювання різних рівнів управління	Розгляд проблематики в галузі навичок на місцевому рівні, узгодження національних цілей із місцевими потребами
Залучення всіх зацікавлених сторін	Координація різних рівнів державного управління та широкого кола зацікавлених сторін, включаючи роботодавців, професійних та промислових асоціацій та торгових палат, профспілок, навчальних закладів

Таким чином, дослідження процесів формування глобального цифрового суспільства дозволяє констатувати, що відповіді на виклики, що стосуються

різних аспектів економічної діяльності, вимагають визначення взаємопов'язаних і всеосяжних підходів на стику різних наукових дисциплін у поєднанні з інтелектуальною глибиною та всебічним обліком довгострокових наслідків прийнятих рішень. Світова спільнота здатна знайти відповіді на питання, що виникають, лише за умов об'єднання зусиль і ресурсів, що вимагає перегляду системи економічних відносин, що склалася.

Інновації на основі даних (DDI) сприяють соціально-економічному розвитку, допомагають вирішувати складні соціально-економічні проблеми. У такому цифровому середовищі, заснованому на передачі даних, також посилюються проблеми забезпечення цифрової конфіденційності, економічної безпеки. Економічний розвиток досягається за рахунок відкритого обміну даними, що, у свою чергу, збільшує складність забезпечення кібербезпеки та управління ризиками в цифровому середовищі. При цьому ризики, пов'язані з цифровістю середовища, повинні розглядатися в соціальній та економічній площинах, а не лише з технічного погляду. Важливо виконувати умови перевищення очікуваними вигодами від розвитку цифрової економіки будуть її негативні прояви. Окремої уваги заслуговує підтримка бізнесу в зниження ризиків від використання цифрових технологій у економічній діяльності [9].

Найчастіше підприємства стикаються з проблемами в цифровому середовищі, маючи слабкі можливості щодо забезпечення власної економічної безпеки в нових умовах. Така ситуація вимагає нових підходів до управління ризиками, включаючи ринкові інструменти, такі як страхування.

1.3 Загрози інформаційної безпеки в епоху цифрової трансформації

Як було зазначено вище, процеси, які викликає цифрова трансформація (ЦТ), мають і негативну сторону. Революційні зміни, які привносить у бізнес ЦТ, породили певні проблеми для служб інформаційної безпеки (ІБ), а саме виникли

нові вектори загроз ІБ та розширився спектр уразливостей для потенційних кібератак.

«Модна технологія» DevOps є предметом особливої настороженості фахівців ІБ, оскільки вона принципово змінила взаємини між розробниками софту, системними адміністраторами, службами технічної підтримки та кінцевими користувачами. (Методологія DevOps означає інтеграцію діяльності розробників та фахівців з обслуговування ПЗ, мереж та обладнання у командах та компаніях).

Також хочеться відзначити, що однією із серйозних перешкод для швидкого впровадження ЦТ у компаніях є старі (успадковані) технології, які обслуговують виробничі та офісні процеси вже багато років. З одного боку, їх неможливо замінити швидко (без зупинки бізнес-процесів), а з іншого боку вони погано вписуються в процеси цифрової трансформації та несуть у собі численні загрози ІБ [16].

Розглянемо основні проблеми інформаційної безпеки в умовах ЦТ.

1 Непрозорість подій ІБ у корпоративній інфраструктурі підприємств.

У великих компаніях повсюдно використовують різні технологічні локації, розгорнуті в хмарних сервісах, причому оснащені власними інструментами ІБ і різними внутрішніми сервісами. Однак, поки що є проблеми, як з інтеграцією таких рішень, так і з прозорістю та фіксацією всіх інцидентів та подій ІБ у такій складній ІТ-інфраструктурі. Мало того, цифрова трансформація передбачає значне зростання як хмарних рішень, так і ускладнення корпоративної інфраструктури за рахунок впровадження IoT, блокчейну, тощо.

2 Труднощі з питанням автоматизації всіх процесів ІБ.

У звичайній середній або навіть великій компанії багато процесів інформаційної безпеки залишаються неавтоматизованими, при цьому не вироблено навіть загального підходу до їх автоматизації. Однак у співробітників департаментів ІБ таких компаній є впевненість у тому, що захист працює по всіх можливих векторах атак, як усередині периметра, так і в хмарах, на мобільних пристроях, веб-серверах і т. д. Можливо, окремі рішення ІБ (антивіруси,

міжмережні екрани, системи виявлення вторгнень тощо) поки що забезпечують певний рівень безпеки на окремих ділянках і знижують кількість інцидентів ІБ, але без вироблення загальної стратегії та політики безпеки в такій організації обов'язково будуть проблеми з ІБ у майбутньому, в ході впровадження ЦТ .

3 Інтеграція ІБ-рішень.

Хочеться відзначити, що в більшості організацій досі погано з інтеграцією різних ІБ-рішень немає наскрізної видимості всіх загроз, погано з контролем відповідності вимогам регуляторів (compliance).

4 Гнучке масштабування.

За результатами опитувань та досліджень у галузі інформаційної безпеки експертами з'ясовано, що на багатьох підприємствах чверть корпоративної інфраструктури так і залишається незахищеною. Відповідно до зростання ІТ-інфраструктури, викликаного цифровою трансформацією, а також у зв'язку з ускладненням кібератак, виникає потреба в масштабованості ІБ-рішень. І навіть якщо в компанії є рішення, що ефективно працюють, захищають окремі компоненти інфраструктури ІТ (наприклад, антивіруси, міжмережові екрани і т.д.), то в цілому це не підвищує загальний рівень безпеки в організації через погану інтеграцію і масштабованість цих окремих рішень.

На даний момент найбільшу проблему у фахівців з кібербезпеки викликають складні для блокування поліморфні кібератаки, цільові кібератаки (APT, advanced persistent threat, «розвинена стійка загроза»), а також зростання використання методології DevOps, яка підвищує ризики несвоєчасного виявлення нових ураз.

5 Наслідки оновлень ПЗ.

До цих пір залишаються небезпечними загрози, пов'язані з оновленням софту, оскільки часто разом з «патчами» та «апдейтами» може бути інстальовано і шкідливе програмне забезпечення.

У майбутньому ЦТ може бути використана як для позитивних змін у соціумі, так і для реалізації загрози для світової стабільності та безпеки. Таким негативним прикладом є так звана «кіберзброя». Для того, щоб в умовах

нестабільності, що постійно наростає, позначити стратегію безпеки свого бізнесу та систем державного управління, необхідно усвідомити для себе в цілому, що таке «безпека» і яка вона буває.

Таким чином, саме поняття «безпека» поділяється на 3 великі групи: особисту, громадську та державну [16].

Особиста безпека - це такий стан, коли людина захищена від будь-якого виду насильства (наприклад, психологічного, фізичного чи ін.)

Громадська безпека - здатність соціальних інститутів держави захистити особистість та суспільство від різного виду загроз (в основному внутрішніх).

Державна безпека - система захисту держави від зовнішніх та внутрішніх загроз.

Ще одним важливим напрямом у галузі безпеки є інформаційна безпека та захист інформації. Мета роботи фахівців із захисту інформації - це забезпечення її конфіденційності, доступності та цілісності. Загалом, ці три ключові принципи ІБ називають тріадою CIA, нижче розкриємо зміст цих понять [8].

Confidentiality (з англ. "конфіденційність") - це властивість інформації бути закритою для неавторизованих осіб;

Integrity (з англ. «цілісність») - властивість збереження правильності та повноти даних;

Availability (з англ. — «доступність») — властивість інформації бути доступною та готовою до використання на запит авторизованого суб'єкта.

Основна мета інформаційної безпеки в контексті ЦТ — забезпечити захищеність як інформації, так і IT-інфраструктури від випадкових або навмисних впливів (атак і т.д.), які можуть завдати неприйнятної шкоди власникам інформаційних активів [4].

Особливу увагу необхідно приділити інцидентам ІБ на об'єктах критичної інформаційної інфраструктури (КІІ), це можуть бути як таргетовані атаки (АРТ), так і техногенні катастрофи, фізичне викрадення активів та інші загрози. Відповідно до ускладнення атак нарощуються і засоби оборони (тобто інфраструктура ІБ).

На цьому фоні все більшої популярності набирають системи SIEM (Security information and event management), основне завдання яких — це моніторинг корпоративних систем та аналіз подій безпеки в режимі реального часу, у тому числі з широким використанням систем ІІ та глибокого машинного навчання (Deep learning) .

Великі технологічні компанії, які лідирують в галузі ЦТ, набагато частіше за інших інтегрують свої продукти та засоби ІБ у єдину архітектуру корпоративної безпеки. Слід зазначити, що в таких компаніях віддають перевагу стратегічному підходу та формуванню політики безпеки, що дозволяє [5]:

- швидко виявляти загрози та оперативно реагувати на них;
- забезпечувати якісний захист інформаційних активів;
- мати прозоре виявлення загроз технологічне середовище.

Лідери цифрової трансформації, як правило, охочіше автоматизують ІБ-процеси в компанії, це набагато ефективніше за ручний моніторинг загроз і подій ІБ, який застосовувався повсюдно до періоду ЦТ. Позитивним прикладом такої автоматизації та комплексного підходу є запровадження SOC (Security Operations Center, центр забезпечення безпеки). Однак потрібно враховувати, що налаштування автоматизації всіх робочих процесів потребує більшого часу для тестування та необхідності залучення грамотних спеціалістів.

Однією з особливостей ІБ в епоху цифрової трансформації є впровадження в корпоративну систему засобів централізованого контролю відповідності як промисловим стандартам, так і стандартам ІТ та ІБ, що підвищує ефективність роботи такого напрямку ІБ, як compliance.

Однією з серйозних перешкод на шляху компаній до ЦТ є необхідність забезпечення високого рівня інформаційної безпеки, що не завжди є посильним для більшості компаній, особливо фірмам із сектора SMB. При цьому необхідно враховувати фактори наростання як внутрішніх, так і зовнішніх загроз ІХ, пов'язані зі значним зростанням сектору кіберзлочинності, а також ризиками, що виникають природним шляхом у ході реалізації методології DevOps, хмарних технологій, IoT тощо.

Один із досить нових, але ефективних підходів у сфері безпеки інформаційних активів — це застосування методів проактивного захисту, здатних не просто захистити, а й запобігти кібератакам. Тут хочеться відзначити такі технології, як «ханіпоти» (honeypots і honeynets), а також більш просунуті системи розгортання розподіленої інфраструктури помилкових цілей (Distributed Deception Platform, DDP) [8].

У результаті, можна виділити найкращі практики ІБ, які ми можемо порекомендувати компаніям та бізнесу під час процесу цифрової трансформації:

- побудувати єдину архітектуру безпеки, яка забезпечить централізоване управління ІТ-інфраструктурою та прозорість усіх подій ІБ;
- розробити стратегію захисту корпоративної мережі та політику безпеки компанії;
- запровадити вбудовані засоби контролю відповідності стандартам та вимогам регуляторів;
- використовувати методи як превентивного, так і проактивного захисту.

1.4 Інформаційна безпека у логістиці та на транспорті

Цифровізація широко поширилася серед компаній у сфері транспорту та логістики (ТіЛ), удосконаливши весь цикл процесів у галузі. Це сприяло безпрецедентному підвищенню ефективності, спрямованому розширення каналів доходу. Це позитивний бік. Мінус у тому, що цифровізація виявила низку проблем у компаніях ТіЛ, які роблять їх надзвичайно вразливими перед кібератаками. Це стосується кожного сектора галузі, включаючи морські, залізничні, автомобільні перевезення, логістику та доставку посилок. Наслідки коштують дорого, порушують роботу і можуть спричинити фінансову відповідальність, особливо якщо допускається витік конфіденційних відомостей про клієнтів [6].

Є безліч факторів уразливості транспорту та логістики. По-перше, ширше

використання операційних технологій (BOT), нових комунікаційних та бездротових каналів, безпосередньо пов'язаних із цифровими екосистемами компаній ТіЛ, роблять компанії легкою метою для хакерів. По-друге, це застаріле регулювання та стандарти в галузі ІТ, недостатня поінформованість у галузі кібербезпеки і, нарешті, чи не найістотніший чинник - брак кваліфікованих кадрів, здатних забезпечити захист.

Кібератаки в секторі ТіЛ раніше відбувалися раз на кілька років. Тепер, схоже, одна-дві з них організовуються щомісяця. Деякі їх масштабні. Наприклад, кібератака в травні 2021 року, по суті, приблизно на тиждень зупинила роботу компанії Colonial Pipeline, яка постачає нафтопродукти майже для половини східного узбережжя США. Компанія заявила, що сума викупу та втрати через порушення діяльності могли досягти 50 мільйонів доларів і більше. Інші кібератаки, навіть спрямовані на великі транспортні компанії, які страждали вже не раз, привертають менше уваги преси, але часто включають дезорганізацію систем електронної пошти та логістики.

Крім того, хакери все частіше намагаються вкрасти дані, що зберігаються в мережах, які життєво необхідні для модернізації та розвитку галузі ТіЛ, оскільки вони забезпечують більш ефективне та якісне обслуговування клієнтів. Ці мережі дозволяють впровадити цифрові покращення, такі як автоматизовані замовлення, відстеження вантажу та доступ до інформації облікового запису. Хоча подібні плюси для клієнта є надзвичайно цінними, вони вимагають зберігання великих обсягів конфіденційної інформації, зібраної через онлайн-платформи, телефонні програми та інші мобільні пристрої, які через відсутність суворих протоколів кіберзахисту є одними з найненадійніших каналів.

І, в той час як охоплення потенційних кібератак у секторі ТіЛ збільшується, а характер ризику стає дедалі різноманітнішим, витрати на злам суттєво скоротилися.

Враховуючи зростаючу актуальність проблеми, компанія BCG досліджувала причини, через які галузь настільки вразлива перед кібератаками. У BCG виробили ряд інтегрованих рішень, які можуть застосувати компанії, щоб знизити

вплив цих ризиків і створити життєздатні і надійні методи захисту від них.

Найпростіший підхід до проблем, з якими стикаються компанії ТіЛ, - це розподіл їх факторів уразливості за трьома категоріями: технології, регулювання, а також люди та процеси. Необхідно уважно вивчити кожен з цих категорій, щоб зустріти у всеозброєнні нові загрози, яким схильна галузь в цілому [2].

Технології. У кожному сегменті галузі ТіЛ очевидне розширення поверхні кібератак. Наприклад, серед морських перевізників щодо прості системи оповіщення про лиха та забезпечення безпеки були замінені повноцінними місцевими мережами, що базуються на хмарних технологіях, такими як програма електронної навігації Міжнародної морської організації (ММО). Ці мережі є привабливою метою для хакерів, оскільки вони постійно збирають, інтегрують та аналізують бортову інформацію, щоб відстежити положення суден, дані про вантаж, технічні проблеми та цілий спектр питань, пов'язаних з океанічним середовищем.

Аналогічна ситуація в залізничному секторі: традиційні провідні системи управління рухом поїздів (СУРП), зв'язок яких із зовнішніми системами раніше був обмежений, поступаються бездротовим стандартам, таким як GSM-Railway - відносно широка мережа, що поєднує поїзди з пунктами управління рухом. Як і у випадку з усіма пасажирськими компаніями, компанії ТіЛ надають інформаційно-розважальні послуги та використовують інше обладнання, що додає ще один рівень підключення до Інтернету.

Хоча ці мережі, які по суті пов'язують системи ВОТ з внутрішнім ІТ-обладнанням, таким як сервери, комп'ютери і мобільні пристрої, і самі по собі представляють нові шляхи для атаки хакерів, вони іноді стають ще більш вразливими через брак розуміння важливості захисту від кібератак із боку як постачальників ВОТ, і компаній ТіЛ. У деяких випадках постачальники ОТ вимагають вбудувати в їхнє обладнання потенційно вразливі інтерфейси управління для віддаленого доступу, контролю та усунення несправностей. Крім того, комп'ютерне обладнання компаній ТіЛ рідко оновлюється для відповідності суворим протоколам безпеки.

Однаково насторожує і те, що крім відносин з окремими постачальниками від компанії ТіЛ утворюють більш ефективні та технологічні партнерства зі своїми постачальниками та розповсюджувачами, які все більше залежать від мережових зв'язків. Протоколи кібербезпеки цих партнерів зазвичай не контролюються, через що компанії ТіЛ не отримують інформації про те, чи не зростає ризик через їх інтегровані екосистеми.

Регулювання. Хоча комерційні та експлуатаційні аспекти сектору транспорту та логістики регулюються в багатьох регіонах, існує відносно невелика кількість положень, що стосуються кібербезпеки. Незважаючи на глобальний характер діяльності сектора — чи, можливо, через нього — регулюючим органам складно домовитися чи зосередитися на комплексі норм кібербезпеки, які мали б дотримуватися компанії ТіЛ, де б вони не працювали. За відсутності цього комплексу вкладення в кібербезпеку не оптимізовано так, щоб знизити загальний вплив ризику на організації.

Тим не менш, усвідомлюючи можливу небезпеку масштабної кібератаки на галузь ТіЛ для світової торгівлі та економічної стабільності, регулюючі органи починають займати активнішу позицію і вимагати більшої захищеності мереж компаній. Пропоновані або вже прийняті інструменти регулювання включають Директиву ЄС про мережеву та інформаційну безпеку (NIS) і стандарти CLC/TS 50701 і EN 50126, що швидко набирають чинності, для залізничного транспорту, а також ряд правил для морського транспорту, що вводяться Міжнародною морською організацією. По різному ці заходи регулювання спрямовані на дотримання мінімальних норм для захисту найважливіших даних та процесів компаній, особливо даних про клієнтів та інформації про перевезення вантажів.

Люди та процеси. Кіберзагрози постійно розвиваються, але загальна риса деяких найбільш уразливих областей – це люди. Наприклад, співробітники, не здатні розпізнати лист фішингу, можуть бути легко використані хакерами на початковому етапі атаки. Насправді можна сказати, що першим кроком у ланцюжку атак зазвичай і стають дії самих постраждалих, враховуючи, що значно більше половини витоку даних можна безпосередньо простежити і виявити

недоліки в організаційних процесах і компетенціях співробітників або брак їх знань про кібератаки.

Погіршує ситуацію величезний глобальний кадровий дефіцит фахівців з кібербезпеки, що зростає. 4 мільйони посад фахівця з ІКТ були вакантні у 2020 р., згідно з даними галузевої групи із захисту інформації ISC2. Недолік добре підготовлених кіберфахівців частково пояснюється тим, що вища освіта в галузі кібербезпеки — відносно молоде явище, яке існує лише близько десяти років.

Цей брак гостро відчувається в галузі, що розглядається, оскільки випускники з кваліфікацією в галузі кібербезпеки та досвідчені фахівці, які вже працюють у цій сфері, зазвичай не розглядають перевезення та логістику як кращу сферу для побудови кар'єри.

