УДК 658:338.246
DOI: https://doi.org/10.32782/business-navigator.82-44

Токмакова І.В.
доктор економічних наук, професор,
професор кафедри економіки та управління
виробничим і комерційним бізнесом
Український державний університет залізничного транспорту
ORCID: https://orcid.org/0000-0001-6465-1580
Базилєва М.А.
здобувач вищої освіти другого рівня
Український державний університет залізничного транспорту
Тиницький О.В.
здобувач вищої освіти другого рівня
Український державний університет залізничного транспорту

Tokmakova Iryna
Doctor of Economic Sciences, Professor,
Professor of the Department of Economics and Management
Production and Commercial Business
Ukrainian State University of Railway Transport
Bazylieva Mariia
Second-Level Higher Education Applicant (Master's Degree Applicant)
Ukrainian State University of Railway Transport
Tynytskyi Oleksii
Second-Level Higher Education Applicant (Master's Degree Applicant)
Ukrainian State University of Railway Transport

ЕКОНОМІЧНА БЕЗПЕКА ПІДПРИЄМСТВ В УМОВАХ РИЗИКОГЕННОГО СЕРЕДОВИЩА

ECONOMIC SECURITY OF ENTERPRISES IN A RISK-HIGH ENVIRONMENT

У статті проаналізовано актуальні загрози, які впливають на функціонування підприємств, що дозволило обґрунтувати ризикогенний характер сучасного українського бізнес-середовища. Розкрито підходи до побудови системи економічної безпеки, здатної ефективно функціонувати в умовах посилення тиску ризиків. Підкреслено необхідність трансформації традиційних статичних моделей управління на динамічні, технологічно інтегровані механізми, які передбачають безперервний моніторинг, прогнозування загроз, сценарне планування та формування культури безпеки в організаціях. Акцентовано увагу на комплексному підході до забезпечення економічної безпеки підприємств, що реалізується через поетапну модель впровадження, яка охоплює аудит ризиків, інтеграцію ризик-менеджменту, цифрову трансформацію бізнес-процесів та розвиток людського капіталу як стратегічного ресурсу стійкості.

Ключові слова: економічна безпека, ризикогенне середовище, управління ризиками, адаптивні системи, цифрова трансформація, моніторинг загроз, проактивний підхід, культура безпеки.

The article analyzes current threats affecting the functioning enterprises in the unstable economic environment Ukraine. It is revealed that the combination external and internal risks – in particular geopolitical, financial, information and personnel – forms the risk-generating nature of the modern Ukrainian business environment, which requires new approaches to security management. The conceptual principles of building an adaptive economic security system capable functioning effectively in conditions of increasing risk pressure, uncertainty and turbulence are revealed. The need to transition from traditional static management models to dynamic, technologically integrated mechanisms based on the principles of flexibility, proactivity and stability is substantiated. Such mechanisms provide for the implementation continuous risk monitoring, systematic threat forecasting, scenario planning and the formation a security culture at all levels the organizational structure. Particular attention is paid to a comprehensive approach to ensuring economic security, covering financial, information, legal, personnel and technological components. A phased model for implementing an economic security system is proposed, which includes risk audit, integration of modern risk management tools, digital transformation of business processes, and

development human capital as a key strategic resource for ensuring long-term sustainability enterprises. It has been established that GRC platforms are becoming increasingly important in the architecture economic security modern organizations, especially in the context increased regulatory requirements, digitalization business processes, and the growth complex risks. From the point view of ensuring economic security, GRC platforms allow centralizing risk management, automating the processes their identification, assessment, and monitoring. The use the GRC platform contributes to the formation a stable and transparent environment in which the processes control, audit, and response to threats become systematic and manageable.

Keywords: economic security, risk environment, risk management, adaptive systems, digital transformation, threat monitoring, proactive approach, security culture.

Постановка проблеми. Сучасне економічне середовище характеризується високим ступенем невизначеності, нестабільності та непередбачуваності, що дозволяє визначити його як ризикогенне. Під впливом глобальних трансформацій – зокрема геополітичних конфліктів, циклічних економічних криз, технологічних проривів та екзогенних шоків – відбувається поступове стирання меж між внутрішніми та зовнішніми загрозами, що ускладнює процес їх ідентифікації та управління. У результаті підприємства змушені функціонувати в умовах багатовимірного ризикового тиску, який одночасно охоплює фінансову стабільність, виробничу діяльність, кадрову політику, інформаційну безпеку та репутаційні фактори.

Особливої гостроти проблема економічної безпеки набуває в контексті українських реалій, де суб'єкти господарювання змушені адаптуватися до наслідків воєнних дій, частих змін у нормативно-правовому полі, макроекономічної волатильності та стрімкої цифрової трансформації. За таких умов забезпечення економічної безпеки підприємства перестає бути лише елементом оперативного управління і трансформується у стратегічний імператив, що визначає здатність підприємств до виживання, збереження конкурентоспроможності та сталого розвитку.

