Міністерство освіти і науки України

Харківський національний університет радіоелектроніки

Факультет Комп'ютерних наук
(повна назва)

Кафедра Інформаційних управляючих систем
(повна назва)

КВАЛІФІКАЦІЙНА РОБОТА
Пояснювальна записка

рівень вищої освіти другий (магістерський)

Дослідження стратегій прийняття управлінських рішень з управління IT-проєктом в умовах конфлікту

(тема)

Виконав:
здобувач 2 року навчання,
групи УПГІТм-23-2
Даниїл БУРЯК
(власне ім'я, прізвище)

Спеціальність 122 Комп'ютерні науки
(код і повна назва спеціальності)

Тип програми освітньо-наукова
(освітньо-професійна або освітньо-наукова)

Освітня програма Управління проєктами в галузі IT
(повна назва освітньої програми)

Керівник: проф. каф. ІУС Максим ЄВЛАНОВ
(посада, власне ім'я, прізвище)

Допускається до захисту

Зав. кафедри ІУС _____ Костянтин ПЕТРОВ
(підпис) (власне ім'я, прізвище)

2025 р.

Харківський національний університет радіоелектроніки

Факультет Комп'ютерних наук

Кафедра Інформаційних управляючих систем

Рівень вищої освіти другий (магістерський)

Спеціальність 122 Комп'ютерні науки
(код і повна назва)

Тип програми освітньо-наукова
(освітньо-професійна або освітньо-наукова)

Освітня програма Управління проєктами в галузі інформаційних технологій
(повна назва)

ЗАТВЕРДЖУЮ:
Зав. кафедри _____
(підпис)
" 21 " квітня 20 25 р.

ЗАВДАННЯ

НА КВАЛІФІКАЦІЙНУ РОБОТУ

здобувачеві Буряку Даниїлу Вікторовичу
(прізвище, ім'я, по батькові)

1. Тема роботи Дослідження стратегій прийняття управлінських рішень з управління ІТ-проєктом в умовах конфлікту

затверджена наказом по університету від " 28 " березня 2025 р. № 235Ст

2. Термін подання здобувачем роботи до екзаменаційної комісії " 05 " червня 2025 р.

3. Вихідні дані до роботи Науково-технічні публікації та інтернет-джерела з тематики атестаційної роботи; емпіричний досвід українських ІТ-компаній, отриманий шляхом напівструктурованих інтерв'ю; принципи системного мислення, кібернетичного управління та антикрихкості.

4. Перелік питань, що потрібно опрацювати у роботі
Вступ; аналіз еволюції управлінських підходів в ІТ-проєктах від класики до адаптивних стратегій та їхніх обмежень у кризових умовах; ідентифікація та систематизація ризиків, невизначеностей та викликів воєнного часу для ІТ-проєктів та їхній кумулятивний ефект; розробка концептуальної моделі адаптивного управління ІТ-проєктами: архітектура, ключові принципи та механізми; формулювання практичних рекомендацій для забезпечення ситуаційної обізнаності, підвищення стійкості, людиноцентричного управління та безперервного навчання; проведення апробації концептуальної моделі та оцінка її ефективності й отриманих переваг; висновки.

КАЛЕНДАРНИЙ ПЛАН

№	Назва етапів роботи	Термін виконання етапів роботи	Примітка
1	Змістовна постановка задачі призначення пакетів робіт командам виконавців ІТ-проєкту	21.04.2025 - 25.04.2025	Виконано
2	Аналіз існуючих управлінських підходів	25.04.2025 – 29.04.2025	Виконано
3	Остаточна доробка та верифікація Розділу 1: “Еволюція управлінських підходів в ІТ-проєктах”	29.04.2025 – 02.05.2025	Виконано
4	Обробка впливу конфлікту на середу управління ІТ-проєктів	03.05.2025 – 08.05.2025	Виконано
5	Остаточна доробка та верифікація Розділу 2: “Вплив воєнного конфлікту на ІТ-проєкти”	08.05.2025 – 15.05.2025	Виконано
6	Розробка концептуальної моделі та її принципів	16.05.2025 – 20.05.2025	Виконано
7	Опис і формалізація моделі	20.05.2025 – 22.05.2025	Виконано
8	Формулювання практичних рекомендацій	22.05.2025 – 25.05.2025	Виконано
9	Проведення апробації моделі	25.05.2025 – 27.05.2025	Виконано
10	Аналіз результатів апробації моделі	27.05.2025 – 29.05.2025	Виконано
11	Збір та фіналізація основного тексту пояснювальної записки	29.05.2025	Виконано
12	Захист	05.06.2025	

Дата видачі завдання 21 квітня 2025 р.

Здобувач _____
(підпис)

Керівник роботи _____ проф. каф. ІУС Максим ЄВЛАНОВ
(підпис) (посада, власне ім’я, прізвище)

РЕФЕРАТ

Пояснювальна записка кваліфікаційної роботи: 110 с., 2 рис., 3 табл., 2 дод., 40 джерел.

АДАПТИВНІ СТРАТЕГІЇ, ВОЄННИЙ КОНФЛІКТ, ДЕЦИЗІЙНІ ПРОЦЕСИ, ІТ-ПРОЄКТИ, КОНЦЕПТУАЛЬНА МОДЕЛЬ, КРИЗОВІ УМОВИ, ЛЮДИНОЦЕНТРИЧНЕ УПРАВЛІННЯ, НЕВИЗНАЧЕНІСТЬ, РИЗИКИ, СТІЙКІСТЬ.

Об’єктом дослідження кваліфікаційної роботи є процеси управління ІТ-проєктами в умовах підвищеної невизначеності та кризових викликів.

Метою даної кваліфікаційної роботи є розробка та обґрунтування концептуальної моделі адаптивного управління ІТ-проєктами в умовах воєнного конфлікту, спрямованої на підвищення їх стійкості, ефективності та зниження ризиків.

В роботі проведено системний аналіз класичних та адаптивних методологій управління проєктами, а також методів прийняття рішень, виявлено їхні обмеження в екстремальних умовах. Дослідження базувалося на зборі та аналізі емпіричного досвіду українських ІТ-компаній, отриманого шляхом напівструктурованих інтерв'ю. Запропонована концептуальна модель розроблена з використанням принципів системного мислення, кібернетичного управління та антикрихкості.

Систематизовано та проаналізовано ключові категорії ризиків та невизначеностей (кадрові, інфраструктурні, фінансові, кібербезпекові, операційні), що впливають на ІТ-проєкти в умовах воєнного конфлікту. Розроблено архітектуру моделі, яка складається з п'яти взаємопов'язаних модулів (моніторингу середовища, оцінки стійкості та адаптивності, прийняття рішень, реалізації та контролю, зворотного зв'язку та безперервного

навчання), та кількісні показники для їх оцінки. Сформульовано практичні рекомендації щодо застосування адаптивних стратегій, які були апробовані в умовах реальної ІТ-компанії, демонструючи значне підвищення ситуаційної обізнаності, зниження хаосу та покращення психологічного клімату в команді.

Новизна дослідження полягає у розробці цілісної концептуальної моделі адаптивного управління ІТ-проєктами, що вперше системно інтегрує принципи стійкості, динамічної адаптації та людиноцентричності, враховуючи унікальний український досвід функціонування в умовах тривалого воєнного конфлікту.

ABSTRACT

Master’s tesis 110 pages, 2 figures, 3 tables, 2 appendices, 40 sources.

ADAPTIVE STRATEGIES, CONCEPTUAL MODEL, CRISIS CONDITIONS, DECISIONAL PROCESSES, HUMAN-CENTERED MANAGEMENT, IT PROJECTS, MILITARY CONFLICT, RISKS, SUSTAINABILITY, UNCERTAINTY.

The object of research of the qualification work is the processes of IT project management in conditions of increased uncertainty and crisis challenges.

The purpose of this qualification work is to develop and substantiate a conceptual model of adaptive IT project management in the context of military conflict aimed at increasing their sustainability, efficiency and risk reduction.

The study conducted a systematic analysis of classical and adaptive project management methodologies, as well as decision-making methods, and identified their limitations in extreme conditions. The study was based on the collection and analysis of empirical experience of Ukrainian IT companies obtained through semi-structured interviews. The proposed conceptual model was developed using the principles of systems thinking, cyber governance, and anti-fragility.

The key categories of risks and uncertainties (human, infrastructure, financial, cybersecurity, operational) affecting IT projects in the context of military conflict are systematized and analyzed. The architecture of the model, which consists of five interrelated modules (environmental monitoring, resilience and adaptability assessment, decision-making, implementation and control, feedback and continuous learning), and quantitative indicators for their evaluation are developed. Practical recommendations for the application of adaptive strategies have been formulated and tested in a real IT company, demonstrating a significant increase in situational awareness, reduction of chaos, and improvement of the psychological climate in the

team.

The novelty of the study lies in the development of a holistic conceptual model of adaptive IT project management, which for the first time systematically integrates the principles of sustainability, dynamic adaptation and human-centeredness, taking into account the unique Ukrainian experience of functioning in the context of a protracted military conflict.

ЗМІСТ

СКОРОЧЕННЯ ТА УМОВНІ ПОЗНАКИ

ВДК — відсоток доступності команди

ВППП — відсоток персоналу, що потребує психологічної підтримки

ВПЗ — відсоток проєктів із затримками

ІНБД — індекс наближення бойових дій

ІІВ — інфраструктурний індекс впливу

ІКВ — індекс кадрового впливу

ІКЗ — індекс кіберзагрози

ІОВ — індекс операційного впливу

ККА — кількість виявлених кібератак на тиждень

КЗРВ — кількість запитів на ревізію вимог/скоупу

КЗЗ — кількість збоїв інтернет-зв’язку (кількість/день)

ПКС — показники кадрового стану

ПФОВ — показники фінансово-операційного впливу

СПБ — середнє перевищення бюджету (у відсотках)

СІСК — середній індекс стресу команди

СЧВВ — середній час виявлення вразливостей (години)

ТБ — середня тривалість відключень електроенергії (години/день)

ТЗЗ — тривалість збоїв інтернет-зв’язку (години/день)

ЧБ — частота відключень електроенергії (кількість/день)

ЧРКІ — час реагування на критичні інциденти (години)

ВСТУП

Управління ІТ-проєктами, що є критично важливим для створення унікальних продуктів у динамічному та складному середовищі, традиційно стикається з викликами через нематеріальну природу результатів, мінливість вимог та людський фактор. Проте, в умовах повномасштабного воєнного конфлікту в Україні, ця динаміка трансформувалася в безпрецедентну невизначеність, роблячи класичні, передбачувані підходи неефективними. Хоча адаптивні методології пропонують гнучкість, все ще бракує цілісної моделі, яка б системно інтегрувала стратегії реагування на тотальну невизначеність, враховувала унікальний досвід української ІТ-галузі та адекватно вирішувала питання психологічної стійкості команди в екстремальних умовах.

Актуальність даного дослідження зумовлена стратегічною важливістю української ІТ-галузі для економічної стійкості країни та її майбутнього відновлення в умовах триваючого, високо-невизначеного воєнного конфлікту. Існуючі управлінські парадигми виявилися недостатніми для ефективного функціонування в середовищі, де ризики кумулятивно посилюються (від фізичної безпеки персоналу та інфраструктурних збоїв до фінансового тиску та кібератак), а зовнішні шоки є постійними та непередбачуваними. Розробка та впровадження адаптивних стратегій є не просто бажаною практикою, а життєвою необхідністю для забезпечення безперервності бізнесу, збереження кадрового потенціалу та здатності до інновацій. Це дослідження має на меті не лише подолати виявлені дослідницькі прогалини, а й надати практичні інструменти для підвищення антикрихкості ІТ-проєктів, сприяючи їх виживанню та розвитку в найскладніших умовах та формуючи цінні уроки для міжнародного досвіду управління кризовими проєктами.

Метою кваліфікаційної роботи є розробка та наукове обґрунтування цілісної, людиноцентричної концептуальної моделі (фреймворку) адаптивних

стратегій прийняття управлінських рішень в ІТ-проєктах, що функціонують в умовах повномасштабного воєнного конфлікту. Ця модель має забезпечити системний підхід до управління в умовах максимальної невизначеності, інтегруючи принципи ситуаційної обізнаності, стійкості «за замовчуванням», динамічної адаптації та безперервного навчання для підвищення життєздатності, ефективності та здатності до трансформації ІТ-проєктів, а також мінімізації кумулятивних ризиків.

Для досягнення поставленої мети необхідно вирішити наступні задачі:

– поглибити аналіз теоретичних підходів та емпіричного досвіду управління ІТ-проєктами в умовах воєнного конфлікту, оцінивши їхню застосовність та обмеження;

– ідентифікувати та систематизувати ключові фактори впливу воєнного конфлікту на управління ІТ-проєктами (ризики, невизначеності, виклики), з особливою увагою до їхнього кумулятивного ефекту;

– розробити концептуальну модель (фреймворк) адаптивних стратегій прийняття управлінських рішень в ІТ-проєктах, що враховує специфіку кризових умов, включаючи механізми моніторингу, оцінки стійкості, прийняття рішень та безперервного навчання;

– сформулювати практичні рекомендації для ІТ-менеджерів та керівників компаній щодо застосування розробленої моделі/фреймворку, акцентуючи на людиноцентричному підході та підтримці команди;

– провести апробацію розробленої концептуальної моделі/фреймворку на конкретному прикладі (кейс-стаді або симуляція) для демонстрації її потенційної ефективності та практичної цінності.

Об'єктом дослідження є динамічний, людиноцентричний та багаторівневий процес управління ІТ-проєктами, що функціонують в умовах екстремальної невизначеності, постійних загроз та кумулятивних ризиків, спричинених повномасштабним воєнним конфліктом.

Предметом дослідження є сукупність адаптивних, гнучких та стійких стратегій, а також розроблена концептуальна модель прийняття управлінських

рішень, яка передбачає системну інтеграцію принципів ситуаційної обізнаності, міцності «за замовчуванням», динамічної адаптації, людиноцентричності та безперервного навчання для забезпечення життєздатності, ефективності та здатності до трансформації ІТ-проєктів в умовах воєнної агресії.

Кваліфікаційна робота виконана відповідно до вимог методичних вказівок з організації та виконання кваліфікаційної роботи та національних стандартів України.

1 ЕВОЛЮЦІЯ УПРАВЛІНСЬКИХ ПІДХОДІВ В ІТ-ПРОЄКТАХ: ВІД КЛАСИКИ ДО АДАПТИВНИХ СТРАТЕГІЙ В УМОВАХ НЕВИЗНАЧЕНОСТІ

1.1 Сутність та ключові характеристики управління ІТ-проєктами

Управління проєктами є фундаментальною дисципліною, яка забезпечує успішну реалізацію тимчасових зусиль, спрямованих на створення унікальних продуктів, послуг або результатів. В епоху тотальної цифровізації та інновацій, управління проєктами в галузі інформаційних технологій (ІТ) набуває особливого значення, стаючи рушійною силою прогресу та конкурентоспроможності в сучасному світі. На відміну від проєктів у традиційних галузях, таких як будівництво чи виробництво, ІТ-проєкти мають низку унікальних характеристик, що зумовлюють специфіку їхнього планування, виконання, моніторингу та, що найважливіше, процесів прийняття управлінських рішень [1], [7], [38].

За своєю суттю, ІТ-проєкт визначається як тимчасове підприємство, спрямоване на створення нового або вдосконалення існуючого програмного забезпечення, апаратного забезпечення, мережевої інфраструктури, систем інтеграції чи інших цифрових рішень. Прикладами можуть бути розробка мобільного застосунку, впровадження корпоративної ERP-системи, міграція даних у хмарне середовище, розгортання систем кібербезпеки або створення аналітичних платформ. Кожен ІТ-проєкт обмежений у часі та ресурсах, має чітко визначені цілі та вимоги, а його успіх прямо залежить від ефективності управлінських рішень, що приймаються протягом його життєвого циклу [1].

Однією з найбільш виразних рис ІТ-проєктів є нематеріальна природа їхніх результатів. На відміну від фізичних об'єктів (будівель, автомобілів), основними кінцевими продуктами в ІТ є програмний код, конфігурації систем, архітектурні рішення, бази даних та інші логічні компоненти. Ця особливість ускладнює візуалізацію прогресу, вимірювання якості та контроль за

виконанням, вимагаючи специфічних підходів до метрик та звітності. Крім того, наявність багатьох взаємозалежних компонентів, часто розподілених та інтегрованих з численними сторонніми сервісами, створює високий ступінь складності. Зміна в одному компоненті або вибір певної технології може мати неочевидні та далекосяжні наслідки для інших частин системи (ефект метелика), що вимагає від менеджерів системного мислення та здатності передбачати побічні ефекти своїх рішень [5].

Ще однією ключовою характеристикою є надзвичайна динамічність технологічного ландшафту та постійна еволюція вимог. IT-сфера характеризується безпрецедентною швидкістю змін: нові фреймворки, мови програмування, інструменти та парадигми з'являються та швидко змінюються. Водночас ринкові умови та потреби користувачів також швидко еволюціонують, що змушує проєктні команди постійно адаптуватися та коригувати плани. Ця висока невизначеність, яка є невід'ємною частиною IT-проєктів навіть у мирний час, ускладнює точне планування та довгострокове прогнозування. Менеджерам часто доводиться приймати рішення в умовах неповної або швидко застаріваючої інформації, що підвищує важливість гнучких, ітеративних підходів та здатності до швидкого реагування [18].

Нарешті, людський фактор відіграє величезну роль в IT-проєктах. Успіх проєкту значною мірою залежить від професіоналізму, злагодженості та мотивації членів команди. Сучасні IT-команди часто є розподіленими (члени працюють з різних міст і країн), крос-функціональними (об'єднують фахівців різного профілю) та працюють у гібридних форматах. Ефективна комунікація, співпраця та підтримка командного духу є критично важливими для досягнення спільного розуміння та прийняття узгоджених рішень. Це вимагає від менеджерів не лише технічних знань, але й розвинених навичок емпатії, кризової комунікації та управління стресом [19].

Ці фундаментальні характеристики IT-проєктів – нематеріальність, динамічність, складність та людськоцентричність – створюють унікальне середовище для управління. Вони пояснюють, чому IT-проєкти навіть у

стабільних умовах стикаються з типовими викликами, такими як розповзання обсягу (scope creep), перевищення бюджету та термінів, брак кваліфікованих кадрів, технічний борг та кібератаки. Розуміння цих базових аспектів є відправною точкою для подальшого аналізу того, як ці виклики трансформуються та посилюються в умовах екстремальної невизначеності, породженої воєнним конфліктом, що стане предметом наступних розділів цієї роботи [36].

1.2 Огляд основних методологій управління проєктами

Управління IT-проєктами, з його унікальними характеристиками та викликами, вимагає застосування структурованих підходів – методологій, які допомагають командам організовувати роботу, координувати зусилля та досягати поставлених цілей. Історично склалося, що ці методології еволюціонували від жорстких, послідовних моделей до більш гнучких та адаптивних, що відповідає зростаючій динамічності та невизначеності IT-сфери. Розуміння цих підходів є критично важливим для подальшого аналізу їхньої ефективності в екстремальних умовах.

Існуючі методології управління проєктами можна узагальнено класифікувати за їхньою природою та гнучкістю. Виділяють три основні групи:

– класичні (традиційні) методології. Характеризуються лінійним, послідовним підходом до виконання проєкту;

– адаптивні (гнучкі) методології. Виникли як відповідь на потребу у більшій гнучкості та швидкості реагування на зміни;

– гібридні методології. Поєднують елементи класичних та адаптивних підходів, щоб оптимізувати управління в складних проєктах.

