Міністерство освіти і науки України
Національний університет «Полтавська політехніка імені Юрія Кондратюка»
Навчально-науковий інститут фінансів, економіки, управління та права
Кафедра менеджменту і логістики

Кваліфікаційна робота

на здобуття ступеня вищої освіти «бакалавр»
зі спеціальності 073 «Менеджмент»
на тему: «Обґрунтування стратегії цифрової безпеки організації в умовах глобальних викликів»

Виконала:
студентка групи 401-ЕМ
Костенко Софія Сергіївна_____

Керівник:
доцент кафедри менеджменту і логістики,
к.е.н., доцент Кудінова А.О. _____

Полтава – 2026

ЗМІСТ

ВСТУП

Сучасний етап розвитку національних економік характеризується тотальною цифровізацією та стрімким розгортанням концепцій Industry 4.0 та 5.0, де інформаційно-технологічний базис перетворюється на ключовий чинник забезпечення міжнародної конкурентоспроможності. Для національного промислового сектору України, який функціонує в умовах тривалого режиму воєнного стану, актуальність зазначених тенденцій набуває екстремального та безпрецедентного характеру. Вітчизняні промислові гіганти, що належать до об'єктів критичної інфраструктури, перебувають під постійним, системним тиском комбінованих (гібридних) атак, де фізичні руйнування та енергодефіцит свідомо поєднуються з високотехнологічними кібердиверсіями та актами кібершпигунства. За таких умов традиційні, реактивні підходи до захисту інформаційного периметра виявляють свою повну неспроможність, що актуалізує об'єктивну необхідність трансформації кібербезпеки з допоміжної сервісної функції IT-підтримки на наріжну складову загальної стратегії діяльності підприємства, здатну гарантувати його довгострокову операційну стійкість.

Особливої гостроти та практичної значущості процеси стратегічного реінжинірингу систем цифрового захисту набувають для підприємств вітчизняного металургійного комплексу, яскравим представником якого є ПАТ «ІНТЕРПАЙП НТЗ». Специфіка великого машинобудівного та трубного виробництва з безперервним технологічним циклом полягає в тому, що уразливість інтегрованих управлінських контурів (таких як ERP-система SAP) чи несанкціонований доступ до мереж АСУ ТП / SCADA загрожує не просто тимчасовою деградацією офісних сервісів, а аварійною зупинкою плавильних агрегатів і прокатних станів.

Відповідно, метою кваліфікаційної роботи було обрано розробку практичних рекомендацій з удосконалення стратегії цифрової безпеки ПАТ «ІНТЕРПАЙП НТЗ» в умовах глобальних викликів.

Відповідно до сформованої мети були поставленні наступні завдання:

дослідити сутність та особливості розробки стратегії діяльності організації в умовах глобальних викликів;

охарактеризувати методичні підходи до управління цифровою безпекою організації;

проаналізувати міжнародний досвід формування стратегії цифрової безпеки організації;

проаналізувати об'єкт та суб'єкт системи управління ПАТ «ІНТЕРПАЙП НТЗ»;

провести фінансово-економічний аналіз результатів господарської діяльності ПАТ «ІНТЕРПАЙП НТЗ»;

оцінити існуючу стратегію цифрової безпеки на ПАТ «ІНТЕРПАЙП НТЗ»;

удосконалити стратегію ПАТ «ІНТЕРПАЙП НТЗ» в умовах глобальних викликів;

запропонувати напрями формування стратегії цифрової безпеки ПАТ «ІНТЕРПАЙП НТЗ».

Об'єкт дослідження – процес формування стратегії на ПАТ «ІНТЕРПАЙП НТЗ».

Предмет дослідження – удосконалення стратегії цифрової безпеки ПАТ «ІНТЕРПАЙП НТЗ» в умовах глобальних викликів.

Методологічну основу кваліфікаційної роботи становить комплекс загальнонаукових та спеціальних методів, застосування яких дозволило забезпечити системність, об'єктивність та прикладну спрямованість отриманих результатів. Зокрема, у процесі дослідження було використано такі методи: системний підхід та метод теоретичного узагальнення для з'ясування сутнісного змісту цифрової трансформації, еволюції концепцій Industry 4.0/5.0 та обґрунтування ролі кіберзахисту як базового детермінанта операційної стійкості сучасного підприємства; методи класифікації, систематизації та логічного аналізу (індукції та дедукції) під час структурування дев'ятиетапного життєвого циклу стратегічного управління цифровою безпекою та виокремлення

тривимірної архітектури захисту (внутрішнього, зовнішнього та системного контурів); методи фінансово-економічного аналізу, порівняння та групування при дослідженні динаміки техніко-економічних показників діяльності ПАТ «ІНТЕРПАЙП НТЗ», оцінці структури його капіталомістких активів та ідентифікації критичних цифрових ризиків холдингу; монографічний та дескриптивний методи під час дослідження кращих світових практик та міжнародних стандартів комплаєнсу (зокрема, ISO/IEC 27001) з метою їх адаптації до умов вітчизняного металургійного сектору; методи табличного оформлення та графічного зображення даних для наочної візуалізації елементної структури безпекового інструментарію підприємства.Основні положення кваліфікаційної роботи і результати дослідження оприлюднені на конференціях:

Костенко С.С., Кудінова А.О. Особливості управління цифровою безпекою організації в сучасних умовах господарювання. *Матеріали X Міжнародної науково-практичної конференції «Економічна безпека: держава, регіон, підприємство», 13 травня 2026 р.* Полтава: Національний університет імені Юрія Кондратюка. С. 109-110.

Костенко С.С., Кудінова А.О. Міжнародний досвід формування стратегії цифрової безпеки організації. *Матеріали IV Міжнародної науково-практичної Інтернет-конференції: Сталий розвиток: виклики та загрози в умовах сучасних реалій, 04 червня 2026 р.* Полтава: Національний університет імені Юрія Кондратюка. С. 266-267.

Кваліфікаційна робота складається із вступу, трьох розділів (8 підрозділів), загальних висновків, списку використаних джерел, додатків. Загальний обсяг роботи становить 64 сторнки і включає 10 таблиць, 14 рисунків, список використаних джерел – 57 найменувань, 3 додатки.

РОЗДІЛ 1
ТЕОРЕТИЧНІ ОСНОВИ ОБҐРУНТУВАННЯ СТРАТЕГІЇ ЦИФРОВОЇ БЕЗПЕКИ ОРГАНІЗАЦІЇ В УМОВАХ ГЛОБАЛЬНИХ ВИКЛИКІВ

1.1. Сутність та особливості розробки стратегії діяльності організації в умовах глобальних викликів

Будь-яка вітчизняна організація здійснює свою діяльність під впливом глобальних викликів від військових конфліктів та політичної нестабільності до системних економічних криз. Таке мінливе зовнішнє середовище вимагає від суб’єктів господарювання перегляду підходів до формування системи стратегічного управління. Тобто мають бути розроблені адаптивні стратегії, які мають забезпечувати сталий розвиток, активну протидію кіберзагрозам та підвищення конкурентоспроможності [1].

Звичайно, що відбувається постійний еволюційний процес управлінських підходів. Якщо раніше увага зосереджувалася лише на операційному та поточному управлінні, коли вирішувалися лише звичайні завдання, то станом на сьогодні навіть в тих умовах, що склалися, підвищується значення і роль стратегічного управління.

Звичайно, що відмінності в операційному та стратегічному управлінні впливають на процес прийняття рішень, розробку планів та коригування завдань. Проте сьогодні, в епоху цифрової трансформації, вони мають виступати єдиною системою, яка забезпечуватиме постійний розвиток, пошук альтернативних варіантів виходу з кризових процесів.

Станом на сьогодні під час військової агресії росії, організації постійно зіштовхуються з різними ризиками та загрозами, що призводять до втрати ланцюгів постачання, змушують шукати нові логістичні маршрути, шукати можливості поповнення кадрового складу. В таких умовах організація, яка орієнтується на оперативне чи поточне планування, не здатна прорахувати

наперед усі можливі варіанти розвитку подій. Що і актуалізує роль стратегічного управління, як одного з ключових факторів максимізації прибутковості, досягнення місії діяльності, забезпечення життєздатності організації у довгостроковій перспективі.

Одним із глобальних викликів, які підвищують роль стратегічного планування, виступає цифрова трансформація бізнесу. Вона має бути імплементована у загальну стратегію діяльності організації. Саме цифрова стійкість стає тим критичним ресурсом, який дозволяє організації швидко адаптуватися до змін у внутрішньому та зовнішньому середовищі, а також забезпечувати безперервність бізнес-процесів [2].

Дослідження наукової літератури дозволило визначити, що стратегія організації являє собою процес побудови плану розвитку на основі чітко визначених цілей і завдань, узгодженості наявних ресурсів та можливостей з умовами середовища [3]. Розробка такої стратегії в умовах глобальних викликів має враховувати наступні принципи:

орієнтація на глобальні цілі організації (матеріальні, соціальні, монетарні);

розробка множинності альтернатив розвитку;

адаптивність;

безперервність;

постійний моніторинг змін та коригування цілі, завдань;

комплексність та системність;

цифровізація бізнес-процесів;

гнучкість.

Застосування такого комплексного та системного підходу дозволяє організації мінімізувати негативний вплив ризиків та загроз, забезпечити здатність до швидкого відновлення у відповідь на виклики глобалізованого світу.

При обґрунтуванні стратегії в умовах глобальних викликів слід розуміти її ключові ознаки, а також різновиди [4]:

за масштабом – генеральна стратегія та допоміжні стратегії;

за напрямами діяльності та видами ресурсів – маркетингові, фінансові, інвестиційні стратегії тощо;

за темпами розвитку – стратегія прискореного зростання, обмеженого зростання, збереження становища або скорочення чи реорганізація у кризових умовах;

за способами забезпечення розвитку – стратегії концентрованого, диверсифікованого або інтегрованого розвитку.

Звичайно, процес формування стратегії діяльності організації є поетапним. В першу чергу розробка стратегії починається з усвідомлення місії підприємства – його генеральної глобальної цілі. Після формулювання місії та візії діяльності організації, будуються плани на всіх рівнях:

при генеральному плануванні зазначаються загальні цілі діяльності;

при стратегічному плануванні зазначаються вже більш конкретизовані завдання у відповідності до обраних цілей та місії;

при тактичному плануванні визначаються конкретні чіткі завдання для кожного підрозділу та служби в короткому часовому інтервалі;

при операційному плануванні деталізовані завдання доносяться виконавцям на своїх робочих місцях [5].

Таким чином, стратегічне управління є безперервним процесом адаптації організації до викликів середовища. Саме здатність менеджменту вчасно ідентифікувати зовнішні і внутрішні загрози, розробляти альтернативні шляхи упередження їх появи та зменшення негативного впливу стає фундаментом стійкості сучасної організації [6].

Як було визначено у ході дослідження, формування стратегії є складним багатоетапним процесом, вимагає реалізації ключових функцій та принципів менеджменту. Для глибшого розуміння механізму стратегічного управління організацією доцільно розглянути основні функції стратегічного управління та їх характеристики (табл. 1.1):

Таблиця 1.1 – Основні функції стратегічного управління розвитком підприємства

Функції	Характеристика
Аналіз ситуації	Вивчення внутрішнього та зовнішнього середовища на основі проведення SWOT та PEST-аналізу
Формулювання цілей	Визначення стратегічних цілей, розробка планів і пошук ресурсного забезпечення їх досягнення.
Вибір стратегічних альтернатив	Вибір найбільш оптимального варіанту розвитку із альтернатив, що відповідає можливостям організації.
Реалізація стратегії	Впровадження стратегії на всіх рівнях із чітким розподілом обов'язків, постановкою завдань підрозділам.
Моніторинг та оцінка результатів	Моніторинг результатів реалізації стратегії для вчасного виявлення відхилень від наміченого плану.
Коригування стратегії у відповідності до змін	Адаптація обраної стратегії до змін у зовнішньому середовищі для підтримки ефективності та конкурентоспроможності підприємства.

Джерело: побудовано на основі [7-10]

Дотримання вищезазначених функцій та принципів дозволяє вищому керівництву організації розробити стратегію, яка не лише забезпечить підвищення рівня конкурентоспроможності, а й гарантуватиме досягнення стратегічних цілей у довгостроковій перспективі. Узагальнюючи викладене, на основі системного аналізу теоретичних підходів до стратегічного менеджменту нами пропонується наступна концептуальна схема етапів формування стратегії розвитку організації в умовах глобальних викликів (рисунок 1.1).

Запропонована схема орієнтована на визначені раніше принципи та функції стратегічного управління. Враховує взаємозв'язок між системами планування і підтверджує, що стратегічне управління є цілісним процесом, де кожен етап від усвідомлення місії до моніторингу результатів має критичне значення для адаптації організації до глобальних викликів.

Застосування такого підходу в організаціях створить необхідний фундамент для подальшого обґрунтування розробки стратегії цифрової безпеки, яка виступає основою захищеності та стійкості сучасної інформаційно-орієнтованої організації [11].

Рисунок 1.1 – Концептуальна схема етапів формування стратегії розвитку підприємства в умовах глобальних викликів

Джерело: сформовано автором на основі [12]

У висновку можна зазначити, що перехід від оперативного до стратегічного планування дозволить організації не лише формувати напрямки протидії до виникнення кризових явищ, але й пришвидшити процес адаптації до викликів середовища на основі розроблення альтернативних варіантів розвитку та безперервного оновлення стратегічних цілей. Розробка такої стратегії має бути цілісним процесом, який конкретизується на рівні тактичних та операційних планів, забезпечує на всіх рівнях реалізацію місії організації та збільшення конкурентних переваг. При цьому варто при формуванні майбутньої стратегії чи коригуванні існуючої слід визначати також приймати до уваги рівень цифрової безпеки, яка виступає складовою системи економічного та інформаційного захисту організації.

1.2. Характеристика та методичні підходи до управління цифровою безпекою організації

Сучасні підходи до стратегічного планування вимагають враховувати вплив кіберзагроз на діяльність організації, забезпечуючи захист цифрових активів на всіх рівнях управління. Стабільність функціонування будь-якої організації станом на сьогодні залежить не тільки від виробничого циклу, кадрового потенціалу, наявності необхідних ресурсів для забезпечення операційної діяльності, але й від вміння захистити всі бізнес-процеси та ресурси від зовнішнього втручання через інформаційні системи [14].

Відповідно формування системи управління цифровою безпекою організації має бути направлена на захист:

інформаційних активів організації (інтелектуальної власності на програми, винаходи, технічні рішення тощо);

персональні дані працівників та клієнтів;

створену цифрову інфраструктуру взаємодії між відділами, підрозділами та службами при обміні інформацією з метою забезпечення безперервності бізнес-процесів.

Проблема побудови якісної системи управління цифровою безпекою організації якраз і проявляється в тому, що наявний критичний розрив між наявністю сучасних технічних інструментів захисту та відсутністю їх впровадження на всіх рівнях управління. Тобто усі технічні рішення або впроваджуються фрагментарно, тобто відділ ІТ має доступ до конкретного програмного забезпечення, а інші відділи чи служби мають або частковий доступ, або відсутні навички користування макросами та налаштуваннями [15].

З такої позиції на перший план виступає впровадження проактивного управління цифровою безпекою організації, яка передбачає не виправлення помилок чи пошук рішень інформаційного захисту після їх появи, а створення упереджувального надійного контуру безпеки на всіх рівнях [16].