Отже, актуальність дослідження зумовлена необхідністю концептуального переосмислення підходів до побудови систем економічної безпеки, які здатні ефективно функціонувати в умовах постійної ризикогенності, оперативно реагувати на нові виклики та забезпечувати довгострокову стійкість бізнесу.

Аналіз останніх досліджень і публікацій. Вивчення сучасної наукової літератури з проблематики економічної безпеки підприємств засвідчує її багатовимірність, еволюційний характер та зростаючу значущість в умовах ризикогенного середовища. У фундаментальній праці Ареф'євої О.В. та Кузенко Т.Б. [1] закладено концептуальні основи планування економічної безпеки підприємств, де економічна безпека розглядається як стратегічна функція управління, що потребує системного підходу. Дослідження Диканя В.Л. та Воловельської І.В. [2] акцентує увагу на галузевій специфіці, зокрема в контексті залізничного транспорту, і демонструє необхідність адаптації безпекових стратегій до постіндустріальних викликів. Калинюк В.Є. [3] здійснює критичний аналіз наукових підходів до визначення сутності поняття «економічна безпека підприємства», що дозволяє окреслити межі терміна та його ключові характеристики. У роботі Ковальської Л., Голія О. та Голія В. [4] представлено структурно-функціональну модель економічної безпеки, яка охоплює фінансову, інформаційну, кадрову, правову та технологічну складові, що є основою для розробки комплексних механізмів управління ризиками. Крилов Д.В. [5] зосереджується на класифікації загроз економічній безпеці в умовах сучасних викликів, зокрема війни, енергетичної кризи та політичної нестабільності, пропонуючи інструменти аналітичного реагування. Прохорова В.В. та Мушникова С.А. [6] розглядають коеволюційний підхід до управління економічною безпекою, що передбачає взаємну адаптацію підприємства та зовнішнього середовища, з акцентом на проактивність і стратегічну гнучкість.

Незважаючи на позитивну динаміку наукових досліджень в напрямі переосмислення концептуальних засад економічної безпеки, існує низка невизначених і недостатньо опрацьованих аспектів, які потребують подальших теоретичних досліджень та практичної апробації. Їхнє вирішення є критично важливим для побудови ефективних, адаптивних і стійких систем економічної безпеки, здатних функціонувати в умовах складного та мінливого середовища.

Формулювання завдання дослідження. Мета статті полягає у розкритті актуальних ризиків, притаманних сучасному середовищу господарювання українського бізнесу, та розробленні концептуальних засад формування ефективної системи економічної безпеки підприємств в умовах багатовекторного ризикогенного впливу.

Виклад основного матеріалу дослідження. В умовах повномасштабної війни, що триває, українські підприємства зіткнулися не лише з традиційними ризиками, а й з безпрецедентними викликами, які радикально трансформували бізнес-середовище. На відміну від звичайних криз, сучасні загрози мають глибоко взаємопов'язаний та каскадний характер, де одна проблема посилює іншу. Одним із ключових факторів дестабілізації є масштабне руйнування критичної інфраструктури, зокрема енергетичних і транспортних систем, виробничих потужностей та житлового фонду. Це призводить до значного скорочення валового внутрішнього продукту, втрати фізичного капіталу та порушення логістичних ланцюгів, що негативно впливає на економічну активність. Цілеспрямовані атаки на енергетичну інфраструктуру ставлять під загрозу стабільне функціонування промислових підприємств, спричиняючи перебої в енергопостачанні, зниження продуктивності та ускладнення ведення бізнесу. Варто враховувати, що фізичне руйнування інфраструктури (первинна ланка) запускає ланцюгову реакцію і призводить до логістичних та енергетичних збоїв (вторинна ланка). Це, своєю чергою, спричиняє значні фінансові втрати, що обмежує доступ до капіталу, та кризу людського капіталу через масову міграцію та мобілізацію (третинна ланка). Одночасно цифровізація, що є ключовим інструментом для подолання цих викликів, створює нові вектори кіберзагроз (рис. 1).