Частково це проблема сприйняття. Більшість кандидатів на посаду не дивляться на компанії ТіЛ як на інноваційні робочі місця, де фахівці з технологій могли б розвернутися в таких галузях, як роботизація та автоматизація, аналіз даних, блокчейн, безпілотні автомобілі тощо. Замість того, щоб зробити роботу в галузі кібербезпеки привабливішою — можливо, запропонувати вигідніші зарплати та соцпакети, а також заохочувати інновації — багато компаній ТіЛ ставляться до кібербезпеки як до витратної одиниці, яка має вкладатися у жорсткі бюджетні межі.

Компанії ТіЛ повинні почати приймати програму кібербезпеки з оцінки рівня кіберзахисту в їхньому обладнанні та програмах ВОТ та ІТ. Далі вони можуть вжити заходів захисту у найважливіших та вразливих додатках та мережах. Визначення областей з підвищеним ризиком кібератак та розробка портфеля заходів захисту можуть бути спрощені за допомогою моделей та інструментів, таких як програма управління кіберрисками та їх кількісною оцінки. Компанії повинні оцінити свої фактори вразливості на основі ризикового підходу, де пріоритет надаватиметься ймовірності та наслідкам реалізації кіберзагроз для ключових активів. Потім можна ранжувати проєкти на основі здатності кожного з них підвищити стійкість з урахуванням витрат і, таким чином, по суті, оптимізувати свої бюджети вкладень у кібербезпеку.

Після вжиття цих запобіжних заходів компаніям ТіЛ потрібно зосередитися на реалізації більш комплексних концепцій кіберзахисту, таких як архітектура нульової довіри. Дана методологія передбачає, що всі пристрої, користувачі або програми, які намагаються взаємодіяти з мережею, є потенційною загрозою. Стратегію нульової довіри можна реалізувати, сегментуючи та розділяючи мережі з використанням технології демілітаризованої зони (ДМЗ), що забезпечує жорстко контрольоване середовище, де відстежуються зв'язки всередині організації та поза нею. Того ж принципу слід дотримуватися і для більш строгого контролю внутрішніх процесів, де це можливо, включаючи автентифікацію користувачів, програм та кінцевих пристроїв перед наданням їм доступу до інформації або активів. Компанії ТіЛ можуть зробити три дії, щоб удосконалити свої внутрішні навички в галузі кібербезпеки.

По-перше, у корпоративній культурі слід перейти від неуваги до питань кібербезпеки до визнання гострої необхідності боротьби з погрозами. У кожному підрозділі ідея зміцнення кібербезпеки по всій організації має бути явним та ключовим аспектом. Часті тренінги, що підвищують рівень обізнаності з кібербезпекою, можуть серйозно сприяти формуванню колективу, що усвідомлює ризики. Потрібно наголошувати на заходах, які можуть вжити окремі співробітники, щоб забезпечити захист від хакерів, такі як захист паролів та увага до підозрілої діяльності в мережах компанії.

По-друге, цю особливу увагу до управління кіберризиками варто використовувати, щоб залучити фахівців з кібербезпеки з університетів та приватного сектору. Заявіть, що мета організації — стати випереджаючим часом лідером у сфері кібербезпеки. Компанії можуть залучити найкращих фахівців з кібербезпеки, повідомивши їм, що вони зможуть розробити програми кіберзахисту з нуля, використовуючи останні технології та замінюючи застарілі системи. Організаціям також можна розглянути варіант отримання консультацій у неупереджених постачальників обладнання, які не прагнуть продати свої технології.

Зрештою, треба знайти серед технологічних співробітників компанії людей,

які готові зайнятися ініціативами в галузі кібербезпеки та які продемонстрували основні здібності, необхідні успішним кандидатам. Підвищення кваліфікації цих працівників та пропозиція їм компенсації, а також заходи заохочення залежно від посади за освоєння необхідних навичок могли б дозволити компаніям ТіЛ швидко заповнити щонайменше частину бракуючої робочої сили в кібербезпеці.

Багатьом компаніям ТіЛ може здатися, що заходи, які необхідно вжити для скорочення ризиків кібербезпеки, є непосильними. Однією з практичних порад для підвищення прозорості та поінформованості про мережі ІТ та ВОТ та про їх слабкі місця може бути створення центру обробки кіберінформації. Це центр займався б відстеженням, організацією та наглядом у галузі управління, діяльності, аналітики, процесів та технологій, пов'язаних з кібербезпекою, забезпечуючи розподіл даних та відомостей між ключовими учасниками процесу, щоб виявляти та усувати кіберзагрози.

Крім того, центр обробки кіберінформації оптимізував би діяльність, поєднуючи управління та системи контролю ІТ та ОП. У центрі має поєднуватися досвід і знання фахівців як в галузі ІТ, так і ВОТ, дозволяючи відстежувати будь-яку нестандартну активність і в інтернеті, і у внутрішніх системах — або, що важливо, у точці злиття цих двох систем, яка може вчасно сигналізувати про кібератаку .

Щоб ефективно впоратися з ризиком, компанії ТіЛ повинні створити рівні кіберстійкості, що відповідають високим стандартам, захищати партнерські ланцюжки поставок та дотримуватися орієнтованого ризику підходу при розробці засобів безпеки. Компаніям потрібні інструменти, що дозволяють їх організаціям розвиватися та вживати відповідних заходів кіберстійкості, що охоплюють кілька вимірювань — від технологій до регулювання та процесів до співробітників. Для багатьох компаній ТіЛ заздалегідь продумана політика в галузі кібербезпеки досі не була пріоритетом. Але швидко зростаюче число кібератак і інструменти регулювання, що з'являються, змушують організації усвідомити, що вони недовго зможуть продовжувати зберігати відносну байдужість. Хакери стають все активнішими, і вони добре обізнані про те, які компанії приділяють кібербезпеці

недостатньо уваги. Компаніям ТіЛ бажано не опинятися у цьому списку.

Висновки до розділу 1

Цифрова трансформація — це насамперед інноваційний процес, що вимагає внесення докорінних змін у промислові технології, соціум і культуру, фінансові транзакції та принципи створення нових продуктів та послуг. Фактично, це не просто набір ІТ-продуктів, що підлягають розгортанню, і рішень у компаніях і на виробництві, а глобальний перегляд підходів і стратегій у бізнесі, що виконується за допомогою інформаційних технологій. Цифрова трансформація є перехідним періодом до шостого технологічного укладу під час четвертої промислової революції (Industry 4.0).

Не всі компанії готові до нових і досить жорстких вимог, які їм висуває ЦТ, а саме, до повної модернізації методів ведення бізнесу, перегляду внутрішніх бізнес-процесів та нової культури взаємовідносин усередині компанії. Мало того, менеджмент має бути підготовлений як до позитивних, так і негативних наслідків цифрової трансформації.

Цифрова трансформація — це не просто автоматизація та цифровізація окремих виробничих процесів «на місцях», це інтеграція звичайних офісних та промислових технологій, які ми використовуємо щодня, з абсолютно новими ІТ-напрямами, специфічними для ЦТ (хмарні обчислення, штучний інтелект та машинне навчання, IoT і т.д.).

Розвиток цифрових систем покликаний, в першу чергу, покращувати якість життя, робити транспорт більш зручним для людей та розвитку бізнесу, а інноваційні розробки у моделюванні транспортних систем та регулювання транспортних потоків повинні надавати кінцевим споживачам більшу інформативність і безпеку, а також якісно підвищувати рівень взаємодії учасників.

Подальша реалізація завдань розвитку транспорту в цифровому порядку

дозволить запропонувати партнерам перевірені рішення щодо спрощення та підвищення ефективності взаємодії. І в першу чергу, по помітному зниженню тимчасових та фінансових витрат у транспортному повідомленні, транскордонних переходах, що допоможе також і в реалізації міжнародних ініціатив для інтеграції у світову транспортну систему.

Реалізація та впровадження передових цифрових технологій дозволить підвищити задоволення потреб у перевезеннях. А пріоритетними і перспективними напрямками розвитку перевезень слід вважати цифрові технології при оформленні перевезення та контроль доставки. Такі технології необхідно впроваджувати на всіх цілях руху вантажів від відправника до одержувача. Оновлена транспортна система, яка використовує такі технології, забезпечуватиме чітку, злагоджену роботу всіх ланок перевезення пасажирів, вантажів, забезпечувати максимальний комфорт, якість та швидкість перевезення.

Таким чином, в результаті проведеного в розділі дослідження з метою систематизації проблем забезпечення економічної безпеки в умовах розвитку глобальної цифровізації отримані наступні теоретичні результати.

По-перше, показано, що пріоритетною за дачею забезпечення економічної безпеки, особливо помітної в швидко мінливих умовах сучасного глобального світу, є прогнозування викликів та загроз все загальної цифровізації.

По-друге, виділено особливості розвитку цифрової економіки, які включають наявність інтелектуальних активів, збільшення значимості даних, мережеву організацію господарювання, широке впровадження інтернету та глобальний характер обміну даними.

По-третє, систематизовано проблеми економічної безпеки в умовах цифрової економіки, диференційовані на системні, структурні та галузеві проблеми, особливо сфери транспорту, а також підприємств та окремих громадян. До основних проблем економічної безпеки віднесено проблеми «цифрової нерівності», відсутності власної елементної бази, зміни на ринку праці, промисловий шпигунство, маніпулювання особистими даними та інші.

По-четверте, визначено інструменти вирішення проблем цифрового

суспільства, до яких віднесено цифрові платформи для розвитку «часткової економіки», а також «хмарні» технології та методи обробки великих баз даних. Інструментом моніторингу розвитку мережевого цифрового суспільства є індекс мережевої готовності

По-п'яте, сформульовані принципи щодо будови систем розвитку навичок в умовах цифровізації, що дозволяють вирішувати проблеми економічної безпеки суспільства.

До таких принципів віднесено раціональне використання ресурсів, об'єднання короткострокових і довгострокових цілей розвитку, навчання протягом усього життя, системність, вирівнювання різних рівнів управління та залучення до процесу цифровізації всіх зацікавлених сторін.

Широкомасштабне вирішення проблем економічної безпеки транспорту у цифровому суспільстві дозволить забезпечити цілеспрямоване формування процесу економічного зростання та підвищення економічного добробуту всього суспільства.

2 Дослідження стану і тенденцій розвитку підприємств залізничного транспорту

2.1 Загальна характеристика АТ «Укрзалізниця»

Акціонерне товариство «Українська залізниця» – національний перевізник вантажів та пасажирів. Метою діяльності товариства є задоволення потреб у безпечних та якісних залізничних перевезеннях, забезпечення ефективного функціонування та розвитку залізничного транспорту, створення умов для підвищення конкурентоспроможності галузі тощо [47].

Свою господарську діяльність АТ «Укрзалізниця» розпочало 1 грудня 2015 року. Товариство є правонаступником усіх прав і обов'язків Державної адміністрації залізничного транспорту України, а також підвідомчих підприємств і закладів, що мали статус окремих юридичних осіб.

Наразі компанія забезпечує 82 % вантажних і майже 50 % пасажирських перевезень, які здійснюються усіма видами транспорту. За обсягами вантажних перевезень українська залізниця займає четверте місце на Євразійському континенті, поступаючись, зокрема, залізницям Китаю та Індії.

Наразі АТ «Укрзалізниця» розвивається в умовах системної кризи, що виражається в негативній динаміці низки показників його розвитку. Сучасний стан і тенденції розвитку підприємств залізничного транспорту в останні роки свідчать про критичне скорочення їх економічного потенціалу і поступову втрату технічної спроможності повноцінно задовольняти вимоги споживачів до транспортних послуг [23].

Реалізація корінних організаційно-структурних змін у системі господарювання залізничного транспорту і поступова лібералізація ринку залізничних перевезень відбувалася в умовах поглиблення міждержавних конфліктів, ускладнення політичної та економічної ситуації, впровадження епідеміологічних обмежень у зв'язку з поширенням пандемії і скорочення обсягів

роботи підприємств, що призвело до загострення конкуренції на ринку транспортних послуг і скорочення частки АТ «Укрзалізниця» на ринку перевезень України.

2.2 Аналіз кількісних та якісних показників роботи компанії

Підвищення ефективності виробництва характеризується більш повним задоволенням потреб суспільства, у зв'язку з чим головним показником економічної ефективності виробництва виступає виробництво продукції у натуральному вираженні з характеристикою її натуральних властивостей. Продукцією транспортної системи є транспортування/переміщення вантажів та пасажирів.

На кожному виді транспорту діє система кількісних і якісних показників з урахуванням специфіки кожного виду транспорту. Але існують такі кількісні показники, які є загальними для всіх видів транспорту [55].

Для вимірювання роботи з перевезення використовують такі показники:

перевезення вантажів, пасажирів;

– відправлення і прибуття вантажів, пасажирів;

– вантажообіг;

– пасажирообіг.

Ці натуральні показники визначаються вантажо- та пасажиропотоками між кореспондуючими пунктами.

Вантажопотоки характеризують транспортно-економічні зв'язки, які створюються в процесі виробництва й обміну товарами між відправником та отримувачем вантажу і розподіляються за різними шляхами сполучення. Вантажопотоки характеризуються: – напрямком і розміром вантажообміну, які залежать від розміщення виробництва, пунктів відправлення вантажу, пунктів споживання і баз складування товарів, технологічних особливостей виробництва та

його спеціалізації, розміщення шляхів сполучення і перевізної здатності транспорту, а також від системи організації товароруку; – відстанню перевезень; – періодом перевезень (доба, місяць, квартал, рік).

Сумарний вантажопотік транспортної мережі складається з окремих вантажопотоків у прямому та зворотному напрямках. Прямим є напрямок з більшим вантажообігом. Вивчення вантажопотоків необхідне для аналізу транспортного ринку, виявлення нераціональних перевезень, визначення сфер ефективного використання різних видів транспорту та обґрунтування перспектив його розвитку.

Класифікація вантажопотоків [69]:

- за призначенням: міжнародні, міжрайонні, місцеві та внутрішньогосподарські транспортно-економічні зв'язки;
- за видами вантажів: визначаються та аналізуються основні масові вантажі, частка яких у загальному обсязі перевезень значна для певного регіону країни;
- за видами транспорту: виділяють передусім універсальні види транспорту загального користування, які виконують масові первинні перевезення (залізничний, річковий, морський); автомобільний транспорт виконує значну частину повторних перевезень, які аналізують окремо.

Пасажиропотік – це кількість пасажирів, перевезених транспортом у певному напрямку. Пасажиропотоки характеризуються напрямком (прямий і зворотний), періодом перевезень (доба, місяць, квартал, рік), обсягами перевезень, кількістю прибулих та відправлених пасажирів.

Пасажиропотоки можуть бути [32]:

- постійними або змінними (за годинами доби, за днями тижня, за місяцями року);
- одно- і двосторонніми;
- рівномірними і нерівномірними;
- періодично виникаючими та зникаючими.

Кількісні показники діяльності АТ «Укрзалізниця» за 2016- 2022 рр. наведено в таблиці 2.1 та на рисунках 2.1 та 2.2.

Таблиця 2.1 – Аналіз кількісних показників діяльності АТ «Укрзалізниця»

Показник	Значення за роками						
	2016	2017	2018	2019	2020	2021	2022
Вантажообіг, млн ткм	187557,5	191914,1	186344,1	181844,7	175587,1	18031,0	165935,7
Обсяг перевезених вантажів, млн т	344,1	339,5	322,3	312,9	305,5	314,3	318,2
Кількість перевезених пасажирів, млн. пас.	389,5	165,0	158,0	154,8	68,3	81,3	1600,6
Пасажиروобіг, млн.пас.км	37360,1	28001,3	28614,9	28356,0	10696,2	15709	31142,8

Аналізуючи динаміку кількісних показників роботи підприємства за період 2016-2022 рр. можна дійти наступних висновків. Протягом 2016-2022 рр. обсяг перевезень кожного року зменшувався, у 2022 р. він становив 318,2 млн. т, що на 7,5 % менше порівняно з 2016 р. Найнижчим цей показник був у 2020 році та склав 305,5 млн т , що на 11,2% нижче ніж у 2016 році (рисунок 2.1).



Рисунок 2.1 -Показники обсягу перевезених вантажів АТ «Укрзалізниця» за 2016-2022 рр.

Пасажирообіг підприємств залізничного транспорту у свою чергу також характеризується тенденцію падіння (рисунок 2.2). У цьому сенсі слід вказати на той факт, що починаючи з 1 січня 2017 р. змінився порядок обліку перевезень пасажирів залізничним транспортом у приміському сполученні, що мають пільгу на безкоштовний проїзд. Разом із загостренням коронакризи і обмеженням міжнародної та внутрішньої мобільності населення це в сукупності призвело до такого роду коригування обсягових показників роботи підприємств залізничного транспорту у сфері пасажирських перевезень. Збільшення показника кількість перевезених пасажирів у 2022 році пов'язано з агресією рф.



Рисунок 2.2 - Показники кількості перевезених пасажирів АТ «Укрзалізниця» за 2016-2022 рр

Змінювалися і якісні показники роботи підприємства (таблиця 2.2). Покращується ефективність використання вагонного парку: протягом 2016-2020 рр. оборотність вагона зменшилася з 9,56 діб у 2016 р. до 7,82 діб у 2020 р. (найгірше значення у 2018 р. – 10,35 діб). Позитивною динамікою характеризуються такі показники: простій вагонів під однією вантажною операцією (зниження з 66,01 до 23,86 годин, найгірше значення у 2018 р. – 66,55 год.); середньодобова продуктивність вагона (збільшення з 3591 до 4555 т-км.

нетто, найкраще значення у 2020 р. – 4555 т-км. нетто). Негативною динамікою характеризуються такі показники: простій вагонів під однією технічною операцією (зростання з 11,45 до 11,55 год., найкраще значення у 2016 р. – 11,45 год.); середня дільнична швидкість (зниження з 45,1 до 42,4 км/год., найкраще значення у 2017 р. – 45,2 км/год.); середня вага вантажного поїзда (зниження з 3407 до 3224 т., найкраще значення у 2016 р. – 3407 т); середньодобова продуктивність локомотива (зниження з 1379 до 1238 тис. т-км бруто, найкраще значення у 2017 р. – 1410 тис. т-км бруто).

Таблиця 2.2 – Аналіз якісних показників діяльності АТ «Укрзалізниця»

Показник	Значення за роками					
	2016	2017	2018	2019	2020	2021
Обіг вантажного вагона, діб	9,56	9,34	10,35	9,68	7,82	7,71
Простій вагонів під однією вантажною операцією, годин	66,01	62,54	66,55	50,57	23,86	24,93
Середня вага вантажного поїзда бруто, тонн	3407	3357	3264	3208	3224	3226
Середньодобова продуктивність вагона, т-км нетто	3591	3753	3497	3775	4555	4604
Середня дільнична швидкість, км/годин	45,1	45,2	43,3	42,1	42,4	35,5
Середньодобова продуктивність локомотива т-км, тис. бруто	1379	1410	1227	1161	1238	1232

Значне погіршення якісних показників роботи підприємств залізничного транспорту стало результатом скорочення їхнього технічного ресурсу для здійснення перевезень, що пов'язано з наростанням проблеми зношеності і технічної непридатності залізничної інфраструктури і рухомого складу

Таким чином, загалом слід відзначити неоднорідність тенденцій розвитку підприємств залізничного транспорту в розрізі кількісних та якісних показників їх діяльності. У 2020 -2022 р. порівняно з попереднім періодом кількісні та якісні показники діяльності залізничної компанії демонструють негативну динаміку її

розвитку і погіршення ефективності функціонування, що пов'язано із ковідними обмеженнями та військовою агресією проти нашої держави.

