УДК ОО4.8:354

М. В. Василинич

А. В. Василинич

М.О. Притула

РОЛЬ ШТУЧНОГО ІНТЕЛЕКТУ В ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ УКРАЇНИ

Вінницький національний технічний університет

Анотація

Штучний інтелект (ШІ) стає важливим інструментом у забезпеченні інформаційної безпеки, особливо в умовах загострення кіберзагроз, що загрожують Україні. Завдяки можливостям автоматизації, аналізу великих обсягів даних і прогнозуванню, ШІ допомагає виявляти, попереджати та ефективно реагувати на кібератаки. Ця теза досліджує ключову роль ШІ в кібербезпеці, його впровадження та потенційний вплив на захист інформаційних систем країни.

Ключові слова: штучний інтелект (ШІ), кібербезпека, прогнозування загроз, інформаційна безпека, машинне навчання, аномалії у трафіку, автоматизація безпеки.

Abstract

Artificial intelligence (AI) is becoming an important tool in ensuring information security, especially in the conditions of aggravation of cyber threats threatening Ukraine. With automation, big data analysis, and predictive capabilities, AI helps detect, warn, and effectively respond to cyberattacks. This thesis examines the key role of AI in cyber security, its implementation and potential impact on the protection of the country's information systems.

Keywords: artificial intelligence (AI), cyber security, threat prediction, information security, machine learning, traffic anomalies, security automation.

Вступ

Інформаційна безпека стає критичною складовою національної безпеки, оскільки зростає кількість кібератак на державні та приватні структури. Україна, як країна, що активно впроваджує цифрові технології, стикається з викликами у цій сфері. Одним із перспективних рішень є використання ШІ, який здатний прогнозувати загрози та забезпечувати ефективний захист даних.

Результати дослідження

1. Використання ШІ у виявленні загроз

Системи штучного інтелекту стали потужним інструментом для виявлення та запобігання кіберзагрозам, завдяки чому вони значно випереджають традиційні підходи у сфері кібербезпеки [3]. Одним із ключових напрямів їх застосування є аналіз мережевого трафіку. Алгоритми машинного навчання дозволяють системам ШІ створювати базу нормальної поведінки системи і користувачів, після чого автоматично визначати відхилення, які можуть свідчити про потенційні загрози. Це забезпечує оперативну і точну реакцію на аномальні дії, що є критично важливим у протидії складним атакам, таким як фішинг чи впровадження шкідливих програм.

Прогнозування є ще однією важливою перевагою ШІ [2]. Використовуючи історичні дані та поведінкові моделі, системи можуть передбачати можливі вектори атак, дозволяючи організаціям вживати заходів ще до того, як загроза набуде активного характеру. Наприклад, алгоритми можуть аналізувати дані про попередні атаки з урахуванням специфіки інфраструктури та створювати прогнозовані сценарії розвитку подій. Це допомагає своєчасно розробляти ефективні стратегії захисту. Однією з головних переваг ШІ є його здатність автоматизувати процеси безпеки. Наприклад, після виявлення потенційної загрози система може автоматично блокувати доступ з підозрілих IP-адрес,

запускати захисні протоколи чи інформувати адміністраторів. Це значно зменшує час реагування та мінімізує ризики, пов’язані з людським фактором.

Ще одним важливим аспектом є можливість обробки великих обсягів даних. Сучасні системи ШІ аналізують інформацію, що надходить із багатьох джерел, таких як журнали подій, метадані трафіку чи записи активності користувачів. Це дозволяє виявляти складні зв'язки між подіями, які можуть залишатися непомітними для звичайних засобів моніторингу [1]. Наприклад, інтеграція ШІ допомагає ідентифікувати багатовекторні атаки, де зловмисники комбінують кілька методів для досягнення своєї мети. В умовах постійної еволюції методів атак, таких як соціальна інженерія чи багатоступеневі кіберзагрози, ШІ показує високу ефективність завдяки здатності адаптуватися до нових умов. Компанії в Україні, такі як Wezom, вже активно використовують подібні рішення для підвищення рівня безпеки своїх інформаційних систем, забезпечуючи швидше виявлення і нейтралізацію загроз [3]. Це особливо актуально в умовах дефіциту кадрів у сфері кібербезпеки, адже автоматизація допомагає компенсувати нестачу людських ресурсів і підвищити загальну ефективність захисту.

2. Автоматизація процесів безпеки

Автоматизація процесів безпеки за допомогою штучного інтелекту (ШІ) має велике значення в умовах зростаючої кількості кіберзагроз та обмежених людських ресурсів у сфері кібербезпеки [3]. Використання ШІ дозволяє перекласти на системи автоматизовані завдання, такі як постійний моніторинг системи для виявлення аномалій, фільтрація великої кількості даних для виявлення шкідливих елементів і швидке реагування на інциденти. Цей підхід значно зменшує залежність від людського фактору, який є вразливим через ризик помилок, упущень або недостатньої швидкості обробки загроз. Наприклад, системи ШІ можуть автоматично блокувати небажані IP-адреси, ізолювати скомпрометовані ділянки мережі або запускати попередньо налаштовані протоколи захисту одразу після виявлення підозрілої активності. У контексті України, де існує дефіцит висококваліфікованих кадрів у сфері кібербезпеки, автоматизація стає критично важливою. Вона дозволяє організаціям залишатися стійкими до атак навіть за обмеженої кількості фахівців. ШІ також забезпечує цілодобову роботу без перерв, що знижує ймовірність того, що потенційна загроза залишиться непоміченою.