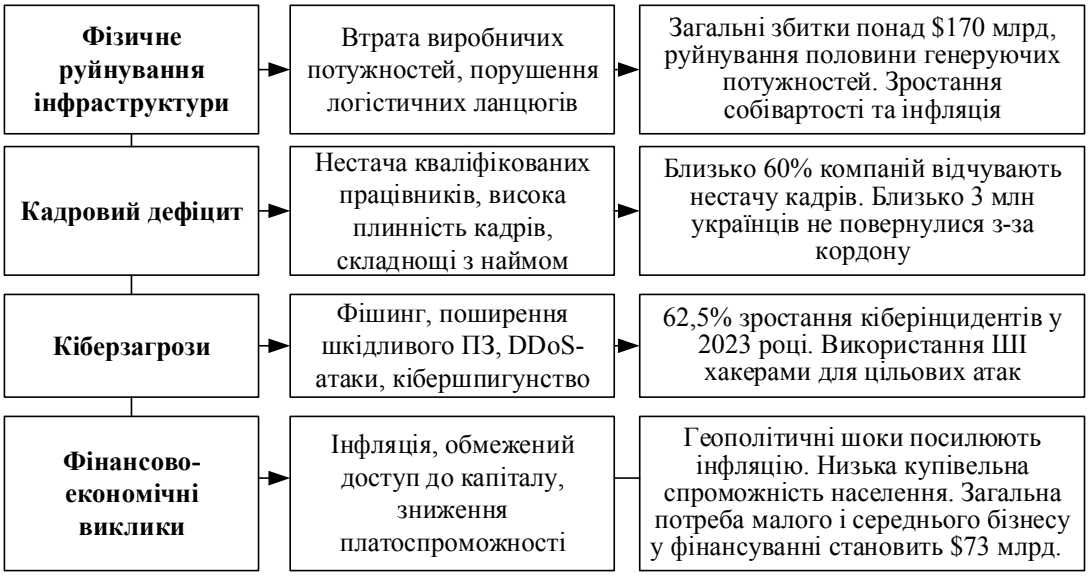

Рис. 1. Актуальні ризики, що впливають на діяльність підприємств України

Джерело: складено авторами на основі [7–10]

Порушення логістичних ланцюгів, дефіцит товарної пропозиції та зростання витрат на виробництво формують стійкий інфляційний тиск, який слід розглядати як одну з ключових загроз економічній безпеці суб'єктів господарювання. Незважаючи на впровадження жорсткої монетарної політики з боку Національного банку України, інфляційні ризики залишаються на високому рівні, що зумовлює нестабільність цінового середовища та ускладнює фінансове планування для підприємств. Додатковим чинником дестабілізації виступає висока волатильність національної валюти, яка обумовлена залежністю економіки від зовнішнього фінансування, стану експортних надходжень та загальної геополітичної ситуації. Девальвація гривні спричиняє подорожчання імпортних товарів, що, у свою чергу, посилює інфляційні процеси та знижує купівельну спроможність населення. Зростання обсягів державного боргу, викликане необхідністю покриття значного бюджетного дефіциту, створює ризики боргової нестійкості в середньостроковій і довгостроковій перспективі, зумовлюючи потребу в системному залученні зовнішніх кредитних ресурсів, що підвищує залежність країни від міжнародних фінансових інституцій і обмежує фіскальну автономію. Ускладнення експортної діяльності, зокрема внаслідок блокування морських портів та запровадження торговельних обмежень з боку суміжних держав, негативно впливає на обсяги валютних надходжень, що послаблює фінансову стійкість експортно-орієнтованих галузей, знижує конкурентоспроможність українських товарів на зовнішніх ринках і поглиблює структурні дисбаланси в економіці.

Високий рівень безпекових ризиків стримує залучення прямих іноземних інвестицій, оскільки інвестори утримуються від активної участі в економіці країни до стабілізації ситуації та отримання гарантій безпеки капіталу. Пріоритетне фінансування оборонного сектору в межах державної бюджетної політики формує значний дефіцит бюджету, який покривається переважно за рахунок міжнародної фінансової допомоги та внутрішніх запозичень, що створює додаткове боргове навантаження.

Поряд з вказаним вище, український бізнес наразі стикається з суттєвими обмеженнями у доступі до фінансових ресурсів. За оцінками, загальна потреба малих і середніх підприємств у додатковому фінансуванні перевищує $73 мільярди [10]. Низький рівень інвестиційної привабливості країни, зумовлений воєнними ризиками та макроекономічною нестабільністю, у поєднанні з обмеженою платоспроможністю підприємств, формує замкнене коло: дефіцит інвестицій стримує економічне відновлення, що, своєю чергою, підвищує ризики для потенційних кредиторів та інвесторів. Такий системний дисбаланс вимагає комплексного підходу, що включає як внутрішні адаптаційні механізми – зокрема реформування фінансово-кредитної політики, покращення інституційного середовища та стимулювання підприємницької активності – так і зовнішню підтримку у вигляді міжнародної технічної допомоги, гарантій для інвесторів та розширення доступу до глобальних фінансових інструментів. Лише за умови синергії внутрішніх реформ і зовнішньої підтримки можливо забезпечити стійке фінансове оздоровлення бізнес-середовища та активізувати процеси економічного зростання.

