УДК 331.1:316.77:004.77
DOI: https://doi.org/10.32782/2786-8141/2026-15-8

Дегтярь Д. В.
аспірант,
Донецький національний університет імені Василя Стуса
ORCID: https://orcid.org/0009-0009-1571-9644
Dmytro Dehtiar
Vasyl' Stus Donetsk National University

СТРАТЕГІЯ МІНІМІЗАЦІЇ РИЗИКІВ ТА ПІДВИЩЕННЯ СТІЙКОСТІ ГЕОРОЗПОДІЛЕНИХ ІТ-КОМАНД В УМОВАХ НЕСТАБІЛЬНОСТІ

STRATEGY FOR MINIMIZING RISKS AND ENHANCING THE RESILIENCE OF REMOTE IT TEAMS IN VOLATILITY

Анотація. *У статті обґрунтовано актуальність формування стратегії мінімізації ризиків та підвищення стійкості георозподілених ІТ-команд в умовах нестабільності, спричиненої воєнними, економічними та технологічними викликами. Визначено, що георозподілені команди виступають домінуючою формою організації діяльності ІТ-компаній, що зумовлює необхідність адаптації підходів до управління з урахуванням асинхронної комунікації, мультикультурності, високої залежності від цифрової інфраструктури та глобального характеру взаємодії. Сформульовано авторське визначення стратегії мінімізації ризиків та підвищення стійкості георозподілених ІТ-команд як комплексної системи управлінських рішень, спрямованих на ідентифікацію, оцінку та зниження ризиків, а також забезпечення здатності команд адаптуватися до змін, протистояти кризовим впливам і відновлювати ефективну діяльність. Обґрунтовано структурні елементи стратегії, зокрема принципи, фактори впливу, суб'єкти управління, інструменти та ресурси, а також алгоритм її реалізації. Визначено ключові принципи, серед яких адаптивність, проактивність, системність, гнучкість, цифровізація, людиноцентричність, прозорість та безперервне вдосконалення. Розроблено інтегровану концептуальну модель стратегії, яка поєднує підходи управління ризиками та модель організаційної стійкості, що базується на взаємозв'язку адаптивності, стійкості до шоків і відновлюваності. Доведено, що врахування зовнішніх (військові дії, кіберзагрози, економічна нестабільність, глобальний ринок, нормативно-правове середовище, технологічні зміни) та внутрішніх факторів (цифрова зрілість, структура команди, компетенції персоналу, комунікації, ресурси) забезпечує підвищення обґрунтованості управлінських рішень. Встановлено, що реалізація запропонованої стратегії сприяє підвищенню стійкості георозподілених ІТ-команд, зростанню продуктивності та якості роботи, мінімізації ризиків і втрат, покращенню комунікації, підвищенню рівня довіри та залученості персоналу, забезпеченню безперервності бізнес-процесів і формуванню конкурентних переваг.*

Ключові слова: *георозподілені ІТ-команди, управління ризиками, стійкість, стратегія, модель, адаптивність, комунікації, корпоративна культура, управління персоналом, цифрова економіка, цифрові технології, воєнний стан.*

Abstract. *The article substantiates the relevance of forming a strategy for minimizing risks and increasing the resilience of remote IT teams in the conditions of instability caused by military, economic and technological challenges. It is determined that remote teams are the dominant form of organizing the activities of IT companies, which necessitates the adaptation of management approaches taking into account asynchronous communication, multiculturalism, high dependence on digital infrastructure and the global nature of interaction. The author's definition of the strategy for minimizing risks and increasing the resilience of remote IT teams is formulated as a comprehensive system of management decisions aimed at identifying, assessing and reducing risks, as well as ensuring the ability of teams to adapt to changes, resist crisis impacts and restore effective activity. The structural elements of the strategy are substantiated, in particular, principles, influencing factors, management subjects, tools and resources, as well as the results of its implementation. Key principles have been identified, including adaptability, proactivity, systematicity, flexibility, digitalization, people-centeredness, transparency, and continuous improvement. An integrated conceptual model of strategy has been developed that combines risk management approaches and an organizational resilience model based on the interrelationship of adaptability, shock resistance, and resilience. It has been proven that taking into account external (military actions, cyber threats, economic instability, global market, regulatory environment, technological changes) and internal factors (digital maturity, team structure, personnel competencies, communications, resources) ensures increased validity of management decisions. It has been established that the implementation of the proposed strategy contributes to increasing the resilience of remote IT teams, increasing productivity and quality of work, minimizing risks and losses, improving communication, increasing the level of trust and staff involvement, ensuring the continuity of business processes and creating competitive advantages.*