Кожна з цих груп має свої унікальні принципи, переваги та недоліки, які

роблять їх більш чи менш придатними для різних типів проєктів та умов їх реалізації.

1.2.1 Класичні (традиційні) методології

Класичні методології, часто називані каскадними або послідовними (Waterfall), домінували в управлінні проєктами протягом багатьох десятиліть, особливо в галузях з чітко визначеними вимогами та передбачуваними процесами. Їхня основна ідея полягає в лінійному, поетапному проходженні проєкту, де кожен наступний етап починається лише після повного завершення попереднього. Цей підхід забезпечує високий рівень контролю, деталізоване планування на початку та чітку документацію.

Модель Waterfall (Водоспадна модель) є найвідомішим прикладом класичної методології. Вона передбачає суворо послідовне виконання фаз: збір і аналіз вимог, проєктування, реалізація (кодування), тестування, розгортання та підтримка. Кожна фаза має чіткі входи та виходи, і перехід до наступної можливий лише після затвердження результатів попередньої.

PMBOK (Project Management Body of Knowledge), хоча й не є методологією в чистому вигляді, а скоріше збіркою стандартів, керівних принципів та найкращих практик управління проєктами, є основоположним для багатьох традиційних підходів. PMBOK описує 10 областей знань та 5 груп процесів, надаючи всебічний інструментарій для управління [1].

Класичні методології добре працюють для проєктів з високою стабільністю вимог, невеликою невизначеністю та чітко визначеними технологічними рішеннями. Однак у сучасній IT-сфері, де зміни є нормою, а ринкові умови постійно еволюціонують, їхня ефективність часто знижується. Переваги та недоліки класичних методологій управління проєктами наведено у табл. 1.1.

Таблиця 1.1 – Переваги та недоліки класичних методологій управління проєктами

Критерій	Переваги	Недоліки
Структура та контроль	Чітка, лінійна структура проєкту; Легкість контролю прогресу; Деталізоване планування на початкових етапах.	Низька гнучкість до змін вимог; Труднощі з адаптацією на пізніх етапах.
Документація	Висока якість та повнота документації; Чіткі входи та виходи для кожної фази.	Надмірна бюрократія; Високі вимоги до попереднього збору вимог.
Зворотний зв'язок	Передбачуваність витрат і термінів за стабільних вимог.	Відсутність раннього зворотного зв'язку від замовника; Ризик невідповідності кінцевого продукту.
Виявлення проблем		Виявлення помилок та проблем лише на етапі тестування або пізніше.
Застосування	Ідеально для проєктів зі стабільними та чітко визначеними вимогами.	Неефективні в умовах високої невизначеності та частих змін.
Ресурси		Можуть бути надмірно витратними в плані ресурсів та часу для невеликих проєктів.

1.2.2 Адаптивні (гнучкі) методології

Адаптивні методології, відомі як Agile, виникли як відповідь на недоліки традиційних підходів в умовах швидких змін та високої невизначеності, характерних для IT-сфери. Їхня філософія базується на цінностях та принципах, викладених в Agile-Маніфесті (2001 рік), що акцентують увагу на індивідах та взаємодії, працюючому програмному забезпеченні, співпраці з замовником та реагуванні на зміни. Адаптивні методології передбачають ітеративний та інкрементальний розвиток продукту, гнучкість до змін та постійний зворотний зв'язок [2].

Scrum є одним з найпопулярніших фреймворків у рамках Agile. Він організує роботу в коротких, фіксованих за часом ітераціях, званих спринтами (зазвичай 1-4 тижні). Кожен спринт має чітко визначені цілі, і команда працює над ітерацією продукту. Ключові ролі (власник продукту, скрам-майстер, команда розробки) та процедури (планування спринту, щоденний скрам, огляд спринту, ретроспектива спринту) забезпечують прозорість, адаптацію та безперервне вдосконалення [2].

Kanban – це методологія, що фокусується на візуалізації робочого потоку, обмеженні незавершеної роботи (Work in Progress) та безперервному постачанні. Робота організовується на Kanban-дошці з колонками, що представляють етапи робочого процесу. Елементи роботи (картки) рухаються по дошці, і їхній прогрес відстежується. Головна мета – оптимізувати потік, зменшити час циклу та підвищити пропускну здатність [4]. Переваги та недоліки адаптивних (гнучких) методологій управління проєктами наведено у табл. 1.2.

Таблиця 1.2 – Переваги та недоліки адаптивних (гнучких) методологій управління проєктами

Критерій	Переваги	Недоліки
Гнучкість та адаптація	Висока гнучкість до змін вимог;	Може бути складно застосувати у великих, сильно регульованих проєктах.
	Швидка адаптація до нових умов.	
Поставка продукту	Швидка та часта поставка працюючого продукту; Раннє виявлення проблем та їх вирішення.	Менша передбачуваність довгострокових термінів та бюджету на початку.
Зворотний зв'язок	Постійний зворотний зв'язок від замовника; Прозорість прогресу для всіх стейкхолдерів.	Вимагає високої зрілості команди та активної участі замовника.
Командна робота	Підвищення мотивації та самоорганізації команди; Тісна співпраця всередині команди та із замовником.	
Застосування	Ідеально для проєктів з високою невизначеністю, мінливими вимогами, інноваційних проєктів.	Може бути менш структурованим та менш підходить для жорстких контрактів.
Документація		Менший акцент на формальній документації, що може бути викликом для аудиту.

1.2.3 Гібридні методології

Зростаюча складність та різноманітність проєктів у сучасній ІТ-індустрії призвели до появи гібридних підходів. Ці методології прагнуть поєднати переваги як класичних, так і адаптивних моделей, щоб максимізувати ефективність управління в умовах, які не ідеально підходять для жодного з чистих підходів. Гібридні методології дозволяють проєкту адаптуватися до різних частин свого життєвого циклу або до різних компонентів, де вимоги до стабільності та гнучкості можуть відрізнятися [37].

Наприклад, для великого, довгострокового проєкту може використовуватися Waterfall-підхід на початкових етапах збору високорівневих вимог та архітектурного проєктування, де потрібна чітка структура та повна документація. Водночас, для етапів детальної розробки та реалізації окремих модулів, де очікуються зміни та потрібна швидка поставка, застосовуються Agile-фреймворки (наприклад, Scrum або Kanban). Це дозволяє поєднати стабільність та передбачуваність стратегічного планування з гнучкістю та швидкістю реагування на операційному рівні. Іншим прикладом є використання елементів Kanban для візуалізації та управління потоком у команді, яка працює за Scrum-спринтами.

Гібридні методології надають менеджерам проєктів інструменти для створення індивідуалізованих підходів, що найкраще відповідають унікальному контексту кожного проєкту, його вимогам, команді та зовнішньому середовищу. Це дозволяє оптимізувати процеси, мінімізувати ризики та забезпечити більш успішне досягнення цілей. Переваги та недоліки гібридних методологій управління проєктами наведено у табл. 1.3.

Таблиця 1.3 – Переваги та недоліки гібридних методологій управління проєктами

Критерій	Переваги	Недоліки
Адаптивність та гнучкість	Оптимальна адаптація до різної природи частин проєкту; Баланс між контролем та гнучкістю.	Складність впровадження та управління, вимагає ретельної інтеграції.
Планування та передбачуваність	Поєднання передбачуваності на високому рівні з гнучкістю на детальному рівні.	Необхідність чіткого розмежування зон застосування різних підходів.
Оптимізація ресурсів	Можливість використовувати найкращі практики з різних методологій; Ефективне використання ресурсів у залежності від фази проєкту.	Вимагає висококваліфікованих менеджерів, які розуміють обидва типи методологій.
Якість продукту	Здатність інтегрувати переваги обох підходів для підвищення якості та відповідності вимогам.	
Застосування	Ідеально для великих, складних проєктів з мінливими та стабільними частинами; Проєкти з гібридними вимогами.	Потенційна складність комунікації та координації між різними моделями роботи.
Адаптивність та гнучкість	Оптимальна адаптація до різної природи частин проєкту; Баланс між контролем та гнучкістю.	Складність впровадження та управління, вимагає ретельної інтеграції.

1.3 Аналіз класичних методів прийняття управлінських рішень та їхніх обмежень у кризових умовах

Управлінські рішення в IT-проєктах можуть бути класифіковані за рівнем впливу (стратегічні, тактичні, операційні) та горизонтом планування, охоплюючи широкий спектр виборів від вибору технологічного стеку до щоденного пріоритизації завдань. Для підтримки цих рішень тривалий час активно використовувалися класичні аналітичні інструменти, розроблені для умов стабільності та передбачуваності. Вони базуються на раціональному підході, що передбачає наявність повної інформації, чітких цілей та можливість оцінки всіх можливих альтернатив. Однак, в умовах екстремальної невизначеності, породженої воєнним конфліктом, ці методи виявляють значні обмеження.

SWOT-аналіз, який дозволяє ідентифікувати сильні та слабкі сторони організації (внутрішні фактори), а також можливості та загрози зовнішнього середовища, традиційно застосовується для формулювання стратегій. В IT-сфері він може бути корисним для оцінки конкурентних переваг нового продукту або аналізу готовності команди до складного завдання. Проте в умовах війни його цінність суттєво обмежується. Швидка зміна реалій робить результати SWOT-аналізу застарілими майже миттєво, вимагаючи постійного, майже безперервного перегляду. Об'єктивна оцінка всіх факторів в атмосфері хаосу та емоційного напруження стає вкрай складною, що знижує його достовірність як інструменту для глибокого стратегічного планування, перетворюючи його скоріше на засіб швидкої фіксації поточного стану [12].

Аналогічні обмеження стосуються і PESTLE-аналізу, що використовується для структурованого вивчення ключових макросередовищних факторів: політичних, економічних, соціальних, технологічних, правових та екологічних. В мирний час він допомагає прогнозувати тенденції та оцінювати потенційні ризики. Однак під час війни,

коли політична нестабільність, економічна руйнація, масова міграція та постійні кібератаки змінюються з надзвичайною волатильністю, прогностична цінність PESTLE-аналізу прямує до нуля. Збір достовірної та актуальної інформації щодо кожного аспекту стає майже неможливим, а динамічність цих факторів вимагає постійного моніторингу та швидкого реагування, що не відповідає статичній природі цього інструменту [11].

Дерево рішень – графічна модель, що візуалізує послідовність рішень, можливі випадкові події з відповідними ймовірностями та їхні фінансові результати – є корисним інструментом для вибору варіантів дій з урахуванням ризиків. Проте ефективність цього методу критично залежить від здатності адекватно оцінити ймовірності настання подій. В умовах війни, коли тривалість бойових дій, інтенсивність обстрілів, успішність військових операцій чи тривалість блекаутів є абсолютно непередбачуваними, присвоєння точних або навіть приблизних ймовірностей стає спекулятивним. Це позбавляє дерево рішень математичної обґрунтованості, перетворюючи його на якісний інструмент для структурування мислення, але не для об'єктивного вибору оптимального шляху [17].

Аналіз витрат та вигод (Cost-Benefit Analysis, CBA), що передбачає систематичне порівняння очікуваних витрат та вигод від певного рішення чи проєкту, є важливим для обґрунтування інвестицій. В IT-проєктах він застосовується для оцінки рентабельності впровадження систем або закупівлі ПЗ. Однак в умовах війни кількісна оцінка багатьох факторів стає вкрай складною. Нематеріальні вигоди, такі як безпека персоналу чи репутація, важко виміряти. Витрати ускладнюються інфляцією, логістичними проблемами та непередбачуваністю цін. Тому CBA може застосовуватися лише з великою обережністю, фокусуючись на найбільш очевидних аспектах та усвідомлюючи значні обмеження точності розрахунків [13].

Загальні обмеження класичних методів у рамках воєнного конфлікту:

– надмірна залежність від стабільності та передбачуваності. Класичні методи розроблені для умов, де зовнішнє середовище є відносно стабільним, а

майбутні події можна прогнозувати з високою точністю. Війна руйнує цю базову передумову;

– неадекватність в умовах високої невизначеності. Вони не можуть ефективно функціонувати, коли інформація є неповною, швидко застаріваючою або її просто бракує, а події є безпрецедентними;

– низька швидкість реакції та гнучкість. Послідовний характер та орієнтація на деталізоване планування на початку проєкту роблять ці методи повільними та негнучкими до оперативних змін, що є критично важливим в кризових умовах;

– відсутність механізмів адаптації. Класичні підходи не мають вбудованих механізмів для постійної адаптації до динамічного середовища та навчання на помилках;

– слабка підтримка людського фактору в кризі. Вони не достатньо враховують вплив стресу, психологічного стану команди та фізичної безпеки на ефективність прийняття рішень.

1.4 Дослідження адаптивних та кризових стратегій прийняття управлінських рішень: переваги та потенціал в екстремальних умовах

В умовах, коли класичні методи управління проєктами та прийняття рішень виявляють свою неспроможність, на перший план виходять адаптивні та кризові стратегії. Ці підходи, народжені з потреби реагувати на швидкі зміни та високу невизначеність, набувають особливої значущості в екстремальних умовах, таких як повномасштабний воєнний конфлікт. Вони відрізняються від традиційних парадигм фундаментальними принципами, що дозволяють ІТ-проєктам не лише виживати, а й ефективно функціонувати в хаотичному середовищі [35].

Одним із наріжних каменів адаптивного управління є гнучкість та

ітеративність. Замість прагнення до створення єдиного, всеохоплюючого довгострокового плану, який швидко стає застарілим у динамічному середовищі, адаптивні підходи пропонують працювати короткими, фіксованими циклами. Ці цикли включають планування, виконання, оцінку результатів та коригування планів на основі отриманого зворотного зв'язку. Такий ітеративний процес дозволяє командам регулярно отримувати актуальну інформацію, швидко реагувати на зміни обставин та оперативно змінювати напрямок руху або пріоритети. Це забезпечує постійну відповідність продукту мінливим вимогам та зовнішнім умовам, що є критично важливим, коли ситуація на полі бою або в інфраструктурі змінюється щодня.

Тісно пов'язаний з цим принципом є фокус на навчанні та експериментуванні. В умовах невизначеності помилки розглядаються не як фатальні провали, а як неминуча частина процесу пошуку оптимальних рішень та джерело цінних знань. Адаптивні стратегії заохочують проведення невеликих експериментів, пілотних запусків або створення прототипів для швидкої перевірки гіпотез та збору даних, перш ніж приймати масштабні рішення чи інвестувати значні ресурси. Постійний збір та аналіз зворотного зв'язку від користувачів, клієнтів та самої команди є ключовим елементом цього навчального циклу, дозволяючи системам та процесам постійно вдосконалюватися.

Швидкість реакції є ще одним фундаментальним принципом. У динамічному середовищі здатність швидко реагувати на несподівані події, загрози чи можливості часто є більш важливою, ніж ретельність аналізу, що може призвести до паралічу аналізу. Адаптивні стратегії спрямовані на скорочення часу циклу від виявлення проблеми до прийняття рішення та початку дії. Це часто досягається шляхом децентралізації прийняття рішень та уповноваження команд або окремих співробітників, наближаючи процес прийняття рішень до точки виникнення проблеми або до джерела актуальної інформації. Така автономія вимагає високого рівня довіри до компетенції

команд та їхньої відповідальності.

В умовах постійних загроз та потенційних збоїв, характерних для воєнного конфлікту, критично важливим стає принцип стійкості (resilience) та відмовостійкості (fault tolerance). Замість того, щоб намагатися уникнути всіх можливих проблем (що неможливо в складному та хаотичному середовищі), акцент робиться на побудові систем, процесів та команд, які здатні витримувати несподівані удари, продовжувати функціонувати (можливо, на зниженому рівні) під час збою та швидко відновлюватися після нього. Це може досягатися шляхом резервування критичних компонентів, диверсифікації (наприклад, географічного розподілу команд чи інфраструктури), створення планів аварійного відновлення та розвитку культури взаємодопомоги та гнучкості всередині команди [9].

Серед конкретних підходів, що втілюють ці принципи, варто виділити Agile-методології, такі як Scrum та Kanban. Вони, завдяки своїй ітеративності, фокусу на швидкій поставці цінності та тісній співпраці, виявилися надзвичайно затребуваними. Замість спроб прийняти всі ключові рішення на самому початку, Agile пропонує розбивати процес на короткі цикли, що дозволяє командам швидше реагувати на зміни, підтримувати комунікацію в розподілених командах та пріоритизувати завдання залежно від поточної ситуації (наприклад, повітряної тривоги чи відсутності світла).

Сценарне планування підтвердило свою репутацію як потужний інструмент для роботи в умовах глибокої невизначеності. Замість марних спроб вгадати майбутнє, розробка кількох логічно обґрунтованих, хоча й різних, сценаріїв розвитку подій дозволяє керівництву компаній та проєктів продумати потенційні наслідки та підготувати відповідні плани дій для кожного з них. Це не усуває невизначеності, але суттєво підвищує рівень готовності до різних варіантів майбутнього та сприяє формуванню більш гнучкого стратегічного мислення.

На операційному рівні ключову роль відіграють процеси планування безперервності бізнесу (BCP) та аварійного відновлення (DR). В умовах війни

вони перестали бути формальними документами, а перетворилися на динамічні стратегії та основу для прийняття щоденних рішень. Ідентифікація критично важливих бізнес-функцій, оцінка ризиків їхнього порушення та розробка конкретних планів дій для забезпечення безперервності стали життєво необхідними.

Для ситуацій, що вимагають дуже швидкої реакції, корисною є концепція циклу OODA (Observe-Orient-Decide-Act), розроблена військовим стратегом Джоном Бойдом. Цей цикл описує процес прийняття рішень в умовах конфлікту або швидких змін: постійне спостереження за тим, що відбувається, швидка орієнтація (інтерпретація інформації в поточному контексті), прийняття рішення та негайна дія. Здатність проходити цей цикл швидше за супротивника чи кризову ситуацію дає вирішальну перевагу.

Мислення в термінах реальних опціонів також знаходить своє застосування, особливо при прийнятті інвестиційних рішень в умовах високої невизначеності. Замість того, щоб робити великі, незворотні ставки, цей підхід заохочує робити менші кроки, які створюють можливості для майбутніх дій, зберігаючи гнучкість та можливість змінити курс, коли з'явиться більше інформації. Це цінно при виборі архітектурних рішень або виході на нові ринки в непередбачуваному середовищі.

Нарешті, невід'ємною складовою будь-якої кризової стратегії є управління комунікаціями. Прозоре, часте, чесне, своєчасне та емпатичне спілкування з усіма ключовими стейкхолдерами – співробітниками, клієнтами, партнерами, керівництвом – допомагає підтримувати довіру, керувати очікуваннями та забезпечувати координацію дій. Це також сприяє підтримці морального духу команди, що є критично важливим в екстремальних умовах.

1.5 Формування дослідницьких прогалин та постановка завдання

Проведений у попередніх підпунктах аналіз сутності ІТ-проєктів, еволюції управлінських методологій та методів прийняття рішень, а також їхньої застосовності в екстремальних умовах воєнного конфлікту, дозволяє виявити низку критичних дослідницьких прогалин. Незважаючи на появу та популяризацію адаптивних та кризових стратегій, залишаються невирішеними питання щодо їхньої систематичної інтеграції та оптимального застосування в безпрецедентному контексті тривалої гібридної війни.

