Управління фінансово-кредитними системами та соціально-гуманітарна компонента їх розвитку

Management of financial and credit systems and the socio-humanitarian component of their development

DOI: 10.26565/2786-4995-2024-2-12
УДК 005.334:330.131.7

Валерія Баранова
доктор економічних наук, доцент
професор кафедри банківського бізнесу та фінансових технологій
ННІ «Каразінський банківський інститут»
Харківський національний університет імені В.Н. Каразіна
майдан Свободи, 4, м. Харків, 61022, Україна
e-mail: v.v.baranova@karazin.ua
ORCID ID: 0000-0002-8163-881X
Кристина Дворник
здобувач першого (бакалаврського) рівня вищої освіти
ННІ «Каразінський банківський інститут»
Харківський національний університет імені В.Н. Каразіна
майдан Свободи 4, 61022, Україна,
e-mail: kdvornik03@gmail.com

Діджиталізація ризик-менеджменту: новий вектор стратегічного успіху та сталого розвитку

Анотація. Діджиталізація та цифрова трансформація бізнесу сприяють зростанню продуктивності в усіх галузях економіки, створюючи додаткову вартість для споживачів, відбувається оптимізація внутрішніх бізнес-процесів підприємств та зниження їх витрат. У соціально головних галузях, діджиталізація та цифрова трансформація сприяють вирішенню соціальних проблем, покращенню доступу до державних і соціальних послуг.

Стрімкий прогрес технологій та зростання складності бізнес-середовища робить ефективне управління ризиками критичним фактором для стратегічного успіху підприємств у всіх секторах економіки. Особливо важливим у цьому контексті є трансформація традиційних методів ризик-менеджменту за допомогою цифрових інструментів та аналітики даних. Впровадження цифрових технологій у процес управління ризиками може стати вирішальним для досягнення конкурентних переваг та забезпечення сталого розвитку в Україні.

У статті охарактеризовано основні принципи управління цифровими ризиками; досліджуються методи управління ризиками через відбір варіантів з урахуванням сталості; розглядається сучасна практика та аналізуються інструменти управління інформацією. В рамках проведеного дослідження розглянуто зарубіжний досвід; а також, за допомогою аналізу методу «EBIOS RM» сформульовано рекомендації щодо предметної області дослідження.

Детальна увага приділена сучасному стану галузі інформаційних технологій України та виокремленню ключових проблем інформаційного менеджменту. Проаналізовано ефективні механізми управління інформацією та проведено систематизацію інструментів цифрового ризик-менеджменту.

Ключові слова: *діджиталізація, ризик-менеджмент, сталий розвиток, альтернативні інструменти управління.*

Формули: –; рис.: 1; табл.: 7; бібл.: 30.

Для цитування: Баранова В., Дворник К.. Діджиталізація ризик-менеджменту: новий вектор стратегічного успіху та сталого розвитку. Фінансово-кредитні системи: перспективи розвитку. №2(13)2024. С. 132-144. DOI: https://doi.org/10.26565/2786-4995-2024-2-12

Вступ. У сучасному світі глобалізації та швидкого технологічного розвитку підприємства стикаються з численними ризиками, які можуть значно підірвати їхню стійкість і конкурентоспроможність. Незважаючи на наявність різноманітних стратегій управління ризиками, важливо ефективно впроваджувати інструменти ризик-менеджменту, що відповідають сучасним умовам і вимогам ринку. Відсутність цілісної системи ризик-менеджменту на підприємствах може призвести до непередбачуваних фінансових втрат, втрати репутації та зниження конкурентоспроможності в умовах зростаючої конкуренції та ринкової нестабільності. Ефективне управління ризиками є необхідним елементом сучасної підприємницької діяльності, що забезпечує безперебійне функціонування та досягнення високої результативності. Стратегічні цілі такої системи включають забезпечення стійкого зростання прибутку, підтримку фінансової стабільності, створення можливостей для розвитку підприємства через підвищення продуктивності та конкурентоспроможності, а також виконання соціальних функцій.

Метою статті є розкриття можливості цифровізації управління ризиками як інструменту підвищення конкурентоспроможності та стійкості бізнесу в умовах постійних змін та нестабільності економічного середовища. В умовах невизначеності виникає потреба аналізу та виокремлення методів боротьби із загрозами в управлінні ІТ-підприємствами. Підставою, для цього є те, що у 2024 році ця сфера стала однією з найбільш затребуваних на експортному ринку України.

Аналіз досліджень та постановка завдання. Аналіз досліджень вчених показує, що такі науковці як Балдинюк В. [1], Горго І. [2], Данченко О. [3], Занора В. [3], Дуброва О. [4], Перевозова І. [5], Шайбан В. [5] ,Деделюк О. [5], Калініна Л. [6] [7] [8], приділяють значну увагу різним аспектам ризик-менеджменту в цілому, його цифровізації та наслідкам цієї еволюції в діяльності підприємств.

Загрозам у сфері ІТ, а саме неефективному управлінню інформацією та перешкодам при впровадженні успішних стратегій інформаційного менеджменту присвячено багато наукових досліджень, серед них: Васильків Н. [9], Вовчак І. [10], Жежнич П. [11], Кузьміних В. [12], Тараненко Р. [12].

На підставі аналізу праць вчених, можна зазначити, що ефективне управління інформацією є ключовим для досягнення переваг у ризик-менеджменті. Науковці наголошують до уважного розуміння поняття цифрових ризиків та сталого розвитку і пропонують дотримуватися певних принципів при впровадженні його у корпорації. Доступ до точної, своєчасної та відповідної інформації дозволяє приймати обґрунтовані рішення. Отже, дослідження цієї теми є необхідним, оскільки в умовах постійних змін та зростаючої складності бізнес-середовища в Україні, здатність швидко і точно реагувати на ризики стає вирішальним фактором для забезпечення стійкості та конкурентоспроможності підприємств.

