УДК 004.056.55:004.8
Вавриневич В.–ст. гр. КН-421
Відокремлений структурний підрозділ «Тернопільський фаховий коледж Тернопільського національного технічного університету імені Івана Пулюя»

ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ ДЛЯ ВИЯВЛЕННЯ І ЗАПОБІГАННЯ КІБЕРАТАКАМ

Наукові керівники: викладач-методист, спеціаліст вищої категорії Марціяш Г.Я., спеціаліст вищої категорії Цимбалюк Л.В.

Vavrynevych V.
Separate Structural Subdivision «Ternopil Professional College of Ternopil Ivan Puluj National Technical University»

USING ARTIFICIAL INTELLIGENCE FOR DETECTION AND PREVENTION OF CYBERATTACKS

Supervisors: teacher-methodologist, specialist of the highest category Martsiiyash G., specialist of the highest category Tsymbaliuk L.

Ключові слова: штучний інтелект, кібербезпека, виявлення атак, машинне навчання.
Keywords: artificial intelligence, cybersecurity, attack detection, machine learning.

Сьогодні штучний інтелект уже не просто новітня технологія, а ключовий елемент нашого повсякденного життя. Він постійно змінює різні галузі, допомагаючи автоматизувати рутинні процеси, вирішувати складні завдання та підвищувати ефективність роботи.

Особливо важливу роль ШІ (штучний інтелект) відіграє у сфері кібербезпеки, де його алгоритми аналізують великі масиви даних, виявляючи нестандартні активності в мережах і попереджаючи потенційні загрози.

Штучний інтелект відіграє важливу роль у виявленні несанкціонованих спроб доступу до інформаційних систем. Завдяки аналізу поведінки користувачів і мережевого трафіку, такі системи здатні виявляти підозрілу активність, зокрема шкідливий код або нетипові дії. Наприклад, якщо система зафіксує спробу доступу до конфіденційних даних у незвичний час, це може свідчити про потенційну загрозу, що потребує негайного реагування.

Різноманітні інструменти та ресурси, що ґрунтуються на ШІ-технологіях, дають змогу ефективніше аналізувати дані, прогнозувати ризики, автоматизувати рутинні завдання та реагувати на інциденти.

Системи виявлення вторгнень (IDS) використовуються для захисту мереж та систем від несанкціонованого доступу, атак та зловживань. IDS постійно моніторять мережевий трафік та шукають підозрілу активність, яка може свідчити про кібератаку. Це може включати сканування портів, атаки на відмову в обслуговуванні (DoS), спроби проникнення. IPS роблять те ж саме, що й IDS, але з однією ключовою відмінністю: вони можуть блокувати підозрілий трафік, щоб запобігти йому досягнення цілі. ШІ революціонізує IDS/IPS, роблячи їх більш ефективними та точними [3].

Системи Deception розгортають у мережі фальшиві сервери, веб-сайти, програми та інші ресурси, які імітують реальні системи, що можуть зацікавити зловмисників. Ці приманки можуть бути налаштовані для імітації різних типів систем, від банківських до управління контентом [1].

Системи SIEM (Security Information and Event Management) збагачені ШІ, революціонізують аналіз даних безпеки, пропонуючи нові можливості для зменшення кількості хибних спрацювань, прогнозування майбутніх атак та пріоритизації попереджень [1].

Системи UEBA (User and Entity Behavior Analytics) аналізують поведінку користувачів та пристроїв у мережі. Збираючи дані з журналів подій, мережевого трафіку та даних кінцевих точок, система створює базові профілі "нормальної" активності. Постійний моніторинг дозволяє виявляти відхилення від цих профілів, що можуть свідчити про потенційні загрози: незвичний час входу, доступ до нетипових файлів, підозрілий об'єм переданих даних тощо [1].

У світі веб-розробки Cross-Site Scripting (XSS) вразливості залишаються однією з найпоширеніших та небезпечних загроз. XSS дозволяє зловмисникам впроваджувати шкідливий код на веб-сторінки, що може призвести до крадіжки даних, або й отримання повного доступу над ресурсом. Традиційні методи статичного аналізу коду (SAST) часто не здатні виявити складні XSS вразливості, що виникають через поєднання різних факторів та контекстів. Для вирішення цієї проблеми дослідники звертаються до глибокого навчання, яке дозволяє навчати моделі на великих обсягах даних та виявляти складні патерни в коді. Важливо пам'ятати про ризик помилкових спрацювань та складність інтерпретації результатів. Тому SAST з ШІ рекомендується використовувати в поєднанні з іншими інструментами аналізу коду, ретельно перевіряючи результати та застосовуючи його для раннього виявлення XSS вразливостей [1].

DeepSign, як приклад DAST, дає можливість виявляти вразливості, які неможливо знайти за допомогою статичного аналізу, наприклад, ті, що залежать від умов виконання або вводу користувача. Цей метод має високу точність завдяки здатності DBN виявляти складні патерни в поведінці шкідливого ПЗ (програмне забезпечення), роблячи його універсальним інструментом для аналізу широкого спектру загроз [2]

Висновки. Використання штучного інтелекту у сфері кібербезпеки є одним із найефективніших підходів для виявлення та запобігання сучасним кібератакам. Завдяки аналізу великих масивів даних, виявленню аномалій та прогнозуванню загроз, ШІ-технології значно підвищують рівень захисту інформаційних систем.

Основні інструменти, такі як IDS/IPS, Deception, SIEM та UEBA, демонструють високу ефективність у моніторингу мереж, виявленні вторгнень та аналізі поведінки користувачів. Використання моделей глибокого навчання, таких як DeepSign, дозволяє автоматично генерувати сигнатури для виявлення нових загроз, що значно покращує можливості систем кіберзахисту.

Список використаних джерел

1. Ваврик Ю. Л., Опірський І. Р. Штучний інтелект: Кібербезпека нового покоління. Ukrainian Scientific Journal of Information Security. 2024. С. 244. URL: https://doi.org/DOI: 10.18372/2225-5036.30.19235.

2. David O. E., Netanyahu N. S. (2015). DeepSign: Deep learning for automatic malware signature generation and classification, https: // arxiv.org / pdf/1711. 08336.pdf.

3. Rjoub G., Bentahar J., Abdel Wahab O., Mizouni R., Song A., Cohen R., Otrok H., Mourad A. (2023). A Survey on Explainable Artificial Intelligence for Cybersecurity https://arxiv.org/pdf/2303.12942.pdf.