

Managing the economic security of an enterprise using artificial intelligence technologies

Denys Magdysyuk

Lesya Ukrainka Volyn National University, Lutsk

<https://orcid.org/0009-0003-5249-0021>

Abstract. This article examines the possibilities of using artificial intelligence (AI) technologies to improve the economic security of enterprises. Areas of improvement of economic security are identified, including risk analysis, cybersecurity monitoring, and business process optimization. Practical examples and challenges that arise during the integration of AI are described, and recommendations are provided to improve the effectiveness of the use of AI in the field of economic security.

Keywords: business, management, artificial intelligence, economic security, business process, enterprise.

Управління економічною безпекою підприємства за допомогою технологій штучного інтелекту

Денис Магдисюк

Волинський національний університет імені Лесі Українки, м. Луцьк

<https://orcid.org/0009-0003-5249-0021>

Анотація. У цій статті розглядаються можливості застосування технологій штучного інтелекту (ШІ) для підвищення економічної безпеки підприємств. Визначено напрями вдосконалення економічної безпеки, серед яких аналіз ризиків, моніторинг кібербезпеки та оптимізація бізнес-процесів. Описано практичні приклади та виклики, які виникають під час інтеграції ШІ, а також наведено рекомендації для покращення ефективності використання ШІ у сфері економічної безпеки.

Ключові слова: бізнес, управління, штучний інтелект, економічна безпека, бізнес-процес, підприємство.

Зростання економічних та кіберризиків створює значні виклики для підприємств, особливо в умовах глобалізації. Сучасний бізнес обробляє величезні обсяги даних, що збільшує ризик фінансових втрат, втрати інформаційної безпеки та пошкодження репутації компаній. Сучасні інструменти для забезпечення економічної безпеки можуть включати елементи штучного інтелекту, які здатні виявляти загрози, прогнозувати ризики та оптимізувати процеси. ШІ надає можливості для автоматизації та підвищення швидкості реагування на загрози, забезпечуючи конкурентні переваги та знижуючи загальні ризики.

Економічна безпека – це здатність підприємства протидіяти економічним загрозам, захищати свої активи та забезпечувати стабільність діяльності [5]. Основні аспекти економічної безпеки включають:

1. Фінансова стабільність – підтримка ліквідності, зниження ризиків, пов'язаних з боргами, та мінімізація можливості фінансових втрат.

2. Інформаційна безпека – захист конфіденційної інформації, комерційних секретів та захист від кіберзагроз.

3. Ризик-менеджмент – ідентифікація, оцінка та управління ризиками, що можуть зашкодити діяльності підприємства.

Технології штучного інтелекту значно розширюють можливості підприємств у сфері економічної безпеки, дозволяючи ефективніше обробляти великі обсяги даних, прогнозувати ризики та автоматизувати рутинні завдання. ШІ аналізує дані з різних джерел, виявляючи потенційні загрози завдяки розпізнаванню аномалій [3]. На основі алгоритмів машинного навчання можливе побудування точних прогнозів щодо ризиків, таких як кіберзлочинність, шахрайство або банкрутство. Крім того, автоматизація зменшує кількість людських помилок, підвищує точність процесів і знижує витрати на управління безпекою [7].

Використання алгоритмів ШІ для обробки великих обсягів даних дозволяє виявляти фінансові ризики, а також оцінювати ймовірність банкрутства та шахрайства. Наприклад, компанія Kavout використовує машинне навчання для аналізу великих наборів неструктурованих даних з метою побудови моделей ризику в режимі реального часу [8].

ШІ дозволяє автоматизувати моніторинг інформаційних систем, зокрема виявлення аномальної активності у мережі, яка може свідчити про можливі загрози. Наприклад, поєднання ШІ з технологіями блокчейну забезпечує безпеку та незмінність даних у фінансових транзакціях [1].

ШІ може аналізувати історичні дані, будувати прогнози та підтримувати керівників у прийнятті рішень. Дослідження McKinsey вказує, що впровадження ШІ здатне значно підвищити ефективність управлінських рішень та забезпечити більш точне прогнозування ризиків [10].

Розглянемо практичні приклади та кейси застосування технологій ШІ компаніями.

IBM Watson пропонує інструменти на базі ШІ для аналізу великих обсягів даних. Ця система надає компаніям можливість виявляти ризики та прогнозувати загрози, допомагаючи у забезпеченні економічної безпеки [4].

JPMorgan Chase, використовуючи систему COiN, JPMorgan Chase автоматизує обробку юридичних документів, що знижує ризик помилок та пришвидшує процеси, зменшуючи ризики, пов'язані з договірними зобов'язаннями [5].

Банк HSBC використовує технології ШІ для моніторингу транзакцій та виявлення шахрайства, що дозволяє підвищити рівень безпеки фінансових операцій і захистити клієнтів [6].

Щодо напрямів удосконалення управління економічною безпекою виділяють такі основні:

- Підприємства можуть адаптувати алгоритми ШІ до специфіки своєї діяльності, що дозволяє знижувати кількість помилкових спрацювань і підвищувати ефективність захисту. Наприклад, банки можуть використовувати ШІ для оцінки фінансових ризиків, а виробничі компанії – для захисту від шахрайства [7].

- Ефективність ІІІ залежить від якості даних, тому підприємства мають запровадити системи для обробки та очищення даних, що дозволить підвищити точність прогнозів і знизити ризики [8].

