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: «Управління цифровою безпекою організації як чинник забезпечення економічної стійкості»

Виконав:
студент групи 401-ЕМ
Борицький Владислав Олександрович

Керівник:
доцент кафедри менеджменту і логістики,
к.е.н., доцент Гришко В.В.

Полтава – 2026

ЗМІСТ

ВСТУП

Проблема управління цифровою безпекою набуває для підприємств телекомунікаційної сфери, діяльність яких пов’язана з обробкою значних обсягів даних, функціонуванням складної цифрової інфраструктури та забезпеченням безперервності надання послуг. В умовах зростання кількості кібератак, витоків інформації, загроз для критичної інфраструктури та поширення цифрових ризиків підприємства змушені адаптувати свої системи управління.

Актуальність теми дослідження зумовлена необхідністю підвищення ефективності процесу управління цифровою безпекою підприємств в умовах цифрової трансформації економіки, посилення кіберзагроз та нестабільності зовнішнього середовища. Для українських підприємств проблема забезпечення цифрової безпеки є особливо важливою в умовах воєнного стану, оскільки кібератаки стали одним із ключових інструментів впливу на діяльність бізнесу та критичної інфраструктури.

Питання цифрової безпеки, кіберзахисту та управління ризиками досліджувалися у працях вітчизняних і зарубіжних науковців. Значний внесок у розвиток підходів до управління інформаційною та цифровою безпекою зробили дослідники у сфері менеджменту, інформаційних технологій та економічної безпеки. Водночас аналіз наукових праць свідчить про наявність недостатньо досліджених аспектів щодо інтеграції процесу управління цифровою безпекою.

Метою кваліфікаційної роботи є розробка теоретичних положень та практичних рекомендацій щодо підвищення ефективності управління цифровою безпекою підприємства з метою забезпечення його економічної стійкості в умовах сучасних кіберзагроз.

Для досягнення поставленої мети у роботі визначено такі завдання:

1) дослідити сутність цифрової безпеки підприємства та її роль у забезпеченні економічної стійкості;
2) визначити основні підходи до процесу управління цифровою безпекою підприємства;
3) проаналізувати світовий досвід управління цифровою безпекою підприємств;
4) провести аналіз об’єкта та суб’єкта процесу управління цифровою безпекою ПрАТ «Київстар»;
5) здійснити діагностику фінансово-господарської діяльності підприємства;
6) оцінити процес управління цифровою безпекою та його вплив на економічну стійкість підприємства;
7) обґрунтувати стратегічні напрями вдосконалення процесу управління цифровою безпекою підприємства;
8) розробити комплексне забезпечення системи управління цифровою безпекою ПрАТ «Київстар».

Об’єктом дослідження є процес управління цифровою безпекою телекомунікаційного підприємства.

Предметом дослідження є теоретичні, методичні та практичні аспекти управління цифровою безпекою як чинника забезпечення економічної стійкості підприємства на прикладі Київстар.

У процесі дослідження використано сукупність загальнонаукових і спеціальних методів дослідження. Теоретичні методи застосовано для узагальнення наукових підходів до визначення сутності цифрової безпеки та процесу управління нею. Методи аналізу і синтезу використано для оцінювання сучасного стану цифрової безпеки підприємства. Метод порівняння застосовано при дослідженні вітчизняного та світового досвіду управління цифровою безпекою. Для оцінювання зовнішнього та внутрішнього середовища підприємства використано SWOT-аналіз, PESTLE-аналіз та метод бенчмаркінгу. Економіко-статистичні методи використано для аналізу

фінансово-господарських показників діяльності підприємства. Графічні та табличні методи застосовано для візуалізації результатів дослідження.

Інформаційну базу дослідження становлять законодавчі та нормативно-правові акти у сфері цифрової безпеки та кіберзахисту, наукові праці вітчизняних і зарубіжних учених, статистичні матеріали, фінансова звітність підприємства, аналітичні матеріали та офіційні дані ПрАТ «Київстар».

Практична значущість отриманих результатів полягає у розробці рекомендацій щодо вдосконалення процесу управління цифровою безпекою підприємства, які можуть бути використані у практичній діяльності ПрАТ «Київстар» з метою підвищення рівня захищеності інформаційних ресурсів, зниження рівня кіберризиків та забезпечення економічної стійкості підприємства. Запропоновані рекомендації можуть бути використані для вдосконалення управлінських рішень у сфері цифрової безпеки підприємств телекомунікаційної галузі.

Наукова новизна одержаних результатів полягає в удосконаленні підходів до управління цифровою безпекою підприємства шляхом інтеграції процесів оцінювання кіберризиків у систему забезпечення економічної стійкості підприємства.

Основні положення кваліфікаційної роботи пройшли наукову апробацію під час участі у IV Міжнародній науково-практичній Інтернет-конференції «Сталий розвиток: виклики та загрози в умовах сучасних реалій».

Гришко В.В., Бобрицький В.О. Управління цифровою безпекою як інструмент забезпечення економічної стійкості організації. IV Міжнародній науково-практичній Інтернет-конференції *«Сталий розвиток: виклики та загрози в умовах сучасних реалій»*. Полтава 2026.

Робота складається зі вступу, трьох розділів, висновків, списку використаних джерел та додатків. Загальний обсяг роботи становить 90 сторінок. Робота містить 7 таблиць, 10 рисунків, список використаних джерел із 38 найменувань та 3 додатки.

РОЗДІЛ 1. ТЕОРЕТИЧНІ ТА ПРАКТИЧНІ АСПЕКТИ ФОРМУВАННЯ БІЗНЕС-МОДЕЛІ ІННОВАЦІЙНОГО РОЗВИТКУ СУЧАСНОГО ПІДПРИЄМСТВА.

1.1. Сутність цифрової безпеки підприємства та її роль у забезпеченні економічної стійкості

У сучасних умовах розвитку світової економіки цифровізація стала одним із ключових чинників трансформації діяльності підприємств. Активне впровадження інформаційних технологій, автоматизація бізнес-процесів, використання цифрових платформ та хмарних сервісів суттєво змінюють підходи до управління підприємствами, підвищують ефективність їх функціонування та формують нові конкурентні переваги. Цифрова трансформація охоплює практично всі сфери господарської діяльності, починаючи від управління персоналом і фінансами до логістики, маркетингу та комунікацій із клієнтами.

Сучасні підприємства значною мірою залежать від функціонування інформаційних систем та цифрової інфраструктури. Використання корпоративних мереж, хмарних технологій, автоматизованих систем управління, електронного документообігу та цифрових каналів взаємодії забезпечує безперервність бізнес-процесів і швидкість прийняття управлінських рішень. Водночас така залежність від інформаційних технологій супроводжується зростанням кількості цифрових ризиків та кіберзагроз, що можуть негативно впливати на фінансовий стан, ділову репутацію та економічну стійкість підприємства.

У процесі цифровізації підприємства все частіше стикаються з такими загрозами, як кібератаки, витоки конфіденційної інформації, несанкціонований доступ до даних, шкідливе програмне забезпечення, фішингові атаки та блокування інформаційних систем. Особливо небезпечними є атаки на

критичну цифрову інфраструктуру підприємств, оскільки вони можуть призвести до значних фінансових втрат, порушення операційної діяльності та втрати довіри клієнтів і партнерів.

Питання цифрової безпеки набувають особливої актуальності для підприємств телекомунікаційної галузі, діяльність яких безпосередньо пов’язана з передачею, збереженням та обробкою великих обсягів інформації. Функціонування таких підприємств потребує високого рівня захисту інформаційних ресурсів, стабільної роботи мережевої інфраструктури та постійного моніторингу кіберзагроз. За умов недостатнього рівня цифрового захисту навіть короткочасне порушення роботи інформаційних систем може спричинити значні економічні збитки та негативно вплинути на конкурентні позиції підприємства на ринку.

Важливим чинником посилення загроз цифровій безпеці для українських підприємств стали умови воєнного стану та активізація кібератак на державний і приватний сектори економіки. Війна суттєво підвищила рівень кіберризиків для бізнесу, оскільки інформаційна інфраструктура підприємств стала однією з цілей кібервпливу. У таких умовах питання забезпечення цифрової безпеки виходить за межі технічного захисту інформації та перетворюється на стратегічний елемент системи управління підприємством.

Цифрова безпека сьогодні є важливою складовою економічної стійкості підприємства, оскільки забезпечує захист інформаційних ресурсів, безперервність бізнес-процесів, стабільність фінансової діяльності та збереження конкурентних переваг. Ефективне управління цифровою безпекою дозволяє підприємствам своєчасно реагувати на кіберзагрози, мінімізувати можливі втрати та адаптуватися до змін зовнішнього середовища. Саме тому дослідження сутності цифрової безпеки та її ролі у забезпеченні економічної стійкості підприємства є важливим напрямом сучасних наукових досліджень у сфері менеджменту та економічної безпеки.

Цифровізація діяльності сучасних підприємств передбачає формування складного цифрового середовища, яке об’єднує інформаційні ресурси,

технологічну інфраструктуру, персонал та бізнес-процеси підприємства. Ефективність функціонування такого середовища значною мірою залежить від рівня захищеності його складових та здатності підприємства своєчасно реагувати на цифрові загрози. Основні складові цифрового середовища підприємства наведено на рисунку 1.1 [1, с. 5].

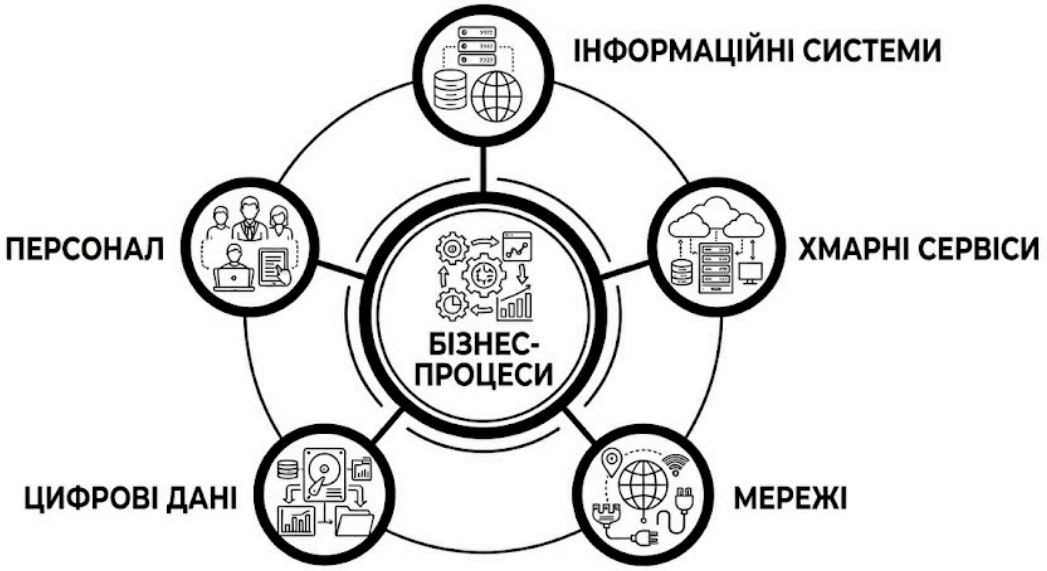

Рисунок 1.1 – Основні складові цифрового середовища підприємства

Примітка. Авторська розробка.

Як видно з рисунка 1.1, цифрове середовище підприємства є комплексною системою взаємопов’язаних елементів, функціонування яких забезпечує реалізацію основних бізнес-процесів підприємства. Порушення роботи хоча б однієї зі складових може негативно вплинути на стабільність діяльності підприємства, спричинити фінансові втрати та зниження рівня економічної стійкості. Саме тому забезпечення цифрової безпеки повинно охоплювати всі елементи цифрового середовища підприємства та здійснюватися на системній основі.

У сучасній науковій літературі поняття цифрової безпеки підприємства розглядається з різних позицій залежно від сфери дослідження, рівня цифровізації економіки та підходів до управління інформаційними ресурсами. З

розвитком цифрових технологій та поширенням кіберзагроз відбулося суттєве розширення змісту поняття цифрової безпеки: від технічного захисту інформації до комплексної системи управління ризиками та забезпечення економічної стійкості підприємства.

Дослідження наукових підходів свідчить про те, що більшість авторів пов'язує цифрову безпеку із захистом інформаційних ресурсів, інформаційних систем та цифрової інфраструктури підприємства. Водночас сучасні наукові концепції дедалі частіше розглядають цифрову безпеку як складову стратегічного управління підприємством, що забезпечує його стабільне функціонування в умовах цифрової економіки.

На думку Брюса Шнайєра, цифрова безпека повинна розглядатися не лише як технологічний процес, а й як складова системи управління ризиками підприємства. Автор наголошує на необхідності постійного моніторингу загроз, оцінювання ризиків та адаптації системи безпеки до змін зовнішнього середовища [2, с. 41].

У свою чергу EC-Council University визначає цифрову безпеку як комплексну практику захисту інформації від несанкціонованого доступу чи знищення, яка реалізується через багаторівневу систему захисту мереж, програмних додатків, кінцевих пристроїв та хмарних середовищ. Дана установа акцентує увагу на тому, що цифрова стійкість досягається завдяки інтеграції засобів автентифікації та постійному моніторингу вразливостей, що є критично важливим для забезпечення конфіденційності й цілісності даних у таких стратегічних галузях, як медицина, фінанси та ритейл. Таким чином, технологічні інструменти захисту стають практичним механізмом для реалізації стратегії управління ризиками, адаптуючись до нових викликів цифрової епохи, зокрема загроз у сфері штучного інтелекту [3].

Отже, під цифровою безпекою підприємства доцільно розуміти комплекс організаційних, інформаційних, технологічних та управлінських заходів, спрямованих на забезпечення захисту цифрових ресурсів, інформаційних систем, мережевої інфраструктури та бізнес-процесів підприємства від

внутрішніх і зовнішніх кіберзагроз з метою забезпечення стабільного функціонування, безперервності діяльності та економічної стійкості підприємства.

На відміну від традиційних підходів, які розглядають цифрову безпеку переважно як технічний захист інформації, сучасний підхід передбачає інтеграцію цифрової безпеки у систему стратегічного управління підприємством. У такому контексті цифрова безпека виступає не лише інструментом мінімізації кіберризиків, а й важливим чинником підтримання конкурентоспроможності, фінансової стабільності та адаптивності підприємства до змін зовнішнього середовища.

В умовах цифрової трансформації підприємства цифрова безпека повинна охоплювати всі ключові елементи цифрового середовища, включаючи інформаційні системи, цифрові дані, хмарні технології, корпоративні мережі, програмне забезпечення та людський фактор. Особливого значення набуває здатність підприємства своєчасно виявляти кіберзагрози, оцінювати рівень цифрових ризиків та впроваджувати ефективні механізми реагування на можливі інциденти інформаційної безпеки.

Цифрову безпеку доцільно розглядати як невід'ємну складову системи управління сучасним підприємством, яка забезпечує захист його цифрового середовища, підтримує стабільність бізнес-процесів та сприяє забезпеченню економічної стійкості в умовах зростання рівня цифрових загроз.

У сучасних умовах цифровізації економіки забезпечення цифрової безпеки є одним із ключових чинників підтримання економічної стійкості підприємства. Активне використання інформаційних технологій, автоматизація бізнес-процесів, розвиток електронної комерції та цифрових сервісів значно підвищують залежність підприємств від стабільного функціонування цифрового середовища. Водночас зростання кількості кіберзагроз створює додаткові ризики для фінансової діяльності, ділової репутації та конкурентоспроможності підприємств.

Економічна стійкість підприємства характеризується його здатністю забезпечувати стабільне функціонування, ефективно використовувати ресурси, адаптуватися до змін зовнішнього середовища та протидіяти негативним впливам внутрішніх і зовнішніх факторів. Одним із таких факторів у сучасних умовах виступають цифрові ризики та кіберзагрози, які можуть суттєво впливати на результати господарської діяльності підприємства.

Значний вплив кіберзагроз простежується насамперед на фінансових результатах діяльності підприємства. Кібератаки можуть спричиняти прямі фінансові втрати через викрадення коштів, блокування інформаційних систем, втрату даних або припинення операційної діяльності. Окрім прямих збитків, підприємства часто несуть додаткові витрати на відновлення цифрової інфраструктури, модернізацію систем захисту, проведення аудиту безпеки та ліквідацію наслідків кіберінцидентів. Особливо небезпечними є атаки типу ransomware, які блокують доступ до інформаційних ресурсів підприємства та можуть призводити до повної зупинки окремих бізнес-процесів [4].

Рисунок 1.2 – Наслідки кібератак: вплив на бізнес [4]

Важливим наслідком недостатнього рівня цифрової безпеки є погіршення ділової репутації підприємства. Витоки конфіденційної інформації,

компрометація персональних даних клієнтів або порушення стабільності цифрових сервісів негативно впливають на рівень довіри споживачів, партнерів та інвесторів. У сучасних умовах інформація є одним із найцінніших ресурсів підприємства, тому її втрата або несанкціоноване поширення може спричинити суттєві репутаційні ризики та зниження ринкових позицій підприємства.

Особливо актуальним це питання є для підприємств телекомунікаційної галузі, діяльність яких безпосередньо пов'язана з обробкою значних обсягів даних та забезпеченням безперервності цифрових комунікацій. Для таких підприємств рівень цифрової безпеки безпосередньо впливає на рівень довіри клієнтів та конкурентоспроможність на ринку.

Кіберзагрози також мають суттєвий вплив на конкурентоспроможність підприємства. У сучасному бізнес-середовищі здатність підприємства забезпечувати високий рівень захисту цифрових ресурсів стає важливою конкурентною перевагою. Підприємства, які впроваджують сучасні системи цифрової безпеки, мають вищий рівень довіри з боку клієнтів і партнерів, можуть ефективніше розвивати цифрові сервіси та швидше адаптуватися до змін ринку. Натомість недостатній рівень цифрового захисту може стримувати розвиток підприємства, обмежувати можливості цифрової трансформації та негативно впливати на його ринкові позиції.

