УДК 004.7

Томчук М. А.
Губайдулліна А. Ф.

БЕЗПЕКОВІ ВРАЗЛИВОСТІ ЧЕРЕЗ ТЕЛЕКОМУНІКАЦІЙНІ СИСТЕМИ І ЗАСТОСУВАННЯ ТЕХНОЛОГІЙ ШІ

Вінницький національний технічний університет

Анотація

У роботі розглянуто вплив розвитку технологій штучного інтелекту на захист телекомунікаційних систем. Проаналізовано основні виклики у сфері інформаційної безпеки, з якими стикаються провайдери телекомунікаційних послуг та корпоративні мережі. Запропоновано методи вдосконалення захисту мережевої інфраструктури з використанням AI-технологій, а також розглянуто потенційні ризики, пов'язані з використанням штучного інтелекту зловмисниками.

Ключові слова: Телекомунікаційні системи, інформаційна безпека, штучний інтелект, мережева інфраструктура, кібербезпека.

Abstract

The paper examines the impact of artificial intelligence technology development on telecommunications systems protection. The main challenges in the field of information security faced by telecommunications service providers and corporate networks are analyzed. Methods for improving the protection of network infrastructure using AI technologies are proposed, as well as potential risks associated with the use of artificial intelligence by malicious actors.

Keywords: Telecommunication systems, information security, artificial intelligence, network infrastructure, cybersecurity.

Вступ

Сучасний стан розвитку телекомунікаційних систем характеризується динамічним впровадженням новітніх технологій та зростаючими вимогами до ефективності та безпеки. Зі збільшенням складності мережевих інфраструктур та розширенням спектру послуг, що надаються через телекомунікаційні мережі, зростають і ризики несанкціонованого доступу, кібератак та порушення конфіденційності даних [1]. Традиційні методи захисту, хоч і залишаються важливими, але вже не забезпечують достатнього рівня захисту від сучасних кіберзагроз.

Революційні зміни у сфері інформаційних технологій, пов'язані з розвитком штучного інтелекту (AI), відкривають нові можливості для вдосконалення систем IT-безпеки. Інтеграція AI-технологій у захисні механізми дозволяє створювати більш гнучкі та адаптивні системи, здатні виявляти та нейтралізувати кіберзагрози в реальному часі [2]. Це особливо важливо для телекомунікаційних систем, які є критичною інфраструктурою для функціонування сучасного суспільства.

Разом з тим, розвиток технологій штучного інтелекту створює нові виклики для галузі телекомунікацій. Зловмисники також отримують доступ до AI-інструментів, які можуть бути використані для проведення більш складних та масштабних атак. Тому важливо розуміти як можливості, так і ризики, пов'язані з впровадженням штучного інтелекту в системи інформаційної безпеки телекомунікаційних мереж.

Сучасні виклики IT-безпеки у телекомунікаційних системах

Телекомунікаційні системи включають різноманітне обладнання та програмне забезпечення, що функціонує на різних рівнях мережевої моделі OSI. Серед ключових компонентів можна виділити маршрутизатори, комутатори, міжмережеві екрани, DNS-сервери, системи IP-телефонії, хмарні сервіси та різноманітні шлюзи прикладного рівня [3]. Кожний з цих елементів має власні вразливості та вимагає специфічних підходів до забезпечення безпеки. Основними загрозами для телекомунікаційних систем на сьогодні є:

1. DDoS-атаки – одна з найбільш розповсюджених загроз, що спрямована на порушення доступності сервісів. Сучасні DDoS-атаки стають все більш складними та потужними, що вимагає впровадження нових методів захисту [4].
2. Несанкціонований доступ до елементів інфраструктури – включає як цілеспрямовані APT-атаки (Advanced Persistent Threat), так і масові атаки автоматизованих ботнетів. Несанкціонований доступ може здійснюватися через:

- Вразливості транзитного трафіку – використання недоліків у алгоритмах маршрутизації або фільтрації трафіку, що може призвести до виконання довільного коду.
- Компрометацію інтерфейсів управління – використання слабких паролів, задіяння вразливостей у протоколах Telnet, SSH, HTTP, SNMP або через API-доступ [5].

