**DOI:** https://doi.org/10.30837/EK.2023.026

**Шейко І.А.,**
*к.е.н., доцент, доцент кафедри економічної кібернетики*
*та управління економічною безпекою,*
*Харківський національний університет радіоелектроніки*
*ORCID: https://orcid.org/0000-0002-5770-3677*
**Степаненко Р.Д.,**
*здобувач,*
*Харківський національний університет радіоелектроніки*
*ORCID: https://orcid.org/0009-0008-0586-0903*
**Кондрашов І.Є.,**
*здобувач,*
*Харківський національний університет радіоелектроніки*
*ORCID: https://orcid.org/0009-0008-0359-4605*

# АНАЛІЗ МЕТОДИЧНИХ ПІДХОДІВ ДО УПРАВЛІННЯ РИЗИКАМИ ПІДПРИЄМСТВА В УМОВАХ ЦИФРОВОГО РОЗВИТКУ

Цифрові технології відіграють ключову роль в управлінні ризиками та підвищенні економічної безпеки компаній у сучасному динамічному бізнес-ландшафті. Зі стрімким розвитком технологій компанії використовують цифрові інструменти для зміцнення своїх економічних основ. У сучасному ландшафті цифрова ера відкриває безпрецедентні можливості, але вона також породжує низку ризиків, які вимагають вмілих стратегій управління.

Швидкі темпи цифрової трансформації революціонізували спосіб роботи компаній, підвищивши ефективність, а також наразивши їх на безліч ризиків. Від кіберзагроз до витоку даних організації стикаються з проблемами, які вимагають проактивного управління ризиками для захисту своїх активів і репутації.

У [1] виділені 9 цифрових ризиків, які проявляються у трьох основних областях для компаній, що стали на шлях цифрової трансформації: збільшення ефективності нових процесів (ризики, пов'язані з впровадженням нових процесів для підвищення ефективності), нещодавно впроваджені системи та процеси ризики, пов'язані із з модернізацією застарілих процесів і впровадженням нових бізнес-моделей), ефективність обслуговування клієнтів (ризики, які можуть перешкоджати роботі служби підтримки клієнтів). У таблиці 1 наведені основні типи цифрових ризиків [1].

Таблиця 1 – Систематизація цифрових ризиків в межах трьох областей

| Області прояву цифрових ризиків | | |
|---|---|---|
| Збільшення ефективності нових процесів | Нещодавно впроваджені системи та процеси | Ефективність обслуговування клієнтів |
| *Кібератаки*: коли цифрова трансформація збільшує площу для атак<br>*Хмарна трансформація*: ризики, які виникають через розгортання нових рішень або зміни в хмарній архітектурі<br>*Витік даних*: несподіване або сплановане відкриття конфіденційних даних<br>*Ризики, пов'язані із персоналом*: цифрові ризики, які є побічним продуктом дефіциту талантів серед робочої сили | *Ризики відповідності*: неефективні заходи безпеки можуть перешкоджати нормам відповідності<br>*Ризики третіх сторін*: кіберзагрози, створені сторонніми постачальниками<br>*Ризики автоматизації процесів*: ризики, пов'язані із помилками у плануванні або виконанні автоматизації процесів | *Ризик стійкості бізнесу*: доступність сервісу викликає витік даних або загрозу кібератак<br>*Ризик конфіденційності даних*: ризики, пов'язані з розкриттям конфіденційних і приватних даних клієнтів |

*Джерело: побудовано авторами на основі [1, 2]*

Враховуючи поширеність кіберзагроз, ефективне управління ризиками в епоху цифрових технологій вимагає надійної системи кібербезпеки. Це передбачає впровадження передових заходів безпеки, проведення регулярних перевірок і виховання культури обізнаності серед співробітників, щоб зменшити ризик кібератак.

Цифровий ландшафт пов’язаний із потоками даних, що робить конфіденційність даних першорядною проблемою. Організації повинні не лише дотримуватися правил захисту даних, але й активно керувати ризиками, пов’язаними з обробкою конфіденційної інформації. Невиконання цього не лише спричиняє юридичні наслідки, але й шкодить довірі та цілісності бренду.

