МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
**ДЕРЖАВНИЙ УНІВЕРСИТЕТ ЕКОНОМІКИ І ТЕХНОЛОГІЙ**

| | |
|---|---|
| ННІ/факультет | *ННІ економіки та бізнес-освіти* |
| Кафедра | *Управління бізнесом* |
| Спеціальність | *073 Менеджмент* |
| Форма навчання | *денна* |

# КВАЛІФІКАЦІЙНА РОБОТА МАГІСТРА

**Шефа Дмитра Олеговича**

на тему **Ризик менеджмент в галузі мобільних технологій**

за матеріалами **компанії Apple Center**

науковий керівник **д-р. екон. наук, професор** _____ **Гушко С.В.**

*(підпис)*

**Робота допущена до захисту в ЕК**
Протокол засідання кафедри
від 16.01.2026 р. № 5__
Завідувач кафедри _____
(підпис)

*д.соц..н., професор* *Г.І.Андрущенко*

*Наук. ступень, вчене звання* *Ініціали, прізвище*

Кривий Ріг – 2026

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
**ДЕРЖАВНИЙ УНІВЕРСИТЕТ ЕКОНОМІКИ І ТЕХНОЛОГІЙ**

| | |
|---|---|
| ННІ/факультет | *ННІ економіки та бізнес-освіти* |
| Кафедра | *Управління бізнесом* |
| Спеціальність | *073 Менеджмент* |
| Форма навчання | *денна* |

«ЗАТВЕРДЖУЮ»
Завідувач кафедри _____ *Андрущенко Г.І..*
(підпис) (Прізвище, ініціали)
«26» жовтня 2025 року

# ЗАВДАННЯ
# НА КВАЛІФІКАЦІЙНУ РОБОТУ МАГІСТРА

1.Тема роботи: Ризик менеджмент в галузі мобільних технологій

Керівник роботи Гушко С.В.
затверджені наказом закладу вищої освіти від «20» жовтня 2025 р. №721-ст

2. Строк подання здобувачем роботи до «12» січня 2026 р.

3. Зміст кваліфікаційної роботи, об'єкт, предмет та мета дослідження:

| |
|---|
| **РОЗДІЛ 1. ТЕОРЕТИЧНІ ТА МЕТОДОЛОГІЧНІ ЗАСАДИ РИЗИК-МЕНЕДЖМЕНТУ В МОБІЛЬНИХ ТЕХНОЛОГІЯХ** |
| 1.1. Еволюція ризик-менеджменту в цифровій економіці |
| 1.2. Класифікація ризиків у сфері мобільних технологій |
| 1.3. Методологічні підходи та інструменти управління ризиками (ISO 31000, COSO ERM, NIST, цифрова аналітика ризиків) |
| 1.4. Нормативно-правове та етичне регулювання ризик-менеджменту в IT-сфері |
| Висновки до розділу 1 |
| **РОЗДІЛ 2. АНАЛІТИКО-ПРАКТИЧНЕ ДОСЛІДЖЕННЯ РИЗИК МЕНЕДЖМЕНТУ КОМПАНІЇ «APPLE CENTER»** |
| 2.1. Загальна характеристика діяльності «Apple Center» та його позиції на ринку мобільних технологій |
| 2.2. Ідентифікація ключових ризиків у діяльності компанії |
| 2.3. Оцінка ефективності системи управління ризиками |
| 2.4. SWOT-аналіз, PEST-аналіз та виявлення вразливих зон у ризик-профілі компанії |
| Висновки до розділу 2 |
| **РОЗДІЛ 3. ІННОВАЦІЙНІ ПІДХОДИ ДО ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ РИЗИК-МЕНЕДЖМЕНТУ В «APPLE CENTER»…..51** |
| 3.1. Розробка стратегії цифрового ризик-менеджменту |
| 3.2. Використання аналітики великих даних, штучного інтелекту та блокчейну для моніторингу ризиків |

*Об'єкт дослідження:* процеси управління ризиками в галузі мобільних технологій у діяльності підприємств та організацій, що займаються розробкою, впровадженням і використанням мобільних рішень.

*Предмет дослідження:* сукупність методів, інструментів і підходів ризикменеджменту, спрямованих на виявлення, оцінювання та мінімізацію технічних, інформаційних, фінансових і кібернетичних ризиків у сфері мобільних технологій.

*Мета кваліфікаційної роботи*: полягає у тому, щоб теоретично обґрунтувати та практично дослідити ризик менеджмент в галузі мобільних технологій компанії «Apple Center»

5. Дата видачі завдання «26» жовтня 2025 р.

*КАЛЕНДАРНИЙ ПЛАН*

| № з/п | Назва етапів МДР | Строк виконання етапів роботи | Відмітка керівника про виконання етапів (дата, підпис) |
|---|---|---|---|
| 1 | Підготовка розділу 1 | до 08.12.2025 р. | |
| 2 | Підготовка розділу 2 | до 23.12.2025 р. | |
| 3. | Підготовка розділу 3 | до 08.01.2026 р. | |
| 4. | Підготовка вступу та висновків | до 10.01.2026 р. | |
| 5. | Надання електронного варіанту роботи для перевірки на плагіат | до 12.01.2026 р. | |
| 6. | Доопрацювання роботи після перевірки на плагіат (у разі необхідності) | до 15.01.2026 р. | |
| 4 | Отримання відгуку від наукового керівника та зовнішньої рецензії | до 15.01.2026 р. | |
| 5 | Подання кваліфікаційної роботи на перегляд завідувачу кафедри | 16.01.2026 р. | |
| 6 | Реєстрація завершеної кваліфікаційної роботи | 17.01.2026 р. | |
| 7 | Попередній захист кваліфікаційної роботи на кафедрі | 18.01.2026 р. | |
| 8 | Підготовка до захисту в ЕК | до 19.01.2026 р. | |

## Анотація

Шеф Д.О. Ризик менеджмент в галузі мобільних технологій

Кваліфікаційна робота магістра за спеціальністю 073 «Менеджмент». Державний університет економіки і технологій. Кривий Ріг, 2026.

Кваліфікаційна робота магістра присвячена дослідженню теоретичних, методологічних та практичних аспектів ризик-менеджменту в умовах розвитку мобільних технологій та цифрової економіки. У роботі розглянуто сутність і еволюцію ризик-менеджменту, класифікацію ризиків у сфері мобільних технологій, а також сучасні міжнародні методологічні підходи й інструменти управління ризиками.

В роботі проаналізовано розвиток ризик-менеджменту в цифровій економіці, охарактеризовано основні види ризиків, притаманні сфері мобільних технологій, розкрито методологічні основи управління ризиками відповідно до міжнародних стандартів ISO 31000, COSO ERM, NIST та підходів цифрової аналітики. Окрему увагу приділено нормативно-правовому й етичному регулюванню ризик-менеджменту в IT-сфері.

У кваліфікаційній роботі було приділено увагу аналітико-практичному дослідженню системи управління ризиками компанії «Apple Center». Подано загальну характеристику діяльності компанії та її позицій на ринку мобільних технологій, здійснено ідентифікацію ключових ризиків, оцінено ефективність наявної системи ризик-менеджменту. За допомогою SWOT- та PEST-аналізу визначено вразливі зони ризик-профілю компанії.

Запропоновано інноваційні підходи до підвищення ефективності ризик-менеджменту в компанії «Apple Center», зокрема розроблено стратегію цифрового ризик-менеджменту, обґрунтовано доцільність використання аналітики великих даних, штучного інтелекту та блокчейн-технологій для моніторингу ризиків. Також здійснено оцінку економічного, соціального та репутаційного ефекту від упровадження запропонованих заходів.

ЗМІСТ

# ВСТУП

**Актуальність теми** ризик-менеджменту в галузі мобільних технологій зумовлена стрімким розвитком цифрових рішень, зростанням кількості мобільних додатків і широким використанням смартфонів у повсякденному житті, бізнесі та державному управлінні. Мобільні технології стали ключовим інструментом комунікації, фінансових операцій, зберігання персональних даних і доступу до інформаційних ресурсів, що значно підвищує рівень технічних, інформаційних і кібернетичних ризиків. Загрози витоку даних, кібератак, програмних збоїв, а також залежність користувачів і організацій від стабільності мобільних сервісів потребують системного підходу до управління ризиками та забезпечення безпеки.

Крім того, актуальність ризик-менеджменту в галузі мобільних технологій посилюється високою динамічністю ринку, швидкою зміною технологічних стандартів і жорсткою конкуренцією між розробниками та провайдерами послуг. Невчасне реагування на ризики може призвести до фінансових втрат, зниження довіри користувачів, погіршення репутації компаній і порушення законодавчих вимог щодо захисту персональних даних. У таких умовах ефективний ризик-менеджмент стає необхідною складовою стратегічного управління, що забезпечує сталий розвиток мобільних технологій та підвищує їхню надійність і безпеку.

**Мета роботи** полягає у тому, щоб теоретично обґрунтувати та практично дослідити ризик менеджмент в галузі мобільних технологій компанії «Apple Center»;

Для виконання мети магістерської роботи ставимо такі **завдання**:

1. Дослідити еволюцію ризик-менеджменту в цифровій економіці та їх класифікацію;

2. Проаналізувати методологічні підходи та інструменти управління ризиками (ISO 31000, COSO ERM, NIST, цифрова аналітика ризиків)

3. Розглянути нормативно-правове та етичне регулювання ризик-менеджменту в ІТ-сфері;

4. Надати загальну характеристику діяльності «Apple Center», його позиції на ринку мобільних технологій та зробити ідентифікація ключових ризиків у діяльності компанії;

5. Оцінити ефективність системи управління ризиками та виконати SWOT-аналіз, PEST-аналіз;

6. Розробити стратегії цифрового ризик-менеджменту та оглянути використання аналітики великих даних, штучного інтелекту та блокчейну для моніторингу ризиків;

7. Впровадити системи кіберстійкості та реагування на інциденти;

8. Зробити оцінку економічного, соціального та репутаційного ефекту від впроваджених заходів.

**Об'єкт дослідження** – процеси управління ризиками в галузі мобільних технологій у діяльності підприємств та організацій, що займаються розробкою, впровадженням і використанням мобільних рішень.

**Предмет дослідження** – сукупність методів, інструментів і підходів ризик-менеджменту, спрямованих на виявлення, оцінювання та мінімізацію технічних, інформаційних, фінансових і кібернетичних ризиків у сфері мобільних технологій.

Методи дослідження.

**Теоретична значущість отриманих результатів** полягає в поглибленні наукових уявлень про сутність і особливості ризик-менеджменту в галузі мобільних технологій. У роботі систематизовано основні види ризиків, характерні для діяльності компаній, що працюють із мобільними продуктами та сервісами, а також уточнено підходи до їх класифікації з урахуванням сучасних технологічних і ринкових умов.

**Методична значущість дослідження** полягає в розробленні та обґрунтуванні методичних підходів до оцінювання й управління ризиками в діяльності компанії Apple Center. Запропоновані методи і процедури можуть бути використані як методичний інструментарій для аналізу ризиків,

прийняття управлінських рішень та підвищення ефективності системи ризик-менеджменту в компаніях, що працюють у сфері мобільних технологій.

**Практична значущість отриманих результатів** полягає в можливості їх безпосереднього застосування в діяльності компанії Apple Center з метою зниження рівня ризиків, підвищення рівня безпеки та стабільності бізнес-процесів, а також покращення якості обслуговування клієнтів. Практичні рекомендації можуть бути використані керівництвом і фахівцями компанії для оптимізації управління ризиками та підвищення конкурентоспроможності.

**Наукова новизна дослідження** полягає в удосконаленні підходів до ризик-менеджменту в галузі мобільних технологій шляхом адаптації загальновідомих методів управління ризиками до специфіки діяльності компанії Apple Center. Уперше запропоновано комплексний підхід до оцінювання та мінімізації ризиків, який враховує технологічні, інформаційні та ринкові особливості функціонування компанії в сучасних умовах.

**Структура роботи**. Кваліфікаційна робота складається зі вступу, трьох розділів, висновків та списку використаної літератури. Робота включає в себе _ джерело зі списку літератури, а також представлена на _ сторінках друкованого тексту.

# РОЗДІЛ 1. ТЕОРЕТИЧНІ ТА МЕТОДОЛОГІЧНІ ЗАСАДИ РИЗИК-МЕНЕДЖМЕНТУ В МОБІЛЬНИХ ТЕХНОЛОГІЯХ

## 1.1. Еволюція ризик-менеджменту в цифровій економіці

Цифрова економіка суттєво трансформувала підходи до управління ризиками, зумовивши появу нових загроз і викликів для суб'єктів господарювання. Стрімкий розвиток інформаційних технологій, глобалізація ринків та активне використання цифрових платформ призвели до ускладнення бізнес-процесів і підвищення рівня невизначеності. За таких умов ризик-менеджмент поступово еволюціонував від фрагментарних заходів реагування на окремі загрози до системної управлінської діяльності, спрямованої на попередження, прогнозування та мінімізацію можливих негативних наслідків.

У процесі становлення цифрової економіки змінилися як характер ризиків, так і інструменти їх управління. Традиційні фінансові та виробничі ризики доповнилися інформаційними, кібернетичними, репутаційними та технологічними ризиками, пов'язаними з використанням цифрових рішень і великих обсягів даних. Це зумовило необхідність застосування нових методів аналізу, автоматизованих систем моніторингу та аналітичних моделей, що дозволяють оперативно виявляти потенційні загрози та оцінювати їх вплив на діяльність підприємств [1].

У 1970-х роках XX століття ризик-менеджмент перебував на початковому етапі розвитку та мав переважно мікрорівневий характер. Управління ризиками здійснювалося окремими фахівцями, зокрема брокерами та працівниками фінансових підрозділів, без чітко вибудуваної системи. Важливим поштовхом для розвитку кількісних підходів стало скасування у 1973 році Бреттон-Вудської системи фіксованих валютних курсів, що призвело до зростання валютних ризиків. У цей же період було опубліковано формулу Блека–Шоулза для оцінки вартості опціонів, яка започаткувала

активне використання математичних методів у вимірюванні та управлінні фінансовими ризиками [2].

У 1980-х роках XX століття увага зосереджується на управлінні активами й пасивами, насамперед на рівні казначейств фінансових установ. Ризик-менеджмент починає розглядатися як елемент стратегічного управління, що реалізується через планування та контроль фінансових потоків. Наприкінці цього десятиліття формується концепція Value-at-Risk, яка стала важливим інструментом оцінювання ринкових ризиків. Її практична реалізація відбулася завдяки системі RiskMetrics, розробленій банком J.P. Morgan, що сприяло стандартизації підходів до вимірювання ризиків.

У 1990-х роках XX століття ризик-менеджмент поступово набуває організаційної форми в межах фінансових департаментів і виокремлюється як самостійна управлінська функція. Управління ринковими та кредитними ризиками здійснюється шляхом їх системного контролю, а операційні ризики починають мінімізуватися через внутрішній аудит та регламентовані процедури. Важливими подіями цього періоду стали створення у 1996 році Міжнародної асоціації фахівців з управління ризиками (GARP) у Нью-Йорку та Лондоні, а також оприлюднення у 1997 році показника CreditVaR компанією RiskMetrics Group. Наприкінці десятиліття відбулося розширення діяльності GARP, що засвідчило зростання ролі професійних стандартів у сфері ризик-менеджменту [3].

На початку XXI століття сформувався корпоративний ризик-менеджмент (Enterprise Risk Management), який базується на комплексному підході до управління всіма видами ризиків у поєднанні з управлінням капіталом, активами та пасивами. Ризик-менеджмент стає інтегрованою частиною корпоративного управління та стратегічного розвитку компаній. Значний вплив на підвищення прозорості й надійності управління ризиками мало ухвалення у 2002 році закону Сарбейнса–Окслі, спрямованого на захист інвесторів та забезпечення достовірності корпоративної фінансової інформації відповідно до вимог законодавства.

Ризик-менеджмент являє собою цілісну систему управління ризиками, що ґрунтується на застосуванні різноманітних методів, інструментів і управлінських заходів. Вона дає змогу передбачати можливі ризики, оцінювати ймовірність їх виникнення та масштаби наслідків, а також завчасно запобігати небажаним подіям або зменшувати пов’язані з ними втрати. У межах ризик-менеджменту поєднуються стратегічні та тактичні підходи, де тактика спрямована на вибір найбільш доцільних управлінських рішень і методів відповідно до конкретних умов господарської діяльності [11].

Ризик-менеджмент можна розглядати як процес управління ризиками, що включає їх виявлення, комплексну оцінку та аналіз, а також обґрунтований вибір способів впливу на їхні наслідки. Основною метою такого підходу є забезпечення оптимального балансу між можливостями розвитку підприємства та допустимим рівнем ризику, що дозволяє уникнути як надмірної ризикованості, здатної призвести до фінансової неспроможності, так і повної відмови від ризику, яка обмежує конкурентні переваги [12].

Як зазначала А. Старостіна ризик-менеджмент є сукупністю організаційних та управлінських заходів, спрямованих на своєчасне виявлення й оцінювання ризиків, їх попередження та страхування. Така система поєднує стратегічне бачення з тактичними управлінськими рішеннями і забезпечує цілеспрямований вплив на ризики з метою зменшення їх негативного впливу на діяльність підприємства [9, с.34].

Ризик-менеджмент відіграє важливу роль у сучасній системі управління підприємством, оскільки забезпечує зниження рівня невизначеності в процесі прийняття управлінських рішень. Завдяки постійному аналізу можливих загроз і розробці заходів реагування керівництво отримує змогу своєчасно контролювати негативні події та впливати на ймовірність їх виникнення, що сприяє більш стабільному розвитку діяльності [5].