Одним із ключових аспектів впливу цифрової безпеки на економічну стійкість підприємства є забезпечення безперервності бізнес-процесів. Порушення роботи інформаційних систем, серверів або цифрових платформ може призвести до тимчасового припинення діяльності підприємства, зниження продуктивності праці та втрати частини клієнтів. У сучасних умовах навіть короткочасний збій у роботі цифрової інфраструктури може мати значні економічні наслідки, особливо для підприємств, діяльність яких залежить від цифрових комунікацій та онлайн-сервісів.

Забезпечення цифрової безпеки дозволяє підприємству підтримувати стабільність діяльності, знижувати рівень ризиків та формувати основу для довгострокового розвитку. Ефективна система управління цифровою безпекою

забезпечує своєчасне виявлення кіберзагроз, мінімізацію можливих втрат та швидке реагування на інциденти інформаційної безпеки. Саме тому цифрова безпека сьогодні розглядається не лише як технічна функція, а й як важливий елемент системи стратегічного управління підприємством.

Взаємозв'язок цифрової безпеки та економічної стійкості підприємства доцільно подати схематично на рисунку 1.3.

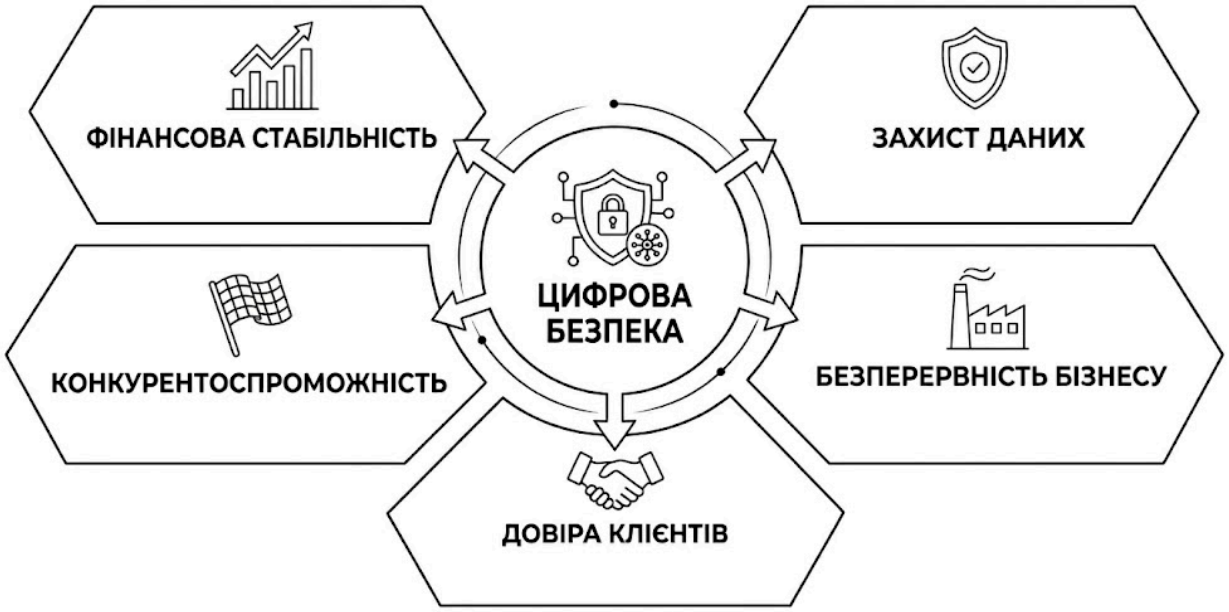

Рисунок 1.3 – Вплив цифрової безпеки на економічну стійкість підприємства

Примітка. Авторська розробка.

Як видно з рисунка 1.3, цифрова безпека є важливим елементом забезпечення економічної стійкості підприємства, оскільки впливає на ключові напрями його діяльності. Належний рівень цифрового захисту сприяє підтриманню фінансової стабільності, забезпечує безперервність бізнес-процесів, захищає інформаційні ресурси підприємства та формує довіру клієнтів і партнерів. У сучасних умовах цифрової економіки ефективне управління цифровою безпекою є необхідною умовою стабільного функціонування та довгострокового розвитку підприємства.

Проте реалізація цього потенціалу стає дедалі складнішою через стрімку еволюцію зовнішніх та внутрішніх викликів. Для формування дієвої системи захисту необхідно чітко ідентифікувати сучасні цифрові загрози, які безпосередньо атакують згадані вектори стійкості. Як продемонстровано на рисунку 1.4, спектр інструментів кіберзлочинців є надзвичайно широким — від маніпуляцій людською психологією до високотехнологічних атак на інфраструктуру.

Рисунок 1.4 – Основні кіберзагрози для бізнесу [5]

Однією з найбільш деструктивних загроз для фінансової стабільності є віруси-вимагачі. За даними звітів IBM Security, цей тип атак спричиняє не лише прямі збитки через вимоги викупу, а й колосальні непрямі втрати внаслідок зупинки операційної діяльності. У поєднанні з DDoS-атаками, які спрямовані на перевантаження мережевих ресурсів, вони здатні повністю паралізувати цифрові сервіси, що є критичним для безперервності бізнесу.

Особливе місце в ієрархії ризиків посідають фішинг та методи соціальної інженерії. Ці загрози апелюють до людського фактора, який залишається найслабшою ланкою в системі безпеки будь-якого підприємства. За статистикою

Microsoft Security, понад 80% успішних зламів починаються саме з отримання доступу до облікових даних співробітників через обман. Це відкриває шлях до подальшого впровадження шкідливого ПЗ та несанкціонованого витоку даних, що миттєво руйнує довіру клієнтів і репутацію бренду.

У контексті діяльності великих інфраструктурних об'єктів, зокрема атак на телеком-компанії, загрози набувають масштабу національної безпеки. Прикладом є використання складних атак через ланцюги постачання, коли вразливість у програмному забезпеченні одного підрядника стає "вхідними воротами" до систем тисяч корпоративних клієнтів. Додатковою складністю стають новітні методи Deepfake-шахрайства та атаки на хмарні сервіси й IoT-пристрої, які розширюють периметр атаки до неконтрольованих меж.

Ідентифікація та аналіз цих загроз є першим кроком до побудови адаптивної бізнес-моделі, де цифрова безпека виступає не просто технічною функцією, а стратегічним бар'єром проти економічної дестабілізації. Підсумовуючи вищевикладене, можна зробити висновок, що цифрова безпека в сучасних умовах трансформувалася з вузькоспеціалізованого технічного завдання у фундаментальну складову економічної стійкості підприємства. Вона забезпечує не лише цілісність даних, а й безперервність ключових бізнес-процесів, фінансову стабільність та збереження ринкових позицій.

Проблема вразливості організацій суттєво посилюється через тотальну цифровізацію, яка, розширюючи можливості бізнесу, водночас створює нові вектори для потенційних атак. Для українських підприємств, зокрема таких технологічних гігантів, як ПрАТ «Київстар», цей виклик загострюється умовами воєнного стану, де кіберзагрози стають інструментом прямого деструктивного впливу на інфраструктуру.

Ефективне управління цифровою безпекою стає невід’ємною частиною загальної системи стратегічного управління. Саме здатність організації оперативно ідентифікувати, оцінювати та нейтралізувати цифрові ризики визначає її спроможність адаптуватися до змін агресивного зовнішнього середовища та підтримувати сталий розвиток у довгостроковій перспективі.

1.2. Сутність, етапи та основні характеристики процесу управління цифровою безпекою підприємства

Процес управління цифровою безпекою підприємства є важливою складовою системи сучасного менеджменту та спрямований на забезпечення захисту цифрового середовища підприємства від внутрішніх і зовнішніх загроз. В умовах активної цифровізації господарської діяльності підприємства дедалі більше залежать від стабільного функціонування інформаційних систем, цифрових платформ, корпоративних мереж та електронних каналів комунікації. Саме тому ефективне управління цифровою безпекою набуває стратегічного значення та стає необхідною умовою забезпечення економічної стійкості підприємства.

На відміну від традиційного технічного підходу до захисту інформації, сучасний процес управління цифровою безпекою передбачає комплексне поєднання організаційних, управлінських, інформаційних та технологічних заходів. Такий процес охоплює планування, організацію, реалізацію, контроль та постійне вдосконалення механізмів цифрового захисту підприємства відповідно до змін зовнішнього середовища та появи нових кіберзагроз.

У науковій літературі процес управління цифровою безпекою розглядається як безперервний управлінський цикл, спрямований на своєчасне виявлення цифрових ризиків, оцінювання рівня загроз, впровадження заходів захисту та забезпечення стабільності функціонування підприємства. Основною метою такого процесу є мінімізація негативного впливу кіберзагроз на діяльність підприємства та підтримання належного рівня захищеності цифрової інфраструктури [6, с. 113].

Важливою особливістю процесу управління цифровою безпекою є його інтеграція у загальну систему менеджменту підприємства. У сучасних умовах цифрова безпека не може функціонувати ізольовано від інших напрямів управління, оскільки вона безпосередньо впливає на фінансову стабільність,

операційну діяльність, кадрову політику, систему управління ризиками та стратегічний розвиток підприємства. Саме тому процес управління цифровою безпекою повинен бути узгоджений із загальною стратегією розвитку підприємства та інтегрований у систему прийняття управлінських рішень.

Ефективне управління цифровою безпекою передбачає реалізацію послідовного управлінського циклу, який охоплює аналіз поточного стану цифрового середовища, виявлення вразливостей, розробку політик безпеки, впровадження технічних заходів захисту, навчання персоналу, контроль ефективності системи захисту та постійне вдосконалення механізмів реагування на кіберінциденти. Безперервність такого процесу обумовлена постійною зміною цифрових загроз та необхідністю швидкої адаптації підприємства до нових умов функціонування.

Рисунок 1.5 – Процес побудови системи кіберзахисту [5]

Одним із ключових етапів процесу управління цифровою безпекою є проведення аудиту кібербезпеки підприємства. Аудит дозволяє оцінити рівень захищеності цифрової інфраструктури, виявити наявні вразливості та визначити потенційні ризики для діяльності підприємства. На основі результатів аудиту формуються політики інформаційної безпеки та визначаються напрями вдосконалення системи цифрового захисту.

Важливе значення у процесі управління цифровою безпекою має формування внутрішніх політик та процедур інформаційної безпеки. Вони визначають правила користування інформаційними ресурсами, порядок доступу до цифрових систем, відповідальність працівників та механізми реагування на кіберінциденти. Наявність чітко визначених політик дозволяє знизити рівень цифрових ризиків та підвищити ефективність управління цифровою безпекою підприємства.

Не менш важливим елементом процесу управління цифровою безпекою є побудова багаторівневого технічного захисту, який включає використання антивірусного програмного забезпечення, фаєрволів, систем резервного копіювання, шифрування даних та багатофакторної автентифікації. Комплексне використання технічних засобів захисту дозволяє мінімізувати ризик несанкціонованого доступу до інформаційних ресурсів підприємства та забезпечити безперервність функціонування цифрової інфраструктури [7, с. 15].

Окрему роль у процесі управління цифровою безпекою відіграє людський фактор. Значна частина кіберінцидентів виникає через помилки персоналу, використання ненадійних паролів або недотримання правил кібергігієни. Саме тому важливою складовою управлінського процесу є регулярне навчання працівників, проведення тренінгів із цифрової безпеки та формування культури безпечного використання цифрових технологій.

Крім того, ефективне управління цифровою безпекою передбачає створення системи резервного копіювання даних та розробку плану реагування на кіберінциденти. Це дозволяє підприємству оперативно відновлювати роботу інформаційних систем, мінімізувати наслідки кібератак та підтримувати стабільність бізнес-процесів навіть в умовах виникнення цифрових загроз.

Важливою складовою процесу управління цифровою безпекою підприємства є вибір ефективної моделі управління, яка повинна відповідати особливостям діяльності підприємства, рівню цифровізації бізнес-процесів, масштабам інформаційної інфраструктури та характеру кіберзагроз. У сучасних умовах підприємства використовують різні моделі управління цифровою

безпекою, що відрізняються за структурою управління, способами реагування на загрози та рівнем інтеграції у систему менеджменту підприємства.

Однією з найбільш поширених моделей є централізоване управління цифровою безпекою. Такий підхід передбачає концентрацію основних функцій управління, контролю та прийняття рішень у межах одного структурного підрозділу або спеціалізованого центру кібербезпеки. Централізована модель забезпечує єдину політику цифрової безпеки, спрощує контроль за інформаційними ресурсами та дозволяє швидше координувати дії у разі виникнення кіберінцидентів. Особливо ефективною така модель є для великих підприємств із розгалуженою цифровою інфраструктурою та високими вимогами до захисту інформації.

Водночас централізоване управління має певні недоліки, серед яких високий рівень залежності від центрального підрозділу, складність швидкого реагування на локальні загрози та значні витрати на підтримання системи управління. У деяких випадках надмірна централізація може знижувати гнучкість управлінських рішень та уповільнювати процес реагування на нові цифрові ризики [8, с. 99].

Альтернативним підходом є децентралізоване управління цифровою безпекою, при якому окремі функції захисту інформаційних ресурсів розподіляються між різними структурними підрозділами підприємства. Така модель забезпечує більшу гнучкість управління та дозволяє швидше реагувати на специфічні загрози в окремих напрямах діяльності підприємства. Децентралізований підхід часто використовується у великих міжнародних компаніях або підприємствах із територіально розподіленою структурою управління [9].

Разом із тим децентралізована модель може створювати труднощі у координації дій між підрозділами, призводити до дублювання функцій та ускладнювати формування єдиної політики цифрової безпеки. За відсутності належної координації між структурними підрозділами зростає ризик виникнення прогалин у системі цифрового захисту підприємства.

За характером реагування на кіберзагрози виділяють проактивну та реактивну моделі управління цифровою безпекою. Проактивне управління передбачає завчасне виявлення потенційних загроз, постійний моніторинг цифрового середовища, аналіз ризиків та впровадження превентивних заходів захисту. Основною метою проактивного підходу є попередження виникнення кіберінцидентів та мінімізація можливих негативних наслідків для діяльності підприємства.

Проактивна модель вважається найбільш ефективною в умовах сучасного цифрового середовища, оскільки дозволяє підприємству своєчасно адаптувати систему безпеки до нових загроз, підвищувати рівень захищеності інформаційної інфраструктури та забезпечувати безперервність бізнес-процесів. Реалізація такого підходу потребує використання сучасних систем моніторингу, аналізу цифрових ризиків, автоматизованих засобів виявлення загроз та постійного вдосконалення політик безпеки.

На відміну від проактивної моделі, реактивне управління цифровою безпекою базується переважно на реагуванні після виникнення кіберінциденту. У такому випадку основна увага приділяється ліквідації наслідків кібератак, відновленню інформаційних систем та мінімізації збитків. Реактивний підхід є менш ефективним, оскільки підприємство реагує вже після виникнення проблеми, що може призводити до значних фінансових втрат, порушення стабільності діяльності та погіршення ділової репутації [10].

Крім того, у системі управління цифровою безпекою виділяють стратегічне та оперативне управління. Стратегічне управління орієнтоване на довгострокове планування розвитку системи цифрової безпеки, інтеграцію цифрового захисту у загальну стратегію підприємства та формування політики управління цифровими ризиками. Воно передбачає визначення основних напрямів розвитку системи безпеки, розподіл ресурсів та формування механізмів адаптації до змін зовнішнього середовища [11].

Оперативне управління цифровою безпекою спрямоване на поточний контроль функціонування системи захисту, моніторинг цифрового середовища,

реагування на кіберінциденти та забезпечення стабільної роботи інформаційної інфраструктури підприємства. Саме оперативний рівень управління забезпечує практичну реалізацію заходів цифрової безпеки у повсякденній діяльності підприємства.

Для більш детального порівняння основних моделей управління цифровою безпекою доцільно узагальнити їх характеристики у таблиці 1.3.

Таблиця 1.1 – Порівняльна характеристика моделей управління цифровою безпекою

Модель	Переваги	Недоліки
Централізована	Єдина політика безпеки, високий рівень контролю	Менша гнучкість, значні витрати
Децентралізована	Швидке реагування на локальні загрози, гнучкість	Складність координації, можливе дублювання функцій
Проактивна	Попередження загроз, постійний моніторинг ризиків	Високі витрати на впровадження та підтримку
Реактивна	Швидке усунення наслідків інцидентів	Реагування після виникнення загрози
Стратегічна	Довгострокове планування та інтеграція у систему менеджменту	Потребує значних ресурсів і часу
Оперативна	Постійний контроль та швидке реагування	Орієнтація переважно на поточні завдання

Примітка. Авторська розробка.

Вибір моделі управління цифровою безпекою залежить від масштабів діяльності підприємства, рівня цифровізації бізнес-процесів та специфіки цифрових ризиків. У сучасних умовах найбільш ефективним вважається поєднання проактивного, стратегічного та централізованого підходів, що дозволяє забезпечити високий рівень захищеності цифрового середовища підприємства та підтримувати його економічну стійкість.

Щодо стандартів, одним із найбільш поширених міжнародних стандартів у сфері управління інформаційною та цифровою безпекою є стандарт ISO/IEC 27001. Даний стандарт визначає вимоги до створення, впровадження, підтримки та постійного вдосконалення системи управління інформаційною безпекою

підприємства. Основною метою ISO/IEC 27001 є забезпечення конфіденційності, цілісності та доступності інформаційних ресурсів підприємства. Використання цього стандарту дозволяє підприємствам систематизувати процеси управління цифровою безпекою, підвищити рівень контролю за інформаційними ризиками та забезпечити відповідність міжнародним вимогам у сфері кіберзахисту [12].