Воєнні дії також провокують масову міграцію населення, особливо висококваліфікованих фахівців, що призводить до дефіциту трудових ресурсів і ускладнює процеси економічного відновлення та модернізації. Поглиблюється демографічна криза, яка проявляється у зниженні рівня народжуваності та старінні населення [8].

Окрім воєнних викликів, значну загрозу становлять системні ризики, які існували задовго до початку збройного конфлікту. Високий рівень корупції та неефективність судової системи є ключовими факторами, що стримують інвестиційну активність і перешкоджають розвитку підприємництва. Недосконалість

регуляторної політики, зокрема непрозорі та складні адміністративні процедури, створює бар'єри для започаткування та ведення бізнесу, знижуючи загальну конкурентоспроможність національної економіки. Невідповідність освітньої системи потребам ринку праці, низький рівень оплати праці та активні міграційні процеси спричиняють хронічний дефіцит кваліфікованих кадрів. Обмежений доступ до фінансових ресурсів, зумовлений високими обліковими ставками та консервативною політикою банків, ускладнює розвиток малого і середнього бізнесу, а також реалізацію інноваційних проєктів.

Цифрова трансформація, попри її значний потенціал для модернізації економіки, водночас виступає джерелом нових загроз, що набувають системного характеру. В умовах триваючого збройного конфлікту кіберпростір України фактично перетворився на арену бойових дій. Так, у 2023 році кількість зареєстрованих кіберінцидентів зросла на 62,5%, а лише за перше півріччя 2025 року Державний центр реагування на комп'ютерні інциденти CERT-UA зафіксував 535 підтверджених випадків. Основними цілями атак стали урядові та оборонні установи, однак приватний сектор також активно піддається кіберзагрозам [9]. Найпоширенішими типами атак залишаються сканування мереж, спроби експлуатації вразливостей, розповсюдження шкідливого програмного забезпечення та фішингові кампанії. Якщо раніше кібератаки мали переважно кримінальний характер, то нині вони трансформувалися в інструмент гібридної війни, спрямованої на підрив національної безпеки та дестабілізацію економічної системи. Особливу загрозу становить використання штучного інтелекту для створення високоточних та реалістичних атак, зокрема через діпфейки, автоматизований шантаж партнерських структур і моделювання поведінки користувачів. У цьому контексті подальше впровадження цифрових технологій – таких як штучний інтелект (AI), великі дані (Big Data) та Інтернет речей (IoT) – створює нові точки вразливості. Виникає парадоксальна ситуація, коли інструменти, призначені для управління ризиками та підвищення ефективності бізнесу, одночасно використовуються зловмисниками для реалізації більш складних і масштабних атак. Довгостроковим викликом для кібербезпеки є так званий «шифрувальний обрив» (encryption cliff), який може настати до 2030 року у зв'язку з очікуваним проривом у розвитку квантових обчислень. Потенційна здатність квантових комп'ютерів до зламу чинних криптографічних стандартів ставить під загрозу конфіденційність і цілісність цифрових даних. У зв'язку з цим бізнес-середовище має вже сьогодні розробляти довгострокові стратегії цифрової безпеки, передбачати перехід до квантово-стійкої криптографії та адаптувати IT-інфраструктуру до нових викликів [9].

Отже, в умовах ризикогенного середовища забезпечення економічної безпеки набуває статусу одного з ключових стратегічних пріоритетів для суб'єктів господарювання.

Як відзначається в наукових дослідженнях [11–13] функціонування системи економічної безпеки в ризикогенному середовищі має ґрунтуватися на безперервній діагностиці та моніторингу ризиків. Це передбачає не лише ідентифікацію вже існуючих загроз, таких як недобросовісні дії конкурентів, ринкова нестабільність чи регуляторні зміни, а й прогнозування появи нових факторів ризику. Ключовим елементом такої системи економічної безпеки є систематична ідентифікація загроз, що охоплюють фінансові, операційні, технологічні, правові, ESG та репутаційні аспекти. Для кожного ризику необхідно проводити оцінку ймовірності його настання та масштабів можливої шкоди, що дозволяє ефективно ранжувати ризики та раціоналізувати розподіл ресурсів. Система моніторингу повинна функціонувати у форматі безперервного збору та обробки даних у режимі реального часу, що забезпечує своєчасне виявлення та аналіз змін як у зовнішньому середовищі – зокрема політичних рішень, макроекономічних тенденцій та нормативно-правових трансформацій, – так і у внутрішньому контексті, включаючи показники ефективності бізнес-процесів, фінансову стабільність та кадрові ризики. Такий підхід дозволяє забезпечити високий рівень адаптивності системи управління ризиками, сприяє оперативному прийняттю управлінських рішень та підвищує загальну стійкість організації до динамічних викликів зовнішнього і внутрішнього характеру.