Keywords: *remote IT teams, risk management, resilience, strategy, model, adaptability, communications, corporate culture, human resources management, digital economy, digital technologies, martial law.*

Постановка проблеми. Сучасний розвиток ІТ-індустрії характеризується активною трансформацією організаційних форм праці, серед яких провідне місце займають георозподілені команди. Такий формат взаємодії забезпечує доступ до глобального ринку талантів, підвищує гнучкість бізнес-процесів та сприяє оптимізації витрат, однак одночасно супроводжується зростанням складності управління та підвищенням рівня ризиків. Особливої гостроти зазначена проблема набуває в умовах нестабільності, спричиненої військовими діями, економічними кризами та зростанням кіберзагроз. Для георозподілених ІТ-команд, значна частина яких функціонує в умовах воєнного стану, характерними є такі дестабілізуючі фактори, як порушення комунікацій, нестабільність енергетичної та цифрової інфраструктури, вимушена релокація

працівників, підвищене психоемоційне навантаження, а також ризики втрати або компрометації даних.

Водночас традиційні підходи до управління ризиками, сформовані в умовах відносної стабільності та локалізованих організаційних структур, не враховують специфіки георозподілених ІТ-команд, зокрема асинхронності комунікацій, мультикультурності, децентралізації управління та високої залежності від цифрових технологій. Це зумовлює їхню обмежену ефективність у сучасних умовах. Отже, виникає об'єктивна необхідність у розробці науково обґрунтованої стратегії мінімізації ризиків та підвищення стійкості георозподілених ІТ-команд, яка б враховувала сучасні виклики нестабільного середовища, специфіку ІТ-сфери та особливості функціонування команд в умовах воєнного стану.

Аналіз останніх досліджень і публікацій. Проблематика управління георозподіленими командами в ІТ-сфері активно досліджується як у зарубіжній, так і у вітчизняній науковій літературі, що зумовлено стрімким розвитком цифрової економіки, глобалізацією ринку праці та поширенням дистанційних і гібридних форм організації діяльності. Значний внесок у формування теоретичних засад управління віртуальними та георозподіленими командами здійснили зарубіжні дослідники. Зокрема, С. Ярвенпаа (S. Jarvenpaa) та Д. Лайднер (D. Leidner) [1] обґрунтовують у своїх працях ключову роль довіри та комунікації у забезпеченні ефективності глобальних віртуальних команд, визначено особливості формування міжособистісної взаємодії в умовах цифрового середовища. Г. Хертел (G. Hertel), С. Гайстер (S. Geister) та У. Конрадт (U. Konradt) [2] узагальнюють емпіричні підходи до управління віртуальними командами, виокремлено організаційні, технологічні та соціально-психологічні чинники їх результативності. Окремий напрям досліджень пов'язаний із управлінням ризиками в георозподілених командах. Зокрема, Дж. С. Перссон (J. S. Persson) та Л. Матіассен (L. Mathiassen) [3] пропонують процесний підхід до ідентифікації, оцінки та управління ризиками в розподілених командах, що враховує специфіку віртуальної взаємодії.

В українському науковому просторі дослідження георозподілених ІТ-команд набуває особливої актуальності у зв'язку з розвитком ІТ-сектору, цифровізацією економіки та функціонуванням підприємств в умовах воєнного стану. Вітчизняні науковці зосереджують увагу на адаптації міжнародного досвіду до національних умов, досліджені трансформації управління персоналом, розвитку цифрових інструментів комунікації та забезпеченні безперервності бізнес-процесів [4; 5]. Окремо досліджуються питання впливу війни на організацію праці, релокацію персоналу та підвищення ролі психологічної підтримки працівників [6; 7]. У контексті сучасних викликів значної актуальності набувають дослідження організаційної стійкості (resilience), інтеграції ризик-менеджменту з цифровими інструментами та Agile-підходами, що є особливо актуальним для ІТ-сфери [8; 9; 10].

