

СИМУЛЯЦІЇ ТА МОДЕЛЮВАННЯ В ДОСЛІДЖЕННЯХ КІБЕРБЕЗПЕКИ

Струк Д. О.

Національний університет «Одеська юридична академія»

Україна, Одеса

icestruck0@gmail.com

Анотація. Алгоритм ШІ та методи аналізу даних дозволяють системам безпеки автономно виявляти, аналізувати та реагувати на нові загрози в режимі реального часу. Створення симуляційного кіберполігону дозволяє моделювати атаки та їх вплив, розробляти та тестувати стратегії захисту, оптимізувати систему кібербезпеки для реальної інфраструктури.

Ключові слова: штучний інтелект; кібербезпека; системний аналіз; симуляція; моделювання сценаріїв; автоматизація.

Вступна частина. Симуляція та моделювання важливі в прогнозуванні й протидії потенційним кіберзагрозам. Через складність викликів безпеки важко, а подекуди неможливо якісно протестувати готові програмні продукти на комп'ютерах, на яких вони розроблялися. Потрібно створити безпечне, контрольоване середовище для тестування різних сценаріїв кіберзагроз та оцінки вразливостей програмної системи. Такого роду «полігон» дозволяє досліджувати та перевіряти інноваційні рішення щодо посилення безпеки системи без ризиків для реальної інфраструктури.

Мета роботи – проаналізувати роль симуляції та моделювання для сфери кібербезпеки.

Основна частина. Методи моделювання в кібербезпеці допомагають оцінити ефективність механізмів захисту, наприклад, через імітацію реальних сценаріїв атак, включаючи розподілені атаки на відмову в обслуговуванні (DDoS), фішингові схеми та проникнення шкідливого програмного забезпечення. Застосування машинного навчання надає фахівцям з кібербезпеки можливість моделювати поведінку як зловмисників (чорних хакерів), так і захисників (білих хакерів). Завдяки спостереженням за моделями атак і впливом стратегій захисту в режимі реального часу, спеціалісти оптимізують системи та захищають місця виникнення потенційних загроз. Прикладом такого роду симуляції є навчальна гра «червона проти синьої команди» (Red Team vs. Blue Team) [1]. Під час моделювання складного злому мережі червона команда, виступаючи в ролі зловмисників, намагається проникнути в мережу компанії, в той час як синя команда, відповідальна за захист, працює над виявленням і пом'якшенням атак. Навчання дозволяє організації виявляти критичні вразливості, покращувати свої можливості реагування на інциденти та вдосконалювати захисні стратегії [2].

Симуляції кібербезпеки засобами ШІ допомагають зменшити кількість помилкових тригерів, моделюючи поведінку мережі як під час атак, так і за нормальних умов. Це покращує здатність прогнозувати майбутні кібератаки, аналізувати їх потенційний вплив, забезпечує командам кібербезпеки кращу готовність і зменшує час реагування [3]. Крім того, залучення симуляцій, заснованих на досвіді минулих атак або шаблонах, створених системами ШІ, допомагає у розробці надійних стратегій захисту, які розвиваються разом з появою нових загроз.

Моделювання в дослідженнях кіберзагроз, які імітують динаміку кібератак і захисту, часто базуються на методах ШІ та машинного навчання. Це допомагає виявляти закономірності, прогнозувати вразливості та пропонувати стратегії пом'якшення наслідків. Поширеним підходом є використання методів контрольованого та неконтрольованого

навчання, які аналізують дані для розподілу поведінки в мережі на нормальну та аномальну. Так, системи виявлення вторгнень (Intrusion Detection Systems, IDS) на основі аномалій використовують моделі для відстеження відхилень від нормального мережевого трафіка, виявляючи потенційні загрози в режимі реального часу. Іншим прикладом є моделі на основі ШІ, які використовують розпізнавання образів для виявлення підозрілих дій на пристроях без потреби розшифровувати дані. Ці моделі розроблені для автономної роботи та самонавчання, що робить їх важливими в сучасних архітектурах кібербезпеки.

Додатково моделювання кібербезпеки поширюється на імітацію процесів прийняття рішень зловмисниками. Генеративні змагальні мережі (generative adversarial networks) та моделі навчання з підкріпленням (reinforcement learning models) застосовують для прогнозування та протидії кіберзлочинній діяльності шляхом імітації поведінки зловмисників у контрольованому кіберсередовищі. Цей процес допомагає виявляти вразливі місця в системах ще до настання реальних загроз.

Впровадження ШІ в симуляції та моделювання кіберзагроз дозволяє розробити адаптивні, інтелектуальні системи кібербезпеки. Використовуючи моделі на основі ШІ, операційні центри безпеки автоматизують виявлення загроз, реагування на них і стратегії пом'якшення наслідків. Моделювання на основі ШІ надає можливість створювати динамічні тестові середовища, адаптовані до появи нових загроз, які постійно вдосконалюють систему безпеки. Так, ШІ-моделі Darktrace аналізують нормальну поведінку користувачів і пристроїв у мережі. Встановлюючи базову лінію нормальної діяльності, система Darktrace виявляє аномалії, які можуть свідчити про потенційні загрози. Якщо аккаунт співробітника раптом починає отримувати доступ до конфіденційних даних у незвичний час або завантажувати великі обсяги інформації, ШІ Darktrace позначає таку поведінку як підозрілу [4].

ШІ-моделі підтримують прийняття рішень за умов високих ризиків, швидко і точно обробляючи величезні обсяги даних. Вони виявляють «тонкі» аномалії, які люди-аналітики можуть не помітити. Для прикладу, системи ШІ в симуляціях кібербезпеки у режимі реального часу інформують про ефективність певних протоколів захисту, що є критично важливим для мінливого ландшафту загроз.

Висновки. Отже, симуляції та моделювання є важливими у дослідженнях в сфері кібербезпеки, пропонуючи контрольоване середовище для вивчення потенційних загроз і розробки контрзаходів. Інтеграція ШІ в ці системи створює простір для адаптивного навчання і реагування на загрози в режимі реального часу, що робить їх незамінними інструментами в сучасних стратегіях кібербезпеки.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

- [1] Blue Goat. (2024). *Red Team vs. Blue Team: Cybersecurity Exercises Explained*. <https://bluegoatcyber.com/blog/red-team-vs-blue-team-cybersecurity-exercises-explained/>
- [2] Christie, St. (2023, June 27). *What is Cyber Attack Simulation?* Validatio. <https://validato.io/what-is-a-cyber-attack-simulation/>
- [3] IBM. (2024). *AI and automation for cybersecurity*. <https://www.ibm.com/ai-cybersecurity>
- [4] Elastic. (2024). *Darktrace*. <https://www.elastic.co/docs/current/integrations/darktrace>

Struk Dmytro

Simulations and modeling in cyber security research

Abstract. AI algorithm and data analysis methods allow security systems to autonomously detect, analyze and respond to new threats in real time. Creating a simulation cyber polygon allows you to simulate attacks and their impact, develop and test protection strategies, optimize the cyber security system for real infrastructure.

Keywords: artificial intelligence; cybersecurity; system analysis; simulation; scenario modelling; automation.