2.3 Аналіз ефективності використання трудових ресурсів та рівня оплати праці АТ «Укрзалізниця»

Трудові ресурси – специфічний і найважливіший із усіх видів економічних ресурсів. Як фактор економічного розвитку людські ресурси – це працівники, що мають визначені професійні навички і знання і можуть використовувати їх у трудовому процесі [17].

Специфіка трудових ресурсів у порівнянні з іншими факторами економічного розвитку полягає в тому, що:

- люди не тільки створюють, але і споживають матеріальні і духовні цінності;
- багатогранність людського життя не вичерпується лише трудовою діяльністю, а, отже, щоб ефективно використовувати людську працю, необхідно завжди враховувати потреби людини як особистості;
- науково-технічний прогрес і гуманізація громадського життя стрімко збільшують економічну роль знань, моральності, інтелектуального потенціалу й інших особистих якостей працівників, що формуються роками і поколіннями, розкриваються людиною лише в сприятливих умовах.

Під персоналом організації розуміють всіх співробітників організації, це і керівники, і фахівці, і службовці, і працівники, і молодший обслуговуючий персонал.

Персонал організації складається з персоналу управління цією організацією і її підрозділів, службовців і інженернотехнічного персоналу, що не відносяться до персоналу управління, основних і допоміжних робітників, молодшого обслуговуючого персоналу і працівників охорони.

Працівників апарату управління організацією або її підрозділами називають

менеджерами. Менеджери повністю або переважно зайняті управлінською працею. Вони виконують принаймні одну із загальних або специфічних функцій управління. Найпоширенішою класифікаційною ознакою управлінських кадрів є ступінь відношення до управлінського рішення. За цією ознакою управлінські працівники підрозділяються на три групи: керівники, фахівці і технічні виконавці. Керівники ухвалюють рішення, фахівці готують спеціальну інформацію для їх ухвалення, технічний персонал апарату управління доводить рішення до виконавця. Керівники підрозділяються на лінійний і функціональний персонал.

Лінійні керівники здійснюють управління виробничими підрозділами (ділянками, цехами) підприємств, товариств, фірм. Функціональні – керівники функціональних служб (відділів, бюро тощо) і їх заступники. Лінійний або функціональний характер керівництва визначається перш за все посадовими зв'язками, а не родом діяльності. Так, наприклад, керівник дослідницької лабораторії науково-дослідного інституту буде лінійним керівником, а керівник дослідницької лабораторії промислового підприємства – функціональним. Лінійні підрозділи знаходяться в оперативному взаємозв'язку з організацією в цілому; функціональні керівники забезпечують реалізацію однієї з функцій управління, наприклад, начальник виробничо-диспетчерського відділу, головний конструктор тощо.

Фахівці апарату управління (економісти, інженери, диспетчери, юристи, програмісти тощо) покликані виконувати конкретні функції управління для сприяння в ухваленні управлінських рішень, а також забезпечувати діяльність лінійних і функціональних підрозділів (фінансові, бухгалтерські, технологічні, планово-економічні і т. д.) [17].

Технічний, або допоміжний, персонал (секретарі, кур'єри, діловоди тощо) здійснюють обслуговування процесу управління і забезпечують передачу управлінської інформації, її збір, первинну обробку, зберігання. У групі керівників виділяють рівні, категорії, ступені. Керівники первинних ступенів управління, або керівники первинної категорії, – це майстри, бригадири, завідувачі секторами, начальники бюро, відділів тощо.

Первинні управлінські колективи існують в апараті управління підприємством, апараті територіальних органів, міністерств, концернів і холдингових компаній. Керівники первинної категорії підрозділяються на виробничих керівників; керівників первинних підрозділів апарату управління підприємством; первинних керівників територіального міністерського і відомчого рівнів. Керівники середньої категорії керують групою первинних колективів, наприклад на підприємстві – це цех, служба, відділ, філіал, управління.

Керівники вищої категорії – це керівники самостійних організацій, які мають свої апарати управління. Структуризація складу менеджерів має свої особливості в кожній організації і визначається штатним розкладом [17].

Діяльність залізничного транспорту України в сучасних ринкових умовах потребує нових підходів до управління трудовими ресурсами та оцінки ефективності їх використання.

Розпочати аналіз слід із розгляду контингенту працівників підприємств залізничного транспорту (таблиця 2.3).

Таблиця 2.3 — Дані чисельності працівників АТ «Укрзалізниця»

Показник	Значення за роками					
	2016	2017	2018	2019	2020	2021
Середньооблікова кількість співробітників, тис. осіб	280,7	276,1	272,4	255,0	247,9	236,5

Так, за період 2016-2021 рр. відбулися такі зміни: у 2016 р. середньооблікова чисельність працівників склала 280,7 тис. осіб, у 2017 р. середньооблікова чисельність працівників склала 276,1 тис. осіб, що на 1,6 % менше порівняно з попереднім роком, у 2018 р. – на 1,3 % менше (272,4 тис. осіб), у 2019 р. – на 6,5 % менше (255,0 тис. осіб), у 2020 р. – на 2,8 % менше (247,9 тис. осіб), у 2021 р. – на 4,6 % (236,5 тис. осіб). При цьому зберігається гострий дефіцит працівників таких робітничих професій як машиністи, помічники машиністів, диспетчери, складачі поїздів, чергові по станції, оглядачі вагонів,

слюсарі з ремонту рухомого складу тощо.

Важливим етапом аналізу ефективності використання трудових ресурсів є і вивчення динаміки оплати праці. Зокрема на підприємствах залізничного транспорту заробітна плата складається з основної та додаткової заробітної плати, інших заохочувальних і компенсаційних виплат. Фонд основної заробітної плати формується за рахунок обсягу виконаних робіт (відпрацьованих годин), тарифних ставок та окладів. До складових додаткової заробітної плати відносяться доплати за роботу у вечірній та нічний час, у святкові та вихідні дні, за роботу з шкідливими умовами праці, надбавки за вислугу років, премії, оплата інших додаткових відпусток тощо. Інші заохочувальні і компенсаційні виплати включають загалом винагороду за підсумками роботи за рік, матеріальну допомогу на оздоровлення та інші види виплат. Аналіз фонду оплати праці в розрізі основної та додаткової заробітної плати та інших виплат представлено у таблиці 2.4.

Таблиця 2.4 – Аналіз фонду оплати праці працівників АТ «Укрзалізниця»

Показник	2016	2017	2018	2019	2020
Фонд оплати праці, млрд. грн, у т. ч.:	19,3	26,05	33,31	37,11	34,51
- фонд основної заробітної плати, млрд. грн	9,46	12,76	15,99	17,07	16,22
- фонд додаткової заробітної плати, млрд. грн	8,49	11,46	14,99	17,07	16,57
- інші заохочувальні і компенсаційні виплати, млрд. грн	1,35	1,83	2,33	2,97	1,72

Зокрема у 2017 р. фонд оплати праці склав 26,05 млрд. грн. У 2018 р. – збільшився на 21,8 % за рахунок зростання фонду основної заробітної плати на 20,2 %, фонду додаткової заробітної плати – на 23,5 % за рахунок зростання

доплат і надбавок за роботу із важкими та шкідливими умовами праці, за роботу у вечірній та нічний час, за суміщення професій, за виконання обов'язків тимчасово відсутнього працівника, розширення зон обслуговування, професійну майстерність тощо, інших заохочувальних і компенсаційних виплат – на 21,5 % за рахунок збільшення винагороди за підсумками року. У 2019 р. фонд оплати праці збільшився на 10,2 % порівняно з попереднім роком за рахунок зростання фонду основної заробітної плати збільшився на 6,3 % у зв'язку з підвищенням тарифних ставок та посадових окладів, фонду додаткової заробітної плати – на 12,2 % за рахунок зростання доплат за вислугу років, за роботу з важкими та шкідливими умовами праці, за роботу у вечірній та нічний час тощо, інших заохочувальних і компенсаційних витрат – на 21,5 % за рахунок збільшення виплат винагород за підсумками року. У 2020 р. фонд оплати праці знизився на 7 % порівняно з попереднім роком, що викликано введенням в дію Антикризового плану заходів АТ «Укрзалізниця» внаслідок погіршення його фінансового стану, яке було спричинено пандемією COVID-19 та карантинними обмеженнями, що запроваджені на всій території України, що наглядно видно на рисунку 2.3.



Рисунок 2.3 – Показники фонду оплати праці АТ «Укрзалізниця» за 2016-2020 рр.

Важливим показником аналізу ефективності використання трудових ресурсів є продуктивність праці. Оцінка продуктивності праці та її вимірювання на підприємствах залізничного транспорту базується як на загальних підходах (уже розкритих у наукових працях), так і на власних, характерних саме для певного виду діяльності залізничного транспорту.

Аналіз продуктивності праці працівників підприємства залізничного транспорту наведено в таблиці 2.5.

Таблиця 2.5 – Аналіз продуктивності праці працівників підприємства

Показник	Значення за роками					
	2016	2017	2018	2019	2020	2021
Обсяг перевезень у приведених т-км, млн.	263418,6	260103,8	257211,2	255626,8	232083,6	244128,4
Середньооблікова кількість працівників на експлуатаційній роботі, тис. осіб	216,7	191,3	168,5	162,6	156,2	144,8
Продуктивність праці, тис. т-км/ос.	1216	1360,0	1527,0	1573,0	1486,0	1686,0

Протягом аналізованого періоду 2016-2021 рр. продуктивність праці зазнала таких змін: у 2016 р. склала 1216 тис. т-км/ос.; у 2017 р. склала 1360 тис. т-км/ос., що на 11,18% більше порівняно з 2016 роком; у 2018 р. – 1527 тис. т-км/ос., що на 10,9 % більше, порівняно з 2017 р.; у 2019 р. – 1573 тис. т-км/ос., що на 2,9 % більше, порівняно з попереднім роком; у 2020 р. – 1486 т-км/ос., що на 5,5 % менше, порівняно з попереднім 2019 р., у 2021 р. – 1686,0 тис. т-км/ос., що на 13,6 % більше, порівняно з попереднім роком. Однак, незважаючи на зростання показника продуктивності праці за останні роки, слід вказати, що відбулося це в основному не за рахунок зростання обсягу робіт, виконаних одним працівником, а пов'язано із скороченням персоналу основної діяльності.

2.4 Аналіз стану та ефективності використання основних фондів підприємства

Діяльність підприємства, особливо такої інфраструктурної галузі, як залізничний транспорт, нерозривно пов'язана з наявністю та використанням основних засобів, які повинні характеризуватися відповідним складом та структурою для здійснення процесу виробництва [26].

Для забезпечення конкурентоспроможності підприємства та отримання необхідної величини прибутку необхідно здійснювати постійний аналіз ефективності використання основних засобів та досліджувати фактори, які впливають на цю зміну.

Показники стану й ефективності використання основних засобів можна об'єднати в три групи, які характеризують:

- забезпечення підприємства основними засобами;
- стан основних засобів;
- ефективність використання основних засобів.

До показників, які характеризують забезпеченість підприємства основними засобами, належать: фондомісткість, фондоозброєність, коефіцієнт реальної вартості основних виробничих засобів у майні підприємства.

Фондомісткість є величиною зворотною до фондовіддачі. Цей показник дає можливість визначити вартість основних засобів на одну гривню виробленої продукції і характеризує забезпеченість підприємства основними засобами. За нормальних умов фондовіддача повинна мати тенденцію до збільшення, а фондомісткість – до зменшення.

Забезпеченість підприємства основними виробничими засобами визначається рівнем фондоозброєності праці. Останню розраховують як відношення вартості основних виробничих засобів до чисельності працівників підприємства. Збільшення рівня фондоозброєності є позитивним фактором. Коефіцієнт реальної вартості основних виробничих засобів у майні підприємства

визначається як відношення вартості основних виробничих засобів (за вирахуванням суми їхнього зносу) до вартості майна підприємства.

Якщо коефіцієнт реальної вартості основних виробничих засобів у майні підприємства сягає критичної позначки (0,2 - 0,3), то реальний виробничий потенціал підприємства буде низьким і треба терміново шукати кошти для виправлення становища [27].

Стан основних виробничих засобів характеризують через такі коефіцієнти: зносу основних засобів; придатності; оновлення; вибуття (приросту) основних засобів.

В таблиці 2.6 наведено показники стану вартості та ступеня зносу основних фондів підприємств залізничного транспорту.

Таблиця 2.6 – Аналіз вартості та ступеня зносу основних фондів

Показник	Значення за роками				
	2017	2018	2019	2020	2021
Первісна вартість основних фондів, млрд. грн	447,6	462,9	469,6	478,9	482,4
Знос основних фондів, млрд. грн	264,8	278,1	287,2	301,6	308,2
Залишкова вартість основних фондів, млрд. грн	182,8	184,8	182,4	177,3	174,2
Ступінь зносу основних фондів, %	59,1	60,1	61,1	62,9	63,9

З дані таблиці 2.6 видно, що зношеність основних фондів коливається в межах 59,1-63,9 %. При цьому найвище значення показника зафіксовано у 2021 р. на рівні 63,9 % (рисунок 2.4).



Рисунок 2.4 –Показники рівня зносу основних фондів АТ «Укрзалізниця»
за 2017-2021 рр.

До показників, які характеризують ефективність використання основних засобів, належать: фондівіддача, рентабельність основних засобів, сума прибутку на одну гривню основних засобів. Найбільш загальним показником, який характеризує ефективність використання основних засобів, є фондівіддача. У таблиці 2.7 наведено значення фондівіддачі, фондомісткості та фондоозброєності працівників АТ «Укрзалізниця» (таблиця 2.7).

Таблиця 2.7 – Аналіз показників ефективності використання основних фондів підприємств залізничного транспорту

Показник	Значення за роками				
	2017	2018	2019	2020	2021
Фондовіддача, грн/грн	0,31	0,35	0,39	0,33	0,29
Фондомісткість, грн/грн	3,19	2,85	2,60	3,06	2,97
Фондоозброєність, тис. грн / ос.	1075,96	1236,12	1273,37	1321,62	1284,68

За даними таблиці 2.7 можна зробити наступний висновок щодо динаміки показників ефективності використання основних фондів. Так, загалом за 2017-2021 рр. фондівддача знизилася на 6,5 % з 0,31 грн/грн у 2017 р. до 0,29 грн/грн у 2021 р., фондомісткість – на 6,9 % з 3,19 грн/грн у 2017 р. до 2,97 грн/грн у 2021 р. У свою чергу, фондоозброєність зросла на 19,4 % з 1075,96 тис. грн/ос. у 2017 р. до 1284,68 тис. грн/ос. у 2021 р.

2.5 Аналіз операційних витрат підприємства залізничного транспорту

Витрати на залізниці згідно з П(С)БО поділяють на операційні, інвестиційні та фінансові. Методика формування операційних витрат за принципами бухгалтерського обліку є єдиною для всіх структурних підприємств та залізниці. Але правила обліку окремих господарських операцій є специфічними для різних структурних підприємств [33].

Номенклатурою витрат передбачено формування витрат основної (операційної) діяльності залізничного транспорту за такими видами економічної діяльності:

- пасажирські перевезення у внутрішньому (крім приміського) та міжнародному сполученнях;
- пасажирські перевезення у приміському сполученні;
- вантажні перевезення;
- утримання та експлуатація об'єктів інфраструктури;
- надання послуг локомотивної тяги (у пасажирському та вантажному русі);
- ремонт рухомого складу.

Ці види економічної діяльності покладені в основу організації бухгалтерського обліку та формування галузевої звітності. Кожний вид економічної діяльності на залізничному транспорті України має свої особливості, пов'язані зі структурою управління, особливостями фінансування, формуванням

доходів, ціноутворенням, які впливають на організацію управління виробничо-економічною діяльністю обліку та планування.

Ведення обліку витрат здійснюється на підставі первинних документів на рівні структурних підрозділів залізниць – дистанції колії, автоматики, телемеханіки та зв'язку, електропостачання, депо локомотивних, вагонних, станцій тощо, підприємств, що входять до сфери управління Укрзалізниці, та їх структурних підрозділів. При цьому, структурним підрозділом будь якого господарства залізниці (підприємства Укрзалізниці) використовуються ті статті витрат, визначені у Номенклатурі витрат, які відповідають характеру робіт, що ним виконуються. Таким чином, на рівні структурних підрозділів залізниць (підприємств) забезпечується формування витрат за видами економічної діяльності.

Формування витрат за видами перевезень здійснюється на рівні залізниць та підприємств. Система управління витратами має бути узгоджена зі стратегічними цілями підприємства (структурного підрозділу), що визначаються системою стратегічного менеджменту залізничного транспорту [28].

Стратегічною метою управління витратами на залізничному транспорті є формування оптимального рівня фінансово-економічних показників поточного і довгострокового періодів, які забезпечують необхідний прибуток для виконання перевезень і підсобно допоміжної діяльності підприємств

Аналіз операційних витрат АТ «Укрзалізниця» наведено в таблицях 2.8-2.9.

Таблиця 2.8 – Аналіз операційних витрат АТ «Укрзалізниця» за 2016-2018 рр.

Показник	Значення за роками						
	2016	2017			2018		
	звіт, тис. грн	звіт, тис. грн	абс., тис. грн	відн., %	звіт, тис. грн	абс., тис. грн	відн., %
1	2	3	4	5	6	7	8
Витрати на оплату праці	25665850	31973995	6308145	124,6	40585068	8611073	126,9
Амортизація	17910127	14662305	-3247822	81,9	12547478	-2114827	85,6

Продовження таблиці 2.8

1	2	3	4	5	6	7	8
Електроенергія	7813910	7865933	52023	100,7	9155746	1289813	116,4
Пальне	5877363	7307862	1430499	124,3	9405550	2097688	128,7
Матеріали, ремонт та обслуговування	5316235	5809691	493456	109,3	7030203	1220512	121
Витрати на соціальне забезпечення	283186	470130	186944	166	677887	207757	144,2
Інші операційні витрати	1008650	1061392	52742	105,2	270818	-790574	25,5
Усього	64728154	68603550	3875396	106	79900779	11297229	116,5

Аналіз даних таблиць 2.8-2.9 свідчить, що у 2016 році операційні витрати склали 64728154 тис. грн; у 2017 р. - 68603,55 тис. грн. У 2018 р. операційні витрати склали 79900,71 тис. грн, що на 11297,23 тис. грн або на 16,5 % більше, порівняно з попереднім роком, зокрема витрати на оплату праці зросли на 27,3 %, відрахування на соціальні заходи – на 25,4 %, амортизація зменшилася на 14,4 %, витрати на електроенергію збільшилися на 16,4 %, витрати на пальне зросли на 28,7 %, витрати на матеріали, ремонт та обслуговування збільшилися на 21 %, інші операційні витрати зросли на 3,3 %.

