Менеджмент

УДК 658.56:621.39

DOI https://doi.org/10.5281/zenodo.14260381

Розробка стратегій антикризового управління для підвищення стійкості телекомунікаційних підприємств

Кузьменко Віталій Володимирович,
аспірант, НБУ «Дніпровська політехніка», м. Дніпро, Україна,
https://orcid.org/0009-0007-6948-7194

Прийнято: 18.11.2024 | Опубліковано: 02.12.2024

Анотація: Актуальність дослідження зумовлена необхідністю ефективних стратегій, які дозволять телекомунікаційним підприємствам успішно протистояти викликам, що виникають зі зростанням масштабів кризових ситуацій, зокрема військових конфліктів, економічної нестабільності та кіберзагроз. Телекомунікаційна галузь є критично важливою для забезпечення стабільного функціонування суспільства, тому розробка дієвих підходів щодо антикризового управління визначається як необхідна умова для підвищення їхньої стійкості та конкурентоспроможності. Метою статті є визначення ключових факторів, що впливають на формування стійкості телекомунікаційних підприємств, і розроблення практичних рекомендацій щодо впровадження ефективних стратегій антикризового управління. У дослідженні використано аналітичний підхід, за допомогою якого виявлено основні загрози та виклики, перед якими постають телекомунікаційні підприємства в умовах кризи. Методи дослідження ґрунтуються на аналізі сучасної літератури та практичного досвіду компаній, які функціонують у надзвичайних ситуаціях. У роботі змодельовано

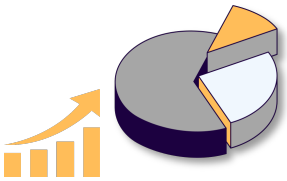
сценарії антикризового управління, адаптовані до реальних умов функціонування телекомунікаційної інфраструктури. У результаті дослідження виявлено, що основними загрозами для телекомунікаційних підприємств є кібератаки, пошкодження інфраструктури, економічні труднощі, регуляторні зміни та соціальні кризи. Доведено, що подолання цих викликів потребує розробки багаторівневих стратегій управління, орієнтованих на довгострокову стійкість. Для цього запропоновано чотири ключові стратегії: інфраструктурна резильєнтність, що забезпечує фізичну стійкість мережі; цифрова адаптивність, що передбачає впровадження технологій для моніторингу та управління кризами; соціальна взаємодія, спрямована на зміцнення зв'язків із громадами та державними структурами; багатовекторна диверсифікація, що дозволяє розширювати спектр послуг і джерела доходів. У висновках доведено, що успішне антикризове управління потребує інтеграції адаптивних технологічних рішень, фінансової підготовки, створення програм підтримки персоналу та активної співпраці з партнерами. У статті надано практичні рекомендації, які дозволяють мінімізувати вплив кризових ситуацій та забезпечити довгостроковий розвиток галузі. Перспективи подальших досліджень полягають у створенні інструментів оцінювання ефективності впроваджених стратегій, аналізі використання штучного інтелекту для прогнозування ризиків та розвитку міжгалузевих моделей партнерства, які сприятимуть підвищенню стійкості телекомунікаційних підприємств.

Ключові слова: операційна гнучкість, ризик-менеджмент, корпоративна стійкість, адаптивні рішення, кризове планування.

Development of Crisis Management Strategies to Enhance the Resilience of Telecommunication Enterprises

Vitalii Kuzmenko,
Postgraduate, Dnipro University of Technology, Dnipro, Ukraine,
https://orcid.org/0009-0007-6948-7194

Abstract: The relevance of the study is driven by the increasing scale of crises affecting the operations of telecommunication enterprises, including military conflicts, economic instability, and cyber threats. The telecommunications sector is critically important for maintaining the stable functioning of society, making the development of effective crisis management strategies a necessary condition for enhancing its resilience and competitiveness. The purpose of the article is to identify the key factors influencing the resilience of telecommunication enterprises and to develop practical recommendations for implementing effective crisis management strategies. The research applies an analytical approach to identify the main threats and challenges faced by telecommunication enterprises during crises. The methods of the study are based on analyzing contemporary literature and practical experiences of companies operating in emergency situations. The study includes modeling crisis management scenarios adapted to real-world conditions of telecommunications infrastructure operations. The study reveals that the primary threats to telecommunication enterprises are cyber threats, infrastructure damage, economic difficulties, regulatory changes, and social crises. It is demonstrated that addressing these challenges requires the development of multi-level management strategies aimed at long-term resilience. Four key strategies are proposed: “infrastructural resilience”, which ensures the physical stability of infrastructure; “digital adaptability”, which incorporates technologies for crisis monitoring and management; “social engagement”, aimed at strengthening ties with communities and governmental bodies; “multi-vector diversification”, which



