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

УДК 336.71:004.8

Худолій Юлія Сергіївна,
кандидат економічних наук, доцент
Токар Олександр Олександрович,
студент
Національний університет «Полтавська політехніка імені Юрія Кондратюка»

ШТУЧНИЙ ІНТЕЛЕКТ ЯК ІНСТРУМЕНТ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ БАНКІВ УКРАЇНИ

Постійне зростання обсягів даних і збільшення кількості кіберзагроз вимагає нових підходів до їх виявлення та нейтралізації. Традиційні методи кібербезпеки не здатні забезпечити належний рівень захисту банківської системи через їхню обмежену ефективність і необхідність значних ресурсів для аналізу великих обсягів даних. Застосування штучного інтелекту у виявленні кіберзагроз відкриває нові можливості для автоматизації процесів і підвищення ефективності кіберзахисту. ШІ дозволяє автоматично аналізувати великі масиви даних, виявляти аномалії та передбачати потенційні загрози, що значно скорочує час реакції на загрози і знижує ризики для інформаційної безпеки. Інтеграція методів штучного інтелекту в системи кібербезпеки банків України дає змогу забезпечити проактивний підхід до виявлення та нейтралізації загроз [1].

Кількість та інтенсивність кібератак, яка оцінюється European Repository of Cyber Incidents (EuRepoC) за шкалою від 1 до 15 балів, виходячи з фактичних наслідків та соціально-політичної серйозності кіберінциденту, в Україні за період повномасштабної війни досить стрімко зросла, в порівнянні з 2021 роком [2].

Рис. 1. Динаміка кількості та інтентивності кібератак протягом 2021 – 2024 років

Джерело: створено авторами на основі [2].

До основних кіберзагроз, з якими постійно стикаються українські банки варто віднести наступні.

1. Фішингові атаки – надсилання шахраями електронних листів або текстових повідомлень, що маскуються під повідомлення від легітимних організацій, щоб отримати доступ до конфіденційної інформації клієнтів.

2. Malware – зловмисне програмне забезпечення, яке може бути використано для крадіжки даних, пошкодження систем або вимагання викупу, та поширюється через електронну пошту, веб-сайти або заражені USB-накопичувачі.

3. DDoS-атаки – атаки через бот-мережі чи програмні застосунки, що проявляються у відмові в обслуговуванні та можуть призвести до того, що банківські платіжні системи стають недоступними для клієнтів [3].

Штучний інтелект суттєво посилює можливості українських банків у боротьбі з основними кіберзагрозами. Для протидії фішинговим атакам проводиться аналіз величезних обсягів вхідних електронних листів і SMS,

виокремлюючи ті, що містять ознаки фішингу: незвичні посилання, нетипові домени відправника, аномальну структуру повідомлення чи стилістику тексту. Такі системи використовують як класичні ознаки (URL-сканування, перевірка SPF/DKIM), так і поведінкові моделі, навчені на реальних фішингових кампаніях проти українських банків, що дозволяє виявляти навіть «нульові дні» (zero-day phishing) без попередніх сигнатур.

Для боротьби з Malware системи, які побудовані на основі штучного інтелекту, застосовують комбінацію поведінкового та сигнатурного аналізу. Традиційні антивіруси залежать від оновлення бази сигнатур, тоді як штучний інтелект навчається на зразках відомого шкідливого ПЗ і виявляє нові мутації за допомогою евристичних моделей. Наприклад, рішення на основі нейронних мереж відстежують нетипові виклики API, підозрілі спроби шифрування файлів або несанкціоноване встановлення драйверів, миттєво блокуючи процес ще на етапі запуску [4].

Щодо DDoS-атак, рішення штучного інтелекту забезпечують адаптивний захист на рівні мережі та прикладного шару. Платформи на основі поведінкового аналізу постійно моніторять трафік, виділяючи «білий список» легітимних запитів та виявляючи аномальні піки, що характерні для бот-мереж. Завдяки машинному навчанню система автоматично формує фільтри в режимі реального часу, блокуючи зловмисні потоки і перенаправляючи їх через scrubbing-центри без залучення оператора [5].

Підсумовуючи, можемо дійти до висновку, що штучний інтелект суттєво посилює можливості українських банків та має потужний потенціал для зміцнення фінансової стійкості банківської системи шляхом управління ризиками, автоматизації процесів та обслуговування клієнтів. Водночас ефективне впровадження ШІ вимагає значних інвестицій, захисту даних та систематичного контролю [6].

Література

1. Лунгол О.М. Автоматизація виявлення кіберзагроз із застосуванням штучного інтелекту: робота на здобуття кваліфікаційного ступеня магістра: спец. 125 – Кібербезпека та захист інформації / наук. кер. В.В. Муж. Тернопіль: Тернопільський національний технічний університет імені Івана Пулюя, 2024. 91 с.

2. Overview of cyber incidents against Ukraine between 01-01-2021 and 31-12-2024. *European Repository of Cyber Incidents (EuRepoC).* URL: https://surli.cc/rocamt (дата звернення: 16.04.2025)

3. Вовченко О.С. Кібербезпека як сучасний тренд розвитку банківської системи України // Економіка. Фінанси. Бізнес. Управління: матеріали III Міжнар. форуму. – К.: Ліра-К, 2024. – С. 35-37.

4. IBM Security X-Force Research Advisory: New Destructive Malware Used In Cyber Attacks on Ukraine. *IBM - United States.* URL: https://surl.li/wxzmix (дата звернення: 16.04.2025).

5. Ukraine's Response to Cyber Threats a Model in DDoS Prevention. *Radware Captcha Page.* URL: https://surl.li/gahqfk (дата звернення: 16.04.2025).

6. Худолій Ю.С., Приймак А.Ю. Фінансова стійкість банків у контексті інтеграції штучного інтелекту: світовий досвід та українські перспективи // Розвиток фінансового ринку в Україні: загрози, проблеми та перспективи: матеріали VI Міжнар. наук.-практ. конф., м. Полтава, 27 листоп. 2024 р. – Полтава: Нац. ун-т ім. Ю. Кондратюка, 2024. – С. 101–103.

7. Onyshchenko S., Yanko A., Hlushko A., Maslii O., Cherviak A. Cybersecurity and improvement of the information security system. *Journal of the Balkan Tribological Association*. 2023. 29(5). pp. 818–835.