Важливе значення у сфері цифрової безпеки також має методологія NIST, яка широко використовується у міжнародній практиці для управління кіберризиками. Framework NIST Cybersecurity Framework базується на п’яти ключових функціях: ідентифікація загроз, захист, виявлення інцидентів, реагування та відновлення. Перевагою підходу NIST є його гнучкість та можливість адаптації до особливостей діяльності підприємства незалежно від галузі чи масштабів діяльності [13].

Сучасні системи управління цифровою безпекою також активно використовують risk-based approach — ризик-орієнтований підхід. Його сутність полягає у визначенні найбільш критичних цифрових ризиків для підприємства та концентрації ресурсів на їх мінімізації. Такий підхід дозволяє підприємствам ефективніше розподіляти фінансові, кадрові та технічні ресурси, приділяючи першочергову увагу найбільш небезпечним загрозам для діяльності підприємства [14].

Ризик-орієнтований підхід передбачає постійний аналіз цифрового середовища, оцінювання ймовірності виникнення кіберзагроз та визначення потенційних наслідків для бізнес-процесів підприємства. Особливістю такого підходу є його адаптивність, оскільки система цифрової безпеки постійно вдосконалюється відповідно до змін зовнішнього середовища та появи нових кіберризиків.

Отже, процес управління цифровою безпекою підприємства є комплексним і безперервним процесом, який охоплює організаційні, інформаційні, технічні та управлінські заходи, спрямовані на забезпечення захисту цифрового середовища підприємства. Проведене дослідження

дозволило визначити основні етапи процесу управління цифровою безпекою, охарактеризувати моделі управління та проаналізувати сучасні методичні підходи й міжнародні стандарти у сфері кіберзахисту.

Встановлено, що найбільш ефективним у сучасних умовах є проактивний підхід до управління цифровою безпекою, який передбачає постійний моніторинг цифрового середовища, своєчасне виявлення ризиків та впровадження превентивних заходів захисту. Такий підхід дозволяє мінімізувати негативний вплив кіберзагроз на діяльність підприємства та забезпечувати безперервність бізнес-процесів.

Доведено, що ефективне управління цифровою безпекою повинно бути інтегроване у загальну систему менеджменту підприємства та узгоджене зі стратегічними цілями його розвитку. Використання міжнародних стандартів ISO/IEC 27001, методології NIST та ризик-орієнтованого підходу сприяє підвищенню рівня цифрового захисту підприємства, зміцненню його економічної стійкості та підвищенню конкурентоспроможності в умовах цифрової економіки.

1.3. Світовий досвід управління цифровою безпекою підприємств

У сучасних умовах цифрової трансформації економіки питання управління цифровою безпекою набуває глобального значення. Активний розвиток цифрових технологій, поширення хмарних сервісів, автоматизація бізнес-процесів та використання штучного інтелекту суттєво підвищують залежність підприємств від цифрової інфраструктури. Водночас це спричиняє зростання кількості кіберзагроз та масштабів кібератак, що змушує держави та міжнародні компанії постійно вдосконалювати системи управління цифровою безпекою.

Світовими тенденціями розвитку цифрової безпеки є посилення уваги до захисту даних, формування систем цифрової стійкості підприємств, збільшення інвестицій у кіберзахист та впровадження проактивних моделей управління

кіберризиками. Значний вплив на розвиток цифрової безпеки має також використання технологій штучного інтелекту та машинного навчання, які дозволяють автоматизувати процеси виявлення загроз, аналізу ризиків та реагування на кіберінциденти.

Упродовж останніх років світові витрати на кібербезпеку демонструють стабільне зростання. Це обумовлено збільшенням кількості цифрових загроз, розвитком дистанційної роботи, активним використанням хмарних технологій та необхідністю забезпечення захисту критичної цифрової інфраструктури. Особливо актуальним питання цифрової безпеки стало після зростання кількості кібератак на великі корпорації, телекомунікаційні компанії, банки та державні установи.

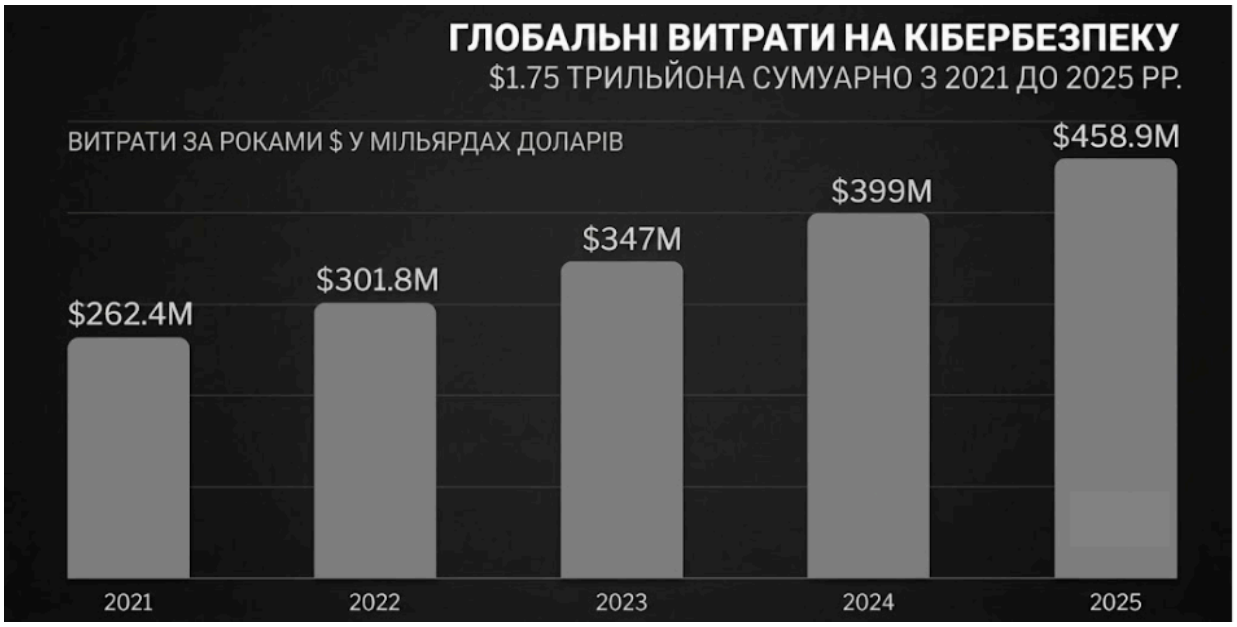

Рисунок 1.6 – Світові витрати на кібербезпеку [15]

Як видно з рисунка 1.6, світові витрати на кібербезпеку щороку зростають, що свідчить про підвищення ролі цифрового захисту у забезпеченні стабільності діяльності підприємств та економічної безпеки держав.

Однією з країн-лідерів у сфері управління цифровою безпекою є Сполучені Штати Америки. Американська модель базується на risk-based approach — ризик-орієнтованому підході, який передбачає постійне оцінювання

цифрових ризиків та адаптацію систем захисту до нових загроз. Важливу роль у США відіграє методологія NIST Cybersecurity Framework, яка використовується як державними структурами, так і приватними компаніями. Значна увага приділяється розвитку партнерства між державою та бізнесом у сфері кібербезпеки, а також підтримці інноваційних технологій цифрового захисту [16, с. 1].

Країни Європейського Союзу реалізують переважно регуляторний підхід до управління цифровою безпекою. Одним із ключових елементів є Загальний регламент захисту даних GDPR, який встановлює високі вимоги до захисту персональних даних та відповідальності підприємств за їх обробку [17]. Важливе значення також має директива NIS2, спрямована на забезпечення високого рівня кіберстійкості критичної інфраструктури та цифрових сервісів у країнах ЄС. Європейська модель орієнтована на комплексне регулювання цифрового середовища та підвищення рівня цифрової стійкості підприємств [18].

Особливий інтерес у сфері цифрової безпеки становить досвід Ізраїлю, який вважається одним із світових лідерів у галузі кіберзахисту. Ізраїльська модель базується на проактивному підході до управління цифровою безпекою та активному використанні інноваційних технологій. У країні функціонують спеціалізовані кіберцентри, що забезпечують моніторинг кіберзагроз, координацію реагування на інциденти та підтримку розвитку кіберіндустрії. Значна увага приділяється співпраці між державою, бізнесом та науковими установами у сфері кібербезпеки [19].

Важливим прикладом ефективного управління цифровою безпекою є також Японія, яка активно впроваджує концепцію цифрової стійкості та захисту критичної інформаційної інфраструктури. Особлива увага приділяється розвитку систем кібермоніторингу, автоматизації процесів реагування на кіберзагрози та підготовці висококваліфікованих фахівців у сфері цифрової безпеки [20].

Також важливий практичний досвід у сфері управління цифровою безпекою демонструють провідні міжнародні компанії, діяльність яких безпосередньо пов’язана з обробкою значних обсягів цифрових даних та функціонуванням глобальної інформаційної інфраструктури. Сучасні корпорації активно впроваджують проактивні моделі кіберзахисту, автоматизовані системи моніторингу загроз та багаторівневі механізми захисту цифрового середовища.

Одним із лідерів у сфері цифрової безпеки є Microsoft , яка активно використовує концепцію Zero Trust, що базується на принципі постійної перевірки користувачів та пристроїв незалежно від їх місця перебування у мережі. Компанія впроваджує багатофакторну автентифікацію, AI-моніторинг кіберзагроз та автоматизовані системи реагування на інциденти інформаційної безпеки. Значна увага приділяється використанню штучного інтелекту для аналізу аномальної активності та прогнозування можливих кібератак [21].

Активно розвиває системи цифрового захисту і Google , яка використовує власні центри моніторингу безпеки, технології машинного навчання та комплексні механізми захисту хмарної інфраструктури. Компанія реалізує концепцію BeyondCorp, що є однією з моделей Zero Trust Architecture, орієнтованої на захист корпоративних ресурсів незалежно від місця підключення користувача [22].

Важливий досвід у сфері управління цифровою безпекою мають також телекомунікаційні компанії, зокрема Vodafone . Компанія використовує комплексний підхід до цифрового захисту, який включає SOC-центри, системи моніторингу мережевого трафіку, захист хмарної інфраструктури та управління цифровими ризиками. Для телекомунікаційних компаній питання цифрової безпеки є особливо важливим через необхідність забезпечення безперервності зв’язку та захисту персональних даних клієнтів [23].

Серед світових лідерів у сфері цифрової безпеки особливе місце посідає Amazon, яка у 2026 році розпочала масштабну адаптацію своїх сервісів до стандарту CMMC 2.0 (Cybersecurity Maturity Model Certification). Ця ініціатива запроваджує посилені протоколи захисту для організацій, що працюють із

Міністерством оборони США, зокрема в аерокосмічній та медичній сферах. Компанія інтегрує інструменти відповідності, що забезпечують багаторівневу перевірку кіберстійкості, захист чутливої інформації та автоматизований моніторинг згідно з державними вимогами. Важливим аспектом є інвестиції Amazon у розмірі 50 млрд дол. у ШІ та суперкомп'ютери, що дозволяє використовувати проактивні AI-рішення для аналізу ризиків та забезпечення безпеки в критичних секторах публічного управління [24].

Водночас в Україні питання управління цифровою безпекою підприємств набуває особливої актуальності в умовах повномасштабної війни та постійного зростання кількості кібератак на критичну інфраструктуру, телекомунікаційні компанії, банківський сектор та державні установи. Українські підприємства функціонують в умовах підвищених цифрових ризиків, що потребує посилення систем кіберзахисту та впровадження сучасних моделей управління цифровою безпекою.

Серед основних проблем розвитку цифрової безпеки в Україні можна виділити недостатній рівень фінансування заходів кіберзахисту, обмеженість технічних ресурсів, нестачу кваліфікованих фахівців у сфері кібербезпеки та недостатню інтеграцію систем управління цифровими ризиками у загальну систему менеджменту підприємств. Крім того, значна частина українських підприємств використовує переважно реактивний підхід до кіберзахисту, який орієнтований на реагування після виникнення інциденту, а не на його попередження [25].

Висновки до розділу 1

1. Обґрунтовано теоретичні засади дослідження, згідно з якими цифрова безпека в сучасних умовах трансформувалася з вузькоспеціалізованого технічного завдання у фундаментальну складову економічної стійкості підприємства. Визначено, що цифрова безпека є комплексним механізмом, який інтегрується в систему стратегічного управління та забезпечує захист

цифрового середовища, підтримує безперервність бізнес-процесів, фінансову стабільність, ділову репутацію та конкурентоспроможність організації в умовах зростання кіберзагроз та дії воєнного стану.

2. Досліджено процес управління цифровою безпекою підприємства як послідовний управлінський цикл, що охоплює аудит кібербезпеки, ідентифікацію вразливостей, формування внутрішніх політик безпеки, побудову багаторівневого технічного захисту та постійний моніторинг інцидентів. Доведено, що найбільш ефективним у сучасних умовах є поєднання проактивного підходу із ризик-орієнтованими моделями та міжнародними стандартами, що дозволяє адаптувати систему захисту до динамічних змін цифрового середовища.

3. Здійснено аналіз міжнародного досвіду та світових тенденцій, який засвідчив стрімке зростання глобальних витрат на кіберзахист та активне впровадження концепцій Zero Trust і відповідності суворим державним протоколам безпеки, таким як CMMC 2.0. Виявлено, що провідні країни поєднують ризик-орієнтовані та жорсткі регуляторні підходи , а ключовим вектором розвитку систем кіберстійкості стає масштабне фінансування та інтеграція технологій штучного интеллекту і машинного навчання для автоматизації виявлення та нейтралізації загроз.

РОЗДІЛ 2. АНАЛІЗ ПРОЦЕСУ УПРАВЛІННЯ ЦИФРОВОЮ БЕЗПЕКОЮ ПРАТ «КИЇВСТАР»

2.1. Аналіз об’єкта та суб’єкта системи управління ПрАТ «Київстар»

ПрАТ «Київстар» є одним із найбільших операторів телекомунікаційного ринку України та займає провідні позиції у сфері надання послуг мобільного зв’язку, інтернету, цифрових сервісів і телекомунікаційної інфраструктури. Компанія функціонує як важливий елемент цифрового середовища держави та забезпечує стабільне функціонування значної частини інформаційно-комунікаційних процесів в Україні. У сучасних умовах цифрової трансформації економіки та зростання кіберзагроз діяльність підприємства набуває особливого значення, оскільки телекомунікаційна сфера є однією з ключових складових критичної інфраструктури держави.

ПрАТ «Київстар» зареєстроване 03 вересня 1997 року та здійснює свою діяльність у формі приватного акціонерного товариства. Юридична адреса підприємства: 03113, м. Київ, вул. Дегтярівська, буд. 53. Ідентифікаційний код юридичної особи за ЄДРПОУ — 21673832. Статутний капітал підприємства становить 654 763 100 грн. Керівником підприємства є Комаров Олександр Валерійович. Компанія має багаторічний досвід функціонування на ринку телекомунікацій та сформувала одну з найбільш розгалужених цифрових інфраструктур в Україні [26].

Основним видом діяльності ПрАТ «Київстар» відповідно до КВЕД є 61.20 «Діяльність у сфері безпроводового електрозв’язку». Даний вид діяльності охоплює надання послуг мобільного зв’язку, передачі даних, мобільного інтернету та інших цифрових сервісів із використанням безпроводових технологій зв’язку. Водночас підприємство здійснює й інші види діяльності, що забезпечують комплексне функціонування телекомунікаційної системи та цифрової інфраструктури підприємства.

Серед додаткових видів економічної діяльності підприємства важливе значення мають: 61.10 «Діяльність у сфері проводового електрозв'язку», що пов'язана з наданням послуг фіксованого зв'язку та інтернету; 61.90 «Інша діяльність у сфері електрозв'язку», яка охоплює додаткові телекомунікаційні послуги; 42.22 «Будівництво споруд електропостачання та телекомунікацій», що забезпечує розвиток та модернізацію мережевої інфраструктури; 82.20 «Діяльність телефонних центрів», яка спрямована на підтримку клієнтів та інформаційне обслуговування абонентів; 63.99 «Надання інших інформаційних послуг, н.в.і.у.», що включає цифрові інформаційні сервіси та електронні рішення; 73.20 «Дослідження кон'юнктури ринку та виявлення громадської думки», що використовується для аналізу ринку телекомунікаційних послуг та поведінки споживачів.

Крім цього, підприємство здійснює діяльність у сфері продажу телекомунікаційного обладнання, комп'ютерної техніки, програмного забезпечення та електронної апаратури, що підтверджується наявністю КВЕДів 47.41, 47.42, 47.43, 46.51 та 46.52. Також підприємство виконує ремонт і технічне обслуговування обладнання зв'язку та комп'ютерної техніки відповідно до КВЕДів 95.11 та 95.12. Наявність значної кількості видів економічної діяльності свідчить про високий рівень диверсифікації діяльності підприємства та комплексний характер його цифрової екосистеми.

Компанія активно дотримується визначених корпоративних цінностей, серед яких ключове місце займають клієнтоорієнтованість, інноваційність, підприємницький підхід, співпраця та чесність. Місією підприємства є забезпечення стабільного зв'язку та підтримка населення України в умовах цифрової трансформації та кризових викликів. Особливого значення діяльність ПрАТ «Київстар» набула в умовах воєнного стану, коли безперервність функціонування телекомунікаційної інфраструктури стала важливим елементом національної безпеки та стабільності функціонування економіки країни.

Станом на червень 2025 року ПрАТ «Київстар» обслуговує понад 22,4 млн абонентів мобільного зв'язку та більш ніж 1,1 млн користувачів послуг

Домашнього Інтернету. Компанія є одним із найбільших B2C-провайдерів України та володіє найбільшою гігабітною мережею в державі. Значна увага приділяється розвитку сучасних технологій передачі даних, зокрема впровадженню технологій FTTB та GPON, що забезпечують високий рівень швидкості та стабільності інтернет-з'єднання [27].