allows for the expansion of services and revenue streams. The conclusions highlight that successful crisis management necessitates the integration of adaptive technological solutions, financial preparedness, personnel support programs, and active collaboration with partners. The article provides practical recommendations that enable minimizing the impact of crises and ensuring the long-term development of the sector. Future research prospects include developing tools to evaluate the effectiveness of implemented strategies, analyzing the use of artificial intelligence for risk prediction, and exploring cross-sectoral partnership models that contribute to enhancing the resilience of telecommunication enterprises.

Keywords: operational flexibility, risk management, corporate resilience, adaptive solutions, crisis planning

Постановка проблеми в загальному вигляді та її зв'язок із важливими науковими чи практичними завданнями. В умовах нестабільного економічного середовища та глобальних викликів сьогодення телекомунікаційні підприємства потребують створення ефективних стратегій антикризового управління для забезпечення їхньої стійкості та конкурентоспроможності. Постійне зростання ризиків, таких як кібератаки, порушення ланцюгів постачання, регуляторні зміни та вплив непередбачуваних кризових ситуацій, висувають нові вимоги до адаптивності підприємств. Телекомунікаційна галузь, яка є критично важливою для функціонування сучасного суспільства, повинна знаходити шляхи швидкого реагування на загрози, мінімізуючи негативний вплив криз на операційну діяльність.

У цьому контексті постає необхідність формування комплексних підходів до управління ризиками, які враховували б специфіку телекомунікаційних підприємств, забезпечували їхню здатність до швидкого відновлення після безпрецедентних подій і сприяли підвищенню їхньої корпоративної стійкості. Ефективні антикризові стратегії повинні інтегрувати адаптивні рішення, спрямовані на розробку інноваційних механізмів реагування на ризики,

оптимізацію операційних процесів та формування стійкої корпоративної культури.

Наукове значення дослідження полягає в необхідності розробки моделей управління, які поєднували б теоретичні підходи до кризового планування з практичними інструментами їхньої реалізації. Практична важливість зумовлена потребою у створенні дієвих методів ризик-менеджменту, що забезпечували б не лише збереження життєздатності підприємств під час криз, але і їхній подальший розвиток у післякризовий період.

Аналіз останніх досліджень і публікацій. Розробка стратегій антикризового управління для підвищення стійкості телекомунікаційних підприємств є складною та багатогранною проблемою, яка досліджується в різних аспектах сучасної наукової літератури. У цьому контексті значна увага приділяється питанням управління ризиками, інноваційного розвитку, адаптації до кризових умов та розробки практичних стратегій для забезпечення стійкості галузі.

Управління ризиками, яке є центральною темою багатьох досліджень, висвітлюється в працях О. Гусєвої й А. Захаржевської, які аналізують діагностичні підходи до управління ризиками телекомунікаційних підприємств та пропонують рекомендації щодо їхнього вдосконалення [1; 2]. Науковиці наголошують, що традиційні підходи до управління ризиками є недостатніми для ефективного реагування на сучасні виклики, зокрема у сфері цифрових трансформацій. С. Бірбіренко, В. Орлова та Н. Лунгул підкреслюють важливість стратегічного підходу до управління економічною стійкістю, акцентуючи на необхідності інтеграції гнучких управлінських рішень [3].