Класичні підходи, як було показано, виявилися значною мірою неадекватними для динамічного реагування на виклики воєнного часу. Їхня залежність від стабільності середовища, наявності повної та достовірної інформації, а також жорсткість у плануванні роблять їх непридатними для умов, де невизначеність є тотальною, а швидкість реакції – життєво необхідною. Це створює першу, фундаментальну прогалину: відсутність узагальненої, цілісної моделі прийняття рішень, яка б ефективно працювала саме в умовах максимальної невизначеності та волатильності. Існуючі адаптивні фреймворки, хоч і гнучкі, часто зосереджені на внутрішніх процесах команди або на короткострокових ітераціях, але не завжди надають комплексний підхід до стратегічного реагування на зовнішні, макрорівневі шоки.

Друга суттєва прогалина полягає у недостатній систематизації та інтеграції емпіричного досвіду українських ІТ-компаній в теоретичні моделі управління проєктами. Хоча війна породила унікальні адаптивні практики, існуючі наукові праці лише починають осмислювати цей досвід. Бракує комплексних досліджень, які б не просто описували окремі випадки виживання, а узагальнювали ці адаптаційні стратегії до рівня, де їх можна було б формалізувати та використовувати як основу для нових управлінських моделей. Український досвід є безцінним джерелом знань про те, як

працювати в умовах постійних загроз, мобілізації, інфраструктурних збоїв та фінансового тиску, але цей досвід ще не повністю трансформований у структуровані знання для широкого застосування.

Третя дослідницька прогалина стосується недостатнього врахування людського фактору в контексті екстремального стресу та психологічного тиску. Хоча адаптивні методології наголошують на важливості команди, їхні механізми не завжди адекватно інтегрують аспекти психологічної стійкості, вигорання, втрати мотивації та потреби у підтримці. В умовах війни, коли фізична безпека та емоційний стан співробітників стають пріоритетом, традиційні підходи до управління ресурсами виявляються недостатніми. Необхідна модель, яка б явно включала ці аспекти як ключові змінні при прийнятті управлінських рішень.

З огляду на ці прогалини, виникає гостра потреба у розробці такого підходу до управління ІТ-проєктами, який би дозволяв системно враховувати специфіку воєнного конфлікту та ефективно адаптуватися до нього. Недостатньо просто використовувати окремі гнучкі інструменти; потрібен цілісний фреймворк, що інтегрує найкращі практики кризового менеджменту, адаптивні методології та унікальний український досвід, з акцентом на забезпеченні стійкості, безпеки та безперервності бізнесу.

Таким чином, актуальність даного дослідження зумовлена необхідністю забезпечення стабільності та ефективності української ІТ-галузі в умовах триваючого воєнного конфлікту. Виявлені дослідницькі прогалини свідчать про те, що існуючі управлінські підходи потребують суттєвого вдосконалення та адаптації для подолання безпрецедентних викликів.

Метою даної кваліфікаційної роботи є розробка та обґрунтування концептуальної моделі (або фреймворку) адаптивних стратегій прийняття управлінських рішень в ІТ-проєктах в умовах воєнного конфлікту, спрямованих на підвищення їх стійкості, ефективності та зниження ризиків.

Для досягнення поставленої мети необхідно вирішити такі задачі:

– поглибити аналіз теоретичних підходів та емпіричного досвіду

управління ІТ-проєктами в умовах воєнного конфлікту, оцінивши їхню застосовність та обмеження;

– ідентифікувати та систематизувати ключові фактори впливу воєнного конфлікту на управління ІТ-проєктами (ризики, невизначеності, виклики);

– розробити концептуальну модель (фреймворк) адаптивних стратегій прийняття управлінських рішень в ІТ-проєктах, що враховує специфіку кризових умов;

– сформулювати практичні рекомендації для ІТ-менеджерів та керівників компаній щодо застосування розробленої моделі/фреймворку;

– провести апробацію розробленої концептуальної моделі/фреймворку на конкретному прикладі (кейс-стаді або симуляція) для демонстрації її потенційної ефективності та практичної цінності.

2 ВПЛИВ ВОЄННОГО КОНФЛІКТУ НА ІТ-ПРОЄКТИ: РИЗИКИ, НЕВИЗНАЧЕНОСТІ ТА ВИКЛИКИ

2.1 Розмежування понять: ризики, невизначеності та виклики воєнного часу

У мирний час, коли горизонти планування були відносно чіткими, а джерела даних – передбачуваними, управління проєктами оперувало здебільшого категорією ризиків. Ризик – це потенційна подія, яка в разі настання може негативно вплинути на цілі проєкту. Його ключова характеристика полягає у можливості оцінити ймовірність настання та масштаби наслідків, що дозволяє розробляти стратегії реагування, планувати резерви та мінімізувати потенційні збитки. Класичний ризик-менеджмент передбачає ідентифікацію, аналіз, планування реагування та моніторинг цих відомих або передбачуваних загроз. Ми могли говорити про ризики зміни вимог, технологічних проблем, затримок у постачанні чи коливань бюджету – усі вони були в певній мірі приборкані раціональним аналізом [14].

Однак повномасштабний воєнний конфлікт докорінно змінив цю парадигму, вкинувши управління проєктами, особливо в динамічній ІТ-сфері, у вимір, де домінує невизначеність. На відміну від ризику, невизначеність – це стан, коли майбутні події, їхні наслідки або навіть сама можливість їхнього настання є абсолютно невідомими або не піддаються раціональному прогнозуванню. Це так звані невідомі невідомі (unknown unknowns), що виникають через непередбачуваність війни: її тривалості, інтенсивності, географії, майбутнього політичного ландшафту, стану національної та світової економіки. Управляти невизначеністю неможливо так само, як ризиком, бо її не можна виміряти. Вона вимагає не планування реагування, а розробки адаптивних стратегій, які дозволяють системі бути стійкою до шоків, швидко відновлюватися та навіть посилюватися в умовах хаосу – тобто стати антикрихкою [6, 39].

Поряд з ризиками та невизначеностями, воєнний конфлікт породжує численні виклики. Виклики – це загальні, масштабні труднощі або перешкоди, які вимагають значних зусиль та адаптації. Вони можуть бути прямими наслідками ризиків (наприклад, інфраструктурні збої як наслідок обстрілів, що призводить до виклику безперервності роботи) або наслідками невизначеностей (наприклад, загальна економічна волатильність як виклик для фінансового планування). Виклики вимагають не точкового реагування, а системної трансформації процесів, культури та підходів до управління. Це постійний тиск на систему, що змушує її шукати нові шляхи для функціонування [15].

У контексті ІТ-проєктів в Україні, війна створила унікальне операційне середовище, де всі три поняття – ризики, невизначеності та виклики – переплелися у складну мережу взаємозалежностей. Фізичні атаки на інфраструктуру (ризик) призводять до блекаутів (виклику), що, своєю чергою, створює невизначеність щодо можливості безперервної роботи та посилює ризики зриву термінів. Загальна економічна нестабільність (невизначеність) породжує виклик фінансового тиску на компанії, що впливає на їхню здатність утримувати персонал та інвестувати у розвиток. Цей кумулятивний ефект, коли один фактор посилює інший, призводить до радикального збільшення складності управління [23].

Таким чином, розмежування цих понять – не просто термінологічна вправа, а необхідний крок для розробки адекватної управлінської стратегії. Усвідомлення, що не все можна спрогнозувати та контролювати (ризики), а значна частина майбутнього є невідомою (невизначеність), змушує відмовлятися від ілюзії повного контролю. Натомість фокус переміщується на розвиток здатності системи та команди до адаптації, швидкого реагування та стійкості перед обличчям постійних викликів. Це є фундаментальною передумовою для переосмислення управлінських підходів, що буде детальніше розглянуто у наступних підпунктах цього розділу [29].

2.2 Категоризація та детальний аналіз ключових ризиків для ІТ-проєктів в умовах війни

Воєнний конфлікт в Україні створив безпрецедентне операційне середовище для ІТ-галузі, трансформувавши традиційну матрицю проєктних ризиків. Якщо у мирний час ризики переважно стосувалися технічних викликів, бюджетних обмежень чи термінів, то тепер домінуючими стали загрози, що мають екзистенційний характер. Систематизація цих ризиків є критично важливою для розробки адекватних стратегій управління та підтримки безперервності бізнесу. Ключові категорії ризиків включають кадрові, інфраструктурні, фінансові, кібербезпекові та операційні аспекти [20].

2.2.1 Кадрові ризики

Людський капітал є найціннішим активом будь-якої ІТ-компанії, але в умовах війни він опиняється під найбільшою загрозою, породжуючи комплекс критичних ризиків. Найперший і найстрашніший з них – ризик для фізичної безпеки та життя співробітників та їхніх родин. Постійні ракетні обстріли міст, бойові дії поблизу місць проживання, загроза окупації – усе це створює пряму загрозу. Проєкт може миттєво втратити члена команди через трагічні обставини, що неможливо передбачити чи запобігти. Приклад: 24 лютого 2022 року, коли міста України почали зазнавати масованих обстрілів, абсолютним пріоритетом для ІТ-компаній стала негайна евакуація співробітників із зон підвищеної небезпеки, часто з мінімальним плануванням та в умовах повного хаосу [20].

Інший критичний аспект – мобілізація ключових фахівців. Раптовий та часто непередбачуваний призов спеціалістів, які володіють унікальними

знаннями (наприклад, Senior DevOps Engineer, який працює з критичною інфраструктурою клієнта), може призвести до значних затримок у проєктах, зниження якості продукту та необхідності термінового пошуку заміни або перерозподілу обов'язків. Приклад: проєкт з розробки нового функціоналу для банківської системи може бути зупинений на кілька місяців, якщо його єдиний архітектор буде мобілізований, а передача знань займе тривалий час.

Міграція та релокація персоналу також становлять значний ризик. Хоча багато компаній успішно організували переїзд співробітників у безпечніші регіони України або за кордон, залишається ризик довгострокової еміграції талановитих кадрів, які обирають стабільність за кордоном. Це призводить до втрати інтелектуального капіталу та зменшення кадрового резерву. Крім того, внутрішня релокація може спричинити фрагментацію команд та проблеми з комунікацією, коли співробітники опиняються в місцях із нестабільним зв'язком або складними побутовими умовами. Приклад: команда розробників, що працювала разом в одному офісі, тепер розподілена по трьох країнах та п'яти містах, що ускладнює щоденні синхронізації та призводить до прогалин у розумінні завдань через різницю в часових поясах та якості зв'язку [25].

Надзвичайно важливим, хоча й менш вимірним, є вплив війни на психологічний стан співробітників. Хронічний стрес, підвищена тривожність, проблеми з концентрацією уваги, професійне вигорання та ризик розвитку посттравматичного стресового розладу (ПТСР) – усе це безпосередньо позначається на продуктивності праці, якості виконання завдань та загальному моральному дусі команди. Приклад: розробник, який пережив обстріл свого міста, може демонструвати знижену концентрацію та швидкість кодування, навіть якщо фізично він знаходиться в безпеці, що впливає на терміни виконання його завдань у проєкті [16].

2.2.2 Інфраструктурні ризики

Війна безпосередньо б'є по операційній діяльності, створюючи значні ризики, пов'язані з фізичною та мережевою інфраструктурою. Найбільш очевидним є ризик тривалих та масових відключень електроенергії (блекаутів), спричинених цілеспрямованими атаками ворога на енергетичну систему. Це робить неможливим стабільну роботу для багатьох співробітників, навіть за наявності генераторів, які перевантажуються або потребують постійного дозаправлення. Приклад: взимку, під час масованих ракетних атак, IT-компанії зіштовхувалися з ситуаціями, коли офіси були знеструмлені на 8-12 годин на добу, а домашні коворкінги співробітників не мали стабільного доступу до електроенергії, що унеможливлювало виконання робіт [22].

Тісно пов'язані з цим перебої з мобільним зв'язком та доступом до Інтернету. У багатьох регіонах України якість та доступність зв'язку значно знизилася, що створює значні комунікаційні ризики для розподілених команд. Ефективний та своєчасний обмін інформацією є життєво важливим для IT-проєктів, але технічні проблеми, асинхронні графіки роботи та загальний стрес можуть призводити до затримок у передачі критичної інформації, неправильного розуміння завдань чи вимог, що підвищує ймовірність помилок. Приклад: важливе оновлення вимог від замовника, надіслане у чаті, може бути прочитане розробником із запізненням на кілька годин через відсутність Інтернету, що призведе до розробки невідповідного функціоналу.

Існує також ризик фізичного пошкодження або руйнування активів внаслідок прямих влучань ракет чи снарядів. Це стосується офісних приміщень, центрів обробки даних (особливо тих, що не мігрували в хмару або за кордон), а також персонального обладнання співробітників, які опинилися в зоні бойових дій. Приклад: IT-компанія, що мала головний офіс у Харкові, зіткнулася з необхідністю термінової релокації після пошкодження будівлі

внаслідок обстрілу, що призвело до тимчасової втрати доступу до серверного обладнання та фізичних документів [32].

2.2.3 Фінансові ризики

Економічні наслідки війни генерують значні фінансові ризики для IT-проєктів. Ризик втрати або нестабільності клієнтів є одним з найсерйозніших. Попри доведену стійкість українського IT, деякі клієнти, особливо нові або ті, що працюють у консервативних галузях, можуть розірвати контракти, заморозити поточні проєкти або відмовитися від нових замовлень через загальні побоювання щодо стабільності роботи в країні, що воює, або формально посилаючись на форс-мажорні обставини. Приклад: міжнародна компанія, що планувала замовити розробку великого продукту в українського аутсорсера, могла скасувати контракт після початку війни, побоюючись зриву термінів та проблем з безперервністю [20].

Зростання операційних витрат також створює значний тиск. Компанії змушені інвестувати в енергонезалежність (генератори, Starlink), посилені заходи безпеки, релокацію та підтримку співробітників. Ці додаткові витрати виникають на тлі потенційного зниження доходів через втрату клієнтів або затримки з оплатами. Це може призводити до ризику касових розривів, зниження рентабельності проєктів або навіть загрози банкрутства для менш стійких компаній. Приклад: компанія щомісяця витрачає десятки тисяч доларів на оренду генераторів та закупівлю пального для підтримки роботи офісів, хоча до війни такі витрати були відсутні [22].

Додатковими фінансовими факторами є валютні ризики, оскільки більшість контрактів укладено в іноземній валюті, а витрати здійснюються переважно в гривні, що робить бізнес чутливим до коливань курсу. Також існує ризик виникнення контрактних спорів з клієнтами, пов'язаних з

тлумаченням пунктів про форс-мажорні обставини, визначенням відповідальності за затримки (спричинені, наприклад, блекаутами або мобілізацією) або неможливістю виконати певні специфічні зобов'язання через війну. Приклад: клієнт вимагає компенсації за затримку проєкту, посилаючись на договір, тоді як українська компанія аргументує затримку форс-мажорними обставинами, пов'язаними з постійними повітряними тривогами та відключеннями світла [24].

2.2.4 Кібербезпекові ризики

Війна в Україні супроводжується безпрецедентною за масштабами та інтенсивністю кібервійною, що робить кібербезпекові ризики одними з найвищих. ІТ-компанії, їхні клієнти та державні установи стали постійними мішенями для різноманітних кібератак, що часто координуються та спонсоруються державою-агресором. Це включає масовані DDoS-атаки, спрямовані на порушення роботи веб-сайтів та сервісів; фішингові кампанії для викрадення облікових даних співробітників та клієнтів; атаки з використанням програм-вимагачів (ransomware) з метою шифрування даних та отримання викупу; спроби кібершпигунства для викрадення комерційної таємниці, інтелектуальної власності або даних клієнтів; а також дезінформаційні кампанії, спрямовані на підрив довіри до українських компаній. Приклад: російські хакери можуть здійснити цілеспрямовану DDoS-атаку на портал електронних послуг, розроблений українською ІТ-компанією, що призводить до його тимчасової недоступності та значних репутаційних втрат [21].

Ризик успішної кібератаки є надзвичайно високим і може призвести до катастрофічних наслідків: витоку конфіденційних даних клієнтів (наприклад, персональних даних або банківських реквізитів), порушення роботи критично

важливих сервісів (наприклад, медичних чи банківських систем), значних фінансових збитків та непоправної шкоди репутації. Додаткову складність створює невизначеність щодо векторів, методів та часу майбутніх атак, що вимагає постійної пильності та інвестицій у проактивні заходи безпеки та посилення захисту критичної інфраструктури, зокрема промислових систем (OT security) [34].

2.2.5 Операційні ризики

Війна ставить під сумнів ефективність стандартних операційних процесів управління проєктами. Методології, які передбачають регулярні ритмічні цикли (наприклад, Scrum-спринти), стає важко застосовувати послідовно, коли робота команди постійно переривається повітряними тривогами, відключеннями світла або необхідністю вирішувати нагальні особисті проблеми співробітників. Це створює ризик зриву термінів проєктів та зміни їхнього обсягу. Дотримання запланованих термінів стає надзвичайно складним, якщо не неможливим завданням для багатьох проєктів. Це, своєю чергою, породжує ризик того, що клієнти, зіткнувшись із постійними затримками, вимагатимуть скорочення обсягу робіт, щоб отримати хоча б частину функціоналу в прийнятні терміни, або ж взагалі переглянуть доцільність продовження проєкту. Приклад: команда розробки, яка мала завершити інкремент продукту до кінця спринту, не змогла цього зробити через щоденні багатогодинні блекаути, що вимагало перенесення функціоналу на наступний спринт та пояснення клієнту причин затримки.

Виникає також невизначеність щодо доцільності обраної до війни методології та потреба її докорінної модифікації. Проєктні менеджери можуть бути змушені відмовитися від структурованих підходів на користь хаотичного, реактивного управління в режимі постійного гасіння пожеж. Це призводить до

зниження ефективності, підвищення ризику помилок та загального хаосу в управлінні проєктом.

Ця багатогранна категоризація ризиків підкреслює, що вплив воєнного конфлікту на ІТ-проєкти є комплексним і глибоким, вимагаючи від управлінців не лише традиційних навичок, а й здатності до кризового мислення та швидкої, але виваженої адаптації.

2.3 Взаємодія факторів впливу та їхній кумулятивний ефект на процеси прийняття рішень

Проведений аналіз окремих категорій ризиків, що постали перед українськими ІТ-проєктами в умовах війни, виявляє лише частину складної картини. Справжня глибина впливу воєнного конфлікту полягає у взаємодії цих факторів та їхньому кумулятивному ефекті, що створює безпрецедентну мережу взаємозалежностей і багаторазово посилює виклики для управлінського процесу. На відміну від мирного часу, де ризики часто розглядалися ізольовано, війна об'єднує їх у динамічний, взаємно підсилюючий цикл, що радикально змінює контекст прийняття рішень.

Ця взаємодія проявляється на всіх рівнях. Наприклад, інфраструктурні ризики (такі як тривалі блекаути та перебої зі зв'язком) безпосередньо посилюють кадрові ризики. Коли співробітники не мають доступу до стабільної електроенергії чи Інтернету вдома, їхня продуктивність знижується, психологічна напруга зростає, а це, своєю чергою, збільшує ризик вигорання або рішення про релокацію. Відсутність зв'язку також ускладнює комунікацію всередині розподілених команд, що може призвести до неправильного розуміння завдань та операційних ризиків зриву термінів. Кумулятивний ефект полягає в тому, що проєкт не просто затримується через відсутність світла, а й втрачає частину команди та ефективність комунікації,

що погіршує ситуацію експоненційно [31].

Фінансові ризики також тісно переплітаються з іншими категоріями. Зростання операційних витрат на генератори та заходи безпеки (наслідок інфраструктурних та кібербезпекових ризиків) відбувається на тлі потенційного зниження доходів через втрату клієнтів. Це створює ножиці, що тиснуть на фінансову стійкість компанії, змушуючи керівництво приймати складні рішення про оптимізацію витрат, які можуть вплинути на мотивацію персоналу або обсяг інвестицій у розвиток. Приклад: компанія може бути змушена скоротити бонуси або відмовитися від навчання співробітників, щоб забезпечити кошти на Starlink та генератори, що, своєю чергою, може знизити моральний дух команди та збільшити ризик витоку кадрів.

