

ШТУЧНИЙ ІНТЕЛЕКТ У СИСТЕМІ ПРЕВЕНТИВНОГО УПРАВЛІННЯ ЕКОНОМІЧНОЮ БЕЗПЕКОЮ ПІДПРИЄМСТВА

У сучасних умовах цифрової трансформації економіки та зростання складності зовнішнього середовища забезпечення економічної безпеки підприємства потребує переходу від реактивних до превентивних моделей управління. Як зазначають Й. Шнайдер та співавтори, ефективне AI-управління на рівні підприємств передбачає інтеграцію даних, моделей та систем управління ризиками в архітектуру корпоративного контролю [1]. Це створює основу для формування інтелектуальних систем раннього попередження загроз.

У наукових працях Ю. Бенджіо, Г. Хінтона та колег підкреслюється, що сучасні системи штучного інтелекту (ШІ), з одного боку, значно підвищують ефективність прийняття рішень, а з іншого – формують нові класи ризиків, пов'язаних із автономністю алгоритмів і складністю їх контролю [2]. Це є особливо важливим для економічної безпеки підприємств, де помилки прогнозування можуть мати критичні фінансові наслідки.

Дослідники М. Шмітт та ін. наголошують, що застосування технологій машинного навчання виявляється ефективним у задачах кіберзахисту, виявлення аномалій та захисту цифрових інфраструктур, що безпосередньо пов'язано з економічною безпекою підприємств [3]. Таким чином, ШІ виступає не лише інструментом аналізу, але й активним елементом системи безпеки.

У роботах українських науковців, зокрема О. Халіної та В. Шмагала, доведено, що впровадження технологій ШІ суттєво впливає на підвищення ефективності систем управління економічною безпекою підприємств через покращення якості аналітики ризиків і прогнозування загроз [4]. При цьому підкреслюється необхідність адаптації управлінських механізмів до цифрового середовища.

Водночас О. Скіцько та інші дослідники звертають увагу на зростання ризиків використання ШІ, зокрема кіберзагроз, маніпуляцій даними та правових невизначеностей, що потребує формування комплексних систем управління ризиками на основі штучного інтелекту [5].

Таким чином, у науковій літературі формується консенсус щодо подвійної ролі ШІ: як інструменту підвищення ефективності превентивного управління економічною безпекою та водночас як джерела нових ризиків, що потребують окремого управлінського контролю.

ШІ у системі превентивного управління економічною безпекою підприємства виконує низку ключових функцій. По-перше, це моніторинг та аналіз великих масивів даних у режимі реального часу, що забезпечує оперативне виявлення аномалій у фінансово-господарській діяльності. По-друге, прогнозування ризиків на основі історичних даних і поведінкових моделей, що дає змогу завчасно реагувати на потенційні загрози. По-третє, автоматизація процесів прийняття управлінських рішень, що зменшує вплив людського фактору та підвищує точність оцінок. Застосування технологій ШІ в системі економічної безпеки підприємства охоплює широкий спектр функціональних напрямів, що забезпечують як превентивне виявлення загроз, так і підвищення ефективності управлінських рішень.

Фінансовий моніторинг і виявлення аномалій. ШІ активно використовується для аналізу фінансових потоків підприємства з метою виявлення нетипових операцій, шахрайських схем та помилок у бухгалтерському обліку. Алгоритми машинного навчання

здатні ідентифікувати приховані закономірності у великих масивах фінансових даних, що дозволяє оперативно реагувати на фінансові ризики.

Прогнозування фінансових та операційних ризиків. На основі історичних даних та зовнішніх факторів (ринкові коливання, інфляція, політичні ризики) системи ШІ формують прогнози щодо ймовірності виникнення кризових ситуацій. Це дозволяє підприємству завчасно розробляти сценарії реагування та адаптаційні стратегії.

Кібербезпека та захист інформаційних систем. Одним із ключових напрямів є застосування ШІ для виявлення кібератак, шкідливого програмного забезпечення та несанкціонованого доступу до корпоративних даних. Інтелектуальні системи безпеки аналізують поведінку користувачів у реальному часі та блокують підозрілі дії.

Аналіз контрагентів і управління діловими ризиками. ШІ використовується для оцінки надійності партнерів, постачальників і клієнтів. Системи аналізують фінансову звітність, репутаційні дані, судові реєстри та інші відкриті джерела для формування комплексного профілю ризику контрагента.

Управління комплаєнс-ризиками. Інтелектуальні системи допомагають контролювати дотримання законодавчих вимог, внутрішніх політик та міжнародних стандартів. Це особливо важливо для підприємств, що працюють у регульованих галузях або на міжнародних ринках.

Моніторинг репутаційних ризиків. Завдяки технологіям обробки природної мови (NLP) ШІ аналізує інформаційний простір – соціальні мережі, новини, відгуки клієнтів – з метою виявлення потенційних загроз для ділової репутації підприємства.

Оптимізація управлінських рішень. ШІ підтримує керівництво підприємства у прийнятті рішень шляхом моделювання різних сценаріїв розвитку подій. Це дозволяє оцінити наслідки управлінських дій до їх реалізації та мінімізувати ризики.

Виявлення внутрішніх загроз (інсайдерських ризиків). Системи аналізують поведінку працівників, доступ до даних та операційні дії з метою виявлення потенційних внутрішніх порушень або зловживань.

Таким чином, ШІ формує багаторівневу систему підтримки економічної безпеки підприємства, що охоплює фінансову, інформаційну, операційну та репутаційну складові. Його застосування дозволяє перейти від фрагментарного контролю до інтегрованої превентивної системи управління ризиками. Отже, інтеграція технологій ШІ у систему економічної безпеки підприємства дозволяє реалізувати превентивний підхід до управління ризиками, забезпечити раннє виявлення загроз, підвищити адаптивність підприємства до змін зовнішнього середовища.

Список використаних джерел

1. Schneider J., et al. Artificial Intelligence in Enterprise Risk Management: Frameworks and Applications. *arXiv preprint*. 2020. URL: <https://arxiv.org/abs/2011.10672> (дата звернення: 17.04.2026).
2. Bengio Y., Hinton G., et al. The role of artificial intelligence in decision-making systems and associated risks. *arXiv preprint*. 2023. URL: <https://arxiv.org/abs/2310.17688> (дата звернення: 17.04.2026).
3. Schmitt M., et al. Machine Learning for Cybersecurity: Applications and Challenges. *arXiv preprint*. 2024. URL: <https://arxiv.org/abs/2401.01342> (дата звернення: 17.04.2026).
4. Халіна О., Шмагало В. Використання технологій штучного інтелекту в системі управління економічною безпекою підприємства. *Економіка та суспільство*. 2023. № 49. URL: <https://economyandsociety.in.ua/index.php/journal/article/view/3938> (дата звернення: 17.04.2026).

5. Скіцько О. Системи штучного інтелекту в кібербезпеці та управлінні ризиками підприємств. *Cybersecurity: Education, Science, Technique*. 2022. № 3. URL: <https://csecurity.kubg.edu.ua/index.php/journal/article/view/520> (дата звернення: 17.04.2026).

Науковий керівник: Петренко Л.М., к.е.н., доцент