ШТУЧНИЙ ІНТЕЛЕКТ ЯК ІНСТРУМЕНТ ДЛЯ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ

Борозняк Д.С., Пастушенко М.С.

Харківський національний університет радіоелектроніки,
кафедра інфокомунікаційної інженерії ім. В.В. Поповського,
Україна.

E-mail: mykola.pastushenko@nure.ua,
denys.borozniak@nure.ua

Abstract

The world is developing rapidly, and with it, cyber threats. Criminals are using increasingly sophisticated attack methods, which requires us to constantly look for new protection tools. One such tool is artificial intelligence (AI). This technology opens up new horizons in cyber security, allowing us to detect threats faster, more accurately and more effectively.

Існуючі проблеми

Світ стрімко розвивається, а з ним і кіберзагрози. Злочинці використовують все більш складні методи атак, що вимагає від нас постійного пошуку нових інструментів захисту. Одним з таких інструментів є штучний інтелект (ШІ). Ця технологія відкриває нові горизонти в забезпеченні кібербезпеки, дозволяючи нам виявляти загрози швидше, точніше та ефективніше.

Штучний інтелект (ШІ) має низьку переваг, а саме:

1) Швидкість обробки даних: ШІ здатний аналізувати величезні обсяги даних за лічені секунди, виявляючи аномалії, які людському оку можуть бути непомітними [1].
2) Автоматизація рутинних завдань: ШІ може автоматизувати багато рутинних завдань з кібербезпеки, таких як моніторинг мережі, аналіз логів та виявлення вторгнень [5].
3) Адаптивність: Системи на основі ШІ здатні адаптуватися до нових загроз і змінювати свої алгоритми в реальному часі [7].
4) Прогнозування: ШІ може прогнозувати майбутні атаки на основі аналізу історичних даних та виявлення трендів.

Застосування штучний інтелект (ШІ) в кібербезпеці:

1) Виявлення аномалій: ШІ може виявляти відхилення від нормальної поведінки мережі або систем, що може свідчити про наявність загрози [1].
2) Класифікація загроз: ШІ може класифікувати різні типи загроз, такі як фішинг, DDoS-атаки, ransomware та ін.[2].
3) Аналіз вразливостей: ШІ може автоматично сканувати системи на наявність вразливостей і оцінювати їх критичність [3, 4].
4) Розслідування інцидентів: ШІ може допомогти в розслідуванні кіберінцидентів, швидко ідентифікуючи джерело атаки та масштаби збитків.
5) Розробка нових методів захисту: ШІ може використовуватися для розробки нових алгоритмів шифрування, систем автентифікації та інших засобів захисту [6].

Приклади використання ШІ в кібербезпеці:

1) Системи виявлення вторгнень (IDS): ШІ дозволяє IDS більш точно виявляти загрози, адаптуючись до нових тактик зловмисників.
2) Системи запобігання вторгнень (IPS): ШІ може автоматично блокувати підозрілі з'єднання та атаки.
3) Аналіз логів: ШІ може аналізувати великі обсяги лог-файлів для виявлення аномалій та загроз.

4) Розпізнавання мови: ШІ може аналізувати голосові команди для виявлення соціальної інженерії.

Аналіз даних у кібербезпеці за допомогою штучного інтелекту

Якість даних є критичним фактором для ефективності моделей штучного інтелекту (ШІ). Ось кілька ключових аспектів, як якість даних впливає на продуктивність та точність ШІ. Тобто, якщо дані містять помилки або хибні відомості, модель ШІ буде навчатися на неправильній інформації, що призведе до поганих результатів. Наприклад, для мовної моделі важливо, щоб текст був граматично правильним і зрозумілим, інакше вона може генерувати неправильні або нелогічні відповіді [8].

Дані повинні містити достатньо інформації, щоб модель могла охопити всі можливі сценарії та приклади. Якщо певні аспекти або категорії не представлені належним чином, модель буде мати «сліпі зони» — ситуації, де її прогноз буде ненадійним або неточним. Це особливо критично для застосувань, таких як медична діагностика чи аналіз фінансових ризиків, де неповні дані можуть призвести до небажаних наслідків.