Кібербезпекові ризики стали не просто загрозою, а постійним фоновим шумом, що впливає на всі операції. Необхідність постійно протистояти атакам вимагає значних ресурсів (фінансових та людських), відволікаючи їх від основної розробки. Успішна атака може призвести до витоку даних, що не лише є репутаційним ризиком, а й може мати прямі фінансові наслідки через штрафи та втрату довіри клієнтів. Це також посилює операційні ризики, оскільки відновлення систем після кібератаки може паралізувати роботу проєкту на тривалий час.

Ця взаємозалежність факторів означає, що управління одним ризиком не може відбуватися ізольовано від інших. Рішення, прийняте в одній області, неминуче впливає на інші. Приклад: рішення про релокацію всієї команди в безпечніший регіон (реакція на ризик фізичної безпеки) може значно збільшити операційні витрати (фінансовий ризик) і створити нові виклики для комунікації та координації (кадрові та операційні ризики).

Кумулятивний ефект усіх цих взаємодій призводить до глибокої, всеохоплюючої невизначеності, що є основною характеристикою операційного середовища для українського ІТ під час війни. Ця невизначеність торкається найфундаментальніших параметрів: неможливо спрогнозувати тривалість та інтенсивність бойових дій, їхню географію, майбутній

політичний ландшафт, стан національної та світової економіки, обсяги та стабільність міжнародної підтримки. Така тотальна невизначеність радикально впливає на процес прийняття управлінських рішень, роблячи практично неможливим точне довгострокове планування, що було стандартом у мирний час.

Замість спроб створити один єдино правильний план, менеджери змушені відмовлятися від ілюзії повного контролю. Вага адаптивних стратегій зростає, вимагаючи від управлінців здатності швидко оцінювати ситуацію, приймати відповідальні рішення в умовах неповної інформації та готовності брати на себе обґрунтований ризик. Розуміння цієї складної мережі взаємодіючих ризиків та невизначеностей є критично важливим для розробки ефективної концептуальної моделі, яка зможе забезпечити стійкість та ефективність ІТ-проєктів у цих безпрецедентних умовах.

3 КОНЦЕПТУАЛЬНА МОДЕЛЬ АДАПТИВНОГО УПРАВЛІННЯ ІТ-ПРОЄКТАМИ В УМОВАХ КОНФЛІКТУ: АРХІТЕКТУРА ТА МЕХАНІЗМИ

3.1 Архітектура та ключові принципи концептуальної моделі

Розробка ефективної управлінської моделі для ІТ-проєктів в умовах воєнного конфлікту вимагає кардинального переосмислення традиційних підходів, оскільки хаотичне та високоневизначене середовище робить їх значною мірою нерелевантними. Виявлені у попередніх розділах дослідницькі прогалини свідчать про гостру потребу в цілісному фреймворку, який не просто реагує на окремі загрози, а системно інтегрує принципи стійкості, динамічної адаптації та людиноцентричності як фундаментальні пріоритети. Запропонована концептуальна модель є відповіддю на цей виклик, пропонуючи нову архітектуру для прийняття управлінських рішень, що забезпечує життєздатність та ефективність проєктів в умовах безпрецедентного тиску та невизначеності [10].

Основна ідея моделі полягає у переході від лінійного, передбачувального планування до ітеративного, циклічного процесу, орієнтованого на постійне сприйняття, адаптацію та навчання. Вона базується на припущенні, що в умовах війни нормальний стан відсутній, і управління має бути не реактивним, а проактивно-адаптивним, постійно скануючи середовище та коригуючи стратегії. Модель інтегрує елементи системного мислення, кібернетичного управління (цикли зворотного зв'язку) та принципів антикрихкості, що дозволяє системі не просто витримувати шоки, а й потенційно посилюватися в результаті стресів [6].

Архітектура моделі представлена п'ятьма взаємопов'язаними модулями, кожен з яких виконує специфічну функцію та постійно обмінюється інформацією з іншими. Ці модулі формують безперервний цикл, що дозволяє керівникам проєктів отримувати актуальні дані, оцінювати стан проєкту з

урахуванням кризових факторів, приймати виважені рішення та оперативно їх коригувати.

На рис. 3.1 зображено схему, що зображує п'ять модулів, розташованих циклічно з двосторонніми стрілками, що відображають взаємодію. Кожен модуль має вхідні та вихідні дані.

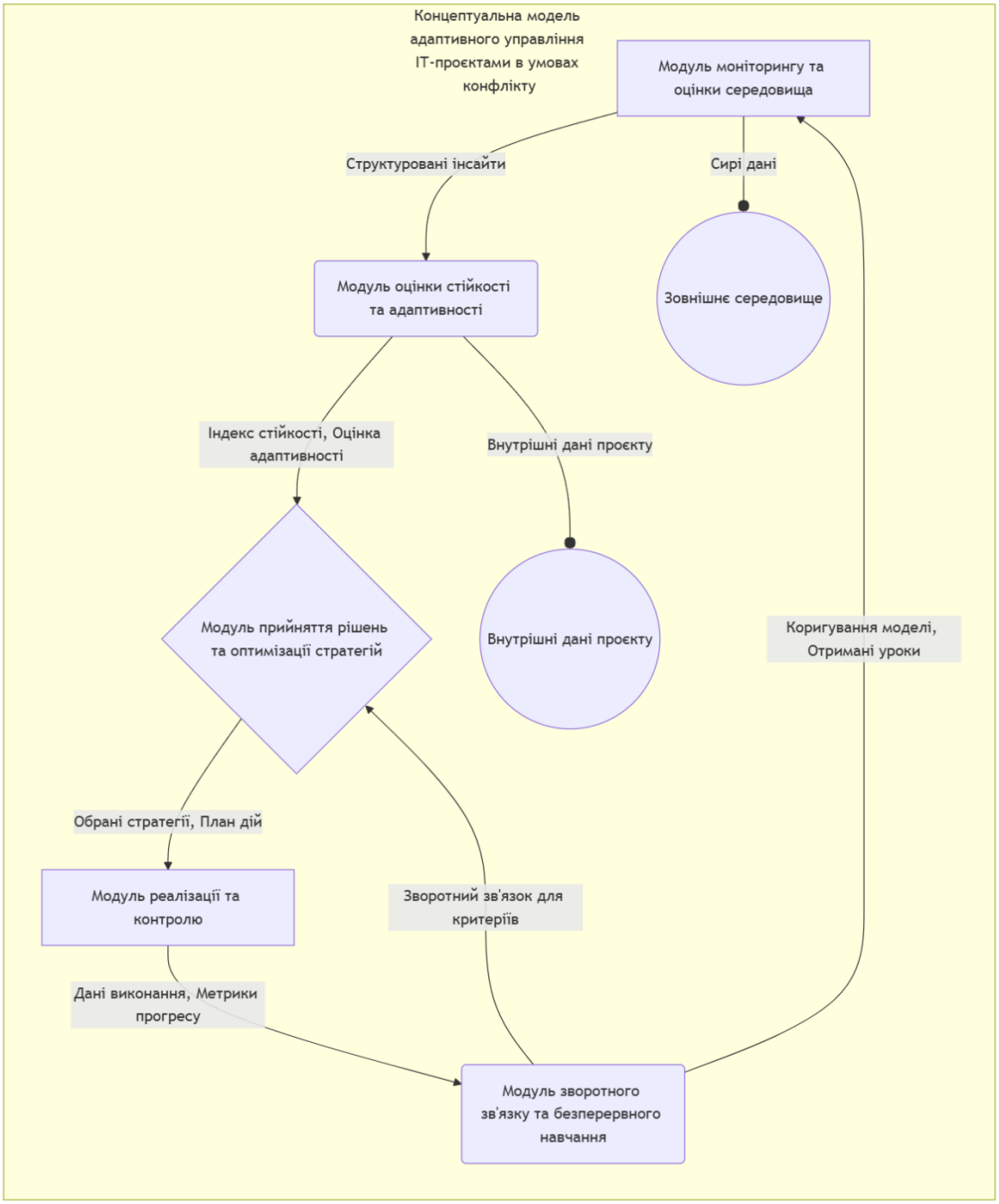

Рисунок 3.1 – Загальна архітектура концептуальної моделі адаптивного управління IT-проєктами в умовах конфлікту

Ключові принципи, що формують парадигму моделі та забезпечують її функціональність, є інтегрованими компонентами, що взаємодоповнюють один одного та визначають логіку роботи кожного модуля.

Принцип тотальної обізнаності (Situational Awareness) виходить за рамки звичайного моніторингу проєктних метрик, надаючи пріоритет безперервному, інтегрованому збору та аналізу інформації з усіх доступних джерел. Це охоплює як формальні дані, що існують у проєкті (системи моніторингу, звіти про прогрес, дані про використання ресурсів), так і неформальні та зовнішні джерела, що стосуються воєнного конфлікту (актуальні новини, офіційні зведення, дані про обстріли та стан критичної інфраструктури, аналіз настроїв у суспільстві та в команді). Основний фокус не просто на отриманні сирих даних, а на їхній інтерпретації та конвертації у структуровані інсайти з урахуванням динамічного воєнного контексту. Це дозволяє керівникам формувати максимально повну, актуальну та релевантну картину стану проєкту та його оточення, виявляючи не лише очевидні загрози, а й приховані взаємозв'язки, потенційні чорні лебеді та можливості для адаптації. Такий підхід забезпечує неперервне розуміння того, що відбувається тут і зараз і що може вплинути на проєкт. Формула ситуаційної обізнаності має такий вигляд:

$$SA(t) = F\big(D_{int}(t), D_{ext}(t), Context_w(t)\big), \tag{3.1}$$

де $SA(t)$ – ситуаційна обізнаність у момент часу;

$D_{int}(t)$ – внутрішні проєктні дані;

$D_{ext}(t)$ – зовнішні дані про кризове середовище;

$Context_w(t)$ – поточний воєнний контекст;

F – функція інтеграції та інтерпретації даних.

Принцип стійкості за замовчуванням (Resilience by Design) є фундаментальним відходом від традиційного ризик-менеджменту. В умовах тотальної невизначеності війни, де багато загроз неможливо передбачити чи

уникнути, модель інтегрує стійкість у саму архітектуру проєкту та кожен процес прийняття рішень. Це означає, що будь-яке рішення – від вибору технологій та архітектури до формування команди та визначення процесів – оцінюється не тільки за стандартними показниками ефективності (вартість, терміни, якість), а й за його прямим внеском у зміцнення здатності проєкту витримувати шоки та швидко відновлюватися після збоїв. Це передбачає системне вбудовування надмірності, диверсифікації (географічної, технологічної), автономності (джерела живлення, зв'язку) та гнучкості як базових властивостей. Наприклад, вибір дорожчого, але географічно розподіленого хмарного рішення, або дублювання ключових ролей у команді, розглядається не як перевитрата, а як критична інвестиція у довгострокову життєздатність проєкту. Коефіцієнт стійкості рішення *(КСР)* визначається за формулою:

$$КСР(P) = \frac{\Delta\text{Стійкість(P)}}{\Delta\text{Вразливість(P)}}, \quad (3.2)$$

де *P* – конкретне управлінське рішення;

ΔСтійкість(P) – потенційне покращення стійкості проєкту внаслідок прийняття рішення;

ΔВразливість(P) – потенційне збільшення вразливості проєкту внаслідок прийняття рішення.

Рішення з КСР>1 є бажаними.

Принцип динамічної адаптації та ітеративності (Dynamic Adaptability & Iteration) визнає, що довгострокове, статичне планування неможливе в умовах війни, де нормальний стан відсутній. Натомість модель пропагує безперервний, швидкий ітераційний цикл управління, що ґрунтується на концепції циклу OODA (Observe-Orient-Decide-Act) або принципах Agile-Scrum. Кожен цикл є міні-проєктом адаптації, що дозволяє команді постійно коригувати курс проєкту відповідно до змін обставин. Це вимагає вбудованої гнучкості в розподілі ресурсів, оперативному перегляді пріоритетів та швидкій реакції на нові вхідні дані з модуля моніторингу.

На рис. 3.2 ілюструється класична схема OODA ітераційного циклу. На діаграмі наглядно представлено круговий зв’язок між елементами від Моніторингу до Дії, і далі по колу.

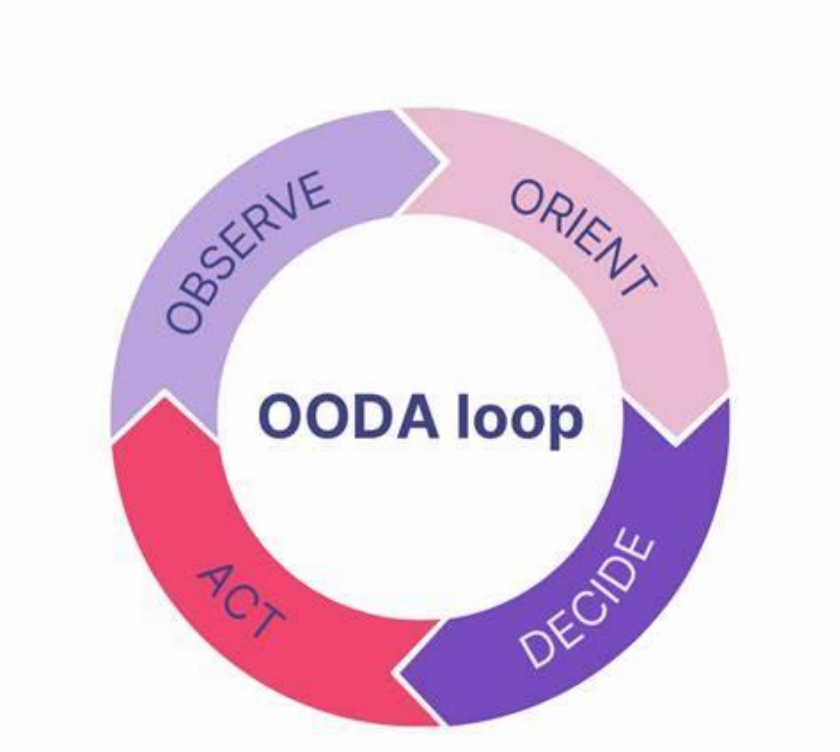

Рисунок 3.2 – Цикл динамічної адаптації моделі OODA-типу

Швидкість адаптації стає однією з ключових конкурентних переваг у кризовому середовищі, дозволяючи проєкту оперативно реагувати на загрози та використовувати можливості, які швидкоплинно з'являються та зникають. Час циклу адаптації визначаємо за формулою:

$$ЧЦА = Час_{Моніторингу} + Час_{Оцінки} + Час_{Рішення} + Час_{Реалізації}, \quad (3.3)$$

де $ЧЦА$ – загальний час, необхідний для повного циклу адаптації;

$Час_{Моніторингу}$ – час на збір та первинну обробку даних;

$Час_{Оцінки}$– час на аналіз та інтерпретацію даних;

$Час_{Рішення}$ – час на прийняття управлінського рішення;

$Час_{Реалізації}$ – час на впровадження рішення.

Оптимізація моделі прагне до мінімізації ЧЦА для прискорення реакції на зміни.

Принцип людиноцентричності та психологічної стійкості (Human-Centricity & Psychological Resilience) інтегрує людський фактор не просто як ресурс, а як критично важливий елемент стійкості та продуктивності проєкту. Модель визнає глибокий та часто руйнівний вплив воєнного конфлікту на психологічний стан співробітників (хронічний стрес, тривога, вигорання, травми) та абсолютну необхідність активної підтримки їхнього благополуччя, безпеки та ментального здоров'я. Рішення, що спрямовані на підтримку морального духу, запобігання вигоранню, забезпечення фізичної безпеки та створення комфортних умов праці, розглядаються як стратегічні інвестиції, що мають прямий вплив на довгострокову життєздатність та продуктивність проєкту. Цей принцип вимагає інтеграції метрик залученості, рівня стресу, показників вигорання та плинності кадрів у загальну систему моніторингу моделі. Індекс психологічної стійкості визначаємо за формулою:

$$ІПС = \alpha \cdot F_{підтр} - \beta \cdot L_{стресу} - \gamma \cdot B_{виг} \quad (3.4)$$

де α, β, γ – вагові коефіцієнти, що відображають важливість кожного фактору;

$F_{підтр}$ – показник рівня психологічної підтримки та благополуччя;

$L_{стресу}$ – показник рівня стресу в команді;

$B_{виг}$ – показник ризику вигорання.

Мета – максимізувати ІПС для забезпечення стабільної продуктивності.

Принцип безперервного навчання та інституціоналізації досвіду (Continuous Learning & Institutionalization of Experience) є завершальним та забезпечує еволюцію самої моделі. Він передбачає систематичний збір уроків, отриманих з кожного циклу адаптації та реалізації рішень, та їхню інтеграцію

в організаційну базу знань. Це дозволяє команді та організації вчитися на власних помилках і успіхах, підвищуючи свою зрілість, швидкість та ефективність в управлінні кризовими проєктами. Досвід війни, трансформований у структуровані знання, стає стратегічним активом, що дозволяє не лише реагувати, а й передбачати, вбудовувати превентивні механізми та підвищувати загальну стійкість. Цей процес відображається через постійне оновлення параметрів моделі, критеріїв прийняття рішень та оптимізацію внутрішніх процесів управління. Коефіцієнт зростання стійкості визначається за формулою:

$$КЗС = \frac{ІІС_{після\ події}}{ІІС_{до\ події}}, \quad (3.5)$$

де $ІІС_{після\ події}$ – індекс психологічної стійкості після певної кризової події та реалізованих адаптаційних рішень;

$ІІС_{до\ події}$ – індекс психологічної стійкості до події.

Значення КЗС>1 свідчить про зростання стійкості завдяки успішному навчанню та адаптації.

3.2 Модуль моніторингу та оцінки середовища: кількісні показники впливу

Модуль моніторингу та оцінки середовища є сенсорним елементом запропонованої концептуальної моделі, відповідальним за безперервний збір, агрегацію та первинну інтерпретацію даних, що відображають стан проєкту та його зовнішнього оточення в умовах воєнного конфлікту. Його основна функція полягає у конвертації хаотичних та різнорідних сирих даних (Raw Data) у структуровані інсайти (Structured Insights) – кількісні показники та індекси, які можуть бути використані для об'єктивної оцінки впливу ризиків

та невизначеностей. Без такого постійного та систематичного моніторингу, управлінські рішення залишалися б інтуїтивними та реактивними, що є неприпустимим у кризових умовах. Збір даних у цьому модулі охоплює як внутрішні проєктні метрики (наприклад, фактичний прогрес виконання завдань, використання ресурсів), так і критичні зовнішні сигнали, що надходять з воєнного та економічного середовища. Для забезпечення об'єктивності та оперативності, використовується комбінація автоматизованих систем збору даних (моніторинг мережі, доступності сервісів) та періодичного ручного збору (звіти про безпекову ситуацію, опитування команди) [28, 40].