Актуальність теми дослідження зумовила необхідність сформулювати наступну ціль та мету дослідження, які полягають у формуванні рекомендацій і пропозицій, спрямованих на ефективне подолання ризиків у цифровому середовищі ІТ-підприємств України. Діджиталізація ризик-менеджменту розширить область усвідомлення проблем розвитку та розробки альтернативних шляхів їх вирішення. Для досягнення поставленої мети і вирішення наукових завдань використовувались наступні методи дослідження: порівняльний аналіз, теоретичний аналіз наукових джерел, метод узагальнення даних, системний підхід, структурно-логічне узагальнення.

Інформаційною базою роботи були монографічні видання, періодичні наукові видання, інформаційні матеріали Всесвітнього економічного форуму, Французької асоціації управління ризиками, Французького національного агентства безпеки інформаційних систем, Королівської інженерної академії Великобританії.

Результати дослідження. Цифрова економіка стимулює впровадження цифрових технологій та інновацій у всіх секторах бізнесу, створює нові робочі місця та прискорює економічне зростання. Згідно зі звітом OECD, частка цифрової економіки становить від 4,5

до 15,5% світового ВВП, який стрімко зростає. Дослідження Oxford Economics і Huawei надає сценарій зростання цифрової трансформації, згідно з яким глобальна цифрова економіка може зрости до 24,3% світового ВВП до 2025 року, що дорівнює 23 трильйонам доларів США. Розвиток цифрової економіки дає змогу країнам прискорити зростання ВВП і зайнятості, підвищити продуктивність бізнесу та економічну ефективність, покращити суспільний добробут і принести користь споживачам завдяки економії коштів або часу.

У цифровій економіці споживачі отримують швидший доступ до продуктів і послуг за нижчою ціною. Тому перехід до цифрової економіки є важливим стратегічним пріоритетом урядів усіх країн. Цифрово трансформовані організації виграють від нематеріальних активів, мереж, нових бізнес-моделей, що створюють синергетичний ефект, створюючи цінності за допомогою цифрових технологій і цифрового середовища [13].

У першому кварталі 2022 року індустрія інформаційних технологій України досягла рекордних 2 мільярдів дол експортних надходжень, навіть у зв'язку з воєнним станом, мобілізацією, примусовою релокацією та переселенням бізнесу. Це значно перевищує показник у 1,44 мільярда дол за аналогічний період 2021 року, що свідчить про зростання обсягу ІТ-експорту на 28% згідно з даними Національного банку України [14]. Це дозволяє зробити висновок, що підприємства ІТ-сектору є критично важливими для української економіки сьогодення. У сфері ІТ однією з основних загроз є неефективне управління інформацією (табл. 1). Фахівцям у галузі ІТ доводиться подолати безліч перешкод під час впровадження успішних стратегій управління інформацією.

Таблиця 1. Головні загрози інформаційного менеджменту ІТ сектора
Table 1. The main threats to IT sector information management

Системи «Легасі»	Ускладнюють інтеграцію сучасних методів управління інформацією зі старими платформами, що призводить до конфліктів та проблем
Складність даних	Збільшується за рахунок наявності неструктурованої інформації, такої як соціальні мережі та дані з сенсорів, що потребує нових підходів до їх зберігання та обробки
«Вибух» даних	Ситуація, коли обсяг інформації стрімко зростає, перевищуючи можливості традиційних систем зберігання та обробки даних, що ускладнює їх управління та використання
Опір змінам	В організаційному мисленні та культурні фактори можуть утруднити широкомасштабне впровадження нових процесів управління інформацією
Дані в силосах	Виникає, коли інформація розділена між різними відділами та системами, що ускладнює аналіз та співпрацю між командами

Джерело: побудовано авторами на підставі [6, 7, 8]
Source: prepared by the authors on the basis of [6,7,8]

Ефективне керування інформацією допомагає відповідати галузевим регуляторним вимогам, таким як GDPR, HIPAA тощо. Використання даних надає можливість отримати унікальні інсайти для інновацій, випередження конкурентів та адаптації до тенденцій ринку. Правильне керування інформацією допомагає мінімізувати ризики порушення безпеки даних, втрати та несанкціонованого доступу, що забезпечує конфіденційність. Інформація, яка знаходиться у всіх сферах управління, значно впливає на функціонування різних організаційних структур і призводить до досягнення економічних результатів. Це призводить до змін у сприйнятті суспільством організацій, оскільки в умовах розвитку ринкових відносин надзвичайно важливо ефективно керувати інформаційними ресурсами у різних організаційних структурах.

Ефективне управління інформаційними ресурсами може значно підвищити продуктивність, забезпечити конкурентні переваги та забезпечити успіх організації в цій динамічній галузі. В дослідженні, також, детально розглянуто моделі та концепції інформаційного менеджменту сфери ІТ. Однак варто відзначити, що ці концепції та моделі є лише окремими прикладами того, як ІТ-компанії можуть використовувати інформаційний менеджмент для підвищення організаційної ефективності. Вибір моделей та концепцій повинен відповідати конкретним потребам та характеру діяльності компанії.

DevOps – це концепція, яка спрямована на поліпшення співпраці між розробниками програмного забезпечення та операторами систем. Це досягається за допомогою автоматизації процесів розробки, тестування та впровадження програмного забезпечення. DevOps допомагає підвищити швидкість впровадження змін, зменшити час відклику та забезпечити більшу стабільність систем. Основні принципи DevOps представлені на рис. 1, це культурний та методологічний підхід до розробки програмного забезпечення, спрямований на поліпшення співпраці між розробниками програмного забезпечення (Developers) та операторами систем (Operations) з метою автоматизації процесів розробки, тестування та впровадження програмного забезпечення.