Незважаючи на наявність значної кількості досліджень у сфері управління проєктами, ризик-менеджменту та організації дистанційної роботи, питання формування цілісної стратегії мінімізації ризиків та підвищення стійкості георозподілених ІТ-команд, особливо в умовах війни, залишаються недостатньо розробленими. Зокрема, потребують подальшого наукового обґрунтування складові такої стратегії, механізми її реалізації, а також інтеграція моделей організаційної стійкості в систему управління командами.

Метою статті є розробка теоретико-методичних засад формування стратегії мінімізації ризиків та підвищення стійкості георозподілених ІТ-команд в умовах нестабільності, зокрема воєнного стану, шляхом обґрунтування її структурних елементів, принципів, інструментів реалізації та побудови інтегрованої моделі стійкості, що базується на взаємозв'язку адаптивності, стійкості до шоків і відновлюваності.

Виклад основного матеріалу дослідження. Сучасний етап розвитку ІТ-індустрії характеризується масштабною цифровізацією, глобалізацією та поширенням георозподілених моделей організації праці. Особливої актуальності набуває проблема забезпечення ефективності та стійкості функціонування таких команд в умовах кризових явищ, зокрема воєнних конфліктів, економічної нестабільності та кіберзагроз. Необхідність формування стратегії мінімізації ризиків та підвищення стійкості георозподілених ІТ-команд обумовлюється такими чинниками: зростання ролі георозподілених команд як домінуючої форми організації ІТ-проєктів; підвищення складності координації та комунікації, що призводить до інформаційних бар'єрів та часових лагів; вплив війни та міграційних процесів, що змінюють структуру людського капіталу та організацію праці; зростання кіберризиків та загроз безпеці даних, пов'язаних із геополітичними факторами; неадекватність традиційних підходів до ризик-менеджменту, сформованих у стабільному середовищі. Отже, стратегія має носити адаптивний, багаторівневий та динамічний характер, орієнтований на забезпечення безперервності діяльності.

Стратегію мінімізації ризиків та підвищення стійкості георозподілених ІТ-команд доцільно визначати як інтегровану систему цілей, принципів, інструментів і управлінських рішень, спрямованих на ідентифікацію, оцінку та зниження ризиків, а також на забезпечення здатності команди адаптуватися до змін, протистояти кризовим впливам і ефективно відновлювати свою діяльність в умовах нестабільності, з урахуванням специфіки ІТ-сфери та географічної розподіленості (рис. 1).

Формування стратегії мінімізації ризиків та підвищення стійкості георозподілених ІТ-команд відбувається під впливом комплексу взаємопов'язаних зовнішніх і внутрішніх факторів, які визначають умови функціонування команд, характер ризиків та можливості забезпечення їх ефективності. Системний аналіз зазначених факторів є необхідною передумовою розробки адаптивної та результативної стратегії в умовах нестабільності.

Зовнішні та внутрішні фактори формують складне динамічне середовище функціонування георозподілених ІТ-команд, яке характеризується високим рівнем невизначеності та ризиків (рис. 2).

Зовнішні фактори формують сукупність викликів і обмежень, що безпосередньо впливають на функціонування георозподілених ІТ-команд. До них належать військові дії та безпекові ризики, які підвищують рівень невизначеності, спричиняють перебої інфраструк-

Рисунок 1 – Інтегрована концептуальна модель стратегії мінімізації ризиків та підвищення стійкості георозподілених IT-команд в умовах нестабільності

Джерело: сформовано автором

тури та потребу релокації персоналу; кіберзагрози, що посилюються в умовах геополітичної напруги; а також вплив глобального ринку IT-послуг, який зумовлює високі вимоги до якості, швидкості та координації роботи. Важливу роль відіграють економічна нестабільність і нормативно-правове середовище, що визначають ресурсні можливості компаній та умови їх діяльності. Додатково технологічні зміни формують як нові можливості, так і нові ризики, вимагаючи постійного оновлення підходів до управління.