Тобто вище керівництво визначає стратегічний вектор діяльності організації, розробляє політику взаємодії на всіх рівнях, ІТ-служби забезпечують впровадження технічних рішень захисту, а звичайні працівники реалізують на своїх рівнях реалізацію цих заходів. Звичайно, що після практичної підготовки та пояснення алгоритмів роботи різних інформаційних систем та рішень.

В мовах глобальних викликів при формуванні системи цифрової безпеки організації слід дотримуватись наступних принципів кіберзахисту:

принцип конфіденційності, коли доступ є лише в операторів, він надається на робочому місці (працівник не має доступу до файлів чи програм віддалено з дому);

принцип цілісності, коли все програмне забезпечення утворює єдину систему кіберзахисту, яка забезпечує точність даних, виявляє маніпуляції з даними і запобігає їх деструктивному впливу на бізнес-процеси;

принцип доступності полягає в тому, що мають усі працівники можливість доступу до своїх даних, обміну між відділами, а також подачі запитів на перегляд різних системних збоїв чи невідповідностей [17].

принцип відповідальності, який передбачає формування відповідної культури кібергігієни, навчання персоналу протидії кібератакам різних типів та видів;

принцип адаптивності, який полягає в тому, що при появі нових вразливостей чи викликів середовища, система захисту швидко шукає шляхи впровадження нових інновацій з метою забезпечення стійкості діяльності організації [18].

Саме тому на основі вищезазначеного пропонуються наступні ключові елементи цифрової безпеки, які слід впроваджувати в організації при побудові надійної системи інформаційного захисту (таблиця 1.2).

Таблиця 1.2 – Ключові елементи цифрової безпеки організації

Елемент	Сутнісна характеристика
Захист програмного забезпечення	Розробка певних процедур, інструментів і практичних порад для забезпечення встановленого програмного забезпечення від зовнішнього втручання
Хмарне середовище	Створення хмарного середовища, де зберігаються усі важливі файли, документи, програми
Швидке аварійне відновлення	Пошук програм, інструментів, що дозволять забезпечити швидке відновлення інформаційної системи при атаках та інших кризових ситуаціях
Реагування на появу інцидентів	Побудова алгоритму реагування на появу кібератак, порушення безпеки даних, а також швидке усунення негативного впливу
Захист цифрової інфраструктури	Постійне оновлення системи захисту цифрової інфраструктури, апаратного та програмного забезпечення
Управління вразливостями	Пошук потенційних вразливостей, формування системи захисту від їх появи, слідкування за появою таких атак серед організацій, що займаються подібною діяльністю для опрацювання досвіду

Джерело: сформовано автором на основі [19-22]

Саме тому забезпечення безперервності процесу впровадження та оновлення цифрових рішень є критично важливим аспектом сучасного управління, що передбачає не лише регулярну модернізацію програмних продуктів та інформаційних систем, а й системне планування навчання персоналу. Формування нових цифрових навичок та компетенцій є необхідною умовою для підвищення якості роботи працівників і загальної результативності організації [23].

У широкому розумінні цифрова безпека виступає невід'ємною складовою економічної безпеки підприємства. Вона спрямована на комплексне впровадження заходів, що гарантують конфіденційність, доступність та цілісність інформаційних ресурсів, а також їхній захист від несанкціонованого впливу, вірусних атак та інших кіберзагроз. Взаємозв'язок ключових елементів управління системою економічної безпеки на основі інноваційних цифрових технологій відображено на рис. 1.2.

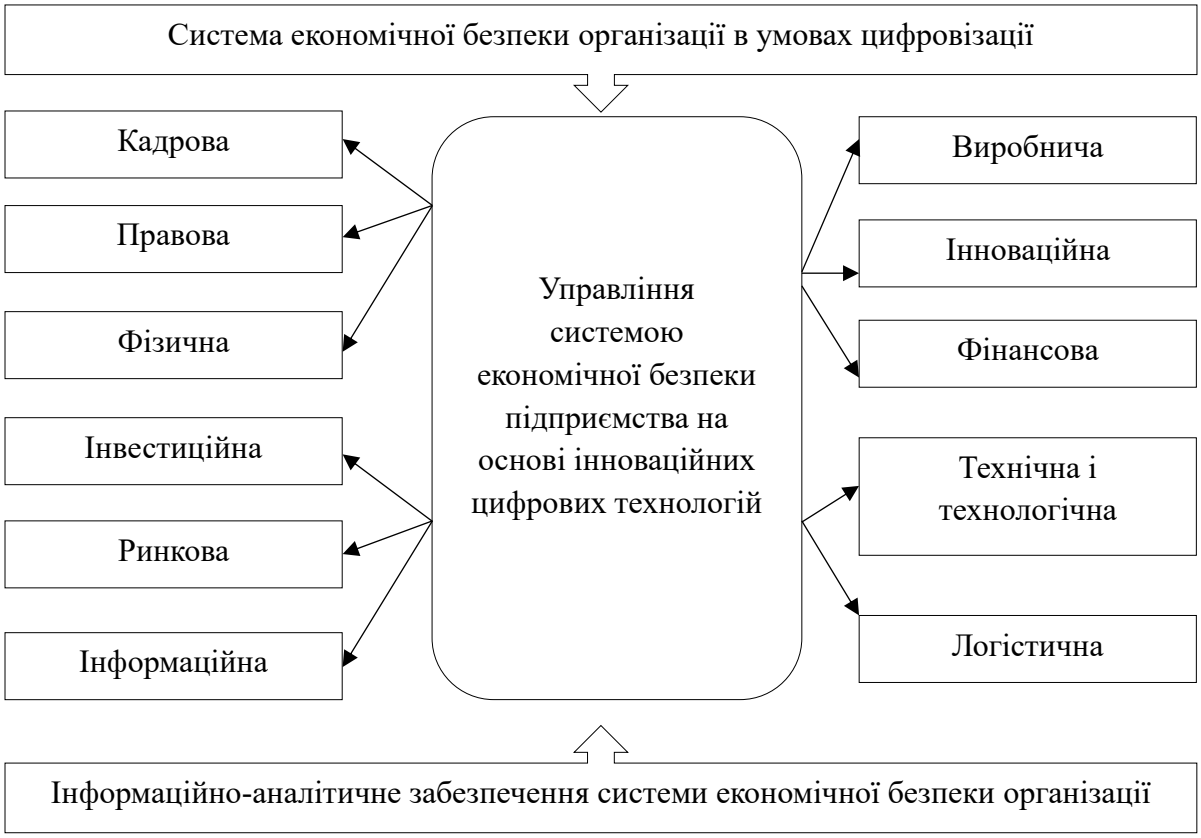

Рисунок 1.2 – Складові управління системою економічної безпеки підприємства на основі інноваційних цифрових технологій

Джерело: сформовано автором на основі [24-33]

Таким чином, синергічна взаємодія технологічних інновацій, безперервного розвитку людського капіталу та адаптивної корпоративної культури, що в сукупності забезпечує стратегічну стійкість підприємства перед обличчям глобальних викликів та підвищує рівень цифрового захисту організації.

Саме тому для формування сучасної системи цифрової безпеки організації має відбуватися за наступними етапами (рисунок 1.3):

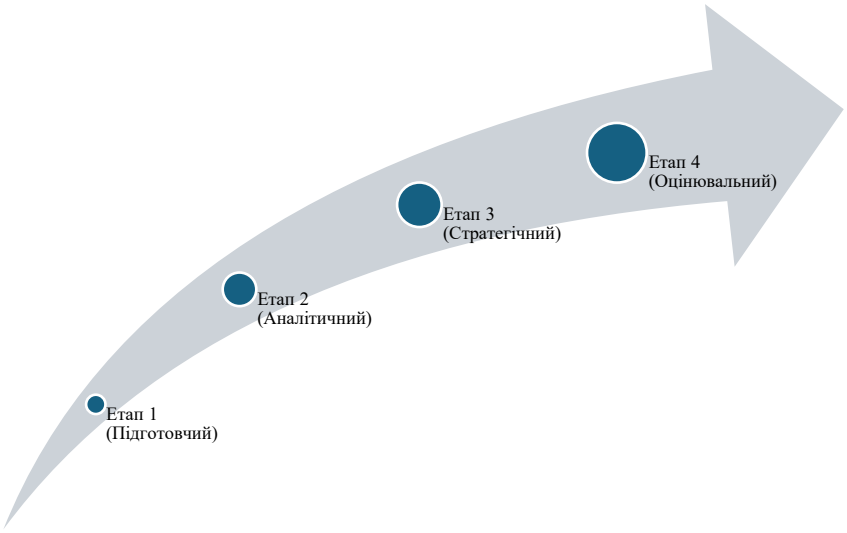

Рисунок 1.3 – Етапи управління цифровою безпекою організації

Джерело: авторська розробка

Етап 1 (Підготовчий) полягає у здійсненні моніторингу, виявленні та оцінці даних про стан і динаміку внутрішнього та зовнішнього середовищ підприємства з акцентом на рівень цифровізації та наявні IT-ресурси.

Етап 2 (Аналітичний) передбачає визначення якісних параметрів використання консолідованих ресурсів та обчислення кількісних показників економічної безпеки, зокрема її інформаційно-цифрової складової.

Етап 3 (Стратегічний) передбачає розробку та обґрунтування комплексних заходів щодо впровадження та вдосконалення системи управління економічною безпекою на основі обраних цифрових моделей.

Етап 4 (Оцінювальний) направлений на діагностику фактичної ефективності впроваджених заходів, аудит захищеності та визначення пріоритетних напрямів подальшого покращення системи.

Використання такого структурованого методичного підходу дозволяє своєчасно ідентифікувати загрози фінансовій та інформаційній стабільності підприємства, застосовуючи превентивні заходи для мінімізації їхнього деструктивного впливу на виробничо-економічну діяльність у глобалізованому цифровому просторі».

Підсумовуючи, слід зазначити, що сучасні інформаційні системи та технології є життєво важливим фундаментом забезпечення економічної безпеки підприємства в умовах цифрової економіки. Вони надають менеджменту необхідний інструментарій для навігації у складному бізнес-середовищі, збереження конкурентоспроможності та проактивного захисту від потенційних ризиків. Проте їх ефективна імплементація потребує стратегічного підходу, фокусу на кібербезпеці та безперервного процесу навчання й адаптації персоналу [32].

Для досягнення високого рівня стійкості підприємство повинно інтегрувати інноваційні технології, такі як штучний інтелект, машинне навчання та аналітика великих даних (Big Data), що дозволяє прогнозувати ринкові тенденції, оптимізувати операційну діяльність та випереджати конкурентів.

У межах даного дослідження пропонуємо формування цифрової екосистеми проводити як стратегічну складову економічної безпеки підприємства. Така екосистема має забезпечувати синергію новітніх технологій (AI, Cloud Computing, Predictive Modeling, IIoT) та профільних інформаційних систем (ERP, HRM, MES, CRM, SCM тощо) з метою створення єдиного контуру збору, зберігання та інтелектуальної обробки даних [33].

Функціонування такої екосистеми сприятиме:

активному виявленню та аналізу латентних загроз;

точній оцінці впливу ризиків на функціонування підприємства в умовах цифровізації;

прийняттю обґрунтованих управлінських рішень щодо мінімізації управлінських, інформаційних, кадрових та технологічних ризиків.

Саме такий екосистемний підхід дозволить забезпечити комплексну трансформацію системи безпеки та підвищити загальний рівень економічної стійкості суб’єкта господарювання в умовах глобальних цифрових трансформацій.

1.3. Міжнародний досвід формування стратегії цифрової безпеки організації

У сучасній світовій практиці забезпечення сталого розвитку та конкурентоспроможності суб'єктів господарювання безпосередньо корелює з рівнем їхньої технологічної адаптивності. Сьогодні ключовими чинниками трансформації світової економіки виступають системи штучного інтелекту (AI), Інтернет речей (IoT), хмарні та суперкомп'ютерні обчислення, нейронні мережі та квантові технології. Саме під впливом цих чинників змінюється характер економічної кон'юнктури, що вимагає переосмислення механізмів управління конкурентними перевагами. Динамічна здатність організацій успішно функціонувати у складному конкурентному середовищі тепер прямо залежить від їхньої спроможності інтегрувати інтелектуальний потенціал у захищену цифрову екосистему.

Цифрова інфраструктура, що базується на аналітиці великих даних (Big Data), блокчейні, хмарних обчисленнях та технологіях цифрових двійників, надає організаціям інструменти для швидкого масштабування та адаптації. Проте, стираючи межі між традиційним менеджментом та високими технологіями, цифрова трансформація одночасно створює нові управлінські виклики. Міжнародний досвід свідчить, що успішна стратегія цифрової безпеки організації повинна базуватися не на ізольованому захисті інформації, а на створенні комплексного безпекового середовища, де технологічні інновації, юридичні регламенти та корпоративні цінності формують єдину архітектуру стійкості до зовнішніх впливів [34].

Еволюція бізнес-стратегій у період глобальної діджиталізації ознаменувала фундаментальний відхід від традиційних моделей менеджменту. Якщо класичні підходи базувалися переважно на оптимізації внутрішніх операційних процесів, нарощуванні масштабу за рахунок фізичних активів та встановленні ринкового домінування через контроль каналів розподілу, то поява цифрових технологій зумовила зміну парадигми формування стратегії розвитку організації (рис. 1.4).

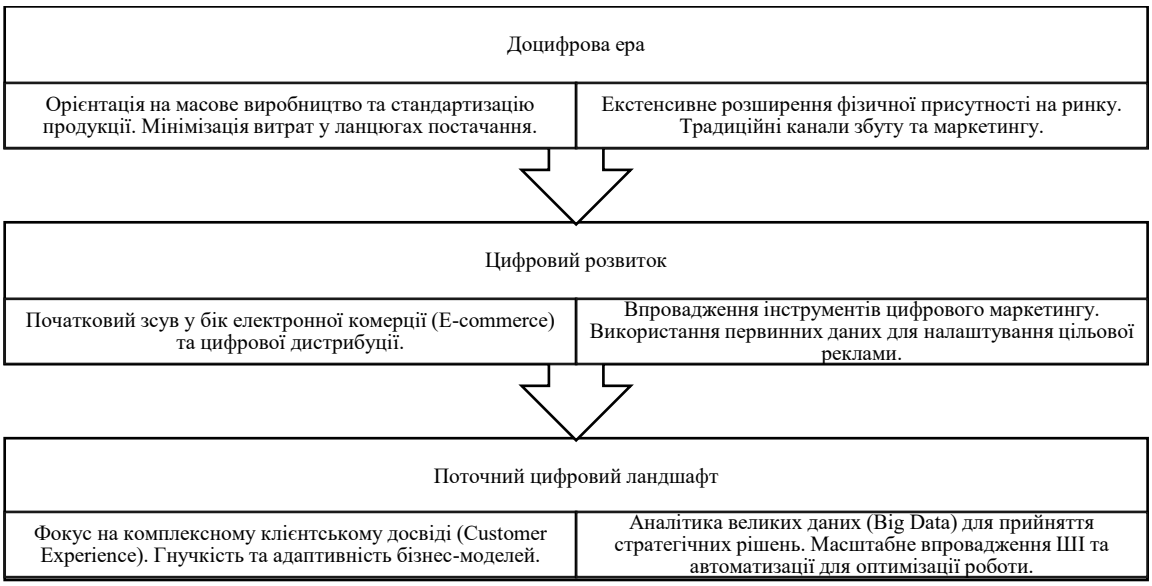

Рисунок 1.4 – Зміна парадигми формування стратегії розвитку організації в умовах цифрової трансформації

Джерело: авторська розробка

Традиційні бізнес-моделі, що ігнорують цифрові виклики, стикаються з експоненційним зростанням ризиків з боку «digital-native» конкурентів. Цифрова трансформація відкриває безпрецедентні можливості для залучення клієнтів та оптимізації вартості, оскільки корпоративний фокус зміщується на конвергенцію фізичних продуктів у цифрові формати [35]. Така трансформація не лише модернізує робочі процеси, а й створює якісно нові конкурентні переваги, підвищуючи організаційну стійкість та здатність генерувати додаткову цінність у волатильному середовищі.

