5. Яновський Д. В., Тищенко В. С. Захист хмарної інфраструктури від кібератак. *Сучасний захист інформації*. 2022. № 2. С. 52-58. URL: https://journals.dut.edu.ua/index.php/dataprotect/article/view/2639/2538.

***Худіков П.В, аспірант***
*Київський національний економічний університет імені Вадима Гетьмана*
*pavelkhudikov77@gmail.com*

## МЕТОДИ ШТУЧНОГО ІНТЕЛЕКТУ МОНІТОРИНГУ ЗАГРОЗ ЕКОНОМІЧНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА

У сучасних умовах, коли глобалізація економіки та цифровізація бізнес-процесів призводять до зростання різноманітних загроз для економічної безпеки підприємств, важливо застосовувати новітні технології для своєчасного виявлення і запобігання цим загрозам. Одним із таких інструментів є штучний інтелект (ШІ), який здатен значно підвищити ефективність моніторингу та управління економічною безпекою підприємства. ШІ дозволяє обробляти великі обсяги даних і виявляти аномалії, що можуть свідчити про потенційні загрози. Використання методів ШІ забезпечує проактивний підхід до управління ризиками і забезпечення економічної стабільності підприємств.

Методи ШІ активно використовуються для автоматизації процесів моніторингу та аналізу економічних загроз. Вони дозволяють оперативно виявляти нетипові зміни в фінансових показниках, порушення в ланцюгах постачання, можливі прояви шахрайства, а також передбачати потенційні загрози.

1. **Машинне навчання (ML)**

Одним із найбільш розповсюджених методів ШІ є машинне навчання, яке дозволяє автоматично виявляти патерни і аномалії на основі великих масивів даних. Алгоритми машинного навчання здатні навчатися на історичних даних і здійснювати прогнозування ризиків у майбутньому. Це дозволяє вчасно виявляти загрози, пов'язані, наприклад, з несанкціонованими фінансовими операціями або маніпуляціями з фінансовими показниками.

2. **Глибинне навчання (Deep Learning)**

В рамках глибинного навчання використовуються нейронні мережі, які можуть аналізувати набагато складніші структури даних, такі як текстові документи, зображення або відео. Завдяки цьому, такі системи можуть виявляти загрози, які неможливо побачити за допомогою традиційних методів аналізу. Наприклад, глибинне навчання застосовується для моніторингу корпоративних комунікацій або виявлення аномалій у поведінці користувачів інформаційних систем.

3. **Обробка природної мови (NLP)**

Штучний інтелект також активно використовується для аналізу текстової інформації, що є важливою частиною моніторингу загроз. Методи обробки природної мови дозволяють аналізувати контракти, угоди, листи та інші документи, виявляючи потенційно небезпечні або підозрілі елементи. Це особливо актуально для виявлення можливих спроб економічного шпіонажу або внутрішнього шахрайства.

4. **Аналіз великих даних (Big Data)**

Одним з основних інструментів ШІ є аналіз великих даних, який дозволяє інтегрувати і обробляти різноманітні типи даних з численних джерел (фінансові транзакції, ланцюги постачання, внутрішні комунікації і т.д.). Використання методів ШІ для обробки великих даних дає змогу не лише виявляти аномалії, але й передбачати розвиток подій, що дозволяє підприємствам адаптувати свою стратегію управління безпекою в реальному часі.

**Переваги використання ШІ для моніторингу загроз**

1. **Автоматизація та зменшення людського фактору**: ШІ дозволяє автоматизувати процеси моніторингу, що значно знижує вплив людських помилок і забезпечує оперативність реагування на загрози.
2. **Прогнозування і превенція**: Завдяки здатності аналізувати великі обсяги історичних і реальних даних, ШІ може передбачити можливі загрози до того, як вони матимуть серйозні наслідки для підприємства.
3. **Підвищена точність**: Алгоритми ШІ дозволяють виявляти навіть найменші аномалії в поведінці фінансових або операційних процесів, що може бути важко виявити вручну.

**Недоліки та обмеження використання ШІ**

1. **Потреба в великих обсягах даних**: Для ефективного навчання моделей ШІ необхідно мати доступ до великих, якісних і структурованих даних. Це може бути проблемою для деяких підприємств, особливо в тих випадках, коли дані не зібрані в одному місці або мають низьку якість.
2. **Висока вартість впровадження**: Встановлення та підтримка ШІ-систем вимагає значних фінансових витрат, а також спеціалізованих знань для їх налаштування та оптимізації.
3. **Складність інтерпретації результатів**: Деякі методи ШІ, такі як глибинне навчання, часто є «чорними ящиками», що означає, що їх результати можуть бути складними для розуміння і інтерпретації. Це може бути проблемою для прийняття управлінських рішень.

**Перспективи розвитку ШІ для моніторингу загроз**

Штучний інтелект продовжує розвиватися, і в майбутньому можна очікувати ще більше інновацій у цій сфері. Підвищення точності алгоритмів, інтеграція з іншими технологіями (наприклад, блокчейн для підвищення прозорості фінансових операцій) і розвиток нових методів аналізу даних сприятимуть ще ефективнішому моніторингу економічних загроз.

Застосування методів ШІ в моніторингу загроз економічної безпеки підприємств відкриває нові можливості для підвищення ефективності та своєчасного виявлення загроз. Хоча існують певні виклики щодо впровадження і оптимізації таких систем, переваги від їх використання значно перевищують потенційні ризики. Важливою є комплексна інтеграція ШІ в систему управління безпекою підприємства, що дозволить підвищити стійкість бізнесу до внутрішніх і зовнішніх загроз.

### *Список використаних джерел*


1. Nadide Beyza Dakur**.** Artificial Intelligence (AI) Applications in Cyber Security, Режим доступу - https://www.researchgate.net/publication/367253331_Artificial_Intelligence_AI_Applications_in_Cyber_Security
2. Myroslava Bosovska, Marharyta Boiko, Liudmila Bovsh, Alla Okhrimenko. Artificial Intelligence in Ensuring the Business Economic Security. Режим доступу - https://www.researchgate.net/publication/377794493_Artificial_Intelligence_in_Ensuring_the_Business_Economic_Security
3. Поляков П.А Роль інформаційного забезпечення в управлінні економічною безпекою підприємств машинобудування. The role of information provision in economic security management of machine-building enterprises/ П.А Поляков / Економіка та управління підприємствами.- Випуск 22. 2018.-С.99-102. — Режим доступу https://chmnu.edu.ua/wp-content/uploads/2019/07/Polyakov-P.-A..pdf.


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