У контексті зростаючої економічної нестабільності традиційні статичні моделі управління ризиками поступово втрачають свою ефективність, що обумовлює необхідність переходу до більш гнучких та адаптивних підходів у забезпеченні економічної безпеки. Відповідна система має демонструвати здатність до оперативного коригування стратегій захисту, розробки варіативних сценаріїв реагування на широкий спектр можливих подій, зокрема економічні кризи, нормативно-правові зміни та інфляційні коливання. Ключовим фактором підвищення адаптивності виступає інтеграція сучасних цифрових технологій, таких як штучний інтелект, машинне навчання та аналітика великих даних, що дозволяють здійснювати прогнозування ризиків з високим ступенем точності, а також автоматизувати процеси виявлення загроз і реалізації превентивних заходів. Такий підхід сприяє формуванню проактивної моделі управління ризиками, здатної забезпечити стійкість економічної системи в умовах динамічного та багатофакторного середовища..

Забезпечення економічної безпеки в умовах ризикогенного середовища вимагає системного та комплексного підходу, який охоплює всі ключові аспекти функціонування підприємства, передбачаючи інтеграцію багатовимірних механізмів захисту, спрямованих на підтримання стабільності, стійкості та здатності до адаптації в умовах динамічних викликів. Фінансова безпека реалізується через ефективне управління грошовими потоками, контроль дебіторської та кредиторської заборгованості, а також впровадження заходів щодо мінімізації фінансових втрат. Інформаційна безпека передбачає захист конфіденційної інформації, комерційної таємниці та забезпечення протидії кіберзагрозам шляхом впровадження сучасних технологій шифрування, автентифікації та моніторингу. Кадрова безпека орієнтована на превентивну перевірку персоналу, управління ризиками, пов'язаними з людським фактором, та запобігання несанкціонованому розголошенню критично важливої інформації. Правова безпека забезпечується шляхом дотримання чинного законодавства, захисту прав власності, а також ефективного управління договірними зобов'язаннями та

юридичними ризиками. Технологічна безпека охоплює захист виробничих потужностей, інфраструктури та обладнання від впливу зовнішніх і внутрішніх загроз, включаючи техногенні ризики, саботаж, а також збої в роботі критичних систем. Сукупність зазначених компонентів формує основу для побудови цілісної системи економічної безпеки.

Слід вказати, що у сучасних умовах ризикогенного середовища, обмеження виключно реактивними заходами є недостатнім для забезпечення належного рівня економічної безпеки підприємства. Ефективна система економічної безпеки має функціонувати як складний, динамічний та адаптивний механізм, здатний до превентивного виявлення, запобігання та мінімізації наслідків як актуалізованих, так і латентних ризиків. Застосування проактивного підходу передбачає впровадження стратегій, спрямованих на диверсифікацію джерел доходу, формування резервних фінансових ресурсів, зміцнення партнерських зв'язків та розвиток стійких бізнес-екосистем, що здатні ефективно функціонувати в умовах невизначеності. Одним із ключових факторів забезпечення економічної стійкості є формування внутрішньої культури безпеки, за якої кожен працівник усвідомлює свою відповідальність у підтриманні стабільності організації та дотримується встановлених регламентів і процедур. Така культура сприяє інтеграції безпекових практик у всі рівні управління та операційної діяльності.

Побудова ефективної системи економічної безпеки українських підприємств в умовах в умовах невизначеності та багатовекторних ризиків передбачає реалізацію низки послідовних етапів. На початковому етапі здійснюється комплексний аудит та ідентифікація ризиків, що охоплюють як внутрішні, так і зовнішні загрози, включаючи цифрові, кадрові та екологічно-соціальні компоненти. Наступним кроком є впровадження ризик-менеджменту, заснованого на ризик-орієнтованому підході, який дозволяє розглядати ризики не лише як загрози, а й як потенційні можливості для розвитку та інновацій. Третій етап передбачає технологічну модернізацію, що включає інвестиції в GRC-платформи та інші цифрові інструменти, здатні забезпечити автоматизацію управлінських процесів, підвищення точності прогнозування та безперервний моніторинг ризиків. Завершальним етапом є розвиток людського капіталу шляхом впровадження програм безперервного навчання, спрямованих на підвищення цифрової компетентності персоналу та формування проактивної ризик-культури, що є необхідною умовою для ефективного функціонування системи економічної безпеки в умовах складного та мінливого середовища.