Перша важлива категорія структурованих інсайтів – показники інфраструктурного впливу (ІФВ). Вони відображають прямі та непрямі наслідки впливу на фізичну та мережеву інфраструктуру. До таких показників належить середня тривалість та частота відключень електроенергії (ТБ, ЧБ), що вимірюються, наприклад, в годинах/день та кількості/день відповідно, і можуть бути отримані з моніторингу енергопостачання або з локальних чатів про відключення. Аналогічно, відстежуються кількість та тривалість збоїв інтернет-зв'язку (КЗЗ, ТЗЗ), вимірювані у кількості/день та годинах/день відповідно, що оцінюються за допомогою внутрішніх систем моніторингу мережі або опитувань співробітників. Додатково, для всебічної оцінки фізичних загроз, може бути введений індекс наближення бойових дій (ІНБД), який оцінюється за шкалою від 0 до 5 (де 0 – відносно безпечний тил, а 5 – зона активних бойових дій), відображаючи географічне розташування ключових команд та інфраструктури відносно лінії фронту чи зони обстрілів. Ці показники агрегуються в загальний інфраструктурний індекс впливу (ІІВ) за формулою:

$$ІІВ = w_1\ ТБ + w_2 ЧБ + w_3 КЗЗ + w_4 ІНБД\ , \qquad (3.6)$$

де w_i – вагові коефіцієнти, що відображають важливість кожного параметра,

визначені експертно.

Наступна критична група – показники кадрового стану (ПКС), що фокусується на доступності та благополуччі людських ресурсів. Сюди входить відсоток доступності команди (ВДК), який відображає частку співробітників, здатних продуктивно працювати онлайн протягом робочого дня, вимірюючись у відсотках. Для оцінки ментального здоров'я вводиться середній індекс стресу команди (СІСК), що може вимірюватися за допомогою анонімних опитувань або спеціалізованих платформ психологічного моніторингу за шкалою, наприклад, від 1 до 5 (де 5 – високий рівень стресу). Також важливим є відсоток персоналу, що потребує психологічної підтримки (ВППП). Ці показники інтегруються в загальний індекс кадрового впливу (ІКВ):

$$ІКВ = \alpha \cdot (1 - ВДК) + \beta \cdot СІСК + \gamma \cdot ВППП\,, \qquad (3.7)$$

де α, β, γ – вагові коефіцієнти, що відображають значимість кожного фактора для кадрового впливу.

Третя група – показники кібербезпекового середовища (ПКБС), які відображають активність загроз та ефективність систем захисту. Ключовими тут є кількість виявлених кібератак на тиждень (ККА), дані про які можуть надходити із систем SIEM/SOC, що вимірюються у кількості/тиждень. Додатково відстежується середній час виявлення вразливостей (СЧВВ), вимірюваний у годинах від моменту появи вразливості до її ідентифікації, та час реагування на критичні інциденти (ЧРКІ), що відображає години від виявлення до повного усунення критичного інциденту. Ці дані формують індекс кіберзагрози (ІКЗ):

$$ІКЗ = \delta \cdot ККА + \epsilon \cdot СЧВВ + \zeta \cdot ЧРКІ\,, \qquad (3.8)$$

де δ, ϵ, ζ – вагові коефіцієнти, що відображають значимість кожного показника для кібербезпекового впливу.

Нарешті, показники фінансово-операційного впливу (ПФОВ) дають уявлення про економічний та операційний стан проєкту. Сюди належить відсоток проєктів із затримками (ВПЗ), який відображає частку проєктів, що не дотримуються запланованих термінів. Моніторинг середнього перевищення бюджету (СПБ) у відсотках від початкового плану дає розуміння фінансових відхилень. Також важливим є відстеження кількості запитів на ревізію вимог (КЗРВ), що може бути показником нестабільності вимог або необхідності адаптації до мінливих умов. Ці метрики інтегруються в індекс операційного впливу (ІОВ):

$$ІОВ = \eta \cdot ВПЗ + \theta \cdot СПБ + \iota \cdot КЗРВ\,, \qquad (3.9)$$

де η, θ, ι – вагові коефіцієнти, що відображають значимість кожного показника для операційного впливу.

Модуль моніторингу та оцінки середовища є критично важливим для переходу від інтуїтивного управління до управління, що базується на даних, навіть в умовах війни. Його вихідні дані – структуровані інсайти та агреговані індекси – є безпосереднім вхідним потоком для Модуля оцінки стійкості та адаптивності, забезпечуючи фундамент для прийняття обґрунтованих та адаптивних управлінських рішень.

3.3 Модуль оцінки стійкості та адаптивності: розрахунок потенціалу проєкту

Модуль оцінки стійкості та адаптивності є аналітичним хабом концептуальної моделі, що перетворює розрізнені сигнали та індекси, отримані з модуля моніторингу середовища, на комплексне розуміння життєздатності та потенціалу проєкту в умовах кризового впливу. Він слугує

містком між сирим аналізом загроз та стратегічним прийняттям рішень, надаючи керівникам чітку картину, наскільки проєкт здатний витримувати шоки та ефективно реагувати на непередбачувані обставини. Цей модуль поєднує структуровані інсайти (наприклад, інфраструктурний індекс впливу, індекс кадрового впливу), з глибинними внутрішніми даними проєкту, які відображають його внутрішні резерви та здатність до трансформації.

Основна функція цього модуля полягає у вимірюванні двох ключових аспектів – стійкості (Resilience) та адаптивності (Adaptability). Стійкість у цьому контексті розуміється як внутрішня здатність проєкту поглинати та витримувати зовнішні шоки, мінімізуючи їхній руйнівний вплив. Вона формується за рахунок вбудованих резервів, дублювання критичних систем, диверсифікації ресурсів та наявності чітких протоколів для аварійного відновлення. Оцінка стійкості занурюється у вивчення таких елементів, як частка критичної інфраструктури, що забезпечена автономним живленням, наявність та протестованість планів безперервності бізнесу (BCP/DR), ступінь крос-функціональності команди, що дозволяє швидко перерозподіляти ролі, а також рівень фінансового буфера, здатного покрити непередбачені витрати. Це не просто констатація факту, а динамічна оцінка готовності проєкту до випробувань.

Паралельно зі стійкістю оцінюється адаптивність – динамічна здатність проєкту швидко змінювати курс, переорієнтувати пріоритети, впроваджувати інноваційні рішення та навчатися на досвіді в умовах постійного тиску. Адаптивність залежить від гнучкості процесів, швидкості циклів прийняття рішень, готовності команди до змін та її здатності до самоорганізації. Цей аспект включає аналіз того, наскільки легко команда може переходити між завданнями, чи є вона відкритою до експериментів, і наскільки ефективно впроваджуються уроки, отримані з попередніх кризових ситуацій. Оцінка адаптивності відображає потенціал проєкту до трансформації та розвитку, а не лише до виживання.

Інтегруючи всі ці фактори, модуль формує два агреговані вихідні

показники: інтегрований індекс стійкості (ІІС) та оцінку адаптивності (ОА). Ці індекси є кількісним відображенням загального стану проєкту та його потенціалу до успішного функціонування в умовах війни. Вони є комбінацією численних параметрів, кожен з яких відображає певну грань внутрішньої міцності та гнучкості проєкту. Наприклад, ІІС може включати зважену суму індексів інфраструктурної, кадрової, фінансової та кібербезпекової стійкості, доповнену оцінкою якості управлінських процесів та командної згуртованості.

Концептуальна формула для інтегрованого індексу стійкості (ІІС) агрегує показники впливу з попереднього модуля та внутрішні фактори стійкості:

$$ІІС = \phi_1 * (1 - ІІВ) + \phi_1 * (1 - ІКВ) + \phi_1 * (1 - ІКЗ) + \phi_1 * (1 - ІОВ) + \phi_1 * КЯУП + \phi_1 * ФБР\,, \quad (3.11)$$

де *ІІВ, ІКВ, ІКЗ, ІОВ* – показники впливу (інфраструктурного, кадрового, кіберзагрози, операційного), що переведені в одиничний інтервал;

КЯУП – коефіцієнт якості управлінських процесів (наприклад, рівень впровадження BCP/DR);

ФБР – фінансовий буферний рейтинг (показник ліквідності та резервів);

ϕ_i – вагові коефіцієнти, що відображають пріоритети моделі в кризових умовах.

Оцінка адаптивності (ОА) може базуватися на метриках, що відображають гнучкість команди, швидкість навчання та спроможність до інновацій. Вона є не менш важливою, адже навіть найстійкіший проєкт може зазнати краху, якщо не зможе адаптуватися до кардинальних змін у середовищі. Завдяки цілісному підходу, цей модуль надає керівникам не просто набір цифр, а глибоке розуміння реального стану проєкту та його потенціалу виживання та розвитку у вирі воєнного конфлікту. Отримані ІІС та ОА є безпосереднім входом для модуля прийняття рішень, дозволяючи формувати стратегії, що базуються на об'єктивній оцінці внутрішньої міцності проєкту перед зовнішніми викликами.

3.4 Модуль прийняття рішень та оптимізації стратегій: критерії та механізми вибору

Модуль прийняття рішень та оптимізації стратегій є інтелектуальним ядром запропонованої концептуальної моделі. Саме тут, на основі всебічних структурованих інсайтів, отриманих з модуля моніторингу середовища (3.2), та комплексної оцінки стійкості й адаптивності проєкту (3.3), формуються та обираються управлінські рішення, що спрямовані на забезпечення життєздатності та ефективності ІТ-проєктів в умовах воєнного конфлікту. Цей модуль перетворює аналітичні дані на конкретні дії, виходячи за рамки традиційної оптимізації лише фінансових чи часових показників.

На відміну від мирного часу, де критерії прийняття рішень були переважно економічними та функціональними, в умовах війни вони кардинально змінюються. До традиційних цілей проєкту додаються нові, життєво важливі пріоритети, що віддзеркалюють екстремальний характер середовища. Серед ключових критеріїв, які цей модуль враховує при виборі стратегій, виступають безпека та людиноцентричність, що передбачають пріоритизацію життя, здоров'я та психологічного благополуччя команди. Кожне потенційне рішення оцінюється з точки зору його впливу на індекс психологічної стійкості та загальний рівень безпеки співробітників, навіть якщо це призводить до збільшення витрат або затримок [8].

Далі, критичним критерієм є безперервність критичних операцій. Модуль орієнтується на забезпечення функціонування ключових сервісів та процесів проєкту, навіть за умови зниження загальної продуктивності або тимчасового заморожування менш пріоритетного функціоналу. Це вимагає здатності швидко перерозподіляти ресурси та фокусуватися на мінімально життєздатній функціональності. Не менш важливою є швидкість реагування, що відображає час від виявлення загрози (з Модуля моніторингу) до імплементації контрзаходів. Рішення, які дозволяють діяти оперативно,

отримують вищий пріоритет, адже в умовах війни швидкість часто є синонімом виживання. Також модуль враховує ефективність використання обмежених ресурсів, оскільки війна створює дефіцит фінансових та людських резервів, вимагаючи оптимального розподілу наявних можливостей. Нарешті, будь-яке рішення має сприяти збільшенню адаптивності проєкту для майбутнього, тобто не тільки вирішувати поточну проблему, а й підвищувати здатність системи до подальших адаптацій та трансформацій.

Механізм прийняття рішень у цьому модулі є ітеративним та динамічним, що дозволяє постійно коригувати стратегії відповідно до змінюваних обставин, а не дотримуватися жорсткого плану. Він використовує агреговані вхідні дані: інтегрований індекс стійкості (ІІС) та оцінку адаптивності (ОА) з попереднього модуля, а також детальні індекси впливу (ІІВ, ІКВ, ІКЗ, ІОВ) з модуля моніторингу. Ці показники інтегруються для формування комплексного уявлення про поточний стан проєкту та рівень кризової загрози.

Модуль використовує систему зваженої оцінки альтернативних стратегій на основі визначених критеріїв. Для кожної потенційної стратегії розраховується її індекс ефективності стратегії (ІЕС) (формула (3.13)), який враховує очікуваний вплив стратегії на кожен з пріоритетних критеріїв (безпека, безперервність, швидкість, використання ресурсів, адаптивність).

$$IEC = \sum_{k=1}^{N} w_k * Вплив(Стратегія, Критерій_k) , \qquad (3.13)$$

де w_k – вага k-го критерію (визначена відповідно до поточних пріоритетів та серйозності загрози, наприклад, безпека може мати вищу вагу при прямій загрозі життю);

Вплив(Стратегія,Критерій$_k$) – оцінка впливу стратегії на k-й критерій.

Також модуль включає фактор пріоритизації, що впливає на вибір стратегії залежно від критичності поточного ризику та наявного рівня стійкості проєкту. Якщо, наприклад, інфраструктурний індекс впливу (ІІВ)

дуже високий, пріоритет отримають стратегії, спрямовані на забезпечення автономності енергопостачання, навіть якщо вони є дорожчими. Механізми моделі дозволяють швидко генерувати кілька альтернативних сценаріїв реагування та оцінювати їх за допомогою цих метрик, що є ключовим у швидкозмінному воєнному середовищі.

Результатом роботи цього модуля є обрані адаптивні стратегії та деталізований план дій, що враховує динаміку кризового середовища, внутрішню міцність проєкту та його здатність до трансформації. Ці вихідні дані безпосередньо передаються до модуля реалізації та контролю, замикаючи цикл управлінського процесу та забезпечуючи перехід від аналізу до цілеспрямованої дії в умовах безпрецедентної невизначеності.

3.5 Модуль зворотного зв'язку та безперервного навчання: адаптація моделі

Модуль зворотного зв'язку та безперервного навчання є кульмінаційним та водночас стартовим пунктом циклу адаптивного управління в концептуальній моделі. Він являє собою своєрідний мозок, що навчається, який забезпечує постійну еволюцію та вдосконалення всієї системи прийняття рішень на основі реального досвіду. В умовах воєнного конфлікту, коли кожна подія є унікальним уроком, а стабільність відсутня, здатність організації швидко навчатися та інституціоналізувати отримані знання стає вирішальним фактором виживання та успіху [10].

Цей модуль отримує критично важливу інформацію з Модуля реалізації та контролю, зокрема дані виконання (Execution Data) та оцінку результатів (Outcome Assessment) впроваджених стратегій. Він аналізує, наскільки успішно були реалізовані рішення, які були непередбачені труднощі, які фактори сприяли успіху, а які – невдачі. Це не просто збір постфактумних

даних, а глибокий аналіз відхилень від очікуваних результатів та ідентифікація кореневих причин цих відхилень. Наприклад, якщо стратегія, спрямована на підвищення інфраструктурної стійкості, не дала очікуваного ефекту, модуль аналізуватиме, чому (можливо, були недооцінені логістичні ризики постачання обладнання, або ж зміна характеру обстрілів перевершила передбачені сценарії).

Основна функція модуля полягає у генерації уроків (Learned Lessons) – цінних, дієвих інсайтів, які можуть бути застосовані для покращення майбутніх рішень. Ці уроки не є лише констатацією факту, а пропозиціями щодо коригування параметрів моделі, удосконалення механізмів оцінки, розширення критеріїв прийняття рішень або навіть доповнення бази знань новими типами ризиків та невизначеностей. Іншими словами, модуль перетворює емпіричний досвід на інституціоналізоване знання, що дозволяє уникнути повторення помилок та ефективніше реагувати на подібні виклики у майбутньому.

Вихідні дані цього модуля – коригування моделі (Model Adjustment) та отримані уроки – безпосередньо впливають на інші компоненти фреймворку. Вони можуть включати:

– коригування вагових коефіцієнтів у формулах Модуля моніторингу (наприклад, збільшення ваги певних інфраструктурних показників, якщо їхній вплив виявився критичнішим, ніж очікувалося);

– уточнення метрик у Модулі оцінки стійкості (наприклад, додавання нових параметрів для оцінки психологічної стійкості команди, якщо попередні були недостатніми);

– перегляд критеріїв прийняття рішень у відповідному Модулі (наприклад, якщо було виявлено, що безпека команди вимагає ще вищого пріоритету, ніж раніше вважалося).

Оновлення бази знань організації про ефективні стратегії та вивчені пастки в умовах війни.

Цей безперервний цикл навчання є критично важливим, оскільки він

гарантує, що модель залишається релевантною та ефективною в динамічному середовищі. Він дозволяє системі самовдосконалюватися, перетворюючи кожен виклик на можливість для зростання. Коефіцієнт зростання стійкості (КЗС), введений у принципах моделі, є ілюстрацією того, як модуль навчання сприяє підвищенню загальної міцності проєкту з часом.

4 ПРАКТИЧНІ РЕКОМЕНДАЦІЇ ДЛЯ АДАПТИВНОГО УПРАВЛІННЯ ІТ-ПРОЄКТАМИ В УМОВАХ ВІЙНИ

4.1 Методологія збору емпіричних даних та характеристика респондентів

Формування дієвих практичних рекомендацій, здатних ефективно застосовуватися в умовах воєнного конфлікту, неможливе без глибокого розуміння реального досвіду та викликів, з якими стикаються управлінці ІТ-проєктів. З огляду на це, значна частина даного дослідження ґрунтувалася на первинних емпіричних даних, отриманих шляхом проведення серії цільових інтерв'ю з представниками різних типів компаній, що функціонують в українському ІТ-секторі або мають значні ІТ-відділи. Цей підхід дозволив не лише підкріпити теоретичні висновки практичними інсайтами, а й виявити унікальні адаптивні стратегії, що були розроблені на передовій управління в умовах війни [26].

Методологія збору даних була побудована на проведенні напівструктурованих інтерв'ю. Такий формат дозволив, з одного боку, забезпечити охоплення ключових аспектів, що цікавлять дослідження (наприклад, управління ризиками, кадрові питання, адаптація методологій), а з іншого – надати респондентам достатню свободу для висвітлення неочікуваних викликів та унікальних рішень, що виникли в їхній практиці. Усі інтерв'ю проводилися з гарантією повної анонімності компаній та особистостей респондентів, що сприяло більшій відкритості та щирості у викладі досвіду, особливо з огляду на чутливий характер теми воєнного конфлікту та безпекових питань. Перед початком кожного інтерв'ю респонденти були ознайомлені з метою дослідження та принципами конфіденційності, що відповідало етичним нормам проведення наукових досліджень.

Характеристика респондентів була ретельно продумана для

забезпечення широкого спектру досвіду та охоплення різних бізнес-моделей ІТ-індустрії. Загалом було опитано представників трьох основних груп:

– провідні аутсорсингові ІТ-компанії. Ця група представляє значний сегмент українського ІТ, що працює переважно з міжнародними клієнтами. Респондентами були проєктні менеджери, керівники програм та директори з інжинірингу. Їхній досвід є критичним для розуміння викликів, пов'язаних з підтримкою міжнародних контрактів, управлінням розподіленими командами, релокацією персоналу та забезпеченням безперервності сервісів для глобальних замовників в умовах місцевого конфлікту;

– ІТ-компанії, що розробляють та продають власні програмні продукти. Ця категорія компаній зосереджена на життєвому циклі продукту, його розвитку, підтримці та захисті інтелектуальної власності. Респондентами були Product Managers, керівники R&D відділів та CTO. Їхні інсайти дозволили зрозуміти особливості управління розробкою та підтримкою продукту в умовах війни, адаптацію продуктових стратегій до мінливого ринку та загрози для кібербезпеки власних систем;

– компанії з великими ІТ-відділами, де ІТ не є основним видом бізнесу, але критично важливий для функціонування (наприклад, оператори критичної інфраструктури, великі фінансові установи). Ця група є джерелом унікальних та надзвичайно важливих даних. Респондентами були керівники ІТ-департаментів, відповідальні за операції та кібербезпеку. Їхній досвід відображає управління ІТ-ризиками, що мають прямі критичні наслідки для національної безпеки, життєво важливих систем та безперервності надання базових послуг (енергетика, фінанси). Аналіз їхніх стратегій (наприклад, розробка комплексних протоколів кіберзахисту операційних технологій, створення багаторівневих систем резервування, управління фізичною безпекою інфраструктури) є ключовим для формування рекомендацій, оскільки вони стикаються з максимальним рівнем тиску та відповідальності.