Внутрішні фактори визначають здатність організації ефективно реагувати на зовнішні виклики та забезпечувати стійкість команд. Ключовими серед них є рівень цифрової зрілості, який впливає на ефективність віддаленої взаємодії, структура та культура команди, що визначають швидкість прийняття рішень і рівень довіри, а також компетенції персоналу як основного ресурсу IT-команд. Важливу роль відіграють корпоративна культура та рівень комунікацій, які забезпечують узгодженість дій і знижують ризики взаємодії. Наявність достатніх ресурсів та надійної інфраструктури є базовою умовою безперервного функціонування команд навіть у кризових ситуаціях.

Комплексне врахування середовища та факторів впливу дозволяє сформувати обґрунтовану стратегію, спрямовану на підвищення адаптивності, стійкості до шоків та відновлюваності команд, що є ключовими передумовами їх ефективної діяльності в умовах нестабільності.

Реалізація стратегії мінімізації ризиків та підвищення стійкості георозподілених ІТ-команд базується на сукупності взаємопов'язаних принципів, що забезпечують її ефективність у нестабільному середовищі [10].

Принцип адаптивності передбачає здатність команди та організації оперативно реагувати на зміни зовнішніх і внутрішніх умов, трансформуючи процеси та управлінські підходи. Проактивність орієнтує на попередження ризиків шляхом їх ранньої ідентифікації та розробки превентивних заходів. Системність забезпечує комплексне врахування взаємозв'язків між усіма елементами стратегії, включаючи ризики, ресурси та результати діяльності. Водночас гнучкість визначає можливість швидкого коригування управлінських рішень і організаційних структур відповідно до динаміки ІТ-середовища.

Принцип цифровізації передбачає широке використання сучасних технологій та цифрових інструментів