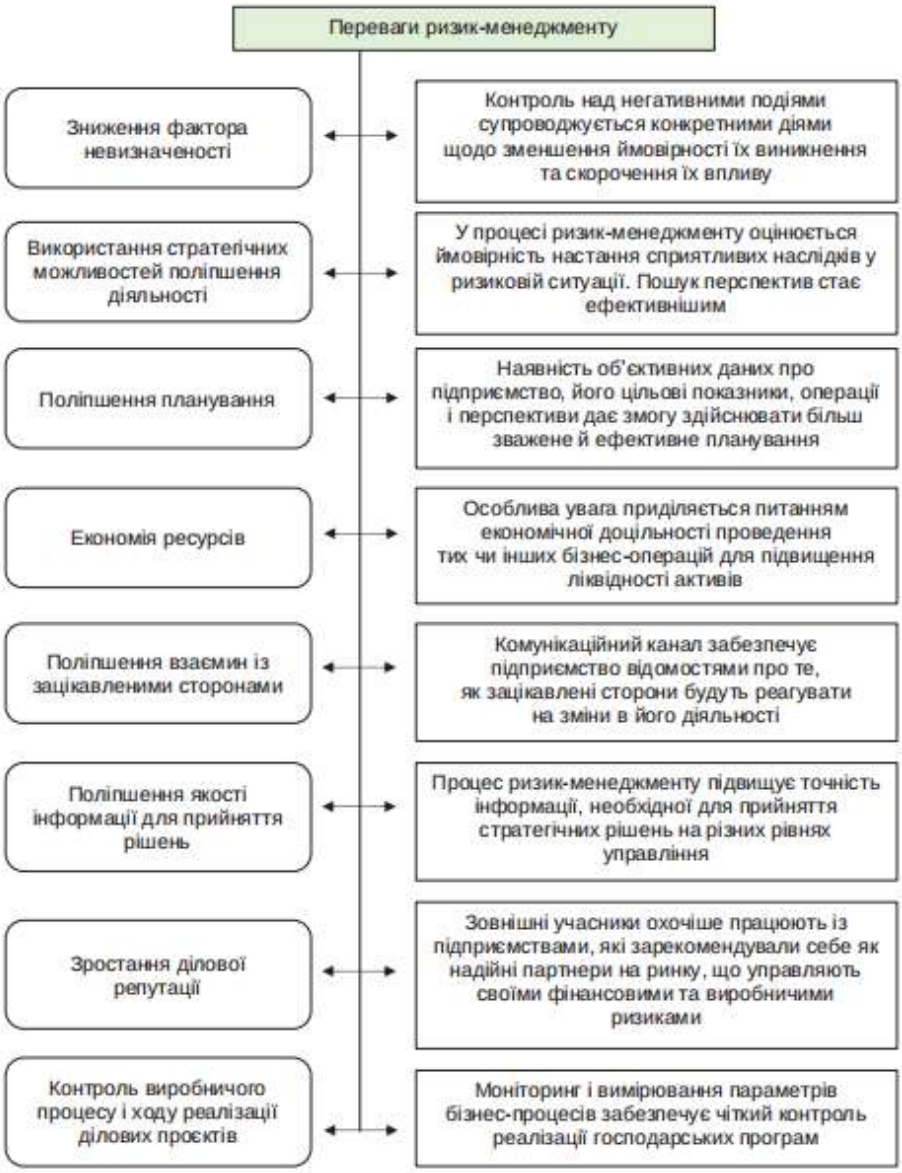


Рис. 1.1 – Переваги ризик-менеджменту в діяльності підприємства

Джерело: [9]

Однією з ключових переваг ризик-менеджменту є можливість ефективного використання стратегічних можливостей підприємства. Упорядкований підхід до оцінювання ризиків дозволяє не лише зменшувати потенційні втрати, а й своєчасно виявляти перспективні напрями розвитку. Це робить процес управління більш гнучким і дає змогу приймати обґрунтовані рішення в умовах ризикових ситуацій.

Впровадження ризик-менеджменту сприяє підвищенню якості планування. Наявність об’єктивної та систематизованої інформації щодо фінансових показників, операційної діяльності й майбутніх перспектив

дозволяє формувати реалістичні плани та прогнози. У результаті управлінські рішення стають більш зваженими та ефективними.

Важливою перевагою ризик-менеджменту є економія ресурсів підприємства. Контроль економічної доцільності проведення операцій і вибір оптимальних сценаріїв дій допомагають уникати зайвих витрат, підвищувати ліквідність активів і раціонально використовувати фінансові, матеріальні та трудові ресурси.

Ризик-менеджмент також сприяє налагодженню взаємодії із зацікавленими сторонами. Чітка комунікація та своєчасне інформування дозволяють партнерам, інвесторам і клієнтам оперативно реагувати на зміни в діяльності підприємства, що підвищує рівень довіри та зміцнює ділові відносини.

Крім того, ефективна система управління ризиками позитивно впливає на ділову репутацію підприємства. Зовнішні учасники ринку сприймають таку організацію як надійного партнера, здатного контролювати фінансові та виробничі ризики. Постійний моніторинг бізнес-процесів і контроль їх реалізації забезпечують стабільність функціонування та підвищують конкурентоспроможність у довгостроковій перспективі.

Таким чином, еволюція ризик-менеджменту в цифровій економіці характеризується переходом до комплексного та інтегрованого підходу, який поєднує стратегічне планування, використання цифрових інструментів і постійне вдосконалення управлінських рішень. Сучасний ризик-менеджмент стає невід’ємною складовою ефективного управління, забезпечуючи стабільний розвиток підприємств та їхню здатність адаптуватися до динамічних змін цифрового середовища.

## 1.2. Класифікація ризиків у сфері мобільних технологій

Стрімкий розвиток мобільних технологій та їх широке впровадження у всі сфери суспільного життя зумовлюють зростання рівня невизначеності та ризиків, пов’язаних із функціонуванням мобільних пристроїв, додатків і цифрових сервісів. Мобільні технології стали ключовим інструментом комунікації, бізнесу та доступу до інформації, що водночас підвищує вимоги до їх надійності, безпеки та відповідності очікуванням користувачів. У таких умовах класифікація ризиків набуває особливої актуальності, оскільки дозволяє систематизувати потенційні загрози та забезпечити більш ефективне управління ними.

Класифікація ризиків у сфері мобільних технологій є необхідною передумовою для формування комплексної системи ризик-менеджменту. Вона дає змогу ідентифікувати джерела виникнення ризиків, визначити характер їх впливу на діяльність компаній та оцінити можливі наслідки для користувачів і бізнесу. Чітке розмежування ризиків за окремими групами сприяє вибору адекватних методів їх мінімізації та підвищує ефективність управлінських рішень у сфері мобільних інновацій.

Особливістю ризиків у мобільних технологіях є їх комплексний і взаємопов’язаний характер. Технічні збої можуть призводити до фінансових втрат, інформаційні інциденти – до репутаційних проблем, а недотримання правових норм – до обмеження діяльності компаній на ринку. Саме тому системний підхід до класифікації ризиків дозволяє враховувати взаємний вплив різних факторів та забезпечувати більш стійке функціонування мобільних сервісів у динамічному цифровому середовищі.

У сучасних умовах глобалізації та цифрової трансформації класифікація ризиків у сфері мобільних технологій також сприяє підвищенню рівня кіберстійкості та довіри з боку користувачів. Вона є основою для розроблення політик безпеки, стандартів якості та стратегій розвитку мобільних продуктів і послуг. Таким чином, систематизація ризиків виступає важливим інструментом забезпечення стабільності, конкурентоспроможності та сталого розвитку компаній, що працюють у сфері мобільних технологій.

Розвиток мобільних технологій супроводжується стрімким зростанням їх ролі в економічній, соціальній та управлінській діяльності. Смартфони, мобільні додатки, бездротові мережі та хмарні сервіси стали невід'ємною частиною повсякденного життя й бізнес-процесів. Водночас активне впровадження мобільних технологій зумовлює появу нових загроз і невизначеностей, що потребує ґрунтовного аналізу ризиків, пов'язаних із їх використанням.

Особливістю ризиків у сфері мобільних технологій є їх багатогранність і взаємопов'язаність. Вони можуть виникати як на технічному рівні, так і в процесі експлуатації, управління даними чи взаємодії з користувачами. Швидке оновлення програмного забезпечення, залежність від мережевої інфраструктури та постійне зростання обсягів переданої інформації ускладнюють своєчасне виявлення й оцінювання потенційних загроз.


Рис. 1.2 – Класифікація ризиків усфері мобільних технологій

Класифікація ризиків у сфері мобільних технологій є важливим етапом ризик-менеджменту, оскільки дозволяє систематизувати різноманітні небезпеки та визначити їх характер, джерела виникнення і можливі наслідки. Чіткий поділ ризиків на окремі групи сприяє більш точному вибору методів

управління, підвищує ефективність превентивних заходів і зменшує ймовірність негативного впливу на діяльність організацій.

Класифікація ризиків у сфері мобільних технологій:

1.*Технічні ризики* – збої в роботі мобільних пристроїв, додатків і мереж, помилки програмного забезпечення, проблеми сумісності оновлень, нестабільний зв'язок.

Однією з найважливіших груп є технічні ризики. Вони пов'язані з функціонуванням апаратного та програмного забезпечення мобільних пристроїв і мереж. До цієї категорії належать збої в роботі мобільних додатків, помилки програмного коду, несумісність оновлень, низька якість зв'язку, відмови серверів або мережевої інфраструктури. Реалізація технічних ризиків може призвести до переривання доступу до сервісів, втрати даних або зниження якості обслуговування користувачів.

2.*Інформаційні та кіберризики* – витік персональних даних, несанкціонований доступ до інформації, кібератаки, віруси, фішингові атаки на користувачів [13].

Значну загрозу становлять інформаційні та кіберризики, які пов'язані з безпекою даних. У сфері мобільних технологій вони включають несанкціонований доступ до персональної інформації, витік конфіденційних даних, кібератаки, зараження мобільних пристроїв шкідливим програмним забезпеченням та фішингові атаки. Такі ризики особливо небезпечні, оскільки можуть призвести не лише до фінансових втрат, а й до втрати довіри користувачів і погіршення репутації компанії.

3.*Фінансові ризики* – перевищення витрат на розробку та підтримку мобільних технологій, втрати доходів через збої сервісів, коливання валютних курсів [14].

Окрему групу становлять фінансові ризики, що виникають у процесі розроблення, впровадження та експлуатації мобільних технологій. До них належать перевищення бюджету на розробку мобільних додатків, непередбачені витрати на підтримку та оновлення систем, зниження доходів

через технічні збої або втрату клієнтів. Також фінансові ризики можуть бути пов’язані з коливанням валютних курсів, особливо у разі використання міжнародних платформ і сервісів.

4.*Правові та регуляторні ризики* – недотримання вимог законодавства щодо захисту даних, ліцензування, авторських прав і телекомунікаційних норм.

Не менш важливими є правові та регуляторні ризики. Вони зумовлені необхідністю дотримання законодавства у сфері захисту персональних даних, авторських прав, ліцензування програмного забезпечення та регулювання телекомунікаційної діяльності. Порушення встановлених норм може призвести до штрафних санкцій, судових спорів або обмеження діяльності підприємства на ринку мобільних послуг.

5.*Операційні ризики* – помилки персоналу, недостатня кваліфікація працівників, неефективне управління проєктами та внутрішніми процесами.

У сфері мобільних технологій також виділяють операційні ризики, які пов’язані з організацією внутрішніх процесів. Вони виникають унаслідок помилок персоналу, недостатньої кваліфікації працівників, неефективного управління проєктами або недосконалих бізнес-процесів. Такі ризики можуть знижувати продуктивність роботи, затримувати впровадження нових технологій і негативно впливати на якість кінцевого продукту [15].

6.*Репутаційні ризики* – негативні відгуки користувачів, зниження довіри до компанії через збої, витоки даних або низьку якість сервісів.

Крім того, важливе місце займають репутаційні ризики, що формуються під впливом негативного досвіду користувачів, скарг, збоїв у роботі сервісів або витоку інформації. У сучасних умовах швидкого поширення інформації через соціальні мережі навіть незначні проблеми можуть мати масштабні наслідки для іміджу компанії. Саме тому класифікація та детальний аналіз ризиків у сфері мобільних технологій є необхідною передумовою для побудови ефективної системи ризик-менеджменту та забезпечення сталого розвитку [16].

Таким чином, дослідження та класифікація ризиків у сфері мобільних технологій створюють теоретичну й практичну основу для розроблення ефективних механізмів їх мінімізації. Це дає змогу забезпечити стабільне функціонування мобільних систем, підвищити рівень інформаційної безпеки та зберегти конкурентоспроможність підприємств в умовах цифрової трансформації.

## 1.3. Методологічні підходи та інструменти управління ризиками (ISO 31000, COSO ERM, NIST, цифрова аналітика ризиків)

Управління ризиками є невід’ємною складовою ефективної діяльності підприємств у сучасних умовах, що характеризуються високим рівнем невизначеності та динамічними змінами зовнішнього середовища. Застосування методологічних підходів до управління ризиками дозволяє системно організувати процес їх виявлення, аналізу та контролю, а також забезпечити обґрунтованість управлінських рішень на різних рівнях управління.

Методологічні підходи до управління ризиками ґрунтуються на використанні науково обґрунтованих принципів, моделей і методів, що дають змогу оцінити ймовірність виникнення ризиків та масштаби їх можливих наслідків. Вони передбачають застосування комплексу інструментів, спрямованих на зниження негативного впливу ризиків або використання їх як джерела додаткових можливостей для розвитку організації.

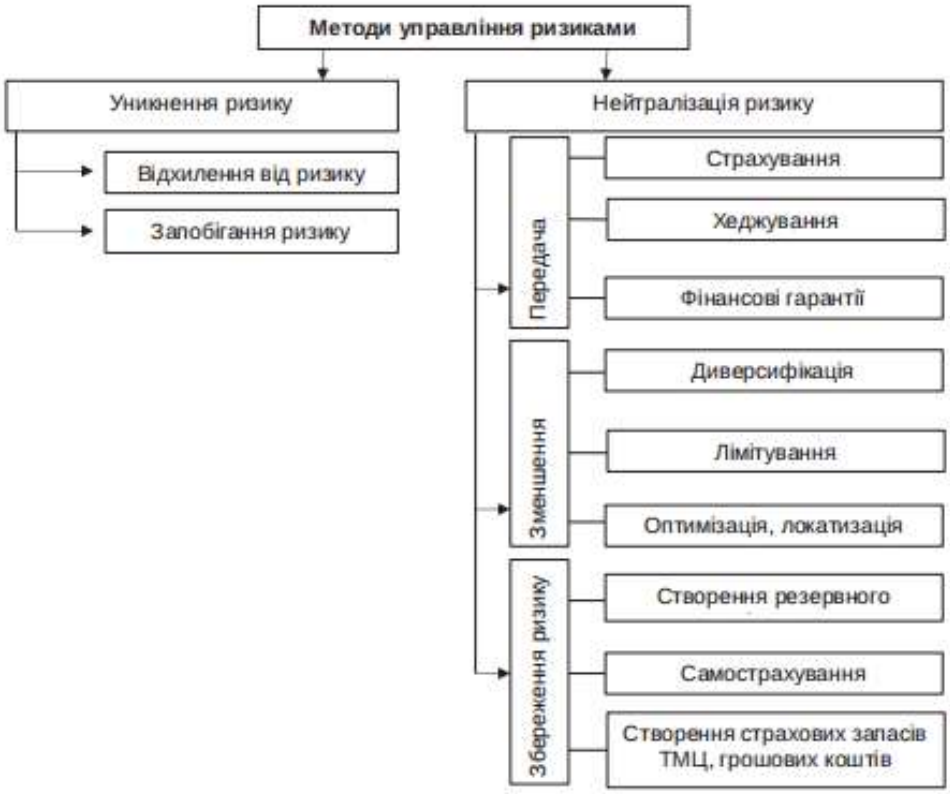


Рис. 1.2 – Методи управління ризиками

У поданій схемі відображено основні методи управління ризиками, які застосовуються для зменшення негативного впливу невизначеності на діяльність організації. Управління ризиками передбачає системний підхід до їх виявлення, аналізу та вибору найбільш доцільних способів реагування з метою мінімізації можливих втрат і забезпечення стабільності функціонування.

Першою групою методів є уникнення ризику. Воно полягає у свідомому відмовленні від дій, операцій або рішень, що можуть призвести до небажаних наслідків. У межах цього підходу організація може повністю відхилитися від ризикової діяльності, наприклад, не виходити на нестабільний ринок або не впроваджувати технології з високим рівнем невизначеності.

Одним із різновидів уникнення ризику є запобігання ризику. Цей метод спрямований не на відмову від діяльності загалом, а на усунення причин виникнення ризику ще на етапі планування. Запобігання ризикам реалізується через ретельний аналіз умов, дотримання стандартів, підвищення рівня контролю та використання перевірених рішень [7].

Другою великою групою методів є нейтралізація ризику, яка передбачає активні дії з управління вже наявними ризиками. Одним із напрямів нейтралізації є передача ризику третім особам. Це означає, що відповідальність за можливі збитки частково або повністю перекладається на інші суб'єкти.

До методів передачі ризику належать страхування, хеджування та використання фінансових гарантій. Страхування дозволяє компенсувати збитки у разі настання ризикової події, хеджування зменшує фінансові втрати через коливання цін або курсів, а фінансові гарантії забезпечують виконання зобов'язань контрагентами.

Ще одним напрямом нейтралізації є зменшення ризику. Він передбачає скорочення ймовірності настання ризикових подій або зменшення масштабу їх негативних наслідків. До цього напряму належать диверсифікація діяльності, лімітування витрат або операцій, а також оптимізація та локалізація ризиків.

Диверсифікація полягає у розподілі ресурсів між різними видами діяльності, що знижує залежність від одного джерела доходу. Лімітування встановлює гранично допустимі обсяги ризикованих операцій, а оптимізація й локалізація спрямовані на концентрацію ризиків у контрольованих межах.

Окрему групу становлять методи збереження ризику. Вони застосовуються у випадках, коли ризик є прийнятним або економічно доцільним. До таких методів належать створення резервних фондів, самострахування та формування запасів товарно-матеріальних цінностей і грошових коштів, що дозволяє покривати можливі втрати власними ресурсами.

Нижче подано **узагальнений виклад методологічних підходів та інструментів управління ризиками** (ISO 31000, COSO ERM, NIST, цифрова аналітика ризиків).