ПрАТ «Київстар» надає широкий спектр сучасних цифрових послуг із використанням мобільних та фіксованих технологій зв'язку. Підприємство активно впроваджує технології 4G, сервіси Big Data, Cloud Solutions, рішення у сфері кіберзахисту, цифрового телебачення та інші інноваційні цифрові продукти. Одним із важливих напрямів розвитку компанії є інвестування у модернізацію телекомунікаційної інфраструктури та розвиток новітніх цифрових технологій. Упродовж 2023–2027 років підприємство планує інвестувати близько 1 млрд доларів США у розвиток телекомунікаційної галузі та цифрової інфраструктури України.

Важливе місце у структурі цифрових сервісів підприємства займає платформа «Київстар ТБ», яка є одним із лідерів українського ринку OTT TV. Платформа надає доступ до понад 430 телевізійних каналів, а також містить відеобібліотеку з більш ніж 20 тисяч фільмів, серіалів, мультфільмів та телевізійних шоу. Розвиток цифрових мультимедійних платформ свідчить про поступову трансформацію підприємства з традиційного мобільного оператора у багатофункціональну цифрову екосистему.

ПрАТ «Київстар» володіє найбільшою телекомунікаційною інфраструктурою в Україні. Компанія експлуатує понад 70,7 тисячі базових станцій та використовує власну волоконно-оптичну мережу загальною протяжністю понад 44 тис. км із пропускною спроможністю 16 Тбіт/с. Масштабність цифрової інфраструктури підприємства суттєво підвищує вимоги до забезпечення цифрової безпеки, оскільки навіть незначні порушення функціонування мережі можуть спричинити значні економічні та соціальні наслідки.

Особливу увагу підприємство приділяє питанням управління інформаційною безпекою та забезпечення якості телекомунікаційних послуг. Компанія впроваджує сучасні системи кіберзахисту, проводить постійний моніторинг цифрового середовища та використовує міжнародні підходи до управління інформаційною безпекою. Наявність сертифікованої системи управління інформаційною безпекою свідчить про високий рівень інтеграції процесів цифрового захисту у загальну систему управління підприємством.

ПрАТ «Київстар» також здійснює значний економічний вплив на розвиток держави. Компанія входить до числа найбільших платників податків України та є найбільшим платником податків у телекомунікаційній сфері. За період діяльності підприємство забезпечило понад 90 млрд грн податкових надходжень до державного бюджету та інвестувало близько 6 млрд доларів США у розвиток телекомунікаційної інфраструктури України. Такі масштаби діяльності підтверджують стратегічне значення підприємства для функціонування цифрової економіки держави.

Важливим напрямом діяльності ПрАТ «Київстар» є впровадження інноваційних технологій та модернізація телекомунікаційного ринку України. Компанія першою серед українських операторів впровадила низку технологічних рішень, зокрема послугу SMS, технологію WAP-доступу до мережі Інтернет, пакетні тарифні плани та сучасні стандарти мобільної передачі даних. Крім того, підприємство здійснило модернізацію комутаційної мережі для підтримки технологій 3G, 4G (LTE) та VoLTE, а також сприяло розвитку 4G-зв’язку в Україні шляхом добровільного перерозподілу частини радіочастотного спектра.

Умови повномасштабної війни суттєво посилили роль ПрАТ «Київстар» як стратегічно важливого підприємства. Компанія забезпечує підтримку населення та бізнесу шляхом надання безоплатних послуг зв’язку, доступу до інформаційних та освітніх ресурсів, а також підтримки критично важливих категорій населення. Підприємство активно бере участь у благодійних та

гуманітарних ініціативах, спрямованих на підтримку держави, військових, медичних закладів та постраждалого населення.

Організаційна структура управління ПрАТ «Київстар» сформована відповідно до масштабів діяльності підприємства, специфіки телекомунікаційної галузі та високого рівня цифровізації бізнес-процесів. Для підприємства характерна функціональна організаційна структура управління з елементами дивізійного та процесного підходів, що дозволяє ефективно координувати діяльність окремих напрямів, забезпечувати контроль за бізнес-процесами та оперативно реагувати на зміни зовнішнього середовища. Такий тип структури є характерним для великих телекомунікаційних компаній, діяльність яких пов’язана з управлінням складною технічною та цифровою інфраструктурою.

Особливістю організаційної структури ПрАТ «Київстар» є поєднання стратегічного управління, технічного адміністрування, розвитку цифрових сервісів та системи управління інформаційною безпекою в межах єдиного корпоративного середовища. Організаційна структура підприємства забезпечує взаємодію між адміністративними, технічними, фінансовими та інформаційними підрозділами, що є важливим фактором стабільного функціонування телекомунікаційної системи підприємства.

Важливу роль у системі корпоративного управління відіграє міжнародна структура власності підприємства. Материнською компанією ПрАТ «Київстар» є міжнародна група VEON, штаб-квартира якої розташована в Дубаї (Об’єднані Арабські Емірати). Акції VEON перебувають у вільному обігу на фондових біржах США та Європейського Союзу, а серед акціонерів компанії присутні великі міжнародні інвестиційні фонди та приватні інвестори. При цьому жоден із власників акцій не має мажоритарного пакета, що знижує ризики надмірної концентрації управлінського впливу та сприяє формуванню більш прозорої системи корпоративного управління [27].

Після початку повномасштабної війни група VEON здійснила реорганізацію структури корпоративного управління та повністю припинила

діяльність на російському ринку. Особи, які потрапили під міжнародні санкції, були виключені зі складу ради директорів групи, а їхній вплив на діяльність компанії повністю припинено. Такі рішення позитивно вплинули на міжнародну репутацію підприємства та знизили репутаційні ризики для ПрАТ «Київстар» як одного з найбільших операторів телекомунікаційного ринку України.

Безпосереднє керівництво діяльністю ПрАТ «Київстар» здійснюють Президент компанії та Наглядова рада. Президентом підприємства є Олександр Комаров, який координує стратегічний розвиток компанії, забезпечує реалізацію корпоративної політики та здійснює загальне управління бізнес-процесами підприємства. Наглядова рада компанії представлена фахівцями міжнародного рівня та включає представників України, США, країн Європейського Союзу та Туреччини, що забезпечує використання міжнародного управлінського досвіду у процесі прийняття стратегічних рішень.

Організаційна структура ПрАТ «Київстар» включає значну кількість функціональних підрозділів, діяльність яких спрямована на забезпечення стабільного функціонування підприємства та розвиток цифрової інфраструктури. Серед ключових напрямів управління важливе місце займають технічний, фінансовий, IT-напрям, управління персоналом, корпоративна стратегія, розвиток бізнесу та правове забезпечення діяльності підприємства.

Технічний напрям підприємства очолює технічний директор Володимир Лутченко, який відповідає за функціонування телекомунікаційної мережі, модернізацію інфраструктури, розвиток базових станцій та забезпечення стабільності роботи цифрових сервісів. Діяльність технічного департаменту безпосередньо пов’язана із забезпеченням безперервності функціонування цифрової інфраструктури підприємства, що є важливою складовою цифрової безпеки.

Важливе місце у структурі управління займає IT-напрям, який очолює Андрій Жуковський — директор з інформаційних технологій Київстару та директор Kyivstar.Tech. Даний підрозділ відповідає за розвиток цифрових платформ, підтримку інформаційних систем, автоматизацію бізнес-процесів,

розвиток хмарних технологій та функціонування цифрових сервісів компанії. Саме ІТ-підрозділи є основою реалізації сучасних механізмів управління цифровою безпекою, оскільки вони забезпечують функціонування систем моніторингу, захисту даних та контролю кіберризиків.

Рисунок 2.1 – Організаційна структура ПрАТ «Київстар»

Примітка. Авторська розробка.

Окрему роль у системі управління відіграють підрозділи, пов’язані із забезпеченням цифрової безпеки та корпоративного контролю. Зокрема, директорка з комплаєнсу та етики Тетяна Кирик координує процеси дотримання корпоративних стандартів, внутрішнього контролю, етичних норм та управління ризиками. В умовах зростання кіберзагроз комплаєнс-система набуває важливого значення для забезпечення інформаційної безпеки, захисту персональних даних та дотримання міжнародних вимог у сфері цифрового захисту.

Фінансове управління підприємством здійснює фінансовий директор Борис Долгушин. Фінансовий департамент відповідає за формування фінансової стратегії, управління інвестиціями, контроль витрат та забезпечення економічної стійкості підприємства. У сфері цифрової безпеки фінансовий

напрям відіграє важливу роль у забезпеченні фінансування заходів кіберзахисту, модернізації телекомунікаційної інфраструктури та впровадження новітніх цифрових технологій.

Важливою складовою організаційної структури підприємства є напрям управління персоналом та розвитку організації, який очолює Оксана Олійник. Даний підрозділ забезпечує формування кадрової політики підприємства, розвиток цифрових компетенцій працівників та організацію корпоративного навчання. Враховуючи значний вплив людського фактора на рівень цифрової безпеки, система управління персоналом безпосередньо впливає на ефективність реалізації політики кіберзахисту підприємства.

Напрями розвитку бізнесу підприємства представлені підрозділами масового та корпоративного ринку. Директор з розвитку бізнесу на масовому ринку Озан Аслан відповідає за розвиток B2C-сегменту, впровадження цифрових послуг для населення та підвищення якості клієнтського сервісу. Директор з розвитку бізнесу на корпоративному ринку, Костянтин Вечір, координує роботу із бізнес-клієнтами, цифровими рішеннями для підприємств та розвитком корпоративних телекомунікаційних сервісів.

Крім того, до структури управління входять підрозділи корпоративної стратегії, правового забезпечення та корпоративних комунікацій. Вони забезпечують стратегічне планування, юридичний супровід діяльності підприємства, управління репутаційними ризиками та інформаційну взаємодію із зовнішнім середовищем.

Для комплексної оцінки зовнішніх факторів доцільно використати PESTLE-аналіз, який дозволяє дослідити політичні, економічні, соціальні, технологічні, правові та екологічні фактори впливу на підприємство.

Для ПрАТ «Київстар» особливе значення мають політичні фактори, пов’язані з воєнним станом, загрозами кібербезпеці та державним регулюванням сфери телекомунікацій. Економічні фактори визначаються рівнем інвестицій у цифрову інфраструктуру, динамікою валютного ринку та загальним станом економіки країни. Соціальні фактори характеризуються зростанням

потреб населення у стабільному цифровому зв’язку та онлайн-сервісах. Водночас технологічні фактори пов’язані зі швидким розвитком цифрових технологій, впровадженням 4G, хмарних рішень та систем кіберзахисту.

Правові фактори для підприємства визначаються вимогами законодавства у сфері захисту інформації, телекомунікацій та персональних даних. Екологічні фактори проявляються через необхідність енергоефективного функціонування телекомунікаційної інфраструктури та забезпечення безперервності роботи обладнання в умовах кризових ситуацій.

Для оцінювання сили впливу факторів на діяльність підприємства використовується шестибальна шкала, де градація починається з 0 балів, що означає повну відсутність помітного ефекту чи необхідності врахування чинника у стратегії, та продовжується 1 балом для локальних і епізодичних мікро впливу, які не потребують реакції топ менеджменту.

Слабкий вплив оцінюється у 2 бали й передбачає лише періодичне спостереження за окремими операційними аспектами без зміни ринкової позиції, тоді як 3 бали відображають середній, системний ефект, який враховується під час ухвалення поточних рішень, але не загрожує загальній життєздатності бізнесу.

Високий ступінь детермінації у 4 бали виставляється чинникам, які безпосередньо диктують умови конкурентоспроможності й вимагають обов'язкової інтеграції адаптаційних механізмів у планування, а найвищий показник у 5 балів маркує фундаментальні, критичні чинники, що виступають головними рушіями або загрозами для майбутнього компанії, повністю визначають її стратегічні перспективи та вимагають негайних антикризових рішень і масштабних внутрішніх трансформацій.

Таблиця 2.4. PESTLE-аналіз ПрАТ «Київстар»

Політичні фактори	Вага , V	Бал , B	Добуток, P	Економічні фактори	Вага , V	Бал , B	Добуток, P	Юридичні фактори	Вага , V	Бал , B	Добуток, P
Воєнний стан та ризики кібератак	0,35	5	1,75	Інфляційні процеси та валютні ризики	0,3	4	1,2	Законодавство у сфері захисту персональних даних	0,3	5	1,5
Державне регулювання телекомунікацій	0,25	4	1	Високий рівень інвестицій у цифрові технології	0,25	5	1,25	Вимоги до кібербезпеки критичної інфраструктури	0,3	5	1,5
Інтеграція до цифрового простору ЄС	0,2	4	0,8	Зростання попиту на цифрові послуги	0,25	5	1,25	Ліцензування телекомунікаційної діяльності	0,2	4	0,8
Підтримка розвитку цифрової інфраструктури	0,2	5	1	Конкуренція на телекомунікаційному ринку	0,2	4	0,8	Міжнародні стандарти інформаційної безпеки	0,2	5	1
Середня оцінка впливу політичних факторів			4,55	Середня оцінка впливу економічних факторів факторів			4,5	Середня оцінка впливу юридичних факторів			4,8
Сила впливу політичних факторів			значний вплив	Сила впливу економічних факторів			значний вплив	Сила впливу юридичних факторів			значний вплив
Соціальні фактори	Вага , V	Бал , B	Добуток, P	Технологічні фактори	Вага , V	Бал , B	Добуток, P	Екологічні фактори	Вага , V	Бал , B	Добуток, P
Зростання потреби у цифровому зв'язку	0,35	5	1,75	Розвиток 4G та цифрових технологій	0,3	5	1,5	Енергоспоживання телеком. інфраструктури	0,35	4	1,4
Популяризація дистанційної роботи та навчання	0,25	5	1,25	Використання хмарних технологій та Big Data	0,25	5	1,25	Потреба резервного енергозабезпечення	0,3	5	1,5
Зростання вимог до якості цифрових сервісів	0,2	4	0,8	Розвиток систем кіберзахисту	0,25	5	1,25	Вплив воєнних дій на інфраструктуру	0,2	5	1
Високий рівень залежності населення від телеком.	0,2	5	1	Висока швидкість технологічних змін	0,2	4	0,8	Використання енергоефективних технологій	0,15	4	0,6
Середня оцінка впливу соціальних факторів			4,8	Середня оцінка впливу технологічних факторів			4,8	Середня оцінка впливу екологічних факторів			4,8
Сила впливу соціальних факторів			значний вплив	Сила впливу технологічних факторів			значний вплив	Сила впливу екологічних факторів			значний вплив

Примітка. Авторська розробка.

Проведений PESTLE-аналіз свідчить про те, що найбільший вплив на діяльність ПрАТ «Київстар» мають технологічні, соціальні та правові фактори. Це обумовлено високим рівнем цифровізації діяльності підприємства, необхідністю забезпечення стабільного функціонування телекомунікаційної інфраструктури та постійним зростанням кіберзагроз. Водночас значний вплив мають політичні фактори, пов’язані з воєнним станом та потребою забезпечення безперервності роботи цифрових сервісів в умовах кризових ситуацій.

Отже, результати PESTLE-аналізу підтверджують, що ефективність функціонування ПрАТ «Київстар» значною мірою залежить від здатності підприємства адаптуватися до змін зовнішнього середовища, впроваджувати сучасні цифрові технології та забезпечувати високий рівень управління цифровою безпекою.

2.2. Діагностика показників фінансово-господарської діяльності підприємства ПрАТ «Київстар»

Ефективність функціонування підприємства значною мірою визначається результатами його фінансово-господарської діяльності, рівнем прибутковості, фінансової стійкості та здатністю забезпечувати стабільний розвиток в умовах динамічного зовнішнього середовища. Для підприємств телекомунікаційної галузі особливого значення набуває здатність підтримувати високий рівень інвестиційної активності, модернізувати цифрову інфраструктуру та забезпечувати стабільність функціонування інформаційно-комунікаційних систем.

У сучасних умовах цифрової трансформації та зростання кіберзагроз фінансово-господарські показники безпосередньо впливають на можливість підприємства реалізовувати ефективну систему управління цифровою безпекою. Саме тому доцільним є проведення комплексного аналізу основних фінансово-економічних показників ПрАТ «Київстар» за 2023–2025 роки [28].

Таблиця 2.5 – Фінансові показники ПрАТ «Київстар» (2023–2025 рр.)