У 2019 р. операційні витрати склали 85532,77 тис. грн, що на 5632,06 тис. грн або на 7,0 % більше, порівняно з попереднім роком, зокрема витрати на оплату праці зросли на 8,7 %, відрахування на соціальні заходи – на 7,7 %, амортизація зменшилася на 1,2 %, витрати на електроенергію зменшилися на 7,3 %, витрати на пальне зменшилися на 12,4 %, витрати на матеріали, ремонт та обслуговування зменшилися на 21,3 %, при цьому значно зросли інші операційні витрати (майже у 6 разів).

У 2020 р. операційні витрати склали 78050,56 тис. грн, що на 7482,21 тис. грн або на 8,7 % менше, порівняно з попереднім роком, зокрема витрати на оплату праці знизилися на 6,9 %, відрахування на соціальні заходи – на 5,6 %, амортизація зросла на 3,1 %, витрати на електроенергію знизилися на 10,5 %, витрати на пальне – на 33,8 %, витрати на матеріали, ремонт та обслуговування – на 21,6 %, інші операційні витрати знизилися на 0,9 %.

Таблиця 2.9 – Аналіз операційних витрат АТ «Укрзалізниця» за 2019-2021 рр.

Показник	Значення за роками								
	2019			2020			2021		
	звіт, тис. грн	абс., тис. грн	відн., %	звіт, тис. грн	абс., тис. грн	відн., %	звіт, тис. грн	абс., тис. грн	відн., %
Витрати на оплату праці	44056208	3471140	108,6	41116369	-2939839	93,3	36272,67	2535,19	107,5
Амортизація	12402695	-144783	98,8	12786783	384088	103,1	12216,55	-570,23	95,5
Електроенергія	8484771	-670975	92,7	7596828	-887943	89,5	8152,85	556,02	107,3
Пальне	8237492	-1168058	87,6	5455890	-2781602	66,2	7042,30	1586,41	129,1
Матеріали, ремонт та обслуговування	5530092	-1500111	78,7	4335809	-1194283	78,4	4686,46	350,65	108,1
Витрати на соціальне забезпечення	543395	-134492	80,2	381991	-161404	70,3	7996,26	617,37	108,4
Інші операційні витрати	3045621	2774803	1124,6	2758037	-287584	90,6	5452,36	-1306,52	80,67
Усього	85532726	5631947	107	78050557	-7482169	91,3	81819,45	3768,89	104,8

У 2021 р. операційні витрати склали 81819,45 тис. грн, що на 3768,89 тис. грн або на 4,8 % більше, порівняно з попереднім роком, зокрема витрати на оплату праці зросли на 7,5 %, відрахування на соціальні заходи – на 8,4 %, амортизація знизилася на 4,5 %, витрати на електроенергію зросли на 7,3 %, витрати на паливе – на 29,1 %, витрати на матеріали, ремонт та обслуговування – на 8,1 %, інші операційні витрати знизилася на 19,33 %.

2.6 Аналіз фінансових результатів і фінансового стану АТ «Укрзалізниця»

Провідна роль фінансових результатів полягає у тому, що вони забезпечують зміцнення бюджету держави, сприяють інвестиційній привабливості, діловій активності підприємств у виробничій та фінансовій сферах. Кожне підприємство, яке здійснює фінансово-господарську діяльність, повинне самостійно фінансувати всі напрями своїх витрат відповідно до виробничих планів, розпоряджатися наявними фінансовими ресурсами, вкладаючи їх у виробництво продукції з метою одержання кінцевого результату – прибутку [29].

Ефективність фінансової діяльності виявляється у досягнутих фінансових результатах. Для визначення фінансового результату діяльності підприємства за звітний період необхідно порівняти доходи звітного періоду і витрати, понесені для одержання цих доходів.

Доходи підприємства – це збільшення економічних вигод у вигляді надходжень активів або зменшення зобов'язань, які призводять до зростання власного капіталу (крім зростання капіталу за рахунок внесків власників) [33].

Основними завданнями аналізу фінансових результатів діяльності є:

- вивчення можливостей одержання прибутку відповідно до наявного ресурсного потенціалу підприємства і кон'юнктури ринку;
- систематичний контроль за процесом формування прибутку і зміною його

динаміки; - визначення впливу як зовнішніх, так і внутрішніх факторів на фінансові результати й оцінювання якості прибутку;

- виявлення резервів збільшення суми прибутку і підвищення рівня прибутковості бізнесу;

- оцінювання роботи підприємства з використання можливостей збільшення прибутку і рентабельності;

В таблицях 2.10 та 2.11 наведено аналіз фінансових результатів АТ «Укрзалізниця» за 2016-2021 рр.

Таблиця 2.10 – Аналіз фінансових результатів діяльності підприємства за 2016-2018 рр.

Показник	Значення за роками						
	2016	2017			2018		
	звіт	звіт	абс., грн	відн., %	звіт	абс., грн	відн., %
Чистий дохід від реалізації продукції (товарів, робіт, послуг) грн	66570164	73938151	7367987	111,1	83402407	9464256	112,8
Собівартість реалізованої продукції, грн	63696856	67346681	3649825	105,7	77104073	9757392	114,5
Валовий прибуток від реалізації продукції, грн	2873308	6591470	3718162	229,4	6298334	-293136	95,6
Витрати на 1 грн реалізованої продукції, грн	0,96	0,91	-0,05	94,8	0,92	0,01	101,1

Таблиця 2.11 - Аналіз фінансових результатів діяльності підприємства за 2019-2021 рр.

Показник	Значення за роками								
	2019			2020			2021		
	звіт	абс., грн	відн., %	звіт	абс., грн	відн., %	звіт	абс., грн	відн., %
Чистий дохід від реалізації продукції (товарів, робіт, послуг), тис. грн	90352319	6949912	108,3	75291560	-15060759	83,3	84120,12	8828,56	111,73
Собівартість реалізованої продукції, тис. грн	80774665	3670592	104,8	73902120	-6872545	91,5	79769,16	5867,04	107,94
Валовий прибуток від реалізації продукції, тис. грн	9577654	3279320	152,1	1389440	-8188214	14,5	4350,96	2961,52	313,14
Витрати на 1 грн реалізованої продукції, грн	0,89	-0,03	96,7	0,98	0,09	110,1	457,0	12356,69	-

Аналізуючи дані таблиць 2.10-2.11 відзначимо, що чистий дохід у 2016 році склав 66570,164 млн. грн, у 2017 р. склав 73938,15 млн. грн, що на 10% менше за дані 2016 року, у 2018 р. – 83402,41 млн. грн, що на 9464,26 млн. грн або 12,8 % більше, порівняно з попереднім роком, у 2019 р. – 90352,32 млн. грн, що на 6949,91 млн. грн або на 8,33 % більше, порівняно з попереднім роком, у 2020 р. – 75291,56 млн. грн, що на 15060,76 млн. грн або на 16,7 % менше, порівняно з попереднім 2019 р., у 2021 р. – 84120,12 млн. грн, що на 8828,56 млн. грн або 11,73 % більше, порівняно з попереднім роком.

Щодо собівартості реалізованої продукції, то її значення у 2016 р. 63696,9 млн. грн, у 2017 р. – 67346,68 млн. грн, у 2018 р. – 77104,07 тис. грн, що на 9757,39 млн. грн або на 14,49 % більше, порівняно з попереднім роком, у 2019 р. – 80774,67 млн. грн, що на 3670,60 тис. грн або на 4,76 % більше, порівняно з попереднім роком, у 2020 р. – 73902,12 млн. грн, що на 6872,55 млн. грн або на 8,51 % менше, порівняно з попереднім 2019 р., у 2021 р. – 79769,16 млн. грн, що на 5867,04 млн. грн або на 7,94 % більше, порівняно з попереднім роком

Валовий прибуток у 2016 р. - 2873,308 млн. грн, у 2017 р. – 6591,47 млн. грн, що на у 2018 р. – 6298,33 млн. грн, що на 293,14 млн. грн або на 4,45 % менше, порівняно з попереднім роком, у 2019 р. – 9577,65 млн. грн, що на 3279,32 млн. грн або на 52,07 % більше, порівняно з попереднім роком, у 2020 р. – 1389,44 млн. грн, що на 8188,21 млн. грн або на 85,49 % менше, порівняно з попереднім 2019 р., у 2021 р. – 4350,96 млн. грн, що на 2961,52 млн. грн або у три рази більше, порівняно з попереднім роком.

Фінансовим результатом діяльності аналізованого підприємства у 2017 р. став прибуток у розмірі 114,55 млн. грн, у 2018 р. – 203,85 млн. грн, що на 89,30 млн. грн або на 77,96 % більше порівняно з попереднім роком. Фінансовим результатом діяльності аналізованого підприємства у 2019 р. став збиток у розмірі 2988,25 млн. грн, що на 3192,10 млн. грн менше порівняно з попереднім роком, у 2020 р. – 11899,69 млн. грн, що на 8911,44 млн. грн або на у чотири рази менше порівняно з попереднім 2019 р. Фінансовим результатом діяльності підприємства у 2021 р. став прибуток у розмірі 457,0 млн. грн, що на 12356,99

млн. грн більше, порівняно з попереднім роком.

На рисунку 2.5 наведено динаміку зміни фінансових показників АТ «Укрзалізниця» за 2016-2021 рр.

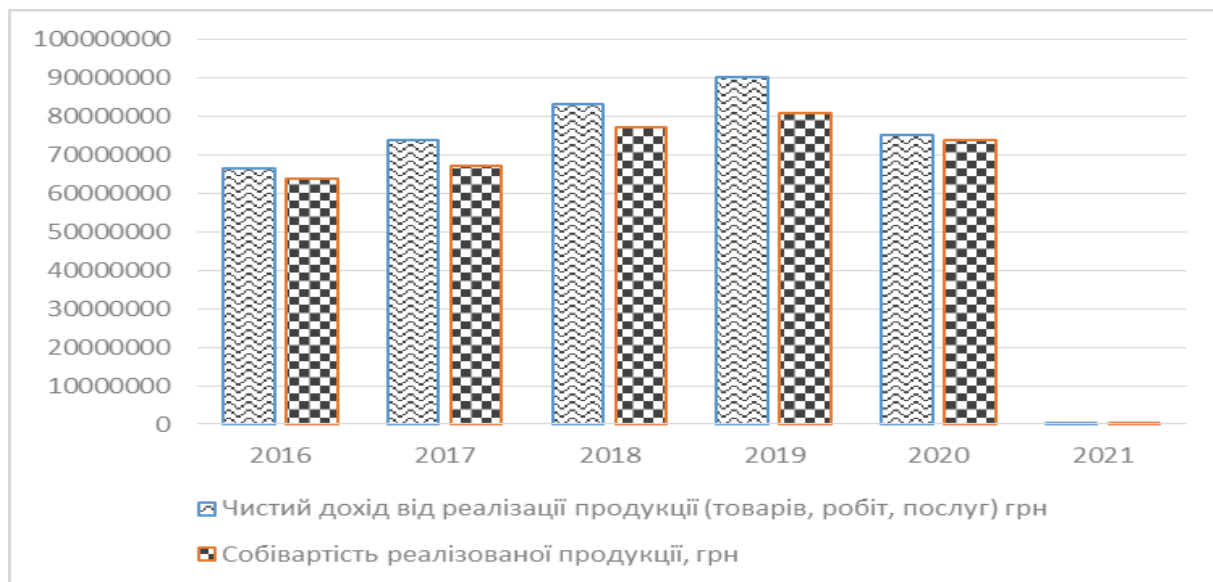


Рисунок 2. 5 – Показники фінансового стану АТ «Укрзалізниця» за 2016-2021 рр.

Завершальним етапом аналізу фінансових результатів та прибутковості підприємства є підрахунок резервів можливого підвищення прибутків підприємства. Резерви збільшення суми прибутку визначають за кожним видом товарної продукції. Основними їхніми джерелами є збільшення обсягу реалізації продукції, зниження її собівартості, підвищення якості товарної продукції, реалізація її на вигідніших ринках збуту і т. д.

Висновки до розділу 2

На сьогодні підприємства залізничного транспорту переживають вкрай складні часи, викликані як накопиченням системних проблем у галузі і непослідовністю та фрагментарністю реалізованих реформаційних заходів, так і

впливом деструктивних факторів зовнішнього середовища функціонування підприємств галузі

В розділі проведено аналіз господарської діяльності АТ «Укрзалізниця», з якого зроблено наступні висновки.

Аналізуючи стан основних фондів встановлено, що їх зношеність коливається в межах 59,1-63,9 %. При цьому найвище значення показника зафіксовано у 2021 р. на рівні 63,9 %. Динаміка показників ефективності використання основних фондів вказує, що фондоддача знизилася на 6,5 %, фондомісткість – на 6,9 %, фондоозброєність зросла на 19,4 %.

Аналіз кадрової політики та ефективності використання трудових ресурсів підприємства дозволив дійти наступних висновків. У 2017 р. середньооблікова чисельність працівників склала 276,1 тис. осіб, у 2018 р. – на 1,3 % менше, у 2019 р. – на 6,5 %, у 2020 р. – на 2,8 %, у 2021 р. – на 4,6 %. Фонд оплати праці у 2017 р. склав 26,05 млрд. грн, у 2018 р. – збільшився на 21,8 % порівняно з попереднім роком, у 2019 р. – на 10,2 %, у 2020 р. – знизився на 7,0 %. Щодо динаміки середньомісячної заробітної плати за 2017-2021 рр., то варто сказати, що станом на кінець грудня 2017 р. середня заробітна плата складала 9392,2 грн, а на кінець грудня 2021 р. – 16515,0 грн. Зростала і продуктивність праці: у 2017 р. склала 1360 тис. т-км/ос.; у 2018 р. – зросла на 10,9 %, у 2019 р. – на 2,9 %, у 2020 р. – зменшилася на 5,5 %, у 2021 р. – зросла на 13,6 %. Однак, незважаючи на зростання показника, слід вказати, що відбулося це в основному не за рахунок зростання обсягу робіт, виконаних одним працівником, а пов'язано із скороченням персоналу основної діяльності.

Аналіз структури витрат підприємства за 2021 р. показав, що найбільшу питому вагу займають витрати на оплату праці (44,33 %), амортизація (14,93 %), витрати на електроенергію (9,96 %), відрахування на соціальні заходи (9,77 %). Питома вага витрат на пальне – 8,61 %, інших витрат – 6,66 %, витрат на матеріали, ремонт та обслуговування – 5,73 %.

Фінансовим результатом діяльності підприємства у 2021 р. став прибуток у розмірі 457,0 млн. грн, що на 12356,99 млн. грн більше, порівняно з попереднім

роком.

Безсумнівно, поглиблення кризового стану підприємств залізничного транспорту і зниження їхньої спроможності задовольняти потреби національної економіки та населення в перевезеннях пов'язано з багаторічним ігноруванням потреби в залученні значних обсягів інвестицій у технічне і технологічне переоснащення основних засобів залізничного транспорту. Відтак загалом за останні десять років обсяг капітальних інвестицій склав 105,6 млрд грн, у т. ч. найвищий рівень інвестиційних вкладень зафіксовано у 2018 р. – 16912,8 млн грн, 147 у свою чергу найнижчий – у 2014 р. 3508,2 млн грн. У 2020 р. вдалося освоїти капітальних інвестицій на суму 8442,3 млн грн, у 2021 р. (за попередніми оцінками) – близько 14 млрд грн.

Складний фінансовий стан АТ «Укрзалізниця» у значній мірі скорочує його інвестиційні можливості. Протягом останніх років виконання інвестиційних планів не перевищувало 70 %, у середньому досягавши лише рівня 50 – 60 % (у 2020 р. виконання плану склало 66,8 %). Як результат стан залізничного транспорту на сьогодні залишається вкрай складним і внаслідок невиконання необхідних обсягів оновлення основних фондів з кожним роком лише погіршується. Про це свідчить зростання обсягів технічно непридатної інфраструктури, збільшення парку зношених вагонів, погіршення виробничо-технічної бази і, як результат, якості обслуговування споживачів послуг залізничного транспорту. У свою чергу, вплив зовнішніх загроз, зокрема пандемії коронакризи, загальної економічної нестабільності в країні та війни, яка ще й призводить до фізичного знищення залізничної інфраструктури, що лише ускладнює становище залізничної компанії.

3 Методологія та технологія антикризового управління на залізничному транспорті

3.1 Роль та місце залізничного транспорту в умовах забезпечення економічної безпеки

Забезпечення економічної безпеки входить до складу найважливіших функцій не тільки держави в цілому, а й галузей економіки та окремих підприємств та установ. Проблема економічної безпеки є похідною від завдань економічного розвитку держави, різних галузей та компаній (організацій та установ). Конкретний зміст поставленої проблеми може змінюватись в залежності від сформованих у кожен тимчасовий період зовнішніх та внутрішніх умов розвитку названих суб'єктів господарювання.

Під економічною безпекою транспортної компанії розуміється система умов і заходів функціонування, що проводяться господарюючим суб'єктом, за яких гранично мала ймовірність його банкрутства; знижено можливість явного зловживання всіма видами ресурсів – виробничих, трудових, матеріальних, фінансових та інформаційних; висока збалансованість усіх його інтересів та забезпечене постійне, хоча б невелике, зростання економічних та фінансових показників, що характеризують операційну та інші види діяльності [16].

Економічна безпека включає такі обов'язкові компоненти, як:

- правові, економічні та фінансові норми, що охороняють інтереси кожного суб'єкта господарювання;
- самостійність його розвитку;
- його місце у галузевому та міжгалузевому поділі праці та фінансово-банківській сфері;
- збереження та функціонування окремо взятого суб'єкта ринку для реалізації поставлених ним власних цілей тактичного та перспективного розвитку.

Необхідність підтримки балансу інтересів розвитку господарюючого суб'єкта робить особливо значущим завдання самозбереження за наявності впливу на нього великої кількості зовнішніх та внутрішніх факторів загроз. Тому потрібний особливий механізм захисту від саморуйнування економічного потенціалу компанії (організації чи установи), збалансованого із загальним потенціалом галузі, куди входить корпорація, або фінансово-банківської сфери, до якої може належати господарюючий суб'єкт.

Структурно систему економічної безпеки на підприємствах залізничного транспорту з позицій концепцій логістики можна подати у вигляді системи взаємозв'язків (рисунк 3.1).

