УДК 338.24:004.8:004.65:005.52
Череп А. В.[1], Воронкова В. Г.[2], Череп О. Г.[3]
[1] д-р екон. наук, проф., завідувач кафедри фінансів, банківської справи та страхування, Запорізький національний університет, м. Запоріжжя, Україна.
[2] д-р філос. наук, проф., завідувач кафедри управління та адміністрування, Інженерний навчально-науковий інститут ім. Ю.М. Потебні Запорізького національного університету, м. Запоріжжя Україна.
[3] д-р екон. наук, проф., професор кафедри управління персоналом і маркетингу, Запорізький національний університет, м. Запоріжжя, Україна.

ІНТЕЛЕКТУАЛІЗАЦІЯ МОНІТОРИНГУ ЕКОНОМІЧНОЇ БЕЗПЕКИ ПІДПРИЄМСТВ НА ОСНОВІ AI-АНАЛІТИКИ ТА BIG DATA

Інтелектуалізація моніторингу економічної безпеки підприємств на основі аналізу з використанням штучного інтелекту (ІІ) та технологій великих даних є ключовою тенденцією у сучасному управлінні підприємствами та запобіганні ризикам. Ця модель перетворює традиційну «перевірку після події» на «раннє попередження до події» та «контроль під час події» за допомогою збору всебічних даних у режимі реального часу та поглибленого аналізу. І. Основні компоненти та технології інтелектуального моніторингу: 1) Багатомірний збір даних (великі дані, націлений на інтеграцію внутрішніх структурованих даних (фінансові дані, дані про продаж) із зовнішніми неструктурованими даними (новини та громадська думка, соціальні мережі, інформацію про ланцюжок поставок) для забезпечення комплексного моніторингу. 2) Аналітика на основі ШІ та машинного навчання, в основі якої використання алгоритмів комп'ютерного зору, обробки природної мови (NLP) та виявлення аномалій для автоматичного виявлення потенційних ризиків у величезних масивах даних. 3) Прогностичне моделювання, що включає використання історичних даних для навчання моделей прогнозування потенційних ризиків, таких як фінансові кризи, судові суперечки чи коливання ринку, а також надання інтелектуальної підтримки прийняття рішень. У хвилі цифровізації технології штучного інтелекту проникли на всі рівні бізнес-операцій, від обслуговування клієнтів та оцінки ризиків до виробництва та підтримки прийняття рішень. Однак це також означає, що якщо системи ШІ зазнають атак або виявляються вразливості, це серйозно вплине на підприємства. Згідно з звітом PwC «Global Digital Trust Insights 2026», понад 36% підприємств назвали ШІ одним із трьох головних пріоритетів інвестицій у кібербезпеку, за яким йдуть хмарна безпека (34%) та кібербезпека (28%) [1]. Ще тривожніше те, що лише 6% підприємств упевнені у своїй здатності протистояти всім типам кібератак, що вказує на те, що стійкість кібербезпеки все ще перебуває в стадії формування, а ШІ стає новою зброєю для хакерів, перетворюючи давні вразливості захисту на фатальні прогалини. Особливо в