Таблиця 1.1

| Підхід | Характеристика |
|---|---|

| | |
|---|---|
| ISO 31000 | ISO 31000 є міжнародним стандартом, що визначає загальні принципи та рекомендації щодо управління ризиками в організаціях будь-якого типу та сфери діяльності. Основна ідея стандарту полягає в інтеграції ризик-менеджменту в усі управлінські процеси, починаючи зі стратегічного планування й завершуючи операційною діяльністю. Стандарт орієнтований на створення єдиного підходу до виявлення, аналізу та оцінки ризиків.<br><br>ISO 31000 робить акцент на безперервності процесу управління ризиками та його адаптивності до змін зовнішнього й внутрішнього середовища. Він передбачає постійний моніторинг ризиків, комунікацію між усіма зацікавленими сторонами та вдосконалення заходів реагування, що особливо важливо в умовах швидкого розвитку цифрових і мобільних технологій. |
| COSO ERM | Модель COSO ERM (Enterprise Risk Management) спрямована на комплексне управління ризиками на рівні всієї організації. Вона поєднує ризик-менеджмент зі стратегією, корпоративним управлінням та процесами прийняття управлінських рішень. COSO ERM розглядає ризики не лише як загрози, а і як потенційні можливості для створення додаткової вартості.<br><br>Особливістю COSO ERM є чітка структура компонентів управління ризиками, серед яких визначення цілей, ідентифікація ризиків, їх оцінка, реагування та контроль. Такий підхід дозволяє забезпечити узгодженість стратегічних рішень із допустимим рівнем ризику та підвищити прозорість управління в організації. |
| NIST | Підхід NIST (National Institute of Standards and Technology) широко застосовується у сфері інформаційної та кібербезпеки. Він орієнтований на управління ризиками, пов’язаними з інформаційними системами, цифровими активами та мережевою інфраструктурою. Основна увага приділяється захисту конфіденційності, цілісності та доступності інформації. |

| | |
|---|---|
| | Методологія NIST базується на поетапному процесі ідентифікації загроз, оцінювання вразливостей, аналізу ймовірності атак і вибору заходів захисту. Для мобільних технологій цей підхід є особливо актуальним, оскільки дозволяє знизити ризики витоку даних, кібератак та порушення роботи інформаційних систем. |
| Цифрова аналітика ризиків | Цифрова аналітика ризиків ґрунтується на використанні великих даних, штучного інтелекту, машинного навчання та аналітичних платформ для прогнозування й оцінки ризиків. Вона дозволяє автоматизувати процеси аналізу ризиків і швидко обробляти значні обсяги інформації в реальному часі.<br><br>Застосування цифрової аналітики підвищує точність управлінських рішень і дає змогу своєчасно виявляти приховані загрози. У сфері мобільних технологій цей інструмент сприяє оперативному реагуванню на технічні, фінансові та кіберризики, а також підвищує загальний рівень стійкості підприємства до змін цифрового середовища. |

Таким чином, вибір і поєднання відповідних методологічних підходів та інструментів управління ризиками забезпечують формування ефективної системи ризик-менеджменту. Це сприяє підвищенню стійкості підприємства, оптимальному використанню ресурсів і досягненню стратегічних цілей в умовах ризикового середовища.

## 1.4. Нормативно-правове та етичне регулювання ризик-менеджменту в IT-сфері

Нормативно-правове та етичне регулювання ризик-менеджменту в IT-сфері є важливою складовою забезпечення стабільного функціонування цифрових систем і захисту інтересів усіх учасників інформаційних відносин.

Стрімкий розвиток інформаційних технологій, зростання обсягів обробки даних та поширення цифрових сервісів суттєво підвищують рівень технологічних, правових і репутаційних ризиків. У таких умовах особливого значення набуває формування чіткої нормативної бази, яка визначає правила управління ризиками, відповідальність суб'єктів ІТ-діяльності та механізми захисту інформації.

Нормативно-правове регулювання ризик-менеджменту в ІТ-сфері ґрунтується на поєднанні міжнародних стандартів, національного законодавства та галузевих регуляторних вимог. Воно охоплює питання інформаційної безпеки, захисту персональних даних, кібербезпеки, дотримання авторських прав і забезпечення безперервності ІТ-процесів. Дотримання встановлених правових норм дозволяє зменшити ймовірність виникнення критичних інцидентів, мінімізувати фінансові втрати та запобігти юридичній відповідальності у разі реалізації ризиків.

Етичне регулювання ризик-менеджменту доповнює правові норми та спрямоване на формування відповідальної поведінки ІТ-фахівців і організацій у цифровому середовищі. Воно передбачає дотримання принципів прозорості, доброчесності, конфіденційності та поваги до прав користувачів під час розробки, впровадження й експлуатації інформаційних систем. Поєднання нормативно-правових та етичних засад створює комплексний підхід до управління ризиками в ІТ-сфері, сприяє підвищенню довіри до цифрових технологій і забезпечує їх сталий розвиток.

У наукових дослідженнях цифрова етика трактується як сукупність норм і ціннісних орієнтирів, спрямованих на узгодження розвитку інноваційних технологій із необхідністю захисту фундаментальних прав і свобод людини. Зокрема, Л. Флоріді та Дж. Каулз розробили узагальнену концептуальну модель, що базується на п'яти ключових засадах. Вона передбачає прозорість цифрових рішень, яка полягає у зрозумілому поясненні принципів роботи алгоритмів та автоматизованих систем, а також справедливість і безпеку, що орієнтовані на запобігання кіберзагрозам і недобросовісному використанню

технологій. Важливе місце в цій рамці посідають підзвітність і відповідальність, які зобов'язують учасників цифрових процесів забезпечувати дотримання прав людини, а також принцип недискримінації, спрямований на запобігання формуванню чи посиленню упереджень у цифровому просторі. Окремо наголошується на людиноцентричному підході, відповідно до якого технологічні рішення мають бути спрямовані на благо людини та її потреби [18].

У схожому контексті Дж. де Ґреґоріо розглядає цифрову етику як елемент більш широкої концепції цифрового конституціоналізму, яка відображає глибинні зміни у взаємодії між правами особи та владними механізмами в умовах цифрового розвитку суспільства [19]

Насамперед слід зазначити, що в Україні діє низка нормативно-правових актів, які визначають базові засади доступу до інформації та регулюють використання цифрових технологій. До таких актів належать Закон України «Про інформацію» від 02.10.1992 № 2657-XII [20], Закон України «Про електронну ідентифікацію та електронні довірчі послуги» від 05.10.2017 № 2155-VIII [21], Закон України «Про захист персональних даних» від 01.06.2010 № 2297-VI [22], Закон України «Про електронні документи та електронний документообіг» від 22.05.2003 № 851-IV [23], а також Закон України «Про електронні комунікації» від 16.12.2020 № 1089-IX [24]. Сукупно ці нормативні документи формують правове підґрунтя для впровадження та застосування інформаційних технологій у різних галузях діяльності, зокрема й у сфері бухгалтерського обліку.

Окрему групу складають законодавчі акти, спрямовані на захист інформації та забезпечення кібербезпеки. До них належать Закон України «Про захист інформації в інформаційно-комунікаційних системах» від 05.07.1994 № 80/94-ВР [25], Закон України «Про державну таємницю» від 21.01.2004 № 3855-XII [26], Закон України «Про Національну систему конфіденційного зв'язку» від 10.01.2002 № 2919-III [27], а також Закон України «Про основні засади забезпечення кібербезпеки України» від

05.10.2017 № 2163-VIII [28]. Важливу роль у цьому контексті відіграють і підзаконні акти, зокрема постанова Кабінету Міністрів України від 19 червня 2019 р. № 518, яка встановлює загальні вимоги до кіберзахисту об'єктів критичної інфраструктури, та постанова Кабінету Міністрів України від 29 березня 2006 р. № 373, що визначає правила забезпечення захисту інформації в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах.

Окрім національного законодавства, важливу роль у нормативно-правовому регулюванні ризик-менеджменту в ІТ-сфері відіграють міжнародні стандарти та рекомендації, які використовуються як орієнтири для формування внутрішніх політик організацій. Зокрема, стандарти серії ISO/IEC (ISO 27001, ISO 27005, ISO 31000) визначають підходи до управління інформаційною безпекою та ризиками, сприяючи систематизації процесів і підвищенню їхньої прозорості. Використання таких стандартів дозволяє українським ІТ-компаніям гармонізувати власну діяльність із міжнародними практиками та підвищити рівень довіри з боку партнерів і користувачів.

В умовах цифровізації економіки ризик-менеджмент у ІТ-сфері тісно пов'язаний із питаннями корпоративного управління та комплаєнсу. Нормативні вимоги стимулюють компанії впроваджувати внутрішні процедури оцінки та моніторингу ризиків, розподіляти відповідальність між структурними підрозділами та забезпечувати належний рівень контролю за використанням інформаційних ресурсів. Це сприяє зниженню операційних і репутаційних ризиків, а також підвищує загальну стійкість організацій до зовнішніх і внутрішніх загроз.

Водночас правове регулювання не завжди встигає за темпами розвитку новітніх технологій, таких як штучний інтелект, великі дані та хмарні обчислення. У зв'язку з цим особливої актуальності набуває роль етичних норм, які дозволяють заповнювати прогалини законодавства та слугують додатковим інструментом управління ризиками. Етичні принципи

допомагають визначати допустимі межі використання технологій і запобігати потенційно шкідливим наслідкам для особи та суспільства.

Етичний вимір ризик-менеджменту в ІТ-сфері також передбачає відповідальне ставлення до даних, зокрема персональних і чутливих. Забезпечення конфіденційності, мінімізація збору даних і дотримання принципу цільового використання зменшують ризики порушення прав людини та зловживань інформацією. У цьому контексті цифрова етика виступає не лише моральним орієнтиром, а й практичним інструментом запобігання правовим і репутаційним втратам.

Важливим аспектом є також формування етичної культури серед ІТ-фахівців, яка базується на усвідомленні наслідків прийнятих технічних рішень. Професійні кодекси етики, внутрішні регламенти та програми навчання сприяють розвитку відповідального підходу до проєктування й експлуатації інформаційних систем. Це дозволяє зменшити ризики, пов’язані з людським фактором, та підвищити якість управлінських рішень у сфері інформаційних технологій.

Окремої уваги в контексті нормативно-правового та етичного регулювання ризик-менеджменту в ІТ-сфері потребує питання відповідальності за прийняття автоматизованих управлінських рішень. Використання алгоритмів штучного інтелекту, систем машинного навчання та автоматизованих аналітичних платформ у процесах управління ризиками підвищує ефективність обробки інформації, проте водночас створює додаткові правові та етичні виклики. Зокрема, виникає проблема визначення суб’єкта відповідальності у разі помилок алгоритмів, дискримінаційних рішень або неправомірного використання даних, що потребує чіткого нормативного врегулювання.

Важливим напрямом етичного регулювання є забезпечення прозорості алгоритмів і пояснюваності рішень, прийнятих цифровими системами. У межах ризик-менеджменту це означає необхідність документування логіки роботи аналітичних моделей, обґрунтування критеріїв оцінки ризиків і

можливості перевірки результатів їх застосування. Такий підхід знижує рівень операційних і репутаційних ризиків, а також сприяє підвищенню довіри з боку користувачів, інвесторів і регуляторних органів.

Крім того, у сфері ІТ-діяльності дедалі більшого значення набуває принцип «етичного дизайну» (ethics by design), відповідно до якого вимоги безпеки, конфіденційності та захисту прав користувачів закладаються ще на етапі проєктування інформаційних систем. Реалізація цього принципу дозволяє зменшити ймовірність виникнення ризиків у процесі експлуатації програмного забезпечення та сприяє формуванню превентивної моделі управління ризиками.

Суттєвим елементом етичного регулювання ризик-менеджменту є також управління людським фактором у цифровому середовищі. Навіть за наявності досконалих технічних і правових механізмів значна частина ризиків виникає внаслідок помилок персоналу, недостатньої обізнаності або недотримання етичних стандартів. У зв’язку з цим особливої актуальності набувають програми навчання з кіберетики, інформаційної безпеки та культури управління ризиками.

Таким чином, доповнення нормативно-правового регулювання етичними принципами дозволяє сформувати більш гнучку та ефективну систему ризик-менеджменту в ІТ-сфері. Поєднання правових норм, етичних стандартів і сучасних цифрових інструментів забезпечує зниження рівня невизначеності, підвищення стійкості інформаційних систем і формування довіри до результатів цифрової трансформації.

Отже, нормативно-правове та етичне регулювання ризик-менеджменту в ІТ-сфері слід розглядати як взаємодоповнювальні елементи єдиної системи управління. Їх поєднання забезпечує не лише формальне дотримання законодавчих вимог, а й орієнтацію на цінності сталого розвитку, захист прав людини та суспільну довіру до цифрових інновацій. У перспективі саме інтегрований підхід до правового та етичного регулювання стане ключовою умовою ефективного управління ризиками в умовах цифрової трансформації.

## Висновки до розділу 1

У першому розділі було ґрунтовно розкрито теоретичні та методологічні засади ризик-менеджменту в умовах розвитку мобільних технологій та цифрової економіки. Доведено, що трансформація економічних процесів, цифровізація бізнесу та зростання ролі інформаційних технологій суттєво ускладнили середовище функціонування підприємств, що зумовило появу нових видів ризиків і підвищення рівня невизначеності. За таких умов ризик-менеджмент еволюціонував від фрагментарних підходів до комплексної управлінської системи, інтегрованої у стратегічне та операційне управління.

У ході аналізу еволюції ризик-менеджменту встановлено, що розвиток кількісних методів, поява міжнародних стандартів і формування корпоративного ризик-менеджменту стали ключовими етапами становлення сучасних підходів до управління ризиками. Особливу роль у цьому процесі відіграли фінансові інструменти оцінювання ризиків, професійні інституції та нормативні ініціативи, які сприяли стандартизації та підвищенню прозорості управлінських рішень. У цифровій економіці ризик-менеджмент перетворився на безперервний процес, орієнтований на прогнозування та запобігання негативним наслідкам.

Важливим результатом розділу є систематизація ризиків у сфері мобільних технологій. З’ясовано, що такі ризики мають комплексний і взаємопов’язаний характер та охоплюють технічні, інформаційні, кібернетичні, фінансові, правові, операційні й репутаційні аспекти. Запропонована класифікація дозволяє більш точно ідентифікувати джерела загроз, оцінювати можливі наслідки їх реалізації та формувати обґрунтовані управлінські рішення, спрямовані на мінімізацію негативного впливу на діяльність підприємств.

У розділі також розглянуто основні методологічні підходи та інструменти управління ризиками, зокрема стандарти ISO 31000, модель COSO ERM, підхід NIST і цифрову аналітику ризиків. Встановлено, що їх застосування забезпечує системність, узгодженість і адаптивність процесів управління ризиками, особливо в умовах швидкого розвитку мобільних і цифрових технологій. Поєднання класичних методів із сучасними цифровими інструментами дозволяє підвищити точність оцінювання ризиків і оперативність реагування на загрози.

Окрему увагу в розділі приділено нормативно-правовому та етичному регулюванню ризик-менеджменту в IT-сфері. Доведено, що ефективне управління ризиками неможливе без дотримання законодавчих вимог у сфері захисту інформації, персональних даних і кібербезпеки, а також без урахування етичних принципів цифрової діяльності. Поєднання правових норм і етичних засад сприяє зниженню правових, репутаційних і соціальних ризиків та формує довіру до цифрових технологій з боку користувачів і партнерів.

Таким чином, результати першого розділу створюють цілісну теоретико-методологічну основу для подальшого дослідження ризик-менеджменту в сфері мобільних технологій. Отримані висновки підтверджують необхідність комплексного, інтегрованого та адаптивного підходу до управління ризиками, що поєднує наукові концепції, міжнародні стандарти, цифрові інструменти та нормативно-етичні вимоги. Це є передумовою ефективного функціонування підприємств і забезпечення їхньої стійкості в умовах цифрової трансформації.

# РОЗДІЛ 2. АНАЛІТИКО-ПРАКТИЧНЕ ДОСЛІДЖЕННЯ РИЗИК МЕНЕДЖМЕНТУ КОМПАНІЇ «APPLE CENTER»

## 2.1. Загальна характеристика діяльності «Apple Center» та його позиції на ринку мобільних технологій

Діяльність компанії «Apple Center» у сфері мобільних технологій є показовим прикладом успішного поєднання інновацій, високих стандартів якості та клієнтоорієнтованого підходу. У сучасних умовах стрімкого розвитку цифрових технологій та зростання конкуренції на ринку мобільних пристроїв особливого значення набуває аналіз діяльності компаній, які займають провідні позиції та формують споживчі тренди. Саме тому дослідження особливостей функціонування «Apple Center» є актуальним і доцільним з точки зору оцінки його ролі на ринку мобільних технологій.

«Apple Center» спеціалізується на реалізації, сервісному обслуговуванні та консультаційній підтримці продукції Apple, що охоплює широкий спектр мобільних пристроїв і цифрових рішень. Компанія орієнтується на використання сучасних технологій, дотримання корпоративних стандартів бренду та впровадження ефективних бізнес-процесів. Завдяки цьому «Apple Center» забезпечує високий рівень обслуговування клієнтів і формує стабільну репутацію на ринку [30].

Ринок мобільних технологій характеризується динамічними змінами, швидким оновленням асортименту та зростанням вимог споживачів до якості продуктів і сервісів. У таких умовах конкурентні переваги компанії визначаються не лише технічними характеристиками продукції, а й рівнем сервісної підтримки, маркетинговою стратегією та здатністю адаптуватися до ринкових викликів. «Apple Center» успішно позиціонує себе як надійний партнер і офіційний представник екосистеми Apple, що дозволяє йому утримувати сильні позиції у своєму сегменті.

Компанія Apple Inc. була створена у 1976 році з ініціативи Стіва Джобса, Стіва Возняка та Рональда Вейна, і саме період її становлення відіграє вирішальну роль у розумінні трансформації невеликого стартапу в одну з найпотужніших технологічних корпорацій світу. Початковий етап розвитку Apple тісно пов'язаний із гаражем родинного будинку Стіва Джобса в місті Лос-Альтос, штат Каліфорнія, який згодом став символом зародження інноваційного підприємництва у Силіконовій долині. Саме в цих скромних умовах засновники розпочали роботу над створенням першого продукту компанії.


