2. Про оперативно-розшукову діяльність : Закон України від 18.02.1992 № 2135-XII.
3. Федчак І. А. Основи кримінального аналізу. Львів : ЛьвДУВС, 2020.
4. ENISA. Artificial Intelligence Cybersecurity Challenges. 2023.
5. Конституція України : Закон України від 28.06.1996 № 254к/96-ВР.
6. Кримінальний процесуальний кодекс України : Закон України від 13.04.2012 № 4651-VI.

ДОПОВНЕНІ ОПЕРАЦІЇ БЕЗПЕКИ ЯК СУЧАСНИЙ ЗАСІБ ЗАСТОСУВАННЯ ШІ У КІБЕРБЕЗПЕЦІ

Пядишев Володимир Георгійович
доктор юридичних наук, професор, професор кафедри кримінального аналізу та інформаційних технологій, Одеський державний університет внутрішніх справ
Волошко Олексій Вікторович
начальник Управління кримінального аналізу, ГУНПУ в одеській області

Сьогодні штучний інтелект (ШІ) у кібербезпеці включає застосування машинного навчання, глибокого навчання та обробку природної мови для автоматизації виявлення загроз, аналізу величезних наборів даних та реагування на інциденти в режимі реального часу. Він діє як множник сили для команд безпеки, забезпечуючи проактивний захист, а не лише реактивне виявлення на основі сигнатур.

При цьому, до найважливіших аспектів застосування ШІ в кібербезпеці належать наступні.

а. Виявлення загроз та ідентифікація аномалій

Поведінкова аналітика (UEBA). ШІ встановлює базову лінію для нормальної мережевої активності та поведінки користувачів, негайно позначаючи відхилення, що вказують на внутрішні загрози, захоплення облікових записів або горизонтальне переміщення [1, с. 1-2].

Виявлення шкідливого програмного забезпечення. Захист кінцевих точок на базі ШІ (EDR) класифікує файли та блокує шкідливе програмне забезпечення, включаючи загрози нульового дня, не покладаючись на відомі сигнатури [2, с. 3].

Безпека електронної пошти. ШІ аналізує вміст, контекст та тон електронних листів для виявлення спроб фішингу [3, с. 4].

б. Автоматизоване реагування та управління інцидентами

Інтеграція SOAR. ШІ інтегрується з платформами оркестрації, автоматизації та реагування безпеки (SOAR - Security Orchestration, Automation, and Response) для автоматичної ізоляції заражених пристроїв, блокування шкідливих IP-адрес та скасування скомпрометованих облікових даних користувачів [4, с. 8].

Автономне виправлення: Системи можуть самостійно ініціювати виправлення або зміни конфігурації безпеки для усунення вразливостей.

в. Управління вразливостями [5, с. 12].

Прогнозна оцінка ризиків: ШІ оцінює інвентаризацію IT-активів та інформацію про загрози, щоб передбачити, де найімовірніше відбудеться порушення, що дозволяє командам пріоритезувати зусилля з виправлення (за допомогою CVSS) [6, с.].

Автоматизований аналіз коду: ШІ сканує програмне забезпечення на наявність вразливостей під час розробки [7, с. 14]..

г. Доповнення операцій безпеки (SecOps)

Зменшення втоми від сповіщень тривоги: ШІ сортує, пріоритезує та співвідносить тисячі сповіщень, зменшуючи кількість хибнопозитивних результатів, щоб аналітики могли зосередитися на критичних загрозах.

Генеративні помічники ШІ: помічники ШІ, такі як Microsoft Security Copilot, дозволяють аналітикам запитувати складні журнали, використовуючи природну мову, для швидшого розслідування інцидентів [8, с. 3].

Кожен зі зазначених аспектів заслуговує на окрему увагу. Проте сьогодні ми зосередимось на одному з них, а саме на так званому «доповненні операцій безпеки».

Отже, доповнення операцій безпеки (SecOps) за допомогою ШІ [9, с. 3]. – це інтеграція штучного інтелекту, включаючи машинне навчання (ML), обробку природної мови (NLP) та генеративний ШІ, до Центру операцій безпеки (SOC) – для покращення,

але не для повної заміни аналітиків-людей. З 2026 року доповнення ШІ переходить зі стану конкурентної переваги до стану необхідності, дозволяючи командам переходити від реактивного (тобто після виявлення події) ручного сортування тривог до проактивного (тобто попереджуючого подію) пошуку загроз та стратегічного управління ризиками. Цей підхід, який часто називають «SecOps на основі ШІ» або «Agentic SOC» (центр операцій з безпеки на основі застосування спеціалізованих програм), діє як «множник сили», що підсилює людським судження швидкістю ШІ.

Отже, ШІ у складі операцій з безпеки покращує наступні критично важливі функції.

Інтелектуальне сортування та зменшення втоми від опрацювання тривог. ШІ обробляє величезні набори даних, корелюючи сигнали між інструментами (наприклад, SIEM, EDR, NDR), щоб розрізняти доброякісну активність та справжні загрози. Це зменшує кількість хибнопозитивних результатів більш ніж на 90% та значно скорочує час розслідування.

Поведінковий аналіз та виявлення аномалій. ШІ постійно контролює мережі, пристрої та поведінку користувачів, щоб виявляти відхилення від встановлених базових рівнів, які вказують на шкідливу активність.