Варто констатувати, що все більш значуще місце в архітектурі економічної безпеки сучасних підприємств набувають GRC-платформи (Governance, Risk and Compliance) [14], особливо в контексті посилення регуляторних вимог, цифровізації бізнес-процесів та зростання комплексних ризиків. Ці платформи є інтегрованими технологічними рішеннями, що забезпечують узгоджене функціонування механізмів корпоративного управління, управління ризиками та дотримання нормативних приписів. Їх застосування сприяє формуванню стійкого та прозорого середовища, в якому процеси контролю, аудиту та реагування на загрози стають системними та керованими.

З точки зору забезпечення економічної безпеки, GRC-платформи дозволяють централізувати управління ризиками, автоматизуючи процеси їхньої ідентифікації, оцінки та моніторингу. Це охоплює широкий спектр загроз, включаючи фінансові, операційні, правові, екологічні, соціальні та управлінські ризики. Наприклад, такі платформи здатні відстежувати ліміти кредитних ризиків, виявляти аномалії у фінансових транзакціях, а також аналізувати ланцюжки поставок з урахуванням геополітичних та репутаційних факторів. Однією з ключових переваг є здатність своєчасно забезпечувати відповідність вимогам законодавства та галузевих стандартів, таких як GDPR, SOX або AML. Системи автоматично інформують відповідальних співробітників про нові нормативні зміни, формують звітність та забезпечують дотримання внутрішніх політик, тим самим знижуючи ймовірність санкцій та репутаційних втрат [14].

Крім того, GRC-платформи сприяють підвищенню прозорості та підзвітності управлінських рішень, формуючи єдине інформаційне середовище для керівництва, аудиторів та регуляторів. Консолідація даних щодо ризиків, аудитів та дотримання політик в єдиному цифровому просторі спрощує аналітичну роботу та прискорює прийняття рішень. Інтеграція GRC із системами управління безперервністю бізнесу та інцидентами дозволяє оперативно реагувати на кризові ситуації, мінімізуючи їх наслідки. У разі кібератак, технологічних збоїв чи інших порушень, платформа активує заздалегідь розроблені сценарії реагування, відстежує їх реалізацію та забезпечує комунікацію із зацікавленими сторонами.

Сучасні GRC-платформи виходять за рамки традиційних інструментів зберігання та обробки даних, все частіше інтегруючи технології штучного інтелекту та машинного навчання. Ці інструменти дозволяють прогнозувати ризики на основі аналізу великих масивів інформації, включаючи зовнішні джерела, такі як ресурси новин та соціальні мережі, що особливо актуально для виявлення репутаційних загроз. Автоматизація аудиту забезпечує перевірку значних обсягів транзакцій на відповідність внутрішнім регламентам та нормативним вимогам, підвищуючи точність та оперативність контролю. Управління політиками також оптимізується за рахунок автоматичного оновлення внутрішніх документів відповідно до змін законодавства, що знижує адміністративне навантаження та підвищує адаптивність організації.

Згідно з аналітичними даними [14], сучасні GRC-рішення охоплюють широкий спектр функцій: від управління політиками та внутрішнім аудитом до контролю за інцидентами, конфігураціями та відповідністю вимогам. Серед найбільш відомих постачальників таких рішень можна виділити SAP, MetricStream, RSA Archer та ServiceNow, кожна з яких пропонує спеціалізовані модулі, адаптовані під галузеві особливості та масштаби бізнесу.

Впровадження GRC-платформи є не просто технічним оновленням, а стратегічно значущим кроком, спрямованим на трансформацію моделі управління від реактивної до проактивної. Це дозволяє організаціям не тільки підвищити стійкість до зовнішніх і внутрішніх загроз, але і зміцнити свою конкурентоспроможність в умовах складності, що зростає, і невизначеності ділового середовища.

В цілому дотримання окреслених рекомендацій дозволить українським підприємствам не лише вистояти в умовах безпрецедентних викликів, але й закласти міцний фундамент для майбутнього відновлення та зростання.

Висновки. Аналіз сучасних тенденцій управління свідчить про те, що економічна безпека підприємства в умовах ризикогенного середовища не може розглядатися виключно як захисна функція, спрямована на нейтралізацію зовнішніх загроз. Натомість вона постає як багатовимірна, динамічна система, що має бути інтегрована у стратегічну парадигму управління підприємством. Такий підхід передбачає не лише реагування на вже реалізовані ризики, а й формування здатності до їх передбачення, запобігання та мінімізації наслідків у довгостроковій перспективі. У контексті зростаючої невизначеності, традиційні методи управління економічною безпекою втрачають свою ефективність. Вони не здатні забезпечити належний рівень захисту від нових, швидкоплинних загроз, що виникають у результаті технологічних змін, геополітичної нестабільності, цифрових трансформацій та еволюції нормативно-правового поля. Це зумовлює необхідність переходу до нової моделі економічної безпеки, яка базується на принципах системності, гнучкості, адаптивності та проактивності. Специфіка функціонування системи економічної безпеки в ризикогенному середовищі полягає у її здатності до постійного оновлення, інтеграції з усіма аспектами операційної та стратегічної діяльності підприємства, а також забезпечення безперервного моніторингу внутрішніх і зовнішніх факторів ризику. Така система має бути здатною до швидкого реагування на зміни середовища, оперативного коригування управлінських рішень та реалізації превентивних заходів, що сприяють збереженню стабільності, конкурентоспроможності та довгострокової стійкості підприємства. Отже, економічна безпека в сучасних умовах трансформується з інструменту захисту в стратегічний ресурс, що забезпечує не лише виживання, а й розвиток підприємства в умовах постійної турбулентності. Її ефективне забезпечення потребує комплексного підходу, що поєднує технологічні інновації, аналітичні інструменти, управлінську гнучкість та високий рівень організаційної культур.