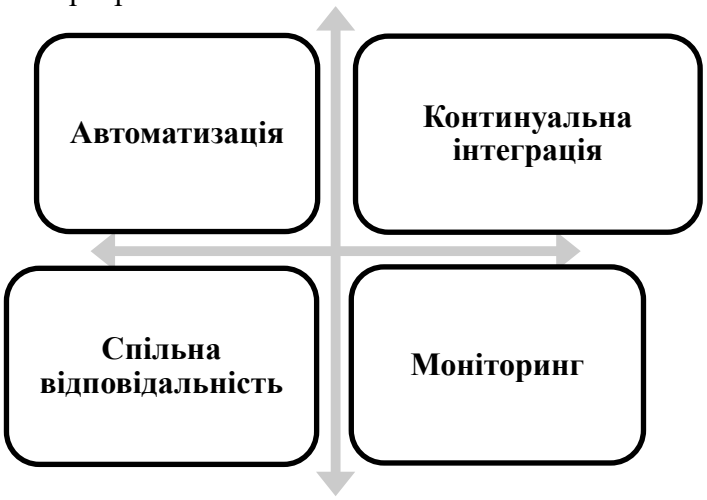

Рис. 1. Основні принципи DevOps, згідно культурного та методологічного підходу до розробки програмного забезпечення
Figure 1. Basic principles of DevOps, according to the cultural and methodological approach to software development
Джерело: побудовано авторами
Source: prepared by the authors

Отже, практика регулярного об'єднання (інтеграції) коду та автоматичної доставки (деплою) змін у виробниче середовище відіграє ключову роль. Співпраця між розробниками та операторами є важливою для досягнення спільної мети та забезпечує ефективне та стабільне впровадження програмного забезпечення. Постійний моніторинг роботи системи та зворотний зв'язок дозволяють постійно вдосконалювати процеси. Рух за автоматизацію технологічних процесів, включаючи складання, налаштування та розгортання програмного забезпечення, зародився у 2009 році для вирішення проблем взаємодії між розробниками та тими, хто відповідає за експлуатацію. Згідно з Puppet, понад 80% організацій вже застосовують DevOps. Прогноз Researchandmarkets.com передбачає зростання ринку DevOps з 10,84 мільярда дол у 2023 році до 24,71 мільярда дол протягом наступних чотирьох років, що відповідає річному темпу зростання у 22,9%.

Наступна методологія розробки програмного забезпечення це **Scrum,** яка базується на ітеративних та інкрементальних процесах. Основні принципи Scrum полягають у розробці продукту шляхом невеликих ітераційних кроків, залученні до процесу клієнтів та постійному вдосконаленні. Це емпіричний процес, де рішення базуються на спостереженнях, досвіді та експериментуванні. Scrum має три основні принципи: прозорість, перевірка та адаптація, що підтримує концепцію ітеративної роботи. Ця методологія сприяє підвищенню ефективності розробки, забезпечує гнучкість у відповіді на змінність вимог та забезпечує високу якість продукту. Scrum широко використовується у сфері програмного забезпечення та інших галузях, де важливо швидко реагувати на зміни та ефективно взаємодіяти з клієнтами. Фреймворк Scrum має просту структуру і включає команду Scrum, що складається з Власника продукту, Майстра Scrum та Розробників, кожен з яких має свої конкретні функції. Основні складові Scrum наведено у табл. 2.

Таблиця 2. Елементи циклу Scrum
Table 2. Elements of the Scrum cycle

Спринти	Короткі періоди часу (1-3 тижні), під час яких розробляється ітерація продукту. Кожен спринт має чітко визначену мету та набір завдань
Майстер Scrum	Особа, яка відповідає за впровадження методології Scrum у команді та забезпечує її дотримання
Команда Scrum	Команда Scrum складається з розробників, тестувальників та інших учасників проєкту, які працюють разом для досягнення спільної мети
Власник	Це представник замовника або клієнта, який визначає вимоги до продукту та визначає його пріоритети
Список завдань	Список завдань або функцій, які потрібно виконати для реалізації продукту. Він постійно оновлюється та пріоритизується за допомогою Власника

Джерело: побудовано авторами на підставі [15]
Source: prepared by the authors on the basis of [15]

Щоденні зустрічі під час спринту є ключовим елементом методології Scrum. Вони проводяться щодня, зазвичай у стоячому форматі, та тривають не більше 15 хвилин в одному і тому ж часі та місці. Під час цих зустрічей команда представляє свій прогрес у досягненні цілей спринту та ідентифікує будь-які можливі перешкоди. Мета полягає не в детальному обговоренні проблем, а в їх виявленні для подальшого вирішення.

Таблиця 3. Систематизація інструментів цифрового ризик-менеджменту
Table 3. Systematization of digital tools on risk management

Термін	**Розуміння**	**Приклади**
Системи управління подіями (SIEM)	Аналізують та обробляють дані з різних джерел для виявлення цифрових загроз та забезпечують централізований моніторинг та управління подіями в реальному часі.	Splunk; IBM Qradar; LogRhythm; McAfee Enterprise Security Manager (ESM)
Audit Logs	Audit Logs (Аудиторські журнали) збирають інформацію про всі події у системі, такі як доступ до даних та зміни конфігурацій, для подальшого аналізу безпеки та виявлення аномальних активностей.	Windows Event Log; Linux Audit Framework; Splunk Enterprise Security
Сканери вразливостей	Сканують мережі та системи на вразливості у програмному забезпеченні, операційних системах та конфігураціях для вживання необхідних заходів для їх виправлення.	Nessus; OpenVAS; Qualys Vulnerability Management
Системи виявлення вторгнень (IDS)	Моніторять мережу та комп'ютери на предмет аномальної або шкідливої активності для вчасного виявлення потенційних загроз і вживання відповідних заходів.	Snort; Suricata; Bro/Zeek; Cisco Firepower; Palo Alto Networks IDS/IPS
Ідентифікація та аутентифікація	Використовуються для перевірки особи або суб'єкта, що намагається отримати доступ до системи, за допомогою систем одноразових паролів, біометрії та інших методів.	Duo Security; RSA SecurID; Google Authenticator; YubiKey
Шифрування даних	Шифрування даних застосовується для захисту конфіденційної інформації від несанкціонованого доступу.	Symantec Endpoint Encryption; BitLocker

