**Карпатський національний університет імені Василя Стефаника**

**Факультет управління**
**Кафедра менеджменту та бізнес-адміністрування**

# КВАЛІФІКАЦІЙНА РОБОТА

на здобуття другого (магістерського) рівня вищої освіти

на тему: **Управління ризиками в проєктному менеджменті**

Виконав: студент ІІ курсу
освітнього рівня «магістр» групи МБА-21м
спеціальності 073 «Менеджмент»
освітньої програми «Бізнес-адміністрування»

Яблончук Олександр Володимирович

Керівник: к.е.н., доц. Томашевська А.В.
Рецензент: д.е.н., проф. Пилипів Н.І.

Івано-Франківськ – 2025 р

# ЗМІСТ

# ВСТУП

**Актуальність теми.** В умовах повномасштабного вторгнення країни-агресора на територію України, управління ризиками набуло визначальної важливості. Збройна агресія проти нашої держави призвела до великих втрат – людських, інфраструктурних та інформаційних – та помітно змінила підхід до належної організації в усіх можливих сферах діяльності. В ІТ-секторі, який є надзвичайно важливим для економіки країни, а ризики стали більш комплексними, зокрема: кібератаки, енергопостачання, міграція кадрів, нові форми невизначеності та порушення необхідних поставок.

За умов війни ризики для вітчизняних компаній перестали носити суто прогнозований характер чи бути керованими, трансформувавшись на різносторонні загрози, що виникають несподівано та потребують миттєвої реакції. Значною мірою це стосується ІТ-сфери, де будь-який збій може привести до втрати важливих даних для роботи, зупинки клієнтських проєктів та порушення роботи систем. Також цю ситуацію ускладнює те, що звичні підходи до управління ризиками вже не надають достатнього рівня захисту, проте вони не враховували реалій релокацій команд, обстрілів, загрози кібершпигування та нестабільності інфраструктури. За таких умов компанії повинні переглядати підходи до організації проєктної діяльності, розробляти нові алгоритми реагування та впроваджувати гнучкі моделі управління. Безпосередньо це робить питання сучасного механізму управління ризиками не тільки безумовно актуальним, а і критично необхідним для забезпечення стійкості та розвитку проєктів, підтримки стабільності економіки та збереження конкурентоспроможності.

Дослідження сучасних українських науковців в цій сфері підтверджують важливість цієї теми, зокрема: О. Ляхова розглядала управління ризиками в проєктному менеджменті як головне для виробничого менеджменту [23]; Я. Панова аналізувала невизначеність та ризики у проєктному менеджменті всіх підприємств справжнього сектору [28]; Н. Трушкіна досліджувала проєктні

ризики ІТ-компаній у кризових ситуаціях [47]. Окрім згаданих вище дослідників, варто звернутись ще і до думок інших, які аналізують проблеми управління ризиками в проєктному менеджменті. Так, І. Малик [24] підкреслює, що за умов нестабільності зовнішнього середовища особливого значення набуває формування системи швидкого попередження ризиків, які спроможні максимально швидко реагувати на критичні зміни в ІТ-компаніях на українському ринку; С. Коваленко [18] розкриває питання щодо економічної стійкості проєктів у період воєнних та післявоєнних криз, акцентуючи, що ризики ІТ-компаній помітно ускладнюється через глобальні порушення логістичних ланцюгів та кіберзагрози, а тому управління ризиками повинно передбачати не тільки превентивні, а і адаптивні механізми. З іншої сторони О. Діденко [9] розглядає управління ризиками зі сторони стратегічного розвитку підприємств, акцентуючи, що в умовах воєнного стану проєктні команди мають формувати багаторівневі моделі стійкості, які включають інформаційні, кадрові, енергетичні та технологічні компоненти. Також дослідниця акцентує, що стабільність ІТ-проєктів безпосередньо залежить від якості оцінки ризиків та їхнього моніторингу протягом усього життєвого циклу.

Хоч управління ризиками в проєктному менеджменті досліджувалось вченими різносторонньо, однак залишаються недослідженими особливості управління ризиками в умовах воєнного стану, оскільки дає змогу адаптувати наукові надбання до реалій діяльності компаній, які функціонують на українських теренах під час війни. Саме ці аспекти і зумовлюють актуальність дослідження цієї теми у відповідності до реалій сьогодення.

**Метою** є різносторонній аналіз системи управління ризиками компаній за умов воєнного стану, розкриття ключових особливостей, шляхів та проблем щодо удосконалення, що дає змогу покращити ефективності діяльності компаній, а також забезпечити її стійкість за кризових умов.

Окреслена мета обумовила вирішення таких **завдань**:

- розкрити понятійний апарат та загальну характеристику проєктного менеджменту;

- виокремити класифікацію проєктного менеджменту;
- дослідити головні етапи управління в проєктному менеджменті;
- охарактеризувати загальні відомості та правові засади діяльності компанії «Українські інформаційні технології»;
- встановити основні способи управління ризиками в компанії «Українські інформаційні технології»;
- визначити проблеми, які виникають під час управління ризиками в компанії «Українські інформаційні технології»;
- проаналізувати світовий досвід покращення управління ризиками в проєктному менеджменті та способи реалізації їх в Україні;
- визначити шляхи удосконалення управління ризиками в сучасних умовах;
- дослідити особливості управління ризиками в умовах дії воєнного стану.

**Об'єктом** є процес управління ризиками у діяльності ІТ-компаній на прикладі ТОВ «Українські інформаційні технології».

**Предметом** є принципи, особливості, механізми та методи управління ризиками, які реалізуються в компаніях під час воєнного стану в Україні.

В рамках даної роботи були використані наступні **методи дослідження**:

- аналітичний – для комплексного вивчення практичного досвіду та наукових джерел управління ризиками;
- системний підхід – слугував для загального аналізу взаємозв'язку зовнішніх та внутрішніх факторів впливу;
- аналіз та синтез – був доцільним при вивченні теоретичних аспектів досліджуваної проблематики;
- порівняльний метод – для того, щоб зіставити український досвід управління ризиками з міжнародним;
- метод узагальнення – для чіткого формування висновків та рекомендацій за результатами дослідження.

Робота має **теоретичне значення**, адже: систематизує наукові підходи щодо управління ризиками у сфері проєктного менеджменту; максимально розширює уявлення про особливості ризик-менеджменту за умов воєнного стану, що стає новим; створює основу для подальших наукових досліджень у галузях інформаційної безпеки та стійкості бізнесу, а також кризового менеджменту.

**Практичне значення** результатів полягає у тому, що результати можуть бути використані для: покращення політики управління ризиками; розроблення заходів щодо підвищення кадрової безпеки, кіберзахисту та бізнес-безперервності діяльності компанії; створення чітких алгоритмів реагування на непередбачувані ситуації; впровадження системи моніторингу ризиків у реальному режимі. Результати дослідження можуть бути прикладом для інших компаній та державних структур.

**Структура роботи** складається зі вступу, трьох розділів (розділи логічно розділені на дев’ять підпунктів), висновків до кожного розділу, загальних висновків, списку використаних джерел, який складається з 57 найменувань та 6 додатків. Загальний обсяг складає 94 сторінки.

# РОЗДІЛ 1
# ОБҐРУНТУВАННЯ ТЕОРЕТИЧНИХ ВІДОМОСТЕЙ ПРО ПРОЄКТНИЙ МЕНЕДЖМЕНТ

## 1.1. Понятійний апарат та загальна характеристика проєктного менеджменту

Сучасні трансформаційні процеси у економіці та в суспільстві загалом, обумовлюють необхідність щодо пошуку дієвих управлінських інструментів. За умов постійних змін в зовнішньому середовищі, зростання конкуренції та помітної обмеженості ресурсів визначальним стає застосування вдалих підходів до організації діяльності. Одним із таких інструментів постає проєктний менеджмент – теперішня концепція управління, яка дає максимальну можливість впроваджувати ресурси, цілі та технології для досягнення визначального результату діяльності.

Загалом проєктний менеджмент на даний час постійно застосовується у різноманітних сферах – освіті, бізнесі, культурі, державному управлінні, науці, соціальних ініціативах та інших які зараз розвиваються. Його головною перевагою є те, що він забезпечує координацію, контроль та планування всіх етапів діяльності, дозволяючи при цьому уникати ризиків та досягати максимальної ефективності.

Сучасний проєктний менеджмент не лише забезпечує структуровану організацію діяльності, а й активно інтегрує інноваційні технології для оптимізації ресурсів та комунікацій. Завдяки застосуванню цифрових платформ, програмних продуктів для планування та контролю, а також методів гнучкого управління, організації можуть швидше реагувати на зміни у зовнішньому середовищі та ефективніше використовувати людський і фінансовий потенціал. Важливим аспектом стає також інтеграція соціально-етичних та екологічних критеріїв при плануванні та реалізації проєктів, що сприяє сталому розвитку та підвищенню довіри зацікавлених сторін [3, с. 14].

А тому, сучасний проєктний менеджмент виступає не лише як інструмент планування та контролю, а й як комплексна система, яка поєднує інноваційні технології, гнучкі методи управління та соціально-етичні пріоритети, підвищуючи загальну результативність та адаптивність організацій.

Загальне вивчення понятійного апарату та детальної характеристики даного феномену дає можливість зрозуміти всю можливу сутність даної сфери, її основні засади, терміни та етапи, які є потрібними для вдалої реалізації всіх проєктів – від соціального чи виробничого до освітнього проєктів. Саме через призму комплексного вивчення головних понять можна зрозуміти логіку побудови проєкту, фактори, які впливають на успіх, а також механізм його реалізації.

Проєктний менеджмент має певні складові, які нами більш детально та наочно продемонстровано на рисунку 1.1.

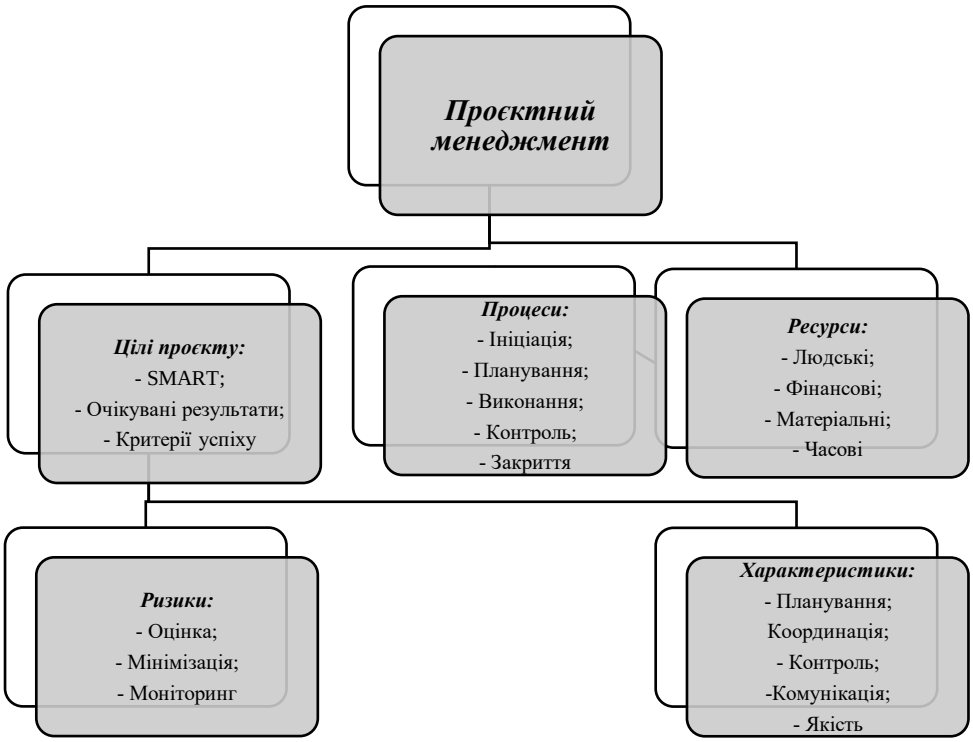



**Рис. 1.1 – Складові проєктного менеджменту [1]**

Як можна побачити з структуризованого та поданого рисунку, проєктний менеджмент передбачає цілі проєкту, демонструє спеціально визначені процеси, залучає потрібні ресурси, має визначальні особливості, і, що важливо, запобігає можливим ризикам, які можуть виникнути під час діяльності щодо реалізації проєктів.

Серед ключових компонентів сучасного проєктного менеджменту можна виділити також інтегровану систему оцінювання ефективності на кожному етапі проєкту, включно з моніторингом витрат, контролем термінів та якісним аналізом результатів. Такий підхід дозволяє керівникам своєчасно виявляти відхилення від плану та оперативно вносити корективи, що значно зменшує ризики та підвищує ймовірність досягнення поставлених цілей. А тому стверджуємо, що структурні складові проєктного менеджменту охоплюють не лише ресурсне забезпечення та планування, а й інтегровані механізми оцінювання, що роблять процес управління більш контрольованим та результативним.

Однак, на початковому етапі нашого дослідження доцільним є визначення його поняття. В сучасній науці та практиці побутує наступне визначення **проєктного менеджменту** – це своєрідна інтегрована управлінська система, що поєднує в собі засади загального менеджменту, спеціалізовані методи управління та міждисциплінарні знання з метою ефективного та вмотивованого використання ресурсів протягом життєвого циклу проєкту для досягнення унікальних, вимірюваних і часово обмежених результатів [3, с. 14]. Вважається, що дана дефініція поняття є найбільш оптимальною, адже враховує головні та важливі характеристики, такі як: результативність, унікальність, часову й ресурсну обмеженість, ризикованість, інноваційність, послідовність та системність.

Однак, це є не єдиним визначенням в літературних джерелах, оскільки проєктний менеджмент має різноманітні трактування в українській науковій літературі. Саме тому, для більшої наочності нами було підібрано найбільш вдалі

трактування серед українських дослідників та розроблено на основі цього таблицю 1.1.

**Таблиця 1.1**

**Трактування поняття «проєктний менеджмент» українськими авторами**

| Автор | Трактування поняття |
|---|---|
| В. Воронкова | розглядає дане поняття як певний вид управлінської діяльності та зорієнтований на створення нового результату діяльності в рамках чітко визначених фінансових та часових рамок [3, с. 14]; |
| М. Козловський | ідентифікує проєктний менеджмент як встановлений комплекс методів та потрібних інструментів для здійснення унікальних завдань, що помітно відрізняє його від звичного управління [20, с. 81]; |
| І. Ткачук | наголошує на стратегічних моментах, оскільки проєктний менеджмент не тільки вирішує виняткові завдання, а і формує довгострокову конкурентоспроможність діючих організацій [46, с. 118]; |
| А. Полянська | максимально уточнює та співвідносить поняття «проєкт» та «міжнародний проєкт», при цьому наголошуючи на важливості класифікаційних ознак та поетапності реалізації [32, с. 21]; |
| Н. Сапич і К. Хамлика | серед головних характеристик виділяють неповторність, плановість, координацію на результат та логічну завершеність [38, с. 453]; |
| Н. Блага | виокремлює відмінність саме між проєктною діяльністю та щоденними операціями, що потребує спеціальних знань та компетенцій [2, с. 152]. |

Отже, різноманітні підходи об’єднує розуміння самого проєктного менеджменту як сукупної управлінської системи, що скоординована на досягнення унікальної цілі за умов певної обмеженості ресурсів та часових рамок.

Виокремивши поняття «проєктний менеджмент» в сучасній літературі, постала доцільність перейти до його характеристики. Саме він має велику кількість особливих рис, які відрізняють його від звичних форм управління, а тому:

1. **Цілеспрямованість та орієнтація на результат**: варто вказати, що всі можливі процеси підпорядковані досягненню конкретної цілі, що має вимірювальні показники [41];
2. **Унікальність:** передбачає, що всі проєкти відрізняються за змістом, масштабом і результатом, що і зумовлює індивідуальний підхід до його належного здійснення [41];
3. **Обмеженість ресурсів:** розуміється, що управління може реалізовуватись в умовах фінансових, матеріальних, людських та часових обмежень [41];
4. **Часові рамки:** вони є особливими, адже життєвий цикл проєкту має конкретно визначений початковий етап та завершальний, що формує чітку логіку управлінських дій [41];
5. **Етапність реалізації:** є одним з найбільш позитивних аспектів, оскільки традиційно містить ініціацію, планування, виконання, моніторинг і завершення [41];
6. **Системність і комплексність:** означає те, що проєктний менеджмент об’єднує стратегічні, операційні та тактичні рішення у одну і цілісну систему управління [41];
7. **Командний підхід:** злагоджена команда – запорука успішності. Тобто успішність напряму залежить від гармонійної роботи команди, дієвих лідерства та комунікацій [41];
8. **Управління ризиками:** є одним з найважливіших, адже проєкт постійно пов’язаний з невизначеністю, тому вагомим є механізм мінімалізації та встановлення можливих ризиків [41];
9. **Інноваційність і креативність:** більша кількість проєктів чітко скоординовані на створення нових (тобто раніше не відомих) та інноваційних

продуктів, послуг чи технологій (або іншого), що підсилює їхню максимальну цінність [41];

10. **Гнучкість та адаптивність:** тобто необхідно акцентувати, що у процесі реалізації проєкти зазвичай потребують корекцій, що потребує швидкої реакції на зміни [41];

11. **Міждисциплінарність:** є важливим аспектом в цій сфері, оскільки проєктний менеджмент поєднує знання з економіки, психології, інженерії, ІТ та соціальних наук, що в поєднанні приводить до вдалого та бажаного результату в самому кінці [41];

12. **Стратегічна значущість:** у великій кількості випадків діяльність ІТ-компаній стає основою для найбільш інноваційного розвитку (як і для організацій яким вони надають послуги, так і для держави в загальному) та посилення її позицій на ринку, якому вона здійснює свою діяльність чи надає послуги [41].

Зважаючи на подане нами вище, сукупність визначальних характеристик таких як: цілеспрямованість та орієнтація на результат, унікальність, обмеженість ресурсів, часові рамки, етапність реалізації, системність і комплексність, командний підхід, управління ризиками, інноваційність і креативність, гнучкість та адаптивність, міждисциплінарність, а також стратегічна значущість – говорить про те, що проєктний менеджмент – це не тільки набір рандомних чи цільових методів, а в більшій мірі комплексна управлінська концепція, котра забезпечує дієве поєднання ресурсів, людського потенціалу та інновацій.

Також виокремимо та більш чітко наголосимо, що проєктний менеджмент вливає звичні управлінські функції у спеціальну логіку проєктної діяльності, зокрема [40, с. 103]:

- планування – визначення чіткої мети, термінів виконання, бюджету та ресурсів;
- організація – формування структури команди та максимально чіткого розподілу ролей;

- мотивація – це належне забезпечення (наприклад: фінансове, технічне, соціальне та інше) залученості всіх членів команди, які потрібні для виконання проєкту;
- контроль та моніторинг – це регулярна оцінка прогресу у виконанні та корекції відхилень, які можуть виникнути під час реалізації запланованого проєкту;
- комунікація – ефективний обмін інформацією між усіма учасниками проєкту.

Наголосимо, що подані аспекти дають змогу продемонструвати, що проєктний менеджмент – це не тільки технологія, злагоджений та чіткий управлінський процес, який потребує ретельного планування, організації та належного контролю.

Таким чином, можемо підбити підсумок за результатами розгляду даного питання, що проєктний менеджмент в теперішньому науковому дискурсі розуміється як своєрідний універсальний інструмент управління з особливими видами діяльності, що має операційне, тактичне та стратегічне значення. Безпосередньо він забезпечує збільшення ефективності діяльності організацій, формує конкурентні переваги та, що важливо, стимулює інноваційний розвиток. А тому, проєктний менеджмент можна ідентифікувати як головну управлінську технологію сучасності, без чого нереальний сталий розвиток бізнесу, державного сектору чи освіти.

## 1.2. Класифікація проєктного менеджменту

Варто вказати для початку, що проєктний менеджмент як сучасна управлінська технологія охоплює організацію, планування реалізацію та контроль унікальних завдань. У різноманітних сферах діяльності, тобто від бізнесу до освітньої чи соціальної галузі, проєкти помітно відрізняються за своїми масштабами, рівнем ризику, тривалістю та методологією управління. Безпосередньо тому значним та визначальним інструментом є його правильна

класифікація. Саме вона дає можливість систематизувати підходи, обирати оптимальні методи реалізації, структурувати управлінські дії, а також передбачати потрібні ресурси та можливі ризики в ході реалізації того чи іншого проєкту [45, с. 16].