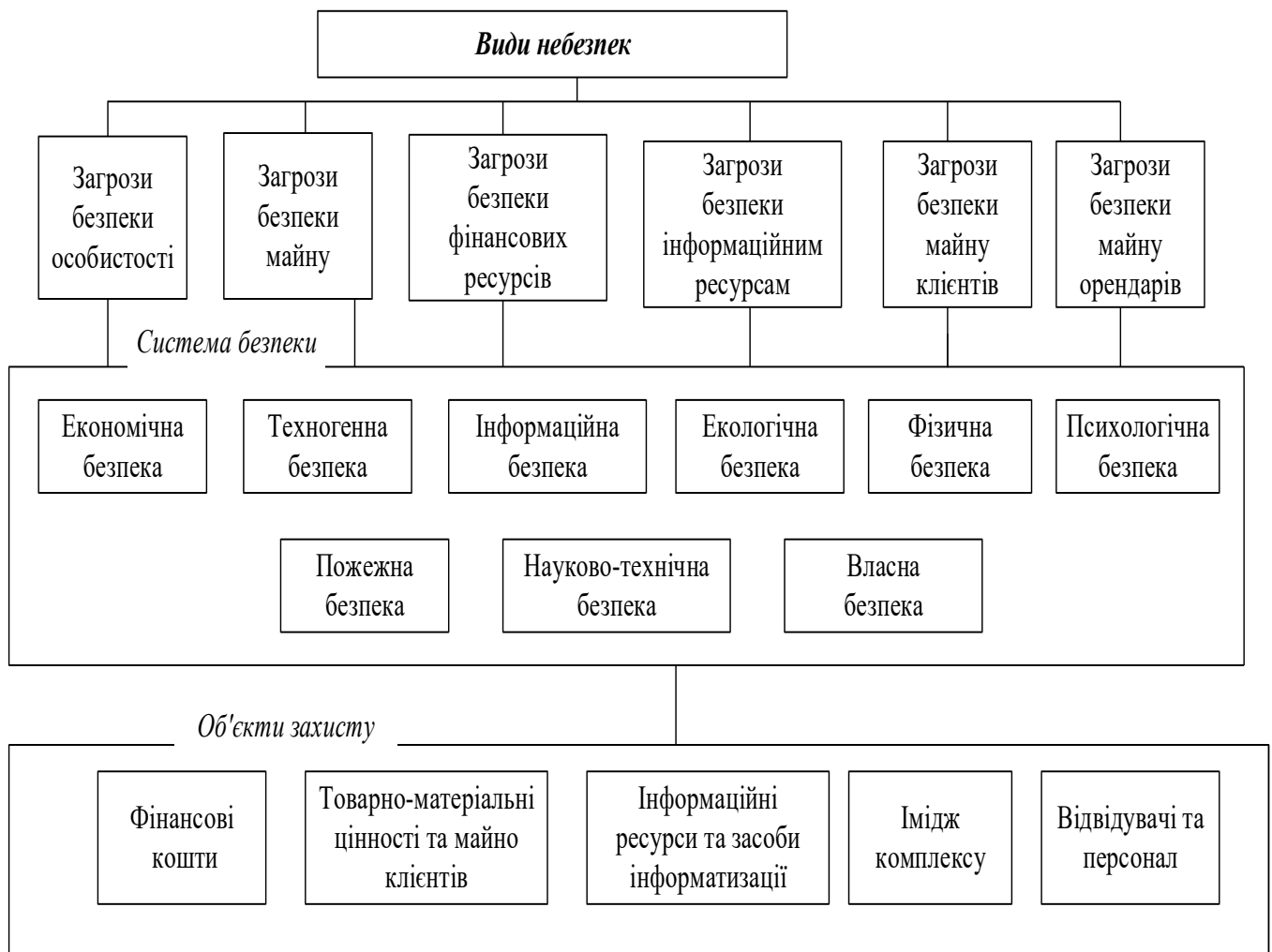


Рисунок 3.1 - Структура економічної безпеки на залізничному транспорт із позиції концепції економічної безпеки

Сам розвиток суб'єкта вже є одним з динамічних компонентів економічної безпеки. Якщо галузь чи навіть певна сфера спільних взаємин не розвивається, то у суб'єкта різко скорочуються можливості економічного виживання, його пристосовності до постійно діючих зовнішніх та внутрішніх факторів-загроз. Тому можна сказати, що безпека – це певний у часі стан господарюючого суб'єкта у загальній системі зв'язків з точки зору здатності до розвитку в умовах постійного та непередбачуваного впливу зовнішніх та внутрішніх факторів-загроз. Чим вища життєздатність суб'єкта, тим оцінка рівня його економічної безпеки вище. Порушення диспропорцій між різними зв'язками в системі, в якій функціонує суб'єкт, та вплив на нього факторів загроз ведуть до переходу від безпечного стану до небезпечного.

Сутність економічної безпеки будь-якої транспортної компанії виявляється у забезпеченні захисту виробничих інтересів і в досягненні достатнього економічного потенціалу навіть при певних несприятливих умовах розвитку та впливу зовнішніх та внутрішніх факторів-загроз. Економічна безпека є не тільки захищеність власних виробничих та економічних інтересів суб'єкта, а також його здатність створити механізм реалізації цих інтересів у майбутньому [16].

Сутність економічної безпеки суб'єкта реалізується у системі критеріїв та показників. Критеріальна оцінка включає оцінку ресурсного потенціалу господарюючого суб'єкта та можливостей його розвитку, рівня ефективності використання ресурсів, сумісності аналогічних суб'єктів у просторі та динаміці, стабільності застосування різних методів та моделей підвищення рівня безпеки. У системі показників економічної безпеки можна виділити економічний ризик та темпи його зниження (збільшення) за певний тимчасовий період, число несанкціонованих входів до інформаційної системи суб'єкта, платоспроможність, величину попиту на продукцію та послуги та ін.

Слід зазначити, що з економічної безпеки важливе значення має не так самі величини показників, а насамперед їх граничні значення, тобто

нормативні значення, недотримання яких перешкоджає нормальному розвитку господарюючого суб'єкта через початок процесу формування негативних тенденцій у його розвитку. Без використання поняття «економічна безпека», що передбачає структурну перебудову методів управління не можна бути впевненим, що господарюючі суб'єкти можуть бути готові до функціонування у жорсткому конкурентному середовищі, до необхідності підтримки ефективності виробництва в умовах постійного впливу економічних ризиків.

Вважаємо, що не можна під фактором впливу на економічну безпеку розглядати будь-який недолік, властивий нестабільному стану нашої економіки. Інакше проблема економічної безпеки «розчинилася» б у характеристиках економічного та соціального розвитку суб'єкта господарювання.

У загальному вигляді всі фактори, що впливають на економічну безпеку господарюючого суб'єкта, можуть бути поділені на зовнішні та внутрішні. До зовнішніх, або загальних факторів-загроз можна віднести ті, які діють у навколишньому суб'єкту господарювання оточенні [45].

Внутрішні фактори включають усі фактори-загрози, якими може керувати сам суб'єкт, тому що ступінь їх впливу на його економічну безпеку регулюється його керуючою підсистемою.

Виходячи з ситуації, яка склалася в економіці країни, всі фактори, що впливають, можна також підрозділити на позитивні та негативні. Позитивні чинники дозволяють підвищити чи стабілізувати нормальний рівень економічної безпеки. Негативні фактори, що впливають на неї, включають в основному різні економічні та інформаційні небезпеки.

З усієї множини зовнішніх ключових факторів-загроз варто виділити наступні:

- війна та пов'язані з нею постійні руйнації інфраструктури;
- блекаути пов'язані з відсутністю електричної енергії;
- зниження інвестиційної та інноваційної активності компаній та кредитних установ. Без великих капітальних вкладень відродити економіку

країни неможливо;

- витік валютних ресурсів суб'єктів господарювання за кордон;
- зростання зовнішнього та внутрішнього боргу країни;
- криміналізацію економічних відносин;
- важке фінансове становище більшості господарюючих суб'єктів країни

через військову агресію

- відставання законодавчої та правової бази від темпів структурної перебудови економіки;

- небажання іноземного капіталу через високі політичні та економічних ризиків брати участь у створенні конкурентоспроможних суб'єктів господарювання;

- кіберзагрози;
- високу інфляцію.

Кібербезпека на транспорті ґрунтується на впровадженні програм з кіберзахисту, цифровізації проєктів інформатизації, їх розвитку, оперативному реагуванні на інциденти пов'язані із спробами втручання в роботу інформаційних систем, електронних інформаційних ресурсів, комунікаційних та/або технологічних систем.

Проблема розробки механізму забезпечення економічної безпеки на транспорті, здатної підтримувати стійкість розвитку господарюючого суб'єкта, видається досить складною та багатогранною, оскільки:

- процес відбувається в умовах невизначеності;
- немає ще адаптованих до вітчизняної економіки відповідних методів і моделей, незважаючи на окремі спроби створити умови для виходу з кризи з збереженням виробничого потенціалу зростання;
- недостатньо високий рівень застосування сучасних комп'ютерних технологій, що базуються на ефективних і одночасно адаптованих до дійсності методів і моделях забезпечення економічної безпеки, що не дозволяє вирішити розглянуту проблему на належному рівні через низку об'єктивних причин, зокрема, наявності високих економічних ризиків;

- наявна недостатня інформаційна безпека господарюючих суб'єктів.

Незважаючи на значні труднощі, розробка напрямів забезпечення економічної безпеки є важливим завданням для будь-якого господарюючого суб'єкта, тож спроби подібної розробки повинні і будуть робитися, зокрема на залізничному транспорті.

3.2 Технологічний процес антикризового управління в транспортно-логістичній системі на залізничному транспорті

Антикризове управління має бути спрямоване на запобігання діяльності факторів, що загрожують самому існуванню компанії або, принаймні, сприяють серйозному обмеженню у виправленні ситуації у найближчому майбутньому як у транспортної компанії, так і в галузі та у всій економіці. У подібному стилі управління головним стає не досягнення максимального значення деякої очікуваної величини, а спроба знизити ймовірні можливості розвитку за дуже несприятливим сценарієм. Інакше кажучи, користуючись термінологією, прийнятою у фінансах, цільовими функціями тут виявляються не середня очікувана прибутковість, а мінімізація цінності під загрозою (value at risk) [68].

Для впровадження технологічних процесів антикризового управління у транспортній компанії необхідно особливу увагу приділити питанням розподілу можливих ризиків.

Оцінюючи ризиків логістичних систем поняття «ризик» досить багатогранне і залежить, перш за все, від сфери його застосування та на практики оцінки ризиків, які склалася у цій галузі.

Менеджмент на залізничному транспорті в нашій країні не відрізняється глибокими традиціями у сфері управління ризиками.

Під ризиком залізничного транспорту доцільно розуміти можливість та

(або) ймовірність виникнення несприятливої ситуації чи невдалого результату виробничо-господарської, фінансової чи іншої діяльності залізничної компанії. При цьому основною причиною ризику вважається не лише статистична ймовірність прояви несприятливих ситуацій, але й такі фактори зовнішнього та внутрішнього середовища, як невизначеність, випадковість і протидія. Наступ кризових явищ сам собою може розглядатися як форма ризику та антикризове управління компаніям передбачає особливий підхід до управління подібними ризиками [16].

Невизначеність – це сума тих обставин, які можна передбачати заздалегідь, але не можна визначити, наскільки вони суттєво вплинуть на підсумкові показники логістичної діяльності.

Випадковість – це сума тих обставин, що виникають незалежно від загальної ситуації та, як правило, під впливом факторів зовнішнього середовища.

Протидія – це навмисний опір обставинам та учасникам логістичного процесу під час його виконання.

Також поняттю «ризик» властиві складність та багатогранність зовнішнього середовища.

Ризики залізничного транспорту можуть бути найрізноманітнішими. За своєю суттю ризики на транспорті поєднують різні види ризиків усіх складових ланок і елементів як у процесі зміни матеріальних, потоків грошових коштів та інформаційних потоків, так і в процесі власне управління ризиками, що виникають у логістичній системі.

У логістиці під підприємницьким ризиком розуміється ризик, що виникає за будь-яких видів та форм підприємницької діяльності, пов'язаних із виробництвом продукції, товарів та послуг, їх реалізацією; товарно-грошовими та фінансовими операціями; комерцією; здійсненням науково-технічних проєктів та ін. В економічному сенсі ризик – це ймовірність втрати вкладеного капіталу.

Сутність підприємницького ризику тісно пов'язана із з'ясуванням

функцій, що виконує ризик. Прийнято виділяти такі функції, як стимулювання, регулювання, захист та альтернативність.

Розглянемо зміст названих функцій.

Стимулююча функція ризику спрямована на пошук нетрадиційних вирішення проблем, що стоять перед керівником. Більшість компаній досягають успіху, стають конкурентоспроможними на основі ризикової діяльності. Слід зазначити, що такий тип господарювання призводить до більш ефективного виробництва, від якого виграють і споживачі, і суспільство загалом.

Регулююча функція ризику орієнтує керівника отримання, насамперед, значних результатів за рахунок подолання інертності, консерватизму, психологічних бар'єрів, що перешкоджають прийняттю та реалізацію перспективних рішень. Ця функція фіксує здатність ризикувати як один із можливих шляхів успішної виробничо-господарської діяльності.

Захисна функція ризику виявляється в тому, що якщо для керівника ризик – природний стан, то нормальним має бути і терпиме ставлення до невдач. Ініціативним та підприємливим господарникам потрібна соціальний захист у вигляді правових, політичних та економічних гарантій.

Функція альтернативності підприємницького ризику пов'язана з тим, що наявність ризику передбачає необхідність вибору одного з можливих варіантів розв'язків. У зв'язку з цим керівник у процесі ухвалення рішення аналізує різні варіанти, вибираючи найбільш рентабельний (у разі звичайного управління) та найменш ризиковий (у разі турботи про економічну безпеку у рамках антикризового управління). Залежно від конкретного змісту ситуації альтернативність має різну ступенем складності та дозволяється різними способами.

Будь-яке підприємство залізничного транспорту – це складна виробничо-економічна система, на яку впливає безліч різних факторів. Їх різний за обсягом та за часом вплив (разом або окремо, або в різних поєднаннях) викликає невизначеність, яка, своєю чергою, є джерелом ризику. Чинники

можуть бути закладені в організації діяльності чи стратегії компанії чи виступати результатом дій його керівника [30].

Чинники, що викликають логістичні ризики, можна умовно поділити на дві групи:

- суб'єктивні та об'єктивні;
- зовнішні та внутрішні.

Цифровізація як тенденція технологічного розвитку транспортної сфери була ідентифікована досить давно. Фактично можна вести мову про те, що проникнення цифрових технологій у транспортну сферу почалося з моменту виникнення електронно-обчислювальної техніки. За цей період було реалізовано велику кількість різних проєктів як з ініціативи урядів, так і приватних компаній.

Необхідно відзначити, що використання автоматизованих транспортних систем усе ще залишається дискусійним питанням, щодо якого в суспільстві немає консенсусу. До загроз і ризиків, які вказуються як прямі наслідки автоматизації на транспорті, слід віднести [47]:

- одночасне вивільнення великої кількості водіїв, які більше в принципі не зможуть працевлаштуватися за професією;
- складності у визначенні рівня відповідальності у разі настання страхового випадку;
- ризик відмови програмного забезпечення і втрата контролю над керованим транспортним засобом.

Взагалі, цифровізація є домінуючим процесом у транспортній сфері. До того ж процеси цифровізації самі по собі відбуваються набагато швидше, ніж попередні технологічні революції. Кінцевий результат цих перетворень передбачити важко. Однак можна виділити два найбільш істотних складника. З одного боку, ефективне використання цифрових технологій у транспортній сфері визначає рівень конкурентоспроможності будь-якої транспортної компанії. Ті з них, хто ігнорує сучасні зміни, ризикують покинути ринок. З іншого боку, саме процеси цифровізації є джерелом підвищених ризиків: і в

контексті економічного розвитку, і в контексті суспільного прогресу.

Для вітчизняних підприємств залізничного транспорту з метою боротьби з кіберризиками необхідно рухатися за трьома напрямками - впроваджувати нові технології, переходити на стандарти безпеки найкращих світових зразків, покращувати процеси та працювати з персоналом.

З технологічної точки зору українським транспортним компаніям слід якомога швидше відмовлятися від софту з російським корінням: від систем бухгалтерського обліку; від популярних crm-системи російської розробки тощо. Звісно, є випадки, коли знайти альтернативу цьому софту за прийнятною ціною досить складно, але це цілком можливо. Особливо з огляду на те, якими ризиками може обернутися використання софту з країни-агресора: від витоку або втрати даних, до саботажу і повного паралічу бізнесу.

Сьогодні на ринку є різноманітні хмарні сервіси та платформи для обліку української розробки, які закривають принаймні базові потреби транспортного бізнесу. Великі компанії можуть замислитись про заміну старого софту на нові CRM- та TMS-системи кастомної розробки. Таке рішення потребуватиме часу та інвестицій, але воно може повністю закрити потреби окремо взятої компанії, знизити до мінімуму ризик несанкціонованого втручання в процеси, локалізувати та убезпечити бази даних, а в подальшому і безпечно інтегрувати компанію у нову національну цифрову інфраструктуру.

Перехід на нові перспективні платформи відкривають шлях і для широкого впровадження нових технологій безпеки:

- блокчейн;
- верифікація даних на основі ШІ;
- методи обчислення для підвищення конфіденційності даних ;
- хмарні платформи з високим рівнем захисту.

У сфері регулювання Україна має і буде рухатись назустріч найкращим світовим практикам кібербезпеки. Євроінтеграція приведе українську логістичну галузь до загальноєвропейських стандартів NIS2, а тісна співпраця з американськими партнерами - до завершення впровадження стандартів

кіберзахисту NIST. Одночасно з цим українські регулятори та законодавці мають деталізувати вимоги до цифрової інфраструктури транспорту та логістики.

Зокрема, у Держспецзв'язку українським підприємцям рекомендують не чекати нормативного закріплення нових стандартів для окремих галузей бізнесу чи критичної інфраструктури, а починати роботу з впровадження принципів NIST просто зараз.

З точки зору процесів українському бізнесу настав час дещо змінити свій спосіб мислення та корпоративну культуру. Логістика історично залишається консервативною галуззю, де об'єктивно важко проводити масштабні реформи. Однак сучасні виклики потребують від неї дуже великої уваги до діджиталу загалом і до кібербезпеки зокрема. Видатки на діджитал в галузі так чи інакше зростатимуть, і важливо зробити так, аби ці інвестиції були максимально ефективними та безпечними.

3.3 Формування підходів антикризового управління підприємствами залізничного транспорту в умовах цифровізації

Антикризове управління в сучасній транспортній компанії передбачає перехід до кардинально іншого підходу до прийняття рішень, починаючи з визначення мети управління діяльністю та закінчуючи схваленням конкретних заходів для досягнення мети [68].

Одним із найважливіших аспектів успішного антикризового управління слід вважати правильну організацію інформаційних та комунікаційних потоків. При цьому часто труднощі виникають не стільки через те, як інформація поширюється, скільки через того, яка інформація та у якому вигляді. При цьому слід розрізняти декілька категорій інформаційних потоків, пов'язаних з організацією в кризових умовах [5]:

- внутрішньоорганізаційні;
- міжорганізаційні;
- між організацією та суспільством;
- між суспільством та організацією.

Будь-які транспортні компанії мають засоби для розповсюдження інформації всередині себе, тим самим забезпечуючи вимоги успішного функціонування у нормальний час. У подібній ситуації система організації інформаційних та комунікаційних потоків пристосована під певні чітко визначені та структуровані типи інформації та їх об'єм. Тим не менш, у момент кризи навантаження на комунікаційну та інформаційну внутрішньоорганізаційні системи різко зростає, що викликано як зростанням клієнтів цієї системи, так і зростанням потреби в інформації. Зростання клієнтів може визначатися залученням додаткової робочої сили та перепризначенням ключових фахівців на нові та додаткові позиції. Зростання потреби в інформації визначається екстраординарним характером проблем, які доводиться вирішувати у момент кризи.