Генеративна допомога з боку ШІ. Помічники ШІ дозволяють аналітикам використовувати природну мову для запитів до платформ безпеки, узагальнення складних інцидентів та пропонування кроків щодо усунення наслідків.

Автономне розслідування та реагування. Агентний ШІ може самостійно досліджувати сповіщення, відстежувати ланцюжки атак у гібридних середовищах та рекомендувати або виконувати дії щодо стримування, як підкреслюють такі інструменти, як FortiSOC від Fortinet.

Зазначене забезпечує наступні переваги.

Більш швидкі виявлення загроз та реагування. Платформи на базі ШІ можуть аналізувати та реагувати за лічені секунди, значно скорочуючи час витримки.

Підвищені ефективність та масштабованість. Автоматизуючи повторювані завдання (наприклад, збагачення даних), аналітики можуть зосередитися на завданнях високої цінності.

Подолання розриву в навичках. ШІ надає покрокові інструкції, дозволяючи менш досвідченим аналітикам обробляти складні інциденти.

Що ж очікується протягом 2026 року?

Перехід до агентних операцій з безпеки. Очікується, що у 2026 рокці ШІ вийде за рамки простої автоматизації – з переходом до автономних, керованих агентами робочих процесів, які підключатимуться до інструментів безпеки через такі фреймворки, як Model Context Protocol (MCP) [10, с. 2-3].. При цьому основні гравці галузі зосередяться на наступному.

Microsoft Security. Пропонування уніфікованих платформ SecOps на базі штучного інтелекту, які об'єднують виявлення, розслідування та реагування.

Fortinet FortiAI. Використання штучного інтелекту для забезпечення агентних робочих процесів для пошуку загроз та реагування на інциденти

Google Cloud SecOps. Використання агентів, які підключаються до різних інструментів, щоб забезпечити на 50% швидший середній час реагування

ВИСНОВКИ

Хоча при здійсненні операцій з кібербезпеки штучний інтелект забезпечує високу швидкість, нагляд людини має вирішальне значення для контексту, стратегії та прийняття рішень на високому рівні. Отже, для забезпечення високої ефективності застосування штучного інтелекту потрібна високоякісна, комплексна інтеграція даних у всьому IT-середовищі. Одночасно важливим аспектом постає гостра необхідність забезпечувати захист власних моделей штучного інтелекту від атак ухилення та отруєння з боку деструктивних систем штучного інтелекту.

Список використаних джерел:

1. What is user and entity behavior analytics (UEBA)? *IBM.Com*. 29 April 2026. 16 p. Site. URL: https://www.ibm.com/think/topics/ ueba

2. What is the Role of AI in Endpoint Security? *Palo Alto Networks*. 2026. 16 p. Site. URL: https://www.paloaltonetworks.com/ cyberpedia/ what-is-ai-in-endpoint-security

3. Eze, Ch. S., Shamir, L. Analysis and Prevention of AI-Based Phishing Email Attacks. Electronics 2024, 13, 1839. 13 p. URL:

https://www.researchgate.net/publication/380475287_Analysis_and_Prevention_of_AI-Based_Phishing_Email_Attacks

4. Blacet, B. How SOAR and AI Are Reshaping Cybersecurity in Real Time. anomali.com. June 9, 2025. 12 p. Site. URL: https://www.anomali.com/blog/how-soar-and-ai-are-reshaping-cybersecurity Blacet, B. How SOAR and AI Are Reshaping Cybersecurity in Real Time. anomali.com. June 9, 2025. 12 p. Site. URL: https://www.anomali.com/blog/how-soar-and-ai-are-reshaping-cybersecurity

5. Aramide, O. AI-Driven Automated Incident Response and Remediation in Networks. May 2025. 25 p. DOI:10.21590/ijtmh.11.02.00. Site. URL: https://www.researchgate.net/publication/393743988_ AI-Driven_Automated_Incident_ Response_and_ Remediation_ in_Networks

6. Kalogiannidis, S., Papaevangelou, O., Giannarakis, G., Chatzitheodoridis, F. The Role of Artificial Intelligence Technology in Predictive Risk Assessment for Business Continuity: A Case Study of Greece. *MDPI.Com*. 23 January 2024. 57 p. Site. URL: https://www.mdpi.com/2227-9091/12/2/19

7. AI-driven code analysis: The new frontier in code security. *GitLab Inc*. 2026. 33 p. Site. URL: https://about.gitlab.com/topics/agentic-ai/ai-code-analysis/

8. Bono, J., Grana, J., Xu, A. Generative AI and Security Operations Center Productivity: Evidence from Live Operations. *ResearchGate*. November 2024. 8 p. DOI:10.48550/arXiv. 2411.03116. Site. URL: https://www.researchgate.net/ publication/ 385560290_ Generative_AI_and_Security_Operations_Center_Productivity_Evidence_from_Live_Operations

9. Gillett, M. How AI Can Reshape Security Operations Through Augmentation, Not Automation. *ESENTIRE.Com*. May 28, 2025. 8 p. Site. URL: https://www.esentire.com/blog/how-ai-can-reshape-security-operations-through-augmentation-not-automation

10. What is the Model Context Protocol (MCP)? *Model Context Protocol*. 2026. 4 p. Site. URL: https://modelcontextprotocol.io/docs/getting-started/intro