Дослідження інноваційного розвитку підприємств та його ролі в підвищенні стійкості телекомунікаційних компаній представлено в працях М. Житаря, І. Зеліско та Д. Шагірманова, які аналізують глобальні тренди інноваційного розвитку, акцентуючи на необхідності адаптації підприємств до швидкозмінних умов ринку [4; 5]. У цьому контексті особливо важливими є

роботи В. Рудевської, Н. Швець і В. Танасе, які підкреслюють, що цивілізаційний розвиток, зокрема, сприяє сталому розвитку телекомунікаційної галузі та дозволяє підвищити її конкурентоспроможність і зменшити вплив кризових явищ [6].

Організаційна стійкість підприємств та їхня здатність адаптуватися до кризових умов є ще одним важливим напрямом досліджень. У працях І. Крейдич і М. Ноняк висвітлюється сучасний стан та тенденції організаційного розвитку телекомунікаційних підприємств в умовах постійної нестабільності [7]. Дослідники підкреслюють, що організаційна гнучкість є ключовим фактором для забезпечення стійкості підприємств, оскільки дозволяє швидко реагувати на зміни в зовнішньому середовищі. У дослідженнях В. Гарькавої, О. Славкової та Т. Волотовської проаналізовано специфічні виклики, перед якими постають телекомунікаційні підприємства, а також запропоновано адаптивні рішення для підвищення їхньої стійкості [8].

Умови воєнного стану в Україні ставлять перед телекомунікаційною галуззю нові виклики, які проаналізовано в роботах таких учених, як O. Vynogradova, N. Drokina, A. Zakharzhevska. Авторки наголошують на необхідності адаптації наявних управлінських стратегій до нових реалій, а також розглядають інструменти для забезпечення стійкості підприємств у післявоєнний період [9]. У цьому контексті важливим є дослідження О. Гудзь та А. Захаржевської, які розробляють комплексні підходи до управління ризиками в реаліях цифрової трансформації, наголошуючи на ролі новітніх технологій [10].

Формування антикризових стратегій для забезпечення економічної стійкості є ще одним ключовим аспектом досліджень. С. Бібіренко та Ю. Жданова запропонували теоретико-методологічні засади для впровадження антикризових рішень, що базуються на системному аналізі внутрішніх та зовнішніх факторів впливу [11]. J. Ruiz-Canela López, S. Birbirenko, S. Yevtukhova, M. Chepeliuk, T. Kravchenko, L. Melnyk акцентують на

організаційно-економічних механізмах формування стійкості, які забезпечують довгострокову ефективність підприємств [12; 13].

Таким чином, наукові дослідження у сфері антикризового управління телекомунікаційними підприємствами охоплюють широкий спектр питань, починаючи від управління ризиками й завершуючи впровадженням інноваційних стратегій.

Виділення невирішених раніше частин загальної проблеми. Попри досягнення у вивченні стійкості телекомунікаційних підприємств, залишаються нерозв'язаними питання щодо аналізу специфічних викликів, таких як кіберзагрози та геополітична нестабільність, що обмежує розуміння кризового впливу. Недостатня емпірична база в дослідженнях ефективності інструментів управління ризиками не дозволяє адаптувати їх до сучасних умов галузі. Відсутність системних адаптивних стратегій та обґрунтованих підходів до формування корпоративної стійкості ускладнює забезпечення гнучкості підприємств у кризових ситуаціях.

Пропоноване дослідження зосереджене на заповненні цих прогалин шляхом розробки інноваційних підходів до управління ризиками, адаптації стратегій до специфіки галузі та формування практичних рекомендацій для підвищення стійкості телекомунікаційних підприємств. Це сприятиме поглибленню наукових знань і підвищенню конкурентоспроможності галузі в умовах сучасних викликів.

Формулювання цілей статті (визначення завдань). Мета статті – дослідити основні підходи до впровадження ефективних стратегій антикризового управління та запропонувати науково обґрунтовані рекомендації, спрямовані на підвищення стійкості телекомунікаційних підприємств у сучасних умовах нестабільності.

Відповідно до мети сформульовано такі завдання:

1. Проаналізувати основні виклики та загрози, що впливають на стійкість телекомунікаційних підприємств, та оцінити ефективність сучасних інструментів управління ризиками в кризових умовах.

2. Розробити адаптивні рішення для забезпечення операційної гнучкості та формування корпоративної стійкості телекомунікаційних підприємств в умовах кризи.