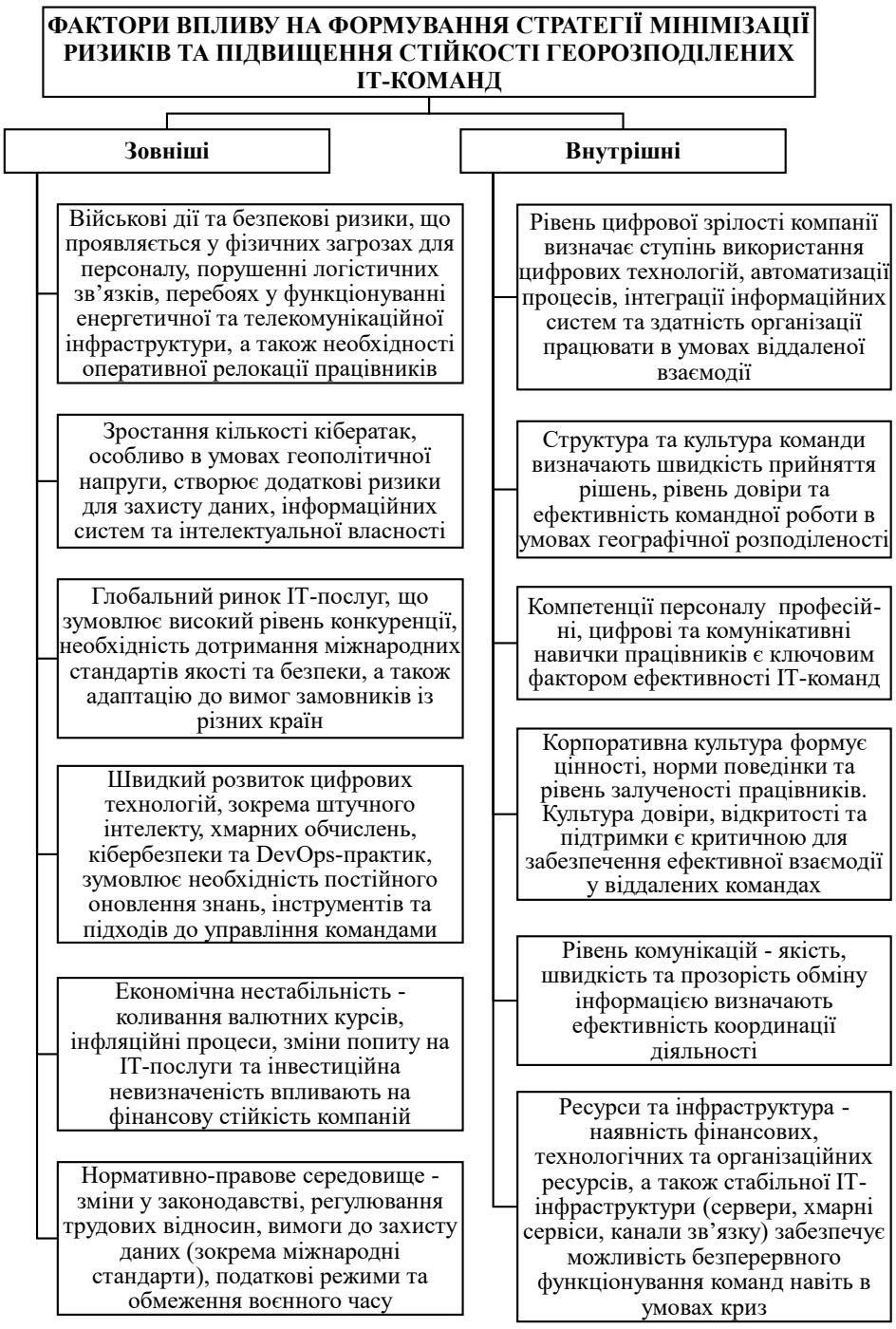

Рисунок 2 – Фактори впливу на формування стратегії мінімізації ризиків та підвищення стійкості георозподілених ІТ-команд

Джерело: сформовано автором

для підтримки комунікації, управління проєктами та забезпечення безпеки даних. Людиноцентричність акцентує увагу на ролі персоналу як ключового ресурсу, враховуючи його потреби, мотивацію та психоемоційний стан, особливо в умовах війни. Прозорість та довіра сприяють ефективній взаємодії в георозподілених командах, знижуючи рівень невизначеності та конфліктності. Завершальним є принцип безперервного вдосконалення, який забезпечує постійний перегляд і оновлення стратегії на основі отриманого досвіду та зворотного зв'язку. Дотримання зазначених принципів забезпечує цілісність, адаптивність і результативність стратегії, створюючи підґрунтя для ефективного управління ризиками та підвищення стійкості георозподілених ІТ-команд в умовах нестабільності.

Блок управління та координації є ключовим елементом реалізації стратегії мінімізації ризиків та підвищення стійкості георозподілених ІТ-команд, оскільки забезпечує узгодженість дій усіх учасників процесу [2]. Провідну роль у цьому блоці відіграє топ-менеджмент, який визначає стратегічні орієнтири, формує політику управління ризиками та забезпечує ресурсну підтримку. Проєктні менеджери здійснюють оперативне управління командами, координують виконання завдань, забезпечують комунікацію та контролюють дотримання термінів і якості результатів. Важливу функцію виконує HR-служба, яка відповідає за формування кадрового потенціалу, розвиток компетенцій персоналу, адаптацію працівників та підтримку їх психологічної стійкості.

ІТ-спеціалісти забезпечують технічну реалізацію проєктів, підтримують функціонування цифрових систем і впроваджують інноваційні рішення, що підвищують ефективність роботи команд. Служба кібербезпеки відповідає за захист інформаційних ресурсів, запобігання кіберзагрозам та забезпечення безперервності функціонування ІТ-інфраструктури. Безпосередні виконавці – команди – реалізують проєктні завдання, забезпечують обмін знаннями та формують основу організаційної стійкості через ефективну взаємодію. Узгоджена взаємодія всіх зазначених суб'єктів забезпечує синергічний ефект та підвищує здатність організації ефективно реагувати на виклики нестабільного середовища.