Цифрова ера характеризується швидким технологічним прогресом, але цей динамізм також створює проблеми для безперервності роботи. Стратегії управління ризиками повинні включати плани пом’якшення збоїв, забезпечення безперервності бізнесу та підвищення операційної стійкості перед обличчям

Європейська агенція з кібербезпеки ENISA [2] у аналізі кібер-загроз у 2023 році зосереджує увагу на наступних восьми основних групах загроз:

– програми-вимагачі – тип атаки, коли зловмисники захоплюють контроль над активами цілі та вимагають викуп в обмін на повернення доступності активу

– шкідливе програмне забезпечення – будь-яке програмне забезпечення, призначене для виконання несанкціонованого процесу, який матиме негативний вплив на конфіденційність, цілісність або доступність системи

– соціальна інженерія – широкий спектр діяльності, яка намагається використати людську помилку або людську поведінку з метою отримання доступу до інформації чи послуг

– загрози проти даних – набір загроз, спрямованих на джерела даних з метою отримання несанкціонованого доступу та розголошення, а також маніпулювання даними для втручання в поведінку систем;

– відмова в обслуговуванні – атаки відбуваються, коли користувачі системи або служби не можуть отримати доступ до відповідних даних, послуг або інших ресурсів. Цього можна досягти шляхом виснаження служби та її ресурсів або перевантаженням компонентів мережевої інфраструктури;

– кампанії дезінформації зростають, що стимулюється збільшенням використання платформ соціальних мереж та онлайн-медіа;

– атака на ланцюг постачання – спрямована на відносини між організаціями та їхніми постачальниками. Щоб атаку можна було класифікувати як атаку на ланцюг поставок, цілями мають бути як постачальник, так і клієнт.

Також у звіті ENISA стверджується, шо кількість кібератак у країнах ЄС (при аналізі даних за період липень 2022 – червень 2023) досягла піку у червні 2023 року та склала 600 атак в місяць, тоді як взимку 2023 року подібна кількість не перевищувала 200 кібератак. Щодо жертв кібератак, то максимальна частка припадає на органи держаного управління країн ЄС, що підтверджує заздалегідь спланований характер таких атак.

У ризик-менеджменті автори виділяють кілька ключових етапів [3]:

– виявлення ризику і оцінка ймовірності його реалізації і масштабу наслідків, визначення максимально-можливого збитку;

– вибір методів та інструментів управління виявленим ризиком;

– розробка ризик-стратегії з метою зниження ймовірності реалізації ризику і мінімізації можливих негативних наслідків;

– реалізація ризик-стратегії;

– оцінка досягнутих результатів і коригування ризик-стратегії.

Ключовим етапом ризик-менеджменту вважається етап вибору методів та інструментів управління ризиком.

Використання цифрових технологій особливого значення набуває для забезпечення конфіденційності та безпеки даних, прийняття інформований рішень на основі аналітики даних, забезпечення надійності фінансових операцій та для організації комунікації менеджменту з усіма стейкхолдерами (інвесторами, партнерами, клієнтами, постачальниками).

Дані, аналітика та IT-архітектура є ключовими факторами цифрового управління ризиками. Сильно фрагментовані архітектури IT і даних не можуть забезпечити ефективну структуру для виявлення цифрових ризиків. На щастя, процеси та методи аналітики тепер можуть підтримувати ці цілі за допомогою сучасних технологій у кількох ключових сферах, включаючи платформи великих даних, хмару, машинне навчання, штучний інтелект і обробку природної мови.

На основі аналізу літературних джерел, присвячених використанню цифрових технологій у ризик-менеджменті, сформовано перелік основних напрямів використання цифрових технологій у діяльності підприємства, а також перелік цифрових інструментів, які при цьому задіються (рисунок 2).