умовах більш складних технологічних екосистем та взаємопов'язаних ланцюжків поставок традиційні засоби захисту від кіберзагроз багатьох підприємств виявляються неефективними. В даний час до основних загроз безпеки систем ШІ відносяться ворожі атаки, отруєння даних, крадіжка моделей та порушення конфіденційності. Зловмисники можуть дурити моделі ШІ за допомогою ретельно підібраних вхідних даних, що призводить до невірних висновків; вони можуть впроваджувати шкідливі дані на етапі навчання, змушуючи модель демонструвати несподіване поведінка. Згідно з дослідницьким звітом PwC "Відповідальний ШІ: від теорії до практики", до 52% підприємств стикалися з інцидентами безпеки, пов'язаними з системами ЩІ, при цьому найбільш поширеними типами атак є витікання даних та зловмисне маніпулювання моделями. Зі зростанням поширеності генеративного ШІ зростає кількість випадків використання технології дипфейків для шахрайства та поширення дезінформації. У звіті також показано, що понад 70% підприємств стурбовані тим, що генеративний ШІ може бути використаний для атак із застосуванням соціальної інженерії проти організацій, що становить серйозну загрозу корпоративній репутації та громадській довірі. Ефективні рішення на основі ШІ вимагають механізмів управління та безпеки на рівні підприємства для забезпечення використання даних у правильному контексті. Примітно, що у звіті PwC «Глобальні дослідження цифрової довіри за 2026 рік» було встановлено, що лише половина підприємств повністю запровадила політики класифікації даних (50%) та розгорнула механізми захисту від витоків даних у ключових точках виходу (48%). Крім того, лише 6% підприємств вказали, що впровадили комплексні заходи управління ризиками, пов'язаними з даними, по всій компанії, що демонструє, що на ринку в цілому ще є значний потенціал для покращення контролю ризиків, пов'язаних із даними для додатків ШІ. Підприємствам необхідно розуміти, що безпека ШІ - це комплексний підхід, що включає організаційні процеси, поінформованість персоналу та структуру управління. Створення багаторівневого механізму захисту та впровадження заходів безпеки протягом усього життєвого циклу, від збору даних та навчання моделей до розгортання та обслуговування, стало першочерговим завданням. Сценарії застосування інтелектуального моніторингу для забезпечення економічної безпеки підприємств; 1) Фінансовий та нормативний моніторин, що може автоматично виявляти аномальні транзакції, фальсифіковану бухгалтерську звітність та податкові ризики, запобігаючи відмиванню грошей та шахрайству. 2) Ризики в ланцюжку постачання та операційні ризики, в основі яких моніторинг у режимі реального часу та реагування на збої в ланцюжку постачання. 3) Мережа та інформаційна безпека, завдяки якій технології уніфікованого поведінкового аналізу (UEBA) можуть у режимі реального часу виявляти аномальні дії

внутрішнього персоналу або зовнішні мережеві атаки, забезпечуючи захист комерційної таємниці та конфіденційності даних. 4) Ризики, пов'язані з громадською думкою та репутацією, у зв’язку з чим слід : використовувати технології обробки природної мови для моніторингу громадської думки в інтернеті та завчасного попередження до того, як вибухне репутаційна криза. Ключові переваги інтелектуального моніторингу: 1) Моніторинг у режимі реального часу та проактивний підхід, що включає технології штучного інтелекту та сприяють перетворенню моніторингу з постфактумного на миттєвий і навіть дозволяє здійснювати профілактичне управління. 2) Підвищена точність порівняно з ручним аналізом, націлена на те, що ШІ може точно виявляти аномалії у складних та масштабних масивах даних, знижуючи частоту помилкових спрацьовувань. 3) Зниження витрат та людських помилок, націлена на те, що автоматизовані процеси зменшують залежність від ручної перевірки, значно підвищуючи ефективність та безпеку роботи. 4) Конфіденційність та управління даними, в основі якої необхідно знайти баланс між обміном даними, дотриманням нормативних вимог та безпекою. 5) Надійність моделі, так як атаки з боку зловмисників можуть призвести до того, що системи ШІ прийматимуть невірні рішення, тому необхідно посилити захист моделі від загроз. 6) Безперервне навчання та оптимізація, яка відбувається у міру зміни форми ризику моделі моніторингу необхідно постійно навчати з використанням нових даних. Ця інтелектуальна система допоможе підприємствам створити комплексну мережу захисту, що включає в себе «безпеку моделі, безпеку даних та безпеку роботи системи. Інтелектуальний моніторинг економічної безпеки підприємства на основі аналізу з використанням штучного інтелекту та технологій обробки великих даних. самонавчання дозволяє підприємствам використовувати великі дані, машинне навчання та когнітивні обчислення для досягнення комплексного та оперативного управління економічними ризиками. Моніторинг фінансів та ризиків у режимі реального часу за допомогою ШІ (починаючи з 2026 року). Інтелектуальна система раннього попередження цілодобово відстежуватиме ризики, пов'язані з ланцюжком поставок, грошовими потоками, ринковими коливаннями та дотриманням законодавства. Вона може автоматично виявляти аномальні транзакції чи фінансове шахрайство, скорочуючи час виявлення ризиків із «місяців» до «днів» чи навіть «реального часу». Прогностична аналітика включає використання аналізу історичних даних та великих обсягів інформації для прогнозування потенційних економічних криз (таких як неплатежі постачальників та збої у грошових потоках) та надання рекомендацій щодо реагування до того, як ризики матеріалізуються. Інтелектуальна власність та безпека сприяє тому, що підприємства все частіше покладаються на ШІ для моніторингу мережевих ресурсів, захисту корпоративної конфіденційності та комерційної таємниці, а також

