УДК 004.89:004.056.5:355.45

ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ ДЛЯ ВИЯВЛЕННЯ ТА РЕАГУВАННЯ НА КІБЕРЗАГРОЗИ ПІД ЧАС ВІЙНИ

Фединець Н.І., Сорока А.А.
Львівський державний університет безпеки життєдіяльності

Анотація. *Сучасна війна характеризується активним використанням кіберпростору як арени бойових дій. Кібератаки стають важливою складовою гібридної агресії. В умовах постійної зміни тактик противника традиційні методи кіберзахисту виявляються недостатньо ефективними. Особливого значення набуває використання технологій штучного інтелекту (ШІ) для автоматизованого виявлення, аналізу та реагування на кіберзагрози*..

***Ключові слова**: кібербезпека, кіберзагрози, штучний інтелект, кіберзахист, моніторинг, кіберпростір*.

***Abstract**: Modern warfare is characterized by the active use of cyberspace as an arena for combat operations. Cyberattacks are becoming an important component of hybrid aggression. In the face of constantly changing enemy tactics, traditional methods of cyber defense are proving to be ineffective. The use of artificial intelligence (AI) technologies for automated detection, analysis, and response to cyber threats is becoming particularly important.*

***Keywords**: cybersecurity, cyber threats, artificial intelligence, cyber defense, monitoring, cyberspace*..

Під час війни зростає кількість і складність кібератак. Зазвичай вони мають цілеспрямований характер і супроводжуються психологічними або інформаційно-підривними операціями. Основними типами загроз є:

- DDoS-атаки на державні портали та критичну інфраструктуру;
- спроби зламу систем управління об’єктами енергетики, транспорту, зв’язку;
- фішингові кампанії, спрямовані на військових і волонтерів;
- дезінформаційні операції, що використовують соціальні мережі та чат-боти;
- злам урядових акаунтів і поширення фальшивих повідомлень [2].

У таких умовах людські ресурси кіберзахисту не можуть оперативно обробляти великий обсяг даних про інциденти. Виникає потреба у використанні інтелектуальних систем, здатних самостійно навчатися, виявляти аномалії та передбачати потенційні атаки.

Штучний інтелект забезпечує новий рівень проактивного кіберзахисту, дозволяючи не лише реагувати на загрози, а й передбачати їх. Одним із ключових напрямків його застосування є машинне навчання для виявлення аномалій [3]. Алгоритми аналізують поведінку користувачів, мережевий трафік та системні журнали з метою визначення відхилень від нормальної діяльності. Наприклад, системи на базі машинного навчання можуть виявити підозрілу активність ще до того, як атака розгорнеться повністю. Іншим ва-

жливим напрямком є використання нейронних мереж для класифікації шкідливого програмного забезпечення. Завдяки глибинному навчанню такі системи здатні швидко розпізнавати нові типи вірусів, троянів або експлойтів, навіть якщо їхні сигнатури раніше не були відомі. Значну роль також відіграє аналіз великих даних (Big Data Analytics), адже системи штучного інтелекту можуть обробляти терабайти журналів подій та телеметрії, оперативно виявляючи зв'язки між окремими інцидентами й формуючи цілісну картину кіберактивності противника. Окрім цього, активно застосовуються інтелектуальні системи реагування, або SOAR-платформи, які інтегрують функції автоматичного реагування на інциденти, що дозволяє мінімізувати час між виявленням загрози та її нейтралізацією.