Блок інструментів та ресурсів забезпечує практичну реалізацію стратегії мінімізації ризиків і підвищення стійкості георозподілених ІТ-команд, інтегруючи методологічні, технологічні та кадрові складові. В основі лежать методології та процеси, зокрема Agile-підходи (Scrum, Kanban), DevOps-практики, а також формалізовані процедури управління ризиками (risk register, оцінка ризиків, сценарне планування), що забезпечують гнучкість і керованість процесів. Цифрові інструменти (системи управління проєктами, платформи комунікації, засоби моніторингу) підтримують координацію діяльності команд, прозорість процесів і оперативний обмін інформацією в умовах географічної розподіленості.

Важливу роль відіграє технологічна інфраструктура, яка включає хмарні сервіси, розподілені обчислювальні ресурси, резервні системи збереження даних та інструменти забезпечення безперервності бізнес-процесів. Невід'ємною складовою є кібербезпека, що передбачає використання систем захисту інформації, контролю доступу, шифрування даних та механізмів протидії кібератакам, особливо актуальних у період воєнної нестабільності. Центральним елементом виступає людський капітал, який охоплює професійні, цифрові та комунікативні компетенції працівників, їх здатність до адаптації, самоорганізації та роботи в мультикультурному середовищі.

З урахуванням представленої концептуальної моделі, зазначені інструменти та ресурси забезпечують підтримку ключових компонентів стійкості – адаптивності, стійкості до шоків і відновлюваності, формуючи основу ефективного функціонування георозподілених ІТ-команд.

Запропонована стратегія має комплексний та багаторівневий характер і передбачає інтеграцію двох ключових управлінських контурів:

1. Контур управління ризиками, що орієнтований на: виявлення потенційних загроз (технологічних, організаційних, кадрових, кібернетичних); оцінку їх ймовірності та впливу; розробку заходів мінімізації або запобігання ризикам; постійний моніторинг та оновлення ризик-профілю [8].

2. Контур забезпечення стійкості (resilience), що орієнтований на: розвиток адаптивності команди; забезпечення стійкості до зовнішніх шоків; формування механізмів швидкого відновлення після криз.

Реалізація стратегії мінімізації ризиків та підвищення стійкості георозподілених ІТ-команд забезпечує досягнення комплексних організаційних, економічних і соціальних результатів. Насамперед, відбувається підвищення стійкості команд, що проявляється у їх здатності ефективно функціонувати в умовах нестабільності, адаптуватися до змін та швидко відновлюватися після кризових впливів. Важливим результатом є зростання продуктивності та якості роботи, що досягається завдяки оптимізації процесів, використанню сучасних цифрових інструментів і підвищенню рівня координації. Одночасно забезпечується мінімізація ризиків і пов'язаних із ними втрат, що сприяє підвищенню ефективності використання ресурсів.

Суттєвою перевагою є підвищення рівня довіри в команді, яке формується через прозорість управління, налагоджену комунікацію та підтримку корпоративної культури. Це, у свою чергу, сприяє покращенню комунікаційних процесів, зниженню інформаційних бар'єрів і підвищенню швидкості прийняття рішень. Важливим соціальним ефектом виступає зростання задоволеності та залученості персоналу, що позитивно впливає на мотивацію, зменшує плинність кадрів і підвищує рівень відповідальності працівників.

Крім того, стратегія забезпечує безперервність бізнес-процесів, навіть за умов зовнішніх шоків, що є критично важливим для ІТ-компаній. У довгостроковій перспективі це формує конкурентні переваги та підвищує інноваційний потенціал організації, оскільки стійкі команди здатні швидше впроваджувати нові технології та адаптуватися до змін ринку. Узагальнюючи, результати реалізації стратегії мають синергічний характер і сприяють підвищенню загальної ефективності та конкурентоспроможності ІТ-компаній в умовах нестабільності.

Стратегія мінімізації ризиків та підвищення стійкості має формуватися з урахуванням специфіки георозподілених ІТ-команд, для яких характерна висока

залежність від цифрової інфраструктури та безперервності її функціонування. Критично важливим є забезпечення сталих комунікаційних процесів, оскільки ефективна взаємодія в таких командах здійснюється переважно через цифрові канали та в асинхронному форматі [4]. Використання гнучких методологій управління (Agile, DevOps) зумовлює необхідність швидкого прийняття рішень, постійної адаптації процесів і високого рівня самоорганізації учасників. Водночас глобальний характер діяльності та мультикультурність команд підсилюють вимоги до координації, управління часовими зонами та міжкультурної комунікації, а висока мобільність персоналу потребує гнучких підходів до організації праці та управління знаннями.

