JEL Classification: D83, L29, K12

Ірина ДИМОН
здобувачка вищої освіти першого (бакалаврського) рівня,
спеціальність 075 «Маркетинг»
Національний університет «Львівська політехніка»
Дмитро ДОНЕЦЬ
старший викладач, провідний фахівець кафедри маркетингу і логістики
Інституту економіки і менеджменту
Національний університет «Львівська політехніка»

Iryna DYMON
student of the first (bachelor's) level of higher education,
specialty 075 "Marketing"
Lviv Polytechnic National University
Iryna.Dymon.MK.2025@lpnu.ua
Dmytro DONETS
Senior Lecturer, Leading Specialist, Department of Marketing and Logistics,
Institute of Economics and Management,
Lviv Polytechnic National University
Dmytro.M.Donets@lpnu.ua

РОЛЬ ШТУЧНОГО ІНТЕЛЕКТУ У КІБЕРБЕЗПЕЦІ ПІДПРИЄМСТВ

THE ROLE OF ARTIFICIAL INTELLIGENCE IN ENTERPRISE CYBERSECURITY

Анотація. Досліджено можливості використання ШІ для виявлення та запобігання кібератакам. Визначено основні виклики, пов’язані із впровадженням ШІ, включаючи питання конфіденційності даних та етичні аспекти. Окреслено необхідність комплексного підходу до кіберзахисту, що поєднує технологічні рішення та освітні ініціативи для підвищення рівня безпеки підприємств.
Ключові слова: штучний інтелект, кібербезпека, фішинг, конфіденційность даних, вірус, автоматизація, управління вразливостями.

Abstract. The possibilities of using AI to detect and prevent cyber attacks are investigated. The main challenges associated with the introduction of AI, including data privacy and ethical aspects, are identified. The necessity of an integrated approach to cyber defense that combines technological solutions and educational initiatives to improve the security of enterprises is outlined.
Keywords: artificial intelligence, cybersecurity, phishing, data privacy, virus, automation, vulnerability management.

Штучний інтелект (ШІ) стає важливим елементом забезпечення кібербезпеки підприємств, оскільки дозволяє ефективно виявляти потенційні загрози, запобігати атакам та автоматизувати захист інформаційних систем. В умовах швидкого розвитку цифрових технологій та зростання рівня кіберзагроз традиційні методи безпеки можуть виявитися недостатньо ефективними. Саме тому застосування ШІ дає змогу оперативно аналізувати великі обсяги даних, виявляти нетипові дії та прогнозувати можливі загрози.

Згідно з прогнозами, фінансові втрати через кіберзлочинність можуть досягти 10,5 трильйона доларів США до 2025 року [1]. Це підкреслює важливість надійних методів кіберзахисту, які здатні адаптуватися до змінного середовища загроз. Використання

штучного інтелекту в цій сфері набуває все більшого значення. Очікується, що до 2027 року ринок ШІ у кібербезпеці зросте до 46,3 мільярда доларів США [2].

Найпоширенішими кіберзагрозами для підприємств є:

- Шкідливе програмне забезпечення – програми, які проникають у систему без відома користувача та можуть викрадати дані, блокувати доступ або здійснювати інші небезпечні дії.
- Програми-вимагачі – шифрують дані та вимагають викуп за їх розблокування.
- Атаки на відмову в обслуговуванні (DoS) – перевантажують мережу фальшивими запитами, що призводить до збоїв у роботі системи.
- Фішинг – метод шахрайства, коли зловмисники видають себе за довірені джерела, щоб отримати конфіденційну інформацію.
- Внутрішні загрози – ризики, що виникають через недбалість або зловмисні дії співробітників компанії.

Для ефективного захисту підприємствам слід використовувати інноваційні підходи. Наприклад, ШІ інтегрується у системи безпеки для аналізу мережевого трафіку, виявлення аномалій та блокування потенційно небезпечних дій. Такі рішення допомагають швидко реагувати на атаки та мінімізувати їхні наслідки.

Використання ШІ у кібербезпеці

1. Аналіз поведінки користувачів – алгоритми ШІ визначають типові шаблони дій користувачів і виявляють будь-які підозрілі активності.
2. Автоматизоване реагування – ШІ здатен оперативно блокувати підозрілі запити без участі людини.
3. Захист від фішингових атак – аналіз електронних листів та виявлення підозрілих елементів.
4. Управління вразливостями – ШІ може аналізувати системи безпеки, знаходити слабкі місця та пропонувати їх усунення.