- Поєднання ІІІ з блокчейном дозволяє забезпечити прозорість та незмінність транзакцій, що особливо важливо для захисту від шахрайства у фінансових операціях.

- ІІІ-системи можуть бути розроблені таким чином, щоб автоматично адаптуватися до нових загроз. Це особливо актуально в умовах постійно змінюваних ризиків, оскільки такі адаптивні системи забезпечують більш гнучкий підхід до управління економічною безпекою [2]. Наприклад, моделі машинного навчання, які оновлюються на основі нових даних, можуть допомогти підприємствам своєчасно реагувати на зміну ризиків та нові типи загроз [10].

Важливим аспектом є також аналіз викликів та ризиків впровадження технологій штучного інтелекту.

Одним із основних викликів у впровадженні ІІІ є захист конфіденційності даних і дотримання етичних стандартів. Зокрема, ІІІ-системи повинні обробляти персональні дані відповідно до вимог захисту конфіденційності, наприклад, регламенту GDPR у ЄС. Використання штучного інтелекту має бути не лише законним, але й етичним, щоб уникнути потенційних ризиків, пов'язаних із зловживанням даними або їх витоком [10].

Ефективність алгоритмів ІІІ значно залежить від якості наданих даних. Неякісні або застарілі дані можуть призвести до хибних висновків, що, у свою чергу, може негативно позначитися на економічній безпеці. Компанії повинні приділяти увагу збору, оновленню та очищенню даних, щоб забезпечити максимальну точність та ефективність рішень, які приймаються за допомогою ІІІ [9].

Впровадження ІІІ в управління економічною безпекою потребує значних інвестицій у технічні ресурси та навчання персоналу, що може обмежувати доступ до цих технологій для малих і середніх підприємств. Високі витрати на впровадження та обслуговування ІІІ-систем можуть бути серйозною перешкодою для багатьох компаній, що потребує розробки спеціальних програм підтримки та державних ініціатив для сприяння цифровій трансформації бізнесу [10].

Подальші дослідження можуть зосередитись на таких аспектах:

1. Створення менш витратних технологій, які дозволять малим і середнім підприємствам використовувати ІІІ для економічної безпеки.

2. Розробка правових рамок та етичних принципів використання ІІІ для захисту даних.

3. Вдосконалення методів обробки, оновлення та очищення даних для забезпечення точності алгоритмів ІІІ.

Таким чином, ІІІ є перспективною технологією для підвищення економічної безпеки підприємств, особливо у сфері управління ризиками та забезпечення кібербезпеки. Подальший розвиток цих технологій сприятиме більшій стійкості бізнесу та покращенню його конкурентоспроможності.

Штучний інтелект стає важливим інструментом для забезпечення економічної безпеки підприємств завдяки своїй здатності аналізувати великі обсяги даних, автоматизувати процеси та виявляти загрози на ранніх стадіях. У статті було розглянуто декілька ключових напрямів використання ШІ для підвищення рівня економічної безпеки, включаючи аналіз ризиків, моніторинг кібербезпеки та оптимізацію процесів.

Використання ШІ в економічній безпеці допомагає підприємствам швидше реагувати на зміни ринкових умов та покращує ефективність управлінських рішень. Однак впровадження ШІ має свої виклики, такі як залежність від якості даних, високі фінансові витрати та етичні аспекти.

Список використаних джерел

1. Вергал К. Ю. Теоретичні підходи до класифікації інноваційних стратегій. *Теоретичні і практичні аспекти економіки та інтелектуальної власності*. 2011. Вип. 2. С. 214–219.
2. Волощук Ю. Р., Іванишин О. В., Богачик С. В. Формування та реалізація стратегії інноваційного розвитку підприємства. *Держава та регіони. Серія "Економіка та підприємництво"*. 2020. № 2 (113). С. 101–106.
3. Глуха Г. Я., Цимбалюк А. І. Сучасний підхід до побудови інноваційної стратегії на підприємстві. *Академічний огляд*. 2018. № 2 (49). С. 62–74.
4. Золевська М. І. Розроблення інноваційної стратегії підприємства. *Вчені записки Таврійського національного університету імені В. І. Вернадського. Серія "Економіка і управління"*. 2018. Т. 29 (68). № 6. С. 59–62.
5. Коваль А. А. Концептуальні підходи до формування стратегії управління інноваційною діяльністю підприємства. *Вісник Київського національного університету технологій та дизайну*. 2011. № 3. С. 134–138.
6. Ковтун О. І. Інноваційні стратегії для вітчизняних підприємств: принципи та методи генерації та вибору альтернатив. *Економіка та держава*. 2013. № 3. С. 27–31.
7. Кузьомко В. М. Можливості використання штучного інтелекту в діяльності сучасних підприємств. *Економіка та суспільство*. №32, 2021. DOI: <https://doi.org/10.32782/2524-0072/2021-32-67>.
8. Могилевська О. Ю., Слободяник А. М., Сідак І. В. Вплив штучного інтелекту на українську і міжнародну економіку. *Київський економічний науковий журнал*, № 1, 2023. С. 45-52.
9. Панухник О. Штучний інтелект в освітньому процесі та наукових дослідженнях здобувачів вищої освіти: відповідальні межі вмісту ШІ. *Галицький економічний вісник*, № 4 (83) 2023 URL: https://doi.org/10.33108/galicianvisnyk_tntu2023.04.
10. Lee M., Scheepers H., Lui A., Ngai E. The implementation of artificial intelligence in organizations: A systematic literature review. *Information & Management*. Volume 60, Issue 5, July 2023.