В умовах воєнного стану стратегія набуває додаткового змісту, орієнтованого на забезпечення безперервності діяльності в умовах підвищених ризиків та невизначеності. Зокрема, вона передбачає створення резервних технічних рішень для підтримки роботи при перебоях енергопостачання та зв'язку, організацію ефективної віддаленої взаємодії в умовах релокації працівників, а також посилення кіберзахисту інформаційних систем. Важливим компонентом є підтримка психологічної стійкості персоналу, що сприяє збереженню продуктивності та зниженню впливу стресових факторів [6]. Крім того, стратегія має включати розробку альтернативних сценаріїв функціонування та резервних каналів комунікації, що забезпечує підвищення загальної стійкості георозподілених ІТ-команд.

Таким чином, запропонована стратегія є інтегрованою управлінською концепцією, яка поєднує інструменти ризик-менеджменту та модель організаційної стійкості, що дозволяє забезпечити ефективне функціонування георозподілених ІТ-команд у складних та нестабільних умовах.

Висновки. В умовах цифрової трансформації та зростання нестабільності, зокрема воєнного стану, георозподілені ІТ-команди виступають ключовою формою організації діяльності, що зумовлює необхідність формування комплексної стратегії управління ризиками та підвищення їх стійкості. Визначено, що ефективне управління такими командами потребує інтеграції підходів ризик-менеджменту та концепції організаційної стійкості. Запропоновано авторське визначення стратегії та розкрито її ключові структурні елементи, включаючи принципи, фактори впливу, інструменти, суб'єкти та алгоритм реалізації.

Особливу увагу приділено розробці інтегрованої концептуальної моделі, яка поєднує управління ризиками із моделлю стійкості, що базується на взаємозв'язку адаптивності, стійкості до шоків і відновлюваності. Доведено, що врахування зовнішніх і внутрішніх факторів дозволяє підвищити обґрунтованість стратегічних рішень та забезпечити ефективну адаптацію до динамічного середовища. Обґрунтовано роль управлінських суб'єктів, інструментів і ресурсів у забезпеченні узгодженості дій та підвищенні результативності командної діяльності.

Встановлено, що реалізація запропонованої стратегії сприяє підвищенню стійкості команд, зростанню продуктивності, покращенню комунікацій, зниженню ризиків та забезпеченню безперервності бізнес-процесів. Практичне значення отриманих результатів полягає у можливості їх застосування ІТ-компаніями для підвищення ефективності управління георозподіленими командами в умовах невизначеності. Перспективи подальших досліджень пов'язані з розробкою методів кількісної оцінки рівня стійкості команд та впровадженням цифрових інструментів прогнозування ризиків.

Бібліографічний список:

1. Sirkka L. Jarvenpaa, Dorothy E. Leidner. Communication and Trust in Global Virtual Teams. *Journal of Computer-Mediated Communication*. 1998. Vol. 3, Is. 4. DOI: https://doi.org/10.1111/j.1083-6101.1998.tb00080.x

2. Hertel G., Geister S., Konradt U. Managing virtual teams: A review of current empirical research. *Human Resource Management Review.* 2005. Vol. 15, Is. 1. P. 69–95.

3. Persson J., Mathiassen L. A Process for Managing Risks in Distributed Teams. *IEEE Software.* 2010. Vol. 27. P. 20–29. URL: https://www.researchgate.net/publication/220092013_A_Process_for_Managing_Risks_in_Distributed_Teams

4. Vaskiv R., Veretennikova N. Features of the use of information and communication technologies to support project processes in distributed teams. *Computer Systems and Information Technologies*. 2023. № 4. P. 36–43.

5. Ільчук П., Горейко Д. Моделі управління віддаленими ІТ-командами: систематичний огляд та концептуальна модель. *Економіка та суспільство*. 2025. Вип. 74. URL: https://economyandsociety.in.ua/index.php/journal/article/view/6076/6015

6. Voloboiev V. Management of War-Influenced Dispersed Teams. *Journal of Vasyl Stefanyk Precarpathian National University.* 2025. Vol. 12, No. 2. P. 43–54.