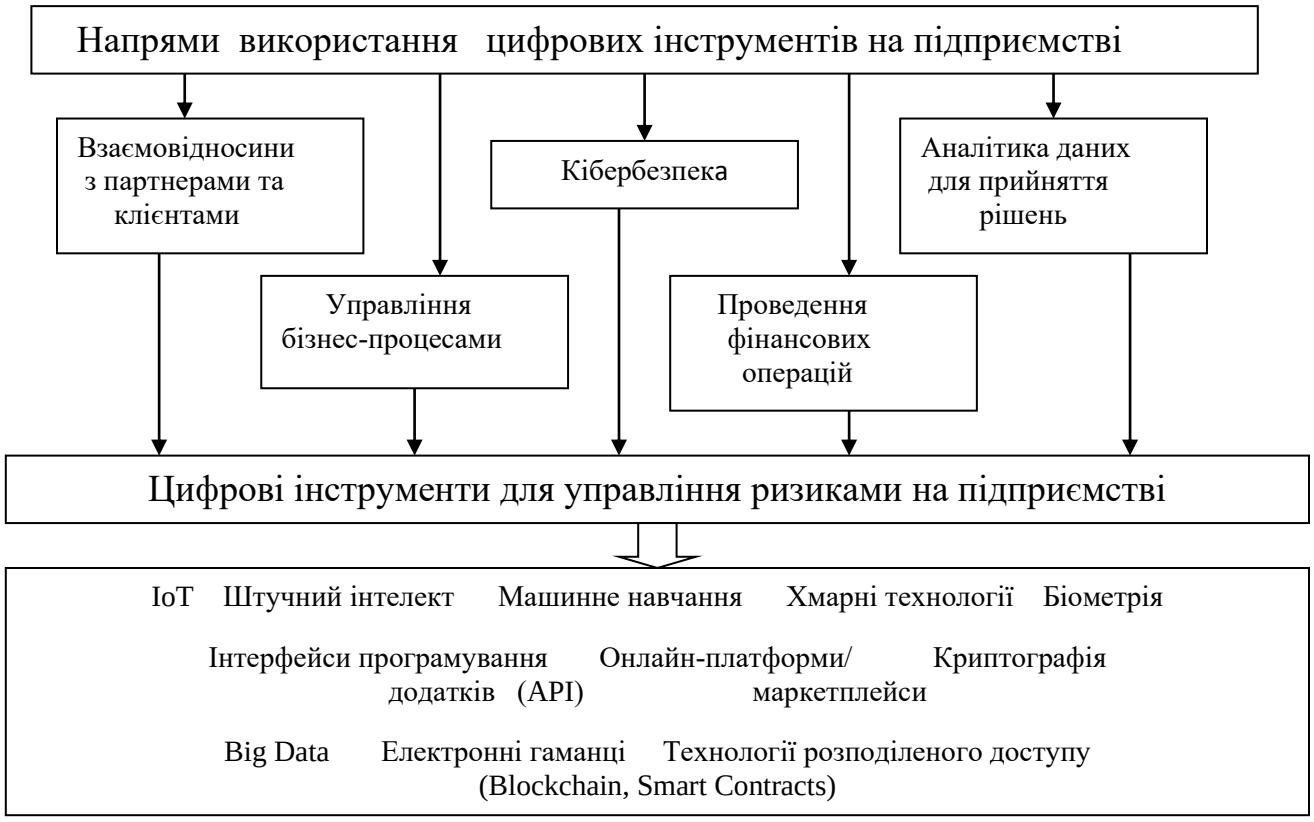


Рисунок 2 – Цифрові інструменти для управління ризиками на підприємстві

*Джерело: побудовано авторами на основі аналізу [3-7]*

Однією з основних сфер, де цифрові технології відіграють ключову роль, є кібербезпека. Кількість пристроїв, підключених до Інтернету, у всьому світі зростає експоненціально; до кінця 2025 року очікується 75,44 млрд таких пристроїв [3]. Оскільки компанії все більше покладаються на цифрові платформи для своїх операцій, ризик кіберзагроз стає більш відчутним. Цифрова трансформація створює значні переваги для безпеки: наприклад, підключені датчики (IoT), відеоаналітика та машинне навчання швидше визначають загрози; технології робочого процесу та автоматизація виявляють, досліджують і виправляють рутинні реакції. Удосконалені методи шифрування, безпечні механізми ідентифікації створюють потужний захист від потенційних зломів, захищаючи конфіденційні фінансові дані та інтелектуальну власність.

Цифрові технології також значною мірою впливають на процес прийняття рішень на основі даних та їх аналізу. Завдяки аналізу величезних наборів даних у режимі реального часу компанії можуть отримати цінну інформацію про ринкові тенденції, поведінку споживачів і внутрішні операції. Обґрунтоване прийняття рішень не тільки підвищує ефективність, але й сприяє загальній економічній стійкості компанії [3].

Також цифрові технології змінюють характер комунікацій з партнерами, інвесторами, клієнтами, дозволяючи підтримувати постійний зв’язок та вирішуючи проблеми у реальному часі [4].