Крім того, автоматизовані системи ШІ мають здатність самонавчатися, тобто удосконалювати свої алгоритми на основі нових загроз, з якими вони стикаються. Це дозволяє системам залишатися актуальними та ефективними навіть у змінному середовищі кіберзагроз, яке постійно еволюціонує.

3. Проблеми впровадження ШІ

Впровадження штучного інтелекту (ШІ) у системи інформаційної безпеки супроводжується низкою викликів, які необхідно враховувати для досягнення максимальної ефективності. Одним із ключових ризиків є захист самих алгоритмів ШІ від зловмисних втручань [2]. Алгоритми машинного навчання можуть бути вразливими до атак, які спрямовані на зміну їхньої поведінки, наприклад, через підробку навчальних даних або маніпуляцію результатами роботи системи. Це створює необхідність впровадження додаткових механізмів захисту самих ШІ-систем, таких як контроль доступу, шифрування та аудити. Ще однією важливою проблемою є відповідність нормативним вимогам, зокрема міжнародним стандартам, таким як GDPR (Загальний регламент захисту даних). ШІ обробляє величезні обсяги даних, часто включаючи особисту інформацію, і порушення конфіденційності чи неправильне використання цих даних може призвести до серйозних юридичних наслідків. Відповідно, необхідно забезпечити прозорість алгоритмів і відповідність етичним нормам, що іноді ускладнює розробку і впровадження.

Крім того, високі витрати на створення, навчання та підтримку таких систем часто стають бар’єром для їх використання, особливо для невеликих організацій або державних установ із обмеженими бюджетами [3]. Розробка ефективних алгоритмів вимагає залучення висококваліфікованих фахівців і значних ресурсів, що може обмежити доступність ШІ-технологій для багатьох суб’єктів, які цього потребують.

Таким чином, хоча ШІ має значний потенціал у сфері кібербезпеки, вирішення цих проблем є важливим кроком для його повноцінної інтеграції.

Висновки

Штучний інтелект відіграє ключову роль у трансформації підходів до забезпечення інформаційної безпеки в Україні. Його впровадження дозволяє оперативно виявляти загрози, автоматизувати процеси та ефективно реагувати на інциденти. Однак для реалізації повного потенціалу ШІ необхідно подолати низку бар'єрів, включаючи фінансові та нормативно-правові аспекти. Активна підтримка держави та інвестиції в розробку таких технологій можуть суттєво підвищити кіберстійкість України.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. *Журнал Державне управління: удосконалення та розвиток - наукове фахове видання з питань державного управління*. URL: [http://www.dy.nayka.com.ua/pdf/1_2022/4.pdf] (дата звернення: 15.11.2024).
2. Прогнозування кібератак за допомогою ШІ: новітні підходи від. *Міжнародна аудиторська компанія BDO - BDO*. URL: [https://www.bdo.ua/uk-ua/insights-2/information-materials/2024/the-role-of-ai-in-cybersecurity-anticipating-and-preventing-attacks] (дата звернення: 15.11.2024).
3. ШІ у кібербезпеці: роль, застосування та переваги | Wezom. *IT-компания полного цикла разработки программных продуктов WEZOM - Киев, Украина*. URL: [https://wezom.com.ua/ua/blog/zastosuvannya-shi-u-kiberbezpetsi-rol-ta-perevagi] (дата звернення: 15.11.2024).

Василинич Анастасія Володимирівна – студентка групи Б-21б, Факультет будівництва цивільної та екологічної інженерії, Вінницький національний технічний університет, Вінниця, e-mail: vasilinichnastya@gmail.com.

Василинич Марія Володимирівна – студентка групи ПЗТ-24б, Факультет інформаційний електронних систем, Вінницький національний технічний університет, Вінниця, e-mail: mariykavasilinich@gmail.com.

Притула Максим Олександрович – *к.т.н., старший викладач кафедри інформаційних радіоелектронних технологій і систем, Вінницький національний технічний університет, м. Вінниця, e-mail: pritulamo@ukr.net*

Vasylynych Anastasiia V. – student of group B-21b, Department of Building, Civil and Environmental Engineering, Vinnytsia National Technical University, Vinnytsia, e-mail: vasilinichnastya@gmail.com.

Vasylynych Mariia V. – student of group PZT-24b, Department of Information Electronic Systems, Vinnytsia National Technical University, Vinnytsia, e-mail: mariykavasilinich@gmail.com.

Prytula Maksym Oleksandrovych - *Ph.D., Senior Lecturer of the Department of Information Radioelectronic Technologies and Systems, Vinnytsia National Technical University, Vinnytsia, e-mail: pritulamo@ukr.net*