Також визначення класифікації допомагає менеджеру проєкту не тільки впорядковувати завдання, а і обирати найкращу методологію, визначити склад команди, рівень необхідної гнучкості планування та структуру контролю. Саме вона формує своєрідну основу для ефективного управління різноманітного типу проєктами, що в результаті дає можливість отримувати максимально швидко та ефективно позитивний результат діяльності [45, с. 18].

Саме тому, на основі досліджених класифікацій у сучасній літературі, ми структуризували та схематично показали класифікацію проєктного менеджменту, з метою подальшої комплексної характеристики кожного виокремленого компоненту (рисунок 1.2).

Для ефективного управління проєктами необхідно не лише знати загальні принципи проєктного менеджменту, а й мати чітке уявлення про різновиди проєктів, що безпосередньо впливає на прийняття управлінських рішень, розподіл ресурсів та методи контролю. Класифікація проєктів дає змогу систематизувати їх за рядом характеристик, враховуючи специфіку завдань, рівень складності, масштаб та сферу застосування. Завдяки цьому менеджер може визначати оптимальний підхід до реалізації кожного проєкту, правильно організовувати команду, передбачати потребу у фінансових та людських ресурсах, а також оцінювати потенційні ризики на різних етапах.

Крім того, класифікація дозволяє інтегрувати методології управління відповідно до масштабу та тривалості проєктів. Наприклад, малі та короткострокові проєкти часто ефективніше реалізуються за допомогою класичних методів, тоді як великі, довгострокові та інноваційні ініціативи потребують гнучких або гібридних підходів, здатних адаптуватися до змін у середовищі та забезпечувати швидке прийняття рішень.

Також важливо враховувати міждисциплінарність проєктів, оскільки різні сфери (IT, будівництво, освіта, соціальні ініціативи) мають свої специфічні вимоги до ресурсів, технологій та компетенцій учасників. У комплексі, класифікація проєктного менеджменту дозволяє розробляти проєктні плани, які поєднують стратегічні, тактичні та операційні аспекти діяльності, забезпечують системність та передбачуваність реалізації, а також підвищують якість контролю та оцінки результатів.

Зважаючи на це, класифікація проєктів є не просто інструментом для систематизації, а й важливим елементом ефективного управління, що впливає на швидкість виконання завдань, адекватність використання ресурсів та оптимізацію процесів прийняття рішень у межах проєктної діяльності. Вона створює підґрунтя для комплексного, інтегрованого та адаптивного підходу до реалізації проєктів будь-якого типу.

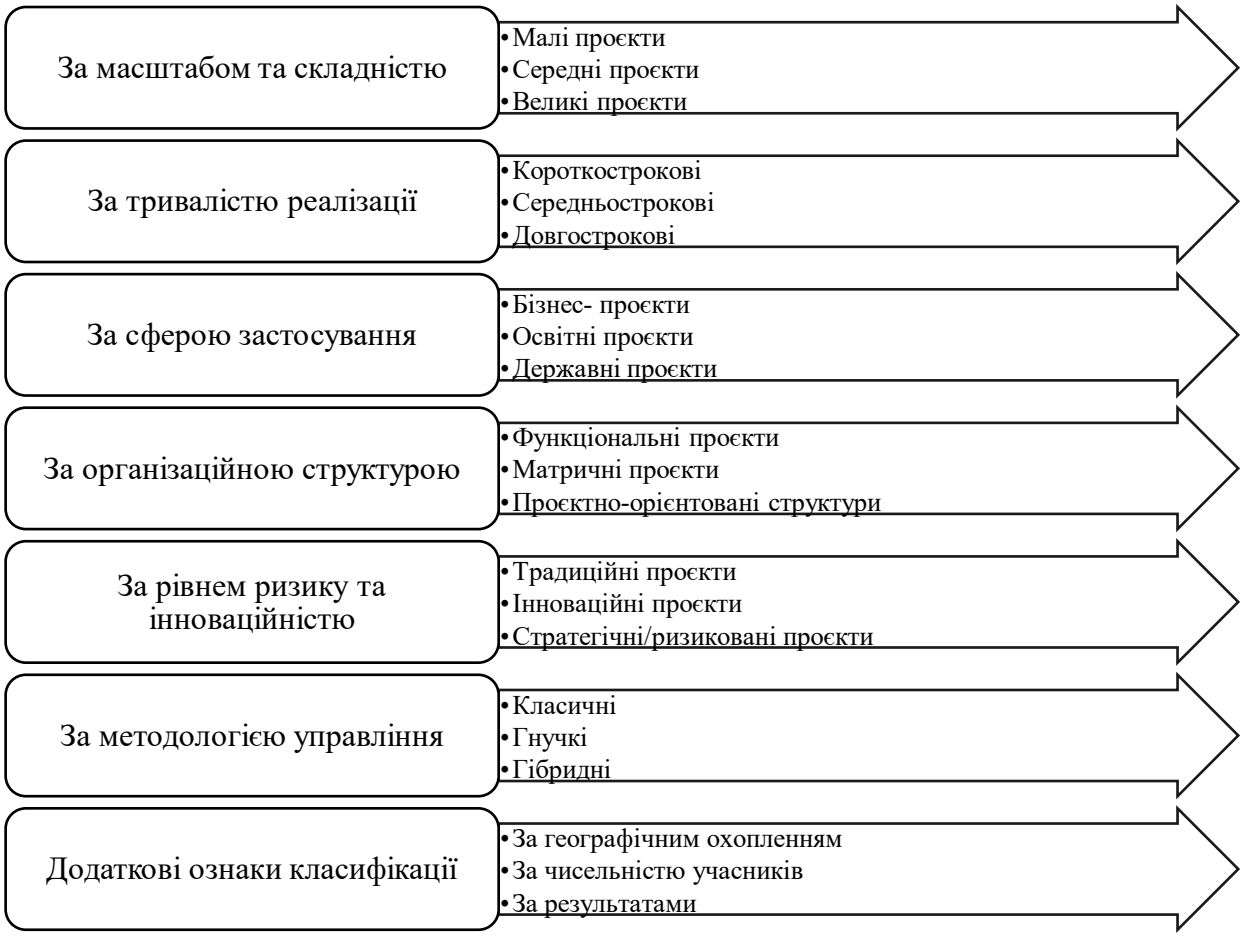



**Рис. 1.2 – Класифікація проєктного менеджменту [46]**

Подавши класифікацію проєктного менеджменту охарактеризуємо кожен елемент більш детально [46]:

1. **За масштабом і складністю бувають наступні [46, с. 118]:**

- малі проєкти – за загальним правилом вони обмежені бюджетними коштами, ресурсами та кількістю учасників, виконуються виключно однією командою;
- середні проєкти – потребують щоб в ньому брали участь декілька підрозділів, середні за своєю тривалістю та бюджетними коштами, а також потребують координації;
- великі проєкти – вони є стратегічними та з великими масштабами, зі значними фінансовими ресурсами та довгим циклом. Включають у себе мультидисциплінарні команди та досить складні системи управління, що і зумовлює його складність.

Загалом, можемо констатувати, що сам масштаб проєкту і визначає організаційні підходи, саму структуру управління та загальний рівень координації в процесі виконання.

2. **За тривалістю реалізації проєкту [46, с. 119]:**

- короткострокові – тривають до шести місяців та направлені на вирішення локальних завдань;
- середньострокові – тривають від шести до двадцяти чотирьох місяців, в ході реалізації потребують проміжного контролю, а також максимально чіткої координації;
- довгострокові – тривають більше як два роки, вони є більш стратегічними, з досить високим рівнем ризиків та невизначеності, що потребує більше ресурсів.

Можемо стверджувати наступне: загальна тривалість проєкту визначає вибір методології управління, особливості та характер ризиків та систему контролю.

3. **За сферою застосування виокремлюють [46, с. 119]:**

- бізнес-проєкти – передбачають комплексну розробку послуг, продуктів, корпоративні чи маркетингові програми;
- інженерні та будівельні – передбачають спорудження інфраструктури чи окремих об’єктів;
- ІТ-проєкти – є особливим видом, оскільки передбачає створення потрібного програмного забезпечення, а також впровадження інформаційних систем;
- освітні та соціальні – такі проєкти передбачені для розвитку територіальних громад, навчальних програм та всіх можливих культурних ініціатив;
- міжнародні та державні – іншими словами, це максимально масштабні програми, які відбуваються на регіональному або на більш глобальному рівнях та потребують більш кваліфікованих спеціалістів.

Отже, сфера застосування проєктного менеджменту визначає специфіку та особливості цілей і кінцевих результатів, а також має безпосередній вплив на методи управління.

4. **За організаційною структурою бувають [46, с. 120]:**

- функціональні проєкти – призначені для того, щоб виконуватись в рамках конкретного підрозділу, а також, що важливо, мають обмежену взаємодію з іншими;
- матричні проєкти – характеризуються тим, що формуються з учасників різних підрозділів, в основному потребують узгодження влади між проєктними і функціональними керівниками;
- проєктно-орієнтовані структури – сама організація в повній мірі орієнтована на реалізацію проєктів, а усі можливі ресурси призначені для цього завдання.

За загальним правилом, саме організаційна структура в проєктному менеджменті є однією з найбільш важливих та максимально визначає дієвість використання необхідних ресурсів та швидкість ухвалення важливих управлінських рішень.

5. **За рівнем ризику та інноваційності [46, с. 120]:**

- традиційні проєкти – вони в основному є передбачуваними, мають мінімальний ризик та використовують в ході його виконання всім відомі технології;
- інноваційні проєкти – за загальним правилом є скоординованими на більш новітні та нестандартні рішення, а також характеризуються підвищеною невизначеністю;
- стратегічні чи ризиковані – це такі проєкти, які можуть помітно та суттєво вплинути на розвиток галузі чи організації, а також потребують максимально ретельного моніторингу.

Таким чином, рівень ризику та інноваційність суттєво впливає на методи контролю, потребу в додаткових ресурсах та саме гнучкість планування проєктного менеджменту.

6. **За методологією управління [46, с. 121]:**

- класичні (Waterfall) – передбачає лінійне виконання всіх етапів, чітке планування кожного моменту, а також фіксовані терміни в які потрібно вкластися;
- гнучкі (Agile, Scrum, Kanban) – максимальна адаптація до змін та можливе гнучке планування;
- гібридні – поєднують в собі два попередні – гнучкий та класичний підходи, забезпечуючи при цьому чіткий баланс щодо адаптивності та стабільності.

Отже, сама методологія управління ідентифікує стиль роботи конкретної команди, швидкість реагування на будь-які ситуації, які стосуються змін та на якість контролю.

7. **Додаткові ознаки класифікації [46, с. 121]:**

- за географічним охопленням – бувають локальні (здійснюються в рамках однієї установи чи організації), регіональні (здійснюються між різними регіонами чи областями), міжнародні (реалізовуються в межах двох і більше країн);

- за чисельністю учасників – індивідуальні (скоординовані на один чіткій аспект), групові (зорієнтовані на цільове виконання двох чи чотирьох аспектів), корпоративні (направлені на виконання всіх важливих завдань цілої великої корпорації);
- за результатами – продуктові (створення нових та інноваційних продуктів), процесні (результативна оптимізація процесів), послугові (впровадження сервісів).

Загалом, класифікація проєктів дає змогу застосовувати комбіновані підходи. Прикладом цього можуть бути гібридні методології у великих міжнародних інноваційних проєктах. Також класифікація допомагає передбачати взаємозв'язок ресурсів та ризиків, що необхідно для ефективного управління людьми і бюджетом. Одночасно класифікація забезпечує системний підхід, оскільки різні параметри (сфера, тривалість чи масштаб) взаємопов'язані та визначають стратегію управління.

Зважаючи на подану класифікацію можна зробити наступні узагальнення: класифікація проєктного менеджменту є головним інструментом постійної проєктної діяльності. Вона дає змогу: визначати складність та масштабність проєкту, формувати найбільш оптимальну структуру управління, планувати необхідні ресурси та прогнозувати можливі ризики, обирати найбільш дієву методологію для реалізації, а також забезпечувати досягнення тактичної та стратегічної мети. Отже, сама класифікація проєктів формує підґрунтя системного підходу до самого управління та робить процес реалізації проєктів передбачуваним, результативним та контрольованим.

### 1.3. Основні етапи управління в проєктному менеджменті

Проєктний менеджмент на даний момент постає не тільки як метод організації роботи, а і як комплексна система управління, яка дає можливість дієво здійснювати завдання різного рівня складності. Успіх будь-якого проєкту залежить напряму від уміння правильно визначати послідовність всіх дій,

зосередженості на найбільш визначальних аспектах та уникнення помилок, особливо на ранніх стадіях. А тому практики та науковці приділяють значну увагу дослідженню етапності управління проєктами, оскільки чітке структурування процесу дає можливість досягти бажаних результатів із найменшими втратами зусиль, ресурсів та часу.

Розглядаючи управління проєктами як поетапний процес, потрібно зупинитись на основних складових даного механізму, оскільки кожен з етапів виконує власну функцію, проте, одночасно, є невіддільною ланкою однієї системи. Послідовний аналіз головних етапів дасть змогу більш повно та досконало зрозуміти особливості та логіку проєктного менеджменту(рисунок 1.3).

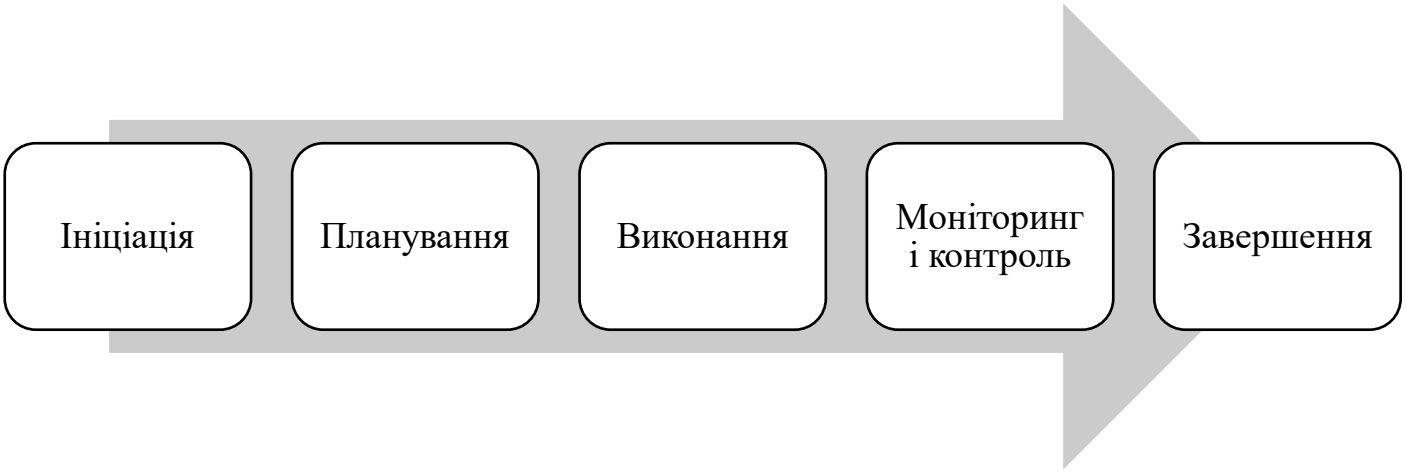



**Рис. 1.3 – Основні етапи управління в проєктному менеджменті [3]**

Показавши схематично основні етапи, постає доцільність їх більш детально охарактеризувати та виокремити головні моменти, що важливо для комплексного висвітлення цієї теми роботи:

1. **Ініціація проєкту** містить наступні логічно пов’язані між собою складові [3, с. 13]:

- формування самої ідеї та ідентифікація проблематики, яку потрібно вирішити належним чином;

- трактування актуальності проєкту та його соціальні і економічні цінності;
- визначення конкретної мети, потрібних завдань та бажаних результатів від проєкту;
- попередня оцінка всіх наявних ресурсів, термінів виконання та можливих ризиків;
- прийняття відповідного рішення про початок виконання проєкту, який вже заплановано.

Отже, можемо узагальнити, що ініціація є точкою відліку всього проєкту, оскільки безпосередньо тут визначається його потрібність та можливість реалізації в подальшому.

2. **Планування проєкту передбачає наступні компоненти [3, с. 14]:**

- розроблення та формування деталізованого плану дій та показників ефективності;
- побудова максимально логічної структури робіт (Work Breakdown Structure);
- визначення термінів виконання та послідовність всіх завдань, що важливо для успіху;
- оптимальний розподіл потрібних ресурсів, тобто: матеріальних, людських та фінансових;
- складання бюджету на період реалізації, тобто від початкового до кінцевого етапу;
- аналіз всіх можливих ризиків та визначення оптимальних механізмів для їх мінімізації.

Можна узагальнити, що саме планування створює підґрунтя для того, щоб організувати всю можливу діяльність та забезпечує скоординованість роботи всієї команди.

3. **Виконання (або реалізація) проєкту [3, с. 15]:**

- поступова та ретельна реалізація всіх запланованих завдань в рамках проєкту;

- максимальна координація здійснюваної діяльності всіх залучених учасників проєкту;
- цільове використання всіх ресурсів у відповідності до затвердженого бюджету;
- забезпечення якісного виконання робіт, які передбачені планом реалізації проєкту;
- поточне управління всіма можливими ризиками в рамках виконуваного проєкту.

Зважаючи виокремлені етапи виконання, можемо констатувати, що воно є найбільш інтенсивним етапом, де стається втілення початкового задуму та перевірка ефективності планування.

4. **Моніторинг та контроль за виконанням [3, с. 16]:**

- постійний збір та повний аналіз інформації щодо перебігу всіх робіт в рамках запланованого проєкту;
- виявлення всіх відхилень від плану та встановлення причин цих відхилень;
- коригування в ході виконання завдань та ресурсів в межах конкретного проєкту;
- забезпечення прозорої звітності;
- підтримка балансу між вартістю, якістю та часом.

А тому, можемо констатувати, що контроль та моніторинг дають можливість уникати зривів термінів виконання та забезпечують стабільний та безперервний розвиток проєкту.

5. **Завершення реалізації проєкту [3, с. 17]:**

- формальне закриття робіт;
- різностороння оцінка всіх досягнутих результатів, які досягнуто в ході реалізації проєкту;
- порівняння фактично отриманих показників із запланованими на початку проєкту;

- аналіз здобутого досвіду під час проєкту, фіксація допущених помилок та позитивних практик;
- передача результатів проєкту замовнику чи потрібним користувачам, тобто досягнення кінцевого результату.

Отже, сам завершальний етап формує кінцеву оцінку всієї ефективності та, свого роду, підґрунтя для реалізації нових проєктів в подальшому на більш високому рівні.

Також важливо відзначити, що деякі сучасні проєкти можуть передбачати паралельне виконання кількох етапів (інкрементальний підхід), що допомагає швидко отримувати проміжні результати. Використання цифрових інструментів для управління проєктами (MS Project, Jira, Trello) забезпечує ефективний контроль та прозорість виконання. Вагомим аспектом є адаптивність та гнучкість команди, оскільки навіть детально спланований проєкт потребує швидкого реагування на внутрішні та зовнішні зміни [4, с. 27].

Сучасна практика проєктного менеджменту дедалі більше орієнтується на гібридні моделі, що поєднують елементи класичного каскадного планування та гнучких методологій. Це дає змогу підвищити адаптивність команди, зменшити затримки та швидше тестувати проміжні результати. Значну роль відіграє управління зацікавленими сторонами: регулярні комунікації, прогнозування очікувань та формування спільного бачення проєкту. Саме ці чинники часто визначають не лише швидкість реалізації, а й загальний рівень підтримки проєкту та якість кінцевих рішень. Крім того, сучасні стандарти, такі як PMBOK 7 та PRINCE2, акцентують увагу на принциповості проєктних підходів – фокусі на цінності, гнучкості, стійкості системи управління та прозорості командної взаємодії [4, с. 28].

Таким чином, проаналізувавши етапи управління в проєктному менеджменті, можемо констатувати, що управління проєктом є багатоступеневим процесом, який складається з ініціації, планування, виконання, контролю та завершення. Кожен з проаналізованих нами етапів має

своє функціональне навантаження, однак всі вони між собою є взаємопов’язаними, і в результаті, формують єдину та логічну систему.