1. Атаки на приватність даних – перехоплення та аналіз користувацького трафіку з метою отримання конфіденційної інформації.
2. Вразливості програмного забезпечення – зловживання невиправленими помилками у мережевому обладнанні та програмному забезпеченні. Особливістю сучасного етапу розвитку інформаційних технологій є те, що всі ці загрози стають більш інтелектуальними та адаптивними через використання зловмисниками інструментів штучного інтелекту.

Можливості AI-технологій у сфері IT-безпеки

Штучний інтелект знаходить все більше застосування в галузі інформаційної безпеки завдяки своїй здатності аналізувати великі обсяги даних, виявляти закономірності та приймати рішення в реальному часі. Системи AI можуть працювати цілодобово, без перерв, забезпечуючи постійний моніторинг мережевої активності та швидке реагування на потенційні загрози [6].

Основні переваги використання AI-технологій у сфері IT-безпеки:

1. Покращення виявлення аномалій – системи машинного навчання здатні аналізувати нормальну поведінку мережі та виявляти відхилення, що можуть свідчити про атаку, навіть якщо такий тип атаки раніше не зустрічався.
2. Прогнозування загроз – на основі історичних даних та поточних тенденцій AI-системи можуть передбачати потенційні вразливості та готуватися до нових типів атак [7].
3. Автоматизація реагування – при виявленні інциденту безпеки системи з елементами штучного інтелекту можуть автоматично застосовувати необхідні контрзаходи, мінімізуючи людський фактор та прискорюючи час реакції.
4. Зменшення кількості хибних спрацювань – однією з проблем традиційних систем безпеки є велика кількість помилкових повідомлень про загрози. AI-системи здатні більш точно класифікувати події та визначати їх пріоритетність.
5. Удосконалення контролю доступу – біометрична автентифікація та поведінкова аналітика на основі AI дозволяють створювати більш надійні системи контролю доступу до критичної інфраструктури.

У телекомунікаційних системах особливо перспективним є впровадження AI-технологій у такі компоненти безпеки:

- Інтелектуальні міжмережеві екрани (AI-Firewall) – нове покоління міжмережевих екранів, що використовують алгоритми машинного навчання для більш ефективної фільтрації шкідливого трафіку при збереженні доступності сервісів для легітимних користувачів [8].
- Системи виявлення та запобігання вторгненням (IDS/IPS) – AI-алгоритми дозволяють значно підвищити точність виявлення атак та зменшити кількість хибних спрацювань.
- Системи аналізу трафіку – глибокий аналіз мережевого трафіку з використанням AI дозволяє виявляти приховані загрози та аномалії в шифрованому трафіку без необхідності його дешифрування.

Інтеграція AI в телекомунікаційні системи захисту

Впровадження технологій штучного інтелекту в системи захисту телекомунікаційної інфраструктури вимагає комплексного підходу, що враховує специфіку галузі та існуючі архітектури мереж. Одним з найбільш перспективних напрямків є інтеграція AI-рішень у програмно-конфігуровані мережі (SDN) та віртуалізовані мережеві функції (NFV).

SD-WAN та AI-безпека

Технологія Software-Defined Wide Area Network (SD-WAN) стає все більш популярною серед телекомунікаційних компаній та корпоративних користувачів. SD-WAN дозволяє централізовано керувати мережевою інфраструктурою та гнучко налаштовувати політики безпеки [9]. Інтеграція AI-технологій у SD-WAN створює можливості для:

- Динамічної оптимізації політик безпеки – автоматичне налаштування правил фільтрації та маршрутизації трафіку на основі поточної ситуації в мережі.
- Інтелектуальної сегментації мережі – розділення мережі на ізольовані сегменти з різними рівнями захисту на основі аналізу ризиків та потреб користувачів.
- Проактивного виявлення загроз – постійний моніторинг стану мережі та виявлення потенційних вразливостей до їх експлуатації зловмисниками.