Джерело: побудовано авторами на підставі [6, 19]
Source: prepared by the authors on the basis of [17]

Майстри Scrum відповідають за ефективне використання цих щоденних зустрічей учасниками команди, а також за забезпечення альтернатив, якщо вони не можуть бути проведені. Відповідно, зростаюча кількість IT-компаній в Україні вимагає впровадження сучасних методів управління інформацією для ефективної конкуренції на міжнародному ринку. За неофіційними [16] даними, в Україні налічується близько 4 тисяч IT-підприємств. Отже, концепції управління інформацією в галузі IT стають все більш важливими для підвищення організаційної ефективності та конкурентоспроможності компаній. Зазначимо, що для ефективного управління цифровими ризиками у стратегічному управлінні можуть

використовуватися різноманітні методи, і в цьому дослідження робиться акцент на деяких інструментах цифрового ризик-менеджменту, проводиться їх систематизація та аналіз (табл. 3).

Далі розглянуто кейс впровадження системи управління подіями (SIEM). Згідно зі статистикою внутрішніх загроз, наведеною у звіті Verizon Data Breach Investigation Report, три з п'яти основних причин порушень безпеки пов'язані з внутрішніми загрозами [17]. Виявлення таких загроз є складним завданням, оскільки зловмисники часто виглядають як звичайні користувачі, що не викликає підозр. Проте SIEM може допомогти виявити індикатори внутрішніх загроз шляхом аналізу поведінки, що дозволяє командам забезпечення безпеки вчасно виявляти та запобігати таким атакам. SIEM використовує аналіз поведінки для виявлення аномалій, що можуть вказувати на компрометацію користувача. Система корелює мережевий трафік з інтелектуальними загрозами, щоб виявити взаємодію зовнішніх атакуючих програм з внутрішніми користувачами. Аналізуючи поведінку, система об'єднує на перший погляд непов'язані події, такі як вставлення USB-накопичувачів, використання особистих електронних поштових сервісів, несанкціоноване зберігання даних у хмарі або надмірне друкування. SIEM також зупиняє шифрування великого обсягу даних, оскільки це може свідчити про атаку вірусом-вимагачем.

EBIOS Risk Manager (або EBIOS RM) є ефективним інструментом у сфері управління цифровими ризиками, розробленим Національним агентством кібербезпеки Франції (ANSSI) з підтримкою Клубу EBIOS. Клуб EBIOS – це асоціація, яка об'єднує експертів та організації з різних секторів, зокрема, як публічних, так і приватних. З 2003 року він активно сприяє розвитку та популяризації французьких стандартів в управлінні ризиками, включаючи стандарт ISO 31000:2018 та стандарти серії ISO/IEC 27000. Метод EBiOS RM використовує ітеративний підхід, що ґрунтується на проведенні п'яти робочих "воркшопів" (табл. 4).

Таблиця 4. Сутність «воркшопів» EBIOS RM
Table 4. The essence of the EBIOS RM "workshops"

«ВОРКШОП» 1	Обсяг і базова безпека
«ВОРКШОП» 2	Походження ризику
«ВОРКШОП» 3	Стратегічні сценарії
«ВОРКШОП» 4	Операційні сценарії
«ВОРКШОП» 5	«Лікування» ризику

Джерело: побудовано авторами на підставі [23]
Source: prepared by the authors on the basis of [23]

В рамках даної концепції цифрового ризик-менеджменту використовується «Трьохрівнева піраміда ризиків». На першому рівні – основа цієї піраміди – знаходяться основні принципи та гігієна. Другий рівень включає регулятивний та стандартний фреймворк. На верхівці – третій рівень – знаходиться оцінка цифрового ризику. Перший «воркшоп» використовується для ідентифікації об'єкта дослідження, учасників та часових рамок роботи, що базується на першому та другому рівнях «піраміди». В цей період складається перелік місій, бізнес-активів та допоміжних активів, що пов'язані з об'єктом дослідження, і визначаються потенційні небезпечні події, що стосуються бізнес-активів, а також, оцінюється ступінь серйозності їхніх наслідків. У другому «воркшопі» визначається та характеризується джерела ризику (ДР) та їх високорівневі цілі, відомі як цільові об'єкти (ЦО). Найважливіші пари ДР/ЦО обираються в кінці цього етапу, а результати формалізуються у картографії джерел ризику. У третьому «воркшопі» отримується чітке уявлення про екосистему та створюється карта цифрових загроз щодо об'єкта дослідження. Це дозволяє розробити стратегічні сценарії, які представляють шляхи атаки для досягнення цілей ризиків. Сценарії розробляються на рівні екосистеми та бізнес-активів об'єкта дослідження та оцінюються за серйозністю. Метою четвертого «воркшопу» є розробка технічних сценаріїв, які включають методи атак, ймовірно використовувані джерелами

ризику для виконання стратегічних сценаріїв. На цьому етапі оцінюється ймовірність отриманих оперативних сценаріїв. Другий, третій та четвертий «воркшопи» базуються на третьому рівні «піраміди ризиків». П'ятий «воркшоп» полягає у підсумковому складанні всіх вивчених ризиків для визначення стратегії обробки ризиків, яка поділяється на заходи безпеки, що записуються у плані постійного вдосконалення [18, 19].