Сам успіх будь-якого проєкту залежить від того наскільки є узгодженість та ефективність виконання кожної стадії, а також, що важливо, від здатності команди своєчасно та правильно реагувати на зміни чи негативні відхилення. А тому, поетапність та дотримання всіх передбачених аспектів виступає гарантом системності, керованості та результативності сучасного проєктного менеджменту. Зважаючи на все, можемо сказати, що дослідження даного питання в межах теми буде доцільним для висвітлення практичних аспектів в подальшому.

**Висновок до розділу 1**

Досліджений теоретичний розділ підтверджує, що проєктний менеджмент є комплексною управлінською системою, яка поєднує тактичні, стратегічні та операційні підходи для помітного досягнення виняткових результатів у межах обмежених часових рамок та ресурсів. Понятійний апарат даного феномену містить наступні визначальні характеристики: цілеспрямованість, унікальність, обмеженість ресурсів, часові рамки, етапність реалізації, системність і комплексність, командний підхід, управління ризиками, інноваційність і креативність, гнучкість та адаптивність, міждисциплінарність, а також стратегічну значущість. Безпосередньо дані характеристики відрізняють проєктну діяльність від традиційних форм управління та забезпечують досягнення результатів у різних галузях: соціальних ініціатив, IT-освіти, бізнесу, міжнародних проєктів та державного управління.

Класифікація проєктного менеджменту за тривалість, масштабом, організаційною структурою, сферою застосування, інноваційності та рівнем ризику, методологією управління та факультативними ознаками забезпечує системний підхід до управління. Вона дає можливість точно визначати методологією реалізації, склад команди, розподіл ресурсів та способи контролю, рівень гнучкості планування, що є надзвичайно важливим для ефективного управління масштабними та складними проєктами. Класифікація одночасно створює підґрунтя для застосування гібридних та компінованих підходів, особливо у інноваційних та міжнародних проєктах, забезпечуючи при цьому оптимізацію ресурсів та прогнозування ризиків.

Визначальним елементом проєктного менеджменту є поетапне управління, яке складається з наступних стадій: ініціація, планування, виконання, моніторинг та контроль, а також завершення. Всі етапи виконують власну функцію, однак вони є взаємопов’язаними та формують одну логічну систему. Дотримання структурованості та послідовності цих етапів дає можливість зменшувати ризиками, забезпечувати якість результатів, оптимізувати витрати

ресурсів та своєчасну реалізацію цілей. Сучасні практики передбачають використання інкрементального підходу, паралельне виконання етапів, цифрових інструментів управління (MS Project, Jira, Trello) та помітний рівень адаптивності команди, що дає змогу швидко реагувати на зміни зовнішнього та внутрішнього середовища.

Таким чином, загальне дослідження понятійного апарату, класифікації та етапів управління показує, що проєктний менеджмент постає універсальним інструментом для організації ефективної діяльності організацій всіх сфер. Саме він забезпечує керованість, системність, передбачуваність та результативність процесу реалізації проєктів, сприяє інноваційному розвитку, формує конкурентні переваги та основною управлінською технологією сучасності.

# РОЗДІЛ 2
# СПЕЦИФІКА УПРАВЛІННЯ РИЗИКАМИ НА ПРИКЛАДІ «УКРАЇНСЬКІ ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ»

## 2.1. Загальна характеристика та правові засади діяльності компанії «Українські інформаційні технології»

Сучасний ІТ-сектор нашої країни належить до найбільш динамічних галузей економіки, який формує суттєву частку експорту та створює для фахівців високотехнологічні робочі місця. За такого роду умов передового значення набувають компанії, які поєднують у своїй діяльності такі аспекти, як: інноваційність, фінансову стабільність та максимально чітке дотримання всіх можливих вимог законодавства у відповідності до особливостей здійснюваної діяльності.

Однією з таких є Товариство з обмеженою відповідальністю «Українські інформаційні технології» (скороченою назвою компанії є ТОВ «УІТ») [57], що більше двадцяти років реалізовує діяльність у сфері програмування та інформатизації на високому рівні, а тому показує чудові результати. А тому, щоб зрозуміти місце даної компанії на ринку та можливі подальші перспективи в її діяльності, доцільно розглянути її організаційну структуру, напрями та масштаби здійснюваної діяльності, а також правові засади функціонування на ринку.

Розпочнемо з загальних відомостей про дану компанію: повне найменування цієї компанії ТОВ «Українські інформаційні технології». Заснована вона у 2003 році та знаходиться на даний момент офіс у місті Львів. Керівником є Плакущенко Володимир Володимирович. Важливо, що статутний капітал є досить великим та становить 5 мільйонів гривень. На даний час там працює понад 400 осіб. Згідно поданої звітності за результатами діяльності у 2024 році чистий дохід компанії становить 461 742 млн грн, а чистий прибуток – 31 085 млн грн [57].

Також компанія має певну власність, зокрема: до структури входить «SoftServe, Inc.» (США), що свідчить про міжнародну інтеграцію. Також для максимально повної характеристики, вбачаємо за доцільне в таблиці 2.1 висвітлити напрями діяльності цієї компанії.

**Таблиця 2.1**

**Основні напрями діяльності ТОВ «Українські інформаційні технології» [57]**

| КВЕД | Вид діяльності |
|---|---|
| 62.01 | Комп'ютерне програмування |
| 58.21;58.29 | Видання програмного забезпечення |
| 62.02 | Консультування з питань інформатизації |
| 63.11 | Обробка даних і хостинг |
| 62.09 | Діяльність у сфері IT та комп'ютерних систем |
| 68.20 | Оренда нерухомості |

Окремої та особливої уваги заслуговує стратегічна орієнтація ТОВ «Українські інформаційні технології», оскільки компанія активно використовує модель стійкого організаційного розвитку, що поєднує інноваційність, цифрову трансформацію та клієнтоцентричний підхід. На відміну від багатьох IT-компаній регіону, ТОВ «Українські інформаційні технології» розвиває багаторівневу систему внутрішнього комплаєнсу, включно з політиками кіберзахисту, управління конфіденційною інформацією та дотриманням міжнародних стандартів безпеки (ISO/IEC 27001, GDPR-орієнтовані практики). Керівництво компанії вибудовує роботу на принципах прозорості, корпоративної відповідальності та інституційної надійності, що позитивно впливає на її імідж і довіру партнерів. Такий стратегічний підхід не лише зміцнює позиції компанії на внутрішньому ринку, але й забезпечує можливість ефективної інтеграції у глобальне IT-середовище.

Виокремивши загальні відомості, можемо чітко сказати, що ТОВ «Українські інформаційні технології» – це стабільна компанія, яка здійснює

діяльність середнього масштабу та поєднує локальну українську ідентичність з міжнародними практиками ведення бізнесу. Саме вона пропонує широке портфоліо IT-послуг та забезпечує працевлаштування та гідну оплату праці сотням львівських фахівців, підтримуючи розвиток українського цифрового середовища на належному рівні.

Ця компанія має певні можливості [57]:

1. **Програмне забезпечення**: дана компанія влучно інтегрує і на високому рівні розробляє програмне забезпечення на замовлення: тобто починаючи від звичайних додатків до непростих корпоративних систем. Послуги компанії включають архітектуру, аналіз вимог, тестування, розробку, впровадження та супровід. Прикладом є впровадження систем обліку, ERP-рішень, CRM-систем;

2. **Хмарні технології:** досліджуваною компанією пропонуються рішення з використанням хмарних сховищ: IaaS, PaaS, SaaS. Дана компанія допомагає всім її клієнтам переходити до хмари, оптимізувати інфраструктуру, використовувати хмарні сервіси для зберігання, обробки даних та запуску додатків;

3. **Cloud Migration and Modernization:** міграція наявних систем у хмару або legacy-інфраструктури – планування міграції, аналіз, оптимізація архітектури, налаштування хмарних сховищ, а також забезпечення масштабності та гнучкості;

4. **Великі дані та аналітика:** рішення обробки, збору та аналізу великих обсягів даних – побудова data-lake, data-warehouse, аналітичні платформи, дашборди, машинне навчання (ML) для прогнозів, оптимізацій та інсайтів бізнесу;

5. **Штучний інтелект:** активне впровадження систем штучного інтелекту – обробка комп’ютерного зору, природної мови, автоматизація процесів на базі AI-алгоритмів та автоматизація процесів;

6. **Генеративний ШІ:** застосування генеративних моделей у бізнес-процесах – створення контенту, автоматизація творчих завдань, інтерактивні чат-боти, персоналізація сервісів та цифрові асистенти;

7. **Інтернет речей:** детальна розробка та цільове впровадження інтернет речей – підключені сенсори, пристрої та обробка даних з «речей», управління смарт-об’єктами, промисловий IoT (IIoT) для покращення виробництва чи логістики;

8. **Сервісний дизайн:** проєктування та покращення цифрових сервісів – UX/UI-дизайн, створення зручного сервісного досвіду, дослідження користувачів, оптимізація взаємодії користувачів із системою та design thinking методики;

9. **Cloud Security and Compliance**: забезпечення відповідності нормативам та безпеки хмарної інфраструктури – сертифікація, аудити, контроль доступу, шифрування, політики безпеки та відповідність GDPR/ISO/ДСТУ і інше;

10. **Цифрові платформи:** чітке створення та впровадження платформ для громадських організацій та бізнесу – багатокористувацькі системи, інтеграція сервісів, маркетплейси, API та екосистеми сервісів;

11. **Розширена реальність:** розробка AR-додатків, маркетингу, інтерактивних рішень для навчання, промисловості – візуалізації, змішана реальність та інтерактивні демонстрації;

12. **Розробка та дослідження:** цільове проведення R&D-активностей – розробка прототипів, патентування, випробовування нових технологій, інноваційні лабораторії, а також співпраця з дослідницькими центрами та співпраця;

13. **Робототехніка:** чітке впровадження робото-технічних рішень – автоматизовані системи управління, роботи-асистенти, інтеграція з IoT, AI, системи контролю за виробництвом;

14. **Інновації та цифрова стратегія:** консалдинг у сфері цифрових змін – оцінка цифрової зрілості організації, розробка цифрової стратегії, виявлення інноваційних підходів та бізнес-моделей;

15. **Операційна ефективність:** автоматизація можливих процесів, скорочення витрат де це можливо, автоматизація, підвищення продуктивності праці – застосування цифрових рішень, Lean, Six Sigma у поєднанні з IT-інструментами;

16. **Керування організаційними змінами:** належне супроводження змін які виникають у організації в ході цифрових змін, тобто це – зміна культури, відповідна підтримка персоналу, комунікація, навчання, управління опором змінам;

17. **Доступність:** тут розуміється на належному рівні проєктування допустимих цифрових рішень – іншими словами дотримання стандартів доступності (WCAG, ДСТУ), створення сервісів для людей з інвалідністю, універсальний дизайн;

18. **ESG та послуги зі сталого розвитку:** впровадження найбільш важливих соціальних, екологічних та управлінських ініціатив – IT-інфраструктура, цифрові рішення для сталого розвитку, енергоефективність та звітність за ESG;

19. **Квантові обчислення:** підготовка та дослідження до використання квантових обчислень – симуляції, експериментальні проєкти, аналіз потенціалу квантових технологій для бізнесу;

20. **Цифрові сервіси та продукти:** компанія створює нові цифрові продукти – веб та мобільні додатки, екосистеми, маркет-плейси, цифрові моделі бізнесу та SaaS-сервіси.

Для ТОВ «Українські інформаційні технології» притаманні наступні індустрії: роздрібна торгівля, фінансові послуги, консалтингові і інженерні послуги, охорона здоров’я, освіта, програмне забезпечення, ланцюг постачання, гірництво та металургія, Energy, нафта і газ, автомобільна промисловість, виробництво та сільське господарство [57].

Окрім загальних характеристик досліджуваної компанії, доцільним є висвітлення її правових засад діяльності [57]:

1. Організаційно-правова форма: ТОВ – це юридична особа, яка функціонує на базі власного статут; також відповідальність учасників обмежується їх внесками;

2. Законодавче регулювання є досить широким, оскільки діяльність цієї компанії регламентується Цивільним кодексом України [50], а також спеціальними законами:

- «Про інформацію» [36];
- «Про захист інформації в інформаційно-комунікаційних системах» [35];
- «Про електронні комунікації» [34];
- «Про державну реєстрацію юридичних осіб та фізичних осіб підприємців» [33].

3. Ліцензійні умови: тобто своєрідний дозвіл головних напрямів діяльності досліджуваного підприємства ТОВ «Українські інформаційні технології» (програмування, консалтинг чи обробка даних) ліцензування не є обов’язковим;

4. Податковий статус: досліджувана нами компанія здійснює свою основну роботу на загальній системі оподаткування, є платником податку на прибуток і ПДВ, що є стандартом для легальної реалізації передбачуваної діяльності;

5. Фінансова прозорість і відповідальність: компанія повинна подавати фінансову звітність, вести бухгалтерський облік та дотримуватись норм чинного податкового законодавства.

У даній роботі основний акцент ставилось на дослідженні системи ризик-менеджменту компанії ТОВ «Українські інформаційні технології». На ринку вона представлена через велику кількість юридичних осіб, проте найбільш відома під брендом SoftServe [57]. Компанія налічує близько 7400 працівників, працює вже понад 20 років, має широку мережу офісів і є міжнародною за

структурою та діяльністю. Це робить її хорошим об’єктом дослідження, адже вона активно використовує найкращі міжнародні практики у сфері управління ризиками [57].

Можемо наголосити на наступному: структурна організація дає змогу ТОВ «Українські інформаційні технології» гармонійно поєднувати стабільність та гнучкість; фінансові показники підтверджують її дієвість та конкурентоспроможність; нормативно-правова база гарантує легальність їх діяльності та захищеність партнерів та працівників; міжнародний капітал (має прямий зв’язок із SoftServe, Inc.) забезпечує доступ до передових світових практик.

Таким чином, можемо узагальнити, що компанія «Українські інформаційні технології» є легальною та стабільною ІТ-компанією, яка поєднує в собі багаторічний досвід, кваліфікований кадровий потенціал та сучасні технологічні рішення. Вона здійснює свою діяльність у межах чинного законодавства нашої держави, показує фінансову стабільність та робить вагомий внесок української цифрової економіки. Завдяки прозорості своєї діяльності та інтеграції в міжнародний ринок компанія залишається вагомим учасником вітчизняного ІТ-сектору.

## 2.2. Основні способи управління ризиками в компанії «Українські інформаційні технології»

За загальним правилом ІТ-компанії працюють у динамічному середовищі, де загрози можуть виникати з різних сторін, як із політичної, так і з економічної чи технічної. Для компанії «Українські інформаційні технології» управління ризиками – це один з головних елементів стабільного розвитку та функціонування вже багато років.

Дана компанія розробила власну систему управління ризиками, яка ґрунтується на прийнятих міжнародних стандартах та практичних механізмах, які перевірені багаторічним досвідом. За умов швидкого розвитку цифрових

технологій та нестабільного ринкового середовища управління ризиками для компанії є потрібною умовою збереження конкурентоспроможності та своєрідної стабільності (рисунок 2.1).


**Рис. 2.1 – Основні способи управління ризиками компанії «Українські інформаційні технології» [57]**

Важливо зазначити, що в ТОВ «Українські інформаційні технології» сформована не лише формальна система ризик-менеджменту, а й усталена корпоративна культура управління ризиками, яка проявляється у високому рівні обізнаності працівників та їх готовності оперативно реагувати на загрози. Компанія приділяє особливу увагу інтеграції процесів оцінювання та контролю ризиків у щоденну операційну діяльність: від планування проєктів до супроводу клієнтів та технічної підтримки. Такий підхід створює стійку модель організаційної поведінки, у межах якої ризики сприймаються не лише як потенційні небезпеки, а й як можливості для вдосконалення внутрішніх процедур та підвищення стандартів роботи. У результаті формується гнучка система, що забезпечує оперативне прийняття рішень, адаптацію до мінливих умов ринку та збереження стабільності навіть у ситуаціях високої невизначеності.

Для комплексного висвітлення основної проблематики, ми проаналізували систему ризик-менеджменту даної компанії на всіх рівнях, тобто від конкретного

проєкту до зовнішнього середовища. Аналізуючи цей аспект було виокремлено наступні рівні:

- 1-ий рівень – це проєкт;
- 2-ий рівень – це департамент (акаунт або юніт);
- 3-ий рівень – загальнокомпанійський;
- 4-ий рівень – зовнішнє середовище.

Однак в процесі дослідження було вирішено візуалізувати систему управління ризиками в досліджуваній компанії для більшої наочності та розуміння.

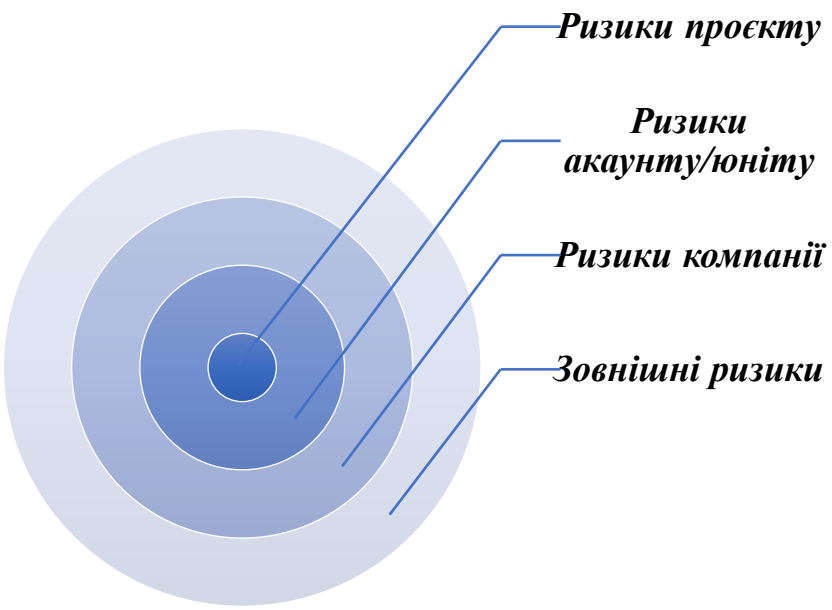



**Рис. 2.2 – Система управління ризиками компанією «Українські інформаційні технології»**

*Джерело: розроблено автором*

Уточнимо що: ризики проєкту виникають на рівні конкретної команди чи проєкту; ризики акаунту/юніту передбачають рівень програми чи портфоліо проєктів окремого департаменту; ризики компанії – це бізнесові ризики; а от зовнішні ризики – це макроекономічні політичні та військові фактори.

Попри те, що загальні принципи ризик-менеджменту однакові на всіх рівнях, кожен із них має свою специфіку. Компанія є проєктно-орієнтованою, тобто основна операційна діяльність – це реалізація проєктів. Відповідно, ризик-менеджмент є ключовим елементом її роботи, оскільки саме ефективне управління ризиками безпосередньо впливає на прибутковість.

Також було виокремлено шість головних способів управління ризиками в компанії «Українські інформаційні технології», для максимального їх розуміння нижче ми більш детально їх охарактеризуємо:

1. **Уникнення ризиків** – це превентивний підхід, коли конкретна компанія відмовляється від підозрілих чи небезпечних партнерів чи проєктів. Дана компанія уникає участі проєктах, котрі мають надто високий рівень наступних загроз: не співпрацює з ненадійними контрагентами, не виходить на ринки з нестабільними умовами, відмовляється від сумнівних угод, де відсутні юридичні гарантії.

Отже, такий метод дає можливість захистити компанію «Українські інформаційні технології» від критичних загроз ще до того як вони виникли чи могли виникнути.

2. **Зниження ризиків** – це є найбільш поширеним способом, який включає в себе: використання хмарних сховищ та резервне копіювання даних, впровадження систем кіберзахисту (firewall, антивіруси, шифрування), регулярне тестування програмного забезпечення, контроль якості на всіх етапах коли створюється продукт. Ця компанія активно постійно та активно застосовує технічні та організаційні заходи, щоб зменшити імовірність чи вплив негативних подій. Даний підхід підвищує якість продуктів та знижує до мінімуму ризики збоїв.

