УДК 004.56

А.В. Притула
Л. М. Куперштейн

ЗАСТОСУВАННЯ ШТУЧНОГО ІНТЕЛЕКТУ ДЛЯ ТЕСТУВАННЯ НА ПРОНИКНЕННЯ

Анотація

Робота присвячена вивченню використання штучного інтелекту (ШІ) для тестування на проникнення в сучасній кібербезпеці. Дослідження ретельно аналізує переваги та недоліки застосування штучного інтелекту в цій сфері. Основними перевагами використання штучного інтелекту є його здатність підвищувати ефективність, точність та автоматизацію процесів виявлення кіберзагроз. Зокрема, розглядається потенціал розвитку систем автоматичного виявлення та вирішення кібератак завдяки застосуванню штучного інтелекту. Особлива увага приділяється перспективам розвитку цієї технології, в тому числі її можливості у розв'язанні складних завдань тестування на проникнення та виявлення нових видів кіберзагроз.

У роботі також відзначено ключові недоліки, які супроводжують застосування штучного інтелекту в кібербезпеці, зокрема, ризик помилок та питання конфіденційності даних.

Це дослідження висвітлює значний потенціал штучного інтелекту для підвищення рівня кібербезпеки та забезпечення безпеки в Інтернет-просторі, а також наголошує на необхідності подальшого дослідження та розвитку цієї технології для ефективного боротьби з кіберзагрозами.

Ключові слова: *штучний інтелект, тестування на проникнення, кібербезпека, системи автоматичного виявлення кібератак, конфіденційність даних*

Abstract

This paper explores artificial intelligence (AI) utilization for penetration testing in modern cybersecurity. The study meticulously analyzes the advantages and disadvantages of employing AI in this domain. The main advantages of using AI include its ability to enhance efficiency, accuracy, and automation of threat detection processes. Specifically, the potential development of automated systems for detecting and addressing cyber-attacks through AI is discussed. Special attention is paid to the prospects of this technology, including its capability to address complex penetration testing tasks and identify new types of cyber threats.

The paper also acknowledges the key disadvantages of applying AI in cybersecurity, such as the risk of errors and concerns regarding data confidentiality.

This study highlights AI's significant potential to elevate cybersecurity levels and ensure safety in cyberspace. Furthermore, it underscores the importance of further research and development of this technology for effective combat against cyber threats.

Keywords: *artificial intelligence, penetration testing, cybersecurity, automated cyber-attack detection systems, data confidentiality.*

Вступ

В сучасному світі, що безупинно перетинається з цифровими технологіями, питання кібербезпеки виявляється одним із найактуальніших та найбільш складних в різних сферах діяльності. Зростання кількості кіберзлочинів та кібератак, спрямованих як на глобальні корпорації, так і на приватних користувачів, робить надійний кіберзахист нагальною потребою [1].

За статистичними даними від дослідницького центру Statista, за останні роки кількість кіберзагроз та кібератак значно зросла. За даними звіту "IBM X-Force Threat Intelligence Index 2023", кількість кібератак на підприємства зросла на 93% у 2022 році порівняно з попереднім роком. Це свідчить про необхідність постійного вдосконалення методів кіберзахисту та активного використання передових технологій, зокрема штучного інтелекту [1].

Основною перевагою використання штучного інтелекту в цій сфері є можливість автоматизувати та покращити процес виявлення вразливостей в інформаційних системах, а також прогнозування та запобігання потенційним кібератакам. Інтелектуальний аналіз результатів тестування, проведеного за допомогою штучного інтелекту, дозволяє виявляти навіть найбільш складні аномалії та підозрілі активності, що забезпечує підвищену ефективність та швидкість виявлення потенційних загроз [2].

Перспективи розвитку цієї технології прямим чином демонструють вдосконалення алгоритмів штучного інтелекту, інтеграцію з іншими технологіями кіберзахисту та підвищення співпраці між людським фактором та штучним інтелектом у сфері кібербезпеки. Результатом цього є забезпечення надійного захисту інформаційних ресурсів в умовах постійної загрози кібератак, що є важливим завданням сучасного інформаційного суспільства [3].

Результати дослідження

Застосування штучного інтелекту в тестуванні на проникнення виявляється критично важливим для забезпечення надійності кіберзахисту в умовах постійної еволюції кіберзагроз. Ця технологія дозволяє автоматизувати процес виявлення вразливостей в інформаційних системах, що забезпечує швидке та ефективне виявлення потенційних проблемних місць, які можуть бути використані зловмисниками для здійснення кібератак.

Однією з ключових переваг застосування штучного інтелекту є можливість проведення глибокого аналізу великих обсягів даних з метою виявлення аномалій та незвичних активностей, що можуть свідчити про наявність вразливостей або потенційних загроз безпеці. Алгоритми штучного інтелекту спроможні виявляти навіть найбільш складні патерни та прояви різноманітних атак, що може значно підвищити ефективність та точність тестування на проникнення.