Список використаних джерел:

1. Ареф'єва О. В., Кузенко Т. Б. Планування економічної безпеки підприємств. Київ : Видавництво Європейського ун-ту, 2004. 169 с.
2. Дикань В. Л., Воловельська І. В. Основні цілі системи економічної безпеки залізничного транспорту в постіндустріальний період. *Вісник економіки транспорту і промисловості*. 2021. № 75. С. 7–15.
3. Калинюк В. Є. Сучасні наукові підходи до визначення сутності поняття «економічна безпека підприємства». *Бізнес Інформ* . 2022. № 12. С. 221–228.
4. Ковальська Л., Голій О., Голій В. Економічна безпека підприємства: сутність, структура та механізм забезпечення. *Економічний форум*. 2023. №1(1). С. 126–137.
5. Крилов Д. В. Характеристика загроз економічній безпеці підприємства в сучасних умовах. *Проблеми сучасної трансформації. Серія: економіка та управління*. 2024. № 13. URL: https://reicst.com.ua/pmt/article/view/2024-13-04-07/2024-13-04-07
6. Прохорова В. В., Мушникова С. А. Коеволюційна основа управління економічною безпекою підприємств. *Бізнес Інформ*. 2020. № 12. С. 440–445.
7. Колісніченко В. Прямі збитки інфраструктури України від війни сягнули $170 млрд – KSE. 18 Лютого 2025. *GmkCenter : веб-сайт*. URL: https://gmk.center/ua/news/pryami-zbitkiinfrastrukturi-ukraini-vid-vijni-syagnuli-170-mlrd-kse/
8. Галузеві тренди. Ринок праці в Україні – виклики для бізнесу в умовах демографічної кризи 22 липня 2025. *Hub.Kyivstar : веб-сайт*. URL: https://hub.kyivstar.ua/articles/galuzevi-trendi-rinok-praczi-v-ukrayini-vikliki-dlya-biznesu-v-umovah-demografichnoyi-krizi
9. Статистичний звіт за результатами роботи Системи виявлення вразливостей і реагування на кіберінциденти та кібератаки в 2023 році. *Державний центр кіберзахисту Держспецзв'язку : веб-сайт*. URL: https://scpc.gov.ua/uk/articles/334
10. Дослідження стану та потреби українського бізнесу під час війни. *Дія : веб-сайт*. URL: https://business.diia.gov.ua/analytics/research/doslidzhennia-stanu-ta-potreb-ukrainskoho-biznesu-pid-chas-viiny
11. Нам'ясенко В. М. Економічна безпека підприємства в умовах воєнного стану. *Економіка України*. 2025. № 6. С. 25–38.
12. Капелюшна Т. В. Формування площини безпеки підприємства під дією ризиків і загроз. *Бізнес Інформ*. 2024. №3. С. 255–262.
13. Прохорова В., Крутова А., Дяченко К. Економічна безпека підприємств України в умовах дестабілізаційного розвитку. *Адаптивне управління: теорія і практика. Серія Економіка*. 2022. Вип. 14(28). URL: https://doi.org/10.33296/2707-0654-14(28)-10
14. Governance Risk And Compliance (GRC) Platform Market – Size and Forecast 2025–2029 : North America (US and Canada), Europe (France, Germany, Italy, and UK), Middle East and Africa (Egypt, KSA, Oman, and UAE), APAC (China, India, and Japan), South America (Argentina and Brazil), and Rest of World (ROW) Jan 2025. 205 p. *Technavio : website*. URL: https://www.technavio.com/report/governance-risk-and-compliance-platform-market-industry-analysis

References:

1. Arefieva O. V., Kuzenko T. B. (2004) Planuvannia ekonomichnoi bezpeky pidpryiemstv [Planning of economic security of enterprises]. Kyiv : Vydavnytstvo Yevropeiskoho universytetu, 169 p.
2. Dykan V. L., Volovelska I. V. (2021) Osnovni tsili systemy ekonomichnoi bezpeky zaliznychnoho transportu v postindustrialnyi period. [The main objectives of the economic security system of railway transport in the post-industrial period]. *Visnyk ekonomiky transportu i promyslovosti*. № 75. P. 7–15.
3. Kalyniuk V. Ye. (2022) Suchasni naukovi pidkhody do vyznachennia sutnosti poniattia "ekonomichna bezpeka pidpryiemstva". [Modern scientific approaches to defining the essence of the concept of "economic security of an enterprise"]. *Biznes Inform*. № 12. P. 221–228.