3. **Перенесення ризиків** – це коли частина ризиків передається іншим структурам чи партнерам: страхування кіберризиків та майна, передача дата-центрових та хостингових послуг на аутсорсинг, а також залучення спеціальних юридичних компаній для того, щоб перевіряти контракти. Ця розкрита нами

стратегія зменшує фінансові витрати у випадку виникнення непередбачуваних ситуацій.

4. **Прийняття ризиків** – якщо витратити на їх усунення перевищують можливі збитки, компанія приймає ризики: коливання валютних курсів, дрібні затримки в реалізації проєктів, незначні зміни вимог клієнтів. Досліджувана нами компанія в повній мірі усвідомлено приймає незначні ризики, якщо їх вплив виправданий з економічної сторони. Такий аспект дає повну можливість оптимізувати витрати, при цьому не перевищуючи передбачену систему контролю.

5. **Диверсифікація** – досліджувана компанія «Українські інформаційні технології» на даний час веде різноманітні види діяльності: адміністрування і хостинг, програмування та консалтинг, оренда своєї нерухомості та видавництво електронних ресурсів. Такий аспект помітно зменшує залежність від одного ринку чи продукту й підвищує стійкість компанії. Правильний розподіл діяльності на кілька напрямів знижує залежність від одного сегмента ринку. Отже, навіть у ризикових умовах ця компанія зберігає на достатньому рівні фінансову стійкість.

6. **Контроль та моніторинг:** постійний та своєчасний контроль дає змогу своєчасно виявити допущені відхилення в ході роботи та належним чином реагувати на них: внутрішні аудити проєктів, аналітика ринку, моніторинг кіберзагроз, система KPI для працівників. Варто вказати, що постійне спостереження за зовнішніми та внутрішніми факторами допомагає своєчасно реагувати на виклики. Даний підхід забезпечує стратегічну гнучкість та адаптивність.

Охарактеризувавши головні способи управління ризиками в компанії «Українські інформаційні технології», ми наведемо приклади для кожного, які подамо в таблиці 2.2.

**Таблиця 2.2**

**Приклади способів управління ризиками в компанії «Українські інформаційні технології» [57]**

| Спосіб | Приклад |
|---|---|
| Уникнення | - у ході відбору партнерів застосовується попередній аудит юридичної та фінансової відповідальності;<br>- комплексна перевірка підрядників, уникнення роботи в регіонах з високо економічною чи політичною нестабільністю. |
| Мінімізація | - всі можливі корпоративні сервери мають так звану систему «дзеркального копіювання», що дає змогу уникнути будь-яких втрат у разі аварії;<br>- постійне тестування програмного забезпечення, впровадження Agile-методології, резервне копіювання, сертифікація у відповідності до міжнародних стандартів (ISO, SOC). |
| Перенесення | - дана компанія використовує страхування на випадок витоку даних реальних клієнтів, що помітно зменшує можливі фінансові втрати;<br>- використання хмарних сервісів, страхування активів та співпраця з юридичними установами. |
| Прийняття | - в ході укладання контрактів у валюті допускаються можливі коливання в рамках 1-2% без інших фінансових компенсацій;<br>- невеликі коливання валютного курсу чи незначні затримки в реалізації проєкту. |
| Диверсифікація | - комбіновані послуги: хостинг, нерухомість, розробка, видавництво, консалтинг. |
| Моніторинг та контроль | - у цій компанії на належному рівні функціонує відділ контролю якості, котрий аналізує не тільки технічні ризики, а і можливі ризики невідповідності проєктів потребам клієнтів;<br>- регулярні KPI-оцінки, внутрішні аудити, моніторинг кіберзагроз, аналіз тенденцій ринку |

Розроблена та подана нами вище таблиця показує реальну комплексність можливого ризик-менеджменту досліджуваної компанії «Українські інформаційні технології». Кожен з методів окрему важливу функцію: від запобігання до адаптації. Завдяки цьому дана компанія підтримує певний баланс між безпекою та розвитком.

Для більш повного розуміння ефективності механізмів управління ризиками, що застосовуються у даній компанії, доцільно провести SWOT-аналіз. Цей метод дає можливість в повній мірі оцінити внутрішні слабкі та сильні сторони системи ризик-менеджменту, а також зовнішні загрози та можливості, які можуть впливати на її ефективність. Саме цей підхід дозволяє в повній мірі розглянути, наскільки стратегія управління ризиками відповідає сучасним викликам ІТ-сфери та забезпечує стабільний розвиток компанії. Результати SWOT-аналізу подано в таблиці 2.3.

**Таблиця 2.3**

**SWOT-аналіз системи управління ризиками ТОВ «Українські інформаційні технології»**

| Сильні сторони | Слабкі сторони |
|---|---|
| - наявність своєї системи управління ризиками, яка побудована на міжнародних стандартах (ISO, SOC);<br>- цільове та систематичне впровадження комплексних заходів мінімізації ризиків;<br>- високий рівень цифровізації та використання хмарних технологій;<br>- ефективна диверсифікація всіх видів діяльності;<br>- постійний моніторинг та внутрішній аудит з використання KPI;<br>- Міжнародна інтеграція через партнерство із SoftServe, Inc | - великі фінансові втрати на кіберзахист;<br>- часткова залежність від людського фактору при моніторингу ризиків;<br>- неповна автоматизація процесу контролю ризиків саме з внутрішньої сторони;<br>- обмеженість географічного охоплення;<br>- певна інерційність у прийнятті управлінських рішень у кризових умовах;<br>- помітна залежність від стабільності глобального ринку ІТ-послуг. |

**Продовження таблиці 2.3**

| Можливості | Загрози |
|---|---|
| - використання штучного інтелекту для автоматизації ризик-аналізу;<br>- розширення партнерства з міжнародними страхувальниками ризиків;<br>- розроблення програм для навчання працівників ризик-менеджменту;<br>- використання ШІ для прогнозування ризиків;<br>- підвищення довіри клієнтів завдяки прозорості процесів контролю ризиків. | - нові види інформаційних атак;<br>- економічні коливання та геополітична нестабільність;<br>- втрата кваліфікованих кадрів через тиск конкурентів;<br>- зміни у регуляторному середовищі (GDPR, кібербезпека, податкові норми);<br>- можливі перебої в інфраструктурі через енергетичні чи воєнні ризики. |

*Джерело: розроблено автором*

Продемонстрований SWOT-аналіз дає підґрунтя для того, щоб стверджувати, що система управління ТОВ «Українські інформаційні технології» має сильну внутрішню базу – сформовані механізми використання міжнародних стандартів, контролю, високий рівень технологічної готовності та ефективну диверсифікацію.

Одночасно існують деякі слабкі місця, напряму пов’язані з витратністю технічної підтримки, людський фактор та обмеженістю географічного охоплення. Наголосимо, що серед зовнішніх можливостей для подальшого покращення потрібно відзначати впровадження інструментів ШІ та аналітики великих даних у процеси ризик-менеджменту, міжнародну співпрацю та розширення програм навчання персоналу. Головними загрозами залишається нестабільність ринкового середовища, зростаюча конкуренція за кваліфікованих працівників, нормативні зміни та кіберзагрози.

Отже, компанія «Українські інформаційні технології» на даному етапі застосовує комплексну систему управління можливими ризиками, що включає: мінімізацію, прийняття, уникнення, перенесення, контроль, диверсифікацію та моніторинг. Завдяки такому підходу ця компанія не тільки захищає себе від

втрат, а і підвищує конкурентоспроможність, забезпечуючи при цьому довіру партнерів та клієнтів.

### 2.3. Проблеми, які виникають під час управління ризиками в компанії «Українські інформаційні технології»

Управління ризиками є невіддільною складовою дієвого функціонування теперішніх ІТ-компаній. Саме дозволяє забезпечити конкурентоспроможність, збереження репутації та фінансову стабільність. Для компанії «Українські інформаційні технології», що спеціалізується на розробці ІТ-консалтингу, програмного забезпечення, оренді нерухомості та хостингу, ризик-менеджмент має стратегічне значення. Незважаючи на присутність управління ризиками, ТОВ стикається з великою кількістю проблем, що ускладнюють її ефективну реалізацію.

Перейдемо до детального розгляду основних проблем досліджуваної компанії та їх впливу на її діяльність, але для початку продемонструємо схематично на рисунку 2.3.


**Рис. 2.3 – Проблеми, які виникають під час управління в ТОВ «Українські інформаційні технології» [57]**

У контексті діяльності ТОВ «Українські інформаційні технології» проблематика управління ризиками зумовлена не лише зовнішніми чинниками,

а й внутрішніми обмеженнями самої організації. Особливістю ІТ-компаній є висока залежність від швидкості технологічних змін, стабільності комунікаційних процесів та здатності оперативно перебудовувати внутрішні операції. Саме тому навіть незначні збої в координації між відділами або недостатня структурованість відповідальності за ризики можуть суттєво послаблювати ефективність функціонування компанії. Додатково, через мультипроєктний характер діяльності ризики в одній сфері здатні швидко поширюватися на інші напрями бізнесу, створюючи ефект «накопичення загроз». Це формує потребу у поглибленому аналізі причин їх виникнення та більш адаптивному підході до управління [57].

Прослідковується, що ми чітко виокремили шість основних проблем, які виникають під час управління, а тому зупинимось на кожній з них більш детальніше:

1. **Нестабільність зовнішнього середовища для компанії:** саме це середовище для цієї компанії характеризується частими змінами податкової політики, змінами законодавства та ринкових умов. Додатково, військова та геополітична ситуація в Україні формує непередбачувані загрози для бізнес-процесів. А тому компанія має постійно адаптовувати свої стратегії та резервувати ресурси для швидкої реакції, що створює додаткове навантаження на управлінські процеси.

2. **Фінансові ризики:** неплатоспроможність клієнтів та партнерів і валютні коливання мають вплив на прибутковість компанії. У ІТ-секторі фінансові ризики особливо значущі через залежність від високої конкуренції та зовнішніх ризиків. Зважаючи на це, фінансові ризики є одними з найкритичніших, оскільки вони загрожують стабільності та розвитку ІТ-компанії.

3. **Кіберзагрози:** компанія, яка працює з закритими чи особистими даними клієнтів та хостингом, постійно піддається найбільшому витоку саме конфіденційної інформації, ризикам кібератак та технічних збоїв. Попри

впровадження захисних систем, в повній мірі уникнути загрози на даний час нереально.

4. **Організаційні труднощі:** неповна комунікація між відділами однієї компанії, недостатність кваліфікованих спеціалістів у вузьких напрямках ризик-менеджменту ускладнюють дієву реалізацію проєктів. Загалом, внутрішня структура компанії не завжди дозволяє швидко й ефективно реагувати на загрози.

5. **Людський фактор:** часто трапляється у працівників професійне вигорання, помилки працівників та висока плинність кадрів створюють додаткові ризики у адмініструванні та розробці систем. Саме людський фактор залишається одним з найбільш складних для контролю та може до суттєвих операційних збоїв.

6. **Репутаційні ризики***:* до цього прийнято відносити всі можливі збої у роботі програмного забезпечення або витік будь-яких даних може погано вплинути на довіру клієнтів та в подальшому зменшити їх кількість. У контексті високої конкуренції на ІТ-ринку, це може привести до витрат на довгий час. Репутація є стратегічним ресурсом, і її втрата здатна суттєво вплинути на позиції компанії.

Аналіз шести груп ризиків демонструє, що значна частина проблем формується через слабку інтеграцію ризик-менеджменту в операційну діяльність компанії. У більшості випадків ризики фіксуються, але не супроводжуються системним аналізом наслідків або корекцією внутрішніх процедур. Крім того, компанія використовує переважно реактивний підхід, що означає реагування після виникнення проблеми, а не завчасну превенцію. Така модель є типовою для багатьох українських ІТ-компаній, але вона істотно обмежує їх стійкість у період нестабільності.

Також в ході дослідження управління ризиками в проєктному менеджменті ТОВ «Українські інформаційні технології» ми провели невелике опитування серед працівників. (Див. додаток Е). На основі інтерв’ю, спілкування з менеджерами та керівником PMO-офісу я з’ясував, що компанія здійснила низку

заходів для управління найкритичнішими ризиками. Детальні приклади я поділив у таблиці за типами ризиків та відповідними стратегіями роботи з ними. Але якщо говорити про ключові дії, то найважливішою була **оптимізація витрат**:

- По-перше, рішення щодо оптимізації приймалися в більшості випадків на рівні конкретних департаментів або юнітів. У багатьох підрозділах було запроваджено заморозку перегляду заробітних плат. Частині працівників тимчасово знизили заробітні плати на певний відсоток – переважно тим, чиї компенсації суттєво перевищували середній рівень для їхнього грейду;
- По-друге, відбулося значне скорочення адміністративного персоналу. В окремих випадках закривалися цілі департаменти. Наприклад, суттєво скоротили підрозділи, які займалися R&D-дослідженнями, а також HR-напрям: частину функцій об’єднали, частину оптимізували з метою зменшення витрат. За даними DOU, частка адміністративного персоналу в SoftServe становила близько 22%, тоді як середньоринковий показник для IT – 8-18%.

Також у відповідальному порядку переглядалося фінансування співробітників без проєктів (так званого bench). У більшості випадків фінансування скорочували. Як я згадував раніше, відбулося значне зменшення кількості працівників рівня junior та middle, що й призвело до статистичного зростання середньої заробітної плати. Додатково були закриті частина офісів або ж переведені в режим ремонту чи оптимізовані під нові формати роботи.

Великий обсяг дій був спрямований на забезпечення безперервності бізнесу та реалізацію BCP-планів. Зокрема, всі офіси було переведено в автономний режим: встановлені потужні дизельні генератори, Starlink, резервні канали зв’язку, а також автономне опалення. Для працівників було організовано програми релокації з небезпечних регіонів до більш безпечних. Передбачалася фінансова допомога у розмірі 1000 доларів на кожного, хто переїжджав. Компанія також займалася бронюванням працівників, допомагала з оформленням документів для переїзду за кордон та подальшої легалізації в інших юрисдикціях, щоб продовжувати співпрацю.

Серед найбільш стратегічних рішень – диверсифікація ринків і перехід до активнішої присутності в Латинській Америці. Це дозволило залучати спеціалістів у часовій зоні клієнтів, а також працівників, менш залежних від військової та політичної ситуації в Україні. Додатково компанія відмовилася від частини високоризикових проєктів.

Після аналізу всіх цих заходів я дійшов висновку, що систему управління ризиками SoftServe умовно можна поділити на **чотири основні елементи**:

- Перше – внутрішня платформа Project Excellence. Вона була створена для того, щоб лінійні проєктні менеджери могли простіше і структурованіше управляти ризиками на своїх проєктах. Платформа містила функціонал ризик-реєстру, загальний ризик-лог, бібліотеку ризиків, можливість подання запитів на внутрішні аудити, фіксацію завдань для роботи з ризиками тощо. Вона давала змогу уніфікувати і стандартизувати роботу з ризиками відповідно до міжнародних підходів, а також забезпечувала прозорість для вищого керівництва, яке могло переглядати агреговані дані по всіх проєктах і департаментах. Проте, як показали інтерв'ю, у практиці система часто використовується формально. Оскільки вона є окремим інструментом, менеджерам незручно дублювати дані й переносити інформацію з основних робочих середовищ (Google Docs, Excel, Confluence). Через це 11 із 15 опитаних менеджерів зазначили, що фактично користуються Project Excellence «для галочки», а не як інструментом реальної щоденної роботи. Основною реальною цінністю вони назвали бібліотеку ризиків, яка спрощує ідентифікацію ризиків і дає змогу швидко підібрати релевантні;
- Другий елемент – система моніторингу кіберзагроз. Вона включає великий набір внутрішніх IT-систем, які відстежують DDoS-атаки, спроби несанкціонованого доступу, підозрілу активність та дії працівників у корпоративних системах. Це критично важливо в умовах військових ризиків і стрімкого розвитку технологій;
- Третій елемент – операційні метрики. Окремо збираються та аналізуються фінансові, HR-метрики та проєктні показники. Вони

використовуються як KPI, а також інтегруються у систему оцінки ризиків на рівні всього бізнесу.

- Четвертим елементом системи управління ризиками є аудити проєктів за запитом. Кожен менеджер може подати запит на проведення внутрішнього аудиту. Для цього існує перелік внутрішніх аудиторів, які мають компетенцію оцінювати різні аспекти проєкту, у тому числі й ризик-менеджмент. За потреби менеджер може ініціювати аудит самостійно, але крім цього в компанії обов'язковим є проходження аудиту раз на пів року.

Такий аудит складається з кількох частин: технічного аудиту, аудиту якості проєкту та загального проєктного аудиту. У межах останнього проєктний менеджер заповнює детальний чекліст щодо процесів, яких він дотримується, прикріплює докази, а також проходить інтерв'ю з аудитором. Це інтерв'ю допомагає визначити проблемні зони на проєкті, включно з усіма аспектами ризик-менеджменту.

У підсумку аудитор формує рекомендації, виписує проєктні ризики, які вносяться в систему Project Excellence, а менеджер отримує зобов'язання виконати необхідні дії для мінімізації цих ризиків у встановлений термін.

Отже, система управління ризиками має складатися з двох ключових аспектів: перший – це сама система та процеси: комплексний, системний підхід, дотримання стандартів, наявність реєстру ризиків, регулярні перевірки, аудит, моніторинг, інструменти та правила, за якими працюють менеджери; другий – це професійні кадри та культура. Навіть ідеальна система не працюватиме ефективно, якщо люди через психологічні чинники чи недостатню компетентність сприйматимуть її формально, виконуватимуть дії «для галочки» або саботуватимуть процеси.

Компанії необхідно приділяти особливу увагу воєнним і макроекономічним факторам. Хорошим прикладом є те, як було організовано та впроваджено BCP-план. Менеджери на всіх рівнях контролювали стан працівників, перевіряли, чи вони у безпеці, чи потрібна допомога, підтверджували можливість продовжувати роботу. Так само проводилась

інтенсивна комунікація з клієнтами, щоб впевнити їх у безперервності роботи компанії.

Потрібно переглянути вагу операційних метрик та цілі, які встановлюються менеджерам. За результатами інтерв'ю було видно, що менеджери часто зосереджуються на досягненні «цифр на папері», навіть якщо ці показники не зовсім відповідають реальному стану компанії. Це призводить до ситуацій, коли топ-менеджмент може виглядати успішним за KPI, але фактичні фінансові показники – дохід і чистий прибуток – суттєво падають.

Для частини проєктів і працівників варто запровадити обов'язкову сертифікацію та регулярне навчання з ризик-менеджменту. Це допоможе сформувати єдину культуру роботи з ризиками та підвищить професійність менеджерів і команд.

Необхідно підтримувати постійний фокус на посиленні кіберзахисту. В компанії вже був критичний випадок – злам внутрішніх даних, під час якого були викрадені близько 200 паспортів працівників. Це спричинило репутаційний удар і призвело до втрати кількох клієнтів. Компанія понесла суттєві збитки, і цей приклад показав, що ризики кіберзагроз є надзвичайно важливими, а наслідки їх спрацювання – дуже болючими для бізнесу.

Сукупність основних ризиків, з якими стикається IT-компанія, формується як зовнішніми, так і внутрішніми чинниками: нестабільне зовнішнє середовище з частими змінами законодавства, податкової політики та геополітичної ситуації вимагає постійної адаптації стратегій; фінансові загрози у вигляді валютних коливань та неплатоспроможності клієнтів безпосередньо впливають на стабільність бізнесу; кіберризики залишаються критичними через роботу з конфіденційними даними; організаційні недоліки та дефіцит кваліфікованих кадрів ускладнюють ефективне управління; людський фактор посилює ймовірність помилок та операційних збоїв; а репутаційні втрати, зумовлені технічними проблемами чи витоком інформації, можуть надовго послабити ринкові позиції. У сукупності ці чинники створюють комплексний виклик, що потребує системного управління ризиками та стратегічної гнучкості.

Охарактеризувавши основні проблеми з якими стикається ТОВ «Українські інформаційні технології», ми хочемо в таблиці показати можливі шляхи їх подолання саме для цієї компанії.