Ще однією важливою характеристикою є здатність штучного інтелекту прогнозувати потенційні кіберзагрози на основі аналізу історичних даних та трендів. Це дозволяє приймати запобіжні заходи заздалегідь та запобігати можливим кібератакам шляхом усунення вразливостей та підвищення рівня кіберзахисту [4].

Використання саме штучного інтелекту в процесі тестування на проникнення обумовлене значним розвитком цієї галузі в останні роки. Завдяки значним досягненням у сфері машинного навчання, глибокого навчання та інших областях штучного інтелекту, відкриваються нові можливості для автоматизації та удосконалення процесів кіберзахисту.

Один з прикладів успішного використання штучного інтелекту в цій галузі - система "Watson for Cyber Security" від IBM [5]. Ця система застосовує когнітивні технології для аналізу мільйонів даних, що надходять від різних джерел, для виявлення потенційних кіберзагроз та вразливостей. Завдяки використанню штучного інтелекту, система здатна вчасно реагувати на нові загрози та надавати рекомендації щодо запобігання кібератак.

Обсяг використання штучного інтелекту в сфері тестування на проникнення з кожним роком лише зростає. За даними IDC, витрати на рішення з кібербезпеки, що базуються на штучному інтелекті та машинному навчанні, прогнозуються зрости до $11.7 мільярдів у 2025 році, що є майже вдвічі більше, ніж у 2021 році [1] (рис. 1). Це свідчить про те, що компанії та організації все більше віддають перевагу інноваційним підходам у кіберзахисті, де штучний інтелект відіграє ключову роль.

За останні роки спостерігається також тенденція до зростання кількості стартапів, що спеціалізуються на розробці рішень з кібербезпеки на основі штучного інтелекту. За даними CB Insights, в період з 2016 по 2020 рік було засновано понад 600 стартапів у цій галузі, які привернули понад $9 мільярдів інвестицій [6].

Це демонструє, що індустрія кіберзахисту все більше розуміє важливість використання штучного інтелекту для виявлення та запобігання кіберзагрозам. Штучний інтелект дозволяє підвищити ефективність, швидкість та точність процесів кібербезпеки, забезпечуючи надійний захист інформаційних ресурсів в умовах постійної еволюції кіберзагроз. Таким чином, це все і обумовлює доцільність використання штучного інтелекту у сфері кіберзахисту для забезпечення безпеки та стійкості цифрових інфраструктур у сучасному цифровому світі [7].

Говорячи про методи та техніки застосування штучного інтелекту в тестуванні на проникнення, важливо зазначити, що існують різноманітні підходи, які спрямовані на виявлення вразливостей та покращення кіберзахисту.

Одним з основних методів є використання машинного навчання для пошуку вразливостей у системах. За допомогою цього підходу моделі штучного інтелекту навчаються розпізнавати патерни, що характеризують вразливості, на основі аналізу великих обсягів даних. Такі моделі можуть виявляти вразливості, які можуть бути непомітними для людського ока, та роблять це значно швидше та ефективніше.

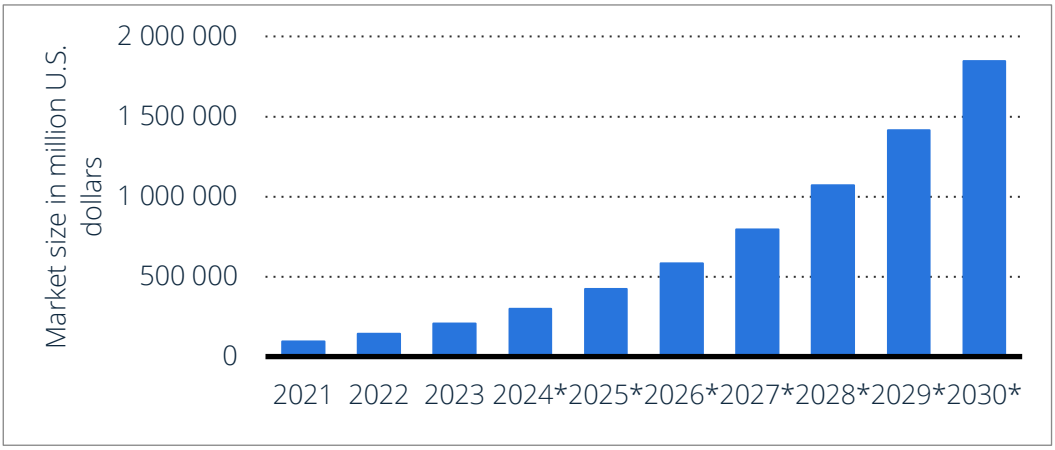

Рисунок 1 – Обсяг світового ринку штучного інтелекту у 2021 році з прогнозом до 2030 року (у мільйонах доларів США)

Інший метод полягає у використанні глибокого навчання для виявлення аномалій та підозрілих активностей в мережах. Глибокі нейронні мережі можуть аналізувати великі обсяги даних та виявляти незвичні патерни, які можуть свідчити про потенційні загрози безпеці. Цей метод дозволяє виявляти нові, раніше невідомі атаки та аномальність в поведінці системи [7].