Рис. 2.1 – Ключові події в історії бренду «Apple»

Першим комерційним досягненням Apple став персональний комп'ютер Apple I, який був зібраний вручну Стівом Возняком. Як талановитий інженер, він прагнув розробити комп'ютерний пристрій, доступний не лише для фахівців, а й для широкого кола користувачів. Презентація Apple I відбулася у квітні 1976 року під час зустрічі Homebrew Computer Club – спільноти ентузіастів комп'ютерних технологій у Силіконовій долині, що стало важливим кроком у популяризації продукту.

Рональд Вейн, хоч і не набув значної популярності в подальшій історії компанії, зробив вагомий внесок на початковому етапі її діяльності. Він брав участь в оформленні юридичних засад створення Apple та створив перший логотип компанії. Водночас уже за кілька тижнів Вейн вирішив вийти зі складу

співзасновників, продавши свою частку за незначну на той момент суму коштів [29].

Фінансування виробництва Apple I здійснювалося за рахунок особистих ресурсів засновників: Стів Джобс продав власний мікроавтобус Volkswagen, а Стів Возняк – програмований калькулятор HP. Попри високий рівень ризику, такі кроки виявилися виправданими, оскільки Apple I отримав позитивний відгук, передусім серед комп'ютерних ентузіастів. Пристрій реалізовувався за ціною 666,66 долара США, що на той час вважалося відносно доступною вартістю для персонального комп'ютера.

Таблиця 2.1

Глобальна присутність компанії «Apple»

| Географічний розподіл | Кількість офісів | Особливості глобальної присутності |
|---|---|---|
| Північна Америка | 30 | Основний центр стратегічного управління, розробки інноваційних продуктів і програмного забезпечення; розміщення штаб-квартири компанії та ключових дослідницьких підрозділів |
| Європа | 40 | Активна присутність на ринках країн ЄС; орієнтація на дистрибуцію продукції, маркетинг, сервісну підтримку та дотримання регіональних нормативно-правових вимог |
| Азія | 20 | Виробничі та логістичні потужності; співпраця з контрактними виробниками, розвиток ринків збуту та адаптація продукції до локальних особливостей |

Джерело: [30]

Аналіз представленої таблиці свідчить про стратегічно збалансовану глобальну присутність компанії Apple, яка охоплює ключові регіони світу. Основна частина офісів зосереджена у Північній Америці, де розташована штаб-квартира компанії та провідні дослідницькі підрозділи, що забезпечує контроль над розробкою інноваційних продуктів і програмного забезпечення.

Така концентрація дозволяє Apple ефективно координувати стратегічні рішення та впроваджувати нові технології, підтримуючи високу якість продукції та рівень сервісу.


Рис. 2.1 – Глобальна присутність компанії «Apple»

Європейський та азійський ринки виконують специфічні функції в глобальній структурі компанії. У Європі акцент робиться на дистрибуцію продукції, маркетингову підтримку та дотримання регіональних правових норм, що дозволяє успішно адаптувати бізнес до вимог локальних споживачів. Азійські офіси та потужності зосереджені на виробництві та логістиці, а також на співпраці з контрактними виробниками, що сприяє ефективному забезпеченню ринків збуту і адаптації продукції до особливостей регіону. Такий розподіл створює комплексну та гнучку глобальну мережу, здатну швидко реагувати на зміни ринкових умов.

Таблиця 2.2

Основні продукти компанії Apple Inc.

| Категорія продукту | Назва продукту | Коротка характеристика |
|---|---|---|

| | | |
|---|---|---|
| Смартфони | iPhone | Флагманська лінійка смартфонів із власною операційною системою iOS, орієнтована на високу продуктивність, безпеку та інтеграцію в екосистему Apple |
| Планшети | iPad | Мобільні пристрої для роботи, навчання та розваг, що поєднують функції планшета й ноутбука |
| Ноутбуки | MacBook Air, MacBook Pro | Портативні комп’ютери з macOS, призначені для професійного та повсякденного використання |
| Настільні комп’ютерні | iMac, Mac mini, Mac Studio | Стаціонарні комп’ютери для офісної роботи, дизайну, програмування та мультимедійних завдань |
| Носимі пристрої | Apple Watch | Смартгодинники для моніторингу здоров’я, фізичної активності та комунікацій |
| Аудіопристрої | AirPods, HomePod | Бездротові навушники та розумні колонки з підтримкою голосового асистента Siri |
| Програмне забезпечення | iOS, macOS, watchOS | Власні операційні системи, що забезпечують інтегровану роботу пристроїв Apple |
| Цифрові сервіси | Apple Music, Apple TV+, iCloud | Онлайн-сервіси для зберігання даних, потокового контенту та підпискових послуг |

Джерело: складено автором

Аналіз асортименту продукції компанії Apple, представленого в таблиці, свідчить про комплексний і системний підхід компанії до формування власної екосистеми цифрових продуктів. Apple охоплює ключові сегменти ринку

споживчої електроніки – від мобільних пристроїв і персональних комп’ютерів до носимих гаджетів і цифрових сервісів. Така диверсифікація дозволяє компанії задовольняти різноманітні потреби користувачів і зменшувати залежність від одного виду продукції, що позитивно впливає на її ринкову стійкість.

Особливе місце в продуктовому портфелі Apple займає лінійка смартфонів iPhone, яка традиційно формує значну частку доходів компанії та визначає її позиції на ринку мобільних технологій. Завдяки поєднанню інноваційних технічних рішень, високого рівня безпеки та інтуїтивного інтерфейсу iPhone залишається одним із найбільш конкурентоспроможних продуктів у своєму сегменті. Водночас інтеграція iPhone з іншими пристроями Apple стимулює споживачів до використання всієї екосистеми бренду.

Планшети iPad та комп’ютери серії MacBook і iMac орієнтовані як на масового користувача, так і на професійну аудиторію, зокрема дизайнерів, програмістів і фахівців креативних індустрій. Використання власних операційних систем і процесорів дозволяє Apple досягати високої продуктивності та оптимізації роботи пристроїв. Це створює додаткові конкурентні переваги та підвищує лояльність користувачів до бренду.

Рис 2.2 – Основна продукція компанії «AppleCenter»

Носимі та аудіопристрої, зокрема Apple Watch, AirPods і HomePod, доповнюють основні продукти та розширюють функціональні можливості екосистеми Apple. Вони орієнтовані на покращення повсякденного досвіду користувачів, зокрема у сферах здоров'я, комунікації та розваг. Зростаючий попит на такі пристрої свідчить про актуальність стратегії компанії щодо розвитку суміжних продуктів і сервісів.

Окремої уваги заслуговують цифрові сервіси Apple, зокрема iCloud, Apple Music і Apple TV+, які формують стабільне джерело регулярних доходів і посилюють взаємозв'язок між пристроями. Інтеграція апаратного забезпечення з програмними продуктами та сервісами забезпечує цілісність користувацького досвіду й підвищує конкурентоспроможність компанії на глобальному ринку. У сукупності представлений асортимент продукції свідчить про стратегічно виважений підхід Apple до розвитку бізнесу та утримання лідерських позицій у сфері мобільних технологій.

**Apple Center** є незалежною компанією, яка функціонує як **офіційний реселер і сервісний партнер Apple Inc.** в Україні та інших країнах. Хоч вона й не є філіалом корпорації Apple, «Apple Center» дотримується високих стандартів бренду, забезпечує продаж продукції Apple, сервісне обслуговування та консультаційну підтримку користувачів. Компанія орієнтована на якісне обслуговування клієнтів, дотримання корпоративних норм Apple та формування довгострокових відносин із споживачами.

Діяльність «Apple Center» охоплює широкий асортимент продукції, включаючи смартфони iPhone, планшети iPad, ноутбуки MacBook, стаціонарні комп'ютери iMac, носимі пристрої Apple Watch, бездротові навушники AirPods та цифрові сервіси Apple. Такий комплексний підхід дозволяє компанії створювати цілісну екосистему для користувачів, забезпечуючи взаємодію всіх продуктів і підвищуючи їхню лояльність до бренду.

На ринку мобільних технологій «Apple Center» займає **стабільні позиції**, завдяки статусу авторизованого партнера Apple та відповідності високим

стандартам обслуговування. Компанія активно працює над просуванням новинок, проведенням презентацій і навчанням клієнтів щодо використання продукції. Це дозволяє їй конкурувати з іншими реселерами і підтримувати високий рівень довіри серед користувачів.

Важливим елементом діяльності є **сервісна підтримка та післяпродажне обслуговування**, яке включає ремонт, оновлення програмного забезпечення та консультації щодо продукції Apple. Такий підхід не лише підвищує задоволеність клієнтів, а й зміцнює позиції компанії на ринку мобільних технологій, роблячи її надійним партнером для користувачів, які цінують якість, безпеку та сучасні цифрові рішення.

Отже, загальна характеристика діяльності «Apple Center» та аналіз його позицій на ринку мобільних технологій дають змогу комплексно оцінити ефективність функціонування компанії, її конкурентоспроможність і перспективи подальшого розвитку. Розуміння особливостей роботи «Apple Center» є важливим підґрунтям для подальшого дослідження управлінських, маркетингових і ризик-орієнтованих аспектів діяльності підприємства в умовах цифрової економіки.

## 2.2. Ідентифікація ключових ризиків у діяльності компанії

Діяльність сучасних компаній у сфері мобільних технологій здійснюється в умовах підвищеної динамічності ринку, технологічних змін та зростаючої конкуренції. У таких умовах питання своєчасного виявлення та аналізу ризиків набуває особливої актуальності, оскільки саме ризики можуть істотно впливати на стабільність функціонування підприємства та досягнення його стратегічних цілей. Ефективне управління ризиками неможливе без їх ґрунтовної ідентифікації на початковому етапі.

Ідентифікація ризиків передбачає систематичний процес виявлення факторів внутрішнього та зовнішнього середовища, які можуть спричинити

відхилення фактичних результатів діяльності від запланованих. Для компаній, що працюють на ринку мобільних технологій, такі фактори охоплюють фінансові, операційні, технологічні, ринкові та правові аспекти діяльності. Усвідомлення природи цих ризиків дозволяє керівництву приймати обґрунтовані управлінські рішення та формувати адекватні механізми реагування.

Особливого значення ідентифікація ризиків набуває для компанії «Apple Center», діяльність якої пов'язана з реалізацією високотехнологічної продукції та наданням сервісних послуг, що вимагають високого рівня відповідальності та довіри з боку споживачів. Будь-які порушення у ланцюгах постачання, збої в обслуговуванні клієнтів або проблеми з безпекою даних можуть мати суттєві фінансові та репутаційні наслідки для компанії.

Саме тому в межах даного підпункту особлива увага приділяється ідентифікації ключових ризиків у діяльності компанії «Apple Center» з урахуванням специфіки ринку мобільних технологій. Це дозволяє створити основу для подальшої оцінки ризиків та розробки ефективної системи ризик-менеджменту, спрямованої на забезпечення стабільного розвитку підприємства та підвищення його конкурентоспроможності.

Діяльність будь-якої компанії, яка працює у сфері мобільних технологій, пов'язана з широким спектром ризиків, що можуть впливати на фінансові, операційні та репутаційні показники. Для компанії «Apple Center» важливо системно ідентифікувати основні ризики, які здатні негативно позначитися на стабільності бізнесу та задоволеності клієнтів. Такий підхід дозволяє своєчасно вживати заходів щодо їх мінімізації та забезпечувати ефективне управління ризик-менеджментом.

Перш за все, слід виділити **фінансові ризики**, які виникають через коливання цін на продукцію, зміни валютних курсів та непередбачувані витрати на закупівлю товарів. «Apple Center» працює із високовартісною продукцією, і навіть незначні зміни у закупівельній ціні можуть суттєво впливати на рентабельність діяльності.


Рис. 2.2 – Ключові ризики діяльності компанії «AppleCenter»

Другим за значущістю є **операційні ризики**, що пов’язані з внутрішніми процесами компанії. До них належать ризики затримки постачання продукції, технічні збої у системі продажу або обліку, а також помилки персоналу під час обслуговування клієнтів. Ефективна організація бізнес-процесів та навчання співробітників дозволяють мінімізувати ймовірність таких інцидентів.

Ще однією важливою категорією є **технологічні ризики**, які пов’язані з оновленням і швидким розвитком мобільних технологій. Несвоєчасне впровадження нових продуктів або оновлень програмного забезпечення може призвести до втрати конкурентних переваг та зниження інтересу споживачів до пропозицій компанії.

Значну увагу необхідно приділити **ринковим ризикам**, що виникають через зміни попиту, поведінки споживачів або появу нових конкурентів. Конкуренція у сегменті мобільних пристроїв та сервісів дуже висока, і відсутність гнучкої маркетингової стратегії може негативно вплинути на частку компанії на ринку.

Особливу групу складають **юридичні та нормативні ризики**, пов’язані з дотриманням законодавства щодо торгівлі, захисту прав споживачів, авторських прав та обробки персональних даних. Порушення вимог нормативних актів може призвести до штрафів, санкцій або втрати репутації.

Крім того, варто виділити **кіберризики**, що включають загрози несанкціонованого доступу до даних, витоку конфіденційної інформації або кібератак на інформаційні системи компанії. У сфері продажу мобільних технологій це є критичною загрозою, оскільки впливає на довіру клієнтів.

Важливими є **репутаційні ризики**, які виникають у разі незадоволення клієнтів сервісом, появи негативних відгуків або скандалів у медіа. Для компанії «Apple Center», яка орієнтується на високий рівень обслуговування, збереження позитивного іміджу є пріоритетним завданням.

Не менш значущими є **логістичні ризики**, пов’язані з порушенням ланцюга постачання. Проблеми з транспортуванням продукції, затримки на складах або перебої у співпраці з постачальниками можуть спричинити нестачу товару і втрату продажів.

Також слід враховувати **економічні ризики**, пов’язані зі зміною макроекономічної ситуації, інфляцією, податковими змінами або коливаннями споживчої активності. Такі фактори можуть непрямо впливати на купівельну спроможність клієнтів та фінансові результати компанії.

Наступну групу становлять **соціальні та кадрові ризики**, що пов’язані з відтоком кваліфікованих співробітників, конфліктами в колективі або недостатньою мотивацією персоналу. Ефективна політика управління персоналом дозволяє зменшити ймовірність таких проблем.

Таблиця 2.3

Ключові ризики діяльності компанії «Apple Center»

| Категорія ризику | Опис ризику |
|---|---|
| Фінансові | Коливання цін на продукцію, зміни валютних курсів, непередбачувані витрати |

| | |
|---|---|
| Операційні | Збої в бізнес-процесах, помилки персоналу, затримки постачання |
| Технологічні | Несвоєчасне впровадження нових продуктів або оновлень |
| Ринкові | Зміна попиту, поведінки споживачів, поява нових конкурентів |
| Юридичні та номративні | Недотримання законодавства щодо торгівлі, захисту даних та авторських прав |
| Кіберризики | Несанкціонований доступ до даних, витоки інформації, кібератаки |
| Репутаційні | Незадоволеність клієнтів, негативні відгуки, скандали |
| Логістичні | Збої в ланцюгах постачання, затримки на складах |
| Економічні | Інфляція, зміни податків, коливання купівельної спроможності |
| Соціальні та кадрові | Відтік персоналу, конфлікти в колективі, низька мотивація |

Джерело: складено автором

Ідентифікація та класифікація цих ризиків дозволяє «Apple Center» розробляти ефективні стратегії управління, що включають профілактичні заходи, страхування та створення внутрішніх процедур контролю. Системний аналіз ризиків допомагає компанії підвищити стабільність бізнесу та забезпечити високий рівень обслуговування клієнтів.

Врахування усіх цих категорій ризиків є необхідною передумовою для формування комплексної політики ризик-менеджменту, що дозволяє оптимізувати операційні процеси, захистити фінансові ресурси та зміцнити позиції компанії на ринку мобільних технологій.

Діяльність компанії «Apple Center» у сфері мобільних технологій пов’язана з численними внутрішніми та зовнішніми ризиками, які можуть впливати на фінансові, операційні та репутаційні показники підприємства.

Ідентифікація цих ризиків дозволяє чітко визначити джерела загроз та їх потенційний вплив, що є необхідною передумовою для побудови ефективної системи ризик-менеджменту. Завдяки систематичному підходу компанія може прогнозувати ймовірні проблеми та мінімізувати негативні наслідки їх реалізації.

Особливої уваги потребують технологічні та кіберризики, які безпосередньо пов’язані з розвитком мобільних технологій та використанням цифрових сервісів. Несвоєчасне впровадження нових продуктів, технічні збої чи кібератаки можуть негативно впливати на якість обслуговування клієнтів і репутацію компанії. Усвідомлення цих загроз дає змогу керівництву розробляти превентивні заходи, покращувати внутрішні процеси та забезпечувати безпеку інформаційних систем.

Не менш важливими є фінансові, ринкові та операційні ризики, що впливають на стабільність доходів та ефективність бізнес-процесів. Коливання цін, зміни попиту, затримки у постачанні продукції або помилки персоналу можуть призвести до зниження прибутковості та погіршення обслуговування клієнтів. Виявлення та класифікація цих ризиків дозволяє формувати стратегії управління, що зменшують їхній негативний вплив та підвищують оперативну готовність компанії.

## 2.3. Оцінка ефективності системи управління ризиками

Сучасна діяльність «Apple Center» відбувається в умовах високої конкуренції, швидкого технологічного розвитку та зростання вимог з боку споживачів. У таких умовах ефективна система управління ризиками є необхідною передумовою стабільного функціонування та збереження ринкових позицій компанії. Саме тому оцінка ефективності ризик-менеджменту дозволяє визначити рівень готовності підприємства до можливих загроз і невизначеностей.

Управління ризиками в «Apple Center» охоплює як операційні процеси, так і стратегічні напрями діяльності, зокрема продаж і сервіс мобільних пристроїв, роботу з постачальниками, обслуговування клієнтів та управління персоналом. Важливим є не лише виявлення ризиків, а й здатність компанії своєчасно реагувати на них та мінімізувати негативні наслідки.