**Таблиця 2.4**

**Шляхи подолання проблем, які виникають під час управління в ТОВ «Українські інформаційні технології»**

| Проблема | Шляхи подолання |
|---|---|
| Нестабільність зовнішнього середовища | моніторинг ринкових та законодавчих змін, резервування ресурсів та гнучке стратегічне планування |
| Фінансові ризики | страхування фінансових ризиків, диверсифікація доходів, політика кредитного контролю та аудит фінансових потоків |
| Кіберзагроза | Залишаються викликом та потребують постійних інвестицій у безпеку та цільового навчання персоналу |
| Організаційні труднощі | створення міжфункціональних команд, оптимізація процесів, впровадження систем управління проєктами та навчання персоналу |
| Людський фактор | навчання персоналу, мотиваційні програми, автоматизація рутинних процесів та контроль якості |
| Репутаційні ризики | Прозора комунікація з клієнтами, розробка кризових PR-стратегій та підвищення стандартів якості продуктів та сервісів |

*Джерело: розроблено автором*

Продемонстрований аналіз показує, що управління ризиками в цій компанії має загальний характер та включає: геополітичні, фінансові та законодавчі – створюють постійний тиск на діяльність компанії; внутрішні ризики: людський фактор, організаційний, комунікаційні бар’єри – створюють операційні складності; кіберзагрози та технічні: залишаються постійним викликом у цифровому середовищі.

Для аналітичного аналізу стану підприємства потрібно аналізувати головні показники його діяльності за 2023-2024 роки. У таблиці, яка представлена нижче показано фінансові результати, рівень забезпеченості ресурсами та показниками кадрового потенціалу.

**Таблиця 2.5**

**Результати діяльності ТОВ «Українські інформаційні технології» 2023-2024 роки [57]**

| Показник | 2023 | 2024 |
|---|---|---|
| Дохід | 1 184 987 000 | 461 742 000 |
| Чистий прибуток | 97 268 000 | 31 085 000 |
| Активи | 557 655 000 | 473 296 000 |
| Зобов'язання | 143 734 000 | 28 290 000 |
| Середня зарплата (до оподаткування) | 15 243 | 20 506 |
| Кількість працівників | 454 | 84 |

Як помітно з продемонстрованих даних, у 2024 році ТОВ показало зниження обсягів діяльності, що проявилося у скороченні доходу більш ніж у 2,5 рази (на 723,2 мільйонів гривень, або на 61%) в порівнянні з 2023 роком. Відповідно, чистий прибуток зменшився майже утричі – з 97,3 мільйонів гривень до 31,1 мільйонів гривень. Це говорить про помітне скорочення обсягів здійснення та перехід на більш вузьку нішу діяльності. Одночасно з цим, загальна вартість активів цього підприємства також скоротилася на 84,4 мільйонів гривень (на 15,1%), що вказує на оптимізацію матеріальних та фінансових ресурсів. Одночасно з цим, зобов'язання компанії зменшилися більш ніж у п'ять разів – із 143,7 мільйонів гривень до 28,3 мільйонів гривень. Це позитивна тенденція, яка свідчить про зниження боргового навантаження, фінансову стабілізацію та підвищення рівня ліквідності компанії [57].

Особливо прослідковується зменшення персоналу – із 454 до 84 працівників, тобто майже у 5,4 рази. Таке зменшення зумовлене реструктуризацією бізнесу та автоматизацією процесів. Одночасно середня

заробітна плата збільшилась у 2024 році зросла з 15 243 гривень до 20 506 гривень (тобто піднялась на 34 %). Отже, діяльність ТОВ «Українські інформаційні технології» у 2024 році характеризується зменшенням масштабів бізнесу при одночасному підвищенні фінансової стійкості та продуктивності праці [57].

Кількість працівників компанії SoftServe також суттєво знизилася в загальному – з приблизно 10 450 до 7 435, згідно з даними DOU за 2024 рік. Причини цього є [57]:

- зміна кон'юнктури американського IT-ринку після ковідного буму;
- глобальна криза та хвиля скорочень у 2022-2024 роках;
- війна в Україні, релокація та мобілізація працівників;
- відмова клієнтів від співпраці через військові ризики;
- внутрішня оптимізація витрат компанії.

Ці фактори стали основними причинами скорочення персоналу та падіння фінансових показників, і саме з ними компанія працювала через різні елементи своєї системи ризик-менеджменту.

Також акцентуємо більш щодо фінансових показників компанії: відчутне зменшення доходу, зменшення дебіторської заборгованості, збільшення середньої зарплати, зменшення кількості працівників – (близько 25%). Причинами таких змін є наступні:

- війна в Україні, часткова мобілізація працівників, їх переїзд за кордон;
- відмова частини клієнтів від співпраці через військові ризики в Україні;
- масові скорочення IT-спеціалістів на ринку США, зменшення витрат на субпідрядників.

А тому досліджувана нами компанія прийняла наступні рішучі дії: оптимізація витрат – заморозка перегляду зарплат, відчутне Скорочення адміністративного персоналу (HR, CoE), високий рівень (22%) адміністративного персоналу (8-18% в середньому по конкурентах); згортання фінансування людей на бенчі; згортання HR програм та витрат на них; значення скорочення працівників рівня Junior та Middle (що призвело до статистичного

зростання середньої заробітної плати); закриття офісів, або їх частин (в тому числі через перехід на ремоут, війну).

Аналіз фінансових показників показав SoftServe, що за останній період дохід компанії знизився майже вдвічі, а чистий прибуток – майже втричі. Також зменшилися активи та зобов'язання. Водночас середня заробітна плата зросла: офіційно – до 20 500 грн у 2024 році, а за неофіційними даними серед працівників (з урахуванням ФОПів) – приблизно до 1900 доларів, що на 200 доларів більше, ніж раніше. Проте зростання відбулося переважно через оптимізацію витрат і скорочення менш ефективних або початкових позицій, а не за рахунок підвищення зарплат [57].

Ефективність управління ризиками у даній сфері в більшій мірі залежить від зовнішніх чинників, що формуються за умов діяльності підприємства. Для того, щоб виявити потенційні проблеми чи бар'єри потрібно провести PEST-аналіз, що дає можливість постійно оцінювати політичні, економічні, соціальні та технологічні аспекти, що впливають на процеси ризик-менеджменту в ТОВ «Українські інформаційні технології».

**Таблиця 2.6**

**PEST-аналіз зовнішнього середовища в контексті управління ризиками ТОВ «Українські інформаційні технології»**

| Фактор | Характеристика впливу на проблеми управління ризиками |
|---|---|
| Політичні | - залежність від воєнної та політичної та політичної стабільності країн (ЄС, США, Україна);<br>- зростання кіберзагроз, посилення регуляцій у сфері безпеки даних (GDPR. NIS2);<br>- зміни оподаткування ІТ-сектору та нормах захисту даних. |
| Економічні | - коливання валют та глобальні економічні спади впливають на проєктне фінансування;<br>- висока конкуренція за таланти підвищує витрати на персонал;<br>- залежність від міжнародних клієнтів і глобальних ринкових трендів. |

**Продовження таблиці 2.6**

| | |
|---|---|
| Соціальні | - вигорання персоналу, спричинене високими навантаженнями, віддаленою роботою, військовими ризиками;<br>- потреба у розвитку культури кібербезпеки серед працівників;<br>- зростання очікувань суспільства щодо прозорості та етичності ІТ-компаній. |
| Технологічні | - стрімкий розвиток AL/ ML та хмарних технологій створює потребу у швидкій адаптації;<br>- зростання складності кіберзагроз і вимог захисту даних;<br>- використання власних R&D-центрів та Gen Al Lab для зниження технологічних ризиків. |

*Джерело: розроблено автором*

Аналізуючи результати проведеного PEST-аналізу, можемо констатувати, що ключовими зовнішніми факторами впливу є:

- політична та економічна залежність від ринків США, Європи та України. Компанія отримує більшість доходів із-за кордону, тому будь-які коливання, нестабільність або глобальні економічні спади мають на неї суттєвий вплив;
- посилення регуляцій та зміни в оподаткуванні;
- технологічні фактори: стрімкий розвиток хмарних технологій та особливо штучного інтелекту, які створюють додатковий тиск і потребу швидко адаптовуватися;
- соціальні та військові фактори: ризики вигорання персоналу, релокації, мобілізація та вплив війни на діяльність компанії в Україні.

Таким чином, можемо узагальнити, що на дану компанію найбільше впливають залежність від міжнародних ринків, військова ситуація в Україні та швидкий технологічний розвиток.

Загалом, система управління ризиками в досліджуваній компанії складається з системи моніторингу та менеджменту: Project Excellence – цифрова система для менеджменту ризиків, але яка часто використовується «для галочки»

через незручність і погану адаптивність під потреби конкретного проєкту. Вона є гарним цифровим реєстром ризиків, але на практиці не користується попитом серед працівників; системи моніторингу кіберзагроз 24/7; велика кількість метрик (фінансових, HR, проєктних), впровадження KPI на їх основі на всіх рівнях; аудити проєктів за запитом

Результати дослідження говорять, що зовнішнє середовище створює загальну систему викликів для управління ризиками досліджуваної компанії. Політична нестабільність та безпекові загрози мають вплив на роботу інфраструктури та кіберризики. Економічна ситуація ускладнює планування бюджету резервів та ризиків. Соціальні чинники – знижують ефективність реагування на ризики. Технологічні зміни потребують постійного оновлення засобів захисту, впровадження нових та передових систем штучного інтелекту та аналітики, що, у свою чергу, потребує інвестицій і спеціалізованої підготовки персоналу.

Додатково варто зазначити, що сучасні тенденції цифрової трансформації створюють для компанії не лише нові можливості, а й нетипові ризики, які раніше не були властивими для IT-сфери. Йдеться про підвищену залежність від алгоритмічних систем, які можуть генерувати помилки внаслідок некоректних даних, а також про ризики, пов’язані з впровадженням штучного інтелекту у внутрішні процеси без належного тестування. У цьому контексті доцільно говорити про появу так званих «гібридних ризиків», де технічні, людські та організаційні фактори поєднуються і здатні створювати каскадні наслідки для компанії. Саме тому підвищується значення стратегічної готовності компанії до непередбачуваних сценаріїв, що передбачає розроблення альтернативних моделей реагування та регулярне оновлення політик безпеки відповідно до актуальних загроз.

Таким чином, для ефективного управління ризиками потрібна паралельна робота над внутрішньою організаційною структурою, зовнішньою адаптивністю та технічною стійкістю. Це дає можливість забезпечити фінансову безпеку, стабільність та збереження репутації на конкурентному ринку.

**Висновок до розділу 2**

Проведений аналіз специфіки управління ризиками у діяльності ТОВ «Українські інформаційні технології» дав можливість в повній мірі оцінити фінансові, організаційні та правові аспекти щодо функціонування компанії, визначити її підхід до ризик-менеджменту, сильні сторони та проблемні зони. Внаслідок цього встановлено, що це підприємство є динамічною та стабільною ІТ-компанією, що поєднує в собі інноваційність, досвід та міжнародну інтеграцію. Ця компанія має широкий спектр діяльності – починаючи з розробки програмного забезпечення та хмарних сервісів до консалтингу, аналітики великих даних, штучного інтелекту й робототехніки. Її правовий статус, організаційна структура та дотримання законодавства забезпечують прозорість та легальність діяльності, а також довіру з боку партнерів та клієнтів.

Під час дослідження визначено, що система управління ризиками у ТОВ «УІТ» є комплексною, поєднує методи мінімізації, уникнення, прийняття, перенесення та іншого. Також компанія в основному застосовує технічні засоби захисту, внутрішній аудит, страхування, сертифікацію та резервне копіювання відповідно до міжнародних стандартів ISO та SOC. Такий підхід забезпечує досить високу адаптивність ТОВ до змін зовнішнього середовища та зменшує випадки критичних витрат.

Проведений SWOT-аналіз продемонстрував, що головними сильними сторонами системи управління ризиками є присутність визначеної стратегії, високий рівень цифровізації, диверсифікація діяльності та міжнародна співпраця. До слабких сторін належить суттєві витрати на кіберзахист, неповна автоматизація внутрішніх процесів контролю, залежність від людського фактора та обмежене географічне охоплення.

Також було визначено низку проблем, що ускладнюють ефективне управління ризиками: нестабільність зовнішнього середовища через війну; ризики через валютні коливання та зменшення платоспроможності потенційних

клієнтів; постійні кіберзагрози; дефіцит кваліфікованих кадрів та їх плинністю; репутаційні ризики, які виникають у випадку технічних збоїв.

Одночасно був важливим PEST-аналіз, який засвідчив, що економічні, політичні, технологічні та соціальні чинники формують складну систему зовнішніх викликів. Зміни податкової політики, військові дії, міграція бізнесу, інфляція, швидкі темпи технологічного розвитку та вигорання персоналу потребують від компанії найвищого рівня адаптації та гнучкого стратегічного планування.

Отже, компанія «УІТ» на даний час залишається прикладом ІТ-компанії, яка, незважаючи на виклики воєнного часу, зберігає сталість, адаптовується до нових умов, покращує управлінські підходи та закладає основу для подальшого розвитку системи управління ризиками на принципах інноваційності, гнучкості та стратегічної відповідальності.

# РОЗДІЛ 3
# ПЕРСПЕКТИВИ ПОКРАЩЕННЯ УПРАВЛІННЯ РИЗИКАМИ В ПРОЄКТНОМУ МЕНЕДЖМЕНТІ В УМОВАХ ВІЙНИ

## 3.1. Світовий досвід покращення управління ризиками в проєктному менеджменті та способи реалізації їх в Україні

У теперішньому світі, де інформаційні технології ідентифіковують темп розвитку темпи розвитку економіки, питання управління ризиками у сфері проєктного менеджменту набуває стратегічного значення. В загальному, українські компанії стикаються з великою кількістю викликів: нестабільністю ринкового середовища, кібератаками, кадровими ризиками, технологічними збоями. Загалом, українські компанії перебувають підвищеної невизначеності через воєнні дії, глобальну конкуренцію та швидкі зміни на ринку цифрових рішень. Саме тому, чітке питання щодо удосконалення системи управління ризиками потребує максимального аналізу як на міжнародному рівні, так і локальному.

Зважаючи на це, ми розглянемо головні проблеми управління ризиками в українських компаніях та всі можливості використання світового досвіду для їх швидкого подолання.

Загалом, в українських компаніях існують наступні проблеми управління ризиками [51]:

1. **Низький рівень формалізації ризик-менеджменту:** тобто компаніям в основному не вистачає єдиної системи документування ризиків. А тому часто стається таке, що ризики фіксуються тільки ситуативно, а не в межах цілісної політики. А тому слабка формалізація збільшує вірогідність допущення помилок однакових у різних проєктах [51, с. 33].
2. **Недостатня підготовка персоналу:** іншими словами велика кількість працівників не мають практичних навичок виявлення та оцінки ризиків, а також ризик-менеджмент зазвичай сприймають як свого роду формальність. Зважаючи

на це, кваліфікація персоналу є критичним чинником, а її нестача робить компанію вразливою [51, с. 34].

3. **Кадрові ризики:** передбачається те, що висока плинність кадрів в різних українських компаніях створює певну загрозу для того, щоб стабільно та вчасно завершувати проєкти. Опираючись на викладене, можемо констатувати, що кадрова стабільність та створення системи внутрішнього резерву кадрів помітно зменшує залежність від окремих працівників [51, с. 35].

4. **Фінансові та ринкові ризики:** українські компанії в сучасних умовах зустрічаються зі складністю прогнозування доходів через змінність курсу валют та скорочення попиту на деякі пропозиції. А тому, ефективне управління фінансовими ризиками потребує диверсифікації ризиків та страхування, що дуже важливо на сучасному етапі [51, с. 36].

**Таблиця 3.1**

**Приклади проблем управління ризиками в українських компаніях [49]**

| Проблема | Приклад |
|---|---|
| Низький рівень формалізації ризик-менеджменту | у ході впровадження нового програмного забезпечення було виявлено певні проблеми з влиттям в наявну IT-інфраструктуру, а і відсутність основної бази ризиків і призводить до затягування строків виконання проєкту |
| Недостатня підготовка персоналу | відсутність тренінгів персоналу з кібербезпеки спричинила витік даних після фішингової атаки на працівників |
| Кадрові ризики | звільнення головного розробника посередині проєкту змусило команду витратити ще ресурси на його заміну, що знизило конкурентоспроможність продукту |
| Фінансові та ринкові ризики | в ході різкої девальвації гривні компанія втратила частину контрактів через зростання вартості розробки |

Розглянувши проблеми управління ризиками в українських компаніях та окресливши всю їх сутність, в подальшому постає необхідність розглянути, які саме практики та інструменти використовуються у світі та яким чином їх реально ефективно використати в Україні:

1. **Використання міжнародних стандартів управління ризиками свідчить про:**

- *стандарти ISO 31000, PMBOK та PRINCE2* – вони є найвживанішими у світі оскільки встановлюють універсальні правила для виявлення, аналізу та моніторингу ризиків;

- можна навести такий *приклад*: всім відома у світі компанія Siemens завдяки ISO 31000 (*додаток А*) зменшила втрати від ризиків у великих інфраструктурних проєктах;

- *можливості для використання в Україні*: впровадження даних стандартів у IT-проєктах та державних закупівлях; проведення сертифікації українських менеджерів за PMBOK/PRINCE2.

Таким чином, саме стандартизація створює передбачуваність та збільшує довіру міжнародних партнерів, що може вивести українські компанії на новий рівень.

2. **Гнучкі методології управління ризиками (Agile, Scrum) у світі є наступними***:*

- Netflix та Spotify використовують Scrum, де ризики обговорюються на щоденних мітингах команд; IBM вливає аналіз ризиків у кожен спринт.

- *можливості для використання в Україні*: застосування Agile-практик у IT-компаніях та стартапах; перенесення таких підходів в розроблювані державні цифрові проєкти (прикладом цього є «Дія», е-сервіси).

Отже, можемо констатувати, що Agile дає змогу українським компаніям працювати продуктивно навіть у кризових умовах, а тому його запровадження та удосконалення на українських теренах є важливим.

3. **Інтеграція кібербезпеки в управління ризиками у світі є наступною***:*

- наголосимо, що Microsoft щорічно інвестує більше як 1 млрд доларів для кіберзахисту; відома компанія Mastercard створила центр цілодобового реагування кібербезпеки.

- *можливостями для нашої держави є:* формування відділів, які будуть відповідальними тільки за кібербезпеку в українських банках та компаніях, що дуже важливо для загально рівня безпечності; використання хмарних серверів для того, щоб копіювати дані; проведення спеціальних навчань та тренінгів для співробітників щодо правильної поведінки під час кіберзагроз.

Зважаючи на наведене, констатуємо, що у воєнних умовах кібербезпеки – це один з найбільш серйозних факторів, через це їх влиття в ризик-менеджмент надзвичайно необхідно.

4. **Використання Big Data та штучного інтелекту у світі:**

- *прикладами* цього можемо назвати наступні – Google може прогнозувати відмови у роботі дата-центрів за допомогою штучного інтелекту; Amazon встановив шахрайські транзакції на основі Big Data.

- *можливості для використання на вітчизняних теренах* – застосування штучного інтелекту для передбачення ризиків у фінансовому секторі та логістиці; співпраця з українськими стартапами у сфері аналітики (Corezoid, Reface).

Зважаючи на це, цифрова аналітика дає можливість вітчизняним компаніям не тільки реагувати на ризики, які вже сталися, а і може передбачати їх.

5. **Культура ризик-менеджменту всередині компаній:**

- яскравим *прикладом* культури є наступні компанії: Toyota запровадила засаду Kaizen, де всі працівники повідомляють про можливі ризики; Google проводить мозкові штурми з оцінки можливих ризиків.

- *можливості для реалізації в Україні* – утвердження постійних «risk meetings» у компаніях; впровадження системи мотивації (бонуси за виявлений ризик); політика «zero blame» – помилка не карається, а аналізується.

Отже, саме сильна корпоративна культура робить безпосередньо управління ризиками системним, а не носить тільки формальний характер, що є позитивним в роботі.

6. **Диверсифікація бізнесу та фінансова стійкість є основою діяльності компаній:**

- яскравим *прикладом* є такі відомі компанії – Apple має мережу постачальників у багатьох країнах світу, для того, щоб в процесі не залежати від одного регіону; Samsung інвестує в різні напрями (смартфони, дисплеї, чипи).
- як і в усіх інших випадках, тут також є *перспективи для України* – для IT-компаній – вихід на ринки ЄС та США; застосування страхування проєктів (кіберризики, зриви контрактів та інше).