Показники	Од. виміру	Джерела інформації, розрахунок	Роки			Відхилення			
			2023	2024	2025	2025 р. до 2023 р.		2025 р. до 2024 р.	
						Абсолютне	Темп. прир., %	Абсолютне	Темп. прир., %
1	2	3	4	5	6	7	8	9	10
1. Капітал підприємства									
1.1. Середня вартість сукупного капіталу	тис. грн	Форма 1 «Баланс»	45 387 179,00	58 421 464,00	75 689 581,00	30 302 402,00	66,76	17 268 117,00	29,56
1.2. Середня вартість власного капіталу	тис. грн	Форма 1 «Баланс»	27 255 967,00	38 273 023,00	50 167 020,00	22 911 053,00	84,06	11 893 997,00	31,08
2. Ресурси підприємства									
2.1. Середньорічна вартість основних засобів	тис. грн	Форма 1 «Баланс»	20 878 653,50	24 275 436,00	30 866 858,00	9 988 204,50	47,84	6 591 422,00	27,15
2.2. Середньорічна вартість нематеріальних активів	тис. грн	Форма 1 «Баланс»	8 567 674,50	9 998 097,00	11 941 114,00	3 373 439,50	39,37	1 943 017,00	19,43
2.3. Середні залишки оборотних засобів	тис. грн	Форма 1 «Баланс»	12 179 178,50	19 957 109,00	24 310 206,50	12 131 028,00	99,60	4 343 097,50	21,81
2.4. Середньооблікова чисельність працівників	осіб	Форма 1-ПВ	3 261	3 296	3 475	214	6,56	179	5,43
3. Економічні показники									
3.1. Чистий дохід (виручка) від реалізації продукції	тис. грн	Форма 1-ПВ	33 165 048,00	36 639 345,00	44 323 192,00	11 158 144,00	33,64	7 643 046,00	20,84
3.2. Обсяг реалізованої продукції	тис. грн	Форма 2 «Звіт про фінансові результати»	33 165 048,00	36 639 345,00	44 323 192,00	11 158 144,00	33,64	7 643 046,00	20,84
3.3. Операційні витрати	тис. грн	Форма 2 «Звіт про фінансові результати»	357 394,00	248 926,00	567 539,00	210 145,00	58,80	318 613,00	128,00
3.4. Фонд оплати праці усіх працівників	тис. грн	Форма 1-ПВ	1 848 602,00	2 727 908,00	2 151 907,00	303 305,00	16,41	-576 001,00	-21,12
3.5. Середньомісячна заробітна плата працівника	грн	(п.3.4 / п.2.4 / 12) * 1000	47 240,16	68 970,17	51 604,48	4 364,32	9,24	-17 365,68	-25,18

Продовження Табл. 2.5.

1	2	3	4	5	6	7	8	9	10
4. Фінансові результати									
4.1. Валовий прибуток (збиток)	тис. грн	Форма 2 «Звіт про фінансові результати»	19 112 641,00	20 646 231,00	24 757 196,00	5 644 555,00	29,53	4 110 965,00	19,91
4.2. Прибуток (збиток) від операційної діяльності	тис. грн	Форма 2 «Звіт про фінансові результати»	14 361 223,00	15 099 116,00	17 953 071,00	3 591 848,00	25,01	2 853 955,00	18,90
4.3. Прибуток (збиток) від звичайної діяльності до оподаткування	тис. грн	Форма 2 «Звіт про фінансові результати»	12 925 050,00	13 950 576,00	15 267 281,00	2 342 231,00	18,12	1 316 705,00	9,44
4.4 Чистий прибуток (збиток)	тис. грн	Форма 2 «Звіт про фінансові результати»	10 542 590,00	11 331 462,00	12 307 536,00	1 764 946,00	16,74	976 074,00	8,61
5. Показники ефективності використання ресурсів та витрат									
5.1. Продуктивність праці працівників	тис. грн/особу	п.3.2 / п.2.4	10 170,21	11 128,69	12 754,88	2 584,67	25,41	1 626,19	14,61
5.3. Фондовіддача	грн./грн.	п.3.2 / п.2.1	1,59	1,51	1,44	-0,15	-9,60	-0,08	-4,97
5.4. Коефіцієнт обіговості оборотних засобів	обороти	п.3.1 / п.2.3	2,72	1,84	1,82	-0,90	-33,05	-0,01	--0,69
5.5. Середній період обороту оборотних засобів	дні	360 дн. / п.5.4	132,20	196,09	197,45	65,25	49,36	1,36	0,69
5.6. Коефіцієнт капіталовіддачі	обороти	п.4.1 / п.1.1	0,42	0,35	0,33	-0,09	-22,33	-0,03	-7,45
5.7. Операційні витрати на 1 грн. реалізованої продукції	коп.	п.3.3 / п.3.2	0,01	0,02	0,01	0,00	18,82	0,01	88,68
6. Показники рентабельності підприємства									
6.1. Рентабельність сукупного капіталу	%	п.4.3 / п.1.1 * 100	28,48	23,88	20,17	-8,31	-29,17	-3,71	-15,53
6.2. Рентабельність власного капіталу	%	п.4.4 / п.1.2 * 100	38,68	29,61	24,53	-14,15	-36,57	-5,07	-17,14
6.3. Рентабельність продукції	%	п.4.2 / п.3.3 * 100	4 018,32	6 065,70	3 163,32	-855,00	-21,28	-2 902,39	47,85

Примітка. Розроблено за джерелами [28, 29].

У період з 2023 по 2025 роки спостерігається стійке зростання обсягів капіталу ПрАТ «Київстар», що свідчить про активне нарощування фінансового потенціалу підприємства та розширення масштабів його діяльності. Зокрема, середня вартість сукупного капіталу компанії у 2023 році становила 45 387 179,00 тис. грн, після чого зросла до 58 421 464,00 тис. грн у 2024 році та досягла 75 689 581,00 тис. грн на кінець 2025 року. Загальне абсолютне відхилення сукупного капіталу у 2025 році порівняно з базовим 2023 роком склало 30 302 402,00 тис. грн, а темп його приросту досяг значної позначки у 66,76%. У короткостроковій динаміці 2025 рік до 2024 року капітал збільшився на 17 268 117,00 тис. грн, що демонструє темп приросту на рівні 29,56% і підтверджує високу інтенсивність залучення ресурсів компанією.

Позитивною тенденцією у структурі джерел фінансування оператора є випереджаюче зростання його власного капіталу. Його середня вартість збільшилася з 27 255 967,00 тис. грн у 2023 році до 50 167 020,00 тис. грн у 2025 році. Абсолютне збільшення власного капіталу за три роки склало 22 911 053,00 тис. грн, а темп приросту сягнув вражаючих 84,06%. Протягом останнього аналізованого року 2025 р. до 2024 р. обсяг власних коштів зріс на 11 893 997,00 тис. грн або на 31,08%. Така динаміка вказує на високу спроможність ПрАТ «Київстар» генерувати внутрішні фінансові ресурси, що суттєво зміцнює фінансову стійкість, незалежність від зовнішніх кредиторів та загальну інвестиційну привабливість підприємства на ринку телекомунікацій.

Аналіз ресурсного потенціалу ПрАТ «Київстар» у розрізі 2023–2025 років свідчить про масштабне розширення та модернізацію матеріально-технічної бази, а також про нарощення оборотних активів компанії. Головну роль у забезпеченні безперебійної діяльності оператора відіграють основні засоби, середньорічна вартість яких демонструє стабільне висхідне спрямування. У 2023 році цей показник становив 20 878 653,50 тис. грн, у 2024 році збільшився до 24 275 436,00 тис. грн, а у 2025 році досяг 30 866 858,00 тис. грн. Загальний приріст за аналізований період склав 9 988 204,50 тис. грн (або 47,84% у

відносному вираженні). У річному вимірі (2025 р. порівняно з 2024 р.) вартість основних засобів зросла на 6 591 422,00 тис. грн (на 27,15%). Таке стрімке накопичення необоротних матеріальних активів безпосередньо пов'язане з капітальними інвестиціями у розбудову мережевої інфраструктури, відновлення пошкодженого обладнання та впровадження новітніх технологій зв'язку.

Паралельно із матеріальними ресурсами компанія активно нарощувала обсяги інтелектуального та технологічного капіталу через збільшення вартості нематеріальних активів. Їхня середньорічна вартість зросла з 8 567 674,50 тис. грн у 2023 році до 11 941 114,00 тис. грн у 2025 році, що відображає абсолютне збільшення на 3 373 439,50 тис. грн (темп приросту склав 39,37%). Протягом останнього року приріст становив 1 943 017,00 тис. грн (або 19,43%). Це підтверджує стратегічну орієнтацію ПрАТ «Київстар» на інноваційний розвиток, зокрема шляхом придбання ліцензій на радіочастотний ресурс, модернізації програмного забезпечення та захисту прав інтелектуальної власності.

Найбільш динамічною складовою майнових ресурсів підприємства стали його оборотні кошти. Середні залишки оборотних засобів у 2023 році дорівнювали 12 179 178,50 тис. грн, після чого помірно зросли у 2024 році до 19 957 109,00 тис. грн, а у 2025 році відбувся стрімкий стрибок до 24 310 206,50 тис. грн. У підсумку за три роки обсяг оборотного капіталу зріс майже вдвічі — абсолютне відхилення склало 12 131 028,00 тис. грн, а темп приросту сягнув 99,60%. Лише за останній рік залишки збільшилися на 8 517 909,50 тис. грн (на 53,94%). Такий високий темп приросту мобільних активів забезпечує підприємству високий рівень поточної ліквідності та платоспроможності, дозволяючи оперативно фінансувати операційні витрати й підтримувати високу фінансову гнучкість у нестабільних ринкових умовах.

Ефективне управління та капіталізація вищезазначених ресурсів супроводжувалися помірним та виваженим розширенням штату працівників. Середньооблікова чисельність персоналу ПрАТ «Київстар» зросла з 3 261 осіб у 2023 році до 3 475 осіб у 2025 році. Абсолютне збільшення кількості робочих

місць за весь період склало 214 осіб (або 6,56%), а за період з 2024 по 2025 роки штат розширився на 179 осіб (на 5,43%). Зіставлення високих темпів приросту вартості виробничих фондів та оборотних коштів із відносно стриманим зростанням чисельності персоналу свідчить про інтенсивний характер розвитку підприємства, підвищення рівня технічної озброєності праці та зростання загальної продуктивності людського капіталу компанії.

Чистий дохід (виручка) від реалізації продукції та обсяг реалізованої продукції — є тотожними за своїми значеннями та демонструють синхронне висхідне спрямування. У 2023 році дохід підприємства становив 33 165 048,00 тис. грн, у 2024 році він зріс до 36 639 345,00 тис. грн, а у 2025 році досяг пікового значення у 44 323 192,00 тис. грн. Загальне абсолютне збільшення виручки у 2025 році порівняно з 2023 роком склало 11 158 144,00 тис. грн, забезпечивши темп приросту на рівні 33,64%. Динаміка останнього року (2025 р. до 2024 р.) також є виражено позитивною: приріст склав 7 683 847,00 тис. грн, або 20,97%, що підтверджує зміцнення ринкових позицій оператора та розширення клієнтської бази.

Особливу увагу в контексті забезпечення операційної ефективності привертає динаміка витрат компанії. Обсяг операційних витрат ПрАТ «Київстар» у 2023 році становив 357 394,00 тис. грн, після чого у 2024 році відбулося їхнє зменшення до 248 926,00 тис. грн, що, очевидно, було пов'язано з інтенсивними аварійно-відновлювальними роботами та подоланням наслідків масштабних кібератак і руйнувань інфраструктури. Проте вже у 2025 році менеджменту компанії вдалося оптимізувати витрати, знизивши їх до 567 539,00 тис. грн. У порівнянні з 2024 роком операційні витрати збільшилися на 318 613,00 тис. грн (або на 128,00%). Попри те, що загальний темп приросту витрат за три роки склав 58,80% (абсолютне відхилення — 210 145,00 тис. грн), тенденція до їх зниження у 2025 році на тлі стрімкого зростання доходів свідчить про відновлення контролю над операційною діяльністю та підвищення загальної рентабельності бізнесу.

Процеси оптимізації та структурних змін торкнулися також і системи матеріального стимулювання персоналу. Фонд оплати праці усіх працівників у 2023 році складав 1 848 602,00 тис. грн, у 2024 році він помітно збільшився до 2 727 908,00 тис. грн, а у 2025 році скоротився до 2 151 907,00 тис. грн. Загалом за три роки фонд оплати праці зріс на 303 305,00 тис. грн (на 16,41%), проте у короткостроковому періоді (2025 р. до 2024 р.) відбулося його зменшення на 576 001,00 тис. грн, що у відносному вираженні становить -21,12%.

Аналогічний тренд притаманний і показникам індивідуального доходу робітників. Середньомісячна заробітна плата одного працівника зросла з 47 240,16 грн у 2023 році до 68 970,17 грн у 2024 році, але у 2025 році скоригувалася до рівня 51 604,48 грн. У підсумку за три роки середня зарплата продемонструвала позитивний приріст на 9,24% (або на 4 364,32 грн), хоча порівняно з попереднім роком вона зменшилася на 17 365,68 грн (на 25,18%). Враховуючи раніше зафіксоване зростання чисельності персоналу у 2025 році, таке коливання заробітної плати та фонду оплати праці після стрибка у 2024 році може свідчити про завершення виплат специфічних антикризових премій чи компенсацій, зміну структури зайнятості або впровадження нових, більш гнучких та оптимізованих моделей нормування праці на підприємстві.

Первинний індикатор ефективності продажів — валовий прибуток — демонструє стійке зростання: у 2023 році він становив 19 112 641,00 тис. грн, у 2024 році збільшився до 20 646 231,00 тис. грн, а у 2025 році досяг 24 757 196,00 тис. грн. Загальний абсолютний приріст за три роки склав 5 644 555,00 тис. грн (або 29,53%), а у річному вимірі (2025 р. порівняно з 2024 р.) валовий прибуток зріс на 4 110 965,00 тис. грн (на 19,91%). Така динаміка підтверджує, що темпи зростання доходів від надання телекомунікаційних послуг суттєво випереджали темпи зміни їхньої собівартості.

Аналогічний позитивний тренд притаманний і показникам операційної ефективності бізнесу. Прибуток від операційної діяльності компанії послідовно зростав із 14 361 223,00 тис. грн у 2023 році до 15 099 116,00 тис. грн у 2024 році, а у 2025 році зафіксований на рівні 17 953 071,00 тис. грн. Абсолютне

збільшення операційного прибутку за весь аналізований період склало 3 591 848,00 тис. грн із темпом приросту 25,01%. Протягом останнього року цей показник покращився на 2 853 955,00 тис. грн (або на 18,90%). Це свідчить про високу якість операційного менеджменту ПрАТ «Київстар» та здатність підтримувати стабільну маржинальність бізнесу навіть за умов значних макроекономічних викликів.

Ефективне ведення основної діяльності дозволило підприємству забезпечити стабільне зростання обсягів прибутку до оподаткування та чистих фінансових результатів. Прибуток від звичайної діяльності до оподаткування збільшився з 12 925 050,00 тис. грн у 2023 році до 15 267 281,00 тис. грн у 2025 році (загальний приріст склав 2 342 231,00 тис. грн, або 18,12%). Кінцевий результат діяльності підприємства — чистий прибуток — також продемонстрував висхідну динаміку протягом усього трирічного циклу. У 2023 році чистий прибуток становив 10 542 590,00 тис. грн, у 2024 році — 11 331 462,00 тис. грн, а у 2025 році він досяг 12 307 536,00 тис. грн.

У підсумку абсолютний приріст чистого прибутку за аналізований період склав 1 764 946,00 тис. грн, що еквівалентно темпу приросту на рівні 16,74%. У порівнянні з 2024 роком чистий прибуток у 2025 році зріс на 976 074,00 тис. грн (або на 8,61%). Слід зазначити, що хоча загальний темп приросту чистого прибутку (16,74%) дещо поступається темпу приросту чистого доходу (33,64%), що зумовлено коливанням операційних та інших витрат у 2024–2025 роках, стабільне накопичення чистого прибутку підтверджує високий рівень самофінансування ПрАТ «Київстар». Це забезпечує надійне підґрунтя для подальшого формування власного капіталу компанії, виконання інвестиційних зобов'язань та підтримання фінансової стійкості у довгостроковій перспективі.

Позитивною тенденцією є стійке зростання продуктивності праці працівників. У 2023 році цей показник становив 10 170,21 тис. грн/особу, у 2024 році зріс до 11 128,69 тис. грн/особу, а у 2025 році досяг 12 754,88 тис. грн/особу. Загальний абсолютний приріст за три роки склав 2 584,67 тис. грн/особу (або 25,41%), а у річному вимірі (2025 р. до 2024 р.) — 1 626,19 тис.

грн/особу (на 14,61%). Це свідчить про високу ефективність управління людським капіталом та випереджаючі темпи зростання обсягів реалізованої продукції порівняно з розширенням штату.

Водночас показники використання матеріальних та фінансових ресурсів демонструють певне зниження віддачі, що є закономірним наслідком вимушених капіталомістких інвестицій. Так, фондовіддача зменшилася з 1,59 грн/грн у 2023 році до 1,44 грн/грн у 2025 році (загальне зниження на 9,60%), що вказує на тимчасове відставання темпів генерування доходу від темпів закупівлі й відновлення основних засобів.

Аналогічна тенденція спостерігається і в сфері управління оборотними активами: коефіцієнт обіговості знизився з 2,72 оборотів у 2023 році до 1,82 оборотів у 2025 році (на 33,05%), а середній період обороту відповідно зріс з 132,20 днів до 197,45 днів (уповільнення на 65,25 днів). Коефіцієнт капіталовіддачі також скоригувався з 0,42 до 0,33 оборотів (на 22,33%). Таке уповільнення ділової активності та капіталовіддачі пов'язане зі значним накопиченням залишків оборотних засобів і сукупного капіталу для формування фінансових резервів та забезпечення безперебійної діяльності оператора в кризових умовах.

При цьому операційні витрати на 1 грн реалізованої продукції залишалися на критично низькому та контрольованому рівні 0,01 грн, причому у 2025 році порівняно з 2024 роком цей показник зріс на 88,68%, підтверджуючи високу відносну ефективність поточних витрат.

Показники рентабельності ПрАТ «Київстар» комплексно відображають кінцеву ефективність функціонування компанії та її здатність генерувати прибуток на кожну інвестовану гривню капіталу чи витрат. Рентабельність сукупного капіталу протягом аналізованого періоду зазнала зниження: з 28,48% у 2023 році до 23,88% у 2024 році та 20,17% у 2025 році. Загальне відхилення склало -8,31 в.п. (зниження на 29,17%), а за останній рік показник зменшився на 3,71 в.п.

Подібну траєкторію продемонструвала і рентабельність власного капіталу, яка знизилася з 38,68% у 2023 році до 24,53% у 2025 році. Слід наголосити, що таке зниження рентабельності капіталу обумовлене не падінням прибутковості — адже чистий прибуток компанії стабільно зростав — а математичним ефектом випереджаючого зростання обсягів самого капіталу, які компанія активно акумулювала на балансі протягом 2023–2025 років для мінімізації ризиків та відновлення інфраструктури. Навіть попри зниження, рівень на позначці 24,53% у 2025 році залишається надзвичайно високим для індустрії та свідчить про високу інвестиційну привабливість підприємства.