Попри технологічний прогрес, людський фактор залишається ключовим у забезпеченні безпеки. Навчання персоналу, дотримання політик кібербезпеки та використання багатофакторної автентифікації значно зменшують ризик атак. Крім того, компаніям слід приділяти увагу етичному використанню ШІ та відповідності його застосування законодавчим нормам.

Впровадження ШІ у кібербезпеку допомагає створити більш стійкі системи захисту, що можуть адаптуватися до сучасних викликів та загроз. Проте важливо не лише покладатися на автоматизовані рішення, а й впроваджувати комплексний підхід, що включає технологічні, організаційні та освітні заходи.

Попри всі технологічні досягнення, людський фактор залишається визначальним у забезпеченні кібербезпеки. Компаніям необхідно формувати культуру обізнаності щодо кіберзагроз, щоб співробітники вчасно розпізнавали потенційні небезпеки та знали, як правильно діяти у кризових ситуаціях. Регулярне навчання персоналу, чітко розроблені протоколи безпеки та постійний моніторинг ризиків допомагають значно знизити ймовірність успішних атак.

Швидкий розвиток штучного інтелекту створює нові перспективи для автоматизації процесів та покращення кіберзахисту, проте водночас породжує нові виклики. Особливу увагу слід приділяти безпеці збереження великих обсягів даних на пристроях, адже зловмисники можуть використовувати їх як слабкі місця для несанкціонованого доступу або навіть модифікації алгоритмів ШІ. Щоб уникнути таких загроз, компаніям необхідно:

- Впровадити сучасні методи шифрування даних на рівні пристрою, а також застосовувати захищені механізми завантаження для запобігання несанкціонованому доступу.
- Використовувати диференційовану конфіденційність, що допоможе мінімізувати ризик витоку критично важливої інформації.

• Постійно оновлювати та вдосконалювати алгоритми ШІ, забезпечуючи їхню стійкість до нових кіберзагроз.

Впровадження штучного інтелекту у сферу кібербезпеки потребує комплексного підходу, що включає не лише технологічні рішення, а й навчальні програми для співробітників, які підвищать рівень їхньої обізнаності та навичок реагування на потенційні загрози.

Кібератаки становлять серйозну небезпеку для бізнесу, і підприємства повинні вживати активних заходів для захисту своїх даних і систем. Особливо вразливими є малі та середні компанії, які не завжди мають достатньо ресурсів для розгортання повноцінної системи безпеки. Це може спричинити суттєві фінансові втрати або негативний вплив на репутацію. Однак штучний інтелект може стати ефективним інструментом для виявлення та запобігання загрозам. Технології на основі ШІ аналізують величезні масиви даних, ідентифікують аномальну поведінку та шкідливі дії, що дозволяє підвищити рівень захисту та покращити продуктивність бізнесу.

Література

1. Роль штучного інтелекту в кібербезпеці: передбачення та запобігання атакам. URL: *https://eba.com.ua/rol-shtuchnogo-intelektu-v-kiberbezpetsi-peredbachennya-ta-zapobigannya-atakam/*
2. Що таке ШІ для кібербезпеки? URL: *https://www.microsoft.com/uk-ua/security/business/security-101/what-is-ai-for-cybersecurity*
3. Як штучний інтелект впливає на кібербезпеку малого та середнього бізнесу. URL: *https://blog.acer.com/ua/discussion/1880/yak-shtuchniy-intelekt-vplivaye-na-kiberbezpeku-malogo-ta-serednogo-biznesu*
4. Розглядаючи конвергенцію кібербезпеки та ШІ. URL: https://surl.li/gmmpdp

References

1. The role of artificial intelligence in cybersecurity: predicting and preventing attacks. URL: *https://eba.com.ua/rol-shtuchnogo-intelektu-v-kiberbezpetsi-peredbachennya-ta-zapobigannya-atakam/*
2. What is AI for cybersecurity? URL: *https://www.microsoft.com/uk-ua/security/business/security-101/what-is-ai-for-cybersecurity*
3. How artificial intelligence affects the cybersecurity of small and medium-sized businesses. URL: *https://blog.acer.com/ua/discussion/1880/yak-shtuchniy-intelekt-vplivaye-na-kiberbezpeku-malogo-ta-serednogo-biznesu*
4. Considering the convergence of cybersecurity and AI: *https://surl.li/gmmpdp*