IT-сектор України загалом показує високу динаміку, проте паралельно - явний дефіцит кадрів та волатильність експортних доходів. Саме тому автоматизація та стандартизація процесів ризик-менеджменту є передовими практиками. У звітах BRDO [53] та Lviv IT Cluster [56] наголошується: компанії, які впроваджують Agile-практики та стандарти, мають більшу стійкість у кризових ситуаціях.

Такі приклади мають практичний сенс для компанії «Українські інформаційні технології», а все тому, що вона: має комплекс послуг (аутсорсинг, хостинг, розробка, нерухомість) – стандартизований RM збільшить більшу прозорість по можливих напрямах і дасть пріоритети в тендерах. Після того як скорочено штат компанія сфокусує на збереженні репутації та якості – формалізація RM зменшує репутаційні ризики та операційні помилки. Сама матриця оцінювання ризиків представлена у *додатку Б*.

Наведемо конкретні пропозиції короткострокові та середньострокові:

1. **Quick wins (до трьох місяців):** важливим є впровадити цифровий Risk Register (*додаток В)* (Jira/Confluence) і шаблон Kick-off, де ризики – це важлива та невід'ємна частина стартового пакета; доцільно провести два дні інтенсиву для PM/Tech-Leads: ISO 31000 basics + Agile risk reviews; також ввести політику «risk owner» для всіх критичних ризиків.

2. **Середньострокові (від трьох до дванадцяти місяців):** сертифікувати 1-2 PM у PMBOK/PRINCE2; інтегрувати risk-reviews у спринти; також розробити DR/BCP і провести tabletop-exercise; почати пілот HR-analytics (churn prediction).

Від впровадження вищезазначеного може бути наступний ефект: краща видимість ризиків, вища довіра клієнтів, менше простоїв та швидша реакція (BRDO, Lviv IT Cluster).

Додатково до цього варто враховувати, що сучасні моделі управління ризиками у провідних світових компаніях усе частіше базуються на концепції «динамічного ризик-менеджменту». Її сутність полягає у тому, що ризики не просто фіксуються на певному етапі проєкту, а постійно переоцінюються відповідно до змін зовнішнього середовища. Такий підхід активно застосовують компанії Bosch, Siemens та Deloitte, які використовують адаптивні алгоритми для моделювання поведінки ризиків залежно від ринкових, політичних чи технічних коливань. Для України цей підхід є особливо актуальним, оскільки він дозволяє враховувати високу волатильність економіки, воєнні чинники та нестабільність нормативно-правового поля. Запровадження динамічних моделей моніторингу ризиків у вітчизняних компаніях сприятиме швидшому виявленню аномалій, прогнозуванню кризових сценаріїв і зміцненню стійкості проєктів навіть за умов непередбачуваності.

Таким чином, можна узагальнити, що страхування та диверсифікація значно знижують залежність бізнесу від окремих та особливих факторів, які мають вплив на функціонування компаній.

Світовий досвід управління показує, що результативність досягається завдяки комплексному підходу: гнучким методологіям, стандартизації, використанню штучного інтелекту, диверсифікації, кіберзахисту та корпоративної культури. В нашій державі дані практики можуть бути здійсненими через: адаптацію міжнародних стандартів (ISO, PMBOK, PRINCE2); розвиток Agile-культури в IT і держсекторі; посилення кіберзахисту в умовах війни; впровадження Big Data для прогнозування; формування

культури ризик-менеджменту у компаніях; диверсифікацію бізнесу та страхування проєктів.

Для нашої держави надзвичайно важливо інтегрувати даний досвід, враховуючи специфіку ринку, кадровий потенціал та воєнні виклики. А тому поєднання міжнародного досвіду з своїми стратегіями управління ризиками дасть змогу українському ІТ-сектору підвищити свою конкурентоспроможність та стійкість до більш масштабних викликів.

### 3.2. Шляхи удосконалення управління ризиками в сучасних умовах

З початком повномасштабного вторгнення суттєво підвищено частоту та масштаб ризиків: енергетичні та логістичні перебої, зміни у зовнішній торгівлі, масові кібератаки. Паралельно зросла роль приватного сектора та донорів у адаптації та відновленні. Українські та світові оцінки показують великий обсяг відновлювальних потреб і необхідність системної стійкості. Таке ставить завдання – постійно і швидко покращити управління ризиками галузевому, національному та корпоративному рівнях.

Саме тому, теперішні умови потребують переходу від реактивного до проактивного, системного ризик-менеджменту з чіткими процесами, інструментами та ресурсами. Водночас сучасні трансформаційні процеси вимагають запровадження так званого інтегрованого ризик-менеджменту, коли ризики не розглядаються окремо за напрямами (фінансові, кібернетичні, операційні), а оцінюються через їх взаємозалежність та кумулятивний ефект. У світових компаніях ця модель функціонує як ERM-платформа (Enterprise Risk Management), що дає змогу поєднувати дані з різних підсистем, будувати єдину карту ризиків та визначати пріоритети за принципом «systemic impact». Для України така модель є особливо важливою через багатовимірність загроз – одночасний вплив енергетичної нестабільності, кіберризиків, логістичних обмежень, кадрових втрат та фінансової турбулентності. Інтегрований ризик-менеджмент дозволяє не лише підвищити точність прогнозів, а й зменшити

витрати на дублювання процесів, пришвидшити ухвалення рішень та посилити стратегічну стійкість організацій, зокрема в IT-секторі.

Особливо важливим є впровадження системи показників стійкості та раннього попередження (Resilience & Early Warning Indicators), що дозволяє не лише реагувати на інциденти, а й прогнозувати потенційні загрози на основі аналітики в реальному часі. Такі системи виявляють вузькі місця в бізнес-процесах, аналізують залежності від критичної інфраструктури та постачальників, а також дають можливість приймати проактивні рішення щодо ресурсного резервування та адаптації процесів. У контексті українських компаній та державного сектору це означає створення «живих» дашбордів ризиків, які інтегрують дані з різних джерел – енергетика, логістика, кібербезпека, HR, фінанси – та автоматично сигналізують про потенційні критичні зони, що підвищує швидкість реагування і мінімізує фінансові й операційні втрати.

1. **Управління на рівні держави та великих організацій** є важливим тому, що у відсутності одностайної координації ризик-менеджменту виникає повільна реакція, «сліпі зони» та дублювання. Великі організації та держава мають мати визначені ролі, механізми і процедури передачі інформації. Світові практики базуються на національних рамках та стандартах (ISO, PMBOK, PRINCE2).

Для впровадження цього необхідно зробити наступні кроки:

- посилити чи створити центральний координаційний орган, який вливає дані від міністерств, бізнесу та критичної інфраструктури; також він формує національну політику ризик-менеджменту та скоординовує допомогу донорів;
- впровадити обов’язкові настанови чи тимчасові правила для головних секторів з компонентами ISO 31000/22301/27001;
- розробити одностайний реєстр ризиків (on-line dashboard) з індикаторами, що збирає інформацію в дійсному часі від державних органів, критичної інфраструктури та волонтерських мереж.

Загалом, наголосимо, що централізація та стандартизація забезпечують максимальну швидкість та узгодженість дій, яка потрібна під час масштабних криз.

2. **Бізнес-безперервність і стандарти BCMS (ISO 22301)** – *операційна готовність підприємств* передбачає свого роду план постійного бізнесу (BCP/BCMS), що дає можливість зменшити простій, зберегти доходи та захистити клієнтів – критично за умов атак на логістику і інфраструктуру. ISO 22301 дає шаблон для такої системи.

Кроками для впровадження можуть бути наступні:

- зобов'язати ключовий бізнес (енерго, банкі, телеком, держпостачальники) мати сертифікований або мінімально відповідний BCP (перехідний період 6–12 місяців);
- стандартизувати BCP-процедури: критичні процеси, альтернативні локації, резервні канали зв'язку, постачання палива чи генераторів;
- регулярні тренування і tabletop-вправи з різними сценаріями (кібер-атака, масові відключення, евакуація персоналу);
- підтримка малих і середніх підприємств (МСБ): шаблони BCP, гранти/консультації від донорів.

Таким чином, можемо констатувати, що інституалізований BCMS з регулярним тестуванням помітно зменшує операційні втрати в ході криз, що є позитивним моментом в попередженні ризиків.

3. **Кібербезпека як інтегрована складова ризик-менеджменту** важлива тому, що кібернапади у війні – щоденна загроза: витік даних, DDoS, підтасування інформації. Деякі настанови, центри реагування (CERT-UA) і безперервний моніторинг – необхідність.

Головними кроками для впровадження є:

- національні до кібергігієни для критичної інфраструктури та державних органів: оновлення, MFA та сегментація мереж;
- розбудова спеціальних центрів щодо моніторингу у державному секторі та публічно-приватні координаційні вузли;

- загальне навчання всього персоналу через базову кібергігієну та спеціальні тести;

- страхування від можливих кіберризиків та угоди з резервними хостинг-провайдерами.

Отже, узагальнимо, що поєднання організаційної координації, технічних заходів та навчання персоналу суттєво знижує кіберуразливість, що позитивно впливає на зменшення ризиків.

4. **Фінансова стійкість:** страхування, резерви, механізми швидкого фінансування потрібні, адже втрата доходів, потреба у відновленні та руйнування активів потребують як довгострокового, так і короткострокового фінансування реконструкції – донори та світові банки вже накопичують ресурси; саме тому наша держава потребує узгодженої фінансової політики.

Найбільш визначальними кроками для впровадження є:

- утворити національний фонд чи сектор швидкого реагування, які доступні для критичних інфраструктур;

- належна підтримка страхових ринків: страхування контрагенських ризиків; покращення кіберстахування; державні субсидії для виплати премій у ті періоди, коли підвищена активність;

- гранти чи кредитні лінії для МСБ (EBRD/World Bank підтримка вже існує – використовувати для масштабування).

Можна узагальнити, що , так би мовити, фінансова «подушка» та доступ до швидкого кредитування зменшують ризик банкрутства та прискорюють його відновлення.

5. **Ланцюги постачання та логістична стійкість** важливо тому, що порушення постачань (енергія, комплектуючі, логістика) заморожує функціонування сервісів та виробництва. Світова практика – запасні маршрути та багатопостачальницька стратегія.

Найбільш доцільними кроками для реалізації є:

- для критичних секторів картографування ланцюгів постачання – тобто виявлення single-point-of-failure;

- створення локальних кластерів та диверсифікація постачальників;
- зберігання запасів і логістичні коридори – стимулювання з державної сторони стратегічних запасів;
- податкова та юридична підтримка для компаній, які переносять деяку частину виробництва у більш безпечні регіони.

На основі вказаного можемо сказати, що стратегічні запаси та відновлювальні ланцюги постачання максимально знижують уразливість секторів в ході екскалацій.

6. **Людський капітал:** підготовка, охорона, психологічна підтримка також необхідна, адже висока плинність кадрів та стрес підвищують ризик помилок та знижують продуктивність праці. А сама підтримка персоналу – підґрунтя будь-якого ефективного BCP.

Визначальними кроками для впровадження є:

- підготовка персоналу та спеціалізовані програми безпеки;
- профілактика професійного вигорання у працівників та належна психологічна підтримка;
- гнучкий характер політики праці: релокація команд, віддалена робота та ротація персоналу;
- схеми забезпечення головних талантів (страхування, бонуси, компенсації).

Отже, інвестиції в кваліфіковані кадри – це найбільш швидкий шлях до стабільності операцій та і загалом до більш високого рівня діяльності українських компаній.

7. **Аналітика, ШІ та цифрові рішення для прогнозування ризиків** важливо тому, що прогнозні моделі дають змогу передбачати збійні сценарії та розподіляти ресурси за рівнем необхідності.

Ключовими кроками для впровадження є:

- пілотні проєкти AI для того, щоб прогнозувати ризики у логістиці та фінансовому секторі;
- влиття даних у національний реєстр ризиків;

- розробка можливих альтернативних сценаріїв.

Загалом, доцільно акцентувати, що цифрова аналітика підвищує передбачуваність та дає змогу більш дієвіше використовувати ресурси, які є обмеженими.

8. **Міжнародна кооперація, донорська допомога та фінансування відновлення** є потрібним тому, що масштаб потреби в інвестиціях та руйнувань перевищують можливості на локальному рівні – потрібний швидкий доступ до фінансування та координація донорів.

Для реалізації будуть доцільними наступні кроки:

- розподіл донорських коштів та одна платформа залучення;
- проєкти стимулів і дерегуляції для приватних інвесторів;
- використання міжнародних програм грантів чи кредитування для великих інфраструктурних проєктів.

Таким чином, залучення та координація зовнішнього капіталу, а також належна координація є критичною умовою швидкої відбудови та помітне підвищення стійкості.

9. **Комунікація, інформаційна безпека та протидія дезінформації** є визначальною тому, що фейки, паніка та ненадійна інформація посилюють ризики. Саме тому потрібні прозорі канали комунікації бізнесу та держави з клієнтами і громадянами.

Зважаючи на це ми подамо певні пропозиції щодо покращення для цієї компанії управління ризиками: системний, комплексний підхід до управління ризиками та професійні кадри які б оптимально контролювали особливості ведення бізнесу; особлива увага до воєнних та макроекономічних факторів (розробка та впровадження BCP); ширше застосування підходу сценарного планування. Система управління ризиками не лише «для галочки», а й її дія в реальності; переглянути пріоритетність метрик, та їх значущість на рівні C-Level менеджменту, щоб уникнути проблеми погоні за метриками та бонусами; системне управління ризиками на рівні команди згідно Agile підходів; регулярне

обов’язкове навчання та сертифікація працівників; посилення кіберзахисту, резервного копіювання.

Можливими кроками для впровадження є:

- одні і ті самі офіційні канали кризової комунікації;
- програми швидкості спростування фейків та медіаграмотності;
- підтримка чіткої клієнтської комунікації (SLA, повідомлення про простій, плани компенсацій).

Отже, важливо виокремити, що якісна комунікація помітно зменшує операційні та репутаційні ризики.

Попри можливості щодо удосконалення управління ризиками в сучасних умовах існують певні перешкоди, а тому ми їх виокремимо та спробуємо розкрити те, як їх подолати:

- недостатнє фінансування – державні гарантії, донорські програми, державні субсидії на страхові премії;
- опір змінам та низька культура ризик-менеджменту – мотиваційні програми, тренінги, «zero-blame» підхід;
- технічні бар’єри (дані, інтеграція) – стандарти відкритих API, підготовка технічних специфікацій;
- корупційні ризики при розподілі допомоги – прозорі платформи (Prozorro-подібні) і зовнішнє аудитування.

Після проаналізованих аспектів ми вдамося до аналітики. Дослідивши особливості роботи передових компаній ми виокремили основні їх шляхи управління ризиками:

1. Стандартизація в поєднанні з сертифікаціє (ISO 31000/27001/22301). Компанії які є лідерами сертифікують процеси, для того, щоб гарантувати дотримання практик RM та безперервності бізнесу.

2. Agile разом з постійними risk-monitoring. Ризики коригуються та обговорюються кожного спринта; у команді є risk-owner.

3. MVP-SOC і кібергігієна. Базовий SOC в поєднанні з регулярними penetration tests і страхування кіберризиків.

4. Big Data для прогнозування**.** Прогнозні моделі для HR-churn, контрактних ризиків, аномалій у CI/CD.

5. ISO 22301 **–** план безперервності бізнесу. Таблетоп-вправи, альтернативні локації, multi-zone cloud strategy.

6. Культура: навчання в поєднанні employer branding. Інвестиції у L&D та прозорі політики – фактори, що знижують churn і підвищують якість.

Продемонстровані шляхи доцільно реалізувати на території нашої держави:

- галузевий та національний рівень: державні та кластерні ініціативи (наприклад, Lviv IT Cluster [56], BRDO [53]) повинні стимулювати впровадження стандартів через доступ до шаблонів і навчання; створити «шаблони BCP/ISO» для МСБ.
- для ТОВ «УІТ» пропонуємо наступну реалізацію: використовувати донорські та грантові програми для часткового фінансування інфраструктури та сертифікації; також це дасть можливість співпрацювати з локальними кластерами та університетами для того, щоб формувати pipeline кадрів та програм стажувань.

Очікуваними в такому випадку будуть наступні результати: скорочення time-to-detect/ time-to-mitigate інцидентів (ціль: –30% за перші 9 міс); зниження churn на 15–25% через L&D і employer-branding; підвищення прозорості в договорах – кращі умови фінансування та менше дебіторки. (статистично підкріплено DOU [55]/BRDO [53] практиками).

Таким чином, можемо зробити висновки за результатами розгляду питання: наголосимо, що саме системний підхід може пермогти різнорівневі дії – централізований координаційний механізм плюс національний реєстр ризиків дають швидкість і видимість, необхідні для реагування в умовах масових криз; операційна готовність підприємств (BCP/ISO 22301) – найпріоритетніша внутрішньо-корпоративна дія: вона зменшує час простою і втрати, які критично важливі під час воєнних атак; кібербезпека – первинна операційна складова – CERT-UA та центри моніторингу мають стати ядром національної системи

раннього попередження; фінансова «подушка» і доступ до швидкого фінансування – державні резерви, донори та страховий ринок мають працювати як єдина екосистема підтримки; технологічні інструменти (AI, big data) – дають конкурентну перевагу: дозволяють передбачати ризики і розподіляти ресурси ефективніше; людський фактор та культура – навчання, захист і мотивування персоналу прямо впливають на стійкість.

### 3.3. Особливості управління ризиками в умовах дії воєнного стану

Зараз управління ризиками є одним з найбільш головних чинників результативного функціонування організацій. У мирний час ризики зазвичай пов'язані з коливаннями в економіці, конкуренцією на ринку, людським фактором або технічними збоями. Проте у період воєнного стану структура ризиків піддається помітним змінам: на перший план виходять загрози буквального знищення виробничих потужностей, розриву логістичних ланцюгів, втрати персоналу та великих кібератак.

Повномасштабне вторгнення в нашій державі показало, що звичні підходи до управління ризиками більше не функціонують в повній мірі. Державі та бізнесу доводиться переробляти системи реагування, створювати нові сценарії та адаптивні моделі розвитку. Зважаючи на це, ми розглянемо більш детально головні особливості управління ризиками, які формують сучасну практику в Україні в умовах воєнного стану [52]:

1. **Зростання стратегічних та операційних ризиків***:* у період війни швидко зростає непередбачуваність. Ввесь бізнес чи організація може зазнати несподіваних втрат – від пошкодження робочих місць до повного знищення будівель. Це означає, що навіть найдетальніше планування має містити кілька альтернативних сценаріїв розвитку подій [52, с. 41]. У сучасних умовах воєнного стану критично важливим стає застосування динамічного сценарного планування та адаптивних моделей. Це означає, що компанії та державні структури повинні не лише передбачати кілька альтернативних сценаріїв, а й

оперативно коригувати їх у міру надходження нових даних. Для цього використовуються регулярні аналізи ризиків, швидке оновлення прогнозів та інтеграція даних із зовнішніх джерел – від інформації про логістичні коридори до сигналів кіберзагроз. Такий підхід дозволяє максимально знизити «сліпі зони» в управлінні та швидко адаптувати бізнес-процеси до змін у воєнній обстановці, що підвищує стійкість організацій і зменшує непередбачувані втрати.

А тому, операційні та стратегічні ризики під час військових дій в країні носять багаторівневий характер. Такий момент потребує переходу від «лінійного» планування до багатосценарного підходу, коли всі рішення супроводжуються декількома варіантами запасних дій.

2. **Безперервність бізнесу як основний пріоритет***:* те, що в мирний час було на другому плані, в умовах воєнного стану стає основою управління. Бізнес-процеси мають працювати навіть у випадку відключення електроенергії, атак ворога на енергетичну інфраструктуру чи неможливості зібрати робочу команду в офісі [52, с. 42].

Отже, план безперервності бізнесу (Business Continuity Plan) у період війни стає найбільш значущим фактором виживання, оскільки він дає змогу підтримувати роботу навіть у ситуації, коли традиційні ресурси повністю недоступні.

3. **Управління кадровими ризиками***:* в умовах війни, коли в країні все нестабільно – людський ресурс став одним з найбільш вразливих аспектів. А все тому, що частина кваліфікованих кадрів мобілізована, а деяка частина – виїхала за межі країни, а також є ще люди, які не можуть працювати через втрати домівок чи сильний стрес. Тому компаніям доводиться шукати нові формати роботи з персоналом [52, с. 43].