3. Надати практичні рекомендації щодо впровадження стратегій антикризового управління, враховуючи специфіку телекомунікаційної галузі та сучасні виклики.

Виклад основного матеріалу дослідження. У кризових умовах телекомунікаційні підприємства постають перед численними викликами та загрозами, які впливають на їхню операційну стійкість та здатність до адаптації. Основними чинниками ризику є зростання кіберзагроз, порушення у функціонуванні інфраструктури, економічна нестабільність, зміни в регуляторному середовищі, а також соціально-політичні кризи. Ці ризики посилюються в періоди глобальних катаклізмів, таких як пандемії чи збройні конфлікти, що вимагає від підприємств високого рівня гнучкості та оперативності в реагуванні (табл. 1).

Таблиця 1

Основні виклики та загрози стійкості телекомунікаційних підприємств у кризових умовах

Категорія загроз	Характеристика	Приклади впливу
Кіберзагрози	Атаки на мережі та системи, що призводять до витоку даних або порушення роботи сервісів	Кібернапади на українські телекомунікаційні компанії під час війни, що в критичні моменти ускладнюють доступ до комунікацій

Інфраструктурні ризики	Фізичне пошкодження мережевих об’єктів через воєнні дії чи стихійні лиха	Руйнування оптоволоконних мереж через воєнні дії в Україні, що призводить до нестабільного зв’язку
Економічна нестабільність	Зниження платоспроможності споживачів та зростання витрат на підтримку операційної діяльності	Зменшення прибутків компаній через втрату клієнтів під час економічного спаду
Регуляторні зміни	Запровадження нових вимог, які потребують значних інвестицій для відповідності стандартам	Адаптація до європейських регуляторних норм, що вимагає модернізації мережевої інфраструктури
Соціально-політичні ризики	Масова міграція та зменшення споживчого попиту внаслідок кризових подій	Зменшення кількості абонентів у регіонах через евакуацію населення під час війни

Джерело: розробка автора на основі джерел [2; 11]

Під час війни в Україні телекомунікаційні підприємства зазнали інтенсивних кібератак, які зумовили нестабільне функціонування державних онлайн-платформ і навіть деяких мобільних операторів. Наприклад, у 2022 році серії атак типу DDoS були спрямовані на провайдерів, які забезпечують доступ до інтернету, через що користувачі втратили можливість здійснювати комунікацію впродовж певного часу, зокрема в критичних регіонах.

Інфраструктурні ризики проявилися під час масованих ракетних обстрілів, коли пошкодження мереж оптоволоконного зв’язку в Київській, Харківській та інших областях призводило до часткового або повного відключення абонентів. Компанії змушені були впроваджувати резервні рішення, такі як мобільні базові станції та аварійне відновлення ліній у рекордно короткі терміни [7].

Економічна нестабільність проявилася в зменшенні доходів абонентів у період пандемії COVID-19 [13]. Наприклад, в Італії та Іспанії оператори змушені були запровадити програми лояльності, надаючи додатковий безоплатний трафік

для підтримки клієнтів, які тимчасово втратили роботу. Аналогічні заходи запроваджувалися і в Україні, зокрема програми «Плати, коли зможеш» від декількох мобільних операторів.

Регуляторні зміни чинять значний тиск на телекомунікаційний сектор. Наприклад, упровадження регламенту GDPR в ЄС змусило багатьох операторів, включно з «Водафон» та «Оранж», інвестувати значні кошти в модернізацію систем захисту даних і навчання персоналу. В Україні під час євроінтеграційних реформ компанії також постають перед викликами відповідності європейським стандартам.

Соціально-політичні ризики, викликані війною в Україні, спричинили не тільки міграцію населення, але й потребу швидкого забезпечення зв'язком тимчасово переміщених осіб у нових регіонах. Наприклад, мобільні оператори створювали спеціальні тарифні плани для українців за кордоном, а також розширювали покриття в регіонах зі значною кількістю переселенців, таких як Львівщина та Закарпаття.