Головна мета цієї методології полягає в допомозі організаціям у виявленні, оцінці та управлінні ризиками, пов'язаними з їх інформаційними системами. Ця методика застосовується як до публічних, так і до приватних організацій, незалежно від їх розміру, галузі діяльності та статусу їхніх інформаційних систем. Подібно до того, як тактичний метод мислення надихає офіцерів на аналіз ситуації перед проєктуванням маневру, який підкорюється рішенню командира, метод EBIOS дозволяє оцінити ризики, що впливають на цифровий проєкт, з метою прийняття відповідних заходів.

Таблиця 5 відображає аналіз першого воркшопу, який було побудовано авторами статті. Оскільки стаття базується на аналізі в галузі інформаційних технологій, то для цього прикладу використовується кібербезпекова компанія, яка спеціалізується на захисті фінансових установ. Важливо зауважити, що на цьому етапі може знадобитися ідентифікувати бізнес-активи або підтримуючі активи, за які відповідають суб'єкти поза межами обраної організації. Ці елементи можуть бути включені в третій воркшоп під час створення мапування цифрових загроз екосистеми. Визначення та опис переймаючих подій (ПП) надає можливість зацікавленим сторонам об'єктивно порівнювати значимість місій та бізнес-активів.

Таблиця 5. Кейс-приклад використання «воркшоп» 1 для компанії IT-галузі
Table 5. Case-example of using "workshop" 1 for an IT company

Місія	Захист фінансових установ від кіберзагроз		
Назва бізнес-активу	Центр операцій з безпеки (SOC)		
Характер бізнес-активу (процес/інформація)	Інформація		
Опис	Центр операцій з безпеки (SOC) контролює кібербезпекові операції фінансових установ, що включає: • Постійний моніторинг мережевого трафіку та подій з безпеки. • Виявлення та аналіз потенційних кіберзагроз. • Реагування на інциденти та їх локалізація. • Проведення форензичного розслідування порушень безпеки. • Впровадження заходів забезпечення безпеки та кращих практик.		
Суб'єкт або особа, відповідальна (внутрішня/зовнішня)	Головний інформаційний безпеки офіцер (CISO)		
Назва пов'язаного підтримуючого активу(ів)	Платформа загроз інтелектуальної безпеки (TIP)	Система управління інформацією та подіями безпеки (SIEM)	Рішення для виявлення та реагування на загрози на кінцевих точках (EDR)
Опис	Агрегує, корелює та аналізує дані про загрози з різних джерел, щоб надати практичні висновки про виникнення кіберзагроз	Збирає та аналізує журнальні дані з мережевих пристроїв, для виявлення інцидентів та порушень безпеки	Моніторить кінцеві точки на предмет підозрілих дій та реагує на інциденти безпеки в реальному часі
Суб'єкт або особа, відповідальна (внутрішня/зовнішня)	Аналітики Центру операцій з безпеки (SOC)	Команда з інформаційної безпеки	Зовнішні постачальники кібербезпекових послуг

Джерело: побудовано авторами на підставі [18, 19, 20]
Source: prepared by the authors on the basis of [18,19,20]

Рівень шкоди або впливу оцінюється за шкалою серйозності, що дозволяє класифікувати події, які відбуваються (табл. 6). Наступним кроком є визначення базового рівня безпеки та виявлення прогалин. Це включає прийняття підходу до відповідності, який відповідає першим двом етапам піраміди управління ризиками. Для цього необхідно визначити всі стандарти безпеки, що застосовуються до досліджуваного об'єкта. До таких стандартів можуть належати: Правила здорової інформаційної системи та найкращі практики безпеки, включаючи рекомендаційні посібники та внутрішні правила безпеки організації; Стандарти, такі як сімейство ISO 27000; Поточні регуляції.

Таблиця 6. Шкала серйозності, яка дозволяє оцінити рівень шкоди або впливу
Table 6. A severity scale that allows you to assess the level of damage or impact

ШКАЛА	НАСЛІДКИ
G4 КРИТИЧНИЙ	Неможливість компанії забезпечити всю або частину своєї діяльності, що може мати серйозний вплив на безпеку осіб та активів. Компанія, ймовірно, не подолає ситуацію (її виживання загрожує)
G3 СЕРЙОЗНИЙ	Високий розклад у виконанні діяльності, що може мати значний вплив на безпеку осіб та активів. Компанія подолає ситуацію з серйозними труднощами (робота у вкрай погіршеному режимі)
G2 СУТТЄВИЙ	Погіршення виконання діяльності без впливу на безпеку осіб та активів. Компанія подолає ситуацію, хоч і з деякими труднощами (робота у погіршеному режимі)
G1 НЕЗНАЧНИЙ	Немає впливу на операції або виконання діяльності або на безпеку осіб та активів. Компанія подолає ситуацію без надмірних труднощів (резерви будуть витрачені)

Джерело: побудовано авторами на підставі [18]
Source: prepared by the authors on the basis of [18]

Якщо об'єктом дослідження є існуюча система або продукт, необхідно оцінити стан впровадження цих стандартів. Це можна зробити за допомогою кольорових індикаторів (зелений – «застосовується без обмежень», помаранчевий – «застосовується з обмеженнями», червоний – «не застосовується»), а також чіткого виявлення прогалин і їх причин. Ці дослідження дозволяють ідентифікувати та впровадити заходи безпеки, які стають частиною базового рівня безпеки компанії і можуть бути перевірені на наступних воркшопах з оцінки ризиків.

Відповідно до філософії EBIOS RM, управління цифровими ризиками повинно розвивати три основні цінності: знання, гнучкість та відданість. Для досягнення цієї мети EBIOS RM сприяє загальному розумінню та відповідальності за цифрові ризики між особами, що приймають рішення, та зацікавленими сторонами. Метою є забезпечення менеджерів розумінням цих ризиків, а також стратегічних, фінансових, юридичних, іміджевих, кадрових та інших ризиків.