Зважаючи на це, управління ризиками в умовах воєнного стану тісно переплітається з HR-менеджментом. Стійкість компанії напряму залежить від збереження найбільш потрібних фахівців та забезпечення умов для їхньої роботи навіть у найкризовіших обставинах.

4. **Посилення кіберзахисту:** важливо вказати, що посилені кібератаки стали ще одним фронтом війни. Кібератаки стали посиленими особливо в цей час, як і в приватних компаніях, так і державних структурах, оскільки вони стали регулярними та мають на меті заморозити роботу всіх важливих систем, викрасти секретні дані чи завдати будь-якої іншої шкоди [52, с. 44]. В умовах воєнного стану ефективним стає застосування цифрових платформ для централізованого моніторингу та прогнозування ризиків. Такого роду платформи дозволяють збирати дані про фінансові потоки, логістику, персонал, кіберзагрози та зовнішні фактори в режимі реального часу, об'єднуючи їх в єдину аналітичну систему. Завдяки штучному інтелекту та алгоритмам прогнозування можна визначати вузькі місця в операційних процесах, ранньо виявляти потенційні загрози та розподіляти ресурси ефективніше. Для українських компаній і державних структур це означає більш гнучку адаптацію до нестабільних умов, зменшення часу на реагування та підвищення ефективності прийняття рішень.

Таким чином, в теперішніх умовах кіберзахист переходить у площину стратегічного управління. Для бізнесу це означає потрібність не тільки технічного захисту, а і для побудови культури інформаційної безпеки серед всіх співробітників.

5. **Ризики логістики та фінансової стабільності:** повномасштабне вторгнення призвело до руйнування найважливіших портів та транспортних шляхів, що створило значні проблеми для імпорту та експорту в загальному. Одночасно з цим загострилися фінансові ризики – від частих змін валютного курсу до ускладнень у міжнародних розрахунках [52, с. 45].

Отже, вдале управління ризиками у фінансах та логістиці ґрунтується на диверсифікації: ні одна компанія не може дозволити собі мати не тільки один шлях постачання чи одне джерело фінансів. Охарактеризувавши детально головні особливості управління ризиками, які формують сучасну практику в нашій державі в умовах воєнного стану, вважаємо за доцільне навести приклади, а тому ми структуризували це в таблицю 3.2.

**Таблиця 3.2**

**Приклади ключових особливостей управління ризиками в умовах воєнного стану [52]**

| Особливості управління | Приклад |
|---|---|
| Зростання стратегічних та операційних | металургійні підприємства України («Азовсталь», «Запоріжсталь») стикнулися з прямими руйнуваннями, а також із заблокованими морськими портами, що зробило експорт майже неможливим. Для виживання довелося частково змінювати ринки збуту та переорієнтовуватися на сухопутні маршрути через ЄС |
| Безперервність бізнесу як основний пріоритет | IT-компанія SoftServe організувала резервні дата-центри за межами України, перевела більшість сервісів у хмару та забезпечила релокацію співробітників. Завдяки цьому навіть масовані ракетні удари та відключення світла не паралізували їхню діяльність |
| Управління кадровими ризиками | у багатьох українських компаніях з'явилися програми психологічної допомоги, підтримки внутрішньо переміщених осіб серед співробітників, а також практика гнучких графіків, що дозволяє працівникам поєднувати роботу з особистими обставинами |
| Посилення кіберзахисту | система «Дія» зазнала сотень атак, проте завдяки потужним інвестиціям у кіберзахист залишилася працездатною. Це стало важливим прикладом того, як критично важливі сервіси можна захистити навіть у період активних воєнних дій |
| Ризики логістики та фінансової стабільності | українські аграрні компанії організували нові маршрути експорту зерна через порти Румунії та Польщі, створюючи багаторівневі ланцюги постачання. Це підвищило витрати, але дозволило зберегти експортний потенціал країни |

Отже, аналіз специфіки управління ризиками в умовах повномасштабного вторгнення в нашій державі дає змогу вказати, що ризики стають непередбачуваними та багатовимірними, що потребує застосування сценарного

мислення; безперервність постає на першому плані, оскільки стабільність діяльності визначає виживання компаній; в цей час людський ресурс стає найціннішим активом, а його збереження – на компонент управління ризиками; сама кібербезпека стає не тільки технічним, а і стратегічним питанням; диверсифікація фінансових та логістичних рішень – потрібна умова для зменшення уразливості.

На основі проаналізованого досвіду передових компаній ми хочемо запропонувати власні пропозиції для ТОВ «УІТ» за умов війни:

1. «Гібридна» модель робочих локацій та безперервності: оптимальним є рішення мати хоч дві-три альтернативні локації, політику віддаленості роботи та релокаційну підтримку. Такі кейси як SoftServe показали, що релокація та multi-zone cloud тримають бізнес працюючим під ударами.

2. Міні-SOC та «кризовий штаб» для миттєвого реагування: для цього доцільно створити кризовий штаб з встановленими ролями та сценаріями; MVP-SOC для моніторингу атак і координації з CERT. Це важливо тому, що централізована координація зменшує дублювання зусиль, робить швидшою координацію з донорами і дає можливість тримати єдину картину інцидентів.

3. Страхування та фінансова «подушка»: оптимальним є формувати резервний фонд, мати певні лінії кредитування та страхувати головні ризики. Це важливо тому, що з огляду на волативність експортних доходів, фінансова стійкість дає можливість пережити періоди збитків чи платежів.

4. Система «critical roles continuity»: таке є доцільним оскільки дає можливість встановити критичні ролі, створити їх дублери та сховища знань. Саме миттєва заміна головного спеціаліста без втрати якості – життєво для проєктів у кризових ситуаціях.

5. Прозорість та швидка комунікація з клієнтами: безпосередньо шаблони кризових повідомлень, SLA-модифікації, прозора публічна інформація про статуси проєктів. Це важливо, оскільки збереження довіри знижує ризики розриву у непростих умовах.

Поєднання технічних, організаційних та фінансових заходів забезпечує повну стійкість – як показують кейси українських ІТ-лідерів та світової практики. Саме тому управління ризиками в нашій державі за умов повномасштабного вторгнення – це сукупний процес, що поєднує стратегічне мислення, людський фактор та технологічне рішення. Його специфіка у тому, що він не тільки зменшує ризик загроз, а і створює умови для розвитку та відновлення в післявоєнний період.

**Висновок до розділу 3**

Можна узагальнити, що результативне управління ризиками за сучасних умов – це не тільки компонент корпоративної стратегії, а і потрібна умова стабільності будь-якого бізнесу, особливо в умовах глобальної невизначеності та воєнних дій. Досліджені світові підходи (ISO 31000, PMBOK, PRINCE2, Agile, Scrum, BCMS, кіберзахист, культура управління ризиками) продемонстрували, що найбільш передові у світі компанії досягають високої стійкості завдяки стандартизації, системності, цифровізації та залученню персоналу до проактивного ризик-менеджменту. Даний досвід є дуже цінним для ТОВ «Українські інформаційні технології» і загалом для інших подібних, оскільки дає змогу підвищити прогнозованість, мінімізувати різнохарактерні ризики, а також підвищити довіку партнерів та клієнтів.

Визначальним є те, що українські IT-компанії потребують переходу від реактивного до проактивного управління ризиками, коли загрози не тільки фіксуються, а і передбачаються. У звітах BRDO та Lviv IT Cluster наголошується, що компанії, які впроваджують Agile-практики, системи безперервності бізнесу (BCP/ISO 22301) і внутрішні політики RM, демонструють вищу стійкість і менші втрати навіть під час активних воєнних дій.

За умов повномасштабного вторгнення управління ризиками набуває багаторівневого змісту: стратегічного, операційного, кадрового і кібернетичного. ТОВ «Українські інформаційні технології» має потенціал для інтеграції цих практик через впровадження цифрового реєстру ризиків**,** системи резервного копіювання та бізнес-континуїті**,** навчальних програм з кібергігієни, а також розвитку аналітики ризиків на основі штучного інтелекту. Зокрема, запровадження моделі «critical roles continuity» та створення «кризового штабу» дозволить підвищити керованість і швидкість реагування на загрози.

В подальшому, безпосередньо вдале поєднання міжнародних практик з національними особливостями стане основою для формування стійкості системи управління ризиками в нашій державі. Такий підхід дає змогу не тільки

результативно реагувати на кризи, а і створювати середовище сталого розвитку бізнесу у післявоєнний період.

Отже, управління ризиками за умов війни – це загальна стратегія, що поєднує цифрові інструменти, стандарти, партнерську взаємодію та людський капітал. Її вдала реалізація дає змогу таким компаніям як ТОВ «УІТ» забезпечити надійність, конкурентоспроможність та адаптивність навіть у найбільш непростих умовах.

# ВИСНОВКИ

Проведене дослідження підтвердило, що проєктний менеджмент виступає не лише технологією організації діяльності, а повноцінною управлінською парадигмою, яка поєднує стратегічні, тактичні та операційні підходи. У своїй сутності він базується на поєднанні чіткої структурованості, цілеспрямованості, інноваційності та гнучкого реагування на зміни середовища. Унікальність, обмеженість ресурсів, визначені часові рамки й етапність реалізації формують той фундамент, що дозволяє проєктним командам досягати чітко вимірюваних результатів у різних галузях сучасної економіки та соціальної практики. Дослідження понятійного апарату, класифікаційних підходів і поетапності управління засвідчило: проєктний менеджмент є універсальним і водночас адаптивним інструментом, який забезпечує системність, прогнозованість і керованість складних процесів у динамічних умовах.

Проведений комплексний аналіз особливостей діяльності ТОВ «Українські інформаційні технології» засвідчив, що дана компанія сформувала достатньо потужну та надійну систему внутрішнього управління, яка поєднує інноваційність, практичний досвід реалізації ІТ-проєктів та розвинену організаційну культуру. Її діяльність охоплює широкий спектр напрямів – від розроблення програмних продуктів і хмарних сервісів до аналітики, робототехніки та впровадження штучного інтелекту, що потребує високої узгодженості процесів та адаптивної моделі управління. Водночас правовий статус, відповідність законодавству та прозорість операційної діяльності формують довіру з боку партнерів і клієнтів, що є критичним чинником для успішності компанії на міжнародному ІТ-ринку.

Дослідження системи управління ризиками показало, що ТОВ «УІТ» застосовує комплексний підхід, поєднуючи методи мінімізації, уникнення, прийняття та перенесення ризиків. Компанія активно використовує інструменти технічного й організаційного захисту: внутрішній аудит, багаторівневий кіберзахист, страхування, сертифікацію відповідно до міжнародних стандартів

ISO та SOC, а також резервне копіювання. Проведений SWOT-аналіз дозволив окреслити сильні сторони компанії – стратегічну орієнтованість, цифровізацію, диверсифікацію діяльності та міжнародну співпрацю. Водночас визначено низку проблемних зон, серед яких значні витрати на кіберзахист, залежність від людського фактора, неповна автоматизація внутрішніх процесів і обмежене географічне охоплення.

Зовнішній контекст діяльності компанії докладно розкритий через PEST-аналіз, який підтвердив, що політичні, економічні, соціальні й технологічні чинники формують складну та мінливу систему викликів. Воєнні дії, зміни податкової політики, валютні коливання, інфляція, масова релокація бізнесів, стрімкий розвиток технологій та зростання емоційного й професійного навантаження на персонал – усе це вимагає від компанії високої адаптивності та стратегічної гнучкості.

Проведене дослідження також підтвердило важливість переходу українських IT-компаній до проактивного управління ризиками. Світові стандарти та методології – ISO 31000, PMBOK, PRINCE2, Agile, Scrum, BCMS – демонструють, що компанії, які інтегрують їх у свою діяльність, досягають значно вищої стійкості до зовнішніх загроз. Рекомендації BRDO та Lviv IT Cluster підкреслюють, що бізнеси, які формують культуру ризик-орієнтованого мислення, цифрові реєстри ризиків, сценарне планування та системи безперервності бізнесу, краще витримують вплив кризових ситуацій, включно з воєнними.

Досвід «УІТ» показує наявність потенціалу для подальшого вдосконалення: розвиток аналітичних інструментів на основі штучного інтелекту, створення кризового штабу, запровадження моделі безперервності ключових ролей, повна автоматизація контролю внутрішніх процесів, розширення географії ринку. У довгостроковій перспективі поєднання міжнародних практик зі специфікою українського ринку стане підґрунтям для створення ефективних, стійких і конкурентоспроможних систем управління ризиками в Україні.

Узагальнюючи результати роботи, можна стверджувати, що управління ризиками в умовах війни набуває стратегічного значення та стає обов'язковою умовою стабільності й розвитку ІТ-компаній. Сучасний ризик-менеджмент – це багаторівнева система, що включає цифрові інструменти, міжнародні стандарти, командну взаємодію та розвиток людського капіталу. Ефективне поєднання цих компонентів дозволяє таким компаніям, як ТОВ «Українські інформаційні технології», забезпечувати надійність, стійкість і гнучкість навіть у найбільш кризових умовах, формуючи основу для сталого та конкурентного розвитку у післявоєнний період.

# СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Балдинюк В. Ризик-менеджмент як інструмент управління діяльності суб'єктів господарювання. *Економіка та суспільство*. 2023. № 55. URL: https://doi.org/10.32782/2524-0072/2023-55-39 (дата звернення 03.05.2025).

2. Блага Н. Управління проєктами: навчальний посібник. Львів: Львівський державний університет внутрішніх справ, 2021. 152 с.

3. Воронкова В. Теоретичні і праксеологічні основи формування концепції менеджменту проєктів. *Вісник Запорізького державного інституту академічного навчання*. 2016. № 67. С. 13–21.

4. Грабина К., Шендрик В. Огляд процесів управління ризиками в IT-проєктах у контексті стандартів проєктного менеджменту. *Управління розвитком складних систем.* 2020. № 43. С. 26-32.

5. Грабіна К., Шендрик В. Метод управління ризиками IT-проєктів з урахуванням загроз та можливостей. *Менеджмент та цифрові системи*. 2023. № 3. С. 56–63.

6. Грабіна К., Шендрик В. Огляд процесів управління ризиками в IT-проєктах у контексті стандартів проєктного менеджменту. *Менеджмент та цифрові системи*. 2020. № 1. С. 78–85.

7. Гуменюк І. Роль ризик-менеджменту у забезпеченні сталого розвитку підприємства в умовах невизначеності. *Формування ринкових відносин в Україні*. 2023. № 6. С. 21–27

8. Демченко Г., Аванесова Н. Інтеграція ризик-менеджменту в загальну стратегію розвитку підприємства. *Проблеми підвищення ефективності інфраструктури*. 2024. № 1. С. 104–110.

9. Діденко О. Стратегічні аспекти управління ризиками в умовах воєнного стану. *Менеджмент підприємства*. 2023. № 3. С. 55–61.

10. Заїчко І. Стратегічний корпоративний ризик-менеджмент як основа антикризового фінансового управління підприємством. *Економічний форум Уманського державного педагогічного університету*. 2025. № 1. С. 33–39.

11. Іщенко І. Управління ризиками інвестиційних проєктів торговельних підприємств. (Дисертація на здобуття наукового ступеня кандидата економічних наук за спеціальністю 08.00.04). Полтава: Вищий навчальний заклад Укоопспілки «Полтавський університет економіки і торгівлі», 2021. 245 с.

12. Калінін О., Мосійчук Т., Дудник О. Ризик-менеджмент у контексті управління проблемними активами. *Вісник КНЕУ*. 2024. № 6. С. 59–68.

13. Кириченко А. Ризик-менеджмент: навчально-методичний посібник Одеса: Фенікс, 2024. 84 с.

14. Кириченко О. Управління ризиками інноваційних проєктів: сучасні методи та практики. *Інвестиції: практика та досвід*. 2023. № 7. С. 47–52.

15. Кірдіна О., Стешенко О. Ризик-менеджмент у страхуванні в умовах воєнного стану. *Бізнес, технології, інновації, економіка*. 2022. № 2. С. 45–52.

16. Книш І. Підготовка фахівців з управління проєктами: особливості підготовки та методики. *Управління проектами: проєктний підхід в сучасному менеджменті*: *матеріали конференції*. 2020. С. 121–124.

17. Коваленко О. Методи якісного аналізу та кількісної оцінки ризиків розробки програмного забезпечення. *Системи управління, навігації та зв'язку*. 2018. № 3. С. 116–125.

18. Коваленко С. Економічна стійкість проєктів у період воєнних загроз: ризик-орієнтований підхід. *Економіка та держав*а. 2023. № 5. С. 64–69.

19. Когут І., Сачук С. Методології управління проєктами в інформаційних технологіях, їх переваги та недоліки. *Міжнародний науковий журнал «Інтернаука». Серія: «Економічні науки».* 2022. №4. URL: https://doi.org/10.25313/2520-2294-2022-4-7957 (дата звернення 09.03.2025).

20. Козловський Є. Особливості управління проєктами в сфері туризму на основі застосування механізмів державно-приватного партнерства. *Інвестиції: практика та досвід*. 2019. № 9. С. 78–82.

21. Кульчицький І. Управління ризиками проєктів у кризових умовах. *Економіка і суспільство*. 2024. № 55. С. 72–78.

22. Левченко Т., Дудко С. Управління ризиками інноваційних та інвестиційних проєктів в Україні. *Бізнес Інформ*. 2024. № 9. С. 112–118.

23. Ляхова О. Управління ризиками в проектному менеджменті. Київ: Національний університет біоресурсів і природокористування України, 2016. С. 142–144.

24. Малик І. Система раннього попередження ризиків у проєктному менеджменті: сучасні підходи. *Інноваційна економіка*. 2021. № 2. С. 101–107.

25. Михайленко І. Система управління ризиками підприємства в умовах цифрової трансформації. *Ефективна економіка*. 2024. № 6. С. 61–70.

26. Мостова Ю. Ризик-менеджмент і забезпечення сталого розвитку підприємства. *Науковий вісник КНЕУ*. 2022. № 9. С. 112–118.

27. Нос М. Огляд сучасних методологій управління вартістю ІТ-проєктів. *Інформаційні технології та суспільство*. 2022. № 1. С. 54–60.

28. Панова Я. Управління ризиками в проектному менеджменті. Полтава: ПДАУ, 2022. С. 123–125.

29. Панова Я. Управління ризиками в проєктному менеджменті. *Наукові праці Полтавського державного аграрного університету*. 2022. № 4. С. 28–35.

30. Петренко Л. Формування системи управління ризиками проєктів у сфері ІТ. *Сучасні проблеми економіки і підприємництва*. 2024. № 53. С. 80–87.

31. Пешко М., Мельник О. Адаптація проєктного менеджменту під час ІТ-кризи 2022–2023 років. *Проблеми економіки*. 2024. №1. С. 14–19.

32. Полянська А. Теоретичні основи дослідження поняття «проєкт» («міжнародний проєкт») та вплив проєктного менеджменту на розвиток бізнесової діяльності підприємств. *Економіка, управління та адміністрування*. 2024 №107. С. 17–25.

33. Про державну реєстрацію юридичних осіб та фізичних осіб підприємців: Закон України. Відомості Верховної Ради України. 2003, № 31-32. URL: https://zakon.rada.gov.ua/laws/show/755-15#Text (дата звернення 04.06.2025).

34. Про електронні комунікації: Закон України. Відомості Верховної Ради України. 2023, № 10-11. URL: https://zakon.rada.gov.ua/laws/show/1089-20#Text (дата звернення 03.06.2025).

35. Про захист інформації в інформаційно-комунікаційних системах: Закон України. Відомості Верховної Ради України. 1994, № 31. URL: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text (дата звернення 02.06.2025).

36. Про інформацію: Закон України. Відомості Верховної Ради України. 1992, № 48. URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text (дата звернення 31.05.2025).

37. Решетняк О., Хаустов М., Юрченко О. Стратегія міжнародного маркетингу високотехнологічного стартапу. *Ефективна економіка*. 2023. № 10. URL: http://doi.org/10.32702/2307-2105.2023.10.12 (дата звернення 09.09.2025).

38. Сапич Н., Хамлика К. Проєктний менеджмент: теорія та практика застосування. Шлях успіху і перспективи розвитку*: матеріали міжнародної науково-практичної конференції (до 26-річчя Харківського національного університету внутрішніх справ)*. Харків: ХНУВС. 2020. С. 450–453.

39. Сидорук М., Григорова А. Концепція управління ризиком в IT-проєктах. *Вісник Херсонського національного технічного університету*. 2024. № 1. С. 88–95.