Сучасні інструменти управління ризиками охоплюють як технологічні рішення, такі як системи моніторингу та аналізу даних у реальному часі, так і організаційні підходи, зокрема ризик-менеджмент на основі сценарного планування. Завдяки таким інструментам компанії можуть не лише знижувати вплив кризових подій, але й підвищувати свою операційну гнучкість. В умовах сучасних викликів, таких як кібератаки, регуляторні зміни та збройні конфлікти, ці інструменти мають вирішальне значення для забезпечення безперервності діяльності (табл. 2).

Таблиця 2

Ефективність сучасних інструментів управління ризиками в телекомунікаційній галузі

Інструмент управління ризиками	Характеристика	Приклад

Системи моніторингу ризиків	Автоматизовані платформи для ідентифікації та аналізу ризиків у реальному часі	Використання SIEM-систем для моніторингу кіберзагроз в українських телекомунікаційних компаніях
Сценарне планування	Розробка альтернативних сценаріїв реагування на потенційні кризи	Застосування сценаріїв евакуації та резервування ресурсів у періоди бойових дій
Страхування ризиків	Фінансовий захист від можливих збитків через укладення страхових контрактів	Страхування інфраструктури телекомунікаційних мереж від пошкоджень під час воєнних дій
Аудит та оцінка ризиків	Регулярний аналіз та оцінка ризиків для коригування управлінських стратегій	Проведення аудиту кібербезпеки в провайдерів інтернету в умовах зростання атак типу ransomware
Резервні системи та дублювання	Створення резервних каналів зв'язку та центрів обробки даних для забезпечення безперервності бізнесу	Використання резервних серверів та автономних базових станцій для підтримання зв'язку в регіонах із пошкодженою інфраструктурою.

Джерело: розробка автора на основі джерел [4; 9; 10]

Сучасні інструменти управління ризиками в телекомунікаційній галузі демонструють свою ефективність завдяки здатності адаптуватися до нових викликів і забезпечувати стійкість бізнесу навіть у складних умовах. Наприклад, системи моніторингу ризиків, такі як SIEM, стали критично важливими для українських компаній під час активізації кібератак у період війни. Ці платформи аналізують величезні масиви даних у режимі реального часу, дозволяючи виявляти атаки на початкових етапах.

Сценарне планування проявляє себе як надзвичайно ефективний стратегічний інструмент у кризових ситуаціях [14]. Наприклад, під час масованих обстрілів інфраструктури в Харківській та Донецькій областях компанії завчасно розробили альтернативні сценарії для резервування мережевих ресурсів, що дозволило уникнути повної втрати зв'язку. Цей підхід також активно використовується європейськими операторами, які розробляють

сценарії реагування на природні катастрофи, наприклад, у разі повеней чи землетрусів.

Страхування ризиків надає можливість телекомунікаційним підприємствам швидше відновлювати пошкоджену інфраструктуру. У випадку руйнування магістральних ліній зв'язку в Україні внаслідок бойових дій у 2022 році страхові компанії компенсували операторам значну частину витрат на відновлення. Такі фінансові інструменти також активно використовуються міжнародними телекомунікаційними корпораціями, що дозволяє зменшити фінансове навантаження під час криз.

Аудит ризиків дозволяє не лише ідентифікувати слабкі місця, але й упроваджувати проактивні заходи для їхнього усунення. Наприклад, аудит кібербезпеки, проведений у 2023 році однією з провідних українських компаній, виявив критичні вразливості в системах віддаленого доступу. Після внесення змін кількість успішних атак скоротилася на 40% [10].

Резервні системи та дублювання, зокрема створення автономних базових станцій, забезпечують безперебійний зв'язок навіть у разі пошкодження основної інфраструктури [14].

В умовах кризи телекомунікаційні підприємства мають потребу швидко адаптуватися до нових викликів, щоб забезпечити стабільність операційної діяльності та задовольнити потреби клієнтів. Адаптивні рішення, спрямовані на підвищення операційної гнучкості, базуються на впровадженні інноваційних технологій, гнучких організаційних підходів та механізмів реагування, що дозволяють мінімізувати вплив кризових ситуацій на діяльність підприємства. Це включає оперативну реструктуризацію процесів, запровадження резервних ресурсів, використання хмарних технологій і забезпечення багаторівневого резервування систем. Такі рішення дозволяють не лише реагувати на кризи, але й закладати основу для довгострокової стабільності (рис. 1).