На додаток до безпосереднього зростання навантаження на інформаційну систему в момент кризи змінюється характер та однорідність типів інформації, які повинні обслуговуватися системою, що може також викликати труднощі ефективної організації інформаційних потоків.

Нарешті, на відміну від звичайної операційної діяльності, антикризове управління вимагає незвичайних напрямів інформаційних потоків, не передбаченої стандартними процедурами та порядками субординації, прийнятими в організаційній структурі підприємства. Все це може підвищити навантаження на інформаційну та комунікаційну системи організації та призвести до негативних наслідків з погляду антикризового управління. Одним із можливих виходів у подібній ситуації слідє вважати попереднє планування та моделювання інформаційних потоків в умовах криз, а також інформування про можливі джерела проблем в організації інформаційних потоків у момент кризи ключових спеціалістів.

Міжорганізаційні інформаційні потоки у звичайних умовах можуть виявитися малоприсадиными в момент кризи, оскільки низка ключових для компанії нових гравців можуть бути не включені. Наприклад, у разі настання кризи передбанкрутного стану для правильної організації антикризового управління можуть знадобитися контакти із зовнішніми юристами, що спеціалізуються у справах про банкрутство. Швидкість реакції, настільки критична в багатьох кризових ситуаціях, може вимагати швидкої організації нових комунікаційних та інформаційних потоків у стислі терміни [8].

Організація інформаційних потоків у момент кризи може також виявитися ключовою в успішному антикризовому управлінні. Так як інформування зовнішніх зацікавлених осіб, особливо пов'язаних із компанією лише опосередковано, у момент кризи виробляється по абсолютно новим правилам, компанії мають тенденцію допускати у цьому процесі серйозні помилки. Зокрема, тісне знайомство з проблемами, що призвели до кризового стану в компанії, значні зусилля та фокус, спрямовані на вирішення відповідних проблем, які часто створюють спотворене бачення у представників компанії про те, якого виду інформація, якої якості та які подробиці потрібно зовнішнім партнерам (клієнтам, постачальникам, держ. регуляторам тощо).

Зрештою, канали інформації від зовнішніх зацікавлених осіб назад до компанії, чиє функціонування мало бути забезпечене і під час звичайної операційної діяльності, що набувають особливого значення в момент кризи. Якщо компанія сподівається подолати кризу і повернутися до життєздатний бізнес, вона має забезпечити діалог зі своїми споживачами, не тільки сприяє розумінню з їхнього боку, а й можливе збереження майбутніх зв'язків.

В момент кризи управління підприємством у сфері використання повноважень та прийняття рішень можуть виникати наступні проблеми:

- втрата ефективності вищої ланки керівництва через переробки;
- конфлікти щодо нових завдань у забезпеченні діяльності компанії;
- конфлікти повноважень звичайної ієрархії та нових виникаючих менш формальних структур управління.

Крім того, виділяються такі проблемні аспекти в галузі забезпечення взаємодії та забезпечення гнучкості управлінської структури:

- відсутність згоди у питаннях взаємодії всередині організації;
- напруга у відносинах, викликана новизною завдань антикризового управління;
- складнощі, викликані масштабом кризи, що розгорнулася.

Сильною стороною логістичного підходу до вивчення ефективності організації управління транспортною компанією є увага, що приділяється загальноорганізаційним цілям діяльності, яким мають бути підпорядковані у структурному та функціональному плані різноманітні логістичні підходи. Так, з точки зору організації антикризового управління логістика диктує виявлення відповідності результатів прийнятих антикризових заходів загальним цілям, для досягнення яких вони робилися.

Як було зазначено раніше, цифрові технології стали базою для створення нових продуктів, цінностей, властивостей та, відповідно, основою отримання конкурентних переваг на більшості ринків. Але масштабна цифровізація сфер життя призведе до того, що громадяни України та бізнес усе більше потерпатимуть від зростання кіберзлочинності.

Найнебезпечнішими для економіки та громадян є кібератаки на критичну інфраструктуру (енергозабезпечення, транспортне управління, банківський та телекомунікаційний сектори, медичне обслуговування, водопостачання тощо).

Нарешті, все складніші та взаємопов'язаніші цифрові технології призводитимуть до виникнення нових форм кібератак (т. з. вразливості «нульового дня»).

Україна та її спеціалізовані організації мають співпрацювати з усіма зацікавленими сторонами, особливо на європейському рівні, задля забезпечення національної кібербезпеки та кіберзахисту. Розробка технічних та організаційних рішень мають, з одного боку, не обмежувати можливостей, які відкриває для країни перехід до цифрових технологій, а з іншого — забезпечувати відповідний рівень довіри та безпеки кожному користувачу.

Національна система кібербезпеки України повинна [6,70]:

- забезпечити передню лінію оборони проти кіберзагроз шляхом посилення загальної ситуаційної обізнаності щодо інцидентів, вразливостей та загроз у середовищі державних установ, на об'єктах критичної інфраструктури, у громадському сегменті;
- запобігати вторгненням завдяки обміну інформацією та впровадженням контрзаходів, здатних зменшити поточні вразливості;
- захищати від повного спектру загроз шляхом підвищення контррозвідувальних та розвідувальних можливостей;
- зміцнити середовище кібербезпеки через освітянські, медійні громадські ініціативи;
- стимулювати та забезпечувати проведення кібернавчань, досліджень і розробок у сфері кібербезпеки.

Відповідно до Закону України «Про основні засади забезпечення кібербезпеки України», затвердженої Указом Президента України Стратегії національної системи кібербезпеки та відповідних рішень Ради Національної безпеки та оборони України, ключовими елементами Національної системи є:

- організаційно-технічна модель,
- відповідні її елементи — від національних центрів управління кібербезпекою до відповідних галузевих, приватних та інших центрів управління безпекою (SOC, Security Operations Centers) або центрів реагування на кіберзагрози (CERT, Computer Emergency Response Team).

Критичні завдання:

- скласти та затвердити перелік систем критичної інфраструктури (СКІ);
- провести аудит стану кібербезпеки СКІ з наданням відповідних рекомендацій щодо збільшення рівня захищеності та реагування на інциденти;
- створити центральні (ДССЗЗІ та СБУ вже створені) та галузеві центри запобігання кіберінцидентам та реагування на них (SOC, CERT) (згідно з європейською практикою, транспортний, енергетичний, фінансовий, телекомунікаційний, медичний, продовольчо-забезпечувальний рівень);

- розробити галузеві стандарти (настанови, інструкції) з кібербезпеки об'єктів СКІ та визначити механізми перевірки їх дотримання та оцінки виконання;

- розробити методику та заходи щодо проведення лабораторних та польових кібернавчань для спеціалістів та керівників СКІ та державних установ.

Довіра користувачів — істотний показник не лише для цифрової комунікації та транзакцій між громадянами, а й для бізнес-моделей, на яких базуються електронна економіка та комерція.

Держава має докласти всіх зусиль, щоб суспільство знало про наявні ризики, а також надати консультаційну та технологічну підтримку у впровадженні та використанні захищених інформаційно-комунікаційних систем, інфраструктур, платформ тощо.

Таким чином, інформаційна безпека — це комплекс заходів в інформаційній сфері із запобігання порушення цілісності, конфіденційності та доступності інформації, тобто кібербезпека — це система заходів в кіберпросторі, спрямована на забезпечення стану захищеності інформаційних ресурсів.

Виокремлюють три рівні забезпечення інформаційної безпеки:

- рівень особи (формування раціонального, критичного мислення на основі принци-пів свободи вибору);

- суспільний рівень (формування якісного інформаційно-аналітичного простору, плюралізм, багатоканальність отримання інформації, незалежні потужні ЗМІ, які нале-жать вітчизняним власникам);

- державний рівень (інформаційно-аналітичне забезпечення діяльності державних органів, інформаційне забезпечення внутрішньої і зовнішньої політики на міждержавному рівні, система захисту інформації з обмеженим доступом, протидія правопорушенням в інформаційній сфері, комп'ютерним злочинам).

Для суб'єктів господарювання, в тому числі й підприємств

залізничного транспорту, реалізація захисних заходів щодо забезпечення безпеки інформації в кіберпросторі можна привести у вигляді моделі наведеної на рисунку 3.2.

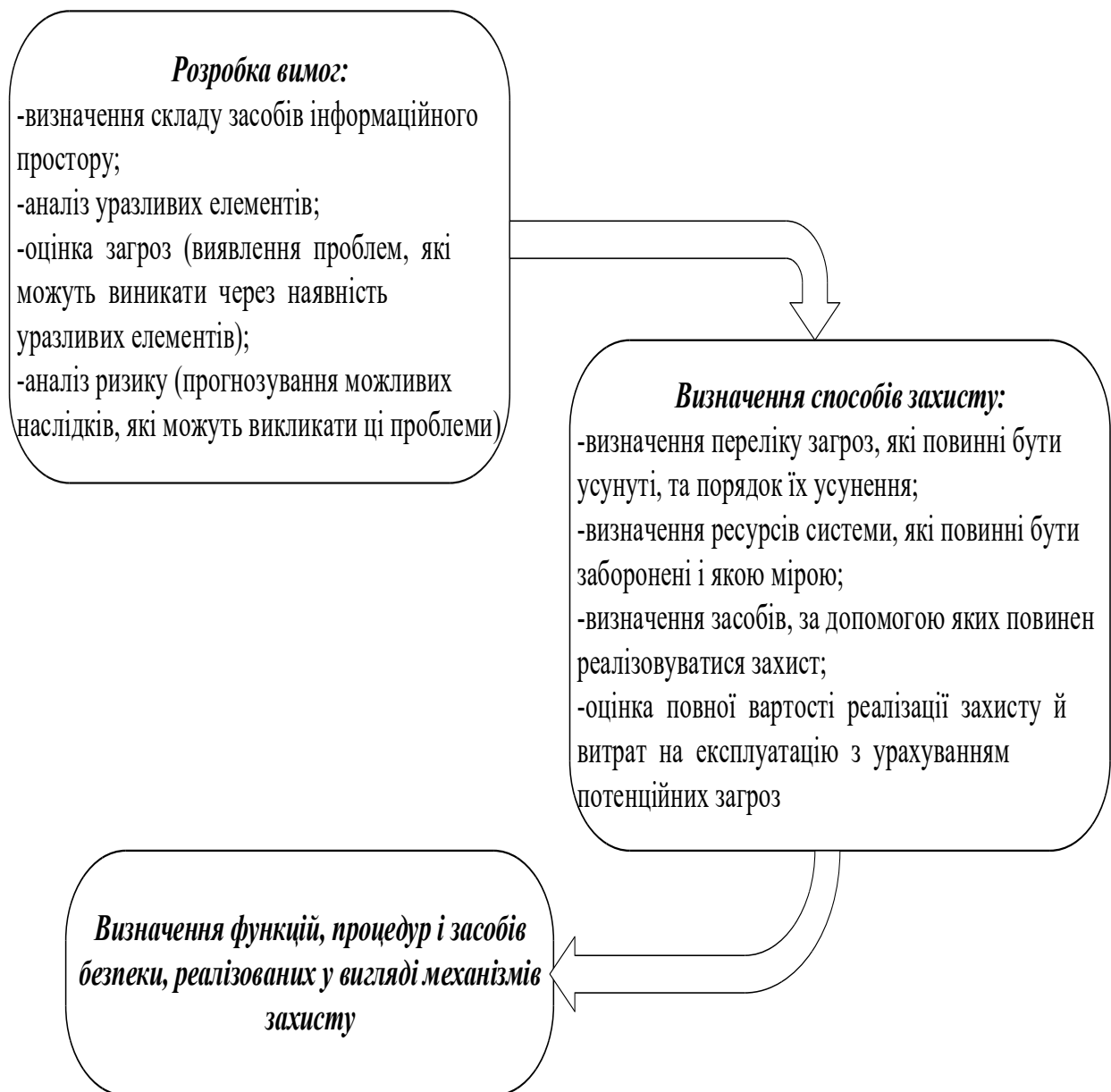


Рисунок 3.2 — Модель реалізації заходів щодо захисту підприємство в умовах цифровізації

В таблиці 3.1 наведено як успішні, так і невдалі аспекти результатів антикризових заходів щодо управління підприємствами залізничного транспорту в умовах цифровізації .

Таблиця 3.1 - Можливі успішні та невдалі результати антикризового управління

Завдання антикризового управління	Невдалий результат	Середній результат	Успіх
1	2	3	4
Розпізнавання кризових ознак	Усі ознаки кризи ігноруються Для організації криза настає абсолютно несподівано	Сигнали про кризу привертають увагу організації	Сигнали розпізнаються досить рано, щоб встигнути застосувати відповідні контрзаходи
Недопущення розростання кризових явищ	Криза виривається за кордони організації Негативно впливає на зовнішніх зацікавлених осіб	Збитки зовнішнім особам незначні	Значні негативні прояви кризи повністю обмежуються рамками організації
Відновлення бізнесу	Операційна діяльність організації повністю припинено Час зупинки операційної діяльності втрачено для відновлення операцій	Області операційної діяльності найбільш порушені кризою тимчасово закриті Час зупинки операційної діяльності мінімально без суттєвого впливу на продукцію (послуги)	Операційна діяльність продовжується у звичайних рамках під час та після кризи Доставка продукції (надання послуг) не постраждала
Засвоєння уроків	Жодних уроків не зроблено Організація повторює ті ж самі помилки у подібних обставинах	Уроки з кризи зроблені, але їх поширення обмежене	Організація змінює внутрішній регламент та процедури відповідно до впливу кризи Уроки кризи застосовуються до майбутніх кризових ситуацій
Підтримка репутації	Репутація терпить довготривалі негативні наслідки Поширене сприйняття організації як лиходія в п'єсі внаслідок неефективного антикризового управління	Негативні ефекти кризи короточасні Клієнти розпізнають помилки в деталях вжитих заходів антикризового управління, але продовжують користуватися послугами (продукцією) компанії	Образ організації виграє через сприйняття ефективності антикризових заходів Організація сприймається в якості героїчної, занепокоєної, що дбає про клієнта, і в

Продовження таблиці 3.1

1	2	3	4
		як зазвичай	якості жертви
Доступ до ресурсів	Організація робить відчайдушні зусилля, але не отримує доступ до необхідних ресурсів для боротьби з кризою	Організація робить відчайдушні зусилля і важко вибирається з кризи через власні резерви та незаплановану допомогу зі сторони	Ресурси організації чи зовнішніх зацікавлених осіб доступні в достатню кількості для проведення антикризових заходів
Прийняття рішень	Повільне прийняття рішень через внутрішні конфлікти Процес прийняття рішень заснований на довільних припущеннях, які суперечать реальності	Повільне прийняття рішень через зовнішні відносно організації обмеження	Своєчасні та доцільні рішення Процес прийняття рішень заснований на фактичних обставинах кризи

Будь-яка практика антикризового управління призводить як до вдалих результатів, так і до окремих невдач. Визначення найбільш успішного підходу до організації антикризового управління можливо за допомогою аналізу цих двох сторін результатів та уважного співвідношення важливості того чи іншого аспекту для успішного виживання компанії за умов кризи.

Як видно з таблиці 3.1, успіх в одному аспекті може супроводжуватись невдачею в іншому, і, виходячи лише з абстрактних, апріорних уявлень про взаємну важливість, не можна дійти невтішного висновку у тому, яка технологія антикризового управління виявиться найбільш вдалою на практиці.

Адаптивна модель інформаційної безпеки вимагає від сучасних технологій захисту, забезпечення спостережності мережі, орієнтацію на загрози і базування на платформі (рисунок 3.3).

Розкриємо компетенції захисту, наведені на рисунку 3.3 більш детально.

Можливість «Запобігання» описує набір політик, продуктів та процесів, які застосовуються для запобігання успішної атаки. Основна мета цієї категорії

полягає в тому, щоб попередньо зменшити вразливість системи, виявити можливі техніки, технології та процедури реалізації кібератак, перш ніж вони розпочнуться.

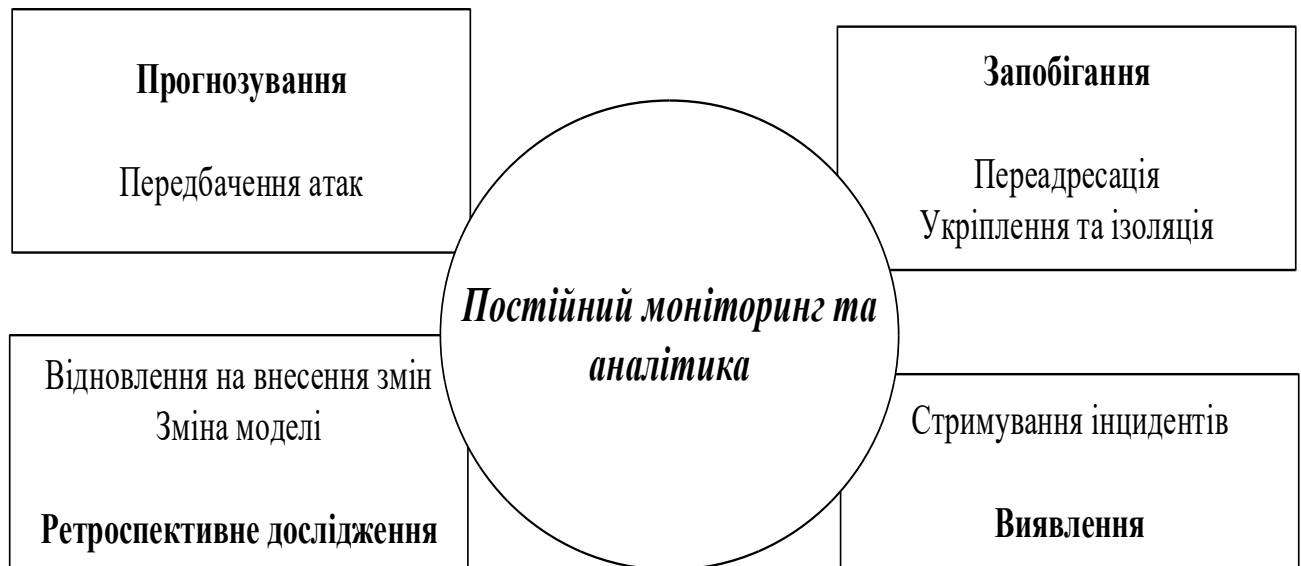


Рисунок 3.3 – Адаптивна модель безпеки

Можливість «Виявлення» призначена для пошуку атак, які «уникнули» запобігання. Основною метою цієї категорії є зменшення часу існування (присутності) загроз в мережі та, таким чином, зниження потенційного збитку, який вони можуть заподіяти. Можливості детектування мають вважатись критичними, оскільки до цього спонукає ризик-орієнтований підхід: необхідно відноситись до критичних даних так, нібито вони вже скомпрометовані.

Можливість «Ретроспективне дослідження» – знання та засоби, необхідні для використання даних, виявлених під час детектування (внутрішніми або зовнішніми акторами), з метою проведення криміналістичного аналізу накопичених раніше даних та аналізу основних причин кіберінциденту, а також напрацювання нових запобіжних заходів, щоб уникнути майбутніх кіберінцидентів.