Загалом, кількість проведених інтерв'ю була достатньою для виявлення спільних тенденцій, унікальних стратегій та підтвердження теоретичних

висновків щодо впливу воєнного конфлікту. Зібрані емпіричні дані є не просто ілюстрацією, а невід'ємною частиною обґрунтування практичних рекомендацій, що будуть сформульовані в наступних підпунктах цього розділу.

4.2 Рекомендації щодо забезпечення ситуаційної обізнаності та моніторингу середовища

В умовах воєнного конфлікту, коли стабільність перетворюється на ілюзію, а кожна година може принести кардинальні зміни, здатність проєкту підтримувати високий рівень ситуаційної обізнаності стає не просто бажаною перевагою, а абсолютною необхідністю. Це вже не просто моніторинг виконання завдань за графіком, а безперервне сканування як внутрішнього стану проєкту, так і надзвичайно мінливого зовнішнього середовища. Саме цей модуль – моніторингу та оцінки середовища – є першим і найважливішим кроком у циклі адаптивного управління, оскільки він живить усі подальші управлінські рішення актуальною та релевантною інформацією. Від ефективності його функціонування залежить швидкість та адекватність реакції на будь-яку загрозу чи можливість, що виникає у цьому хаотичному контексті.

Забезпечення ситуаційної обізнаності вимагає поєднання різних джерел даних та інтеграції їхнього аналізу. Насамперед, йдеться про налагодження систематичного збору даних про безпекову ситуацію. Компанії, що працюють в Україні, мусять постійно відстежувати оперативну інформацію про повітряні тривоги, ракетні обстріли, бойові дії поблизу ключових локацій, а також потенційні загрози для фізичної безпеки персоналу. Під час інтерв'ю з керівниками аутсорсингових компаній було підкреслено, що вони розробили власні системи оповіщення та верифікації інформації, часто використовуючи дані з офіційних джерел (Державна служба з надзвичайних ситуацій, місцеві

адміністрації), а також перевірені Telegram-канали та внутрішні мережі зв'язку. Вони акцентували на важливості не лише отримання сповіщень, а й верифікації джерел та фільтрації дезінформації, яка може посилити паніку та дезорієнтувати команду. Цей безперервний потік даних є основою для протоколів реагування на повітряні тривоги та рішення про тимчасове призупинення роботи або переміщення в укриття.

Окрім безпеки, критично важливим є моніторинг стану інфраструктури, зокрема доступу до електроенергії, інтернету та мобільного зв'язку. Досвід компаній, особливо тих, що оперують значними IT-відділами у сферах критичної інфраструктури, показав, що постійне відстеження тривалості та частоти блекаутів, а також якості зв'язку є обов'язковим. Вони розгорнули власні внутрішні системи моніторингу доступності сервісів та каналів зв'язку, доповнюючи їх зворотним зв'язком від співробітників з різних регіонів. Наприклад, одна з таких компаній розробила інтегровану систему, яка в режимі реального часу відстежує рівень енергоспоживання та доступності мереж у різних містах, що дозволяє швидко перерозподіляти навантаження на резервні дата-центри або координувати дії ремонтних бригад. Ці дані інтегруються у загальні дашборди, які надають керівництву комплексну картину інфраструктурного стану проєкту.

Важливим елементом ситуаційної обізнаності є моніторинг кадрового стану та психологічного благополуччя команди. Війна чинить величезний тиск на людей, і це неминуче впливає на продуктивність та якість роботи. Рекомендовано впроваджувати регулярні, анонімні опитування для вимірювання рівня стресу, вигорання та загального настрою в команді. Керівники аутсорсингових компаній наголошували на важливості відкритої комунікації та створення безпечного простору, де співробітники можуть повідомляти про свої потреби та проблеми. Деякі компанії почали відстежувати показники, такі як кількість днів відпочинку, використання психологічної підтримки та навіть непрямі ознаки зниження продуктивності (наприклад, аномальні зміни у часі виконання завдань). Ці дані допомагають

вчасно ідентифікувати проблеми, що стосуються ментального здоров'я, та пропонувати відповідну підтримку.

На додаток до цього, необхідно здійснювати моніторинг фінансово-операційного середовища. Це включає відстеження змін у попиті на продукт чи послуги, аналіз контрактних зобов'язань з урахуванням форс-мажорних обставин, а також гнучке планування бюджету з урахуванням зростання операційних витрат та валютних коливань. Продуктові компанії акцентували на важливості постійного аналізу поведінки користувачів та тенденцій ринку, щоб швидко адаптувати свої продуктові стратегії. У той же час, аутсорсингові компанії зосереджені на постійній комунікації з клієнтами щодо можливих затримок та прозорому інформуванні про реальну ситуацію, щоб зберегти довіру та уникнути розірвання контрактів.

Ключовим аспектом Модуля моніторингу є не просто збір даних, а їхня оперативна візуалізація та інтерпретація. Розробка інтегрованих дашбордів кризового стану, які в режимі реального часу відображають ключові показники (ІІВ, ІКВ, ІКЗ, ІОВ), дозволяє керівникам швидко оцінювати ситуацію та ідентифікувати червоні прапорці. Це не просто красиві графіки, а інструменти, що дозволяють перетворити великі обсяги інформації на дієві інсайти. Рекомендовано створювати спеціалізовані звіти про безпекову ситуацію, щоденні оновлення інфраструктурного стану та щотижневі звіти про моральний дух команди. Важливо, щоб ці звіти були максимально лаконічними, зосередженими на ключових показниках, що вимагають негайної уваги.

Нарешті, забезпечення ситуаційної обізнаності вимагає вбудованого механізму зворотного зв'язку. Це означає, що дані про ефективність прийнятих рішень та їхній вплив на проєктний стан мають постійно повертатися до Модуля моніторингу, дозволяючи йому навчатися та уточнювати параметри свого аналізу. Цей процес безперервної петлі зворотного зв'язку є фундаментальним для адаптивності всієї моделі, гарантуючи, що інформація, на якій базуються рішення, постійно вдосконалюється та залишається

релевантною у мінливому кризовому середовищі. Це не лише дозволяє швидко виявляти нові загрози, а й сприяє проактивному прогнозуванню потенційних викликів, перетворюючи хаос на керований, хоча й складний, потік інформації.

4.3 Рекомендації щодо підвищення стійкості та адаптивності ІТ-проєктів

В умовах воєнного конфлікту, коли зовнішнє середовище є джерелом постійних та непередбачуваних шоків, здатність ІТ-проєкту не просто реагувати на загрози, а бути стійким (resilient) та адаптивним стає ключовим фактором його життєздатності. Це виходить за рамки традиційного ризик-менеджменту і перетворюється на філософію стійкості за замовчуванням, де кожен елемент проєкту – від архітектури до кадрових стратегій – спроєктований з урахуванням можливості витримувати та швидко відновлюватися після збоїв. Модуль оцінки стійкості та адаптивності, описаний у попередньому розділі, надає кількісне відображення цієї здатності, а даний підпункт трансформує це розуміння у конкретні практичні рекомендації.

Насамперед, забезпечення стійкості вимагає архітектурних та інфраструктурних інвестицій. Компанії, що працюють з критичними ІТ-відділами, наприклад, оператори критичної інфраструктури, засвоїли ці уроки з перших днів війни. Вони наголошували на необхідності географічної диверсифікації ключових систем та даних, переводячи їх у захищені хмарні середовища, розташовані за межами зони активних бойових дій, або навіть за кордоном. Це не просто перенесення даних, а перебудова архітектури для забезпечення безперервності доступу та функціонування, навіть якщо одна локація стає недоступною. Одним із яскравих прикладів є розгортання багаторівневих систем резервування для баз даних та застосунків, що дозволяє

миттєво переключатися на резервні копії у випадку збою. Це вимагає значних інвестицій, але, як зазначили респонденти, ці витрати є меншими, ніж втрати від простою критичних сервісів. Також, критично важливими є інвестиції в автономні джерела енергії та зв'язку. Інтерв'ю показали, що компанії масово закуповували генератори, інвертори та системи Starlink, перетворюючи офіси та навіть домашні робочі місця на автономні опорні пункти. Це не лише забезпечує безперервність роботи, а й знижує психологічний тиск на співробітників [25].

Другим ключовим аспектом є кадрова стійкість та адаптивність. Війна підкреслила, що люди – це наш головний актив не просто гасло, а життєво важлива істина. Рекомендовано розробляти стратегії диверсифікації команди – не лише географічної, а й у навичках. Це означає формування крос-функціональних команд, де кілька співробітників можуть виконувати одні й ті ж ключові ролі, що дозволяє мінімізувати вплив мобілізації, хвороби чи релокації окремих фахівців. Під час інтерв'ю з аутсорсинговими компаніями, які працюють з великими міжнародними проєктами, часто згадувалася практика knowledge transfer – систематичної передачі знань та документації, щоб уникнути єдиної точки відмови в команді. Це включає створення чітких протоколів для передачі відповідальності та доступу у випадку непередбаченої відсутності ключових фахівців. Також, критично важливою є гнучкість у графіках роботи та підходах до управління. Компанії, що успішно адаптувалися, дозволяли співробітникам працювати в асинхронному режимі, враховуючи повітряні тривоги та відключення, пріоритизуючи не кількість годин онлайн, а результат.

Третій напрямок – операційна та процесна адаптивність. Проєкти мають бути здатними до швидкої зміни пріоритетів та обсягу робіт. Рекомендовано впроваджувати Agile-методології (Scrum, Kanban) з акцентом на їхню гнучкість, а не на жорстке дотримання всіх церемоній. Продуктові компанії наголошували на здатності швидко переорієнтувати дорожню карту продукту, реагуючи на зміну ринкового попиту, спричиненого війною, або на появу

нових можливостей (наприклад, попит на рішення для кібербезпеки). Це вимагає вбудованих механізмів для швидкого перегляду та ревізії вимог – замість тривалих процесів затвердження, впроваджуються механізми швидкого консенсусу та делегування повноважень. Критично важливим є також регулярне тестування планів безперервності бізнесу (BCP) та аварійного відновлення (DR). Компанії з критичними IT-відділами зазначили, що вони проводять стрес-тести своїх систем, симулюючи блекаути чи кібератаки, щоб виявити вузькі місця та вдосконалити протоколи реагування. Це дозволяє не просто мати план на папері, а бути впевненим у його дієвості в реальних умовах.

Забезпечення кібербезпекової стійкості є окремим, але надзвичайно важливим аспектом. Зростання інтенсивності кібератак вимагає не лише реактивного захисту, а й проактивних інвестицій. Рекомендовано впроваджувати багаторівневий захист (Next-Generation Firewalls, SIEM-системи, Endpoint Detection and Response), постійно оновлювати програмне забезпечення та протоколи безпеки. Інтерв'ю з представниками компаній, що оперують критичною інфраструктурою, підкреслили необхідність сегментації мереж (відділення операційних технологій (OT) від корпоративних (IT)), щоб уникнути поширення атак. Вони також наголошували на важливості регулярних аудитів безпеки та впровадження внутрішніх протоколів реагування на інциденти, що дозволяють швидко локалізувати та усувати загрози [21].

Нарешті, фінансова стійкість досягається не лише накопиченням резервів, а й гнучким фінансовим плануванням. Рекомендовано створювати фінансові подушки безпеки, диверсифікувати джерела доходу та активно працювати з клієнтами щодо перегляду контрактних умов у випадку форс-мажорів. Продуктові компанії шукають нові ринки збуту, а аутсорсингові – активно інформують клієнтів про заходи, які вони вживають для забезпечення безперервності роботи, щоб зберегти їхню довіру.

Інтегруючи ці рекомендації, IT-проєкти можуть не просто виживати в

умовах війни, а й стати більш міцними, гнучкими та готовими до непередбачуваних викликів. Це перетворює управління на постійний процес адаптації та вдосконалення, де кожен пройдений шок є уроком, що посилює загальну стійкість системи.

4.4 Рекомендації щодо людиноцентричного управління та психологічної підтримки команди

В умовах повномасштабного воєнного конфлікту, коли зовнішнє середовище стає джерелом постійних та непередбачуваних шоків, управління ІТ-проєктами виходить далеко за межі технічних завдань і фінансових показників. На перший план виходить абсолютно критична необхідність людиноцентричного управління, що ставить благополуччя, безпеку та психологічну стійкість команди в основу всіх управлінських рішень. Традиційні підходи, що розглядають персонал як ресурс, виявляються недостатніми перед обличчям безпрецедентного тиску, що чинить війна на кожну особистість. Досвід, отриманий українськими компаніями, недвозначно свідчить: збереження людей – це не лише етичний імператив, а й стратегічний ключ до виживання та ефективності проєкту.

Насамперед, безумовним пріоритетом є забезпечення фізичної безпеки співробітників. Це вимагає розробки та постійного оновлення чітких протоколів реагування на безпекові загрози. Керівники ІТ-відділів у великих компаніях, що оперують критичною інфраструктурою, підкреслювали, що з перших днів конфлікту вони зосередилися на розробці систем оповіщення, що інтегруються з офіційними джерелами повітряних тривог, та на забезпеченні доступу до безпечних укриттів для персоналу. Вони організовували логістичні ланцюжки для екстреної евакуації співробітників із зон бойових дій, надавали фінансову допомогу на переїзд та допомагали з пошуком тимчасового житла

у більш безпечних регіонах. Деякі компанії навіть інвестували у створення власних безпечних коворкінгів, що обладнані укриттями, автономним живленням та зв'язком, аби гарантувати можливість роботи та фізичну безпеку навіть під час тривог. Ця турбота про фізичну безпеку, виражена в конкретних діях, не лише рятує життя, а й формує потужну лояльність та довіру в команді.

Паралельно з фізичною безпекою, надзвичайно гостро постає питання психологічного благополуччя та ментального здоров'я команди. Хронічний стрес, постійна невизначеність, тривога за близьких, втрата домівок – усе це призводить до значного психологічного навантаження, що неминуче позначається на продуктивності, концентрації та емоційному стані. Керівники аутсорсингових та продуктових компаній активно впроваджували різноманітні програми психологічної підтримки. Це включало надання доступу до індивідуальних консультацій з психологами, організацію групових вебінарів зі стресостійкості та тренінгів з управління емоціями. Респонденти зазначали, що важливо було дестигматизувати звернення за психологічною допомогою, заохочуючи співробітників відкрито говорити про свої труднощі. Також, значна увага приділялася створенню внутрішніх спільнот та peer-support груп, де співробітники могли ділитися досвідом та підтримувати один одного, що допомагало подолати відчуття ізоляції та зміцнити командний дух [19].

Ефективне управління в умовах війни неможливе без гнучкості у робочих графіках та виняткової емпатії керівництва. Класичні 8-годинні робочі дні та жорсткі дедлайни часто стають нереалістичними. Компанії, що успішно адаптувалися, дозволяли співробітникам працювати в асинхронному режимі, враховуючи повітряні тривоги, блекаути та особисті обставини. Керівники аутсорсингових компаній часто згадували, що вони змінили фокус з відпрацьованих годин на досягнуті результати, дозволяючи команді самостійно розподіляти свій час, щоб ефективно реагувати на зовнішні події та забезпечувати баланс між роботою та особистим життям. Це вимагало від менеджерів не лише глибокого розуміння завдань, а й здатності проявляти

максимальну емпатію та розуміння до індивідуальних обставин кожного співробітника, адже війна зачепила всіх по-різному. Гнучкість у робочих процесах та графіках була ключовим фактором для збереження продуктивності та уникнення вигорання в умовах постійного стресу [33].

Прозора та емпатична комунікація з командою є ще одним стовпом людиноцентричного управління. В умовах невизначеності та постійних загроз, інформаційний вакуум породжує тривогу та паніку. Керівники всіх типів компаній наголошували на важливості регулярних, чесних та прозорих оновлень щодо стану компанії, її планів, безпекової ситуації та заходів підтримки. Це не просто офіційні звіти, а відкритий діалог, де керівництво демонструє свою підтримку та розуміння. Продуктові компанії, наприклад, регулярно проводили онлайн-зустрічі питання-відповідь з топ-менеджментом, де співробітники могли ставити будь-які питання. Аутсорсингові компанії активно інформували команди про комунікацію з міжнародними клієнтами, демонструючи, що компанія докладає максимум зусиль для збереження проєктів та робочих місць. Ця проактивна та емпатична комунікація допомагає будувати довіру, знижувати рівень тривоги та підтримувати високий моральний дух в умовах постійного стресу.

Нарешті, формування внутрішньої спільноти та соціальної підтримки відіграє величезну роль у боротьбі з ізоляцією та вигоранням. Компанії активно організовували внутрішні заходи, що сприяли зміцненню зв'язків між співробітниками – від онлайн-тімбілдінгів до спільних волонтерських ініціатив. Багато респондентів з усіх типів компаній згадували, як їхні команди об'єднувалися для допомоги Збройним Силам України, збору коштів, закупівлі спорядження чи гуманітарної допомоги. Ця спільна діяльність не лише демонструвала активну громадянську позицію, а й створювала відчуття приналежності, спільної мети та взаємодопомоги, що є потужним антистресовим фактором. Така соціальна відповідальність та волонтерська активність ставали невід'ємною частиною корпоративної культури, зміцнюючи внутрішню єдність та психологічну стійкість команди.

Таким чином, людиноцентричне управління в умовах війни виходить за межі стандартних функцій HR, перетворюючись на фундаментальний стратегічний пріоритет. Воно вимагає від керівників не лише професійних, а й сильних лідерських якостей, здатності до емпатії, прозорості та постійної турботи про благополуччя кожної людини в команді. Це дозволяє ІТ-проєктам не лише зберігати свою ефективність, а й зміцнювати свій найцінніший актив – людський капітал – у найскладніші часи.

4.5 Рекомендації щодо безперервного навчання та інституціоналізації досвіду

В умовах воєнного конфлікту, коли кожна подія може бути безпрецедентною, а стабільність перетворюється на ілюзію, здатність організації до безперервного навчання стає не просто бажаною практикою, а фундаментальним фактором виживання та адаптації. Концептуальна модель адаптивного управління ІТ-проєктами, що розробляється, інтегрує модуль зворотного зв'язку та безперервного навчання як її невід'ємну частину. Цей модуль є свого роду мозком, що навчається, який дозволяє системі не просто реагувати на шоки, а й постійно еволюціонувати, перетворюючи кожен виклик на цінний урок, що посилює загальну стійкість та ефективність [27].

Процес безперервного навчання в умовах війни виходить за рамки традиційних ретроспектив. Це постійне, іноді інтуїтивне, але все частіше формалізоване осмислення досвіду. Він починається з ретельного аналізу даних виконання та оцінки результатів впроваджених адаптивних стратегій. Це означає не лише фіксацію, чи було рішення реалізовано, а й глибинний аналіз його фактичного впливу на проєктні метрики, інтегрований індекс стійкості та оцінку адаптивності. Важливо не просто констатувати факт збою чи успіху, а зануритися у кореневі причини відхилень. Наприклад, якщо

стратегія диверсифікації команди не дала очікуваного ефекту, необхідно з'ясувати, чи була проблема в координації, недостатній передачі знань, чи неврахованому психологічному факторі. Інтерв'ю з керівниками аутсорсингових компаній показали, що вони часто проводять після-інцидентні або «кризові ретроспективи», які є більш сфокусованими та оперативними, ніж звичайні, орієнтовані на виявлення саме уроків з воєнного досвіду [39].