На противагу показникам капіталу, рентабельність продукції продемонструвала високу динаміку та гнучкість. У 2023 році вона становила 4 018,32%, у 2024 році на тлі стрибка витрат знизилася до 2 488,33%, а у 2025 році суттєво зросла — до 3 163,32%. У річному вимірі (2025 р. до 2024 р.) приріст рентабельності продукції склав значні 674,98 в.п. (або 27,13%). Це безпосередньо доводить, що оптимізація операційних витрат, проведена менеджментом у 2025 році, разом із нарощуванням чистого операційного прибутку дозволили компанії суттєво підвищити віддачу від кожної гривні, спрямованої на забезпечення операційної діяльності, зміцнюючи загальну конкурентоспроможність ПрАТ «Київстар» на ринку.

2.3. Оцінка процесу управління цифровою безпекою та його впливу на економічну стійкість підприємства ПрАТ «Київстар»

Система цифрової безпеки ПрАТ «Київстар» базується на комплексному підході до захисту інформаційної інфраструктури та передбачає поєднання організаційних, технічних і програмних засобів захисту. Основою функціонування системи є політики інформаційної безпеки, які регламентують порядок роботи з інформаційними ресурсами, права доступу користувачів, захист персональних даних та процедури реагування на кіберінциденти.

Важливим елементом системи кіберзахисту є постійний моніторинг мережевої активності за допомогою сучасних SIEM-систем, які здійснюють збір, аналіз та кореляцію подій безпеки в режимі реального часу. Такий підхід дозволяє своєчасно виявляти аномальну активність, спроби несанкціонованого доступу та інші потенційні кіберзагрози. Фактично функції центру моніторингу безпеки забезпечують безперервний контроль стану цифрового середовища підприємства та підвищують швидкість реагування на інциденти [30].

Для захисту критично важливих інформаційних ресурсів підприємство використовує багаторівневу систему захисту даних. Одним із ключових механізмів є сегментація мережі, яка передбачає розподіл телекомунікаційної інфраструктури на окремі ізольовані сегменти. Завдяки цьому навіть у разі компрометації одного з компонентів мережі зловмисники не можуть автоматично отримати доступ до інших критичних систем підприємства.

Додатковий рівень захисту забезпечується шляхом шифрування інформації як під час її зберігання на серверах підприємства, так і під час передачі каналами зв'язку. Використання сучасних криптографічних технологій дозволяє мінімізувати ризики несанкціонованого доступу до персональних даних абонентів та службової інформації компанії.

Суттєву роль у забезпеченні цифрової безпеки відіграють механізми резервного копіювання та відновлення інформації. Наявність резервних копій критично важливих даних забезпечує безперервність бізнес-процесів та дозволяє оперативно відновити роботу інформаційних систем у разі виникнення кіберінцидентів або технічних збоїв. Для захисту облікових записів працівників також використовуються сучасні засоби багатофакторної автентифікації, які значно ускладнюють можливість компрометації користувацьких облікових даних.

Важливою складовою системи цифрової безпеки є процес реагування на кіберінциденти та управління ризиками. Підприємство здійснює постійний аналіз потенційних загроз, оцінку рівня ризиків та розробку заходів щодо їх мінімізації. Особливу роль у цьому процесі відіграє взаємодія з державними

органами, зокрема Державною службою спеціального зв'язку та захисту інформації України, яка здійснює аудит кібербезпеки об'єктів критичної інфраструктури та координує дії під час масштабних кіберінцидентів.

Разом з тим досвід кібератаки на ПрАТ «Київстар» у грудні 2023 року продемонстрував, що навіть наявність сучасних технічних засобів захисту не гарантує абсолютної безпеки. Однією з основних вразливостей залишається людський фактор, оскільки використання скомпрометованих облікових записів може дозволити зловмисникам обійти частину механізмів захисту та отримати доступ до критичних ресурсів підприємства [31].

Ефективність системи цифрової безпеки безпосередньо впливає на економічну стійкість ПрАТ «Київстар». Насамперед кіберзахист сприяє збереженню фінансових результатів підприємства шляхом мінімізації збитків від кібератак, витоку даних та простоїв інформаційних систем. Надійна система захисту дозволяє уникати значних фінансових втрат, пов'язаних із відновленням інфраструктури та компенсацією наслідків кіберінцидентів.

Крім того, високий рівень цифрової безпеки забезпечує стабільність функціонування телекомунікаційної мережі та безперервність надання послуг абонентам. Для підприємства, яке обслуговує понад 22 млн користувачів, навіть короткострокове припинення роботи мережі може призвести до суттєвих фінансових і репутаційних втрат.

Для більш комплексної оцінки процесу управління цифровою безпекою ПрАТ «Київстар» доцільно застосувати SWOT-аналіз. Даний метод стратегічного аналізу дозволяє визначити сильні та слабкі сторони підприємства, а також виявити зовнішні можливості та загрози, які можуть впливати на ефективність функціонування системи цифрової безпеки та загальну економічну стійкість компанії.

Особливістю SWOT-аналізу є можливість поєднання внутрішніх факторів діяльності підприємства із впливом зовнішнього середовища. Для ПрАТ «Київстар» це є особливо актуальним, оскільки підприємство функціонує в умовах високої залежності від цифрових технологій, постійного зростання

кіберзагроз та значного впливу воєнних ризиків на телекомунікаційну інфраструктуру. Результати SWOT-аналізу дозволяють визначити основні конкурентні переваги підприємства, виявити наявні проблеми та сформувати напрями подальшого вдосконалення системи управління цифровою безпекою.

Таблиця 2.7 – SWOT-аналіз ПрАТ «Київстар»

Сильні сторони	Слабкі сторони
1. Потужна IT-інфраструктура та найбільша телекомунікаційна мережа в Україні 2. Використання SOC та систем постійного моніторингу безпеки 3. Наявність сучасних засобів кіберзахисту та шифрування даних 4. Сильний бренд та високий рівень довіри клієнтів	1. Високі витрати на підтримку та модернізацію інфраструктури 2. Складність управління великою кількістю інформаційних систем 3. Залежність від людського фактора при адмініструванні систем 4. Значні витрати на забезпечення безперервності роботи мережі 5. Підвищена відповідальність як об'єкта критичної інфраструктури
Можливості	**Загрози**
1. Впровадження систем штучного інтелекту для виявлення кіберзагроз 2. Розвиток технології 5G та нових цифрових сервісів 3. Подальше використання хмарних технологій та Big Data 4. Інтеграція з міжнародними стандартами кіберзахисту	1. Зростання кількості та складності кібератак 2. Воєнні ризики та загроза пошкодження інфраструктури 3. Витік конфіденційної інформації та персональних даних 4. Посилення конкуренції на телекомунікаційному ринку 5. Швидка зміна технологій та поява нових видів кіберзагроз

Примітка. Авторська розробка.

Проведений SWOT-аналіз показує, що ПрАТ «Київстар» має значний потенціал для подальшого розвитку системи цифрової безпеки завдяки наявності сучасної телекомунікаційної інфраструктури, потужних IT-ресурсів та високого рівня цифровізації бізнес-процесів.

Таблиця 2.8 – Стратегія SWOT-аналізу ПрАТ «Київстар»

	Сильні сторони	Слабкі сторони
Можливості	8	9
Загрози	9	10

Примітка. Авторська розробка.

Аналіз стратегічної матриці SWOT, свідчить, що найбільш критичним вектором для підприємства є СЗ-стратегія (мінімізація слабких сторін та захист від загроз), яка отримала найвищу оцінку — 10. Оскільки цей квадрант має найбільшу кількість взаємозв'язків, у поточних умовах для компанії життєво важливо обрати захисну модель управління, спрямовану на зниження внутрішньої вразливості перед потужними деструктивними чинниками зовнішнього середовища. Головний фокус цієї стратегії передбачає посилення кібербезпеки, ліквідацію технологічних вразливостей мережі та фізичний захист критичної інфраструктури від цілеспрямованих кібератак і воєнних руйнувань, що є особливо актуальним з огляду на статус оператора як об'єкта критичної інфраструктури.

Разом із тим дослідження виявило низку слабких сторін, серед яких найбільш суттєвими є значні витрати на підтримку інфраструктури, складність адміністрування великої кількості інформаційних систем та ризики, пов'язані з людським фактором. Саме людський фактор став одним із ключових чинників успішної кібератаки на компанію у 2023 році, що підтверджує необхідність постійного підвищення рівня кіберграмотності персоналу та вдосконалення механізмів контролю доступу [31].

Аналіз зовнішнього середовища свідчить про наявність значних можливостей для подальшого розвитку підприємства. Впровадження технологій штучного інтелекту, розвиток мереж 5G, використання хмарних рішень та розширення портфеля цифрових сервісів можуть суттєво підвищити ефективність системи управління цифровою безпекою та зміцнити ринкові позиції компанії. Водночас найбільшими загрозами для ПрАТ «Київстар» залишаються кібератаки, воєнні ризики та висока динаміка розвитку цифрових технологій. У зв'язку з цим підприємству необхідно постійно вдосконалювати механізми кіберзахисту, розширювати можливості моніторингу цифрового середовища та забезпечувати готовність до реагування на нові види кіберзагроз.

Після SWOT-аналізу логічно перейти до бенчмаркінгу як інструменту порівняння рівня розвитку системи цифрової безпеки ПрАТ «Київстар» із

основними конкурентами телекомунікаційного ринку України. Метод бенчмаркінгу дозволяє визначити сильні та слабкі сторони підприємства шляхом зіставлення ключових показників діяльності та практик управління із найкращими представниками галузі. У межах даного дослідження доцільно порівняти Київстар із Vodafone Україна та lifecell, які є основними конкурентами на ринку мобільного зв'язку та цифрових послуг.

Проведений бенчмаркінг свідчить, що ПрАТ «Київстар» займає лідируючі позиції серед українських операторів мобільного зв'язку за масштабом інфраструктури, кількістю абонентів, географією покриття та рівнем розвитку цифрових сервісів. Компанія володіє найбільшою мережею магазинів та має найширшу присутність на території України, що забезпечує додаткові конкурентні переваги та високий рівень доступності послуг для споживачів.

Таблиця 2.9 – Бенчмаркінг діяльності та систем цифрової безпеки операторів мобільного зв'язку України

Показник	Київстар	Vodafone Україна	lifecell
Кількість магазинів	500	287	300
Кількість міст присутності	280	176	150
Кількість абонентів	понад 22,4 млн	понад 15 млн	понад 9 млн
Вартість базового тарифу (за 4 тижні)	300 грн («LOVE UA Світло»)	270 грн («Joice Start»)	160 грн / 90 грн акційна («Просто Лайф»)
Відсоток передчасних роз’єднань дзвінків (Норма: не більше 5%)	0,07%	0,22%	0,17%
Відсоток з’єднань з нормативною якістю мови (Норма: не менше 7%)	23%	34%	18%
Захист від DDoS-атак	Так	Так	Так
Сертифікація ISO 27001	Так	Так	Так
Розвиток хмарних сервісів	Високий	Високий	Середній
Швидкість передавання даних у мережі 4G	75 Мбіт/с	75 Мбіт/с	48 Мбіт/с
Швидкість приймання даних у мережі 4G	685 Мбіт/с	587 Мбіт/с	439 Мбіт/с
Рівень цифрової інфраструктури	Дуже високий	Високий	Середній

Примітка. Розроблено за джерелами [32].

У сфері цифрової безпеки всі три оператори використовують сучасні засоби захисту інформації, системи моніторингу мережевої активності та механізми протидії кіберзагрозам. Водночас Vodafone демонструє дещо вищий рівень впровадження сучасних концепцій кіберзахисту, зокрема технологій штучного інтелекту для аналізу загроз та принципів Zero Trust. Київстар також активно впроваджує зазначені рішення, проте окремі напрями цифрової безпеки перебувають на стадії подальшого розвитку та вдосконалення.

Разом із тим Київстар має найбільш розвинену телекомунікаційну інфраструктуру та найвищі показники продуктивності мережі, що дозволяє забезпечувати стабільність цифрових сервісів і підтримувати високий рівень економічної стійкості підприємства. Це створює міцну основу для подальшого розвитку системи управління цифровою безпекою та впровадження інноваційних технологій кіберзахисту.

На основі проведеного аналізу можна виділити низку проблемних аспектів, які потребують подальшого вдосконалення. Насамперед це високі витрати на підтримку та модернізацію телекомунікаційної інфраструктури, які щороку зростають через необхідність оновлення обладнання, впровадження нових технологій зв'язку та посилення кіберзахисту.

Другою проблемою є складність моніторингу великої кількості інформаційних систем і мережевих ресурсів. Масштаби діяльності ПрАТ «Київстар» зумовлюють необхідність обробки значних обсягів даних та постійного контролю за станом цифрової інфраструктури, що підвищує вимоги до систем моніторингу та управління інцидентами інформаційної безпеки.

Суттєвим фактором ризику залишається людський фактор. Практика показує, що навіть за наявності сучасних технічних засобів захисту помилки персоналу або компрометація облікових записів можуть стати причиною серйозних кіберінцидентів. Саме тому важливого значення набуває підвищення рівня кіберграмотності працівників та вдосконалення механізмів контролю доступу.

Додатковим викликом є постійне зростання кількості та складності

кіберзагроз. Використання традиційних засобів захисту вже не завжди дозволяє ефективно виявляти нові типи атак, тому підприємству необхідно активніше впроваджувати рішення на основі штучного інтелекту та машинного навчання для прогнозування та автоматичного виявлення кіберзагроз.

Крім того, потребує подальшого розвитку система управління ризиками цифрової безпеки. В умовах воєнного стану та високого рівня кіберзагроз особливого значення набуває вдосконалення процедур оцінювання ризиків, планування безперервності діяльності та формування комплексної стратегії.

Висновки до розділу 2

1. На основі проведеного дослідження об'єкта та суб'єкта системи управління ПрАТ «Київстар» визначено, що підприємство є одним із ключових елементів критичної інфраструктури та цифрового середовища України, що забезпечує стабільність інформаційно-комунікаційних процесів. Встановлено, що компанія має функціональну організаційну структуру управління з елементами дивізійного та процесного підходів, яка інтегрує стратегічний контроль на рівні материнської компанії VEON та Наглядової ради з глибокою операційною координацією технічних, IT- та комплаєнс-підрозділів. За допомогою PESTLE-аналізу доведено, що найбільший вплив на діяльність оператора мають технологічні, соціальні та правові фактори, зумовлені високим рівнем цифровізації та дією воєнного стану, що вимагає постійної адаптації внутрішніх систем кіберзахисту.

2. Діагностика показників фінансово-господарської діяльності ПрАТ «Київстар» засвідчила виняткову комерційну ефективність та високу економічну стійкість компанії, що підтверджується позитивною динамікою доходів і досягненням рекордного рівня чистого прибутку у 2025 році понад 12,3 млрд грн. Аналіз балансових показників виявив високу капіталомісткість та спрямованість стратегії на реінвестування прибутку у модернізацію технологічного ядра і серверного обладнання. Зниження рентабельності

продукції у 2022–2025 роках до 28,1 % обґрунтовано об'єктивним зростанням витрат на відновлення пошкодженої війною інфраструктури, забезпечення енергонезалежності мереж.

3. Оцінювання процесу управління цифровою безпекою компанії дозволило ідентифікувати побудову багаторівневої системи кіберзахисту, інтегрованої із державними органами та побудованої на впровадженні проактивних рішень, хмарних технологій та Big Data. Водночас досвід масштабної кібератаки на ПрАТ «Київстар» у грудні 2023 року продемонстрував, що ключовою внутрішньою вразливістю залишається людський фактор і компрометація облікових даних. Проведений SWOT-аналіз та галузевий бенчмаркінг із ключовими конкурентами підтвердили лідерські позиції компанії на ринку, але виявили потребу у переході до архітектури нульової довіри та вдосконаленні процедур управління ризиками цифрової безпеки в умовах гібридних загроз.

РОЗДІЛ 3. НАПРЯМИ ВДОСКОНАЛЕННЯ УПРАВЛІННЯ ЦИФРОВОЮ БЕЗПЕКОЮ ПІДПРИЄМСТВА ПРАТ «КИЇВСТАР»

3.1. Визначення стратегічних напрямів розвитку процесу управління цифровою безпекою підприємства ПрАТ «Київстар»

Результати проведеного у другому розділі дослідження, зокрема SWOT-аналізу, PESTLE-аналізу та бенчмаркінгу систем цифрової безпеки провідних телекомунікаційних і технологічних компаній, свідчать про необхідність подальшого вдосконалення процесу управління цифровою безпекою ПрАТ «Київстар». Незважаючи на високий рівень розвитку цифрової інфраструктури та впровадження сучасних механізмів кіберзахисту, діяльність підприємства здійснюється в умовах постійного зростання кількості кіберзагроз, активізації атак на об’єкти критичної інфраструктури, розвитку хмарних технологій та поширення рішень на основі штучного інтелекту. Додатковим фактором ризику для українських телекомунікаційних компаній залишається воєнний стан, який суттєво підвищує ймовірність цілеспрямованих кібератак на інформаційні ресурси та мережеву інфраструктуру підприємства.

У таких умовах система цифрової безпеки ПрАТ «Київстар» повинна розвиватися не лише шляхом удосконалення окремих технічних засобів захисту, а й через впровадження комплексного стратегічного підходу до управління цифровими ризиками. Основними напрямами розвитку доцільно визначити перехід до проактивної моделі кібербезпеки, впровадження концепції Zero Trust, посилення управління кіберризиками, використання інструментів штучного інтелекту для виявлення загроз та розвиток цифрової стійкості підприємства.