7. Склярук Т., Турко В. Трансформація стратегій управління людським капіталом ІТ-компаній України під впливом війни, міграції та дистанційної роботи. *Економічний простір.* 2025. № 207. С. 64–71.

8. Антонюк Д.А., Кулик Д.М. Трансформація парадигми ризик-менеджменту підприємств в Україні в умовах воєнного стану. *Менеджмент та підприємництво: тренди розвитку.* 2026. Вип. 1 (35). С. 43–56.

9. Buriak M., Makovoz O. Agile Change Management of Ukraine's IT Sector's and Value Creation Amidst Conflict. *Proceedings 10th London International Conference.* November 15–17, 2023. P. 20–33.

10. Васьків Р., Веретеннікова Н. Інтегрована модель управління ризиками у розподілених ІТ-командах. *Інформаційні системи та мережі.* 2025. Вип. 17. С. 214–225.

References:

1. Sirkka L. Jarvenpaa, Dorothy E. Leidner. (1998) Communication and Trust in Global Virtual Teams. *Journal of Computer-Mediated Communication*, vol. 3, is. 4. DOI: https://doi.org/10.1111/j.1083-6101.1998.tb00080.x

2. Hertel G., Geister S., Konradt U. (2005) Managing virtual teams: A review of current empirical research. *Human Resource Management Review,* vol. 15, is. 1, pp. 69–95.

3. Persson J., Mathiassen L. (2010) A Process for Managing Risks in Distributed Teams. *IEEE Software*, vol. 27, pp. 20–29. Retrieved from: https://www.researchgate.net/publication/220092013_A_Process_for_Managing_Risks_in_Distributed_Teams

4. Vaskiv R., Veretennikova N. (2023) Features of the use of information and communication technologies to support project processes in distributed teams. *Computer Systems and Information Technologies*, vol. 4, pp. 36–43.

5. Ilchuk P., Horeiko D. (2025) Modeli upravlinnia viddalenymy IT-komandamy: systematychnyi ohliad ta kontseptualna model [Remote IT Team Management Models: A Systematic Review and Conceptual Model]. *Ekonomika ta suspilstvo*, vol. 74. Retrieved from: https://economyandsociety.in.ua/index.php/journal/article/view/6076/6015

6. Voloboiev V. (2025) Management of War-Influenced Dispersed Teams. *Journal of Vasyl Stefanyk Precarpathian National University*, vol. 12, no. 2, pp. 43–54.

7. Skliaruk T., Turko V. (2025) Transformatsiia stratehii upravlinnia liudskym kapitalom IT-kompanii Ukrainy pid vplyvom viiny, mihratsii ta dystantsiinoi roboty [Transformation of human capital management strategies of Ukrainian IT companies under the influence of war, migration and remote work]. *Ekonomichnyi prostir*, no. 207, pp. 64–71. (in Ukrainian)

8. Antoniuk D.A., Kulyk D.M. (2026) Transformatsiia paradyhmy ryzyk-menedzhmentu pidpryiemstv v Ukraini v umovakh voiennoho stanu [Transformation of the enterprise risk management paradigm in Ukraine under martial law]. *Menedzhment ta pidpryiemnytstvo: trendy rozvytku*, vol. 1 (35), pp. 43–56. (in Ukrainian)

9. Buriak M., Makovoz O. (2023) Agile Change Management of Ukraine's IT Sector's and Value Creation Amidst Conflict. *Proceedings 10th London International Conference* (November 15–17, 2023), pp. 20–33.

10. Vaskiv R., Veretennikova N. (2025) Intehrovana model upravlinnia ryzykamy u rozpodilenykh IT-komandakh [An integrated risk management model for distributed IT teams]. *Informatsiini systemy ta merezhi*, vol. 17, pp. 214–225. (in Ukrainian)

Стаття отримана: 10.04.2026
Стаття прийнята: 21.05.2026
Стаття опублікована: 26.06.2026