Ключовим результатом цього аналізу є генерація отриманих уроків – дієвих інсайтів, які можуть бути застосовані для покращення майбутніх рішень. Ці уроки не є просто констатацією того, що сталося, а формулюваннями, що пропонують конкретні коригування для елементів моделі або загальних управлінських практик. Наприклад, якщо було виявлено, що протокол реагування на кібератаки виявився недостатнім під час масованої атаки, уроком буде не просто «протокол не спрацював», а «протокол потребує інтеграції з даними про геолокацію атаки для швидшого перекриття вразливостей». Респонденти з компаній, що оперують критичною інфраструктурою, підкреслювали, що кожен інцидент – чи то фізичне пошкодження підстанції, чи кібератака на OT-систему – стає джерелом для негайного перегляду та оновлення всіх відповідних протоколів безпеки та відновлення. Це дозволяє організації не просто реагувати, а вчитися на кожному, навіть найболючішому, досвіді.

Інституціоналізація цього досвіду є не менш важливою, ніж його збір. Це означає перетворення індивідуальних уроків на колективне, формалізоване знання, доступне для всієї організації. Рекомендовано створювати та постійно оновлювати централізовану базу знань «Уроки війни». Це може бути внутрішня Wiki-сторінка або спеціалізована платформа, де документуються: виявлені ризики, їхній фактичний вплив, застосовані стратегії, отримані результати, а також конкретні рекомендації щодо коригування процесів, інструментів та параметрів моделі. Керівники продуктових компаній згадували, що вони інтегрували нові знання у свої пайплайни розробки та CI/CD процеси, щоб автоматично враховувати уроки безпеки або оптимізації.

Це забезпечує, що нові співробітники або команди, що переключаються між проєктами, мають доступ до актуального досвіду, уникнувши повторення помилок.

Процес навчання не обмежується лише технічними аспектами. Він також стосується розвитку кризового мислення та адаптивних навичок у команди. На основі отриманих уроків можуть бути розроблені нові внутрішні тренінги, симуляції кризових ситуацій або воркшопи з управління стресом, що підвищують психологічну стійкість персоналу. Деякі компанії, що успішно адаптувалися, впроваджували сесії обміну досвідом, де співробітники з різних підрозділів ділилися своїми інсайтами щодо подолання конкретних викликів, що виникли під час війни. Це створює культуру безперервного навчання, де кожен член команди відчуває відповідальність за внесок у загальну стійкість організації.

Вихідні дані цього модуля – коригування моделі та отримані уроки – безпосередньо живлять інші компоненти фреймворку, замикаючи цикл управління. Вони можуть включати: перегляд вагових коефіцієнтів у формулах Модуля моніторингу, уточнення метрик у Модулі оцінки стійкості, розширення критеріїв прийняття рішень у відповідному Модулі або навіть доповнення арсеналу стратегій. Це забезпечує, що модель залишається релевантною та ефективною в динамічному середовищі, постійно адаптуючись до нових реалій. Коефіцієнт зростання стійкості (КЗС), про який згадувалося раніше, є кількісною ілюстрацією того, як модуль навчання сприяє підвищенню загальної міцності проєкту з часом, відображаючи реальне зростання здатності системи долати виклики.

Індекс ефективності навчання зображено у формулі:

$$ІЕН = \frac{Кількість\ успішно\ вирішених\ проблем}{Кількість\ виявлених\ проблем} \times Зменшення\ ЧЦА\ , \qquad (4.1)$$

де *Кількість успішно вирішених проблем* – число проблем, які були ефективно усунені завдяки коригуванням моделі на основі отриманих уроків;

Кількість виявлених проблем – загальне число проблем, що виникли за період;

Зменшення ЧЦА – відносне зменшення часу циклу адаптації (ЧЦА) для аналогічних проблемних ситуацій після впровадження уроків.

Високе значення ІЕН свідчить про ефективне навчання та успішну адаптацію системи.

Таким чином, Модуль зворотного зв'язку та безперервного навчання не просто замикає цикл управління, а створює спіраль постійного вдосконалення. Він перетворює кризові події з руйнівних загроз на джерело стратегічного знання, дозволяючи ІТ-проєктам не лише виживати в умовах війни, а й ставати сильнішими та адаптивнішими до майбутніх, навіть непередбачених, викликів. Цей модуль є втіленням принципів антикрихкості, роблячи модель живою та здатною до еволюції разом зі своїм складним середовищем, забезпечуючи довгострокову стійкість українського ІТ-сектору [6].

5 АПРОБАЦІЯ КОНЦЕПТУАЛЬНОЇ МОДЕЛІ АДАПТИВНОГО УПРАВЛІННЯ В УМОВАХ ВОЄННОГО КОНФЛІКТУ

5.1 Обґрунтування вибору кейс-стаді та методологія апробації

Завершальним, але не менш важливим етапом будь-якого наукового дослідження, що прагне мати практичну цінність, є демонстрація дієвості розроблених концепцій. У контексті кваліфікаційної роботи, присвяченої адаптивному управлінню ІТ-проєктами в умовах воєнного конфлікту, ця демонстрація набуває особливого значення. Адже мета дослідження полягала не лише в теоретичній розробці нової моделі, а й у наданні реальних, застосовних рекомендацій для керівників, що функціонують у надзвичайно складному середовищі. З огляду на це, було прийнято рішення провести апробацію ключових елементів концептуальної моделі у формі кейс-стаді. Цей підхід дозволив містком з'єднати теоретичні побудови з реальним досвідом, показавши, як абстрактні принципи можуть трансформуватися у конкретні, відчутні покращення у проєктному менеджменті.

Вибір компанії для проведення кейс-стаді був не випадковим і ґрунтувався на кількох ключових міркуваннях. Перевага була надана невеликій ІТ-компанії, яка до моменту апробації переважно покладалася на емпіричні підходи, інтуїцію та індивідуальний досвід своїх проєктних менеджерів. Такий вибір є надзвичайно релевантним, оскільки саме цей сегмент українського ІТ-бізнесу часто має обмежені ресурси для впровадження складних методологій та інструментів, але гостро відчуває потребу у структурованому підході в умовах воєнного часу. На відміну від великих корпорацій, які можуть мати вже розроблені BCP-плани та департаменти ризик-менеджменту, невеликі компанії нерідко змушені «винаходити велосипед» у відповідь на кожен новий виклик, що призводить до неефективності, стресу та підвищених ризиків. Їхній досвід є показовим для демонстрації того, як навіть часткове застосування пропонованої моделі може

радикально змінити ситуацію, підвищивши рівень керованості та стійкості. Цей вибір також логічно випливає з результатів інтерв'ю, проведених у Розділі 4, де було виявлено, що компанії, що покладаються лише на емпіричні підходи, є найбільш вразливими до кризових впливів [30].

Методологія апробації не передбачала повного, впровадження під ключ всієї концептуальної моделі, адже це є масштабним та тривалим процесом, що виходить за рамки студентської кваліфікаційної роботи. Натомість, фокус був зроблений на застосуванні та оцінці ефективності окремих, найбільш критичних елементів моделі, які були обрані за результатами попереднього аналізу виявлених ризиків та прогалин. Зокрема, особлива увага приділялася принципам ситуаційної обізнаності (Модуль моніторингу), аспектам людиноцентричного управління (інтегрованим у Модуль прийняття рішень та Модуль зворотного зв'язку) та елементам безперервного навчання (Модуль зворотного зв'язку). Цей вибірковий підхід дозволив сконцентрувати зусилля та чітко продемонструвати вплив конкретних інновацій, що були інспіровані розробленою моделлю.

Процес апробації був побудований на спільній роботі з керівництвом та проєктними менеджерами обраної компанії. Це включало:

– діагностичний етап. Проведення початкових напівструктурованих інтерв'ю з керівництвом компанії для глибокого розуміння їхніх поточних управлінських практик, основних болючих точок та викликів, з якими вони стикалися з початку війни. Це дозволило точно ідентифікувати сфери, де елементи розробленої моделі могли б принести найбільшу користь;

– етап рекомендацій та адаптації. Представлення обраних елементів концептуальної моделі (принципів, концептуальних метрик, підходів) та обговорення з керівництвом, як їх можна адаптувати до конкретних умов компанії та інтегрувати у вже існуючі (хоч і неформальні) процеси. Це не було нав'язуванням готових рішень, а спільним пошуком найбільш ефективних інструментів;

– етап застосування та моніторингу. Спостереження за процесом

застосування цих елементів у реальних проєктах протягом визначеного періоду. Це включало періодичні консультації з керівництвом, аналіз внутрішніх звітів компанії (якщо вони були доступні та релевантні) та збір якісних відгуків від проєктних команд.

Оцінка результатів базувалася переважно на якісних показниках, отриманих через повторні напівструктуровані інтерв'ю з керівництвом компанії після періоду застосування елементів моделі, а також на власних спостереженнях. Звісно, у такій короткостроковій апробації та без доступу до чутливих комерційних даних, можливість отримання вичерпних кількісних метрик була обмеженою. Проте якісні індикатори – такі як зміна рівня паніки під час кризових ситуацій, підвищення впевненості у прийнятті рішень, покращення внутрішньої комунікації, більша структурованість проєктних процесів – виступали яскравим свідченням позитивних трансформацій. Ця методологія дозволила створити переконливий наратив про те, як навіть невеликі зміни, інспіровані науково обґрунтованою моделлю, можуть значно підвищити стійкість та полегшити проєктний менеджмент у надзвичайно складних умовах воєнного часу.

5.2 Опис компанії до впровадження елементів моделі: емпіричне управління в хаосі

Для повноцінної демонстрації цінності та ефективності розробленої концептуальної моделі адаптивного управління IT-проєктами, необхідно чітко окреслити вихідну точку – стан компанії до того, як її управлінські процеси були інспіровані елементами запропонованого фреймворку. Кейс-стаді, що проводився в невеликій, але динамічній українській IT-компанії, виявив типову картину, характерну для багатьох гравців цього сегменту ринку, особливо після початку повномасштабного воєнного конфлікту. Її

управлінські підходи можна було охарактеризувати як переважно емпіричні, значною мірою засновані на інтуїції, особистому досвіді керівників та реактивному реагуванні на виклики.

До 24 лютого 2022 року компанія, хоча й працювала досить успішно, не мала чітко формалізованих та систематизованих процесів проєктного менеджменту, а тим паче, кризових планів. Управління проєктами здійснювалося за принципом «як виходить», спираючись на таланти та самоорганізацію ключових фахівців. Рішення приймалися швидко, часто на основі моментального аналізу ситуації та попереднього, хоча й обмеженого, досвіду, що був накопичений до війни. Здавалося, що в умовах відносної стабільності цього було достатньо для підтримки операційної діяльності та задоволення клієнтських вимог. Однак, цей існуючий «хаотичний порядок» був надзвичайно крихким і виявився повністю неспроможним перед обличчям безпрецедентних загроз, які принесла війна.

З початком повномасштабного вторгнення компанія зіткнулася з лавиною викликів, до яких вона була абсолютно не готова. Ситуаційна обізнаність була фрагментованою та емоційно забарвленою. Інформація про безпекову ситуацію (обстріли, тривоги, стан інфраструктури) надходила неструктуровано, переважно з Telegram-каналів, новинних стрічок та особистих контактів. Це призводило до постійної паніки, дезорієнтації та неможливості чітко оцінити реальний рівень загрози для співробітників та інфраструктури проєкту. Керівництво відчувало себе перевантаженим потоком неперевіреної інформації, що робило прийняття оперативних рішень надзвичайно складним і часто призводило до запізнілих реакцій або неоптимальних дій. Наприклад, рішення про евакуацію команди з певного району могли прийматися вже після того, як ситуація ставала критичною, що підвищувало ризики для персоналу.

Відсутність структурованого моніторингу інфраструктури була ще однією болючою точкою. Інформація про блекаути, збої інтернету та зв'язку збиралася постфактум, з особистих повідомлень співробітників або з

внутрішніх чатів. Це означало, що керівництво не мало цілісної картини доступності команди чи функціонування критичних сервісів. Проєкти часто зупинялися без попередження, оскільки виявлялося, що значна частина команди перебуває без світла чи зв'язку. Така ситуація створювала «сліпі зони» в управлінні, унеможливлюючи проактивне планування або перерозподіл ресурсів. Керівники не могли оперативно оцінити загальний вплив інфраструктурних проблем на терміни виконання завдань, що призводило до постійних зривів дедлайнів та напруги у відносинах з клієнтами.

Людський фактор, який є критично важливим в ІТ, в умовах хаосу ставав джерелом додаткових проблем. Компанія не мала системних програм психологічної підтримки або механізмів відстеження рівня стресу в команді. Керівництво реагувало на індивідуальні випадки вигорання чи проблем, але не мало цілісної картини стану команди. Гнучкість у графіках роботи надавалася переважно за запитом, а не як системна політика, що створювало додатковий тиск на співробітників, які намагалися поєднати роботу з реагуванням на повітряні тривоги чи особисті обставини. Комунікація з командою була переважно реактивною, зосередженою на вирішенні поточних проблем, а не на прозорому інформуванні чи підтримці морального духу. Це підвищувало рівень тривожності та невизначеності серед персоналу, потенційно збільшуючи ризик витоку кадрів.

Загалом, проєктний менеджмент у компанії, незважаючи на самовідданість команди, до початку впровадження елементів моделі був хаотичним та реактивним. Рішення приймалися «на колінах», під впливом емоцій або поточних подій, без належного аналізу всіх взаємозв'язків та довгострокових наслідків. Відсутність структурованих даних та системного підходу до моніторингу кризових факторів призводила до того, що компанія постійно «гасила пожежі», втрачаючи час та ресурси. Проєкти зазнавали постійних затримок, внутрішня напруга зростала, а керівництво відчувало себе перевантаженим та дезорієнтованим у цьому безпрецедентному середовищі.

Цей вихідний стан компанії, хоч і був типовим для багатьох невеликих IT-бізнесів, яскраво підкреслював критичну потребу у впровадженні більш адаптивних та структурованих підходів до управління, які були запропоновані в рамках даного дослідження [40].

5.3 Процес впровадження та застосування обраних елементів концептуальної моделі

Після глибокого аналізу вихідного стану компанії, що функціонувала в умовах «емпіричного хаосу», настав етап практичного впровадження та застосування обраних елементів розробленої концептуальної моделі. Цей процес не був радикальною трансформацією всієї компанії, а скоріше ітеративним підходом до інтеграції ключових принципів та механізмів, спрямованих на підвищення ситуаційної обізнаності, підтримку команди та впровадження елементів безперервного навчання. Мета полягала у демонстрації відчутних покращень навіть за умов часткового застосування моделі, що є особливо релевантним для невеликих компаній з обмеженими ресурсами.

Першим кроком у цьому процесі стало забезпечення покращеної ситуаційної обізнаності. Визнаючи фрагментований та неструктурований характер попереднього збору даних, ми зосередилися на впровадженні простих, але ефективних механізмів моніторингу, які відповідали б потребам компанії без створення надмірної бюрократії. Було запропоновано та протестовано протокол щоденного збору інформації про інфраструктурний стан. Співробітники почали заповнювати короткі форми або надсилати стандартизовані повідомлення через внутрішній чат про доступність електроенергії та інтернету у своїх локаціях, вказуючи тривалість відключень. Ці дані агрегувалися проєктними менеджерами у спільній електронній

таблиці, що дозволяло в режимі реального часу відстежувати загальний відсоток доступності команди та локалізувати зони з найбільшими проблемами. Це дало змогу керівництву швидко оцінювати вплив блекаутів на терміни проєктів та приймати рішення про перерозподіл завдань або надання додаткової підтримки. Наприклад, якщо зранку виявлялося, що значна частина розробників перебуває без світла, менеджер міг оперативно скоригувати плани на день, перекинувши менш залежні від енергопостачання завдання тим, хто мав доступ до генераторів, або ж зосередитися на плануванні замість кодування.

Крім інфраструктурного моніторингу, було звернено увагу на безпекову ситуацію. Компанія почала використовувати лише перевірені офіційні джерела для сповіщення про повітряні тривоги та загрози, відмовившись від хаотичного споживання новинних стрічок. Було запроваджено чіткий протокол реагування на тривоги, що включав обов'язкове призупинення роботи на час небезпеки та повернення до неї лише після відбою. Це дозволило зменшити паніку, підвищити почуття захищеності серед команди та забезпечити більш організований робочий процес.

Другим ключовим напрямком впровадження стало посилення людиноцентричних аспектів управління. Визнаючи значний психологічний тиск, що чинить війна, ми зосередилися на практиках, які підтримують благополуччя команди. Було рекомендовано та імплементовано гнучкі робочі графіки, що дозволяли співробітникам адаптуватися до повітряних тривог, відключень електроенергії та особистих обставин. Керівництво компанії почало активно практикувати більшу емпатію, регулярно проводячи короткі, неформальні «чекіни» з командою, щоб зрозуміти їхній емоційний стан та надати підтримку. Це не було формальним опитуванням, а скоріше щирою розмовою, що дозволила багатьом співробітникам почуватися більш захищеними та зрозумілими. Для підвищення прозорості та зниження рівня тривоги, керівництво почало проводити регулярні, хоча й короткі, «апдейти» щодо стану компанії, її фінансових перспектив та комунікації з клієнтами. Ця

відкритість, навіть щодо складних питань, значно знизила рівень невизначеності та сприяла підвищенню довіри всередині команди.

Третій напрямок впровадження стосувався принципів безперервного навчання. Компанія, яка раніше рідко проводила формалізовані ретроспективи, почала імплементувати «міні-ретроспективи» після значних кризових подій. Наприклад, після особливо тривалого блекауту або збою зв'язку, команда проводила короткі сесії, щоб обговорити, що спрацювало, що ні, і які уроки можна винести для майбутнього. Це дозволило ідентифікувати «вузькі місця» в протоколах реагування, покращити внутрішню комунікацію та розробити прості, але дієві рішення. Такі «уроки» документувалися у внутрішній базі знань (наприклад, у спільному документі або wiki-сторінці), що дозволило компанії не просто реагувати на виклики, а й системно вчитися на своєму досвіді, накопичуючи колективне знання. Це сприяло не тільки вирішенню поточних проблем, а й підвищенню загальної адаптивності та готовності до майбутніх криз.

Загалом, процес впровадження був поступовим і гнучким. Елементи моделі не нав'язувалися, а адаптувалися до реалій компанії, демонструючи, що навіть невеликі зміни, засновані на науково обґрунтованих принципах, можуть принести значні покращення. Керівництво компанії активно долучалося до процесу, що було вирішальним для успіху. Це спільне зусилля дозволило компанії почати перехід від інтуїтивного, реактивного управління до більш структурованого, проактивного та людиноцентричного підходу, що заклало фундамент для підвищення стійкості її проєктів у складних умовах воєнного конфлікту.

5.4 Оцінка результатів та отримані переваги

Завершальний етап апробації концептуальної моделі адаптивного управління полягав у ретельній оцінці фактичних результатів та переваг,

отриманих невеликою ІТ-компанією після застосування окремих елементів запропонованого фреймворку. Цей етап дав змогу не просто підтвердити теоретичні гіпотези, а й наочно продемонструвати, як цілеспрямовані, структуровані зміни можуть кардинально трансформувати проєктний менеджмент у вкрай нестабільному середовищі воєнного конфлікту. Оцінка проводилася переважно через якісні інтерв'ю з керівництвом та ключовими менеджерами компанії, що дозволило зафіксувати їхнє сприйняття змін та відчутні покращення.