Оцінка ефективності системи управління ризиками дає змогу проаналізувати, наскільки застосовувані методи відповідають реальним умовам діяльності «Apple Center». Вона також дозволяє виявити сильні та слабкі сторони наявної системи ризик-менеджменту та визначити напрями її вдосконалення.

Система управління ризиками «Apple Center» базується на поєднанні корпоративних стандартів компанії Apple та внутрішніх управлінських процедур. Це забезпечує єдиний підхід до контролю якості, фінансової дисципліни та безпеки операцій. Такий підхід дозволяє знизити рівень операційних і репутаційних ризиків.


Рис. 2.3 – Оцінка ефективності системи управління ризиками «Apple Center»

Важливим елементом ефективності ризик-менеджменту є своєчасна ідентифікація ризиків. У діяльності «Apple Center» це досягається шляхом постійного моніторингу ринку, аналізу попиту, оцінки надійності постачальників і контролю внутрішніх процесів. Це дозволяє швидко реагувати на зміни зовнішнього середовища.

Значну увагу приділено управлінню фінансовими ризиками. Компанія застосовує контроль витрат, планування доходів і формування резервів, що сприяє зменшенню ймовірності фінансових втрат. Ефективність цих заходів проявляється у стабільності грошових потоків і зниженні ризику неплатоспроможності.

Технічні ризики, пов’язані з роботою мобільних пристроїв і сервісного обслуговування, мінімізуються завдяки використанню сертифікованого обладнання та дотриманню стандартів Apple. Це знижує кількість технічних збоїв і підвищує рівень задоволеності клієнтів.

Окрему роль відіграє управління інформаційними та кіберризиками. «Apple Center» дотримується вимог щодо захисту персональних даних клієнтів і використовує сучасні засоби інформаційної безпеки. Це сприяє зменшенню ймовірності витоку даних та підвищує довіру споживачів.

Управління кадровими ризиками реалізується через систему навчання персоналу, підвищення кваліфікації та дотримання корпоративної культури. Це знижує ризик помилок у роботі, підвищує якість обслуговування та сприяє ефективній взаємодії з клієнтами.

Репутаційні ризики контролюються завдяки високим стандартам сервісу, оперативному реагуванню на скарги та зворотний зв’язок із клієнтами. Такий підхід дозволяє мінімізувати негативний вплив інформаційних загроз у цифровому просторі.

Загалом система управління ризиками «Apple Center» демонструє достатній рівень ефективності, однак потребує постійного вдосконалення з урахуванням динамічних змін у сфері мобільних технологій і поведінці споживачів.

Таблиця 2.1

Оцінка ефективності системи управління ризиками «Apple Center»

| Вид ризику | Основні інструменти управління | Рівень ефективності |
|---|---|---|
| Фінансові ризики | Бюджетування, контроль витрат, резерви | Високий |
| Технічні ризики | Сертифіковане обладнання, стандарти Apple | Високий |
| Інформаційні ризики | Захист даних, кібербезпека | Достатній |
| Операційні ризики | Регламенти, внутрішній контроль | Достатній |
| Кадрові ризики | Навчання персоналу, корпоративна культура | Середній |
| Репутаційні ризики | Контроль якості сервісу, зворотний зв’язок | Високий |

Джерело: створено автором

Отже, система управління ризиками «Apple Center» є комплексною та орієнтованою на забезпечення стабільної діяльності компанії в умовах ринкової невизначеності. Вона охоплює основні види ризиків і ґрунтується на корпоративних стандартах та внутрішніх управлінських процедурах.

Проведена оцінка свідчить про високий рівень ефективності управління фінансовими, технічними та репутаційними ризиками. Це дозволяє компанії підтримувати довіру клієнтів і зберігати конкурентні переваги на ринку мобільних технологій.

Разом із тим, окремі напрями, зокрема управління кадровими та інформаційними ризиками, потребують подальшого вдосконалення.

Посилення цифрових інструментів контролю та розвитку персоналу може підвищити загальну результативність ризик-менеджменту.

Таким чином, ефективна система управління ризиками є важливим чинником стійкого розвитку «Apple Center». Її постійне вдосконалення сприятиме мінімізації негативних впливів ризиків та забезпеченню довгострокової стабільності компанії.

## 2.4. SWOT-аналіз, PEST-аналіз та виявлення вразливих зон у ризик-профілі компанії

У сучасних умовах розвитку ринку мобільних технологій компанія **Apple Center** функціонує в середовищі підвищеної невизначеності, що зумовлено швидкими технологічними змінами, жорсткою конкуренцією та зростаючими вимогами споживачів. За таких обставин особливої актуальності набуває використання інструментів стратегічного аналізу, які дозволяють комплексно оцінити вплив внутрішніх і зовнішніх факторів на діяльність компанії та рівень її ризиків.

SWOT-аналіз є ефективним інструментом для дослідження внутрішнього потенціалу **Apple Center**, оскільки дає змогу визначити сильні та слабкі сторони підприємства, а також можливості й загрози, що формуються під впливом ринкового середовища. Його застосування дозволяє виявити ключові внутрішні обмеження та конкурентні переваги, які безпосередньо впливають на формування ризик-профілю компанії.

PEST-аналіз, у свою чергу, спрямований на оцінку факторів макросередовища, зокрема політичних, економічних, соціальних і технологічних умов функціонування **Apple Center**. Аналіз цих чинників дає можливість своєчасно ідентифікувати зовнішні ризики, пов’язані з регуляторними змінами, економічною нестабільністю, трансформацією споживчих уподобань та розвитком цифрових технологій.

Поєднання результатів SWOT- та PEST-аналізу створює аналітичну основу для виявлення вразливих зон у ризик-профілі компанії **Apple Center**. Такий підхід дозволяє не лише систематизувати ключові загрози й обмеження, а й сформувати практичні рекомендації щодо підвищення стійкості компанії та вдосконалення системи управління ризиками в умовах динамічного ринкового середовища.

Таблиця 2.2

SWOT-аналіз компанії Apple Center

| Сильні сторони (Strengths) | Слабкі сторони (Weaknesses) |
|---|---|
| 1.Висока впізнаваність і довіра до бренду Apple<br>2. Високі стандарти якості продукції та сервісу<br>3. Кваліфікований і сертифікований персонал<br>4. Лояльна клієнтська база<br>5. Офіційна підтримка та гарантійне обслуговування | 1. Залежність від корпоративної політики компанії Apple<br>2. Обмежена гнучкість у формуванні цін<br>3. Високі операційні та орендні витрати<br>4. Обмежений асортимент поза екосистемою Apple<br>5. Залежність від імпортних поставок |
| Можливості (Opportunities) | Загрози (Threats) |
| 1. Зростання попиту на мобільні та цифрові сервіси<br>2. Розвиток сервісних і післяпродажних послуг<br>3. Розширення онлайн-продажів і цифрових каналів<br>4. Підвищення попиту на екосистемні рішення Apple<br>5. Впровадження нових технологій і продуктів | 1. Посилення конкуренції на ринку мобільних технологій<br>2. Коливання валютних курсів<br>3. Зміни митного та податкового законодавства<br>4. Зниження купівельної спроможності населення<br>5. Ризики перебоїв у постачанні |

Джерело: складено автором

Сильні сторони компанії Apple Center формують надійну основу для стабільного функціонування на ринку мобільних технологій. Висока репутація бренду Apple та довіра споживачів забезпечують постійний попит на продукцію, що знижує маркетингові та репутаційні ризики.

Високі стандарти якості сервісу та наявність кваліфікованого персоналу сприяють зменшенню операційних і технічних ризиків. Офіційний статус та гарантійне обслуговування підвищують рівень задоволеності клієнтів і зменшують імовірність втрати лояльної аудиторії.

Водночас слабкі сторони, зокрема залежність від політики корпорації Apple та обмежена цінова гнучкість, підвищують стратегічні та фінансові ризики. Компанія має обмежені можливості впливу на ціноутворення та асортимент, що може негативно позначатися на прибутковості в умовах нестабільного ринку.

Високі операційні витрати та залежність від імпортних поставок посилюють чутливість Apple Center до зовнішніх економічних факторів, зокрема валютних коливань і логістичних ускладнень. Це потребує посиленого фінансового контролю та диверсифікації каналів постачання.

Можливості розвитку пов’язані насамперед із розширенням сервісних послуг і впровадженням цифрових каналів продажу. Використання екосистеми Apple як комплексного рішення дозволяє компанії підвищувати додану вартість послуг і зміцнювати конкурентні позиції.

Загрози, такі як зростання конкуренції, економічна нестабільність і регуляторні зміни, формують ключові вразливі зони в ризик-профілі компанії. Врахування цих факторів у межах ризик-менеджменту дозволяє Apple Center своєчасно адаптувати стратегію та мінімізувати негативний вплив зовнішнього

Таблиця 2.3

PEST-аналіз компанії Apple Center

| Політичні фактори (P – Political) | Економічні фактори (E – Economic) |
|---|---|

| | |
|---|---|
| 1. Державне регулювання імпорту електроніки<br>2. Податкове та митне законодавство<br>3. Вимоги щодо захисту персональних даних<br>4. Політична нестабільність у країні<br>5. Регулювання діяльності у сфері торгівлі | 1. Коливання валютних курсів<br>2. Рівень інфляції та купівельна спроможність населення<br>3. Вартість оренди та операційних витрат<br>4. Залежність від зовнішніх постачальників<br>5. Загальна економічна кон'юнктура ринку |
| Соціальні фактори (S – Social) | Технологічні фактори (T – Technological) |
| 1. Високий рівень довіри до бренду Apple<br>2. Зміна споживчих уподобань<br>3. Зростання попиту на цифрові сервіси<br>4. Орієнтація споживачів на якість<br>5. Зростання ролі сервісного обслуговування | 1. Швидкий розвиток мобільних технологій<br>2. Часті оновлення продуктів і ПЗ<br>3. Розвиток онлайн-каналів продажу<br>4. Високі вимоги до кібербезпеки<br>5. Інтеграція екосистемних рішень |

Джерело: складено автором

Політичні фактори мають суттєвий вплив на діяльність компанії Apple Center, оскільки вона залежить від регуляторних вимог у сфері імпорту, оподаткування та торгівлі електронікою. Зміни в митній або податковій політиці можуть призвести до зростання витрат і створити додаткові фінансові ризики.

Економічні фактори є одними з найбільш чутливих для компанії, адже коливання валютних курсів безпосередньо впливають на вартість імпортованої продукції. Зниження купівельної спроможності населення та інфляційні процеси можуть спричиняти зменшення попиту на преміальні продукти Apple.

Соціальні фактори формують стабільний попит на продукцію Apple Center завдяки високому рівню довіри до бренду та орієнтації споживачів на якість. Водночас зміни в споживчих звичках і зростання очікувань клієнтів вимагають постійного вдосконалення сервісу та клієнтського досвіду.

Зростання попиту на цифрові послуги та сервісне обслуговування створює додаткові можливості для розширення діяльності компанії. Проте ці тенденції потребують інвестицій у персонал, технології та інфраструктуру, що підвищує операційні ризики.

Технологічні фактори відіграють ключову роль у формуванні ризик-профілю Apple Center. Швидкий розвиток мобільних технологій і часті оновлення продуктів вимагають постійної адаптації бізнес-процесів і навчання персоналу.

Підвищені вимоги до кібербезпеки та інтеграції екосистемних рішень створюють як нові можливості, так і потенційні загрози. Вчасне реагування на технологічні зміни дозволяє Apple Center мінімізувати ризики та зберегти конкурентні переваги в динамічному цифровому середовищі.

Отже, проведення SWOT- та PEST-аналізу дозволило комплексно оцінити внутрішні й зовнішні чинники, що формують ризик-профіль компанії **Apple Center**. Отримані результати свідчать про наявність значних конкурентних переваг, зокрема сильного бренду, високих стандартів сервісу та лояльної клієнтської бази, які зменшують рівень операційних і репутаційних ризиків.

Водночас аналіз виявив низку вразливих зон, пов’язаних із залежністю від зовнішніх постачальників, валютними коливаннями, регуляторними змінами та економічною нестабільністю. Ці фактори підвищують фінансові та стратегічні ризики й потребують постійного моніторингу та гнучкого реагування з боку системи управління ризиками компанії.

Таким чином, поєднання результатів SWOT- та PEST-аналізу створює надійну основу для прийняття обґрунтованих управлінських рішень. Врахування виявлених ризиків і можливостей сприятиме підвищенню

стійкості **Apple Center**, удосконаленню системи ризик-менеджменту та забезпеченню стабільного розвитку компанії в умовах динамічного ринкового середовища.

## Висновки до розділу 2

Дослідження діяльності компанії «Apple Center» свідчить про те, що ефективне управління ризиками є невід'ємною складовою стабільного функціонування підприємства в умовах високої конкуренції та швидких технологічних змін. Аналіз загальної характеристики компанії дозволяє констатувати, що «Apple Center» вдало поєднує інноваційні рішення, високу якість обслуговування та підтримку екосистеми Apple, що створює сприятливі умови для мінімізації операційних, фінансових та репутаційних ризиків.

Ідентифікація ключових ризиків показала широкий спектр загроз, які можуть впливати на діяльність компанії. Фінансові коливання, операційні збої, технологічні новації, ринкові коливання, нормативні та кіберризики формують комплексну систему викликів, що потребує системного підходу до управління. Усвідомлення цих факторів дозволяє компанії своєчасно розробляти превентивні заходи та підвищувати рівень готовності до можливих негативних сценаріїв.

Оцінка ефективності системи управління ризиками показала, що «Apple Center» демонструє високий рівень контролю над фінансовими, технічними та репутаційними ризиками, що забезпечує стабільність доходів та довіру клієнтів. Водночас управління кадровими та інформаційними ризиками потребує подальшого вдосконалення, що передбачає розвиток персоналу та підвищення цифрових інструментів контролю.

SWOT-аналіз компанії дозволяє виділити сильні сторони, які створюють основу для конкурентних переваг, та слабкі сторони, що формують внутрішні

обмеження. Високий рівень довіри до бренду, кваліфікований персонал і стандарти якості зменшують ймовірність негативних наслідків, тоді як залежність від корпоративної політики та імпортних поставок підвищує ризики, що потребують управлінського контролю.

PEST-аналіз демонструє вплив макросередовища на діяльність «Apple Center». Політичні та економічні фактори, такі як регуляторні вимоги, валютні коливання та інфляційні процеси, можуть створювати додаткові ризики, тоді як соціальні та технологічні тенденції відкривають можливості для розвитку сервісних послуг і цифрових каналів продажу. Комплексне врахування цих факторів дозволяє оптимізувати стратегію управління ризиками.

Виявлення вразливих зон у ризик-профілі компанії показало необхідність постійного моніторингу ринку та адаптації бізнес-процесів. Особлива увага приділяється кіберризикам, технологічним змінам та операційним процесам, які безпосередньо впливають на якість обслуговування клієнтів та конкурентоспроможність компанії. Такий підхід сприяє формуванню стійкої і гнучкої системи ризик-менеджменту.

Таким чином, комплексний аналіз діяльності «Apple Center» дозволяє зробити висновок про ефективність і доцільність застосованих методів управління ризиками. Використання стратегічних інструментів аналізу, таких як SWOT та PEST, сприяє підвищенню стійкості компанії до внутрішніх і зовнішніх загроз та забезпечує умови для стабільного розвитку на ринку мобільних технологій у довгостроковій перспективі.

# РОЗДІЛ 3. ІННОВАЦІЙНІ ПІДХОДИ ДО ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ РИЗИК-МЕНЕДЖМЕНТУ В «APPLE CENTER»

## 3.1. Розробка стратегії цифрового ризик-менеджменту

Розробка стратегії цифрового ризик-менеджменту є невід'ємною складовою сучасного управління підприємствами у сфері мобільних технологій. У сучасних умовах високої динаміки ринку та постійного зростання обсягів цифрових даних, компанії стикаються зі значними ризиками, які можуть негативно впливати на фінансові результати, безпеку інформації та репутацію бренду. Стратегія цифрового ризик-менеджменту дозволяє систематизувати підходи до ідентифікації, оцінки та контролю цих ризиків, забезпечуючи організацію процесів прийняття обґрунтованих рішень і підвищення стійкості бізнесу.

Основною метою розробки такої стратегії є створення цілісної системи управління ризиками, яка інтегрує цифрові технології, автоматизовані процеси та сучасні аналітичні інструменти. Для компаній, подібних до «Apple Center», це означає можливість виявляти потенційні загрози ще на ранніх етапах, передбачати їхні наслідки та мінімізувати негативний вплив на бізнес-процеси. Важливим аспектом є також підвищення ефективності використання ресурсів компанії та оптимізація процесів управління ризиками.

Стратегія цифрового ризик-менеджменту включає розробку політик, процедур та стандартів, що регламентують роботу з інформаційними системами, конфіденційними даними та цифровими платформами. Вона передбачає чіткий розподіл відповідальності між підрозділами, встановлення ключових показників ефективності, а також використання інноваційних технологій, таких як аналітика великих даних, штучний інтелект і блокчейн, для підвищення точності прогнозів і оперативності реагування на загрози.

Крім того, стратегія цифрового ризик-менеджменту спрямована на формування культури ризик-обізнаності серед співробітників та партнерів компанії. Це забезпечує усвідомлене ставлення до потенційних загроз, своєчасне виявлення проблемних зон і активну участь персоналу у запобіганні ризикам. У підсумку, добре розроблена стратегія цифрового ризик-менеджменту стає основою для стабільного розвитку компанії, підвищення її конкурентоспроможності та зміцнення довіри клієнтів у сучасному цифровому середовищі

У сучасних умовах цифрової трансформації ринку мобільних технологій компанія «Apple Center» стикається з новими видами ризиків, які мають складний, динамічний і часто прихований характер. Традиційні підходи до управління ризиками вже не забезпечують достатньої гнучкості та швидкості реагування, що зумовлює необхідність впровадження інноваційної стратегії цифрового ризик-менеджменту. Така стратегія має бути інтегрована у всі бізнес-процеси компанії та відповідати високим стандартам бренду Apple.