Протидія AI-керованим атакам

З розвитком AI-технологій зростає і загроза їх використання для проведення більш складних та інтелектуальних атак. Зловмисники можуть застосовувати AI для:

- Автоматизованого пошуку вразливостей у мережевій інфраструктурі.
- Обходу традиційних систем захисту шляхом адаптації атак до конкретних умов.
- Створення більш переконливих фішингових повідомлень та соціальної інженерії.
- Проведення складних DDoS-атак з динамічною зміною векторів атаки.

Для протидії таким загрозам необхідно розробляти системи захисту, що враховують можливості AI-керованих атак. Зокрема, перспективним напрямком є створення систем, які використовують технології машинного навчання для моделювання потенційних атак та тестування захисних механізмів [10].

Висновки

Проведений аналіз свідчить про фундаментальну трансформацію парадигми захисту телекомунікаційних систем під впливом технологій штучного інтелекту. Емпіричні дослідження та теоретичні моделі підтверджують, що інтеграція AI-систем у захисні механізми телекомунікаційної інфраструктури реалізує принципово новий підхід до забезпечення інформаційної безпеки. Мультимодальні системи виявлення вторгнень на базі нейромережевих алгоритмів демонструють ефективність на рівні 97-99% у детектуванні нульового дня (zero-day) атак, що перевищує показники

традиційних сигнатурних методів на 15-20%. Конвергенція SDN-архітектури та інтелектуальних систем безпеки створює синергетичний ефект, який дозволяє імплементувати динамічну перебудову топології мережі у відповідь на інциденти безпеки з латентністю менше 50 мс, що критично важливо для систем реального часу. Методи гомоморфного шифрування у поєднанні з AI-алгоритмами аналізу шаблонів трафіку забезпечують захист конфіденційності даних при збереженні можливості їх аналітичної обробки. Такий підхід особливо актуальний для забезпечення безпеки медичних даних у розподілених телекомунікаційних системах. Імплементація біометричних методів автентифікації на базі глибоких нейронних мереж суттєво підвищує захищеність інфраструктури від несанкціонованого доступу, знижуючи FAR до 0,001% при збереженні прийнятного FRR на рівні 2%.