Вирішальним фактором виживання на сучасному глобальному ринку стає здатність організації інтегрувати свої бізнес-практики в економіку технологічних платформ. Світовий досвід таких технологічних гігантів, як Google, Amazon, Meta (Facebook), Apple, а також успіх платформних рішень Uber, Airbnb та Alibaba наочно демонструють, що масштабування успіху сьогодні неможливе без формування глобальної цифрової екосистеми. Ці компанії встановили міжнародні стандарти цифрової стратегії, де дані виступають основним стратегічним активом, а мережеві ефекти – головним механізмом зростання ринкової капіталізації [36].

У міжнародній практиці управління цифровим розвитком на рівні окремих суб'єктів господарювання домінує трирівневий алгоритм імплементації цифрових трансформацій (рис. 1.5), що дозволяє мінімізувати ризики та забезпечити стратегічну відповідність інновацій бізнес-цілям.

Рисунок 1.5 – Етапи діджиталізації бізнес-процесів організації

Джерело: авторська розробка

Перший етап (діагностико-стратегічний) фокусується на комплексному аналізі поточної діяльності організації та розробці цільової стратегії. На цьому етапі критичне значення має аудит усіх бізнес-процесів та стратегічних активів для оцінки ефективності роботи підрозділів, виробничих потужностей, а також внутрішніх і зовнішніх комунікацій. Фундаментальною передумовою успіху тут виступає детермінація конкретних, вимірних цілей та розробка дорожньої карти цифрового розвитку [37].

Другий етап (технологічно-операційний) базується на безпосередній інтеграції цифрових рішень. Міжнародний досвід свідчить, що цей етап вимагає значних часових ресурсів для апробації (тестування) технологій, усунення технічних колізій та інструктування персоналу і клієнтів. Формування нових компетенцій у користувачів є запорукою того, що цифрові інструменти будуть використовуватись максимально ефективно.

Третій етап (контрольно-результативний) передбачає отримання результатів, їх моніторинг та оцінку ефективності впроваджених заходів відповідно до встановлених KPI [38-40].

Узагальнення міжнародного досвіду дозволяє виокремити стратегічні пріоритети цифровізації діяльності організації:

конкурентне позиціонування через формулювання нових ціннісних пропозицій;

модернізація інформаційних потоків та комунікаційних ланцюгів у межах інтегрованого цифрового простору;

системне оновлення інформаційної інфраструктури;

впровадження інтелектуальних систем підтримки прийняття рішень для окремих структурних підрозділів;

створення спеціалізованих внутрішніх структур для адміністрування інформаційних послуг;

розвиток техніко-технологічної бази з метою радикального підвищення якості продукції та конкурентоспроможності підприємства на глобальних ринках [41].

Застосування системного підходу, який заснований на кращих міжнародних практиках і методиках, дозволить організації швидше адаптуватися до мінливого середовища. Тим паче, що світовий досвід підтверджує необхідність застосування проактивного управління на основі цифрової екосистеми як ключового елемента стратегічної безпеки організації.

Успіх цифрової трансформації організації безпосередньо залежить від рівня його технологічної зрілості. Сучасні підприємства, що є передовими у процесі цифрової трансформації, фокусуються на комплексній інтеграції Інтернету речей (IoT), кіберфізичних систем, аналітики великих даних (Big Data) та хмарних обчислень. Впровадження передової робототехніки, адитивних технологій (3D-друк) та інших інноваційних елементів дозволяє таким компаніям (наприклад, Google, Amazon, Microsoft, Siemens, Toyota тощо) вдосконалювати бізнес-процеси з використанням якісно нових цифрових рішень [42].

Аналіз міжнародної практики цифрового розвитку дозволяє класифікувати сучасні стратегічні підходи, що застосовуються відомими компаніями, розділивши їх на традиційні (процесно-орієнтовані) та людиноцентричні (командно-орієнтовані).

Традиційна модель стратегічного управління базується на класичній детермінованій схемі: «цілі → шляхи → засоби → результат». Такий підхід виступає дієвим інструментом посилення ключових компетенцій організації, проте в умовах цифрової економіки він часто стає фактором обмеження організаційної гнучкості. Фокусування менеджменту виключно на подоланні масштабних криз нерідко призводить до ігнорування поступових, але безперервних інкрементальних поліпшень процесів, які є критичними для підтримки технологічного лідерства [43].

Водночас інтенсивний НТР, глобалізаційні процеси та виклики створили тренд, коли міжнародні компанії все частіше інтегрують у свої стратегії людиноцентричну парадигму цифрової безпеки. Така стратегія передбачає, що цифрова стійкість організації залежить не лише від досконалості алгоритмів, а й від рівня адаптивності та підготовленості команди до змін, сформованої корпоративної культури. У контексті застосування вітчизняними компаніями міжнародного досвіду це означає, що найбільш успішними стають ті стратегії цифрової безпеки, які поєднують надійність технічних засобів захисту із високим рівнем залученості та обізнаності персоналу організації (рисунок 1.6).

Узагальнення міжнародного досвіду цифрової трансформації дозволяє нам виокремити чотири напрями цифрових стратегій, які спрямовані на максимізацію цінності продукту та зміцнення ринкових позицій:

Діджиталізація продуктів та операційних процесів. Ця стратегія орієнтована на комплексну автоматизацію виробничих циклів, впровадження робототехніки та технологій Інтернету речей (IoT). Ключовим аспектом тут є використання передових методів обробки великих масивів даних (Big Data Analytics) для моніторингу якості в реальному часі та радикальної оптимізації інженерних і логістичних процесів [44].

Інтелектуальна інтеграція та дизайн. Напрям фокусується на архітектурній складності продукту та його відповідності запитам споживача. Цифрові інвестиції спрямовуються на високотехнологічне моделювання (зокрема оцифрування аеро- та гідродинамічних характеристик), що дозволяє через

інтелектуальну інтеграцію розробляти продукти з глибоким розумінням специфічних вподобань цільової аудиторії.

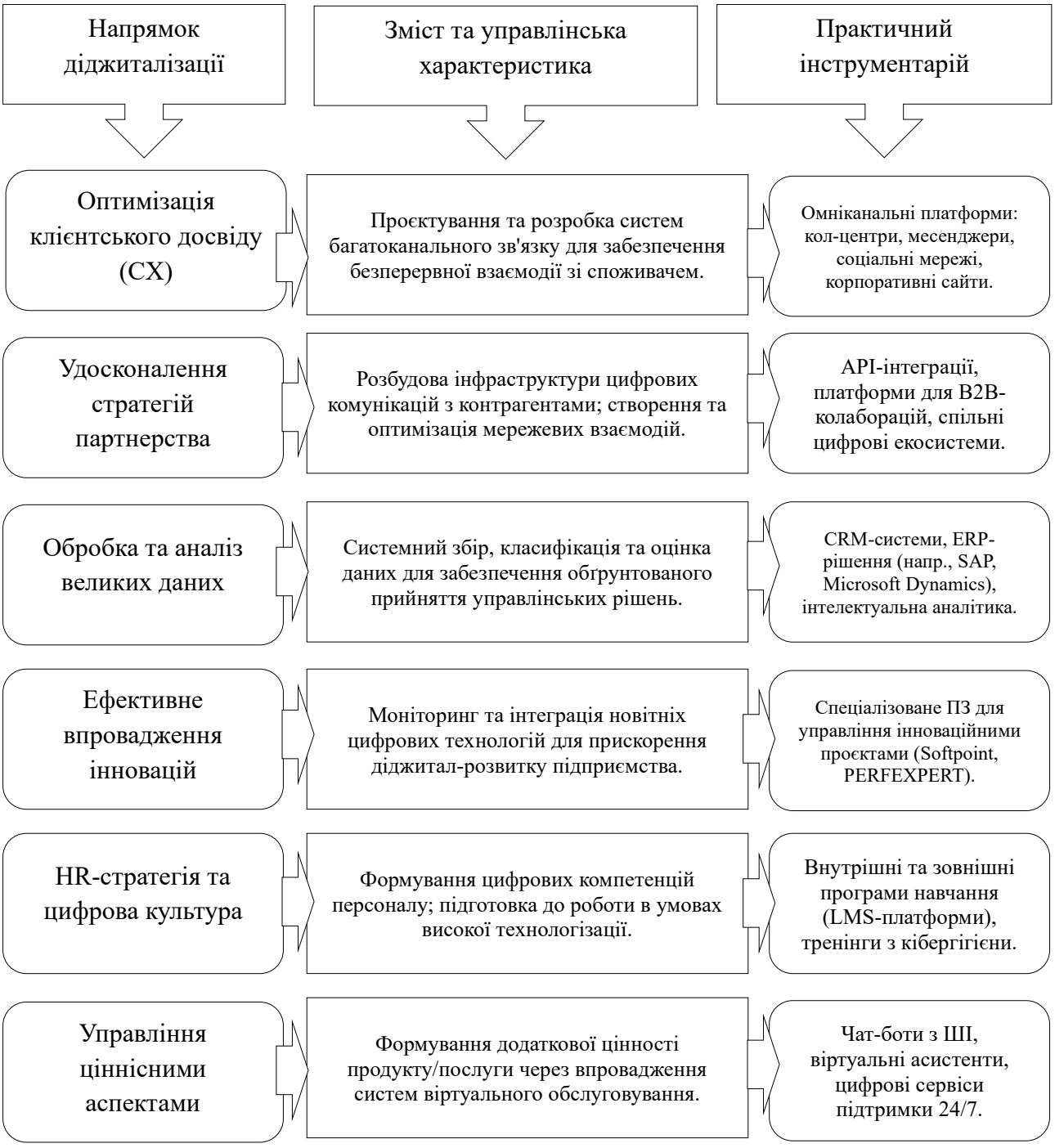

Рисунок 1.6 – Стратегічні напрямки діджиталізації бізнес-процесів та їх характеристика

Джерело: розроблено автором на основі [46-50]

Клієнтська зацікавленість. Стратегія базується на побудові позитивного клієнтського досвіду (Customer Experience, CX), що передбачає збір та аналіз персоналізованих даних про поведінку споживачів, впровадження гнучких механізмів стимулювання та забезпечення безперервної взаємодії через багатоканальні платформи (веб-сайти, соціальні мережі, мобільні додатки) [45].

Формування багатогранних цифрових екосистем. Цей найбільш прогресивний напрям ґрунтується на глибокій інтерактивній колаборації між клієнтами, розробниками та діловими партнерами. Метою є створення мережевих платформ, де додана цінність генерується не лише виробником, а й усіма учасниками екосистеми.

Таким чином, міжнародний досвід свідчить, що успіх стратегії цифрової безпеки та розвитку безпосередньо залежить від здатності менеджменту інтегрувати технології ШІ, великих даних та автоматизації в єдину адаптивну систему, орієнтовану на клієнтський досвід [51-53].

Отже, у ході дослідження встановлено, що в умовах масштабної діджиталізації цифрова трансформація перетворилася з допоміжного інструментарію на фундаментальний рушій бізнес-успіху та конкурентоспроможності. Обґрунтовано, що для українського бізнесу цифровізація є ключовим інструментом підвищення економічної стабільності.

Висновки до розділу 1

Дослідження теоретичних основ стратегії цифрової безпеки організації в умовах глобальних викликів дало можливість сформувати наступні висновки:

1. Визначено, що перехід від оперативного до стратегічного підходу дозволяє організації не лише адаптуватися до поточних криз, а й системно формувати ресурси для збереження конкурентоспроможності, орієнтуючись на багатоваріантність розвитку та безперервність оновлення стратегічних цілей. Обґрунтування стратегії стає цілісним процесом, де усвідомлення місії та ідентифікація ключових факторів успіху створюють основу для прийняття зважених рішень у межах обраного курсу розвитку.

2. Доведено, що сучасні інформаційні системи та технології є життєво важливим фундаментом забезпечення економічної безпеки підприємства в умовах цифрової економіки. Вони надають менеджменту необхідний інструментарій для навігації у складному бізнес-середовищі, збереження конкурентоспроможності та проактивного захисту від потенційних ризиків. Проте їх ефективна імплементація потребує стратегічного підходу, фокусу на кібербезпеці та безперервного процесу навчання й адаптації персоналу.

3. Встановлено, що в умовах масштабної діджиталізації цифрова трансформація перетворилася з допоміжного інструментарію на фундаментальний рушій бізнес-успіху та конкурентоспроможності. Вона системно впливає на архітектуру бізнес-моделей, ефективність маркетингових комунікацій, оптимізацію ресурсів та дозволяє досягати ефекту масштабу. Компанії, що ігнорують ці зміни, стикаються з критичними ризиками втрати ринкових позицій. Обґрунтовано, що для українського бізнесу цифровізація є ключовим інструментом підвищення економічної стабільності. Попри обмежені ресурси, впровадження базових елементів кіберзахисту (шифрування, MFA, хмарні сервіси) та автоматизація обліку дозволяють суттєво мінімізувати ризики та підвищити прозорість управління.

РОЗДІЛ 2
АНАЛІЗ ПРОЦЕСУ ФОРМУВАННЯ СТРАТЕГІЇ ЦИФРОВОЇ БЕЗПЕКИ НА ПАТ «ІНТЕРПАЙП НТЗ»

2.1. Аналіз об’єкта та суб’єкта системи управління ПАТ «ІНТЕРПАЙП НТЗ»

ПАТ «ІНТЕРПАЙП НТЗ» здійснює свою діяльність у місті Дніпрі, є провідним вітчизняним виробником залізничної продукції та входить до INTERPIPE HOLDINGS PLC. Підприємство спеціалізується на випуску коліс, бандажів, осей і колісних пар для вантажного, пасажирського та локомотивного рухомого складу. Виробнича структура товариства включає два основні підрозділи:

колесопрокатний цех, в якому функціонують колесопрокатна та кільцебандажна лінії. Також є дільниці з термообробки та фінішних операцій, які укомплектовані високотехнологічними верстатами Knuth, Hegenscheidt та Sermu Intermato для повнопрофільної обробки;

цех із виробництва осей та колісних пар. Цех оснащений новітнім токарним і фрезерним обладнанням для чистової обробки, пресом для напресовування, а також автоматизованою фарбувальною лінією для готових вузлів. Контроль якості здійснюється у власній випробувальній лабораторії із застосуванням сучасних методів тестування відповідно до міжнародних стандартів. Сировинну базу для виробництва продукції забезпечує інноваційний електросталеплавильний комплекс «ІНТЕРПАЙП СТАЛЬ».

Товариство має сучасний виробничий комплекс, що включає наступні лінії:

лінію виробництва, механічної обробки та неруйнівного контролю;

колісопрокатну лінію;

кільцебандажну лінію;

лінію складання колісних пар.

