Міністерство освіти і науки України

Національний університет
«Полтавська політехніка імені Юрія Кондратюка»

Навчально-науковий інститут фінансів, економіки,
управління та права
Кафедра фінансів, банківського бізнесу та оподаткування

ЕКОНОМІЧНА БЕЗПЕКА: ДЕРЖАВА, РЕГІОН, ПІДПРИЄМСТВО

Матеріали X Міжнародної
науково-практичної конференції

13 травня 2026 р.

Полтава
2026

УДК 657.658

Добровольська Анастасія Артемівна,
студентка
Науковий керівник: Коба Олена Вікторівна,
кандидат технічних наук, доцент
Національний університет «Полтавська політехніка імені Юрія Кондратюка»

ВПЛИВ ШТУЧНОГО ІНТЕЛЕКТУ НА ЕКОНОМІЧНУ БЕЗПЕКУ ПІДПРИЄМСТВ: МОЖЛИВОСТІ ТА ЗАГРОЗИ

Цифрова трансформація глобальної економіки висуває принципово нові вимоги до економічної безпеки суб'єктів господарювання. Традиційних методів моніторингу для запобігання кіберзагрозам стає недостатньо. Впровадження технологій штучного інтелекту дозволяє перейти виправлення наслідків до управління ризиками (прогнозування та запобігання). Штучний інтелект виступає інструментом, який, з одного боку, створює безпрецедентні можливості для захисту активів, а з іншого – генерує специфічні деструктивні виклики, що потребують нових підходів до менеджменту.

Алгоритми машинного навчання здатні опрацьовувати об’ємні масиви даних, здійснювати моніторинг операцій у режимі реального часу дозволяють миттєво виявляти аномалії, що можуть свідчити про корпоративне шахрайство, внутрішні зловживання або несанкціонований витік конфіденційної інформації [1]. Предиктивні моделі дозволяють моделювати стрес-сценарії та оптимізувати стратегії протидії загрозам ще до їх прояву.

Використання технологій Big Data у поєднанні з нейронними мережами забезпечує глибинний аналіз ділової репутації, зв'язків та фінансового стану партнерів, мінімізуючи ризики співпраці з фіктивними компаніями.

Водночас, цифровізація супроводжується зростанням ризиків економічній безпеці. По-перше, зловмисники використовують штучний інтелект для створення адаптивного шкідливого програмного забезпечення та автоматизованого пошуку слабких місць у корпоративних мережах. Крім того, через неможливість простежити логіку нейронної мережі менеджмент може отримувати викривлені рекомендації щодо інвестицій або оцінки кредитоспроможності, що загрожує стратегічними помилками в управлінні фінансами.

Додатковим ризиком є технологічна залежність від сторонніх розробників. Використання хмарних моделей створює загрозу розголошення комерційної таємниці, оскільки дані підприємства можуть потрапляти у відкриті вибірки для навчання глобальних алгоритмів. Автоматизація управлінських функцій часто викликає опір персоналу, що провокує конфлікти та знижує лояльність, створюючи внутрішні загрози кадровій безпеці підприємства.

Підсумовуючи, можна стверджувати, що вплив штучного інтелекту на економічну безпеку має як позитивні, так і негативні наслідки. Для мінімізації загроз підприємствам необхідно впроваджувати інтелектуальні системи захисту, які постійно тестуватимуть периметр безпеки на стійкість до інтелектуальних атак.

Література

1. Таранич А. В., Пелехацький Д. О. Використання штучного інтелекту в процесах стратегічного управління підприємствами. *Економіка України.* 2024. Том 67. № 1 (746), С. 54–65.