Після початку широкомасштабної агресії Росії проти України у 2022 році значно активізувалося впровадження систем штучного інтелекту в оборонному та кібернетичному секторах. Українські структури кіберзахисту, зокрема CERT-UA та їхні партнери, активно використовують системи автоматичного моніторингу на основі технологій машинного навчання для аналізу шкідливого трафіку, виявлення аномальної активності та попередження кібератак на державні й приватні інформаційні ресурси [1]. Паралельно міжнародні технологічні компанії, такі як Microsoft, Google та Mandiant, застосовують алгоритми штучного інтелекту для прогнозування атак з боку російських хакерських угруповань, аналізу їхніх тактик і моделювання можливих сценаріїв кіберагресії. Водночас активну роль у протидії інформаційним загрозам відіграють волонтерські кіберспільноти, які залучають нейронні мережі для аналізу фішингових листів, відстеження бот-мереж, виявлення фейкових новин і дезінформаційних кампаній у соціальних мережах. У результаті штучний інтелект поступово стає невід'ємною частиною оборонної кіберінфраструктури України, підвищуючи її стійкість і ефективність. Завдяки можливості швидко обробляти великі обсяги даних, виявляти закономірності та реагувати на загрози в режимі реального часу, системи ШІ забезпечують такий рівень швидкості, точності та масштабованості реагування, який неможливо досягти лише зусиллями людини.

Попри значний потенціал і широкі можливості, використання систем штучного інтелекту в сфері кібербезпеки супроводжується низкою проблем і обмежень, які впливають на ефективність та надійність їхнього застосування. Однією з ключових проблем є висока залежність ШІ-моделей від якісних і репрезентативних даних. Для навчання таких систем необхідні великі масиви достовірної інформації, однак у воєнний час процес збору, перевірки та оновлення даних часто ускладнений через нестачу ресурсів, кібератаки на джерела даних чи обмежений доступ до інфраструктури. Це може призводити до зниження точності прогнозів або до хибних спрацьовувань. Ще одним серйозним викликом є можливість навмисного обману моделей, так званих adversarial attacks, коли противник модифікує вхідні дані або створює спеціальні патерни, здатні ввести систему в оману.

У результаті ШІ може неправильно класифікувати загрозу, пропустити атаку або, навпаки, помилково вважати безпечну активність підозрілою.

Не менш важливими є етичні та правові аспекти використання штучного інтелекту. Автоматизоване прийняття рішень у кібербезпеці несе ризик неправомірного блокування користувачів, обмеження доступу до інформації чи порушення прав людини у разі помилки алгоритму. Це вимагає створення чітких нормативних рамок, прозорих процедур аудиту моделей та механізмів людського контролю. Крім того, існує проблема нестачі кваліфікованих кадрів. Для ефективного управління системами ШІ потрібні фахівці, які одночасно володіють знаннями у галузях кібербезпеки, машинного навчання, аналітики даних та етики штучного інтелекту. Недостатня підготовка таких спеціалістів може знизити ефективність впровадження технологій та підвищити ризик помилок. Таким чином, хоча штучний інтелект відкриває нові можливості для посилення кіберзахисту, його використання потребує обережності, системного підходу та постійного вдосконалення як технічних, так і організаційних механізмів.

Подальший розвиток застосування штучного інтелекту у кібербезпеці має базуватися на комплексному підході, що поєднує технології, організацію та освіту. Важливим кроком є створення національних платформ кіберзахисту, які інтегрують алгоритми ШІ для виявлення та нейтралізації загроз у режимі реального часу, об'єднуючи інформацію з різних джерел і автоматизуючи реагування на інциденти.

Штучний інтелект відкриває нові можливості для ефективного управління інформаційною безпекою під час війни. Його застосування дозволяє виявляти невідомі раніше загрози, зменшувати час реагування та підвищувати стійкість державних і приватних кіберсистем. Разом із тим, необхідно враховувати етичні, правові та технологічні обмеження, забезпечуючи контроль людини над критичними рішеннями.

Література

1. Microsoft Threat Intelligence. *Defending Ukraine: Early Lessons from the Cyber War*, 2023. URL: https://www.microsoft.com/en-us/security/security-insider/intelligence-reports/defending-ukraine-early-lessons-from-the-cyber-war.

2. Сердюков К.С. Інтелектуалізація кіберзахисту: роль штучного інтелекту у своєчасному виявленні аномалій в умовах еволюції гібридних загроз. №12. 2025. Актуальні питання економічних наук. URL: https://a-economics.com.ua/index.php/home/article/view/602.

3. Трофименко О. Г., Соколов А. В., Чикунов П. О. Штучний інтелект у військовій кіберсфері. Технології та інжиніринг. 2024. № 4 (21). С. 85-92.