Продукція ПАТ «ІНТЕРПАЙП НТЗ»: суцільнокатані залізничні колеса для локомотивів, вантажних і пасажирських вагонів, колеса для вагонів метро, залізничні осі, колісні пари конкурентоспроможні не лише на ринку України, але й світу. Підприємство має співробітництво з відомими компаніями з Австрії, Болгарії, Чехії, Данії, Фінляндії, Франції, Німеччини, Греції, Норвегії, Швеції, Швейцарії, Словенії та Польщі (рисунок 2.1).

Рисунок 2.1 – Компанії-партнери ПАТ «ІНТЕРПАЙП НТЗ»

Для розуміння особливостей функціонування підприємства слід дослідити об’єкт та суб’єкт управління. Об’єктом управління ПАТ «ІНТЕРПАЙП НТЗ» виступає цілісний виробничо-господарський комплекс, який займається виробництвом сталевих труб і залізничної продукції під брендом KLW.

Суб’єктом управління ПАТ «ІНТЕРПАЙП НТЗ» є збори акціонерів. Структура діяльності публічного акціонерного товариства включає корпоративні та виконавчі органи, які працюють для забезпечення стратегічної стійкості, операційної ефективності та економічної безпеки підприємства (рисунок 2.2).

Згідно зі статутом ПАТ «ІНТЕРПАЙП НТЗ», система управління структурована на такі рівні:

загальні збори акціонерів, які є найвищим органом управління. Вони приймають стратегічні рішення щодо розподілу прибутку, зміни капіталу та затвердження річних звітів;

наглядова рада – відповідає за захист прав акціонерів і контроль за діяльністю Правління. У межах Наглядової ради діють комітети, зокрема, з питань аудиту та ризиків, що критично важливо для моніторингу цифрових і фінансових загроз;

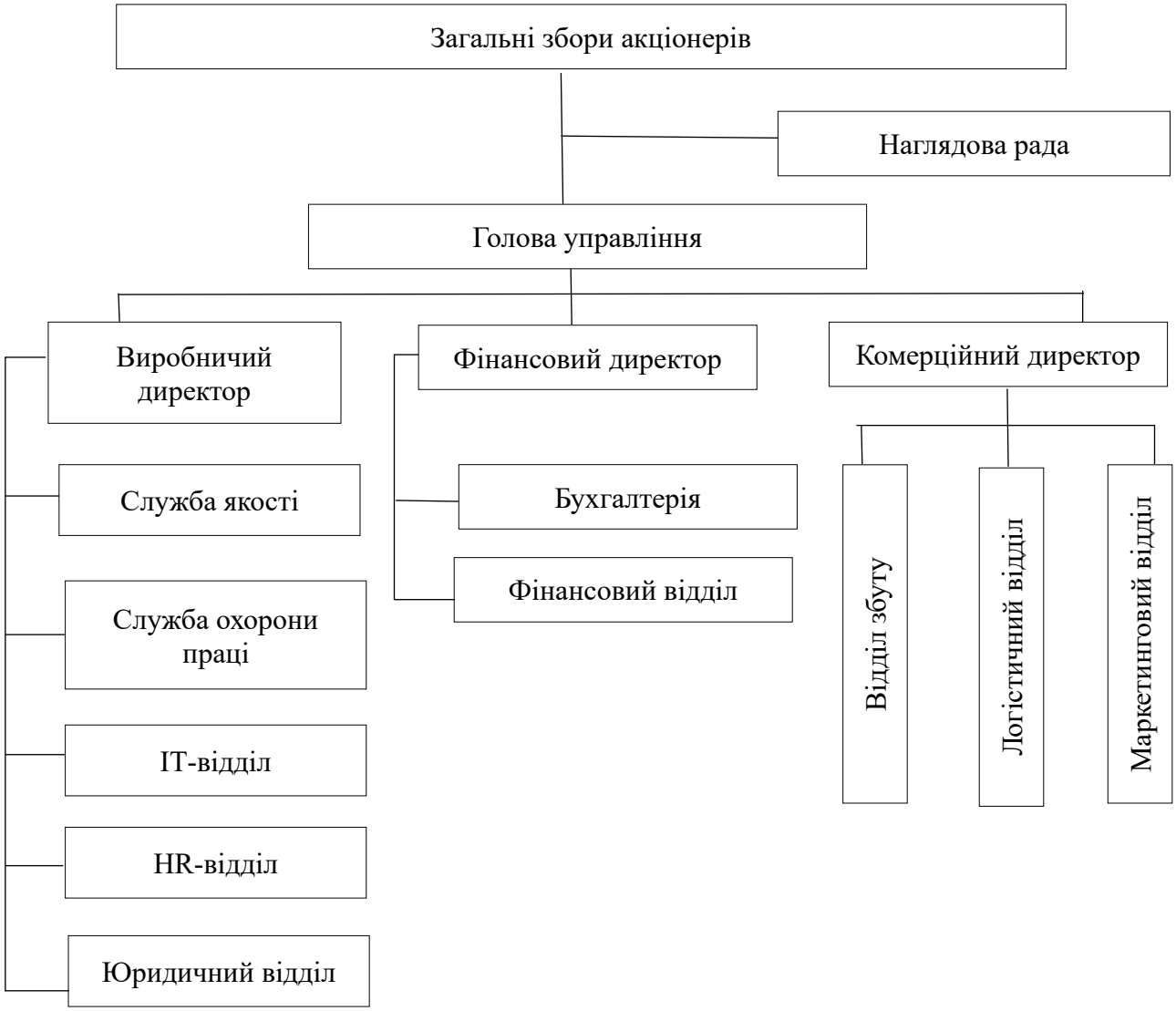

Рисунок 2.2 – Організаційна структура управління ПАТ «ІНТЕРПАЙП НТЗ»

голова правління – безпосередньо керує господарською діяльністю, відповідає за реалізацію цілей, місії діяльності та дотримання параметрів економічної безпеки.

Нами було проаналізовано аудиторський звіт Kreston Ukraine за 2024 рік. У звіті зазначено, що ПАТ «ІНТЕРПАЙП НТЗ» приділяє увагу вдосконаленню

систем внутрішнього контролю та ризик-менеджменту. Проте зростання кількості кібератак на металургійний сектор України вимагає від ПАТ «ІНТЕРПАЙП НТЗ» швидкої адаптації до цих змін. Зокрема, варто розглянути можливість трансформації з класичної адміністративної структури в цифрово орієнтовану систему управління, де безпека інформаційного простору стане базовою складовою економічної та цифрової безпеки всього заводу.

Наступним етапом нашого дослідження є проведення SWOT-аналізу ПАТ «ІНТЕРПАЙП НТЗ» з метою виявлення сильних та слабких сторін, можливостей та загроз у діяльності товариства (табл. 2.1).

Таблиця 2.1 – SWOT-аналіз ПАТ «ІНТЕРПАЙП НТЗ»

Сильні сторони (Strengths)	Слабкі сторони (Weaknesses)
1. Вихід з кризи та отримання прибутку. 2. Діяльність під брендом KLW. 3. Функціонування корпоративної системи SAP. 4. Автоматизований контроль якості. 5. Вертикальна інтеграція в групу INTERPIPE. 6. Наявність міжнародних сертифікатів якості. 7. Унікальні ринкові позиції у колісному сегменті. 8. Технологічна модернізація.	1. Висока питома вага енерговитрат при виробництві продукції. 2. Логістичні обмеження через воєнні дії. 3. Фізичний знос необоротних активів. 4. Залежність від материнської компанії. 5. Брак кваліфікованої робочої сили через наявну міграцію.
Можливості (Opportunities)	Загрози (Threats)
1. Діджиталізація клієнтського сервісу. 2. Предиктивна аналітика на базі Big Data. 3. Залучення грантів для інноваційного розвитку. 4. Масштабна відбудова української інфраструктури. 5. Глобальний тренд на «зелений» транспорт. 6. Поступове заміщення російської та білоруської продукції на європейському ринку. 7. Подальша інтеграція на ринки США та Близького Сходу.	1. Продовження війни. 2. Зростання кількості кібератак. 3. Посилення транскордонного вуглецевого податку. 4. Дефіцит кваліфікованих технічних фахівців. 5. Коливання валютних курсів та цін на брухт. 6. Жорсткий протекціонізм та антидемпінгові розслідування.

Після проведеного SWOT-аналізу ПАТ «ІНТЕРПАЙП НТЗ» нами було визначено, що підприємству варто застосовувати стратегію цифрової та

операційної стійкості. Товариство має фінансовий ресурс (отримало у 2023 та 2024 роках прибуток), міцні ринкові позиції (S), але працює в умовах критичних зовнішніх загроз (T), що свідчить про необхідність зміщення стратегічного фокусу на використання внутрішнього потенціалу.

Отже, проведений аналіз об'єкта та суб'єкта управління ПАТ «ІНТЕРПАЙП НТЗ» дозволяє констатувати, що підприємство виготовляє конкурентоспроможну продукцію на вітчизняних та світових ринках, має вертикально інтегровану структуру управління. Володіючи виробничим потенціалом, стабільними позиціями на глобальних ринках (бренд KLW), товариство водночас перебуває під дією глобальних викликів. Особливої значущості набуває саме забезпечення його цифрової стійкості, оскільки воєнні дії та хакерські атаки можуть напряму вплинути на забезпечення безперервності виробничих процесів.

2.2. Фінансово-економічний аналіз результатів господарської діяльності ПАТ «ІНТЕРПАЙП НТЗ»

Аналіз фінансово-економічних показників ПАТ «ІНТЕРПАЙП НТЗ» є наступним етапом нашого дослідження. Проведення фінансового аналізу дозволить об'єктивно оцінити рівень економічного розвитку товариства, оцінити ефективність прийнятих управлінських рішень та наявний ресурсний потенціал для його подальшої цифрової трансформації.

Аналіз показав, що протягом 2022-2024 рр. господарська діяльність ПАТ «ІНТЕРПАЙП НТЗ» відбувалася під впливом високої кількості ризиків і загроз зовнішнього середовища. Основні ризики, що вплинули негативно на діяльність:

воєнний стан, що спричинив руйнування традиційних логістичних ланцюгів;

енергетична криза, що призвела до дефіциту потужностей для енергоємного металургійного виробництва;

зростання інтенсивності кібератак на інформаційні системи товариства.

В першу чергу, слід визначити, яким чином ці ризики вплинули на динаміку основних фінансових показників діяльності ПАТ «ІНТЕРПАЙП НТЗ». Проведені розрахунки показали, що підприємство продемонструвало стратегічну стійкість, забезпечивши не лише збереження цілісності виробничих потужностей, а й позитивну динаміку ключових фінансових результатів починаючи з 2023 року.

Таблиця 2.2 – Динаміка основних показників фінансових результатів ПАТ «ІНТЕРПАЙП НТЗ» за 2022-2024 рр.

Показник	2022	2023	2024	Відхилення 2024/2023	Відхилення 2024/2022
Дохід (виручка) від реалізації, тис грн	8 183 093	10 407 549	8 317 201	-2090348	134108
Собівартість реалізованої продукції, тис грн	6 141 754	7 687 375	5 792 503	-1894872	-349251
Валовий прибуток, тис грн	2 041 339	2 720 174	2 524 698	-195476	483359
Чистий прибуток / (збиток), тис грн	-1 233 944	748 896	59 855	-689041	1293799

Аналіз даних свідчить, що 2022 рік став переломним для ПАТ «ІНТЕРПАЙП НТЗ». Так, у 2022 році було отримано чистий збиток у розмірі 1,23 млн грн, що було зумовлено впливом введення воєнного стану, втрати логістичних шляхів через блокування портів, стрімкого зростання цін на енергоносії та вимушених простоїв потужностей у Дніпрі.

Але протягом 2023-2024 років темп росту чистого доходу значно випередив темп росту собівартості, що свідчить про прийняття ефективних управлінських рішень щодо оптимізації витрат. Ключовими факторами фінансової реабілітації стали:

переорієнтація відвантажень на залізничні та автошляхи через західні кордони, що дозволило зберегти присутність на ринках ЄС;

діджиталізація операційного управління на основі впровадження точніших алгоритмів прогнозування, яка дозволила мінімізувати втрати сировини та енергії;

часткове відновлення світового попиту на залізничну продукцію;

успішна адаптація енергетичного менеджменту до умов нестабільного енергопостачання.

Як результат, у 2023 році ПАТ «ІНТЕРПАЙП НТЗ» продемонструвало рекордний для воєнного періоду рівень чистого прибутку у сумі 748 896 тис. грн, що дає стратегічну можливість розглянути можливість інвестування в удосконалення системи кібербезпеки.

Наступним етапом нашого дослідження є аналіз стану власного капіталу ПАТ «ІНТЕРПАЙП НТЗ». Ці показники є головними індикаторами фінансової незалежності підприємства та його здатності розраховуватись за боргами.

Таблиця 2.3 – Динаміка активів та капіталу ПАТ «ІНТЕРПАЙП НТЗ» за 2022-2024 рр.

Показник	2022	2023	2024	Відхилення 2024/2023	Відхилення 2024/2022
Середня вартість власного капіталу, тис грн	4831584,5	4717573,5	5056183	338609,50	224598,50
Середня вартість сукупного капіталу, тис грн	18829075	21576565	23490250	1913685,00	4661175,00
Частка власного капіталу в активах	0,43	0,45	0,55	+0,10	+0,12

Аналіз динаміки майнового стану ПАТ «ІНТЕРПАЙП НТЗ» підтверджує висновки про успішне подолання кризи 2022 року та формування позитивної динаміки до покращення фінансових показників. Поступове відновлення фінансової стійкості ПАТ «ІНТЕРПАЙП НТЗ» у 2023-2024 роках стало результатом прийняття правильних управлінських рішень, пошуком нових ринків збуту товарів. Стабілізація експортної діяльності дозволила наростити ресурс, який можна використати для подальшої цифрової трансформації системи управління товариством.

Далі проведемо оцінку ділової активності, яка дозволяє визначити, наскільки ефективно ПАТ «ІНТЕРПАЙП НТЗ» використовує свої ресурси для забезпечення виробництва та сталої діяльності.

Таблиця 2.4 – Показники ділової активності ПАТ «ІНТЕРПАЙП НТЗ» за 2022-2024 рр.

Показник		2022	2023	2024	Відхилення 2024/2022	Відхилення 2024/2023
Коефіцієнт обіговості оборотних засобів	обороти	0,53	0,57	0,41	-0,13	-0,16
Середній період обороту оборотніх засобів	дні	674	634	884	209,20	249,22
Коефіцієнт обіговості активів	обороти	0,11	0,13	0,11	0,00	-0,02
Операційні витрати на 1 грн. реалізованої продукції	коп.	0,99	0,99	1,52	0,53	0,53

Дані таблиці підтверджують, що відбувається поступове покращення використання ресурсного потенціалу ПАТ «ІНТЕРПАЙП НТЗ» після подолання кризових явищ 2022 року. Така динаміка стала можливою завдяки оптимізації складських запасів. Товариство не просто повернуло свої потужності до початку війни, а й створило нову ефективнішу управлінську модель, яка дозволяє отримувати чистий дохід. Проте, варто приділити значну увагу операційним витратам на 1 гривню реалізованої продукції, оскільки у 2024 році вони зросли на 0,53 пункти.

