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 IX Міжнародної
науково-практичної конференції

15 травня 2025 р.

Полтава
2025

Applied Innovations in Information and Communication Technology. ICAIIT 2024. Lecture Notes in Networks and Systems, vol 1338. Springer, Cham. https://doi.org/10.1007/978-3-031-89296-7_29

6. Buriak A., Levchenko I. The role of international organizations in the formation of a security-oriented information environment and the implementation of strategies for ensuring the economic and ecological security of Ukraine. Current problems of sustainable development. 2024. No 1. Vol. 1. P. 7–12.

7. Masliy O.A., Buriak A.A. (2023) Transformation of threats for the economic security and security of the infor-mation environment of Ukraine in the conditions of a full-scale war. State and regions. Series: Economics and Business, no. 3(129), pp. 28–32.

УДК 336

Кудінова Аліна Олександрівна,
кандидат економічних наук, доцент
Черевань Кіра Сергіївна,
студентка
Національний університет «Полтавська політехніка імені Юрія Кондратюка»

ВИКОРИСТАННЯ ШІ ПРИ ЗАБЕЗПЕЧЕННІ БЕЗПЕКООРІЄНТОВАНОГО ІНФОРМАЦІЙНОГО СЕРЕДОВИЩА ПІДПРИЄМСТВА[5]

Практика менеджменту показує, що роль штучного інтелекту (ШІ) в безпекових стратегіях підприємства постійно підвищується, оскільки він стає центральним інструментом у створенні динамічних та стійких інформаційних середовищ,

[5] Тези підготовлено в межах виконання НДР молодих учених «Формування безпекоорієнтованого інформаційного середовища для підвищення економічної безпеки України у воєнний та повоєнний періоди», державний реєстраційний номер 0124U000615

орієнтованих на захист від внутрішніх та зовнішніх загроз, забезпечує аналіз великих обсягів даних у реальному часі та виявляє аномальні поведінкові патерни. Для забезпечення інформаційної безпеки підприємства варто застосовувати ШІ у наступних напрямах: впровадження інтелектуальних систем виявлення вторгнень (IDS/IPS) на основі автоматичного розпізнавання підозрілої активності; машинне навчання для прогнозування загроз з подальшим моделюванням ризиків на основі історичних даних; постійний аналіз поведінки користувачів (UEBA) та виявлення відхилень від нормальної активності працівників [1].

Застосування ШІ за такими напрямами дасть змогу покращити безпеку інформаційного середовища, а також забезпечити швидке виявлення та реагування на кіберзагрози, знизити навантаження на людські ресурси завдяки автоматизації рутинних процесів, удосконалити алгоритми у процесі експлуатації (таблиця 1) [2].

Таблиця 1

Використання ШІ при нейтралізації інформаційних загроз

Загроза	ШІ-рішення
Несанкціоновані доступи, спроби зламу мережі	Системи виявлення вторгнень на основі ШІ (AI-IDS)
Нетипова поведінка користувачів або системних процесів	Машинне навчання для аналізу аномалій
Нові, раніше невідомі шкідливі програми (Zero-Day Threats)	Інтелектуальні антивірусні програми
Затримки в реагуванні на кіберінциденти	Роботизовані системи реагування (SOAR-платформи)
Виявлення трендів атак та запобігання складним атакам	ШІ для аналізу великих даних про загрози (Threat Intelligence)
Модифікація або крадіжка критичних даних	Блокчейн-системи з елементами ШІ
Швидка генерація відповідей на інциденти та автоматизація документування	Генеративні моделі для кіберзахисту (наприклад, ChatGPT-подібні рішення для SOC)

Отже, перспективними напрямами використання ШІ у сфері інформаційної безпеки є розвиток автономних безпекових агентів, глибше впровадження нейронних мереж у системи кіберзахисту та формування глобальних платформ співпраці для обміну інформацією про загрози у режимі реального часу, що у подальшому дозволить забезпечити безпекоорієнтоване інформаційне середовище підприємства.

Література

1. IBM Security. (2022). How AI is transforming cybersecurity. IBM Official Website
2. Gartner Research. (2023). AI in Cybersecurity: Key Trends and Recommendations. Gartner Reports
3. Маслій О.А., Котелевець М.М. Безпекоорієнтований підхід до формування інформаційного середовища як основа економічної безпеки України. Економічна безпека: держава, регіон, підприємство : матеріали VIII Міжнар. наук.-практ. конф., 16 трав. 2024 р. Полтава : Нац. ун-т ім. Юрія Кондратюка, 2024. С. 127–129.
4. Onyshchenko, S., Hlushko, A., Yanko, A. (2020). Role and importance of information security in a pandemic environment. *Economics and Region*, 2 (77), 103–108.
5. Buriak A., Masliy O. (2024). Strategic foundations of security-oriented international space: economic, informational and ecological dimensions. *Економіка і регіон*. 1 (92). 281 – 287. DOI: https://doi.org/10.26906/EiR.2024.1(92).3341.
6. Кудінова А.О., Маслій О.А., Буряк А.А. Формалізація ризиків і загроз економічній безпеці україни в умовах цифровізації. *Управління змінами та інновації*. 2024. №12. С. 25 – 31. DOI: https://doi.org/10.32782/CMI/2024-12-4.
7. Shefer O., Laktionov O., Pents V., Hlushko A., & Kuchuk N. (2024). Practical principles of integrating artificial intelligence into the technology of regional security predicting. *Advanced Information Systems*, 8(1), 86–93.
8. Onyshchenko, V., Yehorycheva, S., Maslii, O., Yurkiv, N. (2020). Impact of Innovation and Digital Technologies on the Financial Security of the State. *Lecture Notes in Civil Engineering*. Volume 181. pp. 749–759.