Одним із ключових стратегічних напрямів удосконалення процесу управління цифровою безпекою ПрАТ «Київстар» є перехід від переважно реактивного до проактивного підходу до кіберзахисту. Традиційна модель безпеки орієнтується насамперед на реагування після виникнення інциденту,

тоді як сучасне цифрове середовище вимагає своєчасного виявлення потенційних загроз ще до моменту їх реалізації. Зростання складності кібератак, використання автоматизованих засобів злому та поширення атак на критичну інфраструктуру свідчать про те, що простого реагування на інциденти вже недостатньо для забезпечення належного рівня захисту.

Перехід до проактивної моделі кібербезпеки передбачає створення системи безперервного моніторингу цифрового середовища підприємства, яка забезпечуватиме оперативне виявлення підозрілої активності та потенційних загроз. Важливим елементом такого підходу є використання технологій Threat Intelligence, які дозволяють отримувати та аналізувати інформацію про актуальні кіберзагрози, джерела атак, нові вразливості та методи діяльності кіберзлочинців. Отримані дані можуть використовуватися для прогнозування можливих сценаріїв атак та своєчасного впровадження превентивних заходів захисту [33].

Крім того, доцільним є впровадження механізмів поведінкового аналізу користувачів та пристроїв, що дозволяють виявляти аномалії у роботі інформаційних систем. Аналіз поведінки користувачів забезпечує можливість автоматичного виявлення підозрілих дій, несанкціонованих спроб доступу або нетипових операцій із даними, що може свідчити про компрометацію облікових записів або підготовку кібератаки. Реалізація такого підходу сприятиме підвищенню швидкості виявлення інцидентів та зменшенню потенційних збитків від їх реалізації.

Важливим напрямом розвитку процесу управління цифровою безпекою ПрАТ «Київстар» також є впровадження концепції Zero Trust Architecture. Необхідність використання даного підходу підтверджується досвідом провідних міжнародних компаній, зокрема Microsoft та Google, які активно застосовують принципи Zero Trust для забезпечення захисту корпоративних ресурсів в умовах розподіленого цифрового середовища [34].

Концепція Zero Trust базується на принципі «ніколи не довіряй — завжди перевіряй», відповідно до якого жоден користувач, пристрій або інформаційна

система не вважаються безпечними за замовчуванням незалежно від їхнього місця розташування в мережі підприємства. У межах такого підходу кожен запит на доступ до корпоративних ресурсів повинен проходити процедуру автентифікації, авторизації та оцінювання рівня ризику.

Для ПрАТ «Київстар» впровадження Zero Trust передбачає посилення контролю доступу до інформаційних ресурсів шляхом використання багатофакторної автентифікації, яка забезпечує додатковий рівень перевірки особи користувача. Застосування MFA дозволяє суттєво знизити ризик несанкціонованого доступу навіть у випадку компрометації паролів або облікових записів співробітників.

Не менш важливим елементом концепції є постійний контроль пристроїв, які підключаються до корпоративної мережі. Перед наданням доступу до інформаційних ресурсів система повинна перевіряти відповідність пристрою встановленим вимогам безпеки, наявність актуальних оновлень програмного забезпечення та відсутність ознак компрометації. Такий підхід дозволяє мінімізувати ризики проникнення шкідливого програмного забезпечення через кінцеві точки мережі.

Додатково доцільним є впровадження мережевої сегментації, яка передбачає розподіл корпоративної мережі на окремі ізольовані сегменти відповідно до рівня критичності інформаційних ресурсів. У разі успішного проникнення зловмисника до одного із сегментів мережі це ускладнить подальше поширення атаки та дозволить локалізувати інцидент із мінімальними наслідками для діяльності підприємства [35].

Перехід до проактивної моделі кібербезпеки та впровадження концепції Zero Trust створюють основу для формування сучасної системи управління цифровою безпекою ПрАТ «Київстар». Реалізація зазначених стратегічних напрямів дозволить підвищити рівень захищеності цифрової інфраструктури, забезпечити більш ефективне управління кіберризиками та зміцнити економічну стійкість підприємства в умовах зростання цифрових загроз

Наступним стратегічним напрямом удосконалення процесу управління цифровою безпекою ПрАТ «Київстар» є посилення системи управління кіберризиками. В умовах зростання кількості цифрових загроз ефективний кіберзахист повинен базуватися не лише на використанні технічних засобів безпеки, а й на системному підході до ідентифікації, оцінювання та контролю ризиків. Для телекомунікаційного підприємства, яке забезпечує функціонування критично важливої цифрової інфраструктури та обслуговує мільйони абонентів, управління кіберризиками має бути інтегроване у загальну систему корпоративного управління та прийняття управлінських рішень.

З метою підвищення ефективності процесу управління цифровою безпекою доцільним є створення єдиної системи оцінки кіберризиків, яка забезпечуватиме централізований підхід до аналізу загроз та визначення пріоритетних напрямів захисту. Така система повинна передбачати формування реєстру кіберризиків, у якому будуть накопичуватися дані про потенційні загрози, джерела їх виникнення, ймовірність реалізації та можливі наслідки для діяльності підприємства. Наявність реєстру дозволить здійснювати постійний контроль рівня цифрових ризиків та забезпечувати своєчасне оновлення заходів кіберзахисту відповідно до змін зовнішнього середовища.

Важливим інструментом управління кіберризиками є використання матриці ризиків, яка дозволяє визначити пріоритетність загроз залежно від імовірності їх виникнення та рівня можливих наслідків. Це сприятиме більш ефективному розподілу фінансових, технічних і кадрових ресурсів між різними напрямами забезпечення цифрової безпеки. Крім того, доцільним є проведення регулярної оцінки кіберзагроз та аудитів цифрової безпеки, що дозволить своєчасно виявляти нові вразливості та адаптувати систему захисту до актуальних викликів.

Необхідність посилення управління кіберризиками підтверджується також попереднім досвідом діяльності ПрАТ «Київстар». Одним із факторів, які можуть призводити до реалізації масштабних кіберінцидентів, є людський фактор та фішингові атаки, спрямовані на компрометацію облікових записів

співробітників. Саме використання методів соціальної інженерії та отримання несанкціонованого доступу через скомпрометовані облікові записи вважається одним із можливих етапів підготовки масштабної кібератаки на інфраструктуру компанії у попередні роки. Це підтверджує необхідність системного контролю кіберризиків та постійного вдосконалення механізмів їх оцінювання.

З урахуванням специфіки діяльності ПрАТ «Київстар» основні кіберризики підприємства доцільно узагальнити у таблиці 3.1.

Таблиця 3.1 – Основні кіберризики ПрАТ «Київстар»

Ризик	Ймовірність	Наслідки	Пріоритет
DDoS-атаки	Висока	Високі	Критичний
Витік даних	Середня	Високі	Високий
Фішинг	Висока	Середні	Високий

Примітка. Авторська розробка.

Як видно з таблиці 3.1, найбільш критичними для ПрАТ «Київстар» залишаються DDoS-атаки, які можуть призводити до порушення роботи телекомунікаційної інфраструктури та недоступності послуг для абонентів. Високий рівень пріоритетності також мають ризики витоку даних та фішингових атак, які можуть спричинити фінансові втрати, репутаційні ризики та несанкціонований доступ до корпоративних інформаційних ресурсів. Тому вдосконалення системи управління кіберризиками повинно стати одним із ключових напрямів розвитку цифрової безпеки підприємства.

Ще одним перспективним напрямом розвитку процесу управління цифровою безпекою ПрАТ «Київстар» є активне використання технологій штучного інтелекту. Сучасні кіберзагрози характеризуються високою швидкістю поширення та складністю виявлення, що значно ускладнює їх аналіз виключно за допомогою традиційних засобів моніторингу. У зв’язку з цим доцільним є впровадження інтелектуальних систем кіберзахисту, здатних автоматично аналізувати великі обсяги даних та оперативно реагувати на потенційні загрози.

Використання AI-моніторингу дозволить здійснювати безперервний аналіз подій інформаційної безпеки в режимі реального часу та своєчасно виявляти підозрілу активність у корпоративній мережі. Важливою перевагою таких рішень є можливість автоматичного виявлення аномалій на основі аналізу поведінки користувачів, пристроїв та мережевого трафіку. Завдяки застосуванню алгоритмів машинного навчання система здатна визначати відхилення від нормальної поведінки навіть у випадках, коли атака використовує раніше невідомі методи проникнення.

Крім того, перспективним напрямом є використання штучного інтелекту для аналізу мережевого трафіку та виявлення потенційних ознак кібератак на ранніх етапах їх реалізації. Автоматизовані системи можуть визначати нетипові мережеві з’єднання, підозрілі дії користувачів або ознаки шкідливого програмного забезпечення значно швидше, ніж традиційні засоби моніторингу. Це дозволить скоротити час реагування на інциденти та мінімізувати можливі наслідки атак.

Доцільним також є впровадження механізмів автоматизованого реагування на кіберінциденти. У разі виявлення підозрілої активності система може автоматично блокувати облікові записи, обмежувати мережеві з’єднання або ізолювати скомпрометовані пристрої без участі оператора. Такий підхід дозволить підвищити ефективність роботи підрозділів цифрової безпеки та забезпечити більш високий рівень захисту інформаційних ресурсів підприємства.

Важливим стратегічним напрямом розвитку системи цифрової безпеки ПрАТ «Київстар» є також підвищення рівня цифрової стійкості. На відміну від традиційного підходу до кіберзахисту, концепція цифрової стійкості орієнтована не лише на запобігання інцидентам, а й на забезпечення здатності підприємства продовжувати функціонування навіть у разі успішної реалізації кібератаки або технічного збою [36].

Основою цифрової стійкості є резервування критично важливої інфраструктури та створення механізмів швидкого відновлення роботи

інформаційних систем. Для ПрАТ «Київстар» доцільним є подальший розвиток резервних дата-центрів, дублювання критичних каналів зв’язку та впровадження сучасних систем резервного копіювання даних. Це дозволить забезпечити безперервність надання телекомунікаційних послуг навіть у випадку виникнення надзвичайних ситуацій.

Не менш важливим елементом є розробка та регулярне оновлення планів відновлення після кіберінцидентів відповідно до концепції Disaster Recovery. Такі плани повинні визначати порядок дій персоналу у разі виникнення аварійних ситуацій, механізми відновлення інформаційних систем та строки повернення до штатного режиму роботи. Наявність детально опрацьованих сценаріїв реагування дозволяє мінімізувати наслідки інцидентів та скоротити час простою цифрової інфраструктури [37].

Крім того, доцільним є впровадження принципів Business Continuity Management, які спрямовані на забезпечення безперервності бізнес-процесів підприємства в умовах кризових ситуацій. Реалізація даного підходу дозволить ПрАТ «Київстар» підтримувати стабільність надання послуг, зберігати довіру клієнтів та забезпечувати виконання стратегічних цілей навіть за умов виникнення значних кіберзагроз або техногенних інцидентів [38].

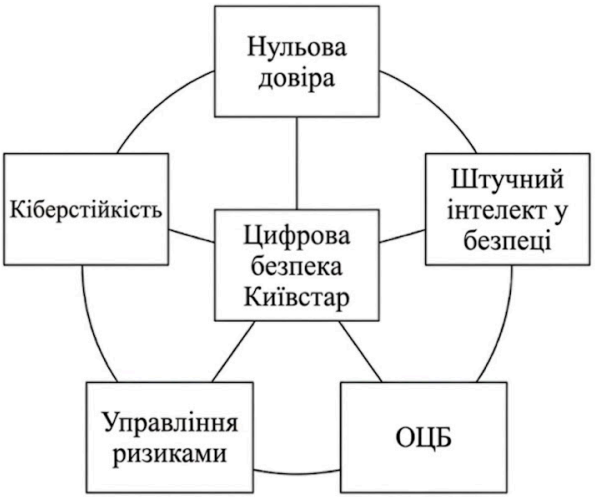

Рисунок 3.1 – Стратегічні напрями розвитку цифрової безпеки ПрАТ «Київстар»

Примітка. Авторська розробка.

Посилення управління кіберризиками, впровадження технологій штучного інтелекту та розвиток цифрової стійкості формують комплексний стратегічний підхід до вдосконалення процесу управління цифровою безпекою ПрАТ «Київстар». Реалізація зазначених заходів дозволить підвищити рівень захищеності цифрової інфраструктури, знизити ймовірність успішної реалізації кіберзагроз та забезпечити стабільний розвиток підприємства в умовах цифрової трансформації економіки.

3.2. Розробка комплексного забезпечення системи управління цифровою безпекою підприємства ПрАТ «Київстар»

Реалізація запропонованих у підрозділі 3.1 стратегічних напрямів розвитку цифрової безпеки потребує формування комплексної системи забезпечення управління цифровою безпекою ПрАТ «Київстар». На сьогодні питання забезпечення цифрової безпеки у ПрАТ «Київстар» реалізуються через взаємодію декількох управлінських напрямів. Технічний директор Володимир Лутченко відповідає за функціонування телекомунікаційної мережі, розвиток інфраструктури та забезпечення безперервності роботи цифрових сервісів. Директор з інформаційних технологій та директор Kyivstar.Tech Андрій Жуковський координує діяльність ІТ-підрозділів, розвиток цифрових платформ, автоматизацію бізнес-процесів та підтримку інформаційних систем. Важливу роль у сфері управління ризиками та контролю відіграє директорка з комплаєнсу та етики Тетяна Кирик, яка забезпечує дотримання корпоративних стандартів, внутрішній контроль та управління ризиками.

Незважаючи на наявність розподілу відповідальності між окремими напрямами діяльності, доцільним є створення централізованої системи управління цифровою безпекою на основі посади директора з цифрової безпеки (Chief Information Security Officer – CISO). Запровадження такої посади дозволить об'єднати функції управління цифровими ризиками, контролю

кібербезпеки та координації діяльності всіх структурних підрозділів, які беруть участь у забезпеченні цифрового захисту підприємства.

Пропонується впровадити наступну організаційну структуру управління цифровою безпекою:

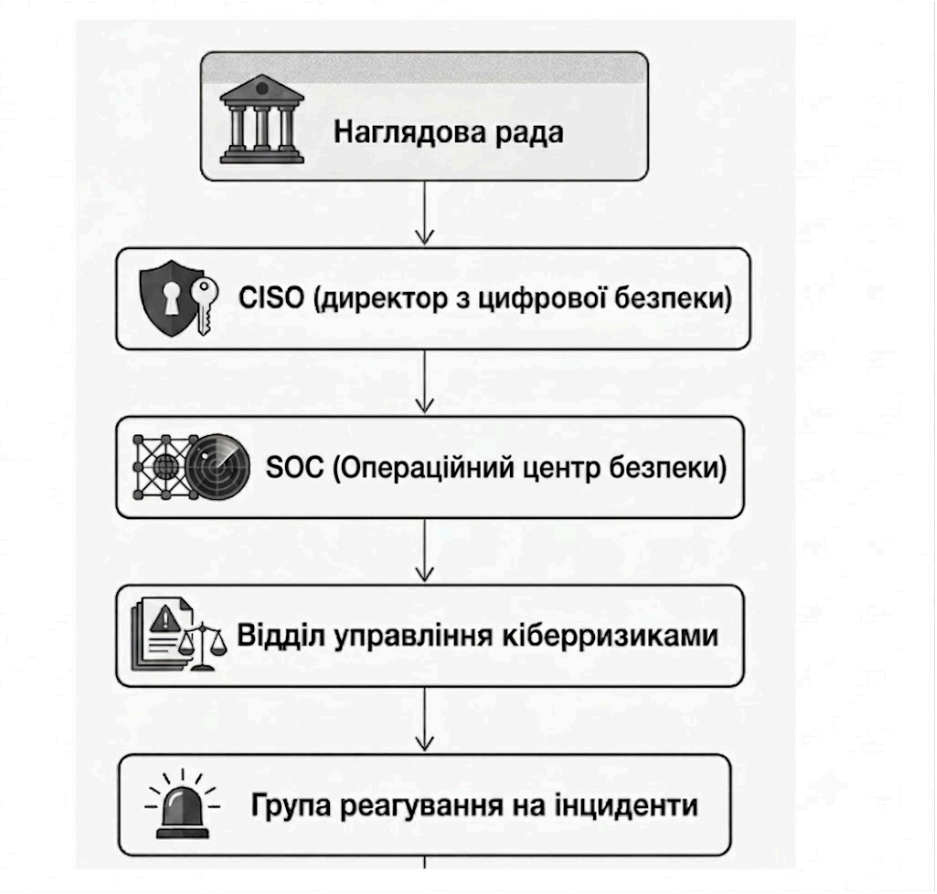

Рисунок 3.2 – Запропонована структура управління цифровою безпекою ПрАТ «Київстар»

Примітка. Авторська розробка.

У межах запропонованої структури CISO відповідатиме за формування політики цифрової безпеки, координацію діяльності підрозділів та контроль виконання стратегічних цілей у сфері кіберзахисту. Це дозволить забезпечити єдину систему прийняття рішень та підвищити ефективність управління цифровою безпекою підприємства.

У запропонованій моделі ключову роль відіграватиме SOC, який здійснюватиме цілодобовий моніторинг інформаційної інфраструктури

підприємства. Основними функціями SOC повинні стати моніторинг подій інформаційної безпеки у режимі 24/7, виявлення кіберзагроз, аналіз інцидентів та координація процесів реагування на них.

Відділ управління кіберризиками повинен забезпечувати проведення оцінки цифрових ризиків, формування реєстру ризиків, організацію аудитів безпеки та підготовку звітності для керівництва підприємства. Діяльність даного підрозділу має бути спрямована на впровадження ризик-орієнтованого підходу до управління цифровою безпекою.