Наступним етапом нашого дослідження є аналіз показників рентабельності, що дозволить зробити комплексні висновки про діяльність товариства у сучасних умовах господарювання.

Динаміка показників рентабельності ПАТ «ІНТЕРПАЙП НТЗ» показала, що рентабельність власного капіталу мала тенденцію до росту. Так, у 2022 році вона складала -25,54%, а вже у 2024 році стала 1,18%. Проте, якщо порівнювати 2024 рік і 2023 рік, вона впала на 14,69%. Тобто, тенденція є неоднозначною. Рентабельність продукції теж знижувалася протягом досліджуваного періоду, так, порівнюючи 2024 і 2022 роки, падіння відбулося на 8,15%, а порівнюючи з 2023 роком, на 11,08%. Такий перебіг подій свідчить, що товариству слід шукати

можливості для зменшення рівня операційних витрат, виходу на нові ринки збуту, забезпечення власної енергетичної незалежності, використання нових логістичних маршрутів.

Таблиця 2.5 – Динаміка показників рентабельності ПАТ «ІНТЕРПАЙП НТЗ» за 2022-2024 рр.

Показник рентабельності	2022	2023	2024	Відхилення 2024/2022	Відхилення 2024/2023
Рентабельність власного капіталу, %	-25,54	15,87	1,18	26,72	-14,69
Рентабельність сукупного капіталу, %	-7,86	6,15	-0,12	7,74	-6,27
Рентабельність продукції, %	29,18	32,12	21,03	-8,15	-11,08

Отже, фінансово-економічний аналіз результатів діяльності ПАТ «ІНТЕРПАЙП НТЗ» підтвердив, що підприємство поступово відновлює свої позитивні показники після початку війни. Проте глобальні виклики, а також висока невизначеність зовнішнього середовища та залежність від материнської компанії можуть негативно вплинути на подальшу діяльність заводу. Для забезпечення його сталого розвитку, а також подальшої можливості впровадження цифрових інструментів для підвищення рівня цифрової безпеки, слід проаналізувати наявну інформаційну систему управління.

2.3. Оцінювання існуючої стратегії цифрової безпеки на ПАТ «ІНТЕРПАЙП НТЗ»

В умовах глобальної цифровізації промислового сектору та стрімкої еволюції кіберзагроз, стратегія цифрової безпеки стає фундаментом економічної стійкості ПАТ «ІНТЕРПАЙП НТЗ». Для підприємства металургійної галузі, що функціонує в режимі безперервного виробничого циклу, захист інформаційного периметру є не лише технічним завданням, а й стратегічною необхідністю.

Ефективність стратегії цифрової безпеки ПАТ «ІНТЕРПАЙП НТЗ» безпосередньо залежить від складності його інформаційно-технологічної екосистеми. Як сучасне промислове підприємство, товариство здійснює свою діяльність на глибокій інтеграції цифрових рішень у всі ланки доданої вартості.

Ключовими компонентами існуючих цифрових рішень товариства є:

автоматизовані виробничі лінії та системи технологічного контролю (OT – Operational Technology);

цифрові системи управління виробництвом (MES);

ERP-система (SAP);

корпоративні інформаційні мережі та системи комунікацій;

електронний документообіг та системи обліку (фінансовий, кадровий).

З огляду на таку структуру, периметр цифрової безпеки ПАТ «ІНТЕРПАЙП НТЗ» трансформується у багаторівневу систему, що охоплює (рисунок 2.3).

Рисунок 2.3 – Існуючі цифрові рішення щодо цифрової безпеки ПАТ «ІНТЕРПАЙП НТЗ»

Аналіз поточної практики управління в ПАТ «ІНТЕРПАЙП НТЗ» свідчить, що стратегія цифрової безпеки реалізується через:

централізацію управління ресурсами, тобто на основі використання єдиних стандартів безпеки для всіх територіально розподілених підрозділів групи;

багаторівневу регламентацію доступу, що передбачає впровадження політик нульової довіри (Zero Trust) щодо критичних баз даних;

гібридне резервування на основі комбінації локальних та хмарних центрів зберігання даних для миттєвого відновлення після збоїв;

інтегрований моніторинг, який полягає у використанні автоматизованих систем виявлення аномалій у мережевому трафіку та виробничих протоколах.

Особливістю ПАТ «ІНТЕРПАЙП НТЗ» є конвергенція виробничої та корпоративної ІТ-інфраструктури, що у майбутньому може посилити вразливість товариства. Тобто навіть атака на звичайну офісну пошту може стати «вхідними воротами» для зупинки системи керування сталеплавильними печами або прокатними станами. Відповідно, можна виділити наступні фактори впливу на цифрову безпеку ПАТ «ІНТЕРПАЙП НТЗ».

Проведений аналіз підтверджує, що ПАТ «ІНТЕРПАЙП НТЗ» перебуває у зоні високого та критичного цифрового ризику. Ключовою проблемою існуючої стратегії є те, що традиційні методи захисту (антивіруси, фаєрволи) уже не є достатніми для протидії комбінованим загрозам.

Проведемо детальний аналіз окремих складових системи кіберзахисту ПАТ «ІНТЕРПАЙП НТЗ» із наступною ідентифікацією зони «цифрової вразливості», яка потребує першочергового управлінського втручання (таблиця 2.6). Результати оцінювання демонструють фрагментарний (клаптиковий) характер існуючої стратегії цифрової безпеки ПАТ «ІНТЕРПАЙП НТЗ». Хоча підприємство має «сильну» базу в питаннях резервування та антивірусного захисту, критично важливі для промислового гіганта зони залишаються недооціненими.

Таблиця 2.6 – Оцінювання елементів стратегії цифрової безпеки ПАТ «ІНТЕРПАЙП НТЗ»

Елемент цифрової безпеки	Оцінка	Ключові прогалини
Резервне копіювання даних	Середня	Відсутність територіально віддаленого сховища (geo-redundancy).
Антивірусний захист	Висока	Встановлені антивірусне програмне забезпечення
Управління ризиками	Середня	Відсутня автоматизація розрахунку потенційних фінансових збитків від простою
Захист корпоративної мережі	Середня	Недостатній рівень внутрішньої сегментації (загроза горизонтального переміщення вірусів)

Контроль доступу	Середня	Відсутність повної багатофакторної автентифікації (MFA) для всіх робочих місць
Інформаційна безпека	Середня	Брак системності не дозволяє відстежувати динаміку захищеності в реальному часі
Моніторинг кіберінцидентів	Середня	Велика частка ручного аналізу кіберінцидентів, відсутність центру безпеки
Захист виробничих систем	Низька	Прямий ризик зупинки АСУ ТП через вразливості застарілих промислових протоколів
Реагування на інциденти	Низька	Відсутність чітких алгоритмів дій для персоналу під час кібератаки
Навчання персоналу	Низька	Майже не проводиться навчання персоналу, процес децентралізований, функції покладені на самих співробітників

Аналіз показав, що найбільш критичними векторами є SCADA-системи та АСУ ТП. Оскільки підприємство рухається в бік Industry 4.0, кількість точок входу в мережу (IIoT-датчики, модулі віддаленого моніторингу) зростає експоненційно, що розширює «поверхню атаки».

Проведений фінансово-економічний аналіз показав, що товариство має певний фінансовий ресурс для удосконалення системи кіберзахисту. Основну увагу слід приділяти навчанню та підвищенню кваліфікації персоналу, який і буде впроваджувати нові цифрові рішення на своїх робочих місцях.

Аналіз негативних сторін існуючої стратегії цифрової безпеки ПАТ «ІНТЕРПАЙП НТЗ» (рисунок 2.6) показав, що товариство має прогалини у системі інформаційного захисту. Звичайно, що усі зазначені слабкі сторони можливо усунути при формуванні якісної стратегії цифрової трансформації. Як було зазначено раніше, ця стратегія має бути включена до загальної стратегії діяльності товариства. Лише тоді, можливо, на всіх рівнях побудувати ефективно діючу систему цифрової безпеки. Тим паче наше дослідження показало, що поєднання воєнного стану та енергетичної нестабільності вимагає від ПАТ «ІНТЕРПАЙП НТЗ» впровадження моделі автономної цифрової стійкості. Модель передбачатиме здатність системи функціонувати в умовах часткової втрати зв’язку або живлення. Саме тому, вважаємо за необхідне зазначити, що існуюча стратегія цифрової безпеки ПАТ «ІНТЕРПАЙП НТЗ» потребує трансформації від пасивного захисту периметру до проактивної системи кіберстійкості. Основний фокус має бути зміщений на захист технологічного контуру та підвищення рівня цифрової грамотності персоналу.

Рисунок 2.4 – Аналіз негативних сторін існуючої стратегії цифрової безпеки ПАТ «ІНТЕРПАЙП НТЗ»

Отже, проведений комплексний аналіз дозволив визначити прогалини у цифровій безпеці товариства. ПАТ «ІНТЕРПАЙП НТЗ» характеризується середнім рівнем цифрової зрілості. Так, маючи сформовану базову систему цифрової безпеки, має можливість підтримувати основні виробничі процеси. Проте із ростом кількості глобальних викликів, ризиків та загроз у функціонуванні, існуюча стратегія цифрової безпеки ПАТ «ІНТЕРПАЙП НТЗ» не повною мірою відповідає викликам воєнного часу та Industry 5.0. Відповідно пропонується її перегляд та впровадження у загальну стратегію діяльності товариства.

Висновки до розділу 2

Аналіз процесу формування стратегії цифрової безпеки на ПАТ «ІНТЕРПАЙП НТЗ» дозволив сформувати наступні висновки:

1. Дослідження системи управління ПАТ «ІНТЕРПАЙП НТЗ» та результати SWOT-аналізу засвідчили, що підприємство має високотехнологічну вертикально-інтегровану структуру управління, адаптовану до кризових умов воєнного стану. Водночас визначено, що безперервність його технологічних процесів критично залежить від стабільності ІТ-інфраструктури, що обґрунтовує необхідність стратегічного переходу від традиційного адміністрування до моделі цифрової резильєнтності в умовах інтенсифікації кіберзагроз.

2. Оцінка фінансово-економічного стану ПАТ «ІНТЕРПАЙП НТЗ» підтвердила наявність ресурсного базису для проведення цифрової трансформації. Високі показники ліквідності, рентабельності та фінансової незалежності формують так званий «фінансовий щит». Він дозволяє підприємству не лише нівелювати потенційні збитки від кіберінцидентів, а й здійснювати випереджальне фінансування проектів у сфері кібербезпеки та технологій Industry 4.0.

3. Комплексний аналіз фінансово-господарської діяльності ПАТ «ІНТЕРПАЙП НТЗ» та інформаційного захисту дозволив ідентифікувати поточний рівень цифрової зрілості підприємства як середній. Попри успішне подолання кризи та наявність сформованої базової системи безпеки, існуюча стратегія кіберзахисту ПАТ «ІНТЕРПАЙП НТЗ» має переважно реактивний характер, що не повною мірою відповідає викликам сьогодення.

РОЗДІЛ 3
ШЛЯХИ УДОСКОНАЛЕННЯ СТРАТЕГІЇ ЦИФРОВОЇ БЕЗПЕКИ ПАТ «ІНТЕРПАЙП НТЗ» В УМОВАХ ГЛОБАЛЬНИХ ВИКЛИКІВ

3.1. Удосконалення стратегії ПАТ «ІНТЕРПАЙП НТЗ» в умовах глобальних викликів

Стратегія діяльності та розвитку ПАТ «ІНТЕРПАЙП НТЗ» в умовах діючих глобальних викликів має виступати фундаментальним документом. Стратегія має визначати ключові вектори розвитку товариства, візію його майбутнього стану, декомпонування на тактичні та операційні плани. Прозора та зрозуміла на всіх рівнях стратегія суттєво підвищує конкурентоспроможність організації, покращує імідж, дозволяє з більшою ймовірністю залучити грантове фінансування для інноваційних проєктів.

З огляду на сферу діяльності ПАТ «ІНТЕРПАЙП НТЗ», а також специфіку його діяльності, пропонується розробити стратегію на термін 2026-2029 років. У зазначеному стратегічному діапазоні на найближчі три роки стратегія має відображати:

удосконалення існуючих стратегічних орієнтирів із урахуванням цифрової безпеки;

корекцію місії та ключових завдань діяльності товариства у сфері цифрової трансформації;

проведення постійного моніторингу щодо існуючих та появи нових критичних вразливостей та глобальних викликів;

формування якісно нової системи корпоративних цінностей;

визначення чітких фінансово-економічних напрямів розвитку та унікальних конкурентних переваг;

специфіку та високу капіталомісткість металургійного виробництва.

Для ПАТ «ІНТЕРПАЙП НТЗ» в умовах глобальних викликів розроблення стратегії терміном до 2029 року має бути проактивною, оскільки якщо буде хоч маленька затримка у цифровізації виробничих процесів це призведе до критичних втрат. Оскільки кількість кіберзагроз з кожним роком буде зростати, необхідність інтеграції системи цифрової безпеки у бізнес-стратегію буде актуальною і неминучою. Як показало дослідження міжнародних практик цифровізації виробничих процесів, зокрема таких промислових гігантів як ArcelorMittal, ThyssenKrupp та Tenaris, цифрова безпека виходить за рамки допомоіжної ІТ-функції. Вона стає ключовим фактором операційної стійкості організації та забезпечує їй сталий розвиток, адаптацію до змін у зовнішньому середовищі.

Застосування такої проактивної стратегії на ПАТ «ІНТЕРПАЙП НТЗ» передбачатиме прогнозування можливих викликів та загроз, а після їх виявлення впровадження конкретних цифрових рішень (рисунок 3.1):

Рисунок 3.1 – Основні напрями впровадження проактивної стратегії на ПАТ «ІНТЕРПАЙП НТЗ»

Джерело. Авторська розробка

інтеграції інноваційних ІТ-рішень, що дозволить ПАТ «ІНТЕРПАЙП НТЗ» впроваджувати інновації без загрози затримки операційної діяльності;

безперервного моніторингу ризиків та загроз, використання білих хакерів (Pentesting) для виявлення вразливостей раніше, ніж їх використають зловмисники;

регулярного патч-менеджменту автоматизованих систем керування технологічними процесами (АСУ ТП / SCADA) та інфраструктури ERP без зупинки безперервного циклу виробництва труб і коліс;

наявності сертифікатів відповідності міжнародним стандартам безпеки (зокрема ISO/IEC 27001);

захисту ланцюгів постачань (Supply Chain Security) та забезпечення безпечного електронного документообігу (EDI) з ключовими глобальними контрагентами;

мінімізації фінансових ризиків від можливих кібератак (на кшталт вірусів-вимагачів), що дозволяє уникати незапланованих збитків і гнучко керувати собівартістю продукції;

відповідності жорстким регуляторним вимогам щодо кібербезпеки та захисту даних, які діють на міжнародних ринках (включаючи європейську директиву NIS 2);

розвитку бренду INTERPIPE, який позиціонуватиметься як стійка та цифрово захищена екосистема, що гарантує безперебійність постачань high-tech продукції.

Критичним для ПАТ «ІНТЕРПАЙП НТЗ» при розробленні компексної загальної стратегії до 2029 року є чітке усвідомлення негативних аспектів, зокрема проактивна стратегія вимагає значних капіталовкладень (CAPEX) у цифрову інфраструктуру, тоді як пасивна – несе в собі ризики повної зупинки доменних чи прокатного виробництв через деструктивні кібератаки на системи SCADA, що зумовлює гостру необхідність адаптації стратегічного контуру підприємства до глобальних викликів.