Крім того, використання нейронних мереж може застосовуватися і для аналізу текстової та візуальної інформації, що дозволяє виявляти вразливості та потенційні кіберзагрози у великому обсязі даних, що поширюються в Інтернеті.

Наприклад, в області аналізу текстової інформації нейронні мережі можуть бути використані для виявлення підозрілих або шкідливих URL-адрес, фішингових листів, криптовалютних шахраїв тощо. Моделі нейронних мереж, навчені на великому обсязі даних про відомі кіберзагрози, можуть аналізувати вхідні дані та автоматично виявляти підозрілі шаблони та сигнали, що вказують на можливі загрози безпеці.

Щодо аналізу візуальної інформації, нейронні мережі можуть бути використані для виявлення аномальних зображень або підозрілих образів, які можуть бути пов'язані з кіберзагрозами, такими як атаки на безпеку мережі або витоки конфіденційної інформації. Наприклад, нейронні мережі можуть бути навчені розпізнавати атаки на веб-сайти за зразками веб-сторінок або програмного коду, що були відомі раніше як складові зловмисницьких дій [8].

В той же час, слід зауважити, що використання штучного інтелекту для тестування на проникнення має як переваги, так і недоліки. Одним з головних полюсів є можливість автоматизації процесів виявлення вразливостей та аналізу кіберзагроз. Згідно з дослідженням компанії PwC, 74% організацій вже використовують або планують використовувати штучний інтелект для автоматизації рутинних завдань у сфері кібербезпеки. Це дозволяє підвищити ефективність процесу тестування та реагування на потенційні загрози [9].

Ще одним плюсом є підвищення точності виявлення вразливостей за допомогою штучного інтелекту. За допомогою алгоритмів глибокого навчання, системи можуть аналізувати великі обсяги даних та виявляти складні патерни, навіть найбільш приховані кіберзагрози.

Однак використання штучного інтелекту також має свої недоліки. Наприклад, ризик помилок може призвести до великої кількості помилок першого та другого роду. Також виникають питання щодо конфіденційності даних, оскільки штучний інтелект може потребувати доступу до великих обсягів конфіденційної інформації для ефективного аналізу. Один з прикладів використання штучного інтелекту в тестуванні на проникнення - система виявлення аномалій в мережі за допомогою машинного навчання. Ця система може виявляти незвичні або підозрілі активності, які можуть вказувати на потенційні кібератаки або вразливості в мережі. Зведена таблиця можливих переваг та недоліків наведена у табл. 1.

Проте дослідження показують, що перспективи застосування штучного інтелекту все ж таки значною мірою перекривають будь-які з наявних викликів, а тому не можуть заперечити його використання. Щодо самих перспектив розвитку в застосуванні штучного інтелекту для тестування на проникнення, можна і надалі очікувати подальше зростання інтересу та впровадження цих технологій в різних сферах. Завдяки постійному розвитку алгоритмів машинного навчання та глибокого навчання, системи штучного інтелекту будуть ставати все більш ефективними в виявленні та аналізі кіберзагроз.

Таблиця 1 – Переваги та недоліки в застосуванні штучного інтелекту для тестування на проникнення

Переваги	Недоліки
Автоматизація процесів	Ризик помилок: штучний інтелект може неправильно інтерпретувати дані або виявляти фальшиві позитиви.
Підвищена ефективність	Питання конфіденційності: використання штучного інтелекту може вимагати доступу до конфіденційних даних, що породжує питання щодо їх захисту.
Покращена точність	Вимога до експертності: впровадження систем штучного інтелекту може вимагати наявності фахівців з високим рівнем кваліфікації для їх налагодження та підтримки.
Можливість виявлення складних патернів	Обмеження швидкості впровадження: імплементація систем штучного інтелекту може вимагати значних зусиль та часу.
Зменшення часу виявлення кібератак	Потенційна відмова від людського втручання: автоматизація процесів може призвести до зниження ролі людини в процесі тестування, що може призвести до неправильних висновків чи втрати контролю.

Однією з ключових перспектив є розвиток систем автоматичного виявлення та вирішення кібератак без необхідності втручання людини. Це може включати розробку алгоритмів, які не лише виявляють кіберзагрози, а й надають рекомендації щодо їх усунення або автоматично вживають заходи для забезпечення безпеки.