Першим і найбільш відчутним результатом стало радикальне підвищення ситуаційної обізнаності та зниження хаосу. До впровадження, керівництво перебувало у постійному інформаційному вакуумі, реагуючи на події постфактум. Після запровадження протоколів щоденного збору даних про інфраструктурний стан (доступність електроенергії, інтернету) та безпекову ситуацію, менеджери отримали чітку, агреговану картину. Як зазначало керівництво, «це було ніби ми вперше побачили карту, а не просто блукали у темряві». Зникла постійна паніка від несподіваних блекаутів, адже тепер вони могли бачити загальну картину доступності команди і оперативно коригувати плани на день. Здатність бачити, скільки співробітників перебуває без зв'язку, дозволила уникнути непотрібних очікувань і перерозподілити завдання більш ефективно, замість витрачання часу на з'ясування причин простою. Це відчуття контролю, навіть у неконтрольованому середовищі, значно покращило психологічний клімат та дозволило приймати рішення не реактивно, а з певним ступенем упередження.

Зміни у людиноцентричному управлінні також принесли значні плоди, що безпосередньо вплинули на моральний дух та продуктивність команди. Запровадження гнучких графіків роботи, що враховували повітряні тривоги та інфраструктурні збої, а також більш емпатична та прозора комунікація з боку керівництва, мали потужний позитивний ефект. Було відзначено, що рівень стресу в команді, хоч і залишався високим через зовнішні обставини, став більш керованим. Співробітники відчули більшу підтримку та розуміння своїх

особистих обставин. Менеджери стали частіше виступати в ролі не просто «наглядачів», а й «опікунів» благополуччя команди, що зміцнило внутрішні зв'язки та лояльність. Ця зміна підходу дозволила компанії ефективніше утримувати своїх фахівців, адже, як було відзначено, «люди стали відчувати, що компанія дбає про них не лише як про робочу одиницю, а як про людину». Це опосередковано вплинуло на стабільність проєктів, оскільки знизився рівень непередбачених відсутностей та підвищилася загальна віддача команди, яка відчувала себе захищеною.

Впровадження елементів безперервного навчання додало неструктурованому проєктному менеджменту необхідну системність. Проведення «міні-ретроспектив» після кризових подій, хоч і були початковими та невеликими за обсягом, мали значний вплив. Компанія почала вчитися на своїх помилках, розробляючи та документуючи прості, але дієві протоколи реагування. Наприклад, після кількох випадків, коли команди не могли оперативно відновити роботу після блекауту, були розроблені чіткі інструкції щодо використання мобільних точок доступу та синхронізації прогресу через резервні канали. Менеджери зазначали, що «кожна наступна криза відчувалася менш хаотичною, тому що ми вже мали базовий план дій, вироблений на попередньому досвіді». Це дозволило скоротити час на відновлення операційної діяльності після збоїв та підвищити загальну ефективність реагування. З'явилося відчуття, що «ми не просто виживаємо, а стаємо сильнішими після кожного удару».

Загалом, застосування елементів концептуальної моделі привело до фундаментальних якісних покращень у проєктному менеджменті. Компанія відчула, що «життя стало кращим» не в сенсі зникнення загроз, а в сенсі підвищення здатності долати ці загрози. Проєктний менеджмент став більш структурованим – з'явилися чіткіші протоколи, дані для аналізу та обґрунтовані рішення. Він став більш проактивним – замість постійного «гасіння пожеж», керівництво почало передбачати потенційні проблеми та вживати превентивних заходів. І, що найважливіше, проєкти стали більш

стійкими – компанія відчула, що її внутрішні механізми захисту та адаптації дійсно працюють, дозволяючи зберегти ключових людей та продовжити роботу навіть у найскладніші періоди. Ці зміни не лише полегшили щоденне управління, а й заклали міцний фундамент для довгострокової життєздатності компанії в умовах триваючого конфлікту, демонструючи практичну цінність розробленої моделі.

5.5 Висновки з апробації та подальші перспективи

Завершення етапу апробації концептуальної моделі адаптивного управління ІТ-проєктами в умовах воєнного конфлікту стало важливим підтвердженням її потенційної дієвості та практичної цінності. Проведене кейс-стаді у невеликій ІТ-компанії, яка донедавна покладалася виключно на емпіричний досвід та інтуїцію, наочно продемонструвало, як навіть часткове впровадження елементів розробленого фреймворку може кардинально трансформувати проєктний менеджмент. Це був міст між абстрактними науковими побудовами та реальним, відчутним покращенням у здатності компанії функціонувати та розвиватися в умовах безпрецедентної невизначеності.

Ключові висновки з апробації свідчать про те, що запропонована модель дійсно закладає фундамент для більш структурованого, проактивного та людиноцентричного управління. Підвищення ситуаційної обізнаності, що стало можливим завдяки систематичному збору даних про інфраструктурні загрози та безпекову ситуацію, дозволило керівництву вийти зі стану постійної паніки та реагувати на виклики з більшою впевненістю. Замість хаотичного «гасіння пожеж», з'явилася можливість бачити цілісну картину, що безпосередньо вплинуло на швидкість та ефективність прийняття рішень. Елементи людиноцентричного управління, такі як гнучкі графіки та емпатична

комунікація, не лише покращили психологічний стан команди, але й зміцнили її лояльність та продуктивність, що є неоціненним активом у кризових умовах. Практики безперервного навчання, хоч і були запроваджені в мінімальному обсязі, вже показали свою спроможність, дозволивши компанії ідентифікувати «уроки» з кризових подій та оперативно коригувати свої внутрішні протоколи, запобігаючи повторенню помилок. Загальне відчуття керівництва компанії, що «життя стало кращим», і що проєктний менеджмент став більш «структурованим» та «керованим», є найпереконливішим якісним результатом цієї апробації.

Однак, важливо усвідомлювати обмеження проведеної апробації. З огляду на рамки кваліфікаційної роботи, дослідження було сфокусоване на невеликій ІТ-компанії та лише на окремих елементах концептуальної моделі. Відсутність широкого доступу до комерційних даних обмежувала можливості для повноцінного кількісного аналізу всіх показників, що були визначені в Модулі моніторингу чи Модулі оцінки стійкості. Також, відносно короткий період апробації не дозволив повною мірою подальші перспективи розвитку та впровадження концептуальної моделі є багатообіцяючими. Одним із ключових напрямків є розробка програмних інструментів, які автоматизуватимуть збір даних для модуля моніторингу, розрахунок індексів стійкості та адаптивності, а також візуалізацію ключових показників для модуля прийняття рішень. Такі інструменти значно полегшать використання моделі в реальних умовах, особливо для компаній з обмеженими ресурсами.

Іншою важливою перспективою є розширення апробації на більші компанії та різні типи ІТ-організацій, включаючи великі аутсорсингові компанії та ІТ-відділи критичної інфраструктури, що дозволить уточнити та адаптувати модель до їхніх специфічних потреб. Також перспективним є поглиблення кількісної оцінки ефективності моделі, використовуючи більш складні метрики та аналітичні методи для вимірювання впливу на терміни, бюджет та якість проєктів. Можливим є також інтеграція елементів штучного інтелекту та машинного навчання для підвищення ефективності модуля

моніторингу (наприклад, для прогнозування ризиків або виявлення аномалій у даних) та модуля прийняття рішень (для рекомендації оптимальних стратегій).

Нарешті, найважливішою перспективою є інституціоналізація та популяризація принципів адаптивного управління в умовах війни в українському ІТ-секторі. Ця концептуальна модель може стати основою для навчальних програм, тренінгів та воркшопів, що допоможуть керівникам проєктів та менеджерам отримати необхідні знання та навички для ефективної роботи в новому, складному світі. Таким чином, результати цієї кваліфікаційної роботи не лише підтверджують її наукову актуальність, а й прокладають шлях до практичних змін, що сприятимуть стійкості української ІТ-галузі та її внеску у післявоєнне відновлення країни.

ВИСНОВКИ

В ході виконання кваліфікаційної роботи було проведено комплексне дослідження еволюції управлінських підходів в ІТ-проєктах, з особливим акцентом на їхню адаптацію в умовах екстремальної невизначеності, спричиненої воєнним конфліктом. Метою роботи була розробка та обґрунтування концептуальної моделі адаптивних стратегій прийняття управлінських рішень, спрямованих на підвищення стійкості, ефективності та зниження ризиків ІТ-проєктів.

Для досягнення поставленої мети було виконано наступні задачі:

– поглиблено аналіз теоретичних підходів та емпіричного досвіду управління ІТ-проєктами в умовах воєнного конфлікту. Встановлено, що класичні методи управління проєктами та прийняття рішень (зокрема, SWOT, PESTLE-аналіз, дерево рішень, аналіз аитрат та вигод) виявилися значною мірою неадекватними для реагування на динамічні та хаотичні зміни, оскільки їхня ефективність залежить від стабільності середовища та повноти інформації, що є відсутньою в умовах війни;

– ідентифіковано та систематизовано ключові категорії ризиків (кадрові, інфраструктурні, фінансові, кібербезпекові, операційні), невизначеностей та викликів, зумовлених воєнним конфліктом. Висвітлено їхню взаємодію та кумулятивний ефект, що створює безпрецедентну складність для управління ІТ-проєктами, змушуючи відмовлятися від ілюзії повного контролю на користь адаптивних стратегій;

– розроблено та обґрунтовано концептуальну модель адаптивного управління ІТ-проєктами в умовах конфлікту. Модель базується на п'яти ключових принципах: тотальної обізнаності, стійкості за замовчуванням, динамічної адаптації та ітеративності, людиноцентричності та психологічної стійкості, а також безперервного навчання та інституціоналізації досвіду. Запропоновано архітектуру моделі, що включає п'ять взаємопов'язаних

модулів (моніторингу, оцінки стійкості та адаптивності, прийняття рішень, реалізації та контролю, а також зворотного зв'язку та навчання), які дозволяють системно реагувати на кризові умови;

– сформульовано практичні рекомендації для IT-менеджерів та керівників компаній щодо застосування адаптивних стратегій. Ці рекомендації охоплюють забезпечення ситуаційної обізнаності (систематичний збір даних про безпеку, інфраструктуру, кадрові показники), підвищення стійкості та адаптивності (інвестиції в інфраструктуру, диверсифікація команд, гнучкі процеси, кібербезпека, фінансова подушка), а також людиноцентричне управління та психологічну підтримку команди (фізична безпека, ментальне здоров'я, емпатична комунікація);

– проведено практичну апробацію ключових елементів розробленої моделі на прикладі невеликої української IT-компанії. Апробація підтвердила, що навіть часткове впровадження запропонованих принципів та механізмів суттєво підвищило ситуаційну обізнаність (знизило хаос, дозволило менеджерам «бачити карту»), покращило моральний дух та продуктивність команди (завдяки людиноцентричному підходу), а також сприяло формуванню системності та проактивності в управлінні проєктами (завдяки безперервному навчанню). Це продемонструвало практичну цінність та дієвість моделі в реальних умовах воєнного конфлікту.

Результати даної кваліфікаційної роботи підтверджують її наукову актуальність та практичну цінність, закладаючи фундамент для більш структурованого, проактивного та людиноцентричного управління IT-проєктами в умовах високої невизначеності.

Перспективи подальших досліджень включають розширення апробації розробленої моделі на більші IT-організації та різні типи проєктів, поглиблену кількісну оцінку її ефективності за допомогою більш складних метрик та аналітичних методів, а також інтеграцію елементів штучного інтелекту та машинного навчання для автоматизації процесів моніторингу, прогнозування ризиків та рекомендації оптимальних стратегій. Інституціоналізація та

популяризація принципів адаптивного управління в українському IT-секторі є ключовим напрямком для забезпечення довгострокової стійкості галузі та її внеску у післявоєнне відновлення країни.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. Project Management Institute. A guide to the project management body of knowledge (PMBOK guide). 2017. 756 p.

2. Larman C., Basili V. R. Iterative and incremental developments. a brief history. Computer. 2003. Vol. 36, no. 6. URL: https://doi.org/10.1109/mc.2003.1204375 (date of access: 20.05.2025).

3. Sutherland J. J. Scrum Fieldbook: Faster Performance. Better Results. Starting Now. Penguin Random House, 2020. 272 p.

4. Kanban: Successful Evolutionary Change for Your Technology Business. Sequim , Washington : Blue hole press, 2010. 261 p.

5. Software engineering: A practitioner's approach. Advances in Engineering Software (1978). 1983. Vol. 5, no. 3. P. 171. URL: https://doi.org/10.1016/0141-1195(83)90118-3 (date of access: 20.05.2025).

6. Mulla E. Antifragile: Things that Gain from Disorder. InnovAiT: Education and inspiration for general practice. 2019. Vol. 13, no. 2. P. 127. URL: https://doi.org/10.1177/1755738019885153 (date of access: 20.05.2025).

7. Renand F. Management challenges for the 21st century. Revista de Administração de Empresas. 2000. Vol. 40, no. 4. URL: https://doi.org/10.1590/s0034-75902000000400011 (date of access: 20.05.2025).

8. Dorf R. C., Raitanen M. The Balanced Scorecard: Translating Strategy Into Action. Proceedings of the IEEE. 1997. Vol. 85, no. 9. P. 1509–1510. URL: https://doi.org/10.1109/jproc.1997.628729 (date of access: 20.05.2025).

9. The Lean Startup: How Today's Entrepreneurs Use Continuous Innovation to Create Radically Successful Businesses. Crown Business, 2011. 336 p.

10. The fifth discipline: the art and practice of the learning organization. Choice Reviews Online. 2007. Vol. 44, no. 05. P. 44–2797–44–2797. URL: https://doi.org/10.5860/choice.44-2797 (date of access: 20.05.2025).

11. Perera R. PESTLE Analysis. Independently Published, 2017. 27 p.

12. Porter M. E. Competitive strategy: Techniques for analyzing industries and competitors. New York : Free Press, 1980. 396 p.

13. Ward J., Daniel E. Benefits Management: Delivering Value from IS and IT Investments. Wiley & Sons, Incorporated, John, 2010. 418 p.

14. Risk management organisation and context / ed. by I. o. R. Management. London : Witherby & Co., 2005. 222 p.

15. Ward S., Chapman C. Transforming project risk management into project uncertainty management. International Journal of Project Management. 2003. Vol. 21, no. 2. URL: https://doi.org/10.1016/s0263-7863(01)00080-1 (date of access: 20.05.2025).

16. Studies of human error. Human Error. 1990. P. 19–52. URL: https://doi.org/10.1017/cbo9781139062367.003 (date of access: 20.05.2025).

17. Kahneman D., Tversky A. Prospect Theory. An Analysis of Decision Making Under Risk. Fort Belvoir, VA : Defense Technical Information Center, 1977. URL: https://doi.org/10.21236/ada045771 (date of access: 20.05.2025).

18. The end of competitive advantage: How to keep your strategy moving as fast as your business. Harvard Business Review Press, 2013. 204 p.

19. Goleman T. S., Intelligence E. Emotional Intelligence: The Ultimate Guide for Cognitive Behavioral Therapy , How to Analyze People, Success at Work, Better Life & Relationships with Positive Psychology Mindset Coaching 2. 0. Independently Published, 2019.

20. McLennan M. Global Risks Report 2024. 19th ed. Geneva : World Economic Forum, 2024. 124 p.

21. Vos P. War, Peace and Military Chaplaincy: Lessons Learned from Ukraine. Handelingen: Tijdschrift voor Praktische Theologie en Religiewetenschap. 2023. Vol. 50, no. 3.. URL: https://doi.org/10.54195/handelingen.18003 (date of access: 20.05.2025).

22. Dligach A., Stavytskyy A. Resilience Factors of Ukrainian Micro, Small, and Medium-Sized Business. Economies. 2024. Т. 12, № 12. С. 319. URL:

https://doi.org/10.3390/economies12120319.

23. Global Outlook. Global Economic Prospects, January 2024. 2024. P. 1–50. URL: https://doi.org/10.1596/978-1-4648-2017-5_ch1 (date of access: 20.05.2025).

24. WORLD ECONOMIC OUTLOOK 2024 APR Steady but Slow: Resilience amid Divergence. Washington : INTERNATIONAL MONETARY FUND, 2024. 202 p.

25. Struk N. Ukraine's Economic Recovery. The Economics of Russia’s War in Ukraine. London, 2024. URL: https://doi.org/10.4324/9781003435433-6 (date of access: 20.05.2025).

26. Digital Tiger: the Power of Ukrainian IT. Kyiv : IT Ukraine Association, 2024. 66 p.

27. Smith-Brooks A. Leading Through Crisis. Advanced Emergency Nursing Journal. 2020. Vol. 42, no. 3. URL: https://doi.org/10.1097/tme.0000000000000304 (date of access: 20.05.2025).

28. Loshin D. Practitioner's Guide to Data Quality Improvement. Elsevier Science & Technology Books, 2010.

29. Najdzik K. Armed conflict risk management – Ukraine casus. Nowoczesne Systemy Zarządzania. 2019. Vol. 14, no. 3. P. 123–132. URL: https://doi.org/10.37055/nsz/132728 (date of access: 20.05.2025).

30. Дудко В., Мельник Т., Шкальова А. Як українська IT-індустрія пережила 2022 рік. Forbes.ua. URL: https://forbes.ua/innovations/it-voennogo-chasu-yak-ukrainska-tekhindustriya-proyshla-mozhlivo-nayvazhchiy-rik-u-svoiy-istorii-u-shesti-grafikakh-23122022-10676 (дата звернення: 20.05.2025).

31. Epel O. V. Lack of labor resources as a challenge for the post-war reconstruction of Ukraine. Al′manah prava. 2024. No. 15. P. 111–119. URL: https://doi.org/10.33663/2524-017x-2024-15-111-119 (date of access: 20.05.2025).

32. Ukraine - Third Rapid Damage and Needs Assessment (RDNA3), February 2022 – December 2023. Washington, DC: World Bank, 2024. URL: https://doi.org/10.1596/41082 (date of access: 20.05.2025).

33. Snider L. Psychological first aid: Guide for field workers / ed. by V. O. M. 1969- et al. Geneva, Switzerland : World Health Organization, 2011. 60 p.

34. Cybersecurity and Infrastructure Security Agency. Insider Threat Mitigation Guide : Defining, Detecting, Assesing, and Managing Insider Threats: Cybersecurity and Infrastructure Security Agency. Independently Published, 2022.

35. Čelesnik G., Radujković M., Vrečko I. Resolving Companies in Crisis: Agile Crisis Project Management. Organizacija. 2018. Vol. 51, no. 4. P. 223–237. URL: https://doi.org/10.2478/orga-2018-0023 (date of access: 20.05.2025).

36. Portny S. E. Project Management for Dummies. Wiley & Sons, Incorporated, John, 2010. 384 p.

37. Ziółkowski A., Deręgowski T. Hybrid Approach in Project Management – Mixing Capability Maturity Model Integration with Agile Practices. Social Sciences. 2014. Vol. 85, no. 3. URL: https://doi.org/10.5755/j01.ss.85.3.8416 (date of access: 20.05.2025).

38. Hayward G. Project management demystified. Technovation. 1993. Vol. 13, no. 4. P. 261. URL: https://doi.org/10.1016/0166-4972(93)90023-o (date of access: 20.05.2025).

39. Leigh A. Leadership on the Line: Staying Alive through the Dangers of Leading. The Leadership Quarterly. 2003. Vol. 14, no. 3. P. 347–356. URL: https://doi.org/10.1016/s1048-9843(03)00022-5 (date of access: 20.05.2025).

40. Data-driven intelligence in crisis: The case of Ukrainian refugee management / K. Sprenkamp et al. Government Information Quarterly. 2025. Vol. 42, no. 1. P. 101978. URL: https://doi.org/10.1016/j.giq.2024.101978 (date of access: 20.05.2025).