Слід також відзначити доцільність забезпечення комплексних передумов, які сприятимуть ефективному формуванню та довгостроковому впровадженню стратегії цифрової безпеки та розвитку ПАТ «ІНТЕРПАЙП НТЗ».

Систематизацію та сутнісно-змістовну характеристику цих передумов стосовно специфіки діяльності ПАТ «ІНТЕРПАЙП НТЗ» на період до 2029 року представлено в табл. 3.1.

Таблиця 3.1 – Формування ефективної стратегії цифрової безпеки ПАТ «ІНТЕРПАЙП НТЗ» до 2029 року

Напрями	Вимоги при впровадженні напрямів в умовах глобальних викликів	Очікуваний стратегічний ефект
Сталий розвиток товариства	Інтеграція контуру цифрової безпеки в загальну стратегію цифровізації виробництва (Industry 4.0/5.0). Забезпечення захисту інноваційних проєктів, впровадження хмарних обчислень та великих даних (Big Data) у металургійному процесі.	Створення захищеного цифрового середовища для безперервної модернізації потужностей заводу та мінімізація технологічних бар'єрів.
Проникнення на нові ринки збуту продукції	Відповідність систем кіберзахисту міжнародним комплаєнс-стандартам (зокрема європейській Директиві NIS 2 та регламенту GDPR) для підвищення експорту власної продукції на міжнародні ринки	Усунення регуляторних викликів на міжнародних ринках, забезпечення прозорості та довіри з боку іноземних споживачів
Утримання конкурентних переваг на міжнародних ринках	Моніторинг глобальних трендів у сфері кіберзагроз та своєчасне впровадження Zero Trust Architecture на базі ШІ	Випереджаючий захист інформаційних активів компанії від новітніх типів цільових кібератак та корпоративного шпигунства.
Покращення ділового іміджу та репутації	Позиціонування ПАТ «ІНТЕРПАЙП НТЗ» як надійного партнера, що гарантує безперебійність навіть в умовах масштабних геополітичних та безпекових викликів.	Зміцнення статусу лідера промислового сектору України та залучення міжнародних інвестицій (грантів)
Ефективна диверсифікація	Створення гнучкої та захищеної IT-системи, що дозволить швидко розгортати нові цифрові сервіси, платформи та удосконалювати системи управління логістикою.	Швидка адаптація до змін кон'юнктури ринку, диверсифікація каналів збуту та клієнтських сервісів через захищені цифрові інструменти.
Сучасна система управління, що включатиме безпековий напрям	Створення власного Операційного центру безпеки, що здійснюватиме безперервний аудит і захист автоматизованих систем керування технологічними процесами (АСУ ТП / SCADA) від фізичних та кібердеструктивних впливів.	Зведення до мінімуму ймовірності зупинки безперервного виробничого циклу через кіберінциденти, зниження потенційних фінансових збитків від простоїв.

Джерело: Авторська розробка

Саме тому, з метою оптимізації існуючої стратегії діяльності ПАТ «ІНТЕРПАЙП НТЗ» на період до 2029 року, пропонується наступна логічна послідовність етапів циклу стратегічного управління з акцентом на забезпечення цифрової безпеки товариства (рисунок 3.2):

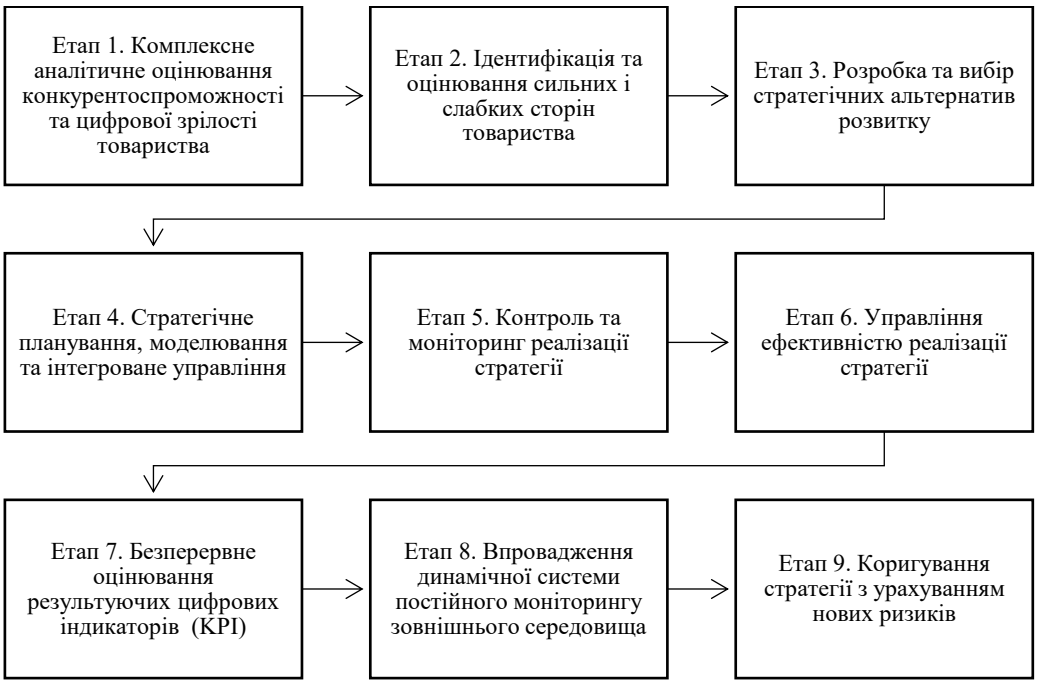

Рисунок 3.2 – Етапи оптимізації стратегії діяльності ПАТ «ІНТЕРПАЙП НТЗ» з акцентом на забезпечення його цифрової безпеки

Джерело: авторська розробка

На першому етапі проводиться аудит поточного стану IT-інфраструктури заводу, оцінку захищеності промислових систем SCADA/АСУ ТП та визначення позицій підприємства на ринку з позиції його технологічної надійності та відповідності стандартам ISO/IEC 27001.

На наступному – проводиться спеціалізований SWOT-аналіз з метою виявлення критичних вразливостей в інформаційних системах ПАТ «ІНТЕРПАЙП НТЗ» та прогнозування потенційних векторів цільових атак у промисловому секторі.

На третьому етапі відбувається формування набору можливих стратегічних сценаріїв (від мінімально комплаєнтного до проактивного з побудовою власного SOC) та вибір оптимальної траєкторії розвитку цифрової безпеки, що найбільше відповідає фінансовим можливостям та глобальним цілям ПАТ «ІНТЕРПАЙП НТЗ».

На четвертому етапі відбувається безпосередня розробка «Стратегії діяльності ПАТ «ІНТЕРПАЙП НТЗ» до 2029 року з акцентом на цифрову

безпеку». На цьому етапі формуються дорожні карти (Roadmaps), визначаються ключові проєкти, розраховуються необхідні капітальні та операційні витрати (CAPEX/OPEX на кіберзахист), розподіляються зони відповідальності.

Наступний етап передбачає передбачає оцінку того, як збої в цифровій безпеці можуть вплинути на екологічну безпеку (наприклад, запобігання кібератакам на системи фільтрації чи охолодження, що може спричинити техногенну аварію) та соціальну сферу (захист персональних даних тисяч працівників заводу, навчання персоналу правилам цифрової гігієни).

На шостому етапі реалізуються заплановані програмні та апаратні комплекси, налаштовуються системи моніторингу інцидентів, відбувається запуск архітектури нульової довіри (Zero Trust) та здійснюється щоденне управління процесами захисту інформаційних активів ПАТ «ІНТЕРПАЙП НТЗ».

На наступному етапі відбувається вимірювання ефективності стратегії через систему чітких метрик (наприклад, середній час виявлення загрози (MTTD), середній час ліквідації інциденту (MTTR), відсоток успішно заблокованих фішингових атак, рівень обізнаності персоналу).

На восьмому етапі проводитиметься моніторинг механізмів зворотного зв’язку, що дозволяють відстежувати появу нових глобальних кіберзагроз, змін в українському та європейському законодавстві.

На останньому етапі відбувається коригування стратегії на основі перерозподілу ресурсів та модернізації систем захисту ПАТ «ІНТЕРПАЙП НТЗ» у випадку виявлення нових вразливостей або критичних змін у зовнішньому середовищі.

Отже, удосконалення стратегії розвитку та діяльності ПАТ «ІНТЕРПАЙП НТЗ» в умовах глобальних викликів, криз, військового стану передбачає створення надійного цифрового фундаменту, який дозволить швидко реагувати на зміни у середовищі. Застосування проактивної стратегії з урахуванням напрямів цифровізації всіх бізнес-процесів на заводі дозволить мінімізувати фінансові втрати, зберегти безперервність виробничого циклу та відповідно до 2029 року отримати нові конкурентні переваги.

3.2. Напрями формування стратегії цифрової безпеки ПАТ «ІНТЕРПАЙП НТЗ»

Формування стратегічних напрямів забезпечення цифрової безпеки ПАТ «ІНТЕРПАЙП НТЗ» на період до 2029 року має передбачати детальний аналіз вразливостей та специфічних цифрових ризиків, що притаманні підприємству (великий промисловий холдинг з безперервним циклом виробництва).

Розробляючи майбутні напрями формування стратегії цифрової безпеки ПАТ «ІНТЕРПАЙП НТЗ», необхідно враховувати наступні ключові виміри деструктивного впливу ідентифікованих ризиків:

в першу чергу впливає конвергенція фізичних та цифрових загроз у площині операційної діяльності. Вона є найбільш критичною за рівнем впливу на прибутковість підприємства. Оскільки кібератаки на виробничі системи та автоматизовані системи керування технологічними процесами означатиме появу реального ризику аварійного припинення плавки металу в цехах та зупинки прокатних станів;

також можлива поява загроз безперервності бізнес-процесів під дією збоїв у зовнішньому енергопостачанні та кібератак. Раптові відключення живлення та переходи на резервні джерела можуть бути навмисно використані зловмисниками для прихованого впровадження шкідливого програмного забезпечення безпосередньо під час перезавантаження;

в третю чергу несанкціонований доступ, злам або маніпулювання даними в інтегрованій корпоративній ERP-системі SAP несе в собі пряму загрозу прихованого спотворення фінансових потоків, компрометації платіжних документів та витоку комерційної таємниці. Враховуючи існуючу ситуацію функціонування товариства, навіть короткочасна втрата контролю над фінансово-управлінським контуром здатна спровокувати дефіцит ліквідності, паралізувати розрахунки з міжнародними постачальниками продукції.

Проведений аналіз у другому розділі кваліфікаційної роботи доводить, що ПАТ «ІНТЕРПАЙП НТЗ» перебуває під постійним, системним тиском високотехнологічних ризиків та загроз. Наявна на підприємстві політика кіберзахисту, хоч і забезпечує певний базовий рівень цифрової стійкості та інформаційної безпеки, проте не повною мірою враховує високу ймовірність складних комбінованих атак, що реалізуються разом з деструктивними факторами війни.

Спираючись на отримані результати після аналізу стану ПАТ «ІНТЕРПАЙП НТЗ» нами сформовано комплекс практичних рекомендацій щодо формування стратегії цифрової безпеки до 2029 року. Він структурований за трьома взаємопов'язаними контурами безпеки, кожен з яких виконує специфічні захисні та адаптаційні функції (рисунок 3.3).

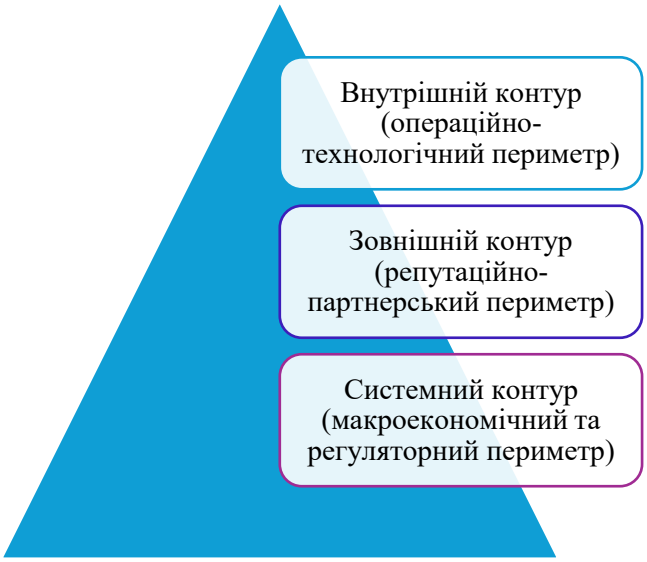

Рисунок 3.3 – Три контури цифрової безпеки ПАТ «ІНТЕРПАЙП НТЗ»

Внутрішній контур (операційно-технологічний периметр) цифрової безпеки ПАТ «ІНТЕРПАЙП НТЗ» має фокусуватися на забезпеченні поточної операційної ефективності заводу, безперервності виробничих процесів у цехах, підвищенні рівня цифрової та кіберграмотності персоналу (мінімізація «людського фактору»), а також на розвитку корпоративної культури етичного та прозорого управління. У межах цього контуру ключовим завданням є захист внутрішніх інформаційних систем (ERP SAP, MES-систем управління

виробництвом) та недопущення внутрішніх ІТ-інцидентів чи витоку комерційних даних.

Зовнішній контур (репутаційно-партнерський периметр) цифрової безпеки ПАТ «ІНТЕРПАЙП НТЗ» має бути спрямований на капіталізацію репутаційної довіри до бренду на міжнародній арені. Він має охоплювати цифрові та юридичні відносини з глобальними постачальниками сировини та обладнання, кінцевими клієнтами (нафтогазовими та залізничними компаніями ЄС та США), державними структурами й регуляторами (включаючи Кіберполіцію та Держспецзв'язку України), а також міжнародними фінансово-кредитними інституціями. Безпека цього контуру досягається через захист каналів передачі даних (EDI), впровадження безпечних B2B-порталів та аудит кіберстійкості підрядників (Supply Chain Security).

Системний контур (макроекономічний та регуляторний периметр) цифрової безпеки ПАТ «ІНТЕРПАЙП НТЗ» має акумулювати в собі глобальні макроекономічні, геополітичні, правові, соціальні та технологічні фактори (тренди Industry 4.0/5.0, вимоги європейського зеленого курсу та декарбонізації, директиви NIS 2 та GDPR), які безпосередньо впливають на довгострокову стратегічну стійкість підприємства. Цей контур забезпечує стратегічну адаптацію бізнес-моделі холдингу до змін у глобальному законодавстві та ландшафті світових кіберзагроз.

Кожен із зазначених контурів перебуватиме у постійній інтерактивній взаємодії з єдиною централізованою системою цифрового моніторингу та управління інцидентами, фіксуватиме потенційні ризики й аномалії, здійснюватиме автоматизовану оцінку ефективності прийнятих управлінських рішень та формування масивів великих даних (Big Data) для довгострокового предиктивного прогнозування.