Можливість «Прогнозування» дозволяє організації вивчати накопичені дані у кореляції з відомостями, отриманими ззовні (надані організаціями, що здійснюють розвідку кіберзагроз, вразливості, розкриті «білими хакерами» в результаті пантеїсту, інциденти та атаки, що відбулись в сторонніх організаціях зі схожими елементами захисту або споріднені за родом діяльності, афілійовані або які є постачальниками довірених послуг), щоб активно передбачати нові типи атак, а також активно наповнювати системи евристичного аналізу, що використовують штучний інтелект як основу для самонавчання.

Також, адаптивна модель інформаційної безпеки вимагає від сучасних технологій захисту, забезпечення спостережності мережі, орієнтацію на загрози і базування на платформі.

Зокрема, спостережність: адміністратори мереж, серверів, а також фахівці підрозділу кіберзахисту повинні відслідковувати все, що відбувається в мережі, на її інформаційних ресурсах, в системах віртуалізації, кінцевих пристроях. Це вимагає поєднання ширини і глибини. Аспект ширини відповідає за можливість збирати дані по усіх напрямках потенційних атак, що охоплює мережу, кінцеві пристрої, поштові та веб-шлюзи, мобільні пристрої, віртуальні і хмарні середовища. Аспект глибини дає можливість співвідносити ці відомості і застосовувати їх, щоб вивчити контекст проблеми, знайти краще рішення і виконати дії як вручну, так і автоматично.

Орієнтація на загрозу: сучасні мережі працюють всюди, де знаходяться співробітники і дані. Незважаючи на значні зусилля, фахівці з кіберзахисту не завжди встигають за зловмисниками, які атакують з нових напрямків. Для скорочення радіуса атаки необхідні спеціальні політики і засоби контролю, однак загрози проникають в мережу. Тому технології захисту повинні бути націлені на виявлення, аналіз і усунення загроз. Орієнтація на загрози означає думати як зловмисник, спиратися на спостережність мережі і контекст для адаптації до змін середовища і знаходити спосіб захисту від загрози. Нове шкідливе програмне забезпечення і атаки нульового дня вимагають постійного вдосконалення захисту. З цією метою необхідний безперервний збір даних хмарної аналітики, які

передаються в усі системи безпеки для підвищення їх ефективності.

Базування на платформі: кібербезпека не обмежується мережею і вимагає інтегрованої системи гнучких і відкритих платформ, які охоплюють мережу, пристрої та хмари. Ці платформи повинні бути розширюваними, масштабованими і централізованими, щоб забезпечити уніфіковані політики і засоби управління. Тобто, вони повинні відповідати масштабу атак. Для цього необхідно перейти від пристроїв точкового захисту до сучасної платформи сервісів та додатків, що масштабуються і легко розгортаються. Підхід на базі платформи не тільки підсилює систему кіберзахисту, усуваючи вразливості і недоліки, але також дозволяє швидше виявити загрозу і визначити захисні дії.

На АТ «Укрзалізниця» цифровий розвиток координується Філією «Головний інформаційно-обчислювальний центр» та ототожнюються безпосередньо з інформаційним забезпеченням експлуатаційної діяльності залізничного транспорту, впровадженням автоматизованих систем управління, програмним забезпеченням обробки оперативної, статистичної та фінансової інформації. Нині в компанії використовуються такі автоматизовані системи управління, як [70]:

- АСК ПП УЗ. Автоматизована система керування пасажирськими перевезеннями(АСК ПП УЗ) забезпечує обслуговування пасажирів щодо перевізних документів. АСК ПП УЗ забезпечує бронювання місць та продаж квитків на пасажирські поїзди. АСК ПП УЗ прийшла на зміну автоматизованих систем Експрес 2 та Експрес Узм. Автоматизована система керування пасажирськими перевезеннями працює на потужному серверному комплексі IBM Z9. Це дає змогу обслуговувати сотні запитів за секунду з мінімальною затримкою;

- АСК ВП УЗ-Є. Єдина автоматизована система керування вантажними перевезеннями (АСК ВП УЗ-Є) була введена в експлуатацію 07.07.2012 замість систем АСОУП та АСК ВП УЗ, які функціонували на рівні залізниць України. Нова система архітектурно побудована для централізованого керування процесом вантажних перевезень;

- АС Клієнт. Система АС Клієнт УЗ надає сучасний сервіс клієнтам залізничного транспорту України по оформленню електронної накладної. Система АС Клієнт УЗ розроблена з метою надання клієнту залізничного транспорту сервісу для оформлення перевезення вантажів згідно вимог Правил перевезень вантажів залізничним транспортом України, відповідно до яких на кожне перевезення вантажу необхідно надавати в товарні контори залізничних станцій електронні дані перевізного документу та комплект паперових перевізних документів – накладну. Електронні дані перевізних документів, що формуються в АС Клієнт УЗ, за структурою та форматом відповідають чинним нормативним документам Укрзалізниці та вимогам автоматизованих систем, що застосовуються в організації автоматизації документообігу даної галузі.

- АС Месплан. Автоматизована система документообігу замовлень на перевезення вантажів та формування планів(АС Месплан) створена для керування вагонним парком Укрзалізниці та можливості більш зручного способу замовлення вагонів під навантаження клієнтами залізничного транспорту України;

- АЦСК Укрзалізниці. Відповідно до чинного законодавства, Укрзалізниця та інші підприємства, що входять до її складу, як державні підприємства повинні використовувати лише посилені сертифікати ключів, які обслуговуються в акредитованому центрі сертифікації ключів (АЦСК). Центр сертифікації ключів (ЦСК) та використання технології електронного цифрового підпису (ЕЦП) дозволяє набути юридичного статусу документам що пересилаються в електронному вигляді між Укрзалізницею, залізницями, організаціями, підприємствами, установами залізничного транспорту, а також між структурами УЗ та їх клієнтами, що суттєво прискорить виробничий процес і дасть гарантію цілісності та достовірності переданій електронній інформації;

- сервіс онлайн резервування та покупки квитків .Сервіс онлайн резервування та покупки квитків хоча є самою молодого системою яку обслуговує філія «ГІОЦ «АТ Укрзалізниця», але від травня 2012 року, коли почали продаватися перші онлайн квитки, сервіс набув великої популярності

завдяки простому та зручному інтерфейсу користувача. Якщо потрібно перевірити наявність квитків, зробити бронювання чи просто придбати для себе або когось іншого пасажирській проїзний документ це просто. Треба лише зайти на сервіс онлайн резервування та покупки квитків Укрзалізниці в мережі Інтернет, вибрати звідки та куди потрібно подорожувати, дату подорожі та конкретні місця. Потім необхідно сплатити за послугу платіжною картою та й все - квиток у пасажирів;

- АС СКЕДО. Автоматизована система керування електронним документообігом Укрзалізниці(АС СКЕДО) створено для переходу на безпаперовий обмін документами між Адміністрацією залізничного транспорту, підприємствами залізничного транспорту та залізницями України. Система АС СКЕДО розроблена в середовищі Lotus Domino та функціонує як складова частина документообігу Укрзалізниці. Працює з цифровими підписами акредитованого центру сертифікації ключів та використовує алгоритми підпису згідно ДСТУ 4145-2002, що дає юридичну силу електронним документам;

- АСК Кадри. Автоматизована система керування кадрами Укрзалізниці(АСК Кадри) створено для ефективного управління кадрами Адміністрацією залізничного транспорту, підприємствами залізничного транспорту та залізницями України.

На даний час АТ «Укрзалізниця» з метою забезпечення кіберзахисту інформаційних систем, електронних інформаційних ресурсів, забезпечення ефективної інформатизації та цифровізації галузі, моніторингу, реагування та запобіганню кіберзагрозам з інформаційної безпеки користується послугами ДП «Галузевий центр цифровізації та кібербезпеки».

Діяльністю підприємства є здійснення моніторингу та аналізу стану кіберзахисту підприємств, установ та організацій, що належать до сфери управління Уповноваженого органу управління, участь у формуванні та впровадженні програм з кіберзахисту, цифровізації, проєктів інформатизації, їх розвитку, оперативне реагування на інциденти пов'язані із спробами втручання в роботу інформаційних систем, електронних інформаційних ресурсів,

комунікаційних та/або технологічних систем. Формування, на основі отриманої інформації, рекомендацій щодо посилення захисту, а також проведення роз'яснювальної роботи із працівниками підприємств галузі з метою підвищення їх рівня обізнаності стосовно сучасних методів та засобів кіберзагроз.

Стратегічними напрямками діяльності ДП «Галузевий центр цифровізації та кібербезпеки» є [70]:

- забезпечення кібербезпеки і безпеки інформаційних ресурсів;
- підвищення ефективності фінансово-господарської діяльності.

У розрізі зазначених напрямів виокремлено основних вісім цілей діяльності:

- підвищення стану захищеності підприємств галузі від кіберзагроз;
- створення учбового центру і- Training;
- створення та розвиток Центру кіберзахисту Міністерства інфраструктури України;
- створення єдиної інформаційної системи Міністерства інфраструктури України;
- отримання статусу галузевого оператора платіжної інфраструктури;
- забезпечення безперервності доступності та безпеки електронних сервісів Міністерства інфраструктури України;
- переведення процесу надання адміністративних послуг в електронний формат;
- виведення з кризового стану та забезпечення операційної ефективності ДП «ГЦЦК».

Але цифровізація суспільства - це динамічний процес. Інформація є основою кібербезпеки. Тож для підприємств залізничного транспорту за спеціалізацією діяльності з кіберзахисту структурно вимальовується потреба у підрозділах:

- розвідки кіберзагроз, що у повсякденній діяльності зосереджені на отриманні (набутті) нових знань про реальні або потенційні загрози і вразливості;

- моніторингу та управління інцидентами безпеки, які у повсякденній діяльності концентруються на виявленні інцидентів, оцінці поточного стану кіберзахисту та кореляції телеметричних даних з іншими потоками даних;

- команди реагування на кіберінциденти, які в режимі постійної готовності очікують детектування кібератаки, та, за умови настання такої ситуації, мобілізують сили і засоби інших підрозділів кіберзахисту, координують свою діяльність із зовнішніми структурами кіберконтррозвідки, кібероборони, кіберрозвідки.

Основною діяльністю підрозділу розвідки кіберзагроз буде регулярний і систематичний збір інформації про кіберзагрози та кібервразливості з різних джерел, а також її подальший аналіз для розуміння поточних і потенційних кібератак, що можуть загрожувати організації, покращення і збагачення бази знань про кіберзагрози й її поширення між суб'єктами кіберзахисту.

Підрозділ моніторингу та управління інцидентами безпеки являє собою інфраструктуру, основою якої є команда інформаційної безпеки, що відповідає за моніторинг та аналіз стану безпеки організації на постійній основі. Метою підрозділу має бути виявлення, аналіз та реагування на інциденти, пов'язані з кібербезпекою, використовуючи комбінацію технологічних рішень.

Команда реагування на кіберінциденти – група експертів в області кібербезпеки, основним обов'язком якої є реагування на інциденти комп'ютерної та кібербезпеки. Ця команда також може надавати необхідні сервіси для обробки інцидентів та підтримки своїх клієнтів у процесі відновлення після виявлення вразливостей в системах безпеки.

Висновки до розділу 3

Антикризове управління передбачає кардинальне зміщення цільових орієнтирів в організації діяльності суб'єкта господарювання, викликане

абсолютним домінуванням міркувань збереження життєздатності компанії та його швидкого повернення у стан нормального функціонування у разі зниження інтенсивності впливу факторів-загроз, що спричинили стан кризи. Як наслідок, характер вживаних керівними органами дій зазнає суттєвих змін, що відображається, в тому числі, і в економічних аспектах організації діяльності транспортних компаній.

Українська логістична галузь останніми роками опинилась в особливо тяжкому становищі. з одного боку, вона змушена швидко йти у діджитал, аби зберегти свою ефективність та конкурентоспроможність на тлі небачених криз. з іншого, цей бізнес ніколи не існував сам по собі, адже це частина критичної інфраструктури, яка забезпечує країні звичне, нормальне життя.

Неконтрольоване зростання кібер-вразливостей - це зворотна сторона стрімкої диджиталізації, якої ніяк не можна уникнути. Нехтування кібербезпекою може стати надзвичайно дорогою помилкою у масштабах цілої країни - спровокувати гуманітарну або політичну кризу. В українських реаліях 2022 року воно може призвести й до трагічних наслідків та людських жертв.

Тож сьогодні логістичні компанії не мають шукати відповіді на складні питання самотужки. допомогти їм має і держава, що може формувати нові стандарти кібербезпеки та сприяти їх впровадженню, і сфера it, яка має відповідну експертизу, фахівців та технології. переконаний, за такої співпраці будь-які глобальні виклики можна подолати з мінімальними ризиками.

Зауважимо, що все різноманіття ризиків діяльності підприємств транспорту набуває особливої актуальності в рамках організації антикризового управління. Саме необхідність забезпечення в першу чергу економічної безпеки компанії, характерне для антикризового управління, диктує уважне ставлення до ризиків та викликає спроби керування ними з урахуванням поставленої мети: а саме, забезпечити виживання компанії у ворожих кризових умовах.

Підсумовуючи все викладене вище, в розділі сформовано модель реалізації заходів щодо захисту підприємств залізничного транспорту в умовах цифровізації та наведено успішні та невдалі аспекти результатів антикризових заходів щодо управління для забезпечення інформаційної безпеки.

Висновки

Цифровий формат сучасного життя змінює традиційні уявлення про способи і механізми зберігання, обігу та захисту інформації, відкриває дорогу до інноваційного розвитку підприємств, що дає можливість поєднати всі виробничі процеси в єдину цифрову систему та максимально автоматизувати управління цією системою:

- використовуючи стратегію Mobile First, компанії отримують і монетизують мобільний трафік, який за своїми показниками вже наздогнав трафік зі стаціонарних пристроїв;

- готові рішення дають змогу економити час на вирішення завдань. Різні програми, розширення та конектори оптимізують роботу компанії і вимагають мінімальних витрат часу на їх впровадження та адаптацію;

- масове впровадження інтелектуальних датчиків в обладнання та виробничі лінії (технології індустріального Інтернету речей);

- перехід на безлюдне виробництво і масове впровадження роботизованих технологій; – перехід на зберігання інформації та проведення обчислювань із власних потужностей на розподілені ресурси («хмарні» технології);

- наскрізна автоматизація та інтеграція виробничих і управлінських процесів у єдину інформаційну систему («від обладнання до міністерства»);

- використання всієї маси збираних даних (структурованої та неструктурованої інформації) для формування аналітики (технології «великих» даних);

- перехід на обов'язкову оцифровану технічну документацію та електронний документообіг («безпаперові» технології);

- цифрове проектування та моделювання технологічних процесів, об'єктів, виробів протягом усього життєвого циклу від ідеї до експлуатації (застосування інженерного програмного забезпечення);

- застосування технологій нарощування матеріалів взамін зрізання («адитивні» технології, 3D прінтинг);
- застосування сервісів із автоматичного замовлення витратних матеріалів і сировини для виробництва продукції й автоматичного постачання готової продукції споживачу, оминаючи посередницькі ланцюжки;
- застосування безпілотних технологій у транспортних системах, у т. ч. для постачання промислових товарів;
- застосування мобільних технологій для моніторингу, контролю процесів та управління ними у житті та на виробництві;
- перехід на реалізацію промислових товарів через Інтернет.

Цифрова революція, яка охопила світову економіку, вражає масштабом, темпами і географією. З кожним роком зростає інтенсивність впровадження нових технологій у виробництво й обслуговування людських потреб. Однак інший бік масштабної цифровізації сфер життя веде до того, що громадяни України та бізнес усе більше потерпатимуть від зростання кіберзлочинності. Найнебезпечнішими для економіки та громадян є кібератаки на критичну інфраструктуру (енергозабезпечення, транспортне управління, банківський і телекомунікаційний сектори, медичне обслуговування, водопостачання тощо) України

Аналіз сучасного стану і тенденцій розвитку підприємств залізничного транспорту дозволив встановити, що назрілі проблеми функціонування вітчизняного залізничного транспорту, діюча система управління галуззю і бізнес-модель розвитку залізничного транспорту не дозволяє в повній мірі скористатися перевагами цифровізації і забезпечити цифрову трансформацію та модернізацію бізнес-процесів підприємств галузі.

На сьогодні перед підприємствами залізничного транспорту постала необхідність вирішення низки викликів, пов'язаних із високим рівнем зношеності рухомого складу та залізничної інфраструктури і, як результат, дефіцитом рухомого складу та обмеженістю використання інфраструктурного потенціалу залізниці, зниженням оборотності вагонного парку, незадоволеністю клієнтів

тарифною політикою компанії і якістю послуг залізничного транспорту, корупційними порушеннями в компанії і посиленням її фінансових зобов'язань перед міжнародними фінансовими установами.

Цифрова трансформація залізничного транспорту є необхідною умовою його подальшого ефективного розвитку і конкурентоспроможності. Однак можливості реалізації цифрових проєктів у залізничній сфері нині обмежуються наявними бар'єрами, серед яких відсутність професійних компетенцій у керівників і фахівців у сфері цифрової трансформації; недостатній рівень інформаційно-комунікаційної інфраструктури; невідповідність вимогам цифровізації організаційних структур управління; відсутність готових інноваційних рішень і висока складність цифрових проєктів у сфері залізничного транспорту; відсутність фінансових коштів. Також значною проблемою є забезпечення безпеки, особливо інформаційної. Адже інформаційна безпека в XXI столітті виходить на перше місце в системі національної безпеки

У сучасному цифровому світі проблема інформаційної безпеки (що частіше замінюється терміном кібербезпека) усвідомлена як найважливіша. Будь-яка діяльність людини в цифровому житті чи то виробнича, соціальна, політична, просто побутова, не може обійтися без надійного захисту інформації та безпечних форм її використання. У зв'язку з чим актуальним завданням стає спроможність захисту інформації. Ця проблема є актуальною для підприємств залізничного транспорту, які активно впроваджують цифрові технології в усі виробничі та технологічні процеси, особливо сьогодні в умовах війни, коли залізниці стали рятівними артеріями країни.

Швидкі темпи технологічного розвитку суспільства та його всеосяжна цифровізація обумовлюють зростання технологічної складності та масштабності кібер-загроз у всіх секторах економіки. Все це потребує розроблення відповідних заходів щодо забезпечення безпеки.

У рамках удосконалення діяльності підприємств залізничного транспорту виникають питання оптимального реагування на зовнішні та внутрішні обставини,

що розвиваються нетрадиційними шляхами. Один з найважливіших класів подібних обставин представлений наслідками розвитку кризових явищ у транспортній системі, суміжних галузях, серед клієнтів і споживачів і, зрештою, у всій економіці країни. Розумно організоване керування транспортно-логістичною системою, сформовані навколо залізничного транспорту, повинні мати обґрунтовані механізми та регламенти дій у разі настання кризових подій

В кваліфікаційній роботі з метою забезпечення безпеки підприємств залізничного транспорту в умовах динамічної цифровізації та військової агресії сформовано підходи до антикризового управління в транспортно-логістичній системі та сформовано модель реалізації заходів щодо захисту підприємства в умовах цифровізації.