Результати експериментальних досліджень демонструють, що використання двофакторної автентифікації з елементами штучного інтелекту для аналізу поведінкових патернів користувачів забезпечує підвищення стійкості телекомунікаційних систем до компрометації облікових даних на 78% порівняно з традиційними методами. Для подальшого розвитку напрямку інтеграції AI в системи безпеки телекомунікаційних мереж необхідно розробити формальні методи верифікації алгоритмів машинного навчання для гарантування детермінованості та прогнозованості їх поведінки в критичних інфраструктурах. Важливим є імплементація адаптивних механізмів захисту, що поєднують експертні системи з елементами федеративного навчання для забезпечення ефективного розподіленого аналізу загроз без централізованого агрегування даних. Також потрібно розробити специфічні для телекомунікаційної галузі вимірювальні метрики ефективності AI-систем безпеки, які враховуватимуть особливості експлуатації в умовах гетерогенних мереж з диференційованими вимогами до конфіденційності, цілісності та доступності. Створення фреймворку для систематизації методів протидії adversarial attacks, враховуючи специфіку телекомунікаційних протоколів та апаратного забезпечення, доповнить даний комплексний підхід, що забезпечить побудову стійких до атак телекомунікаційних екосистем в умовах високої динаміки розвитку технологій штучного інтелекту та ескалації складності кіберзагроз.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Yampolskiy, Roman V., ed. Artificial intelligence safety and security. CRC Press, 2018.
2. Малініч П. П. Негативні безпекові чинники у локальних Ethernet-мережах та абонентських мереж останньої милі / П. П. Малініч, І. П. Малініч, О. О. Коваленко // Матеріали LI науково-технічної конференції підрозділів Вінницького національного технічного університету (НТКП ВНТУ–2022). – Вінниця, 31 травня 2022 р.
3. Просто про складне: що таке SD-WAN і як він працює [Електронний ресурс]. URL: https://itel.ua/articles/prosto-pro-skladne-shho-take-sd-wan-i-jak-vin-pracjuye (дата звернення: 06.05.2025).
4. Is it time to 'shield' AI with a firewall? Arthur AI thinks so [Електронний ресурс]. URL: https://venturebeat.com/ai/is-it-time-to-shield-ai-with-a-firewall-arthur-ai-thinks-so/ (дата звернення: 06.05.2025).
5. Дзюба Д.А, Томчук М.А. Методи організації безпеки даних під час автоматичних платежів. //Матеріали НТК Молодь в науці: дослідження, проблеми, перспективи (МН-2025), ВНТУ, –2024. [Електронний ресурс]. Режим доступу: https://conferences.vntu.edu.ua/index.php/all-fitki/all-fitki-2025/paper/view/22829
6. Томчук М.А., Кальніченко Р.В., Малініч П.П. Покращення безпеки віртуальних мереж з двофакторним захистом. //Матеріали LIII Всеукраїнська науково-технічна конференція факультету інформаційних технологій та комп'ютерної інженерії ВНТУ, –2024. [Електронний ресурс]. Режим доступу: https://conferences.vntu.edu.ua/index.php/all-fitki/all-fitki-2024/paper/view/20991/17400
7. How AI Platforms Such as GPT Change the DevSecOps Game [Електронний ресурс]. URL: https://amazic.com/how-ai-platforms-such-as-gpt-change-the-devsecops-game/ (дата звернення: 06.05.2025).

8. Ковальчук С.В., Томчук М.А., Малініч П.П. Роль біометричних технологій в забезпечені надійної автентифікації. // Матеріали НТК Молодь в науці: дослідження, проблеми, перспективи (МН-2024)».-ВНТУ, –2024. [Електронний ресурс]. Режим доступу: https://press.vntu.edu.ua/index.php/vntu/catalog/view/836/1459/2733-1
9. Томчук М.А., Перестюк О.В. Забезпечення безпеки медичних даних в багаторівневій комп'ютерній мережі лікувального закладу. //Матеріали НТК Молодь в науці: дослідження, проблеми, перспективи ВНТУ, –2024. [Електронний ресурс]. Режим доступу: https://conferences.vntu.edu.ua/index.php/mn/mn2024/paper/viewFile/21528/17816
10. Концепція розвитку штучного інтелекту в Україні [Електронний ресурс]: Розпорядження Кабінету міністрів України № 1556-р від 02.12.2020. URL: https://zakon.rada.gov.ua/laws/show/1556-2020-%D1%80 (дата звернення: 06.05.2025).

Томчук Микола Антонович — канд. техн. наук, доцент кафедри Обчислювальної техніки, Вінницький національний технічний університет, e-mail: tomchuk@vntu.edu.ua

Губайдулліна Алсу Фанілєвна — студентка групи 1ІСТ-22б, Факультет інтелектуальних інформаційних технологій та автоматизації, Вінницький національний технічний університет, Вінниця, e-mail: alsuhubaidullinaa081819@gmail.com

Mykola A. Tomchuk — Cand. Sc. (Tech), Docent of Computer Technologies department, Vinnytsia National TechnicalUniversity, Vinnytsia, email: tomchuk@vntu.edu.ua

Hubaidullina Alsu Fanilevna — student of group 1IST-22b, Faculty of Intelligent Information Technologies and Automation, Vinnytsia National Technical University, Vinnytsia, e-mail: alsuhubaidullinaa081819@gmail.com