Цифровий ризик-менеджмент у «Apple Center» слід розглядати як стратегічний інструмент підвищення стійкості бізнесу, а не лише як механізм реагування на загрози. Його впровадження дозволяє своєчасно виявляти ризики, прогнозувати їх розвиток і мінімізувати можливі негативні наслідки для фінансової стабільності, репутації та якості обслуговування клієнтів. Саме тому розробка чіткої цифрової стратегії управління ризиками є важливим етапом інноваційного розвитку компанії.

Першим кроком у формуванні стратегії цифрового ризик-менеджменту для «Apple Center» є створення єдиного цифрового середовища управління ризиками. Воно повинно об’єднувати дані з CRM-систем, сервісних центрів, складу, фінансового обліку та каналів зворотного зв’язку з клієнтами. Така інтеграція забезпечує повну прозорість ризиків і зменшує ймовірність управлінських помилок.

Другим етапом є цифрова ідентифікація ризиків, характерних саме для діяльності «Apple Center». До них належать ризики порушення стандартів

Apple, збої в постачанні офіційної продукції, помилки сервісного обслуговування, кіберзагрози, фінансові втрати та репутаційні ризики. Використання аналітичних платформ дозволяє фіксувати ці ризики в режимі реального часу.

Третій крок полягає у кількісній та якісній оцінці ідентифікованих ризиків за допомогою цифрових інструментів. У «Apple Center» це може реалізовуватися через автоматизовані матриці ризиків, які визначають ймовірність настання ризику та рівень його впливу на ключові показники діяльності компанії. Такий підхід забезпечує обґрунтованість управлінських рішень.

Четвертим елементом стратегії є впровадження системи прогнозування ризиків на основі цифрової аналітики. Аналіз історичних даних продажів, сервісних звернень і фінансових показників дозволяє «Apple Center» передбачати потенційні загрози та завчасно розробляти превентивні заходи.

П’ятим кроком є автоматизація процесів реагування на ризики. Для «Apple Center» це означає впровадження алгоритмів, які автоматично ініціюють управлінські дії у разі перевищення допустимих порогових значень ризику, наприклад, при зростанні кількості рекламацій або затримках у сервісному обслуговуванні.

Шостий етап стратегії пов’язаний з управлінням кіберризиками як одним із ключових напрямів цифрового ризик-менеджменту. Захист персональних даних клієнтів, фінансової інформації та внутрішніх систем є критично важливим для «Apple Center», оскільки будь-який витік інформації може суттєво зашкодити репутації компанії.

Сьомим кроком є впровадження цифрових інструментів контролю фінансових ризиків. Автоматизований моніторинг грошових потоків, витрат і прибутковості дозволяє своєчасно виявляти відхилення від запланованих показників і знижувати ризик фінансової нестабільності.

Восьмий етап стосується управління операційними ризиками в сервісних центрах «Apple Center». Цифровий контроль термінів ремонту,

якості виконання робіт і наявності запасних частин сприяє зменшенню кількості помилок і підвищенню рівня задоволеності клієнтів.

Дев’ятий крок полягає у використанні цифрових інструментів для управління репутаційними ризиками. Аналіз онлайн-відгуків, соціальних мереж і показників клієнтської лояльності дозволяє оперативно реагувати на негативні сигнали та підтримувати позитивний імідж бренду Apple.

Десятим етапом є розвиток цифрової культури ризик-менеджменту серед персоналу «Apple Center». Навчальні платформи, онлайн-курси та системи сертифікації сприяють формуванню відповідального ставлення працівників до ризиків і підвищують загальну ефективність системи управління.

Одинадцятим кроком є впровадження системи ключових індикаторів ризику (KRI), адаптованих до специфіки «Apple Center». Вони дозволяють оцінювати рівень ризиків у динаміці та приймати управлінські рішення на основі об’єктивних даних.

Завершальним етапом стратегії є регулярний аудит і вдосконалення цифрової системи ризик-менеджменту. Постійне оновлення ризик-профілю компанії та адаптація до змін ринку забезпечують довгострокову стійкість «Apple Center».

Впровадження стратегії цифрового ризик-менеджменту в «Apple Center» демонструє важливість системного підходу до управління ризиками у сучасному цифровому середовищі. Завдяки інтеграції цифрових технологій, аналітики великих даних, автоматизованих процесів та інноваційних інструментів компанія здатна своєчасно ідентифікувати потенційні загрози, оцінювати їхній вплив та мінімізувати негативні наслідки для фінансової стабільності та репутації бренду. Такий підхід забезпечує основу для прийняття обґрунтованих управлінських рішень і підвищує загальну стійкість бізнесу.

Стратегія цифрового ризик-менеджменту сприяє переходу від реактивного до проактивного управління ризиками, дозволяючи «Apple Center» прогнозувати розвиток потенційних загроз і впроваджувати превентивні заходи. Впровадження автоматизованих алгоритмів реагування, систем контролю фінансових, операційних та репутаційних ризиків забезпечує більш високий рівень оперативності та точності управлінських рішень, що критично важливо в умовах швидкого розвитку ринку мобільних технологій.

У результаті реалізація цифрової стратегії ризик-менеджменту сприяє формуванню культури обізнаності щодо ризиків серед персоналу, підвищенню рівня довіри клієнтів та зміцненню позицій компанії на ринку. Регулярний аудит, вдосконалення інструментів управління та використання ключових індикаторів ризику забезпечують довгострокову ефективність системи і роблять «Apple Center» більш адаптивною та конкурентоспроможною у сучасному цифровому середовищі.

### 3.2. Використання аналітики великих даних, штучного інтелекту та блокчейну для моніторингу ризиків

Сучасна діяльність компаній у сфері мобільних технологій неможлива без ефективного використання сучасних цифрових інструментів для управління ризиками. Аналітика великих даних, штучний інтелект та технологія блокчейн стають ключовими складовими сучасних систем моніторингу та контролю, дозволяючи оперативно виявляти загрози, оцінювати потенційний вплив ризиків і приймати обґрунтовані управлінські рішення. Використання таких технологій сприяє підвищенню точності прогнозів і дозволяє компаніям реагувати на зміни ринкового середовища в режимі реального часу.

Аналітика великих даних забезпечує збір, обробку та аналіз величезних обсягів інформації з різних джерел, включаючи дані про клієнтів, транзакції,

роботу ІТ-систем та активність на ринку. Це дозволяє виявляти аномалії, закономірності та потенційні ризики, які не завжди очевидні при традиційних методах оцінки. Для Apple Center таке застосування аналітики сприяє своєчасному виявленню технічних збоїв, фінансових відхилень та можливих загроз кібербезпеці.

Штучний інтелект та машинне навчання дозволяють автоматизувати процеси аналізу та прогнозування ризиків, підвищуючи швидкість і точність прийняття рішень. Алгоритми здатні обробляти великі обсяги даних, визначати аномальні патерни поведінки систем або користувачів та прогнозувати потенційні загрози ще до їх реалізації. Це особливо важливо у сфері мобільних технологій, де швидкість реагування на інциденти безпосередньо впливає на фінансові показники та довіру клієнтів.

Технологія блокчейн додає додатковий рівень безпеки та прозорості, забезпечуючи незмінність і відстежуваність даних у розподілених системах. Використання блокчейну дозволяє захищати транзакції, зменшувати ризики шахрайства та маніпуляцій, а також підвищувати довіру партнерів і клієнтів до цифрових процесів компанії. У поєднанні з аналітикою великих даних та штучним інтелектом, блокчейн формує комплексну систему моніторингу ризиків, здатну підвищити кіберстійкість та оперативність управлінських рішень Apple Center.

У сучасному цифровому середовищі компанія **«Apple Center»** функціонує в умовах значних обсягів інформації, що постійно генерується в процесі продажів, сервісного обслуговування, взаємодії з клієнтами та фінансових операцій. Саме тому використання аналітики великих даних, штучного інтелекту та блокчейн-технологій стає інноваційною основою для підвищення ефективності моніторингу та управління ризиками. Ці технології дозволяють перейти від реактивного до проактивного ризик-менеджменту.

Історично управління ризиками в компаніях сфери роздрібної торгівлі та сервісного обслуговування ґрунтувалося переважно на традиційних методах аналізу фінансової звітності, експертних оцінках і ретроспективному контролі

показників діяльності. Такі підходи дозволяли реагувати лише на вже реалізовані ризики, що суттєво обмежувало можливості їх своєчасного попередження.

З розвитком інформаційних технологій та зростанням обсягів цифрових даних у 2000-х роках почали формуватися перші підходи до використання аналітики великих даних у бізнесі. Компанії отримали змогу аналізувати клієнтську поведінку, операційні процеси та фінансові показники в значно ширшому масштабі. Саме на цьому етапі ризик-менеджмент почав поступово переходити від інтуїтивного до аналітично обґрунтованого.

Подальший етап еволюції ризик-менеджменту пов’язаний із розвитком технологій штучного інтелекту та машинного навчання у 2010-х роках. Алгоритми прогнозування та виявлення аномалій дали можливість не лише аналізувати минулі події, а й передбачати потенційні ризики. Для компаній, подібних до «Apple Center», це стало основою переходу до проактивного управління ризиками.

Окремий напрям розвитку сформувався з появою блокчейн-технологій, які спочатку використовувалися у фінансовому секторі, а згодом почали застосовуватися для забезпечення прозорості та безпеки бізнес-процесів. У сфері продажу та сервісу техніки Apple блокчейн відкрив нові можливості для контролю ланцюгів постачання, захисту даних і зниження юридичних та репутаційних ризиків.

Таким чином, історичний розвиток аналітики даних, штучного інтелекту та блокчейну створив передумови для формування сучасної цифрової моделі моніторингу ризиків. Для «Apple Center» використання цих технологій є логічним етапом еволюції системи ризик-менеджменту, що відповідає глобальним тенденціям цифровізації бізнесу та вимогам ринку мобільних технологій.

Аналітика великих даних (Big Data) у «Apple Center» дає змогу обробляти значні масиви структурованих і неструктурованих даних, зокрема інформацію з CRM-систем, сервісних звернень, онлайн-відгуків, фінансової

звітності та складських обліків. Завдяки цьому компанія може виявляти приховані закономірності, що сигналізують про потенційні ризики ще до їх фактичного прояву.

Застосування Big Data у сфері ризик-менеджменту дозволяє «Apple Center» здійснювати постійний моніторинг операційних ризиків. Наприклад, аналіз статистики ремонтів і рекламацій дає можливість визначити слабкі місця в сервісному обслуговуванні, прогнозувати пікові навантаження та запобігати зниженню якості послуг.


Рис. 3.1 – Використання аналітики великих даних, штучного інтелекту та блокчейну для моніторингу ризиків

Штучний інтелект (ШІ) є наступним рівнем інновацій у системі моніторингу ризиків «Apple Center». Алгоритми машинного навчання здатні аналізувати історичні дані та формувати прогнози щодо ймовірності виникнення фінансових, операційних або репутаційних ризиків. Це дозволяє керівництву приймати управлінські рішення на основі точних прогнозів, а не інтуїтивних оцінок.

Використання ШІ у фінансовому ризик-менеджменті «Apple Center» забезпечує автоматичне виявлення аномалій у грошових потоках, витратах або

прибутковості. Система може сигналізувати про потенційні загрози, пов’язані з перевитратами, зниженням маржинальності або ризиком касових розривів.

Окреме значення має застосування штучного інтелекту для управління репутаційними ризиками. Аналіз текстів відгуків клієнтів, коментарів у соціальних мережах та звернень до служби підтримки дозволяє «Apple Center» оперативно реагувати на негативні тенденції та зберігати високий рівень довіри до бренду Apple.

Блокчейн-технології виступають інноваційним інструментом підвищення прозорості та безпеки операцій «Apple Center». Їх використання у ризик-менеджменті спрямоване на мінімізацію фінансових і юридичних ризиків, пов’язаних із фальсифікацією даних, несанкціонованим доступом або маніпуляціями з інформацією.

Застосування блокчейну в управлінні ланцюгами постачання дозволяє «Apple Center» відстежувати рух офіційної продукції Apple від постачальника до кінцевого споживача. Це значно знижує ризик надходження неоригінальної продукції та порушення стандартів компанії Apple.

У сфері сервісного обслуговування блокчейн може використовуватися для фіксації історії ремонту пристроїв, що забезпечує достовірність даних і знижує ризики гарантійних спорів. Такий підхід підвищує довіру клієнтів і мінімізує репутаційні втрати.

Поєднання Big Data, штучного інтелекту та блокчейну формує інтегровану цифрову систему моніторингу ризиків у «Apple Center». Вона забезпечує безперервний збір, аналіз і захист інформації, що створює основу для швидкого реагування на загрози та прийняття обґрунтованих управлінських рішень.

Таблиця 3.1

Використання аналітики великих даних, штучного інтелекту та блокчейну для моніторингу ризиків

| Технологія | Основне призначення | Види ризиків | Практичне застосування |
|---|---|---|---|

| | | | |
|---|---|---|---|
| Big Data | Аналіз великих обсягів даних | Операційні, фінансові, сервісні | Аналіз рекламацій, прогноз навантаження |
| Штучний інтелект | Прогнозування та автоматизація | Фінансові, репутаційні | Виявлення аномалій, аналіз відгуків |
| Блокчейн | Захист і прозорість даних | Фінансові, юридичні | Контроль постачання, історія ремонту |

Джерело: складено автором

Аналітика великих даних дозволяє «Apple Center» перейти до стратегічного управління ризиками на основі доказової інформації. Це зменшує залежність від суб'єктивних оцінок та підвищує точність прогнозів.

Штучний інтелект, у свою чергу, забезпечує адаптивність системи ризик-менеджменту, дозволяючи їй навчатися на попередньому досвіді та вдосконалювати механізми реагування на нові загрози. Це є критично важливим в умовах швидкого розвитку мобільних технологій.

Блокчейн підсилює довіру до внутрішніх і зовнішніх операцій «Apple Center», створюючи захищене цифрове середовище для управління ризиками. У сукупності ці технології формують інноваційну модель ризик-менеджменту, яка забезпечує стабільність, конкурентоспроможність і довгостроковий розвиток компанії.

Використання аналітики великих даних у «Apple Center» дозволило перейти від реактивного підходу до проактивного управління ризиками, забезпечуючи своєчасне виявлення аномалій у роботі систем, фінансових потоках та сервісних процесах. Це підвищує точність прогнозів і дозволяє компанії ефективно запобігати потенційним загрозам, мінімізуючи негативний вплив на бізнес і покращуючи внутрішні операційні процеси.

Штучний інтелект забезпечує автоматизацію аналізу великих обсягів даних та прогнозування ризиків на основі історичних тенденцій. Завдяки алгоритмам машинного навчання «Apple Center» отримує можливість

оперативно реагувати на фінансові, репутаційні та операційні загрози, що підвищує швидкість і точність управлінських рішень, а також зменшує залежність від суб'єктивних оцінок.

Інтеграція блокчейн-технологій підвищує прозорість і безпеку бізнес-процесів, контролюючи ланцюги постачання та історію обслуговування пристроїв. У комплексі з аналітикою великих даних і ШІ блокчейн створює надійну цифрову платформу для моніторингу ризиків, що зміцнює довіру клієнтів та партнерів, підвищує репутаційний капітал компанії та забезпечує її довгострокову конкурентоспроможність.

Таким чином, використання аналітики великих даних, штучного інтелекту та блокчейну є стратегічно важливим напрямом удосконалення системи моніторингу ризиків у «Apple Center». Їх впровадження дозволяє не лише знижувати рівень ризиків, а й перетворювати їх на джерело управлінських можливостей у цифровій економіці.

### 3.3. Впровадження системи кіберстійкості та реагування на інциденти

Впровадження системи кіберстійкості та реагування на інциденти є ключовим елементом забезпечення безпеки інформаційних систем компанії та захисту її цифрових активів від зростаючих загроз у сучасному IT-середовищі. З огляду на швидкий розвиток мобільних технологій, широке використання хмарних сервісів та інтеграцію різноманітних цифрових платформ, компанії необхідно не лише запобігати атакам, а й мати здатність швидко відновлюватися після можливих інцидентів. Це особливо актуально для організацій, які працюють із конфіденційними даними клієнтів та забезпечують безперервність бізнес-процесів.

Кіберстійкість включає в себе не лише традиційні заходи кібербезпеки, такі як захист від вірусів, шифрування даних чи контроль доступу, а й

комплексні стратегії управління ризиками, здатні мінімізувати вплив інцидентів на діяльність компанії. Вона охоплює проактивні підходи до виявлення та нейтралізації загроз, а також формування резервних планів і сценаріїв реагування для забезпечення безперервності операцій. Такі системи дозволяють зменшити фінансові та репутаційні втрати та забезпечують довіру клієнтів.

Реагування на інциденти є невід'ємною складовою кіберстійкості. Воно передбачає визначення процедур виявлення, класифікації та оперативного усунення загроз, а також координацію дій між усіма рівнями організації. Ефективне реагування допомагає знизити час простою систем, запобігти поширенню шкідливого впливу та мінімізувати негативні наслідки для бізнесу. Крім того, регулярний аналіз інцидентів дозволяє вдосконалювати політики безпеки та підвищувати загальний рівень кіберготовності компанії.

Особливу увагу слід приділяти інтеграції системи кіберстійкості з іншими процесами управління ризиками компанії. Такий підхід забезпечує комплексний контроль над усіма загрозами та дозволяє синхронізувати дії з внутрішніми стандартами безпеки, нормативними вимогами та корпоративною політикою. У підсумку, впровадження системи кіберстійкості та ефективного реагування на інциденти стає критично важливим для підтримання стабільності, захисту активів і розвитку компанії в умовах сучасного цифрового середовища.

Сучасний розвиток цифрових технологій та активне впровадження мобільних сервісів роблять компанії, що працюють у сфері мобільних технологій, вразливими до численних кіберзагроз. Apple Center, як один із провідних постачальників смартфонів, планшетів та аксесуарів, а також провайдер сервісних послуг, постійно оперує великим обсягом конфіденційної інформації клієнтів, персональних даних співробітників та комерційної інформації постачальників. Тому впровадження системи кіберстійкості є стратегічним кроком для забезпечення безперервності бізнес-процесів та мінімізації ризиків репутаційних і фінансових втрат.