Окреме місце в організаційній структурі повинна займати група реагування на інциденти. Основними функціями цього підрозділу є локалізація кібератак, усунення наслідків інцидентів, відновлення функціонування інформаційних систем та проведення внутрішніх розслідувань причин виникнення кіберінцидентів. Такий підхід дозволить значно скоротити час реагування на загрози та мінімізувати можливі збитки.

Для підвищення ефективності управління цифровою безпекою доцільним є створення єдиного інформаційного середовища кіберзахисту. Основою такого середовища повинна стати сучасна SIEM-система (Security Information and Event Management), яка забезпечуватиме централізований збір, аналіз та кореляцію подій інформаційної безпеки з усіх інформаційних ресурсів підприємства.

Важливим елементом інформаційного забезпечення повинна стати платформа Threat Intelligence Platform, яка забезпечуватиме накопичення та аналіз інформації про актуальні кіберзагрози, нові вразливості та методи здійснення атак. Використання таких рішень дозволить реалізувати проактивний підхід до управління цифровою безпекою.

Доцільним також є створення централізованої бази кіберінцидентів, яка міститиме інформацію про всі виявлені інциденти, заходи реагування та результати їх усунення. На основі цієї бази можуть формуватися автоматизовані дашборди для керівництва підприємства, що забезпечуватимуть оперативний контроль рівня цифрової безпеки та основних показників кіберризиків.

Рекомендована схема потоків інформації може мати такий вигляд:

Рисунок 3.3 – Рекомендована схема потоків інформації

Примітка. Авторська розробка.

Важливою складовою вдосконалення системи управління цифровою безпекою є формування сучасної нормативної бази підприємства. Для цього доцільно розробити та затвердити пакет внутрішніх документів, які регламентуватимуть порядок забезпечення цифрової безпеки.

До складу такого пакета пропонується включити Політику цифрової безпеки, Політику управління доступом, Політику резервного копіювання даних, План реагування на кіберінциденти та План відновлення після аварійних ситуацій.

Під час розробки зазначених документів доцільно використовувати вимоги міжнародного стандарту ISO/IEC 27001, рекомендації NIST

Cybersecurity Framework та положення європейської директиви NIS2. Це забезпечить відповідність системи цифрової безпеки міжнародним практикам та підвищить рівень кіберстійкості підприємства.

Людський фактор залишається одним із ключових джерел цифрових ризиків, тому важливим напрямом удосконалення системи цифрової безпеки є розвиток кадрового забезпечення. З метою підвищення рівня цифрової грамотності персоналу доцільно впровадити систему регулярного навчання співробітників з питань кібербезпеки.

Особливу увагу необхідно приділяти проведенню тестових фішингових кампаній, які дозволять оцінити готовність працівників до протидії атакам соціальної інженерії. Результати таких тестувань можуть використовуватися для подальшого вдосконалення програм навчання.

Для працівників підрозділів цифрової безпеки доцільно передбачити проходження міжнародної сертифікації, участь у професійних тренінгах та програмах підвищення кваліфікації. Одночасно необхідно формувати культуру кібербезпеки на всіх рівнях управління підприємством, що сприятиме зменшенню ризиків, пов’язаних із людським фактором.

Впровадження комплексних заходів із модернізації цифрової безпеки ПрАТ «Київстар» дозволить суттєво підвищити захищеність корпоративної інфраструктури та оптимізувати внутрішні процеси реагування на кіберзагрози. Одним із фундаментальних кроків є перехід на архітектуру Zero Trust, що безпосередньо знизить ризик несанкціонованого доступу до критично важливих інформаційних ресурсів. Крім того, розгортання системи SIEM у поєднанні зі створенням власного ситуаційного центру безпеки забезпечить цілодобовий моніторинг цифрового середовища та дозволить критично скоротити час, необхідний для виявлення та локалізації кіберинцидентів.

Паралельно з цим компанія планує активно залучати сучасні технологічні інструменти, зокрема AI-моніторинг, який допоможе повністю автоматизувати процеси виявлення та первинного реагування на виникаючі загрози. Системний підхід до управління потенційними загрозами буде забезпечено через ведення

детального Реєстру кіберризиків, що значно підвищить загальну ефективність менеджменту безпеки. У разі виникнення масштабних кризових ситуацій, чітко структурований план аварійного відновлення гарантуватиме мінімальні терміни відновлення стабільної роботи систем після будь-яких інцидентів.

Окрему увагу в межах стратегії вдосконалення безпеки приділено людському фактору. Організація регулярного та якісного навчання персоналу дозволить сформувати високу культуру кібергігієни серед співробітників, що призведе до помітного зменшення кількості успішних фішингових атак, які часто є головною точкою входу для зловмисників.

Висновки до розділу 3

1. Визначено стратегічні напрями розвитку процесу управління цифровою безпекою ПрАТ «Київстар» в умовах тривалого воєнного стану та постійної еволюції гібридних кіберзагроз. Обґрунтовано необхідність комплексного переходу компанії від традиційного захисту периметра до сучасної архітектури нульової довіри. Доведено, що стратегічний менеджмент кіберстійкості телекомунікаційного оператора як об'єкта критичної інфраструктури має базуватися на інтеграції ризик-менеджменту в загальну систему корпоративного управління та посиленні координації з державними інституціями.

2. Сформульовано та обґрунтовано комплексне забезпечення системи управління цифровою безпекою ПрАТ «Київстар», що поєднує техніко-технологічні, організаційні та кадрові заходи. Запропоновано масштабне залучення інструментів штучного інтелекту для автоматизації процесів раннього виявлення кіберинцидентів, формування деталізованого Реєстру кіберризиків та впровадження плану аварійного відновлення. Системний підхід доповнено заходами з розвитку внутрішньої культури кібербезпеки персоналу шляхом впровадження регулярних навчань та тестових фішингових кампаній для мінімізації впливу людського фактора.

ВИСНОВКИ

У результаті проведеного дослідження було досягнуто поставленої мети, яка полягала в обґрунтуванні теоретико-методичних засад та розробці практичних рекомендацій щодо вдосконалення процесу управління цифровою безпекою ПрАТ «Київстар» з метою підвищення його економічної стійкості. Для досягнення поставленої мети було виконано такі завдання та отримано відповідні результати.

1. Досліджено сутність цифрової безпеки підприємства та її роль у забезпеченні економічної стійкості. Встановлено, що цифрова безпека є одним із ключових чинників стабільного функціонування сучасного підприємства, оскільки забезпечує захист інформаційних активів, безперервність бізнес-процесів, зниження ризику фінансових втрат та підтримання довіри клієнтів і партнерів. Обґрунтовано, що ефективне управління цифровою безпекою безпосередньо впливає на конкурентоспроможність та довгострокову економічну стійкість організації.

2. Визначено основні підходи до процесу управління цифровою безпекою підприємства. Встановлено, що управління цифровою безпекою являє собою безперервний управлінський цикл, який включає ідентифікацію загроз, оцінювання ризиків, розроблення політик безпеки, впровадження технічних засобів захисту та навчання персоналу. За результатами порівняння реактивної та проактивної моделей доведено переваги проактивного підходу, який забезпечує своєчасне виявлення та попередження кіберзагроз.

3. Проаналізовано світовий досвід управління цифровою безпекою підприємств. Визначено, що найбільш поширеними міжнародними практиками є застосування стандарту ISO/IEC 27001 та рамкової моделі NIST Cybersecurity Framework. Доведено, що використання зазначених підходів сприяє формуванню комплексної системи управління безпекою, підвищенню рівня

кіберстійкості та переходу до концепції нульової довіри як сучасного механізму захисту цифрових ресурсів підприємства.

4. Проведено аналіз об’єкта та суб’єкта процесу управління цифровою безпекою ПрАТ «Київстар». Встановлено, що об’єктом управління виступає масштабна цифрова інфраструктура підприємства, яка включає телекомунікаційні мережі, дата-центри, хмарні сервіси та інформаційні ресурси компанії. Визначено, що суб’єкт управління представлений керівництвом компанії, профільними підрозділами інформаційної та кібербезпеки, IT-службами та операційним персоналом. Доведено необхідність посилення координації між структурними підрозділами для забезпечення належного рівня захисту інформаційних активів.

5. Здійснено діагностику фінансово-господарської діяльності ПрАТ «Київстар». Результати аналізу підтвердили високий рівень економічної стійкості та ринкового лідерства підприємства. Водночас встановлено, що фінансові результати компанії значною мірою залежать від стабільності функціонування цифрової інфраструктури та безперервності надання телекомунікаційних послуг. Виявлено, що суттєві інвестиції у відновлення та модернізацію інфраструктури є необхідною умовою підтримання конкурентних позицій компанії.

6. Оцінено процес управління цифровою безпекою та його вплив на економічну стійкість підприємства. На основі аналізу наслідків масштабної кібератаки на ПрАТ «Київстар» у 2023 році встановлено, що реалізація кіберзагроз може спричиняти значні прямі фінансові втрати, додаткові витрати на ліквідацію наслідків інцидентів та суттєві репутаційні ризики. Доведено, що недостатня адаптивність системи захисту негативно впливає на економічну стійкість підприємства та підвищує його вразливість до зовнішніх загроз.

7. Обґрунтовано стратегічні напрями вдосконалення процесу управління цифровою безпекою ПрАТ «Київстар». Визначено доцільність переходу від традиційної моделі кіберзахисту до концепції кіберстійкості, яка передбачає забезпечення здатності підприємства підтримувати функціонування навіть в

умовах успішної реалізації кібератак. За результатами SWOT-аналізу та PESTLE-аналізу сформовано комплекс стратегічних заходів, спрямованих на підвищення рівня цифрової безпеки, ефективніше управління ризиками та зміцнення економічної стійкості підприємства.

8. Розроблено комплексне забезпечення системи управління цифровою безпекою ПрАТ «Київстар», яке охоплює організаційне, технічне, інформаційне та фінансово-економічне забезпечення. Запропоновано удосконалення організаційної структури управління безпекою, впровадження сучасних інструментів моніторингу кіберзагроз, поглиблення сегментації мережі, використання автоматизованих платформ аналізу інцидентів та розвиток системи підготовки персоналу. Розрахунок прогнозного економічного ефекту підтвердив доцільність реалізації запропонованих заходів, їх високу ефективність та здатність забезпечити зниження потенційних збитків від кібератак, підвищення рівня кіберстійкості та зміцнення економічної стійкості підприємства у довгостроковій перспективі.

Результати проведеного дослідження підтверджують досягнення поставленої мети та можуть бути використані у практичній діяльності ПрАТ «Київстар» для вдосконалення системи управління цифровою безпекою, підвищення рівня захищеності цифрових активів та забезпечення стабільного економічного розвитку підприємства в умовах зростання кіберзагроз.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Xu J. Managing Digital Enterprise: Ten Essential Topics. Atlantis Press, 2014. 159 p.

2. Кібербезпека в інформаційному суспільстві: *Інформаційно-аналітичний дайджест* / відп. ред. О.Довгань; упоряд. О.Довгань, Л.Литвинова, С.Дорогих; Державна наукова установа «Інститут інформації, безпеки і права НАПрН України»; Національна бібліотека України ім. В.І.Вернадського. К., 2023. №9 (вересень) . 351 с.

3. What is Digital Security: Overview, Types, and Application. URL: https://www.eccu.edu/blog/what-is-digital-security-overview-types-and-application/ (дата звернення 07.05.2026)

4. Що таке кібератака? URL: https://datami.ee/ua/blog/what-is-a-cyberattack/ (дата звернення 07.05.2026)

5. Кібербезпека для бізнесу. URL: https://datami.ee/ua/blog/cybersecurity-for-business-importance-and-tips-datami/ (дата звернення 07.05.2026)

6. Шейко І.А., Степаненко Р.Д. Управління цифровими вразливостями сучасного підприємства. Економіка і управління. 2025. Вип. 2. С. 112–119. DOI: https://doi.org/10.32782/2312-7872.2.2025.15.

7. Швець В.В. Удосконалення механізмів забезпечення інформаційної безпеки в системі публічного управління в умовах цифрової трансформації. Білоцерківський національний аграрний університет. Біла Церква, 2025. 88 с.

8. Силко С.С. Методи управління безпекою мобільних пристроїв на підприємстві відповідно до концепції NIST. Цифрова трансформація кібербезпеки : тези доповідей Всеукр. наук.-практ. конф. (Київ, 26 квітня 2024 р.). Київ : Державний університет інформаційно-комунікаційних технологій, 2024. С. 98–100.

9. Що таке CESS Network? Пояснення децентралізованої системи.URL: https://www.gate.com/uk/learn/articles/what-is-cess-network/8781 (дата звернення 08.05.2026)

10. Implementing Proactive Cybersecurity Measures vs. Reactive Tactics. URL: https://dotsecurity.com/insights/blog-reactive-proactive-cybersecurity-measures (дата звернення 08.05.2026)

11. Strategic Management in Cyber Security: A Full Overview. URL: https://lset.uk/ethical-hacking/strategic-management-in-cyber-security-a-full-overview/ (дата звернення 08.05.2026)

12. ISO/IEC 2700. URL: https://w.wiki/4aDF (дата звернення 08.05.2026)

13. What is the NIST Cybersecurity Framework? URL: https://www.ibm.com/think/topics/nist (дата звернення 08.05.2026)

14. The risk-based approach to cybersecurity. URL: https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/the-risk-based-approach-to-cybersecurity (дата звернення 08.05.2026)

15. Global Cybersecurity Spending To Exceed $1.75 Trillion From 2021-2025. URL: https://cybersecurityventures.com/cybersecurity-spending-2021-2025/ (дата звернення 08.05.2026)

16. Guide to Getting Started with a Cybersecurity Risk Assessment. Cybersecurity and Infrastructure Security Agency (CISA). 2022. 8 p.

17. Загальний регламент про захист даних (GDPR). URL: https://www.esri.com/uk-ua/privacy/privacy-gdpr (дата звернення 08.05.2026)

18. Директива ЄС NIS2: що це таке, для яких потреб розроблена. URL: https://cip.gov.ua/ua/news/direktiva-yes-nis2-sho-ce-take-dlya-yakikh-potreb-rozroblena-ta-dlya-chogo-ukrayina-yiyi-implementuye (дата звернення 08.05.2026)

19. Why Israel remains the epicenter of global cybersecurity innovation. URL: https://www.calcalistech.com/ctechnews/article/ovesg12ne#google_vignette (дата звернення 08.05.2026)

20. Japan’s Cybersecurity Strategy 2021. URL: https://dig.watch/resource/japans-cybersecurity-strategy-2021 (дата звернення 08.05.2026)

21. Zero Trust: Microsoft’s Approach to Modern Cybersecurity. URL: https://connect.tdsynnex.be/blog/media-library/zero-trust-microsofts-approach-to-modern-cybersecurity/ (дата звернення 09.05.2026)

22. What is BeyondCorp? URL: https://www.paloaltonetworks.com/cyberpedia/what-is-beyondcorp (дата звернення 09.05.2026)

23. CYBER SECURITY. URL: https://www.vodafone.com/sustainable-business/maintaining-trust/society/security-and-resilience/cyber-security?section=our-approach (дата звернення 09.05.2026)

24. Amazon (AMZN) Embraces New Cybersecurity Standards for Defense Contractors. URL: https://www.gurufocus.com/news/8839878/amazon-amzn-embraces-new-cybersecurity-standards-for-defense-contractors (дата звернення 08.05.2026)

25. Pugachov O. I. (2024). Problems of Ensuring Information Security of Ukraine in Modern Conditions. Problems of Modern Transformations. Series: Law, Public Management and Administration, (12). https://doi.org/10.54929/2786-5746-2024-12-02-15

26. ПРИВАТНЕ АКЦІОНЕРНЕ ТОВАРИСТВО "КИЇВСТАР". URL: https://clarity-project.info/edr/21673832 (дата звернення 28.05.2026)

27. Київстар сьогодні. URL: https://kyivstar.ua/about/kyivstar-today (дата звернення 28.05.2026)

28. Інформація для акціонерів та стейкхолдерів. URL: https://kyivstar.ua/about/investors-and-shareholders/issuers (дата звернення 29.05.2026)

29. 21673832 - ПРИВАТНЕ АКЦІОНЕРНЕ ТОВАРИСТВО "КИЇВСТАР". URL: https://smida.gov.ua/db/prof/21673832 (дата звернення 29.05.2026)

30. Як цифрова монополія Київстару загрожує українцям. URL: https://webscraft.org/blog/yak-tsifrova-monopoliya-kiyivstaru-zagrozhuye-ukrayintsyam?lang=de (дата звернення 30.05.2026)

31. Якою була атака хакерів на «Київстар» та як відновлювалась компанія. URL: https://dou.ua/lenta/news/kyivstar-cyber-attack-restoration/ (дата звернення 30.05.2026)

32. Подзігун , С.М., Білошкурська , Н.В., Омельяненко , В.А., & Корнєєва, О.О. (2024). Аналіз конкурентоспроможності мобільних операторів України на основі бенчмаркінгу: оцінка ринку та формування інноваційного бізнес-середовища. Здобутки економіки: перспективи та інновації, (11).

33. What is threat intelligence? URL: https://www.ibm.com/think/topics/threat-intelligence (дата звернення 07.06.2026)

34. What is Zero Trust Architecture (ZTA)? URL: https://www.paloaltonetworks.com/cyberpedia/what-is-a-zero-trust-architecture (дата зверненян 07.06.2026)

35. Що таке сегментація мережі та чому вона важлива? URL: https://www.hostragons.com/uk/

36. What is cyber resilience? URL: https://www.ecb.europa.eu/paym/cyber-resilience/html/index.en.html (дата звернення 07.06.2026)

37. What is disaster recovery? URL: https://cloud.google.com/learn/what-is-disaster-recovery (дата звернення 07.06.2026)

38. What is business continuity? URL: https://www.ibm.com/think/topics/business-continuity (дата звернення 07.06.2026)

ДОДАТКИ