Додатково, зростання кількості доступних даних та покращення їх якості можуть сприяти розвитку систем штучного інтелекту для тестування на проникнення. Використання великих обсягів даних для тренування моделей може покращити їхню точність та надійність [10].

Зокрема, відкриваються нові можливості для використання штучного інтелекту в області кібербезпеки Інтернету речей (IoT), де велика кількість підключених пристроїв створює нові виклики щодо забезпечення безпеки мережі. Штучний інтелект може бути використаний для виявлення та запобігання кібератак на пристрої IoT, що сприятиме підвищенню загального рівня кібербезпеки.

Загалом, перспективи розвитку штучного інтелекту в тестуванні на проникнення включають постійне зростання ефективності, широке впровадження в різні галузі та розвиток нових методів та технологій для забезпечення кібербезпеки.

Висновки

Отже, застосування штучного інтелекту для тестування на проникнення є важливим напрямком в сучасній кібербезпеці. Ця технологія відкриває нові можливості для виявлення та запобігання кіберзагроз, забезпечуючи більшу ефективність, точність і автоматизацію процесів. Розвиток штучного інтелекту в цій галузі дозволяє не лише вчасно реагувати на потенційні загрози, але й передбачати їх та уникати виникнення майбутніх ризиків.

Загалом, штучний інтелект наразі має потенціал стати одним з ключових та найефективнішим інструментом у боротьбі з кіберзагрозами, допомагаючи підвищити рівень кібербезпеки в різних сферах життя. Продовження розвитку цієї технології обіцяє ще більш ефективний та надійний захист від кіберзлочинності, роблячи інтернет-простір безпечнішим для всіх його користувачів.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Statista - the statistics portal. Statista. URL: https://www.statista.com/ (дата звернення: 12.03.2024).
2. Remote host operation system type detection based on machine learning approach / L. Kupershtein et al. Selected papers of the II international scientific symposium "intelligent solutions" (intsol-2021). workshop proceedings. 2022. No. 3106. P. 65–81. URL: https://ir.lib.vntu.edu.ua/handle/123456789/37675 (дата звернення: 12.03.2024).
3. How artificial intelligence will drive the future of penetration testing in IT security - cybersecurity | digital forensics | penetration testing | ermprotect. Cybersecurity | Digital Forensics | Penetration Testing | ERMProtect - Cybersecurity | Digital Forensics | Penetration Testing | ERMProtect. URL: https://ermprotect.com/blog/how-artificial-intelligence-will-drive-the-future-of-penetration-testing/ (дата заверення: 12.03.2024).
4. Pope J. Human vs AI in pen testing. Cybersmart consulting. URL: https://cybersmartconsulting.com/ai-in-pen-testing/ (дата зверенення: 12.03.2024).
5. Investigating threats with watson for cyber security - security intelligence. Security Intelligence. URL: https://securityintelligence.com/investigating-threats-with-watson-for-cyber-security/ (дата звернення: 12.03.2024).
6. The 2020 global CVC report. CB Insights. URL: https://www.cbinsights.com/research/report/corporate-venture-capital-trends-2020/ (date of access: 13.03.2024).

7. Ijlal T. How to start penetration testing of artificial intelligence. Infosec writeups. URL: https://infosecwriteups.com/how-to-start-penetration-testing-of-artificial-intelligence-c11e97b77dfa (дата звернення: 13.03.2024).
8. Küçükkarakurt F. Is it possible to use artificial intelligence for penetration tests?. Make use of. URL: https://www.makeuseof.com/is-it-possible-to-use-artificial-intelligence-for-penetration-tests/ (дата звернення: 13.03.2024).
9. Dsouza M. How artificial intelligence can improve pentesting | Packt Hub. Packt Hub. URL: https://hub.packtpub.com/how-artificial-intelligence-can-improve-pentesting/ (дата звернення: 14.03.2024).
10. Joseph T. The influence of AI and machine learning on pen testing. QASource Blog. URL: https://blog.qasource.com/the-influence-of-ai-and-machine-learning-on-pen-testing (дата зверення: 14.03.2024).

Притула Андрій Вікторович – студент групи 125-23а, факультет інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, Вінниця, e-mail: andrik.pritula@gmail.com.

Куперштейн Леонід Михайлович – к.т.н., доцент кафедри захисту інформації, Вінницький національний технічний університет, м. Вінниця email: kupershtein.lm@gmail.com

Prytula Andrii V. – Student of Faculty of Information Technologies and Computer Engineering, Vinnytsia National Technical University, e-mail: andrik.pritula@gmail.com.

Kupershtein Leonid M. – PhD, Associated Professor of Information Protection Chair, Vinnytsia National Technical University, Vinnytsia, email: kupershtein.lm@gmail.com