Рис. 1. Адаптивні рішення для забезпечення операційної гнучкості телекомунікаційних підприємств в умовах кризи

Джерело: власна розробка автора

Застосування адаптивних рішень для забезпечення операційної гнучкості телекомунікаційних підприємств довело свою ефективність у кризових умовах [12], таких як війна в Україні та пандемія COVID-19. Використання хмарних технологій стало ключовим фактором для збереження стабільності операцій. Наприклад, перехід на хмарні сервіси AWS дозволив українським операторам забезпечити безперервність послуг навіть у зоні активних бойових дій, коли фізичну інфраструктуру було частково зруйновано. Таке рішення не лише мінімізувало ризики втрати даних, але й забезпечило швидкий доступ до ресурсів із будь-якої точки світу.

Резервування мережевих потужностей стало незамінним інструментом у регіонах із пошкодженою інфраструктурою. У Харківській області, де війна спричинила масштабні руйнування, мобільні базові станції стали критично важливими для забезпечення зв'язку в ізольованих громадах, завдяки чому

тисячі користувачів залишилися на зв’язку, що мало вирішальне значення для координації гуманітарної допомоги та реагування на надзвичайні ситуації.

Автоматизація операцій значно скоротила час реагування на кризові події [15]. У 2023 році, під час масованих ракетних атак, автоматизовані системи переналаштування трафіку забезпечили стабільну роботу мережі, навіть коли основні магістральні лінії були перевантажені або пошкоджені. Такі рішення стали важливими не лише для України, а й для міжнародних операторів, які використовують подібні системи для підтримання безперебійної роботи в періоди природних катастроф.

Гібридні моделі роботи стали стандартом для підприємств, які прагнуть поєднати безпеку співробітників зі збереженням продуктивності. Наприклад, компанія «Київстар» успішно впровадила політику віддаленої роботи для працівників у небезпечних регіонах, що дозволило зменшити витрати на фізичні офіси та водночас забезпечити високу продуктивність [1].

Навчання та перепідготовка персоналу відіграють важливу роль у підвищенні адаптивності підприємств [11]. Наприклад, проведення тренінгів із кібербезпеки допомогло значно зменшити кількість інцидентів, пов’язаних із фішинговими атаками. Такий підхід також застосовують міжнародні компанії, які використовують кризові ситуації для підвищення кваліфікації своїх працівників.

Для забезпечення корпоративної стійкості телекомунікаційних підприємств в умовах кризи доцільно розробити комплексні стратегії антикризового управління, які об’єднують різні адаптивні заходи в цілісні підходи. Такі стратегії мають враховувати специфіку галузі, а також особливості кризових ситуацій, що можуть виникнути. Вони дозволяють не лише зменшити вплив загроз, але й створюють умови для ефективного відновлення та подальшого розвитку підприємств.

Першою можна виокремити стратегію інфраструктурної резильєнтності, що спрямована на забезпечення фізичної та технологічної стійкості мереж і

систем підприємства. Вона базується на інтеграції резервних потужностей, хмарних рішень і автономних енергетичних систем, які дозволяють підтримувати зв'язок навіть у разі значних фізичних руйнувань інфраструктури. Використання мобільних базових станцій, а також резервного маршрутизаційного обладнання є ключовим елементом цієї стратегії. Її доцільно застосовувати в регіонах із високим ризиком фізичних пошкоджень, зокрема в зонах воєнних дій або стихійних лих. У таких умовах ця стратегія забезпечує не лише мінімізацію простоїв, але й швидке відновлення послуг для споживачів.

Другою є стратегія цифрової адаптивності, яка акцентує на швидкій інтеграції нових технологій для моніторингу, прогнозування та управління кризами. Використання інструментів штучного інтелекту для аналізу кіберзагроз, розробка моделей прогнозування навантаження на мережі та автоматизація реагування на інциденти є її основними компонентами. Цю стратегію варто впроваджувати в компаніях, які працюють в умовах із високим рівнем технологічних викликів, наприклад, постійними кібератаками або необхідністю обслуговування критично важливих споживачів. Завдяки цифровій адаптивності підприємства можуть не лише ефективніше реагувати на ризики, але й знижувати витрати, пов'язані з ручним управлінням кризовими ситуаціями.