У світовій економіці сучасні тенденції і глобальні виклики вимагають уваги до проблем сталого розвитку. Швидкі зміни і зростаюча невизначеність як у внутрішніх економічних системах, так і на міжнародній арені підкреслюють актуальність цих досліджень. Дослідження необхідні для визначення ефективних інструментів та механізмів, що сприяють сталому розвитку. Згідно з доповіддю «Global Risk 2008» Всесвітнього економічного форуму, основна увага приділяється п'яти групам глобальних ризиків: геополітичним, економічним, технологічним, соціальним та екологічним [21]. При цьому, показники-індикатори загроз сталого розвитку підприємств у сфері IT можна розділити на різні категорії. Для будь-якого підприємства перехід до нової стратегії або її зміна – це певний стрес. Зарубіжні науковці наголошують на необхідності спочатку визначити аспекти охоплення стратегії (табл. 7).

Таблиця 7. Ключові напрямки сталої стратегії IT підприємства
Table 7. Key areas of the company's sustainable IT strategy

Розробка та впровадження програм з підвищення кібербезпеки, що включають у себе регулярні аудити та оцінку загроз, підвищення обізнаності персоналу та застосування передових технологій захисту	Інвестування в кібербезпеку
Розробка та впровадження строгих політик захисту даних, включаючи шифрування, резервне копіювання та контроль доступу	Забезпечення приватності
Систематичне оновлення і підтримка існуючого програмного забезпечення та інфраструктури з метою забезпечення стійкої та ефективної роботи	Оновлення технологій
Впровадження програм корпоративної соціальної відповідальності, що включають у себе ініціативи з підтримки освіти, охорони здоров'я та захисту довкілля	Розвиток персоналу
Мінімізація впливу діяльності підприємства на довкілля шляхом зменшення енергоспоживання, використання відновлювальних джерел енергії та впровадження зелених технологій	«Зелена» ініціатива

Джерело: побудовано автором на підставі [13, 23, 24]
Source: prepared by the authors on the basis of [13,23,24]

Прикладом акцентування важливості цифрової трансформації в контексті загроз є співпраця французьких організацій «AMRAE» (Association pour le Management des Risques et des Assurances de l'Entreprise) і «ANSSI» (Agence Nationale de la Sécurité des Systems d'Information). Об'єднання зусиль цих організацій спрямоване на досягнення ефективності в управлінні цифровими ризиками. Бріжіт Буко, Голова AMRAE, вказує на те, що їхня співпраця приносить результати, оскільки їхні підходи до управління ризиками доповнюють один одного: AMRAE зосереджується на економічних аспектах, які є основою корпоративного управління. Тоді як ANSSI фокусується на технологічних аспектах, які визначають національні стандарти безпеки. Гійом Пупар, Генеральний директор ANSSI, додає, що співпраця є корисною через спільне бачення та обмін знаннями, що дозволяє їм взаємно збагачуватися та краще відповідати на виклики. Обидві організації підкреслюють, що цифровий ризик став дійсно важливим, але ще є багато роботи, перш ніж його можна буде повністю контролювати. Лідери з усього світу, які отримують інформацію від ризик-менеджерів, поступово розуміють важливість цифрового ризику та включають його у загальну стратегію управління ризиками [22]. З метою надання допомоги підприємствам у цьому питанні, AMRAE та ANSSI розробили посібник «Controlling the Digital Risk: The Trust Advantage» (Керування цифровим ризиком: перевага довіри), який пропонує керівникам та менеджерам з управління ризиками поетапний підхід для створення політики управління цифровими ризиками в їх організації. Посібник, також, містить корисні ресурси та поради для консолідації або перенаправлення вже існуючої політики.

Широкий спектр якісних і кількісних підходів до дослідження ризиків і загроз використовується в промисловості та управлінні громадською політикою у Великобританії. У спеціальному дослідженні Британської Королівської Академії Інженерії зосереджувалися на викликах, пов'язаних з проєктуванням сценаріїв, картографуванням взаємозалежностей, оцінкою часових масштабів, використанням даних, інклюзією та процесами введення та експертизи [23]. Ці виклики досліджувалися через набір з 17 випадкових загроз, визначених та розроблених за допомогою структурованих інтерв'ю, експертних відгуків та робочого досвіду. Належна увага приділялася і виявленню характеристик вразливості в архітектурі мережі інфраструктури Великої Британії та розробці моделі для оцінки їх відносної важливості [23]. Ця модель спрямована на ідентифікацію місць та активів з найбільшим ризиком для зменшення вразливості мережі, підвищення стійкості та оцінки ефективності цих заходів. Дослідження, також, включало аналіз умов для масштабних збоїв, зокрема, шляхом моделювання різних профілів електропостачання до 2050 року. Важливо підкреслити, що дослідження допомагає організаціям використовувати збалансований підхід до оцінки ризиків, що зміцнює їх стійкість на практиці. Це сприяє досягненню стратегічної

мети британського уряду зробити стійкість національною справою, щоб країна була готова до наступних криз, незалежно від їхнього характеру.

Висновки. У статті щодо оптимізації ризик-менеджменту в управлінській та корпоративній діяльності українських ІТ-підприємств з урахуванням сталого розвитку досліджено значний прогрес у сфері інформаційного менеджменту. Цей прогрес особливо помітний в контексті розвитку інформаційних технологій, що стали важливою складовою управління ІТ-підприємствами та в процесі глобалізації та інформатизації суспільства. Діджиталізація ризик-менеджменту відкриває нові можливості, включаючи застосування цифрових технологій для виявлення та аналізу ризиків, автоматизацію процесів оцінки та контролю ризиків, а також використання аналітики даних для прогнозування потенційних загроз. Цей підхід сприяє збільшенню ефективності, швидкості та точності в управлінні ризиками.