ШІ має працювати з актуальною інформацією, оскільки старі дані можуть не відображати сучасні реалії. Це важливо для моделей, що використовуються для прийняття рішень у реальному часі, наприклад, для рекомендаційної системи, що враховує зміни в поведінці користувачів або тренди. Здатність до аналізувеликих обсягів даних для виявлення патернів та аномалій за допомогою ШІ в кібербезпеці можливо реалізувати за допомогою різноманітних засобів, включаючи: методи машинного навчання, аналіз поведінки користувачів, системи виявлення вторгнень (IDS), аналіз журналів подій (SIEM), технології Big Data. Систематизовану інформацію щодо перелічених методів представлено у табл. 1.

Таблиця 1. Методи для аналізу даних у кібербезпеці за допомогою штучного інтелекту

Аналіз поведінки користувачів (UBA)	User Behavior Analytics (UBA) використовує ШІ таML (Machine Learning) длямоніторингу та аналізу поведінки користувачів у реальному часі з метою виявлення аномалій, які можуть свідчити про внутрішні загрози або компрометацію облікових записів.	**Моніторинг дій**	Збирає дані про дії користувачів,включаючи логін, доступ до файлів, використання мережевихресурсів та інші операції.
		Виявлення аномалій	Використовує моделі ML для порівняння поточної поведінки з історичними даними та виявлення відхилень, які можуть бути ознаками загрози.
		Адаптивність	Системи UBA можуть адаптуватися до змін у поведінцікористувачів, забезпечуючи постійне оновлення моделей для більш точного виявлення загроз.
Системи виявлення вторгнень (IDS)	Intrusion Detection Systems(IDS) використовують ШІдля аналізу мережевого трафіку та виявлення підозрілих дій, які можутьсвідчити про вторгнення.	**Мережеві IDS (NIDS)**	Моніторять мережевий трафік іаналізують пакети даних для виявлення аномалій. Застосовуються методи сигнатурного та евристичного аналізу.
		Хостові IDS (HIDS)	Моніторять активність на окремих пристроях, такі як журнали подій, цілісність файлів, системні виклики, для виявленнявторгнень.
		Гібридні системи	Комбінують NIDS та HIDS для більш комплексного підходу довиявлення загроз.

Таблиця 1. (Продовження) Методи для аналізу даних у кібербезпеці за допомогою штучного інтелекту

Аналіз журналів подій (SIEM)	Security Information and Event Management (SIEM)системи об'єднують та аналізують журнали подійз різних джерел для виявлення загроз і забезпечення відповідності вимогам безпеки.	**Централізова-незбирання даних**	Збирають дані з мережевих пристроїв, серверів, додатків та інших джерел.
		Кореляція подій	Використовують алгоритми для кореляції подій з різних джерел, що дозволяє виявити складні атаки, які можуть бути непомітні при аналізі окремих подій.
		Робота в режимі реального часу	Забезпечують моніторинг у реальному часі та автоматичне реагування на виявлені загрози.
Техно-логії Big Data	Технології Big Data дозволяють обробляти та аналізувати великі обсягиданих з високою швидкістю, що є критичним для виявленнята реагування на кіберзагрози.	**Розподілена обробка**	Використання платформ, таких як Hadoop та Apache Spark, для обробки великих обсягів даних у розподіленому середовищі.
		Аналіз у реальному часі	Використання технологій потокової обробки, таких як Apache Kafka, для аналізу даних у реальному часі.
		Інтеграція даних	Здатність інтегрувати дані з різних джерел, включаючи мережевий трафік, журнали подій, соціальні мережі та інші джерела.

Перспективи розвитку штучнаго інтелекту в кібербезпеці дійсно виглядають дуже обнадійливо. Незважаючи на виклики, що супроводжують впровадження ШІ, він може здійснити справжню революцію у способах захисту інформаційних систем та даних, особливо в умовах зростаючої складності загроз і численних кібернападів.

Один із ключових аспектів кібербезпеки — виявлення аномалій у величезних масивах даних. ШІ здатний швидко аналізувати великі обсяги інформації, знаходячи аномальні патерни та попереджуючи про потенційні атаки. Завдяки цьому він може виявляти загрози швидше, ніж це здатна зробити людина [1].