Важливого значення цифрові інструменти набувають при здійсненні онлайн-платежів. Цифрові технології зробили революцію у фінансових операціях для бізнесу. Інтеграція захищених онлайн-платіжних систем і спрощених цифрових фінансових процесів не тільки покращує операційну ефективність, але й пом’якшує ризики, пов’язані з традиційними фінансовими методами.  інтеграція цифрових платформ і рішень для електронної комерції покращує фінансові операції компаній [2]. Захищені системи онлайн-платежів і оптимізовані цифрові фінансові процеси не тільки підвищують ефективність роботи, але й пом’якшують ризики, пов’язані з традиційними фінансовими методами. Цей перехід до

цифрових транзакцій підвищує загальну економічну безпеку компаній шляхом мінімізації вразливості у фінансових процесах.

Цифрові технології відіграють значну роль в управлінні бізнес-процесами. Використання системи датчиків забезпечує менеджмент підприємства даними у реальному часі про стан обладнання, параметри зовнішнього середовища. Така інформація створює основу для дистанційного керування обладнанням та корегування параметрів його роботи.

Цифрова трансформація для ризик-менеджменту означатиме низку змін. Насамперед – ширше використання аналітики включаючи нетрадиційні джерела, як-от рейтинги бізнес-оглядів онлайн. Крім того, цифрові технології здатні покращити точність та узгодженість моделей з оцінки ризиків, частково шляхом значного зменшення упереджень [5].

Проте цифровізація ризик-менеджменту має ряд обмежень та викликів. По-перше, застарілі IT-системи та відсутність легкодоступних якісних даних, стали головними проблемами для діджиталізації ризик-менеджменту. По-друге, топ-менеджмент зазвичай консервативний і не згоден занадто ризикувати, а тому відкидає потенційно прибуткові проєкти на ранніх стадіях через їх ризикованість [7].

По-третє, управління ризиками впливає на діяльність всієї компанії, беручи участь у тисячах щоденних рішень. Це вимагає значної співпраці між різними підрозділами, щоб забезпечити цифрове рішення ризику [7].

Цифрове управління ризиками – це термін, що охоплює всі цифрові можливості, які покращують ефективність і ефективність ризиків, особливо автоматизацію процесів, автоматизацію прийняття рішень, а також цифровий моніторинг і раннє попередження. Цей підхід використовує автоматизацію робочого процесу, оптичне розпізнавання символів, розширену аналітику (включаючи машинне навчання та штучний інтелект) і нові джерела даних, а також застосування робототехніки до процесів та інтерфейсів. По суті, цифровий ризик-менеджмент передбачає узгоджене коригування процесів, даних, аналітики та IT, а також загальної організаційної структури, включаючи таланти та культуру.

Таким чином, впровадження цифрових технологій є обов'язковим для компаній, які прагнуть зміцнити свою економічну безпеку. Від зміцнення заходів кібербезпеки до прийняття рішень на основі даних і оптимізації фінансових транзакцій, трансформаційний вплив цифрових інструментів незаперечний. Застосування цих досягнень дає компаніям змогу легко та адаптивно долати складні умови сучасного бізнес-середовища.

**Перелік джерел посилання**


1. An Overview of Digital Risk URL: https://tezo.com/blog/digital-risk-management-the-comprehensive-5-step-guide/.

2. European Union Agency for Cyber Security (ENISA) ENISA Threat Landscape 2022 (October 2022) URL: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022 (дата звернення: 14.11.2023).

3. Оніщенко О.І. Банківська діяльність в умовах розвитку цифрової економіки. *Вісник ОНУ ім. Мечнікова*. 2018. Т. 23. Вип. № 8(73). С. 160-165.

4. McKinsey&Company The future of risk management in the digital era. 2017. December, 15. URL: https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/the-future-of-risk-management-in-the-digital-era.

5. Ganguly S.,Harreis H., Margolis B., Rowshankish K. Digital risk: Transforming risk management for the 2020s. McKinsey&Company. February, 2019. URL: https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/digital-risk-transforming-risk-management-for-the-2020s#/.

6. Shevchenko N., Chick T.A., O'Riordan P., Scanlon T.P., Woody C Threat modeling: a summary of available methods/ Carnegie Mellon University, Software Engineering Institute/ URL: https://insights.sei.cmu.edu/library/threat-modeling-a-summary-of-available-methods/.

7. Qi, Y., Sun, Y., Zhang, Z. et al. The digital economy – technologies, trends, and influences. *Personal and Ubiquitous Computing* . 2023. №27. 1521-1523. URL: https://doi.org/10.1007/s00779-023-01734-z.