40. Скопенко Н., Євсєєва І., Москаленко В. Управління ризиками в проєктному менеджменті. *Вісник Національного університету харчових технологій*. 2013. № 3. С. 102–108.

41. Скопенко Н., Захарченко І. С. Методичні підходи до формування системи ризик-менеджменту. *Ефективна економіка*. 2023. № 2. URL: https://www.nayka.com.ua/index.php/ee/article/view/1141/1150 (дата звернення 01.06.2025).

42. Сметанюк О., Бондарчук А. Особливості системи управління проєктами в IT-компаніях. *Агросвіт*. 2020. № 10. С. 105–111.

43. Стандарт з управління проєктами та настанова до зводу знань з управління проєктами (настанова PMBOK). Сьоме видання. Project Management Institute, Inc, 2021. С. 122–129.

44. Статистика зовнішнього IT 2023: що насправді відбувається з вітчизняним ринком. *Укрінформ.* 07.04.2023. URL: https://www.ukrinform.ua/rubrictechnology/3692904-it-2023-so-naspravdi-vidbuvaetsa-z-vitciznanim-rinkom.html (дата звернення 25.09.2025).

45. Тарасюк Г. Розвиток проєктного менеджменту: основні методології та тренди. *Економіка. Менеджмент. Бізнес*. 2023. № 4.С. 15–22.

46. Ткачук В. Еволюція розвитку проєктного менеджменту як технології управління (огляд). *Економічний простір*. 2024. № 195. С. 117–121.

47. Трушкіна Н. Управління проєктними ризиками у системі ризик-менеджменту IT-компанії: теоретичні аспекти. *Економіка та суспільство*. 2023. № 55. С. 88-101.

48. Україна 2030Е – країна з розвинутою цифровою економікою. Український інститут майбутнього. URL: https://strategy.uifuture.org/kraina-z-rozvinutoyu-cifrovoyu-ekonomikoyu.html#6-2- 13 (дата звернення 26.09.2025).

49. Хаустова В., Решетняк О. Резильєнтність економіки: сутність і виклики для України. *Бізнес Інформ*. 2023. № 7. С. 30–41.

50. Цивільний кодекс України: Відомості Верховної Ради України. 2003, № 40-44. URL: https://zakon.rada.gov.ua/laws/show/435-15#Text (дата звернення 01.06.2025).

51. Чернега В., Клименко М. Сучасні підходи до ризик-менеджменту інвестиційних проєктів. *Молодий вчений*. 2022. № 10. С. 33–38.

52. Ярмусь Д. Ризик-менеджмент в умовах воєнного стану: адаптація моделей управління. *Вісник Херсонського національного технічного університету*. 2025. № 2. С. 41–49.

53. BRDO (Better Regulation Delivery Office). Огляд ТОП-30 українських IT-компаній. Київ: BRDO, 2023. 64 с.

54. DOU.ua. Оцінка компанії «SoftServe». Київ: DOU, 2024. URL: https://jobs.dou.ua/companies/softserve/poll/ (дата звернення 15.10.2025).

55. DOU.ua. Рейтинг IT-роботодавців України. Київ: DOU, 2024. URL: https://jobs.dou.ua/ratings/ (дата звернення 15.10.2025).

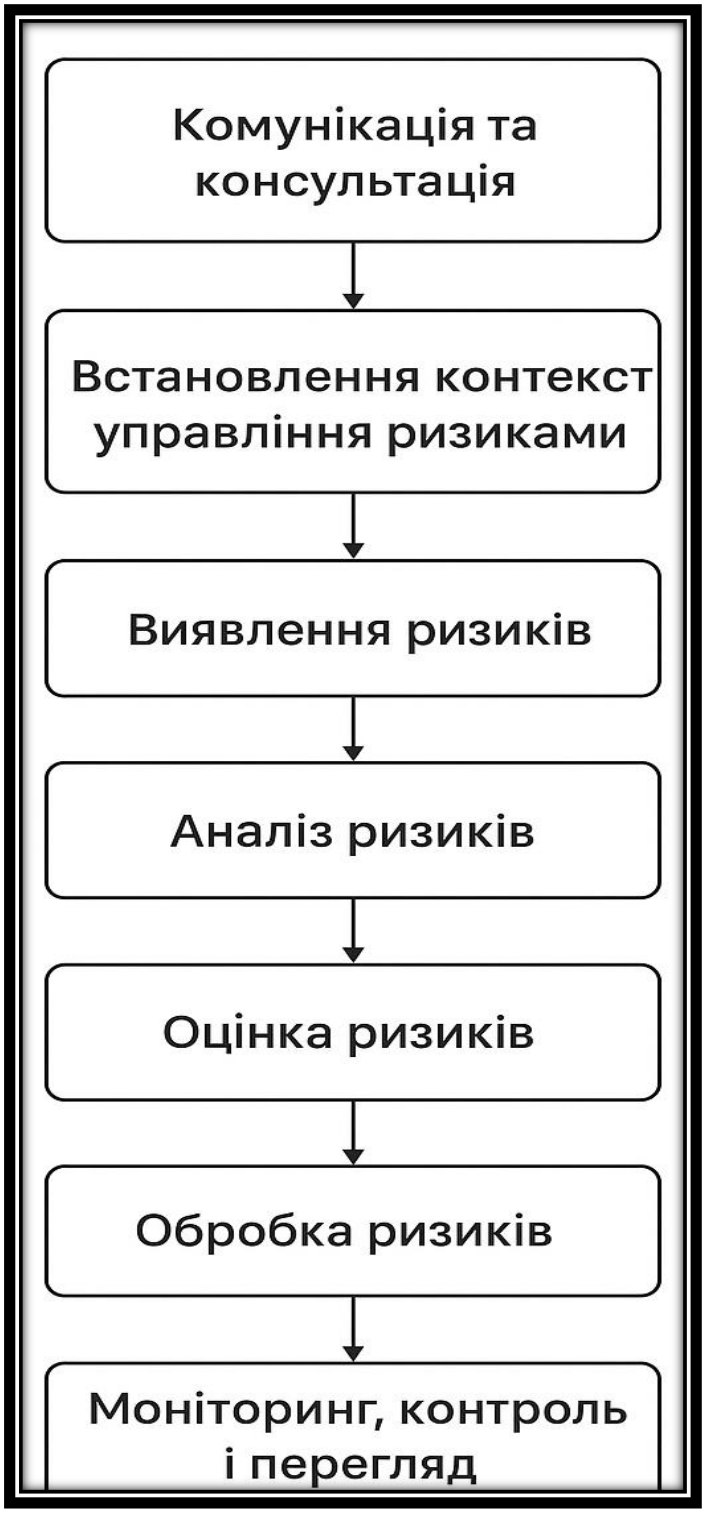
56. Lviv IT Cluster. IT Research Ukraine 2024: Стійкість як нова реальність. Львів, 2024. 75 с.

57. UIT: офіційний сайт станом на 2025. URL: http://softserveinc.com/en-us (дата звернення 01.06.2025).

# ДОДАТКИ

**Додаток А**

**Структурна схема процесу управління ризиками за стандартом ISO 31000**



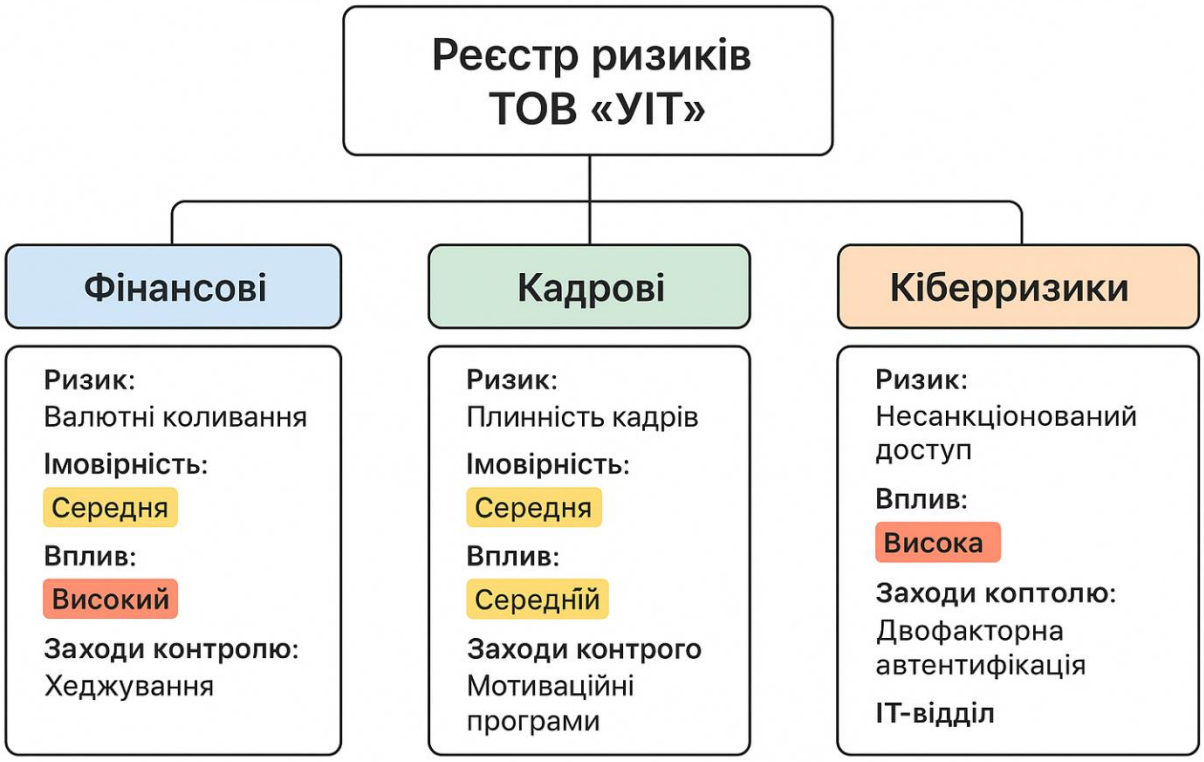
**Додаток Б**

## Матриця оцінювання ризиків (Risk Matrix) для ТОВ «УІТ»

| Ризик | Імовірність | Вплив | Рейтинг (L×I) | Пріоритет реагування |
|---|---|---|---|---|
| Зниження зовнішнього попиту та експорту ІТ-послуг | Високий | Високий | 19 | Критичний |
| Втрата ключових спеціалістів | Середня | Високий | 16 | Високий |
| Кіберзагрози та атаки | Середня | Високий | 16 | Високий |
| Емоційне вигорання та погіршення морального стану | Середня | Середній | 12 | Середній |
| Залежність від ринку США та його політико-економічної ситуації | Середня | Високий | 16 | Високий |
| Труднощі з наймом вузьких експертів | Середня | Середній | 9 | Середній |
| Мобілізація | Низька-середня | Високий | 10 | Середній |
| Податкові та регулярні зміни в Україні | Середня | Середній | 9 | Середній |
| Глобальна корекція на ринку ІТ та AI | Середня | Середній | 9 | Середній |
| Енергетичні перебої після адаптації | Середня | Середній | 6 | Низький |

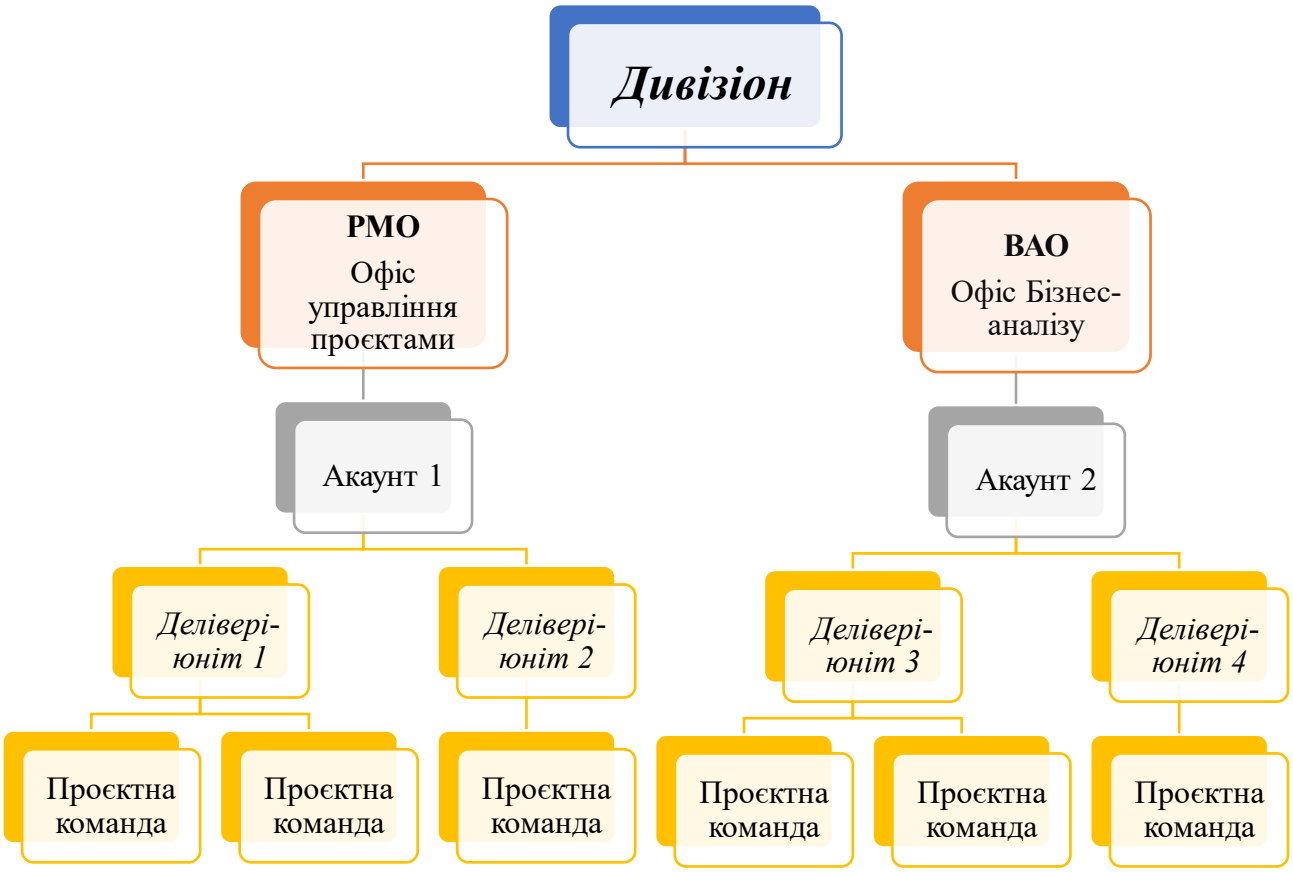
**Додаток В**

**Реєстр ризиків ТОВ «УІТ» (Risk Register)**



**Додаток Ґ**

## Схема організаційної структури ТОВ «УІТ»



**Додаток Д**

## Стратегії управління ризиками

### Перенесення

- страхування кіберризиків і активів;
- використання хмарних сервісів замість власної інфраструктури;
- залучення субпідрядників;
- використання різних контрактних моделей (FP, T&M).

### Прийняття

- допуск валютних коливань у межах 1–2%;
- прийняття дрібних затримок у реалізації проєктів;
- тимчасова заморозка перегляду зарплат (прийняття ризику демотивації)

### Диверсифікація

- найм по всьому світу;
- комбіновані послуги (консалтинг, розробка, тестування);
- диверсифікація ринків: вихід у LatAm.

### Мінімізація

- бронювання працівників (із затримкою).
- регулярне резервне копіювання, кіберзахист, навчання працівників;
- сертифікації ISO/SOC;
- BCP: автономні офіси, релокація, автономне живлення;
- закриття офісів / перехід на remote для зниження операційних ризиків, скорочення адмін персоналу

### Уникнення

- Відмова від високоризикових проєктів
- комплексна перевірка підрядників, уникнення роботи в нестабільних регіонах;
- аудит юридичної та фінансової відповідальності партнерів;
- Регулярні аудити, KPI-оцінки, моніторинг кіберзагроз;
- скорочення Junior/Middle позицій та згортання програм бенчу, щоб уникнути фінансових ризиків

**Додаток Е**

## Результати опитування працівників компанії «Українські інформаційні технології»

### *1. Вплив війни на проєкти*

| ***Рівень впливу*** | ***Кількість РМ*** | ***%*** |
|---|---|---|
| *Низький* | 0 | 0 |
| *Помірний* | 4 | 33 |
| *Високий* | 5 | 42 |
| *Критичний* | 3 | 25 |

*Примітка: 67 % респондентів оцінили вплив війни як критичний або високий*

### *2. Енергетичні ризики (блек-аути)*

| ***Показник*** | ***Так*** | ***Ні*** | ***% (так)*** |
|---|---|---|---|
| *Блек-аути вплинули на строки* | 9 | 3 | 75 |
| *Є внутрішній BCP-план* | 6 | 6 | 50 |
| *Команда забезпечена альтернативним живленням* | 6 | 6 | 50 |

### *3. Кадрові ризики*

| ***Тип ризику*** | ***Кількість згадок*** | ***% РМ*** |
|---|---|---|
| *Вигорання команди* | 9 | 75 |
| *Втрата ключових спеціалістів* | 7 | 58 |
| *Мобілізація* | 4 | 33 |
| *Труднощі з наймом* | 3 | 25 |
| *Релокація працівників* | 2 | 17 |

### *4. Оцінка корисності PE для ризик-менеджменту*

| ***Відповідь*** | ***Кількість*** | ***%*** |
|---|---|---|
| *Дуже допомагає* | 3 | 25 |
| *Частково допомагає* | 6 | 50 |
| *Слабо впливає* | 2 | 17 |
| *Не допомагає* | 1 | 8 |

***5. Внутрішні аудити***

| ***Частота*** | ***Кількість РМ*** | ***%*** |
|---|---|---|
| *Раз на пів року* | 4 | 33 |
| *Раз на рік* | 5 | 42 |
| *Рідше ніж раз у рік* | 2 | 17 |
| *Ніколи* | 1 | 8 |

***6. Використання стандартів ISO 3000/PMBOK/Agile***

| ***Стандарт*** | ***Кількість РМ*** | ***%*** |
|---|---|---|
| *PMBOK Risk Management* | 8 | 67 |
| *Agile* | 9 | 75 |
| *ISO 3000* | 3 | 25 |
| *Внутрішні корпоративні підходи* | 4 | 33 |

***7. Кадрові ризики***

| ***Кадровий ризик*** | ***Кількість згадок*** | ***РМ%*** |
|---|---|---|
| *Емоційне вигорання та погіршення морального стану (тривога, страх мобілізації, неможливість виїзду за кордон тощо)* | 10 | 83 |
| *Втрата ключових спеціалістів (мобілізація, релокація, зміна пріоритетів, тощо)* | 7 | 58 |
| *Ризик мобілізації як окремий фактор (часткове бронювання тощо)* | 5 | 42 |
| *Труднощі з наймом вузьких експертів* | 4 | 33 |
| *Перенавантаження менеджерів і команди через оптимізацію ресурсів* | 4 | 33 |

*Примітка: 12 респондентів – дані узгоджені*

***8. Оцінка корисності***

| ***Відповідь*** | ***Кількість*** | ***%*** |
|---|---|---|
| *Дуже допомагає* | 2 | 17 |
| *Частково допомагає* | 6 | 50 |
| *Слабо впливає* | 3 | 25 |
| *Не допомагає* | 1 | 8 |

***9. Корисність внутрішніх аудитів***

| ***Оцінка*** | ***Кількість РМ*** | ***%*** |
|---|---|---|
| *Дуже корисні* | 2 | 17 |
| *Корисні* | 7 | 58 |
| *Малокорисні* | 2 | 17 |
| *Не бачу користі* | 1 | 8 |

*Примітка: більшість опитаних респондентів вважають аудит корисним; багато зазначило, що впровадження рекомендацій часто ускладнюється через перенавантаження менеджерів*

***10. Застосування стандартів***

| ***Стандарт*** | ***Кількість РМ*** | ***%*** |
|---|---|---|
| *PMBOK Risk Management* | 9 | 75 |
| *Agile* | 8 | 67 |
| *ISO 3000* | 3 | 25 |
| *Внутрішні корпоративні підходи* | 4 | 33 |