Результати дослідження вказують на необхідність впровадження сучасних інструментів цифрового управління ризиками, таких як системи управління подіями (SIEM), сканери вразливостей та рішення для управління ідентичністю. Підвищення здатності організацій реагувати на ризики та відновлювати функціонування після кризи залишається актуальним завданням для українського бізнесу у 2024 році. Досвід імплементації діджиталізації ризик-менеджменту за межами України підтверджує важливість боротьби з цифровими загрозами та необхідність сталого розвитку. Підхід до сталості вже давно застосовується у бізнесі та повсякденному житті таких країн як Франція та Великобританія. Науковці наголошують на важливості розуміння цифрових ризиків та сталого розвитку і рекомендують дотримуватися певних принципів при їх впровадженні в корпорації. У сучасному світі цифрова трансформація підприємств набуває величезного значення, тому сучасні керівники повинні володіти навичками використання спеціалізованого програмного забезпечення та додатків для створення «сталої екосистеми» свого підприємства. Отже, проведене дослідження підтверджує важливість впровадження сучасних інструментів та методів цифрового ризик-менеджменту для українських ІТ-підприємств. Це стратегічне рішення дозволить їм ефективно реагувати на зміни та знижувати ризики, пов’язані з цифровою трансформацією. На основі зарубіжного досвіду важливо надавати перевагу підходам, спрямованим на збереження сталості та забезпечення стійкого розвитку. Таким чином, вміння користуватися цифровими інструментами та програмним забезпеченням стає необхідністю для керівників у будь-якій сфері. За умови врахування цих підходів майбутні покоління нашої країни зможуть насолоджуватися розвинутим суспільством та чистим середовищем.

Список літератури

1. Балдинюк В.М. Ризик-менеджмент як інструмент управління діяльності суб’єктів господарювання. *Економіка та суспільство*. Випуск №55/2023
2. Горго І.О. Оцінка ефективності управління ризиками в системі менеджменту аграрних підприємств.
3. Данченко О.Б., Занора В.О. *Проєктний менеджмент: управління ризиками та змінами в процесах прийняття управлінських рішень.* Монографія. Черкаси: ПП Чабаненко Ю.А., 2019.
4. Дуброва О.С. Сучасний погляд на ризик-менеджмент як важливу складову системи управління підприємством. *Стратегія економічного розвитку України.* 2012. Вип. 1(8).
5. Перевозова І.В., Шайбан В.М., Деделюк О.В. До питання ролі ризик-менеджменту в цифровій трансформації промислового підприємства: сутність та інноваційний потенціал. *Наукові записки Львівського університету бізнесу та права*. Серія економічна. Серія юридична. Випуск № 38/2023.
6. Калініна Л.М. Генезис інформаційного менеджменту як галузі наукового знання. *Стратегічні пріоритети.* 2009. № 4 (13).
7. Калініна Л.М. Інформаційні процеси в управлінській діяльності керівника закладу: сутність, специфіка та характерні ознаки – Освіта і упр. – 2005.
8. Калініна Л.М. Система інформаційного забезпечення управління загальноосвітнім навчальним закладом. – Автореферат, Державний вищий навчальний заклад «Університет Менеджменту Освіти», 2008.
9. Васильків Н.М. Опорний конспект лекцій з дисципліни "Ефективність інформаційних систем". – Тернопіль: Економічна думка, 2005. – 98 с.

10. Вовчак І.С. Інформаційні системи та комп'ютерна техніка в менеджменті: Навч. посіб. – Тернопіль: Карт-бланш, 2002. – 354 с.
11. Жежнич П.І. Технології інформаційного менеджменту [Текст]: Навчальний посібник / П.І. Жежнич. – Львів: Львівська політехніка, 2010. – 260 с.
12. Кузьміних В.О., Тараненко Р.А. Основи управління ІТ проектами. – Навчальний посібник. Київ. 2019.
13. Transformation of the economic system in the context of information technology challenges: Collective monograph. Riga, Latvia: Baltija Publishing, 2024. 236 p. DOI: https://doi.org/10.30525/978-9934-26-437-5-4
14. Українське ІТ у війну: як було, як зараз і які прогнози. AIN.UA. URL: https://ain.ua/2022/12/09/ukrayinske-it-u-vijnu/
15. The home of Scrum. URL: https://www.scrum.org/
16. Продуктивність ІТ-компаній під час війни становить 90% – GlobalLogic. Економічна Правда. URL: https://www.epravda.com.ua/news/2022/03/28/684822/
17. 10 SIEM Use Cases in a Modern Threat Landscape. URL: https://www.exabeam.com/explainers/siem-security/siem-use-cases/
18. Agence Nationale de la Sécurité des Systèmes d'Information ANSSI., Ebios risk manager: an iterative approach in 5 workshops.
19. Agence Nationale de la Sécurité des Systèmes d'Information ANSSI., Ebios risk manager: Going Further.
20. Мостенська Т.Л., Скопенко Н.С. Ризик-менеджмент як інструмент управління господарським ризиком підприємства. *Вісник Запорізького національного університету.* 2010. № 3(7).
21. World Economic Forum: Global Risks Report 2008.
22. Association pour le Management des Risques et des Assurances de l'Entreprise (AMRAE)., Controlling the digital risk: The Trust Advantage.
23. Royal Academy of Engineering (2023). Building resilience: lessons from the Academy's review of the National Security Risk Assessment methodology. URL: https://nepc.raeng.org.uk/media/g31bttwt/raeng-building-resilience.pdf

Стаття надійшла до редакції 27.03.2024
Статтю рекомендовано до друку 12.06.2024

Valeria Baranova
Doctor of Economic Sciences
Professor of Department of Banking Business and Financial Technologies
Educational and Scientific Institute «Karazin Banking Institute»
V.N. Karazin Kharkiv National University, Kharkiv, Ukraine
4, Svobody Sq., Kharkiv, 61022, Ukraine
e-mail: v.v.baranova@karazin.ua
ORCID ID: 0000-0002-8163-881X
Krystyna Dvornyk
a graduate of the first (bachelor) level of higher education
Educational and Scientific Institute «Karazin Banking Institute»
V.N. Karazin Kharkiv National University, Kharkiv, Ukraine
4, Svobody Sq., Kharkiv, 61022, Ukraine
e-mail: kdvornik03@gmail.com

Digitalization of risk management: a new vector of strategic success and sustainable development

Abstract. The digital transformation of business contributes to the growth of productivity in all sectors of the economy, creating additional value for consumers, optimizing the internal business processes of enterprises and reducing costs. In socially significant sectors, digital transformation contributes to solving social problems, improving access to public and social services.