Стратегія соціальної взаємодії спрямована на побудову партнерських відносин із локальними громадами, урядовими структурами та міжнародними організаціями для координації зусиль у періоди кризи. Її ключовими аспектами є спільне планування заходів із відновлення інфраструктури, забезпечення пріоритетного доступу до ресурсів і розробка соціальних програм підтримки для населення. Застосування цієї стратегії є доцільним у регіонах із високою соціальною напругою, наприклад, у місцях із великою кількістю переміщених осіб або під час значних економічних спадів. Такі дії допомагають зберігати лояльність клієнтів, зміцнювати репутацію компанії та забезпечувати стабільний рівень послуг навіть у кризових умовах.

Стратегія багатовекторної диверсифікації передбачає розширення спектра бізнес-моделей, інтеграцію нових послуг і вихід на суміжні ринки. Упровадження IoT-рішень, послуг зберігання даних у хмарі, а також платформ для віддаленої роботи дозволяє компаніям компенсувати втрати в одному сегменті ринку шляхом збільшення доходів в іншому. Ця стратегія найефективніша у великих операторів, які мають доступ до значних фінансових ресурсів для інвестування в розвиток. Вона дозволяє створити стійку бізнес-екосистему, яка менше залежить від короткострокових коливань попиту в окремих сегментах.

Запропоновані стратегії взаємодоповнюють одна одну, а їхня реалізація створює комплексний підхід до забезпечення стійкості телекомунікаційних підприємств у кризових умовах. Це дозволяє не лише зменшувати ризики, але й створювати нові можливості для зростання навіть у найбільш нестабільних ситуаціях.

Висновки. У результаті проведеного дослідження встановлено, що стійкість телекомунікаційних підприємств у кризових умовах значною мірою залежить від здатності інтегрувати сучасні технології управління ризиками, розробляти адаптивні рішення та впроваджувати комплексні антикризові стратегії. Ідентифіковано основні загрози для телекомунікаційної галузі, серед яких – кібератаки, інфраструктурні пошкодження, економічна нестабільність, регуляторні зміни та соціально-політичні кризи.

Основними проблемами є недостатній рівень цифрової готовності підприємств до кризових ситуацій, обмежена здатність оперативно адаптувати операційні процеси до нових умов, а також недостатня інтеграція інноваційних інструментів моніторингу та управління. Відсутність координації між підприємствами й державними органами, а також низький рівень фінансової підготовленості додатково ускладнюють подолання кризових ситуацій.

Для підвищення корпоративної стійкості телекомунікаційних підприємств рекомендовано впроваджувати багаторівневі стратегії, такі як інфраструктурна

резильєнтність, цифрова адаптивність, соціальна взаємодія та багатовекторна диверсифікація. Кожна з цих стратегій об'єднує адаптивні підходи, орієнтовані на оперативність реагування, довгострокову стабільність і підвищення конкурентоспроможності.

Перспективи подальших досліджень пов'язані з розробкою емпіричних моделей оцінки ефективності впроваджених стратегій у різних регіональних та економічних умовах. Необхідно приділити увагу дослідженню впливу штучного інтелекту на оптимізацію кризового управління, а також аналізу міжгалузевої співпраці для зменшення впливу криз на телекомунікаційні системи. Особливо важливо розробити інтегровані інструменти прогнозування ризиків, які б враховували специфіку локальних і глобальних викликів.