Варто також наголосити, що найсучасніші технології кіберзахисту працюють ефективно лише у синергетичному поєднанні з професійно підготовленим та вмотивованим персоналом. Безперервне навчання співробітників ПАТ «ІНТЕРПАЙП НТЗ», постійне оновлення корпоративних

політик безпеки, розробка деталізованих інструкцій щодо специфіки роботи з конфіденційними даними та регулярні практичні тренінги (кібернавчання, симуляції фішингу) формують високий рівень свідомого та пильного ставлення колективу до актуальних кіберризиків. У поєднанні з передовими технічними та програмно-апаратними засобами це створить надійну, багаторівневу систему захисту підприємства.

Оскільки цифрова та кібербезпека є невід'ємною частиною стратегії діяльності ПАТ «ІНТЕРПАЙП НТЗ» можливо виокремити наступний базовий інструментарій забезпечення його подальшої цифрової трансформації (рис. 3.4).

Цифрова трансформація ПАТ «ІНТЕРПАЙП НТЗ» дозволить оперативно адаптуватися до мінливих глобальних викликів та прогресивно розвиватися в умовах підвищеної невизначеності макроекономічного середовища.

Саме така скоординована інтеграція безпекового інструментарію цифрової трансформації дозволить ПАТ «ІНТЕРПАЙП НТЗ» раціонально розподіляти капіталовкладення, забезпечувати високу операційну стійкість і гарантувати безперервність виробничого та фінансово-господарського циклів у перспективі до 2029 року.

В цілому, кожен із перелічених структурних інструментів не діє ізольовано або автономно, вони перебувають у стані перманентної та глибокої синергетичної взаємодії. Цифрові технології потребують високого рівня цифрової культури для їх ефективного та безбар'єрного впровадження в повсякденну практику заводу, тоді як цифрові комунікації виступають безпосереднім провідником стратегічних змін, інтеграції нових рішень та інструментів кібергігієни у загальне бізнес-середовище.

У свою чергу, зовнішнє цифрове представлення ПАТ «ІНТЕРПАЙП НТЗ» та його відповідність міжнародним стандартам комплаєнсу (таким як ISO/IEC 27001) є прямим об'єктивним відображенням внутрішньої цифрової та безпекової зрілості компанії, її відкритості до високотехнологічних інновацій і здатності створювати високу додану вартість у сучасній цифровій економіці.

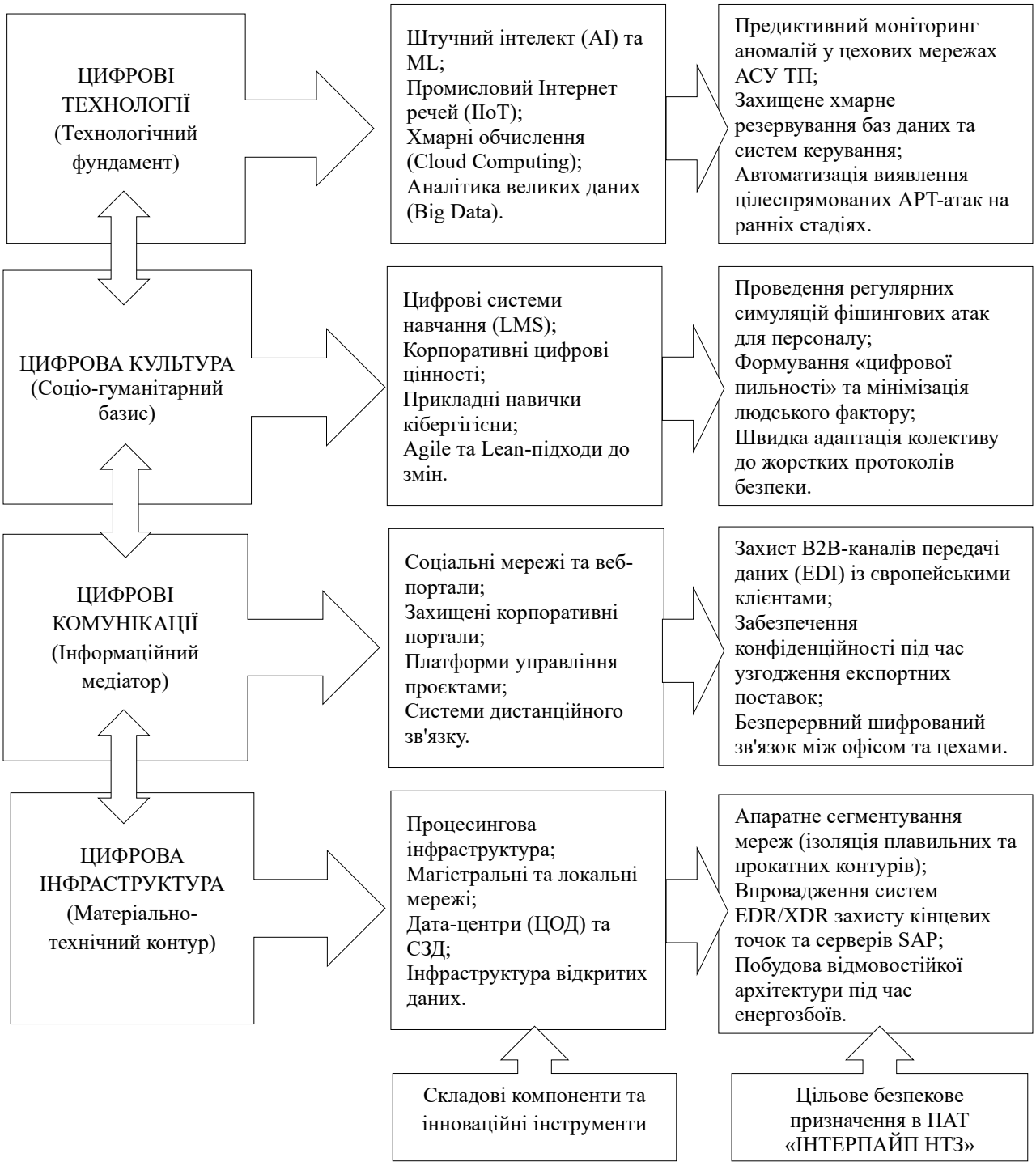

Рисунок 3.4 – Комплексна система та безпековий інструментарій цифрової трансформації в системі захисту ПАТ «ІНТЕРПАЙП НТЗ»

Джерело: Авторська розробка

Така системна інтеграція формує стійку, захищену від зовнішніх та внутрішніх кіберзагроз цифровізовану екосистему підприємства, дозволяючи при цьому з максимальною фінансово-економічною ефективністю та

раціональністю реалізувати розроблену стратегію цифрової безпеки в умовах глобальних викликів.

Пропонується наступна детермінована дорожня карта реалізації стратегічних завдань за визначеними раніше контурами безпеки (внутрішніми, зовнішніми та системними) до 2029 року для ПАТ «ІНТЕРПАЙП НТЗ». Ця дорожня карта дозволить забезпечити раціональне та збалансоване використання інвестиційних ресурсів товариства, мінімізувати поточні ризики воєнного стану та гарантувати планомірне підвищення рівня його цифрової зрілості (таблиця 3.2). Запропонована дорожня карта впровадження стратегії цифрової безпеки ПАТ «ІНТЕРПАЙП НТЗ» має чітко виражений еволюційний та збалансований характер.

Таблиця 3.2 – Дорожня карта впровадження стратегії цифрової безпеки для ПАТ «ІНТЕРПАЙП НТЗ» до 2029 року

Контур безпеки	Стратегічний напрям	2026 рік	2027 рік	2028 рік	2029 рік	Очікуваний безпековий та економічний ефект
Внутрішній контур (операційно-технологічний периметр)	Розроблення Плану відновлення після кібератак	+				Створення географічно розподілених резервних копій. Визначення цільового часу відновлення для критично важливих баз даних в умовах воєнного стану.
	Хмарна «міграція» ядра ERP SAP	+	+			Перенесення фінансово-управлінського контуру в захищене хмарне середовище європейських провайдерів із високим рівнем надійності.
	Сегментація та «ешелонований» захист АСУ ТП / SCADA		+	+		Зниження ризику несанкціонованого впливу на виробничі системи та підвищення стійкості безперервного виробничого циклу.
	Упровадження архітектури «нульової довіри»			+	+	Запровадження багатофакторної автентифікації. Встановлення системи управління з ідентифікацією та доступом для всіх користувачів корпоративної мережі заводу.
Зовнішній контур (репутаційно-партнерський периметр)	Розгортання та запуск Операційного центру безпеки	+	+			Створення інтегрованого центру цілодобового моніторингу, виявлення та реагування на кіберінциденти в режимі реального часу.

	Криптографічний захист логістичних систем		+			Забезпечення захищеного електронного документообігу з вітчизняними та закордонними партнерами. Підвищення стійкості ланцюгів постачання готової продукції на ринки ЄС.
	Комплаєнс-сертифікація за стандартом ISO/IEC 27001			+	+	Приведення системи менеджменту інформаційної безпеки у відповідність до міжнародних стандартів і вимог ЄС. Збереження довіри клієнтів та підтримка контрактної стабільності.
Системний контур (макроекономічний та регуляторний периметр)	Програма корпоративної кібергігієни	+	+	+	+	Проведення безперервних тренінгів і практичних навчань для персоналу.
	Інтеграція в державну екосистему кіберзахисту	+		+		Налагодження взаємодії з профільними державними структурами щодо обміну інформацією про кіберзагрози.
	Аудит і модернізація стратегії				+	Оцінювання досягнутих показників ефективності безпеки, перегляд профілю ризиків промислових активів і адаптація стратегічного контуру підприємства до глобальних викликів.

Джерело: авторська розробка

Отже, протягом 2026-2027 рр. планується впровадження найбільш завдань антикризового характеру. В першу чергу, необхідна розробка Плану відновлення після кіберінцидентів під час воєнного стану, переміщенні вразливих елементів ERP-системи SAP у хмару та запуску Операційного центру безпеки.

Протягом наступних років (2028-2029 рр.) вектор удосконалення стратегії цифрової безпеки має передбачати забезпечення довгострокового технологічного комплаєнсу (сертифікація ISO/IEC 27001, захист АСУ ТП та побудова Zero Trust Architecture), що дозволить компанії остаточно сформувати стійку, цифрово зрілу екосистему промислового лідера.

Таким чином, розроблена дорожня карта є дієвим та реалістичним інструментом інноваційного розвитку, який дозволяє збалансувати процеси капіталомісткої модернізації ПАТ «ІНТЕРПАЙП НТЗ» із жорсткими вимогами щодо збереження економічної, фінансової та технологічної безпеки в епоху глобальних викликів.

Отже, систематизація комбінованих загроз воєнного стану, глобальних викликів та високотехнологічних кіберризиків, що впливають на діяльність ПАТ «ІНТЕРПАЙП НТЗ» дозволила нам виокремити три взаємопов'язані вектори захисту. Сформовано дорожню карту впровадження стратегії цифрової безпеки для ПАТ «ІНТЕРПАЙП НТЗ» терміном до 2029 року. Застосований розподіл завдань за роками та контурами дозволяє забезпечити еволюційний перехід від першочергових антикризових заходів (хмарна міграція SAP, запуск SOC, впровадження DRP) у 2026-2027 рр. до побудови цілісної архітектури «нульової довіри» та довгострокового комплаєнсу до 2029 року.

Висновки до розділу 3

Запропоновано наступні шляхи удосконалення стратегії цифрової безпеки ПАТ «ІНТЕРПАЙП НТЗ» в умовах глобальних викликів:

1. Доведено, що в умовах гібридних викликів та воєнного стану, стратегічний контур цифрової безпеки ПАТ «ІНТЕРПАЙП НТЗ» на період до 2029 року трансформується у фундаментальну детермінанту загальної операційної стійкості підприємства, виходячи за межі класичної сервісної IT-підтримки. Формалізовано авторський дев'ятиетапний життєвий цикл стратегічного управління кіберзахистом, імплементація якого дозволяє синхронізувати дії топ-менеджменту у внутрішньому та зовнішньому середовищах, мінімізувати потенційні матеріально-фінансові збитки й сформувати надійну технологічну базу для його повоєнного відновлення та довгострокової конкурентоспроможності на світовому ринку металопродукції.

2. На основі декомпозиції комбінованих воєнних загроз та релевантних кіберризиків для критичних інфраструктурних вузлів ПАТ «ІНТЕРПАЙП НТЗ» (зокрема, ERP-системи SAP та технологічних контурів АСУ ТП) обґрунтовано тривимірну (контурну) архітектуру захисту та розроблено детерміновану дорожню карту впровадження стратегії цифрової безпеки до 2029 року. Запропонований матричний розподіл завдань забезпечує збалансований

еволюційний перехід від невідкладних тактичних антикризових рішень (географічно розподіленої хмарної міграції даних, розгортання Операційного центру безпеки SOC та впровадження Disaster Recovery Plan) упродовж 2026-2027 рр. до розбудови цілісної концепції нульової довіри (Zero Trust Architecture) та досягнення повного регуляторного комплаєнсу до 2029 року.

ВИСНОВКИ

Проведене у кваліфікаційній роботі дослідження на тему: «Обґрунтування стратегії цифрової безпеки організації в умовах глобальних викликів» дозволило сформувати наступні висновки:

1. Визначено, що перехід від оперативного до стратегічного підходу дозволяє організації не лише адаптуватися до поточних криз, а й системно формувати ресурси для збереження конкурентоспроможності, орієнтуючись на багатоваріантність розвитку та безперервність оновлення стратегічних цілей. Обґрунтування стратегії стає цілісним процесом, де усвідомлення місії та ідентифікація ключових факторів успіху створюють основу для прийняття зважених рішень у межах обраного курсу розвитку.

2. Доведено, що сучасні інформаційні системи та технології є життєво важливим фундаментом забезпечення економічної безпеки підприємства в умовах цифрової економіки. Вони надають менеджменту необхідний інструментарій для навігації у складному бізнес-середовищі, збереження конкурентоспроможності та проактивного захисту від потенційних ризиків. Проте їх ефективна імплементація потребує стратегічного підходу, фокусу на кібербезпеці та безперервного процесу навчання й адаптації персоналу.

3. Встановлено, що в умовах масштабної діджиталізації цифрова трансформація перетворилася з допоміжного інструментарію на фундаментальний рушій бізнес-успіху та конкурентоспроможності. Вона системно впливає на архітектуру бізнес-моделей, ефективність маркетингових комунікацій, оптимізацію ресурсів та дозволяє досягати ефекту масштабу. Компанії, що ігнорують ці зміни, стикаються з критичними ризиками втрати ринкових позицій. Обґрунтовано, що для українського бізнесу цифровізація є ключовим інструментом підвищення економічної стабільності. Попри обмежені ресурси, впровадження базових елементів кіберзахисту (шифрування, MFA, хмарні сервіси) та автоматизація обліку дозволяють суттєво мінімізувати ризики та підвищити прозорість управління.

4. Дослідження системи управління ПАТ «ІНТЕРПАЙП НТЗ» та результати SWOT-аналізу засвідчили, що підприємство має високотехнологічну вертикально-інтегровану структуру управління, адаптовану до кризових умов воєнного стану. Водночас визначено, що безперервність його технологічних процесів критично залежить від стабільності ІТ-інфраструктури, що обґрунтовує необхідність стратегічного переходу від традиційного адміністрування до моделі цифрової резильєнтності в умовах інтенсифікації кіберзагроз.