запобігання витоку даних. Розробники корпоративних додатків можуть використовувати інструменти з низьким або нульовим рівнем кодування у поєднанні з генеративним штучним інтелектом для швидкого створення персоналізованих програм для моніторингу безпеки. Після 2026 року корпоративна безпека буде зосереджена не тільки на запобіганні атакам, а й на підвищенні «стійкості бізнесу». Системи моніторингу будуть тісно інтегровані з операційними процесами підприємства, такими як управління ланцюжками постачання та фінансовий облік [2]. Ключові пріоритети розвитку на 2026-2030 роки: 1) Ініціатива «Штучний інтелект+», у контексті якої підприємства повною мірою впроваджуватимуть ініціативу «Штучний інтелект+», використовуючи ШІ для оптимізації бізнес-процесів, підвищення продуктивності та перетворення технологій ІІ на ключову конкурентну перевагу. 2) Конфіденційність даних та відповідність нормативним вимогам, у контексті яких у міру посилення правил захисту даних системи моніторингу ШІ повинні забезпечувати відповідність транскордонним правилам передачі даних та правилам конфіденційності (наприклад, стандартам оцінки безпеки ШІ в Європі). 3) Прийняття обґрунтованих інвестиційних рішень, приділяючи особливу увагу проектам інтелектуального моніторингу, здатним забезпечити гарантовану окупність інвестицій (ROI). У період з 2026 по 2030 рік моніторинг економічної безпеки підприємств перейде від пасивного аналізу звітів до проактивного інтелектуального прийняття рішень. Підприємствам необхідно розглядати дані як актив та повною мірою використовувати інтелектуальні інструменти для забезпечення безпеки та сталого розвитку у складному глобальному економічному середовищі. Інтелектуалізація моніторингу економічної безпеки підприємств на основі AI-аналітики та Big Data забезпечує проактивне виявлення ризиків, підвищення адаптивності управлінських рішень і стійкість бізнесу в умовах невизначеності.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Череп А.В., Воронкова В.Г., Череп О.Г. Синергетична аналітика штучного інтелекту та Big Data для виявлення ризиків у системі економічної безпеки держави. Цифрова економіка та економічна безпека. 2026. Випуск 2(23). DOI: https://doi.org/10.32782/dees.23-3

2. Череп А.В., Воронкова В.Г., Череп О.Г. Синергія 5G та штучного інтелекту як драйвер розвитку smart-економіки нового покоління. Science and Practice: Synergy of Innovations in Multidisciplinary Dimensions : Proceedings of the 2st International Scientific and Professional Conference (Held in San Francisco, USA | April 2–4, 2026) / Compiled by: V. Shpak, Chairman of the Editorial Board: S. Tabachnikov. Sherman Oaks, CA: GS Publishing Services, 2026. С.81-90.OI: 10.51587/9798-9935-42805-2026-28