Список використаних джерел:

1. Гусєва О. Ю., Захаржевська А. А. Діагностика розвитку управління ризиками телекомунікаційних підприємств. *Бізнес Інформ.* 2023. № 1. С. 196–202. DOI: https://doi.org/10.32983/2222-4459-2023-1-196-202

2. Захаржевська А. А. Управління ризиками телекомунікаційних підприємств: сутнісні аспекти. *Економіка. Менеджмент. Бізнес*. 2022. № 1–2. С. 39–74. DOI: https://doi.org/10.31673/2415-8089.2022.016974

3. Бірбіренко С. С., Орлов В. М., Лунгул Н. С. Концептуальні засади формування стратегічного управління економічною стійкістю телекомунікаційного підприємства. *Науковий вісник Полтавського університету економіки і торгівлі. Серія «Економічні науки».* 2021. № 2–2 (104). С. 12–18. DOI: https://doi.org/10.37734/2409-6873-2021-2-2-2

4. Житар М. О. Концептуальні засади управління інноваційним розвитком телекомунікаційних підприємств. *European scientific journal of Economic and Financial innovation.* 2024. № 1 (13). С. 157–165. URL: https://elibrary.kubg.edu.ua/id/eprint/49088/ (дата звернення: 24.09.2024).

5. Зеліско І. М., Шагірманов Д. О. Глобальні тренди інноваційного розвитку телекомунікаційних підприємств. *Економічний простір.* 2023. № 184. С. 79–83. DOI: https://doi.org/10.32782/2224-6282/184-13

6. Рудевська В., Швець Н., Танасе В. Цивілізаційний розвиток як передумова прогресу в досягненні цілей сталого розвитку. *Socio-Economic Relations in the Digital Society.* 2024. № 1(51). С. 86–96. DOI: https://doi.org/10.55643/ser.1.51.2024.550

7. Крейдич І. М., Ноняк М. В. Сучасний стан та тенденції організаційного розвитку телекомунікаційних підприємств. *Економіка. Менеджмент. Бізнес.* 2020. № 1. С. 21–28. DOI: https://doi.org/10.31673/2415-8089.2020.012128

8. Гарькава В. Ф., Славкова О. П., Волотовська Т. П. Управління ризиками в умовах нестабільності: виклики для менеджменту в Україні. *Актуальні питання економічних наук.* 2024. № 1. DOI: https://doi.org/10.5281/zenodo.13347958

9. Vynogradova O., Drokina N., Zakharzhevska A. Directions of activation of risk management of telecommunications enterprises in Ukraine in martial law and post-war conditions. *Acta Scientiarum Polonorum. Oeconomia.* 2022. Vol. 21. № 3. URL: https://www.ceeol.com/search/article-detail?id=1117243 (date of access: 24.09.2024).

10. Гудзь О. Є., Захаржевська А. А. Розвиток управління ризиками телекомунікаційних підприємств в реаліях цифрової трансформації: монографія. Кропивницький: Видавець Лисенко В. Ф., 2023. 200 с.

11. Бібіренко С., Жданова Ю. Теоретико-методологічні засади управління економічною стійкістю сучасного телекомунікаційного підприємства. *Economic Development: Global Trends and National Peculiarities: Collective monograph.* Poland: “Publishing House “Baltija Publishing”, 2020. С. 442–456. URL: http://baltijapublishing.lv/omp/index.php/bp/catalog/book/59 (дата звернення: 24.09.2024).

12. Ruiz-Canela López J. How can enterprise risk management help in evaluating the operational risks for a telecommunications company? *Journal of Risk*

and Financial Management. 2021. Vol. 14. № 3. DOI: https://doi.org/10.3390/jrfm14030139

13. Birbirenko S., Yevtukhova S., Chepeliuk M., Kravchenko T., Melnyk L. Conceptual fundamentals of organizational and economic mechanism formation of economic sustainability management of a telecommunication enterprise. *Journal on Innovation and Sustainability RISUS.* 2021. Vol. 12. № 3. P. 74–86. DOI: https://doi.org/10.23925/2179-3565.2021v12i3p74-86

14. Beretas C. Information Systems Security, Detection and Recovery from Cyber Attacks. *Universal Library of Engineering Technology*. 2024. Vol. 1. № 1. URL: https://ulopenaccess.com/ulpages/fulltextUlete?PublishID=ULETE20240101_005 (date of access: 24.09.2024).

15. Ouyang Y., Wang L., Yang A., Shah M., Belanger D., Gao T., Wei L., Zhang Y. (2021). The next decade of telecommunications artificial intelligence. *arXiv preprint.* arXiv:2101.09163. URL: https://arxiv.org/abs/2101.09163 (date of access: 24.09.2024).