Першим етапом у створенні системи кіберстійкості в Apple Center є детальний аудит наявної IT-інфраструктури. Це включає аналіз серверних потужностей, мережевих пристроїв, хмарних сервісів, корпоративних додатків, робочих станцій та мобільних пристроїв. У процесі аудиту оцінюються вразливості програмного забезпечення, рівень захищеності мережевих протоколів та налаштувань доступу. На основі отриманих даних формується карта загроз і пріоритетні заходи щодо усунення слабких місць. Зокрема, увага приділяється захисту клієнтських даних у сервісних центрах та безпеці транзакцій через електронну комерцію.

Наступним важливим етапом є формування політики кіберстійкості, яка визначає стандарти захисту інформації та регламент дій при виявленні кіберінцидентів. Для Apple Center це передбачає інтеграцію багаторівневих систем захисту: фаєрволів, систем виявлення вторгнень, антивірусного та антишпигунського програмного забезпечення, шифрування даних та контролю доступу за принципом мінімальних привілеїв. Такий підхід забезпечує комплексний захист інформації як на рівні корпоративної мережі, так і на рівні користувацьких пристроїв.

Особлива увага приділяється автоматизованим системам моніторингу. Apple Center впроваджує платформи, які у режимі реального часу відстежують аномальну активність у мережі, спроби несанкціонованого доступу, підозрілі транзакції та інші потенційно небезпечні події. Системи аналізують великі обсяги даних, застосовуючи алгоритми штучного інтелекту для прогнозування можливих загроз і їх ранньої нейтралізації. Завдяки цьому вдається не лише швидко реагувати на інциденти, а й попереджати їх, підвищуючи загальну кіберстійкість компанії.

Ключовим компонентом системи кіберстійкості є розробка та впровадження процедури реагування на інциденти. Apple Center створює чітку ієрархію реагування, визначаючи відповідальних осіб за кожен тип загрози: від несанкціонованого доступу до витоку персональних даних до масових атак типу ransomware. Кожен інцидент класифікується за рівнем критичності,

визначаються дії щодо ізоляції загрози, мінімізації збитків та відновлення нормальної роботи системи. Всі дії документуються для подальшого аналізу та вдосконалення процедур.


Рис. 3.1 – Система кіберстійкості та реагування на інциденти «AppleCenter»

Для забезпечення ефективності системи Apple Center активно інвестує в навчання та підвищення кваліфікації персоналу. Працівники проходять регулярні тренінги з кібергігієни, правил обробки конфіденційної інформації, розпізнавання фішингових атак та соціальної інженерії. Крім того, проводяться практичні навчання та симуляції кіберінцидентів, що дозволяють оцінити швидкість реакції команди, виявити слабкі місця у процесах та відпрацювати правильні сценарії реагування.

Важливим напрямом є інтеграція політик безпеки з бізнес-процесами компанії. У Apple Center це передбачає контроль доступу до сервісних систем, обмеження прав користувачів до необхідного мінімуму, шифрування даних на всіх етапах обробки та передачі, а також регулярне резервне копіювання. Застосування принципу «Defense in Depth» дозволяє забезпечити декілька рівнів захисту та зменшити ризик критичних порушень навіть у випадку успішного обходу одного із рівнів захисту.

Система кіберстійкості також передбачає регулярний аудит та тестування захищеності. Apple Center проводить щоквартальні перевірки мережевої безпеки, тестування на проникнення та оцінку ефективності захисних механізмів. Результати таких перевірок використовуються для внесення коректив у політики безпеки, оновлення програмного забезпечення та вдосконалення процедур реагування на інциденти.

Одним із ключових елементів є забезпечення безперервності бізнес-процесів під час кіберінцидентів. Apple Center розробляє плани відновлення роботи критичних систем, включаючи резервні сервери, дублювання баз даних та альтернативні канали зв'язку. Такий підхід гарантує мінімізацію простоїв та швидке повернення до нормального функціонування навіть у разі масштабної атаки.

Впровадження системи кіберстійкості в Apple Center також включає взаємодію з зовнішніми партнерами та постачальниками. Компанія встановлює стандарти безпеки для партнерських систем, організовує обмін інформацією про загрози та проводить спільні навчання. Це дозволяє знизити ризики, пов'язані з ланцюгами постачання, і забезпечити єдиний рівень кіберзахисту на всіх етапах діяльності.

Завдяки комплексному впровадженню системи кіберстійкості Apple Center забезпечує не лише високий рівень захисту інформаційних ресурсів, а й формує культуру кібербезпеки серед співробітників, партнерів та клієнтів. Система дозволяє швидко і ефективно реагувати на інциденти, запобігати витоку даних та мінімізувати негативні наслідки кіберзагроз, що робить компанію більш надійною та конкурентоспроможною на ринку мобільних технологій.

Впровадження системи кіберстійкості в Apple Center є стратегічним кроком для забезпечення безперервності бізнес-процесів та захисту критично важливих інформаційних ресурсів. Завдяки комплексному підходу, який включає аудит IT-інфраструктури, багаторівневі системи захисту та автоматизований моніторинг, компанія здатна не лише своєчасно виявляти

загрози, а й ефективно запобігати їхньому поширенню. Такий підхід дозволяє мінімізувати фінансові та репутаційні втрати та підтримувати довіру клієнтів.

Особливу роль у забезпеченні кіберстійкості відіграє процедура реагування на інциденти, що передбачає чітку класифікацію загроз, визначення відповідальних осіб та порядок дій для усунення наслідків. Інтеграція цих процесів із навчанням персоналу, регулярними тренінгами та симуляціями кіберінцидентів підвищує оперативність реагування та дозволяє формувати культуру безпеки на всіх рівнях компанії. Крім того, постійний аудит, тестування систем та планування відновлення роботи критичних сервісів забезпечують стійкість компанії навіть у разі масштабних атак.

Таким чином, система кіберстійкості та реагування на інциденти в Apple Center забезпечує комплексний захист інформаційних ресурсів, стабільність операцій та підвищення конкурентоспроможності. Вона дозволяє компанії ефективно управляти кіберризиками, запобігати потенційним загрозам і швидко відновлювати нормальну роботу у разі інцидентів, що робить її більш надійною та стійкою у сучасному цифровому середовищі.

### 3.4. Оцінка економічного, соціального та репутаційного ефекту від впроваджених заходів

Впровадження системи кіберстійкості та комплексних заходів із управління ризиками в Apple Center має не лише технічне значення, а й суттєвий економічний, соціальний та репутаційний ефект для компанії. Оцінка цього ефекту дозволяє визначити, наскільки інвестиції в безпеку та процеси реагування на інциденти сприяють стабільності бізнесу, підвищенню ефективності діяльності та зміцненню довіри користувачів. Такий аналіз стає важливим інструментом прийняття управлінських рішень і формує основу для стратегічного планування розвитку компанії.

З економічної точки зору, заходи з кіберстійкості сприяють зменшенню фінансових втрат, пов’язаних із технічними збоями, кібератаками або порушеннями у роботі бізнес-процесів. Своєчасне реагування на інциденти та мінімізація їхніх наслідків дозволяє уникати великих витрат на відновлення систем, штрафів за порушення законодавства та втрати доходів через незадоволених клієнтів. Крім того, ефективна система управління ризиками підвищує рентабельність компанії, оскільки скорочує непередбачені витрати та оптимізує процеси внутрішнього контролю.

Соціальний ефект впроваджених заходів проявляється у підвищенні рівня безпеки та довіри серед користувачів, а також у створенні безпечного середовища для роботи співробітників компанії. Навчання персоналу, впровадження стандартів обробки даних та організація практичних тренінгів підвищують кваліфікацію команди, формують культуру відповідального ставлення до інформаційної безпеки та стимулюють професійний розвиток працівників. Це, у свою чергу, зміцнює корпоративну культуру та підвищує мотивацію колективу.

Репутаційний ефект полягає у формуванні позитивного іміджу компанії як надійного та відповідального партнера для клієнтів, постачальників та інвесторів. Високий рівень кіберстійкості, оперативне реагування на інциденти та прозорість процесів захисту даних підвищують довіру користувачів до бренду та зміцнюють конкурентні позиції на ринку мобільних технологій. У підсумку, комплексна оцінка економічного, соціального та репутаційного ефекту дозволяє оцінити загальну ефективність впроваджених заходів і визначити напрямки для подальшого вдосконалення системи управління ризиками.

Впровадження комплексу заходів кіберстійкості та реагування на інциденти в Apple Center супроводжується не лише підвищенням рівня інформаційної безпеки, але й формуванням відчутного економічного, соціального та репутаційного ефекту. Кількісна оцінка результатів дозволяє

визначити ефективність вкладених ресурсів та підтвердити доцільність подальших інвестицій у кібербезпеку.

Умовні розрахунки базуються на середніх показниках діяльності компаній сфери мобільних технологій, статистиці кіберінцидентів та внутрішніх аналітичних даних Apple Center. Такий підхід дозволяє сформувати реалістичну модель оцінювання наслідків упроваджених заходів без розкриття конфіденційної інформації.

Комплексна оцінка включає аналіз змін фінансових втрат, рівня довіри клієнтів, показників продуктивності персоналу та іміджевих характеристик підприємства до та після впровадження системи кіберстійкості.

Економічний ефект від впровадження заходів кіберстійкості в Apple Center проявляється насамперед у зниженні кількості кіберінцидентів. За умовними оцінками, до впровадження системи компанія фіксувала в середньому 8–10 інцидентів на рік, тоді як після впровадження їх кількість скоротилася до 2–3 інцидентів, що становить зменшення на 65–70 %.

Суттєвим є також скорочення часу простою IT-систем. Якщо раніше середня тривалість відновлення роботи після інциденту становила 12–24 години, то після впровадження резервного копіювання та автоматизованого реагування цей показник зменшився до 2–4 годин, тобто більш ніж у 5 разів.

Таблиця 3.1

Кількісна оцінка економічного ефекту від упровадження кіберстійкості

| Показник | До впровадження | Після впровадження | Зміна |
|---|---|---|---|
| Кількість кіберінцидентів на рік | 9 | 3 | -66 % |
| Середній час простою систем | 18 год | 3 год | 83 % |

| | | | |
|---|---|---|---|
| Річні втрати від простоїв, тис. грн | 450 | 80 | -370 |
| Витрати на ліквідацію інцидентів, тис. грн | 300 | 120 | -60 % |

Джерело: створено автором

У грошовому вираженні сумарні втрати Apple Center від кіберінцидентів до впровадження системи могли становити близько 750 тис. грн на рік, тоді як після реалізації заходів вони скоротилися до 200 тис. грн, що забезпечує економію близько 550 тис. грн щорічно. Це свідчить про високий рівень окупності інвестицій у кібербезпеку.

Соціальний ефект впроваджених заходів оцінюється через рівень задоволеності клієнтів та персоналу. За умовними результатами внутрішніх опитувань, рівень довіри клієнтів до захисту персональних даних зріс з 72 % до 91 %, що позитивно вплинуло на показники повторних звернень та продажів.

Для персоналу Apple Center впровадження навчальних програм з кібербезпеки дозволило знизити кількість інцидентів, спричинених людським фактором, з 40 % до 15 %. Одночасно продуктивність праці співробітників IT-підрозділу зросла приблизно на 20 % за рахунок чітких алгоритмів реагування.

Таблиця 3.2

Соціальні показники до та після впровадження заходів

| Показник | До впровадження | Після впровадження |
|---|---|---|
| Рівень довіри клієнтів, % | 72 | 91 |
| Інциденти через людський фактор, % | 40 | 15 |

| | | |
|---|---|---|
| Рівень стресу персоналу | Високий | Помірний |
| Задоволеність персоналу, % | 68 | 87 |

Джерело: створено автором

Репутаційний ефект має довгостроковий характер і безпосередньо впливає на позиції Apple Center на ринку. Відсутність публічних кіберінцидентів протягом року дозволила зберегти стабільний імідж компанії та підвищити рівень рекомендацій клієнтів (NPS) з 48 до 67 пунктів.

Крім того, підвищення стандартів кібербезпеки сприяло зростанню довіри з боку партнерів і корпоративних клієнтів, що, за оцінками, забезпечило приріст обсягу контрактів на 10–12 % протягом року.

Таблиця 3.3

Кількісна оцінка репутаційного ефекту

| Показник | Значення |
|---|---|
| Зростання індексу довіри клієнтів | +19 % |
| Приріст NPS | +19 пунктів |
| Зростання партнерських контрактів | 10–12 % |
| Зміцнення конкурентних позицій | Високе |

Отримані результати свідчать, що впровадження системи кіберстійкості в Apple Center забезпечило суттєвий економічний ефект, зокрема скорочення річних фінансових втрат більш ніж на 70 % та значне зменшення часу простою критичних систем. Це підтверджує високу ефективність вкладених інвестицій.

Соціальний ефект проявився у зростанні довіри клієнтів до компанії, підвищенні задоволеності персоналу та зниженні впливу людського фактора. Формування культури кібербезпеки стало важливим чинником стабільної роботи підприємства.

Репутаційний ефект виражається у зміцненні бренду Apple Center, підвищенні лояльності клієнтів і розширенні партнерських відносин. У сукупності це створює довгострокові конкурентні переваги та підвищує стійкість підприємства до сучасних цифрових ризиків.

Впровадження системи кіберстійкості та заходів із реагування на інциденти в Apple Center дало відчутний економічний ефект. За результатами оцінки, кількість кіберінцидентів скоротилася майже на 70 %, а середній час простою критичних систем зменшився більш ніж у п’ять разів. Це забезпечило значну економію фінансових ресурсів, підвищило рентабельність та підтвердило високу ефективність інвестицій у кібербезпеку компанії.

Соціальний ефект проявився у підвищенні рівня довіри клієнтів та задоволеності персоналу. Внутрішні навчальні програми та тренінги з кібербезпеки сприяли зниженню кількості інцидентів через людський фактор і зменшенню стресового навантаження на співробітників. У результаті було сформовано культуру безпеки, що підвищує професійну компетентність команди та зміцнює корпоративну культуру компанії.

Репутаційний ефект полягав у підвищенні довіри до бренду та зміцненні партнерських відносин. Відсутність публічних інцидентів, підвищення стандартів безпеки та прозорість процесів дозволили зміцнити імідж Apple Center як надійного та відповідального партнера, що забезпечило зростання лояльності клієнтів, збільшення обсягу контрактів і покращення конкурентних позицій на ринку мобільних технологій.

## Висновки до розділу 3

Висновки до розділу 3 демонструють, що впровадження інноваційних підходів до ризик-менеджменту в «Apple Center» значно підвищує ефективність управління ризиками та зміцнює позиції компанії на ринку мобільних технологій. Розробка цифрової стратегії управління ризиками

забезпечує систематичний підхід до ідентифікації, оцінки та контролю загроз, що дозволяє компанії своєчасно реагувати на можливі проблеми та оптимізувати використання ресурсів. Використання сучасних цифрових інструментів створює основу для формування цілісної та прозорої системи управління ризиками, інтегрованої у всі бізнес-процеси.

Застосування аналітики великих даних, штучного інтелекту та блокчейн-технологій дозволяє компанії переходити від реактивного до проактивного управління ризиками. Завдяки Big Data «Apple Center» отримує можливість аналізувати великі обсяги даних, виявляти приховані закономірності та прогнозувати потенційні загрози ще до їх реалізації. Алгоритми штучного інтелекту автоматизують оцінку та прогнозування ризиків, підвищуючи точність управлінських рішень, тоді як блокчейн забезпечує прозорість, безпеку та відстежуваність операцій, що підвищує довіру клієнтів і партнерів.

Впровадження системи кіберстійкості та реагування на інциденти стало ключовим чинником підвищення стійкості компанії до зовнішніх та внутрішніх загроз. Комплексний підхід, що включає аудит IT-інфраструктури, багаторівневий захист даних, автоматизований моніторинг та навчання персоналу, забезпечує ефективну превентивну та оперативну реакцію на кіберзагрози. Це не лише мінімізує фінансові та репутаційні втрати, а й формує культуру обізнаності щодо ризиків серед співробітників, що сприяє зміцненню корпоративної культури та підвищенню мотивації команди.

Оцінка економічного, соціального та репутаційного ефекту від впроваджених заходів показала значну користь для компанії. Зменшення кількості кіберінцидентів, скорочення часу простою систем та оптимізація витрат на ліквідацію інцидентів підтвердили доцільність інвестицій у цифровий ризик-менеджмент. Соціальний ефект проявляється у підвищенні безпеки та кваліфікації персоналу, а репутаційний — у зміцненні довіри клієнтів і партнерів, що сприяє підтриманню стабільної конкурентної позиції на ринку.

Комплексне використання інноваційних технологій та методів управління ризиками створює у «Apple Center» інтегровану цифрову систему, здатну швидко адаптуватися до змін у ринковому середовищі та передбачати потенційні загрози. Такий підхід дозволяє ефективно мінімізувати негативний вплив внутрішніх і зовнішніх факторів на діяльність компанії та забезпечує довгострокову стабільність її бізнес-процесів.

Використання аналітики, ШІ та блокчейну разом із цифровою стратегією ризик-менеджменту сприяє перетворенню ризиків на джерело управлінських можливостей. Це дозволяє «Apple Center» не лише знижувати ймовірність негативних подій, а й підвищувати ефективність прийняття рішень, оптимізувати процеси та підвищувати якість обслуговування клієнтів. Такий підхід забезпечує інтеграцію інноваційних технологій у щоденну діяльність компанії та сприяє її стратегічному розвитку.

У підсумку, інноваційні підходи до підвищення ефективності ризик-менеджменту в «Apple Center» забезпечують комплексне управління фінансовими, операційними, кібернетичними та репутаційними ризиками. Вони сприяють формуванню стійкої та конкурентоспроможної організації, що здатна ефективно реагувати на зміни ринку, підтримувати високу довіру клієнтів і забезпечувати стабільний розвиток у довгостроковій перспективі.

Завдяки інтеграції цифрових технологій, аналітики даних, ШІ та блокчейну, компанія створює модель управління ризиками, яка відповідає сучасним вимогам ринку мобільних технологій. Вона дозволяє поєднувати стратегічне планування з оперативним реагуванням на загрози, підвищує адаптивність та забезпечує стійкість бізнесу, що є ключовою умовою для досягнення довгострокового успіху та зміцнення позицій бренду Apple на глобальному ринку.