4. Kovalska L., Holii O., Holii V. (2023) Ekonomichna bezpeka pidpryiemstva: sutnist, struktura ta mekhanizm zabezpechennia [Economic security of an enterprise: essence, structure and mechanism of ensuring]. *Ekonomichnyi forum*. Vol. 1(1). P. 126–137.

5. Krylov D. V. (2024). Kharakterystyka zahroz ekonomichnii bezpetsi pidpryiemstva v suchasnykh umovakh [Characteristics of threats to the economic security of an enterprise in modern conditions]. *Problemy suchasnoi transformatsii. Seriia: ekonomika ta upravlinnia.* №. 13. Available at: https://reicst.com.ua/pmt/article/view/2024-13-04-07/2024-13-04-07

6. Prokhorova V. V., Mushnykova S. A. (2020) Koevoliutsiina osnova upravlinnia ekonomichnoiu bezpekoiu pidpryiemstv. [Coevolutionary basis for managing economic security of enterprises]. *Biznes Inform*. № 12. P. 440–445.

7. Kolisnichenko V. (2025) Priami zbytky infrastruktury Ukrainy vid viiny siahnuly $170 mlrd – KSE. [Direct losses of Ukraine's infrastructure from the war reached $170 billion – KSE]. *GmkCenter : veb-sait*. Available at: https://gmk.center/ua/news/pryami-zbitkiinfrastrukturi-ukraini-vid-vijni-syagnuli-170-mlrd-kse/

8. Haluzevi trendy. Rynok pratsi v Ukraini – vyklyky dlia biznesu v umovakh demohrafichnoi kryzy (2025) [Industry trends. The labor market in Ukraine – challenges for business in the conditions of the demographic crisis]. *Hub.Kyivstar : veb-sait*. Available at: https://hub.kyivstar.ua/articles/galuzevi-trendi-rinok-praczi-v-ukrayini-vikliki-dlya-biznesu-v-umovah-demografichnoyi-krizi

9. Statystychnyi zvit za rezultatamy roboty Systemy vyiavlennia vrazlyvostei i reahuvannia na kiberintsydenty ta kiberataky v 2023 rotsi. [Statistical report on the results of the work of the Vulnerability Detection and Response System for Cyber Incidents and Cyberattacks in 2023]. *Derzhavnyi tsentr kiberzakhystu Derzhspetszviazku : veb-sait*. Available at: https://scpc.gov.ua/uk/articles/334

10. Doslidzhennia stanu ta potreby ukrainskoho biznesu pid chas viiny [Research on the state and needs of Ukrainian business during the war]. *Diia : veb-sait*. URL: https://business.diia.gov.ua/analytics/research/doslidzhennia-stanu-ta-potreb-ukrainskoho-biznesu-pid-chas-viiny

11. Namiasenko V. M. (2025) Ekonomichna bezpeka pidpryiemstva v umovakh voiennoho stanu [Economic security of an enterprise in conditions of martial law]. *Ekonomika Ukrainy*. № 6. P. 25–38.

12. Kapeliushna T. V. (2024) Formuvannia ploshchyny bezpeky pidpryiemstva pid diieiu ryzykiv i zahroz. [Formation of the security plane of an enterprise under the influence of risks and threats]. *Biznes Inform*. №3. P. 255–262.

13. Prokhorova V., Krutova A., Diachenko K. (2022) Ekonomichna bezpeka pidpryiemstv Ukrainy v umovakh destabilizatsiinoho rozvytku. [Economic security of Ukrainian enterprises in conditions of destabilizing development]. *Adaptyvne upravlinnia: teoriia i praktyka. Seriia Ekonomika*. Vyp. 14(28). Available at: https://doi.org/10.33296/2707-0654-14(28)-10

14. Governance Risk And Compliance (GRC) Platform Market – Size and Forecast 2025-2029 : North America (US and Canada), Europe (France, Germany, Italy, and UK), Middle East and Africa (Egypt, KSA, Oman, and UAE), APAC (China, India, and Japan), South America (Argentina and Brazil), and Rest of World (ROW) (2025). 205 p. *Technavio : website*. Available at: https://www.technavio.com/report/governance-risk-and-compliance-platform-market-industry-analysis