Використання розробленої моделі дає можливість провести оцінювання впливу показників на стан безпеки підприємств залізничного транспорту з метою захисту інформації й сприяти підвищенню ефективності використання інструментів цифрового регулювання транспортної безпеки.

Список використаних джерел

- 1 Про залізничний транспорт: Закон України 273/96-ВР; офіц. текст станом на 04.11.2018. URL: <https://zakon.rada.gov.ua/laws/show/273/96-%D0%B2%D1%80>.
- 2 Про схвалення Національної транспортної стратегії України на період до 2030 року: розпорядження Кабінету Міністрів України від 30 травня 2018 р. № 430-р. URL: <https://zakon.rada.gov.ua/laws/show/430-2018-%D1%80>.
- 3 Про утворення публічного акціонерного товариства «Українська залізниця»: постанова Кабінету Міністрів України від 25 червня 2014 р. N 200. URL: <https://zakon.rada.gov.ua/laws/show/200-2014-%D0%BF#Text>
- 4 Про стимулювання розвитку цифрової економіки в Україні: Закон України. URL: <https://zakon.rada.gov.ua/laws/show/1667-20#Text>
- 5 Про інформацію: Закон України від 2 жовтня 1992 року №2658-XII. URL : <http://zakon3.rada.gov.ua/laws/show/2657-12/ed20110106>.
- 6 Про схвалення Стратегії розвитку інформаційного суспільства в Україні: Розпорядження Кабінету Міністрів України; Стратегія від 15.05.2013 №386-р. URL: <https://zakon.rada.gov.ua/laws/show/386-2013-%D1%80/ed20130515#n21>
- 7 Розпорядження Кабінету Міністрів України «Про схвалення Концепції розвитку цифрової економіки та суспільства України на 2018-2020 роки та затвердження плану заходів щодо її реалізації», №67-р від 17.01.2018р. Режим доступу: <https://zakon.rada.gov.ua>, дата звернення 05.05.2020
- 8 Про Національну програму інформатизації: Закон України від 04.02.1998 №74/98-ВР. Відомості Верховної Ради України. 1998. №27-28. С. 181.
- 9 Про інноваційну діяльність: Закон України від 04. 07. 2002 р. № 40-IV URL: <https://zakon.rada.gov.ua/laws/show/40-15#Text>.

10 Цивільний кодекс України: офіц. тест станом на 10.10.22 р. URL: <https://zakon.rada.gov.ua/laws/show/435-15#Text>

11 Дані щодо колійного господарства (протяжність, відремонтовано, потребують ремонту). URL: <https://data.gov.ua/dataset/a4305cef-c8e0-4232-bb48-637ae4301261>

12 Дикань В.Л., Кірдіна О.Г. Сутнісні аспекти конкурентоспроможності національної економіки. *Вісник економіки транспорту і промисловості*. 2009. № 28. С. 13-20.

13 Дикань В. Л. Індустріально-інноваційні центри як основа технологічного розвитку українських залізниць. *Вісник економіки транспорту і промисловості*. 2017. № 58. С. 7-9.

14 Дикань В. Л. Товарознавство та комерційна діяльність: підручник / В. Л. Дикань та ін.; за ред. В. Л. Дикань. Харків: УкрДУЗТ, 2018. 362 с.

15 Дикань В. Л., Воловельська І. В. Інноваційні стратегії підприємств: проблеми, шляхи вирішення. *Вісник економіки транспорту і промисловості*. 2019. № 67. С. 9–17.

16 Дикань В. Л., Воловельська І. В., Маковоз О. В. Економічна безпека підприємства: навч. Посібник. Х.: УкрДАЗТ, 2011. 243 с.

17 Дикань В. Л., Єлагін Ю .В., Сухорукова Т. Г. Економіка праці на підприємствах залізничного транспорту: підручник. Х.: УкрДАЗТ, 2012. 275 с.

18 Дикань В. Л., Козинець А. С., Чупир Т. Я. Економічний аналіз ефективності діяльності залізниці: навчальний посібник. Харків, 2004. 161 с.

19 Дикань В. Л., Корінь М. В. Державне регулювання промислового розвитку України. *Вісник економіки транспорту і промисловості*. 2018. №. 61. С. 9-19.

20 Дикань В. Л., Маслова В.О. Організація виробництва: навчальний посібник. Харків, УкрДАЗТ, 2013. 422 с.

21 Дикань В. Л., Обруч Г. В. Управління реалізацією спільних інвестиційних проектів за участю підприємств залізничного транспорту в умовах цифровізації.

Вісник економіки транспорту і промисловості. 2020. № 69. С. 9-21.

22 Дикань В.Л. Українська модель економічної системи як нова концепція розвитку національної економіки. *Вісник економіки транспорту і промисловості*. 2013. Вип. 44. С. 11-17.

23 Дикань В.Л., Обруч Г.В. Визначення ефективності реалізації потенціалу конкурентоспроможності вагонобудівних підприємств. *Вісник економіки транспорту і промисловості*. 2016. № 56. С. 9-18.

24 Дикань В.Л., Островерх Г.Є. Удосконалення механізмів державного управління розвитком залізничної галузі України у євроінтеграційному просторі. *Вісник економіки транспорту і промисловості*. 2018. № 62. С. 11–19.

25 Дикань В.Л., Толстова А.В. Розвиток економіки України на основі принципу рівноправності відносин держави, бізнесу та суспільства. *Вісник економіки транспорту та промисловості*. 2018. № 63. С. 9-19.

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

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

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

29 Дикань, В. Л., Воловельська І.В., Каличева Н.Є. Економіка підприємства: конспект лекцій. Ч. 4. Харків : УкрДУЗТ, 2022. 50 с.

30 ДП «Галузевий центр цифровізації та кібербезпеки». URL: <https://icdc.gov.ua/>

31 Древаль І. В. Залізничний вокзальний комплекс як динамічна «візитівка» сучасного міста. Досвід та перспективи розвитку міст України. *Проблеми розвитку найкрупніших міст України*. 2011. Вип. 20. С. 250–259.

32 Ейтутіс Г. Д., Кривопішин О. М., Федорко І. П., Осовик В. М. та ін. Теоретико-прикладні основи реформування залізничного транспорту України: монографія. Ніжин: ТОВ «Вид-тво «Аспект-Поліграф», 2016. 256 с.

33 Економічна діагностика: підручник / В. Л. Дикань, І. В. Токмакова, В. О. Овчиннікова, М. В. Корінь, А. В. Толстова. Харків: УкрДУЗТ, 2022. 285 с.

34 Забезпечення конкурентоспроможності підприємств: підручник / В. Л. Дикань, Ю. Т. Боровик, О. М. Полякова, Ю. М. Уткіна. Харків: УкрДАЗТ, 2012. 415 с.

35 Зношеність локомотивного парку «Укрзалізниці» становить 97 %. URL: <https://gmcenter.ua/news/znoshenist-lokomotivnogo-parku-ukrzhaliznici-stanovit-97/>

36 Каличева Н.Є. Теоретико-методологічні засади забезпечення конкурентоспроможності підприємств залізничного транспорту в умовах трансформації бізнес-середовища: дис. ... д-р екон. наук: 08.00.04. Харків, 2019. 525 с.

37 Каличева Н.Є., Сударська І.В. Теоретико-прикладні аспекти розвитку підприємств залізничного транспорту в умовах структурних зрушень в економіці. *Економічний простір*. 2020. № 159. С. 71-74.

38 Кірдіна О. Г. Проблеми та перспективи інноваційного розвитку залізничного транспорту. *Вісник економіки транспорту і промисловості*. 2015. № 50. С. 285-289.

39 Кірпа Г. М., Корнієнко В. В., Пшинько О. М. та ін. Залізниці світу в ХХІ столітті: монографія / під заг. ред.: Г. М. Кірпи. Дніпропетровськ: Вид-во. Дніпропетр. нац. ун-ту залізн. трансп. ім. акад. В. Лазаряна, 2004. 224 с.

40 Корінь М. В. Інфраструктурні асиметрії розвитку залізничного транспорту України в умовах інтеграції в транспортно-логістичний простір ЄС. *Економічний вісник Запорізької державної інженерної академії*. 2018. Вип. 6 (18). С. 74 – 80.

41 Корінь М. В. Розвиток інфраструктури залізничного транспорту в умовах транскордонного співробітництва: монографія. Харків: УкрДУЗТ, 2019. 401 с.

42 Корінь М. В., Сендюк В. Є., Муквіч О. С. Теоретичні засади модернізації підприємств залізничного транспорту України. *Вісник економіки транспорту і*

промисловості. 2018. № 64. С. 231-240.

43 Кузьменко А.М. Особливості проблем законодавчого забезпечення інформаційної безпеки держави, суспільства і громадянина в умовах інформаційно-психологічного протиборства. *Часопис Київського університету права*. 2010. № 4. С. 317-321.

44 Ломотько Д.В., Філіпський О.В., Кравченко Д.М. Удосконалення роботи транспортно-пересадочних вузлів під час мультимодальних пасажирських перевезеннях за участю залізниць та автотранспорту. *Наукові праці Вінницького національного технічного університету*. 2019. Вип. 4. URL: <https://praci.vntu.edu.ua/index.php/praci/article/view/579>.

45 Наявні проблеми у функціонуванні залізничного транспорту вимагають регуляторних та управлінських заходів задля їхнього вирішення. URL: <https://brdo.com.ua/analytics/nayavni-problemy-u-funktsionuvanni-zaliznychnogo-transportu-vymagayut-regulyatornyh-ta-upravlinskyh-zahodiv-zadlya-yih-vyrishennya/>

46 Нібулон придбав локомотив та отримав дозвіл від УЗ на подачу та забирання вагонів. URL: <https://www.railinsider.com.ua/nibulon-prydbav-lokomotyv-ta-otrymav-dozvil-vid-uz-na-podachu-ta-zabyrannya-vagoniv/>

47 Офіційний сайт АТ «Укрзалізниця». URL: <https://www.uz.gov.ua/>

48 Овчиннікова В.О., Торопова В.І. Розвиток підприємств залізничного транспорту України в умовах цифровізації. *Вісник економіки транспорту і промисловості*. 2019. № 68. С. 175-181.

49 Очікується зростання електрифікації залізниць у Європі. URL: <https://www.railway.supply/uk/ochiku%D1%94tsya-zrostannya-elektrifikaczi%D1%97-zaliznicz-u-%D1%94vropi/>

50 Підприємництво. Реалізація підприємницької діяльності у сучасних ринкових умовах: підручник / С. В. Панченко, В. Л. Дикань, О. В. Шраменко та ін. Харків : УкрДУЗ, 2018. ч. 2. 228 с.

51 Підприємництво. Теоретичні основи організації підприємницької діяльності: підручник / С. В. Панченко, В. Л. Дикань, О.В. Шраменко та ін. Харків : УкрДУЗТ, 2018. ч. 1. 241 с.

52 Підсумки роботи залізничного транспорту України у 2022 році. Національний інститут стратегічних досліджень. URL: <https://niss.gov.ua/news/komentari-ekspertiv/pidsumky-roboty-zaliznychnoho-transportu-ukrayiny-u-2022-r> (дата звернення: 19.10.2023).

53 Приймак Ю.Ю. Національні інформаційні ресурси – джерело державних інформаційних продуктів та послуг. Державне управління: теорія та практика. 2009. No2. URL : www.academy.gov.ua/ej/ej10/doc_pdf/Priymak.pdf.

54 Про запровадження експериментального проєкту щодо забезпечення впровадження замовлення бланків дозволів на поїздки по територіях іноземних держав при виконанні перевезень вантажів автомобільним транспортом у міжнародному сполученні в електронній формі через Транспортний портал електронних послуг — постанова КМУ від 3 червня 2020 р. № 473. Київ. URL: <https://zakon.rada.gov.ua/laws/show/473-2020-%D0%BF#Text>

55 Проєкт оновлення парку вантажних вагонів на 2022-2028 роки. URL: <https://railexproua.com/>

56 Рочняк Ю.А. Моделі простору архітектури залізничних вокзалів. *Містобудування та територіальне планування*, 2019. Вип. 69. С. 344 – 350.

57 Русанова І.В., Склярова І.В. Транспортно-пересадочні вузли у планувальній структурі найбільшого міста. Досвід та перспективи розвитку міст України. *Проблеми розвитку найкрупніших міст України*. 2011. Вип.20. С. 259–268.

58 Синенко М.А., Ткач Ю. М. Математична модель методів активного захисту інформації. *Технічні науки та технології*. 2020. № 2 (20). С.109-115.

59 Скітер І.С., Ткаленко Н.В., Трунова О.В. Математичні методи прийняття управлінських рішень. Чернівці: ЧДІЕУ, 2011. 247с.

60 Смерічевський С., Райчева Л., Михальченко О. Проблеми і перспективи

модернізації транспортного комплексу національної економіки. *Економіка та суспільство*. 2022. № 38. URL: <https://economyandsociety.in.ua/index.php/journal/article/view/1504>

61 Соломніков І.В., Кріцин Е.В. Перспективи розвитку інфраструктури залізниць: першочергові завдання та шляхи їх вирішення. *Вісник економіки транспорту і промисловості*. 2023. № 81-82. С. 336-344

62 Стасюк О. М. Техніко-технологічна модернізація як один з пріоритетів розвитку залізничного транспорту України. *Ефективна економіка*. 2017. № 2. URL: <http://www.economy.nayka.com.ua/?op=1&z=5432>

63 Стрелко О. Г., Бердниченко Ю. А., Соловйова О. С., Кравченко О. В., Дорошенко М. М. Підвищення ефективності залізничних перевезень за рахунок модернізації об'єктів залізничного транспорту загального користування. *Вчені записки ТНУ імені В. І. Вернадського. Серія: Технічні науки*. 2021. Т. 32 (71). № 5. С. 279-285.

64 Ступінь зносу основних засобів за ВЕД «Транспорт, складське господарство, поштова та кур'єрська діяльність». URL: <https://data.gov.ua/dataset/fd9a47c8-50d9-43a8-b544-7419e28b2f35>

65 Ткач Ю.М. Моделі систем захисту інформаційної сфери держави. *Сучасна спеціальна техніка*. 2020. № 2 (61). С.59–66.

66 Ткач Ю.М. Тенденції розвитку сучасного кіберпростору та його захищеності в умовах інформаційного протиборства. *Безпека інформації*. 2020. Т.26(2).С .74–80.

67 Токмакова І. В. Забезпечення гармонійного розвитку залізничного транспорту України : монографія. Х. : УкрДУЗТ, 2015. 403 с.

68 Токмакова І. В. Антикризове управління на підприємствах залізничного транспорту. *Вісник економіки транспорту і промисловості*. 2010. № 31. С. 59-62.

69 Укрзалізниця придбає 130 нових вантажних електротягів від французької компанії «Alstom». Міністерство розвитку громад, територій та

інфраструктури України. URL: <https://mtu.gov.ua/news/32921.html>

70 Філія «Головний інформаційно-обчислювальний центр» АТ «Укрзалізниця». URL: <https://gioc.uz.gov.ua/>

71Ціль 9. Промисловість, інновації та інфраструктура. URL: <https://business.diia.gov.ua/handbook/sustainable-development-goals/cil-9-promislovist-innovacii-ta-infrastruktura>

72 Юдін О.К., Бучик С.С. Концептуальний аналіз уразливості державних інформаційних ресурсів. *Наукоємні технології. Технічні науки*. 2013. №3(19). С.299–304.

73 Чаркіна Т. Ю. Концептуальні засади забезпечення антикризового управління пасажирського комплексу залізничного транспорту. *Економіка та держава*. 2020. № 12. С. 45–49.

74 Яновська В., Медина А. Особливості економічного розвитку транспортних компаній в умовах цифровізації. *Збірник наукових праць ДУІТ. Серія «Економіка і управління»*. 2023. Вип. 53. С. 40 – 48.

75 Яновська В. П., Гарматюк Н. В. Сучасні стратегії розвитку залізничного транспорту України. *Збірник наукових праць ДУІТ. Сер.: Економіка і управління*. 2018. Вип. 42 (2). С. 55–65.

76 Deutsche Bahn створить компанію для управління цифровізацією залізничної мережі Німеччини. Центр транспортних стратегій. URL : https://cfts.org.ua/news/2019/09/26/deutsche_bahn_sozdast_kompaniyu_dlya_upravleniya_tsifrovizatsiey_zh_d_seti_germanii_55424

77 Digital Railway. networkrail.co.uk. URL: <https://www.networkrail.co.uk/running-the-railway/railway-upgrade-plan/digitalrailway/>

78 Nexxiot brings transparency to 9,000 VTG tank containers. oevz.com : URL : <https://oevz.com/en/nexxiot-brings-transparency-to-9000-vtg-tankcontainers/>

79 Prince of Wales opens CAF's first digital factory. International Journal of Railway Transport. URL <https://www.railjournal.com/fleet/prince-ofwales-opens-cafs-first-digital-factory/>

- 80 Simplifying rail freight. traigo.com. URL : <https://traigo.com/>
- 81 The future of mobility is rail. Digitale Schiene Deutschland. URL: <https://digitale-schiene-deutschland.de/en/digital-rail>
- 82 VTG introduces new digital platform. tanknewsinternational.com. URL: <https://tanknewsinternational.com/vtg-introduces-new-digital-platform/>
- 83 Методичні вказівки до виконання кваліфікаційної роботи рівня вищої освіти «другий (магістерський) рівень» усіх форм навчання / каф. «Економіки та управління виробничим і комерційним бізнесом». В. Л. Дикань, В. В. Компанієць, І. В. Токмакова, І.Л. Назаренко. Харків: УкрДУЗТ, 2019. 60 с.
- 84 Студентська навчальна звітність. Текстова частина (пояснювальна записка). Загальні вимоги до побудови, викладення та оформлення: методичний посібник з додержання вимог нормоконтролю у студентській навчальній звітності /Козар Л.М. [та ін.]; за заг. ред. Л.М. Козара. Х.: УкрДУЗТ, 2018. 54 с.

АКТ

перевірки випускної кваліфікаційної роботи на наявність ознак
академічного плагіату

Відповідно до даних сервісу Strikeplagiarism.com кваліфікаційна робота
на тему: «Антикризове управління підприємствами залізничного
транспорту»
автора: Кріцин Едуард Володимирович
(ПІБ автора повністю)

містить 9,77 % запозичень. Ознаки академічного плагіату – відсутні.

Перевірку виконала
доцент кафедри економіки та управління
виробничим і комерційним бізнесом



(підпис)

Ганна ОБРУЧ

07.12.2023 р.

АКТ

перевірки кваліфікаційної роботи магістра на наявність ознак
академічного плагіату

Відповідно до даних сервісу UNICHECK (Advego, etc) кваліфікаційна
робота «Забезпечення конкурентоспроможності підприємства шляхом зміни
економічної поведінки», автора: Орехов Максим Вікторович

(ПІБ автора повністю)

містить 3,51 % запозичень. Ознаки академічного плагіату – відсутні.

Перевірку виконала
доцент кафедри економіки та управління
виробничим і комерційним бізнесом



(підпис)

Ганна ОБРУЧ

04.12.2022 р.