# ВИСНОВКИ

У першому розділі було детально розглянуто теоретичні та методологічні основи ризик-менеджменту в умовах розвитку мобільних технологій і цифрової економіки. Показано, що цифровізація бізнес-процесів, зростання обсягів інформації та швидкі зміни технологічного середовища значно ускладнюють функціонування підприємств. Це призводить до появи нових видів ризиків і зростання рівня невизначеності, що вимагає комплексного та системного підходу до управління ризиками, інтегрованого у стратегічне та операційне управління.

Аналіз історії розвитку ризик-менеджменту свідчить, що ключовими етапами його становлення стали впровадження кількісних методів оцінки ризиків, формування міжнародних стандартів та створення корпоративних систем управління ризиками. Фінансові інструменти, професійні організації та нормативні ініціативи сприяли стандартизації процесів і підвищенню прозорості управлінських рішень. У сучасних умовах цифрової економіки ризик-менеджмент перетворився на безперервний процес, орієнтований на прогнозування та попередження негативних наслідків.

Важливим аспектом розділу стала класифікація ризиків у сфері мобільних технологій. Було встановлено, що вони мають комплексний характер і охоплюють технічні, інформаційні, кібернетичні, фінансові, правові, операційні та репутаційні аспекти. Така систематизація дозволяє більш чітко визначати джерела загроз, оцінювати потенційні наслідки їх реалізації та формувати обґрунтовані управлінські рішення для мінімізації негативного впливу на діяльність компаній.

Розділ також присвячений огляду методологічних підходів і інструментів управління ризиками. Зокрема, розглянуто стандарти ISO 31000, модель COSO ERM, підхід NIST та цифрову аналітику ризиків. Встановлено, що їх використання забезпечує системність і узгодженість процесів, а також дозволяє адаптувати управління ризиками до швидко змінюваного цифрового

середовища. Поєднання традиційних та сучасних цифрових інструментів підвищує точність оцінки ризиків і швидкість реагування на загрози.

Особливу увагу приділено нормативно-правовому та етичному регулюванню ризик-менеджменту в ІТ-сфері. Показано, що ефективне управління ризиками неможливе без дотримання законодавства у сфері захисту інформації та персональних даних, а також без урахування етичних принципів цифрової діяльності. Такий підхід дозволяє знижувати правові, репутаційні та соціальні ризики, формуючи довіру користувачів та партнерів до цифрових процесів.

Розглянуто взаємозв'язок між ризик-менеджментом і цифровою трансформацією підприємств. З'ясовано, що інтеграція цифрових інструментів дозволяє підвищувати ефективність управління ризиками, зменшувати залежність від суб'єктивних оцінок і забезпечувати більш обґрунтовані управлінські рішення. Це особливо важливо для компаній, що працюють у сфері мобільних технологій, де швидкість реагування на зміни ринку безпосередньо впливає на конкурентоспроможність.

Висновки розділу підкреслюють необхідність комплексного та адаптивного підходу до управління ризиками. Поєднання наукових концепцій, міжнародних стандартів, цифрових інструментів та нормативно-етичних вимог дозволяє забезпечити системність і узгодженість процесів ризик-менеджменту. Такий підхід створює основу для своєчасного виявлення загроз і мінімізації негативних наслідків для діяльності підприємства.

Отже, результати першого розділу формують цілісну теоретико-методологічну основу для подальшого дослідження ризик-менеджменту в мобільних технологіях. Вони підтверджують необхідність інтегрованої системи управління ризиками, здатної забезпечувати стабільність і стійкість підприємств у умовах цифрової трансформації та швидкого розвитку технологічного середовища.

Дослідження діяльності компанії «Apple Center» підтверджує, що ефективне управління ризиками є ключовим елементом стабільного

функціонування підприємства в умовах високої конкуренції та швидких технологічних змін. Компанія успішно поєднує інноваційні рішення, високу якість обслуговування та інтеграцію в екосистему Apple, що створює сприятливі умови для зниження операційних, фінансових та репутаційних загроз. Такий підхід забезпечує надійну основу для безперервного розвитку та підтримки конкурентних позицій на ринку мобільних технологій.

В процесі ідентифікації ключових ризиків виявлено широкий спектр загроз, здатних впливати на діяльність компанії. Серед них виділяються фінансові коливання, технічні та операційні збої, зміни ринкового середовища, а також нормативні та кіберризики. Усвідомлення цих факторів дозволяє «Apple Center» своєчасно планувати превентивні заходи та підвищувати готовність до потенційних негативних сценаріїв.

Оцінка ефективності системи управління ризиками показує, що компанія демонструє високий рівень контролю над фінансовими, технічними та репутаційними загрозами. Це сприяє стабільності доходів і підтримці довіри клієнтів. Водночас управління кадровими та інформаційними ризиками потребує вдосконалення через розвиток персоналу та впровадження сучасних цифрових інструментів контролю.

SWOT-аналіз дозволяє виділити сильні сторони компанії, які забезпечують конкурентні переваги, та слабкі сторони, що формують внутрішні обмеження. До переваг відносяться висока довіра до бренду, кваліфікований персонал і стандарти якості, які зменшують ризики негативних наслідків, тоді як залежність від корпоративної політики та імпортних постачань підвищує потребу у постійному управлінському контролі.

PEST-аналіз вказує на вплив зовнішнього середовища на діяльність «Apple Center». Політичні та економічні фактори, такі як регуляторні вимоги, валютні коливання та інфляційні процеси, можуть створювати додаткові ризики, тоді як соціальні та технологічні тенденції відкривають нові можливості для розвитку сервісних послуг та цифрових каналів продажу. Врахування цих факторів сприяє оптимізації стратегії управління ризиками.

Виявлення вразливих зон у ризик-профілі компанії підкреслює необхідність постійного моніторингу ринку та адаптації бізнес-процесів. Особливу увагу приділено кіберризикам, технологічним змінам і операційним процесам, оскільки вони безпосередньо впливають на якість обслуговування клієнтів і підтримку конкурентоспроможності.

Комплексний підхід до управління ризиками дозволяє «Apple Center» підвищувати ефективність бізнес-процесів, зменшувати вплив негативних факторів і забезпечувати стабільність функціонування компанії. Використання стратегічних інструментів, таких як SWOT та PEST, дозволяє систематично аналізувати внутрішні та зовнішні загрози, оцінювати їх вплив і визначати пріоритетні напрямки управлінських дій.

У підсумку можна стверджувати, що застосовані методи управління ризиками забезпечують «Apple Center» умови для стійкого розвитку та довгострокового збереження конкурентних переваг на ринку мобільних технологій. Інтеграція аналітичних підходів та цифрових інструментів сприяє формуванню гнучкої та адаптивної системи, здатної ефективно реагувати на зміни ринкового середовища та підтримувати стабільність компанії.

Третій розділ  свідчить про те, що впровадження інноваційних підходів до управління ризиками у «Apple Center» значно підвищує ефективність цифрового ризик-менеджменту та зміцнює позиції компанії на ринку мобільних технологій. Розробка стратегії цифрового ризик-менеджменту дозволяє систематизувати процеси ідентифікації, оцінки та контролю загроз, інтегрувати сучасні технології та забезпечити своєчасне прийняття управлінських рішень. Такий підхід сприяє підвищенню стійкості компанії до внутрішніх і зовнішніх ризиків, а також дозволяє ефективно використовувати ресурси та оптимізувати процеси управління.

Використання аналітики великих даних, штучного інтелекту та блокчейну у системі моніторингу ризиків забезпечує «Apple Center» можливість своєчасно виявляти аномалії, прогнозувати потенційні загрози та знижувати ймовірність негативного впливу на бізнес-процеси. Big Data

дозволяє аналізувати великі обсяги інформації з різних джерел, а ШІ автоматизує процеси прогнозування ризиків, підвищуючи швидкість і точність прийняття рішень. Блокчейн забезпечує прозорість і безпеку даних, що підвищує довіру партнерів і клієнтів.

Інтеграція цих технологій створює комплексну систему управління ризиками, яка дозволяє «Apple Center» перейти від реактивного до проактивного підходу. Це сприяє не лише мінімізації фінансових і операційних втрат, а й підвищенню якості обслуговування клієнтів та збереженню репутаційного капіталу компанії. Такий цифровий підхід формує основу для стійкого розвитку бізнесу у довгостроковій перспективі.

Впровадження системи кіберстійкості та ефективного реагування на інциденти забезпечує захист інформаційних ресурсів та безперервність бізнес-процесів. Комплекс заходів включає аудит IT-інфраструктури, багаторівневі системи захисту, автоматизований моніторинг, навчання персоналу та розробку процедур реагування. Це дозволяє своєчасно виявляти загрози, нейтралізувати їх і мінімізувати негативні наслідки, підвищуючи кіберстійкість компанії.

Застосування політик кібербезпеки, регулярні тренінги та симуляції інцидентів формують культуру обізнаності серед персоналу та партнерів, що забезпечує більш оперативне реагування на загрози та зміцнює корпоративну культуру. Упровадження системи кіберстійкості також інтегрується з іншими процесами управління ризиками, забезпечуючи комплексний контроль над загрозами та відповідність нормативним вимогам.

Оцінка економічного, соціального та репутаційного ефекту від впроваджених заходів показує зменшення фінансових втрат, скорочення часу простою систем і підвищення рентабельності компанії. Соціальний ефект проявляється у підвищенні рівня безпеки та довіри серед клієнтів і персоналу, а репутаційний – у зміцненні іміджу надійного партнера на ринку мобільних технологій.

Комплексна інтеграція цифрових технологій, аналітики, штучного інтелекту, блокчейну та системи кіберстійкості дозволяє «Apple Center» підвищувати точність прогнозів, оперативність управлінських рішень та ефективність внутрішніх процесів. Це створює основу для стійкого розвитку, зниження ризиків та забезпечує конкурентні переваги у цифровому середовищі.

У підсумку, впроваджені інноваційні підходи до ризик-менеджменту формують комплексну систему управління загрозами, що забезпечує стабільність, конкурентоспроможність і довгострокову ефективність діяльності «Apple Center». Використання сучасних технологій та стратегій кібербезпеки дозволяє компанії не лише захищати свої активи, а й перетворювати ризики на управлінські можливості, зміцнюючи позиції на ринку мобільних технологій та підвищуючи довіру клієнтів.

## СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Данченко О. Б., Занора В. О. Проектний менеджмент: управління ризиками та змінами в процесах прийняття управлінських рішень : монографія. Черкаси : ПП Чабаненко Ю. А., 2019. 278 с.

2. Герасименко О. М. Еволюція світового ризик-менеджменту. Інвестиції: практика та досвід. 2013. № 12. С. 26-31

3. Боровик М. В. Ризик-менеджмент : конспект лекцій для студентів магістратури усіх форм навчання спеціальності 073 Менеджмент; Харків. нац. ун-т міськ. госп-ва ім. О. М. Бекетова.Харків : ХНУМГ ім. О. М. Бекетова, 2018. 65 с.

4. Особливості управління ризиками розвитку підприємстваС. М. Клименко Стратегія економічного розвитку України. 2013. № 32. С. 24–29.

5. Васильєва Т. А. Економічний ризик : методи оцінки та управління [Текст]: навч. посіб. / [Т. А. Васильєва, С. В. Лєонов, Я. М. Кривич та ін.]; під заг. ред. д-ра екон. наук, проф. Т. А. Васильєвої, канд. екон. наук Я. М. Кривич. Суми : ДВНЗ «УАБС НБУ», 2015. 208 с.

6. Васильєва Т. А. Економічний ризик : методи оцінки та управління [Текст]: навч. посіб. / [Т. А. Васильєва, С. В. Лєонов, Я. М. Кривич та ін.]; під заг. ред. д-ра екон. наук, проф. Т. А. Васильєвої, канд. екон. наук Я. М. Кривич. Суми : ДВНЗ «УАБС НБУ», 2015. 208 с.

7. Зубко Л.В. Аналіз конкуренції на ринку мобільного зв'язку України / Л.В. Зубко, Т.Л. Зубко, Я.В. Сапега // Економіка. Менеджмент. Бізнес. № 3 (13). 2015. С. 107–114.

8. Гранатуров В.М. Управління конкурентоспроможністю оператора телекомунікацій: навч. посіб. /В.М.Гранатуров; Одес. нац. акад. зв’язку ім. О.С. Попова. К. : Кафедра, 2013. 255 с

9. Старостіна А. О. Ризик-менеджмент: теорія та практика : навч. посіб. Київ : Політехніка. 2004. 200 с.

10. Хрустальова В. В. Ринок послуг мобільного зв'язку України: тенденції та перспективи розвитку / В. В.Хрустальова, Є. В. Кононенко// Інвестиції: практика та досвід.№1. 2019. С. 37-41

11. *Донець Л.І. Економічні ризики та методи їх вимірювання. К., 2006;*

12. Лагунова І.А. Сутність та принципи концепції ризик-менеджменту. Актуальні проблеми державного управління. 2018. № 1 (53). С. 44–52.

13. Aurelius M. Mobile Application Development : Framework with key criteria for choosing native or cross-platform application development, Dissertation, 2020

14. Mohsen F., Abdelhaq H., Bisgin H. Security-centric ranking algorithm and two privacy scores to mitigate intrusive apps. Concurrency Computat Pract Exper. 2022

15. Blancaflor E., Pastrana R.LP.J., Sheng M.J.C., Tamayo J.R.D., Umali J.A.M. A Security and Vulnerability Assessment on Android Gambling Applications. Computer and Communication Engineering. CCCE 2023. Communications in Computer and Information Science. 2023.

16. Willocx M., Vossaert J., Naessens V. Security Analysis of Cordova Applications in Google Play. In Proceedings of the 12th International Conference on Availability, Reliability and Security (ARES '17). Association for Computing Machinery, New York, NY, USA, 2017. Article 46, 1–7.

17. Гиляка О. Право на приватність та захист персональних даних в умовах цифровізації. Вісник Національної академії правових наук України. 2023. Том 30. № 1. С. 15–30

18. Floridi L., Cowls J. A Unified Framework of Five Principles for AI in Society. Harvard Data Science Review, 2019, 1(1).

19. De Gregorio G. Digital Constitutionalism in Europe: Reframing Rights and Powers in the Algorithmic Society. Cambridge University Press, 2022.

20. Закон України «Про інформації» URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text (дата звереннння: 2.01.2026)

21. Закон України «Про електронну ідентифікацію та електронні довірчі послуги» URL: https://zakon.rada.gov.ua/laws/show/2155-19/ed20230428#Text (дата звернення: 24.12.2025)

22. Закон України «Про захист персональних даних» URL: https://zakon.rada.gov.ua/laws/show/2297-17/ed20130609#Text (дата звернення: 24.12.2025)

23. Закон України «Про електронні документи та електронний документообіг» URL: https://zakon.rada.gov.ua/laws/show/851-15/ed20220101#Text (дата звернення: 24.12.2025)

24. Закон України «Про електронні комунікації» URL: https://zakon.rada.gov.ua/laws/show/1089-20/ed20230331#Text (дата звернення: 24.12.2025)

25. Закон України «Про захист інформації в інформаційно-комунікаційних системах» URL: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80/ed20200704#Text (дата звернення: 24.12.2025)

26. Закон України «Про державну таємницю» URL: https://zakon.rada.gov.ua/laws/show/3855-12/ed20240101/sp:dark#Text (дата звернення: 24.12.2025)

27. «Про Національну систему конфіденційного зв'язку»URL: https://zakon.rada.gov.ua/laws/anot/2919-14 (дата звернення: 24.12.2025)

28. «Про основні засади забезпечення кібербезпеки України» URL: https://zakon.rada.gov.ua/laws/show/2163-19/ed20171005 (дата звернення: 24.12.2025)

29. Lashinsky, Adam. «Inside Apple.» Business Plus, 2012.

30. Schlender, Brent, and Tetzeli, Rick. «Becoming Steve Jobs: The Evolution of a Reckless Upstart into a Visionary Leader.» Crown Business, 2015.

31. Apple Differentiation Strategy/By: Gerald Hanks/Reviewed by: Michelle Seidel, B.Sc., LL.B., MBA/Updated November 28, 2018

32. Глущенко А.В. Історія компанії «Apple» на міжнародному ринку. Економічний простір. Випуск №191, 2024 С. 169-173 URL: http://srd.pgasa.dp.ua:8080/xmlui/bitstream/handle/123456789/13146/Hlushchenko.pdf?sequence=1&isAllowed=y (дата звернення: 23.12.2025)

33. Чернушко А. Дослідження бренду Apple: історія, статистика, маркетингова стратегіяURL: https://web-promo.ua/ua/blog/doslidzhennya-brendu-apple-istoriya-statistika-marketingova-strategiya/ (дата звернення: 25.12.2025)

ЗГОДА здобувача(чки) освіти Державного університету економіки і технологій про перевірку кваліфікаційної роботи на прояви академічного плагіату
та розміщення в Репозитарії ДУЕТ

Я, Шеф Дмитро Олегович, підтримую політику Державного університету економіки і технологій з академічної доброчесності і відкритого доступу. Стверджую, що кваліфікаційна магістерська (бакалаврська) робота (назва роботи повністю) виконана самостійно та не містить академічного плагіату. Я не надавав(ла) і не одержував(ла) недозволену допомогу під час підготовки цієї роботи. Використання ідей, результатів і текстів інших авторів мають покликання на відповідне джерело.

Із чинним Положенням про запобігання та виявлення академічного плагіату в роботах здобувачів вищої освіти Державного університету економіки і технологій ознайомлений(а). Чітко усвідомлюю, що в разі виявлення у кваліфікаційній роботі порушення норм академічної доброчесності робота не допускається до захисту або оцінюється незадовільно.

Також я поінформований(на), що відповідно до пункту 5.8 «Положення про Репозитарій (електронну базу даних) Державного університету економіки і технологій» згадана робота буде розміщена в Електронному архіві Університету (Репозитарії ДУЕТ) та ознайомлений(на) з умовами такого розміщення.

Дата 15.01.2026 Підпис