5. Оцінка фінансово-економічного стану ПАТ «ІНТЕРПАЙП НТЗ» підтвердила наявність потужного ресурсного базису для проведення цифрової трансформації. Високі показники ліквідності, рентабельності та фінансової незалежності формують так званий «фінансовий щит». Він дозволяє підприємству не лише нівелювати потенційні збитки від кіберінцидентів, а й здійснювати випереджальне фінансування проектів у сфері кібербезпеки та технологій Industry 4.0.

6. Комплексний аналіз фінансово-господарської діяльності ПАТ «ІНТЕРПАЙП НТЗ» та інформаційного захисту дозволив ідентифікувати поточний рівень цифрової зрілості підприємства як середній. Попри успішне подолання кризи та наявність сформованої базової системи безпеки, існуюча стратегія кіберзахисту ПАТ «ІНТЕРПАЙП НТЗ» має переважно реактивний характер, що не повною мірою відповідає викликам сьогодення.

7. Доведено, що в умовах гібридних викликів та воєнного стану, стратегічний контур цифрової безпеки ПАТ «ІНТЕРПАЙП НТЗ» на період до 2029 року трансформується у фундаментальну детермінанту загальної операційної стійкості підприємства, виходячи за межі класичної сервісної ІТ-підтримки. Формалізовано авторський дев’ятиетапний життєвий цикл стратегічного управління кіберзахистом, імплементація якого дозволяє синхронізувати дії топ-менеджменту у внутрішньому та зовнішньому середовищах, мінімізувати потенційні матеріально-фінансові збитки й сформувати надійну технологічну базу для його повоєнного відновлення та довгострокової конкурентоспроможності на світовому ринку металопродукції.

8. На основі декомпозиції комбінованих воєнних загроз та релевантних кіберризиків для критичних інфраструктурних вузлів ПАТ «ІНТЕРПАЙП НТЗ» (зокрема, ERP-системи SAP та технологічних контурів АСУ ТП) обґрунтовано тривимірну (контурну) архітектуру захисту та розроблено детерміновану дорожню карту впровадження стратегії цифрової безпеки до 2029 року. Запропонований матричний розподіл завдань забезпечує збалансований еволюційний перехід від невідкладних тактичних антикризових рішень (географічно розподіленої хмарної міграції даних, розгортання Операційного центру безпеки SOC та впровадження Disaster Recovery Plan) упродовж 2026-2027 рр. до розбудови цілісної концепції нульової довіри (Zero Trust Architecture) та досягнення повного регуляторного комплаєнсу до 2029 року.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Білоус С., Трохименко А., Камінський В. Стратегічне управління розвитком підприємства в умовах кризи та військових викликів. *Економіка та суспільство*. 2024. № 68. DOI: https://doi.org/10.32782/2524-0072/2024-68-62

2. Таран-Лала О., Сухорук К. Особливості стратегічного управління підприємством. *Економіка та суспільство*. 2021. № 25. DOI: https://doi.org/10.32782/2524-0072/2021-25-66

3. Талавиря О. М. Особливості формування стратегії розвитку підприємств. *Науковий вісник Національного університету біоресурсів і природокористування України. Серія: Економіка, аграрний менеджмент, бізнес*. 2017. Вип. 260. С. 339–347.

4. Пар'єва Н. О., Буковський О. О., Вікаренко В. Р. Удосконалення системи менеджменту підприємства в умовах глобальних ризиків. *Entrepreneurship and Innovation*. 2023. Вип. 6. С. 14–19. DOI: https://doi.org/10.37634/efp.2023.6.14

5. Польова Н., Когут Р., Дума Ю. Напрями забезпечення безпеки підприємства в умовах цифровізації бізнесу. *Розвиток міста*. 2024. № 1 (01). С. 90–94.

6. Сербіна Т., Куташев І. Функціональні стратегії розвитку підприємства в умовах цифровізації. *Розвиток міста*. 2025. № 4 (08). С. 131–137.

7. Ільчишин М. Є., Пузирьова П. В. Інноваційні аспекти формування міжнародної стратегії підприємств в умовах глобальних викликів. *Інноватика в освіті, науці та бізнесі: виклики та можливості* : тези доповідей міжнар. наук.-практ. конф. Київ : КНУТД, 2025.

8. Швиданенко Г. О. Обґрунтування та формування стратегії розвитку компанії в умовах нестабільності. *Київський економічний науковий журнал*. 2024. № 6. С. 146–153.

9. Чухлата Ж. Г. Особливості стратегічного управління підприємством в сучасних умовах. *Вісник економіки транспорту і промисловості*. 2018. № 62. С. 104–111.

10. Єпіфанова І., Джеджула В. Я., Каплун Р. Особливості стратегічного управління підприємствами в умовах воєнного стану. *Innovation and Sustainability*. 2023. № 4. С. 64–71.

11. Пілецька С., Клюс І., Білоус Н. Особливості формування стратегії розвитку підприємства в умовах макроекономічної нестабільності. *Сталий розвиток економіки*. 2024. № 2 (49). С. 174–179. DOI: https://doi.org/10.32782/2308-1988/2024-49-27

12. Продіус О. І., Гижиця М. В. Реінжиніринг управління бізнес-процесами підприємства. *Інфраструктура ринку*. 2019. Вип. 34. С. 167–173.

13. Рудницька О., Комаровський А. Стратегічне управління підприємством як важлива складова системи менеджменту. *Економіка та суспільство*. 2023. № 57.

14. Плесюк О. Цифрові ризики в управлінні розвитком підприємства. *Bulletin of Sumy National Agrarian University*. 2025. № 3 (103). С. 65–70.

15. Кравченко О., Гаврилюк О., Челомбітько О., Бойко С. Управління економічною безпекою підприємств в умовах цифрової економіки. *Адаптивне управління: теорія і практика. Серія Економіка*. 2024. Т. 19, № 38.

16. Ситнік Є. Обґрунтування стратегії управління системою економічної безпеки підприємства на основі використання інноваційних цифрових технологій. *Сталий розвиток економіки*. 2025. № 5 (56). С. 302–306.

17. Обрамич О. Особливості формування цифрової безпеки на підприємстві. *Економіка та суспільство*. 2024. № 68.

18. Іванова Н. Стратегічні орієнтири інноваційного розвитку промислових підприємств в умовах цифрової трансформації. *Проблеми і перспективи економіки та управління*. 2025. № 1 (41). С. 211–223.

19. Левицький В. В., Радинський С. В., Артеменко Л. Б., Радинська С. Підприємництво України в умовах війни та цифровізації: можливості та

перспективи удосконалення. *Трансформація бізнесу для сталого майбутнього: дослідження, цифровізація та інновації* : монографія. Чернівці : ФОП Паляниця В. А., 2024. С. 235–253.

20. Захарчук Н. Економічна безпека підприємства у цифрову епоху: нові виміри, загрози та управлінські підходи. *Development Service Industry Management*. 2024. № 3. С. 308–313.

21. Олійник Л. В., Кузнєцова А. П. Методологічні засади формування стратегії розвитку підприємства. *Економіка і організація управління*. 2018. № 3. С. 118–126.

22. Беззубко Б., Ткаченко М. Особливості формування стратегій українських підприємств під час війни. *Галицький економічний вісник Тернопільського національного технічного університету*. 2022. Т. 78, № 5-6. С. 96–102.

23. Ревуцька А. О., Смолій Л. В. Особливості формування стратегії розвитку підприємств в умовах невизначеності. *Східна Європа: економіка, бізнес та управління*. 2018. Вип. 2 (13). С. 145–150.

24. Юрій Е. О., Луцик І. Б. Особливості формування стратегії розвитку підприємств в умовах невизначеності зовнішнього середовища. *Науковий вісник Международного гуманітарного університету. Серія: Економіка і менеджмент*. 2015. Вип. 13. С. 131–134.

25. Гросул В. А., Жилякова О. В. Сутність та особливості формування антикризової стратегії підприємства в умовах VUCA-світу. *Бізнес Інформ*. 2015. № 11. С. 393–399.

26. Смачило І. І. Формування економічної стратегії підприємства в сучасних умовах. *Молодий вчений*. 2017. № 12 (52). С. 758–762.

27. Чепелюк М. І. Трансформація українського бізнесу в умовах глобальних викликів. *Український журнал прикладної економіки та техніки*. 2024. Т. 9, № 4. С. 88–95.

28. Боковець В., Пілявоз Т., Григорук І. Забезпечення стабільного розвитку та економічної стійкості підприємств в умовах сучасних викликів.

Herald of Khmelnytskyi National University. Economic sciences. 2025. Т. 338, № 1. С. 465–468.

29. Рибак І., Гарафонова О. Цифрова трансформація як інструмент удосконалення управління стратегічним розвитком підприємства. *Herald of Khmelnytskyi National University. Economic Sciences*. 2025. Т. 346, № 5. С. 93–98.

30. Яценко О. В., Яценко В. М., Яценко В. О. Особливості стратегічного менеджменту підприємства в парадигмі сучасних викликів. *Modern Economics*. 2020. № 23. С. 239–245.

31. Ситнік Є. Теоретичні основи впровадження інноваційних цифрових технологій в управлінні системою економічної безпеки підприємства. *Вчені записки Університету «КРОК»*. 2025. № 1 (77). С. 371–378.

32. Гапєєва О. М., Вітютін В. Є. Диджиталізація як чинник формування економічної стійкості та безпеки підприємств у післявоєнний період. *Здобутки економіки: перспективи та інновації*. 2025. Вип. 25.

33. Маліношевська К. І. Розроблення стратегії розвитку підприємства : кваліфікаційна робота. Ужгород : УжНУ, 2022. URL: https://dspace.uzhnu.edu.ua/items/4f28d4bf-3ad7-4f6c-80b5-e33fcdb69b61

34. Плотніков О. М., Шерстюк Р. П. Основні напрями впровадження стратегії цифрової трансформації підприємства та її вплив на управління ключовими бізнес-процесами. *Наукові інновації та передові технології*. 2025. № 8 (48). С. 449–471.

35. Мисик Ю., Яхура В. Стратегія сталого розвитку як складова системи економічної безпеки підприємства в умовах цифровізації. *Дослідження та інновації*. 2025. Т. 1, № 4 (7). С. 33–38.

36. Чаплик О., Чаплик Т. Системне управління інформаційною безпекою організації: концепції, моделі та механізми захисту інформації з обмеженим доступом. *Дослідження та інновації*. 2025. Т. 1, № 5 (8). С. 101–107.

37. Комеліна О. Використання цифрових технологій та штучного інтелекту (AI) у стратегіях розвитку українських операторів мобільного зв’язку.

Сталий розвиток економіки. 2026. № 1 (5). С. 931–937. DOI: https://doi.org/10.32782/2308-1988/2026-58-124

38. Комеліна О., Корунський В. Цифрові технології та інструменти в проєктному управлінні організаційною стійкістю підприємств. *Сталий розвиток економіки*. 2026. № 6 (57). С. 849–855. DOI: https://doi.org/10.32782/2308-1988/2025-57-117

39. Климчук О. В. Сучасні процеси розвитку в Україні інформаційних систем і технологій в управлінні підприємствами. *Актуальні проблеми, пріоритетні напрямки та стратегії розвитку України* : тези доповідей І Міжнародної науково-практичної онлайн-конференції / за ред. О. С. Волошкіної та ін. Київ, 2021. С. 199–201.

40. Риженко О. М. Особливості впровадження концепції lean management на металургійному підприємстві. *Review of Transport Economics and Management*. 2021. № 6 (22). С. 60–71.

41. Ляхович О. О., Оплачко І. О. Економічна безпека та транспарентність підприємств в умовах цифровізації. *Вісник НУВГП. Серія «Економічні науки»*. 2021. Вип. 2 (94). С. 100–111.

42. Гудзь О. Є. Цифрова економіка: зміна цінностей та орієнтирів в управлінні підприємством. *Економіка. Менеджмент. Бізнес*. 2018. № 2 (24). С. 4–12.

43. Болдуєва О., Дащенко Г., В'ялець О., Блохіна Г., Михайленко О. Особливості стратегічного розвитку підприємств в умовах цифрової трансформації економіки України. *Financial and Credit Activity: Problems of Theory and Practice*. 2025. No. 1 (60). С. 415–426. DOI: https://doi.org/10.55643/fcaptp.1.60.2025.4596

44. Гринько Т., Гвініашвілі Т., Каліберда М. Стратегічне управління підприємством в умовах цифрової економіки. *Економіка та суспільство*. 2023. № 50. DOI: https://doi.org/10.32782/2524-0072/2023-50-71

45. Лисиця Ю. Стратегії розвитку інноваційного потенціалу підприємства в умовах цифровізації. *Економіка та суспільство*. 2024. № 64. DOI: https://doi.org/10.32782/2524-0072/2024-64-106

46. Лєонов С. В., Семко О. В. Інформаційна технологія управління інформаційними ризиками для проєктів цифрової трансформації бізнесу. *Управління розвитком складних систем*. 2023. Вип. 56. С. 64–69.

47. Поврозник П. П. Особливості інноваційного розвитку підприємництва в Україні в контексті глобальних безпекових викликів та ризиків цифровізації. *Міжнародний науковий журнал «Інтернаука». Серія: Економічні науки*. 2023. № 8. С. 113–123.

48. Прокоф'єва О. В., Беспалова Ю. Ю. Кібер-ризики та управління ними в умовах глобалізації та цифрової трансформації. *Ефективна економіка*. 2024. № 5. URL: http://nbuv.gov.ua/UJRN/efek_2024_5_89

49. Хандій О. О., Кобцева Д. А. Можливості та ризики цифровізації для суб'єктів ринку праці. *Вісник економічної науки України*. 2023. № 1. С. 70–76.

50. Швидка О. П., Дзюбенко Л. М. Інноваційні бізнес-моделі в умовах цифрової трансформації: перспективи та ризики для малого бізнесу. *Фінанси України*. 2024. № 11. С. 118–128.

51. Мігус І. П., Шпильовий Б. В. Сучасні підходи та критерії визначення економічної безпеки. *Вісник Черкаського університету*. 2014. № 39 (332). С. 58–62.

52. Рудніченко Є., Гавловська Н., Суходоля С., Лісовський І., Ядуха С. Цифрова економіка та її вплив на розвиток організацій. *Вісник Хмельницького національного університету*. 2020. № 4. С. 172–176.

53. Солона О. В. Застосування цифрових технологій в аграрному виробництві. *Техніка, енергетика, transport АПК*. 2022. № 3 (118). С. 19–25.

54. Тертичний Я. С. Детермінанти впливу цифрового бізнесу на глобальний економічний розвиток. *Економіка і організація управління*. 2016. № 4 (24). С. 363–368.

55. Чайковська І. Розробка моделі інформаційної системи управління знаннями на проєктноорієнтованому підприємстві. *Modeling the Development of the Economic Systems*. 2023. № 2. С. 153–158.

56. Костенко С. С., Кудінова А. О. Особливості управління цифровою безпекою організації в сучасних умовах господарювання. *Економічна безпека: держава, регіон, підприємство* : матеріали X Міжнародної науково-практичної конференції, 13 травня 2026 р. Полтава : Національний університет імені Юрія Кондратюка, 2026. С. 109–110.

57. Костенко С. С., Кудінова А. О. Міжнародний досвід формування стратегії цифрової безпеки організації. *Сталий розвиток: виклики та загрози в умовах сучасних реалій* : матеріали IV Міжнародної науково-практичної Інтернет-конференції, 04 червня 2026 р. Полтава : Національний університет імені Юрія Кондратюка, 2026. С. 266–267.

ДОДАТКИ