Завдяки технологіям машинного навчання, ШІ може "вчитися" в процесі роботи, покращуючи свою здатність розпізнавати нові, невідомі раніше загрози. Це дозволяє системам ШІ швидше адаптуватися до нових видів атак, які можуть виникнути на різних рівнях інфраструктури.

ШІ здатний не лише виявляти загрози, а й автоматично відповідати на них у режимі реального часу. Це може значно знизити навантаження на команди фахівців з кібербезпеки та дозволити їм зосередитись на складніших завданнях.

Наприклад, система може автоматично ізолювати уражений сегмент мережі або блокувати підозрілу активність, щоб запобігти подальшому поширенню загрози.

Штучний інтелект стає незамінним інструментом у сфері кібербезпеки, допомагаючи фахівцям у виявленні та нейтралізації загроз швидше, точніше й ефективніше, ніж це можливо за допомогою традиційних методів. Серед основних переваг ШІ у цій галузі виділяються такі аспекти, як швидкість обробки величезних обсягів даних, можливість автоматизації рутинних завдань, адаптивність до нових загроз і здатність прогнозувати майбутні атаки на основі аналізу історичних даних. Інновації, які ШІ приніс у кібербезпеку, є надзвичайно корисними, особливо в умовах швидкого розвитку технологій і методів атак. Інструменти, що використовують штучний інтелект, дозволяють автоматично моніторити мережі, проводити аналіз логів, здійснювати класифікацію загроз і навіть вести розслідування кіберінцидентів, що значно полегшує роботу фахівців і підвищує рівень захищеності систем.

Висновки

Однак для того, щоб потенціал ШІ в кібербезпеці був повністю реалізований, необхідно вирішити низку викликів. Перш за все, ефективність рішень ШІ залежить від якості та обсягу даних, що використовуються для його навчання: чим більший і різноманітніший масив даних, тим точнішими є результати роботи моделей.

Також необхідно покращити прозорість процесу прийняття рішень, щоб краще розуміти, як ШІ робить свої висновки, що полегшить виявлення та усунення потенційних помилок. Нарешті, не менш важливим є зниження вартості впровадження ШІ-рішень, що відкриє доступ до них для ширшого кола організацій, які зможуть підвищити рівень своєї кібербезпеки.

Перспективи використання ШІ в кібербезпеці є обнадійливими та можуть забезпечити новий рівень захисту в епоху цифрових технологій. Інтеграція ШІ дозволяє не лише підвищити ефективність захисту, а й надає змогу компаніям зосередитися на стратегічних завданнях, покладаючись на автоматизовані системи для відслідковування та нейтралізації загроз у режимі реального часу.

У майбутньому можна очікувати ще більших досягнень у розробці систем, які будуть здатні передбачати і навіть запобігати атакам завдяки можливостям ШІ, що безумовно стане новою віхою у сфері кібербезпеки.

Література

1. Alleyne, C., "The Use of Artificial Intelligence in Cybersecurity: Current Status and Prospects," Cybersecurity in a Digital World, 2021. Available at: https://cybersecurityai.com (accessed 10/28/2024).

2. Billings, S., and Garcia, A., "Cyber Threat Prediction Using Artificial Intelligence," Journal of Information Security, Vol. 9, No. 3, p. 34-45, 2022.

3. Coggs, M., "Artificial Intelligence and Its Role in Securing Corporate Networks," Analytics and Cybersecurity, 2023. Available at: https://corporatesecurityai.org (accessed 10/29/2024).

4. Ковальчук, О. Г., "Ефективність систем запобігання вторгнень із використанням ШІ," Вісник національного університету кібербезпеки, т. 15, № 1, с. 57-63, 2021.

5. Smith, D., and Williams, R., "Machine Learning in Intrusion Detection Systems," Artificial Intelligence Technologies in Security, 2022.

6. Taylor, B., "Development of New Security Algorithms Using Deep Learning," Journal of Information Systems Security, Vol. 17, No. 5, p. 24-32, 2023.

7. Heming, A., "Adaptive Cyber Systems Using Artificial Intelligence," International Journal of Cyber Security, Vol. 6, No. 2, p. 12-19, 2022.

8. Davenport, T. H., & Ronanki, R. (2018). Artificial Intelligence for the Real World: Why Companies are Applying AI to Cybersecurity. Harvard Business Review, 96(1), 108-116.