The rapid advancement of technology and the growing complexity of the business environment make effective risk management a critical factor for the strategic success of enterprises in all sectors of the economy. Especially important in this context is the transformation of traditional methods of risk management with the help of digital tools and data analytics. The implementation of digital technologies in the process of risk management can become decisive for achieving competitive advantages and ensuring sustainable development in Ukraine.

The article describes the main principles of digital risk management; methods of risk management are explored through the selection of options with sustainability in mind; modern practice is considered and information management tools are analyzed. In the framework of the conducted research, foreign experience was considered; and also, with the help of the analysis of the "EBIOS RM" method, recommendations were formulated regarding the subject area of the study.

Detailed attention is paid to the current state of the information technology industry in Ukraine and the identification of key problems of information management. Effective information management mechanisms were analyzed and digital risk management tools were systematized.

Key words: *digitalization, risk management, sustainable development, alternative management tools.*
Formulas: -; fig.: 1; tabl.: 7; bibl.: 30.

For citation: Baranova V., Dvornyk K. Digitalization of risk management: a new vector of strategic success and sustainable development. Financial and Credit Systems: Prospects for Development. №2(13)2024. P. 132-144. DOI: https://doi.org/10.26565/2786-4995-2024-2-12 [in Ukrainian]

References

1. Baldynyuk V.M. (2023. Issue No. 55) Risk management as a tool for managing the activities of business entities. *Economy and society*. [in Ukrainian].
2. Gorgo I.O. Evaluation of the effectiveness of risk management in the management system of agricultural enterprises [in Ukrainian].
3. Danchenko O.B., Zanora V.O. (2019) *Project management: managing risks and changes in management decision-making processes.* Monograph. Cherkasy: PP Chabanenko Yu.A. [in Ukrainian].
4. Dubrova O.S. (2012. Issue 1(8)). A modern view of risk management as an important component of the enterprise management system. *Strategy of economic development of Ukraine*. [in Ukrainian].
5. Perevozova I.V., Shaiban V.M., Dedelyuk O.V. (2023. Issue No. 38). On the question of the role of risk management in the digital transformation of an industrial enterprise: the essence and innovative potential - Scientific Notes of the Lviv University of Business and Law. The series is economical. Legal series. [in Ukrainian].
6. Kalinina L.M. (2009. No. 4 (13)) The genesis of information management as a field of scientific knowledge. *Strategic priorities.* [in Ukrainian].
7. Kalinina L.M. (2005) Information processes in the managerial activity of the head of the institution: essence, specificity and characteristic features - Education and management. [in Ukrainian].
8. Kalinina L.M. (2008) The system of information support for the management of a general educational institution. - Abstract, State higher educational institution "University of Management of Education". [in Ukrainian].
9. Vasylkiv N.M. (2005. 98 p.) Reference summary of lectures on the discipline "Effectiveness of information systems". – Ternopil: Economic Thought. [in Ukrainian].
10. Vovchak I.S. (2002. 354 p.) Information systems and computer technology in management: Education. manual – Ternopil: Carte Blanche. [in Ukrainian].

11. Zhezhnych P.I. (2010. 260 p.) Technologies of information management [Text]: Study guide / P.I. Zhezhnych – Lviv: Lviv Polytechnic. [in Ukrainian].
12. Kuzminykh V.O., Taranenko R.A. (2019). Basics of IT project management. - Tutorial. Kyiv. [in Ukrainian].
13. Transformation of the economic system in the context of information technology challenges: Collective monograph. Riga. Latvia. Baltija Publishing. 2024. 236 p. DOI: https://doi.org/10.30525/978-9934-26-437-5-4
14. Ukrainian IT at war: how it was, how it is now and what are the forecasts. AIN.UA. Retrieved from https://ain.ua/2022/12/09/ukrayinske-it-u-vijnu/ [in Ukrainian].
15. The home of Scrum. Retrieved from: https://www.scrum.org/
16. Productivity of IT companies during war is 90% - GlobalLogic. Economic Truth. Retrieved from https://www.epravda.com.ua/news/2022/03/28/684822/ [in Ukrainian].
17. 10 SIEM Use Cases in a Modern Threat Landscape. Retrieved from https://www.exabeam.com/explainers/siem-security/siem-use-cases/
18. Agence Nationale de la Sécurité des Systèmes d'Information ANSSI., Ebios risk manager: an iterative approach in 5 workshops
19. Agence Nationale de la Sécurité des Systèmes d'Information ANSSI., Ebios risk manager: Going Further
20. Mostenska T.L., Skopenko N.S. Risk management as a tool for managing the enterprise's economic risk. *Bulletin of Zaporizhzhya National University*. 2010. No. 3(7) [in Ukrainian].
21. World Economic Forum: Global Risks Report 2008
22. Association pour le Management des Risques et des Assurances de l'Entreprise (AMRAE)., Controlling the digital risk: The Trust Advantage
23. Royal Academy of Engineering (2023). Building resilience: lessons from the Academy's review of the National Security Risk Assessment methodology. Retrieved from https://nepc.raeng.org.uk/media/g31bttwt/raeng-building-resilience.pdf

The article was received by the editors 27.03.2024
The article is recommended for printing 12.06.2024