УДК 004.7

Томчук М. А.
Крещенко М. С.
Малініч І. П.

ІТ-БЕЗПЕКА У ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМАХ В ЕПОХУ ШТУЧНОГО ІНТЕЛЕКТУ

Вінницький національний технічний університет

Анотація
Телекомунікації, як і технології побудови комп'ютерних мереж, на базі яких вони побудовані залишаються досить консервативними і нові технології впроваджуються у цій сфері впроваджуються лише ті, що зарекомендували себе як стабільні, економічно вигідні та такі, що мають корпоративну підтримку численними вендорами. Революція у ІТ-безпеці, викликана стрімким розвитком AI-технологій, зробить ландшафт телекомунікаційних технологій більш еластичним до швидких змін.

Ключові слова: Телекомунікації, комп'ютерні мережі, ІТ-безпека, AI

Abstract
Telecommunications, as well as the technologies for building computer networks, on which they are based, remain quite conservative, and only those new technologies are introduced in this field that have proven themselves to be stable, profitable and that have enterprise support from many vendors. The revolution in IT security brought by the rapid development of AI technologies will make the telecommunications technology landscape more resilient for rapid changes.

Keywords: Telecommunications, computer networks, IT security, AI

Вступ

Наразі забезпечення ефективної ІТ-безпеки є актуальним пріоритетом для функціонування всієї ІТ-сфери. При цьому самої ефективності рішень інформаційної безпеки недостатньо: подібні рішення мають забезпечувати достатню швидкість виявлення та дієві превентивні заходи. На базі штучного інтелекту можна створити більш ефективні рішення для захисту від кібератак, з прийнятним по швидкості їх виявленням. Інструменти інформаційної безпеки, створені на базі AI можуть застосовувати більш дієві заходи при виникненні інцидентів ІТ-безпеки, оцінюючи їх актуальність та їх потенційні наслідки, при почергових спрацювань у режимі реального часу [1]. Таким чином, доведена ефективність цих технологій в боротьбі з кіберзагрозами.

Захист телекомунікаційних систем є досить складним завданням, оскільки охоплює захист самих різних пристроїв, що працюють на різних рівнях мережевої моделі OSI. Існує багато різних видів телекомунікаційних пристроїв та сервісів, серед них комутатори, маршрутизатори, мережеві екрани, шлюзи прикладного рівня (наприклад проксі-сервери та балансувальники навантаження), контролери мережевого обладнання (хмарні чи серверні), апаратне забезпечення стільникової та IP-телефонії, DNS-сервери та хмарні рішення SD-WAN [2]. Оцінюючи переваги засобів ІТ-безпеки (незалежно від того, чи працюють вони на базі AI-рішень чи ні) необхідно розуміти наскільки широко вони можуть покрити весь спектр існуючого сьогодні телекомунікаційного обладнання. Також необхідно зрозуміти наскільки серйозну загрозу для безпеки телекомунікаційних систем можуть становити AI-системи, що будуть знаходитись на службі зловмисників.

Огляд можливостей AI-систем у ІТ-безпеці

Успішне впровадження AI у корпоративному світі призвело до значного прогресу в автоматизації завдань, які колись виконувалися виключно людьми, наприклад, виявлення шахрайства, пошук потенційних клієнтів та надання підтримки клієнтам. Цікаво, що AI часто виконує ці завдання з більшою точністю та ефективністю ніж люди. Його експертиза полягає саме в орієнтованих на деталі, повторюваних завданнях, таких як аналіз численних юридичних документів для перевірки точності записів у полі. Як наслідок, інструменти AI забезпечують результати з меншими помилками та більшою швидкістю [3]. AI має здатність обробляти величезні обсяги даних. Системи штучного інтелекту

працюють, збираючи великі обсяги позначених навчальних даних, аналізуючи дані на наявність кореляцій і шаблонів і використовуючи ці шаблони для прогнозування майбутніх станів [4].

Програми штучного інтелекту часто обробляють конфіденційну інформацію, таку як особисті дані або фінансові операції. "Неприйнятний ризик" – системи AI, які становлять загрозу безпеці, способу життя чи правам людей. Наразі у багатьох країнах та міждержавних союзах існують заборони на системи такого виду [5]. AI "високого ризику" – системи, що використовуються в державних чи соціальних сферах, або такі, що мають інший прямий вплив на особисту безпеку чи права людини. AI з "обмеженим" або "мінімальним" ризиком — системи з особливим зобов'язанням щодо прозорості. Рішення для IT-безпеки знаходяться саме на такому рівні.

Багато запобіжних заходів у IT-безпеці простіше виконати з використанням штучного інтелекту [6]. Він є перспективним інструментом для боротьби з кіберзагрозами. Це свідчить про те, що алгоритми, натхненні природою, часто використовуються для подальшого покращення продуктивності класичних алгоритмів безпеки мережі, їх потрібно удосконалювати для зменшення помилок. Він також використовується для вибору параметрів точного налаштування та підвищення швидкості навчання для кращих результатів.

Безпекові тренди у телекомунікаційних системах

Телекомунікаційні системи мають дві найбільші проблеми у сфері IT-безпеки: DDoS-атаки та несанкціонований доступ. При роботі над подоланням DDoS-атак використання AI показує хороші результати у відслідковуванні та аналізі цих атак. Найбільш прогресивною ідеєю на даний момент є фаєрвол з інтегрованим AI [7], як еволюція концепції Next Generation Firewall (NGFW). Його перевагами є більш гнучка фільтрація шкодоносного трафіку, що дозволяє зменшити недоступність ресурсів для легітимного трафіку.

Іншою ключовою проблемою є несанкціонований доступ до телекомунікаційної інфраструктури. До цієї проблеми входять як більш серйозні APT-атаки, так і випадки інфікування елементів інфраструктури ботнетами. Поверхня атаки у таких елементів мережі передбачає два типи атак:

- транзит. Вразливості, що використовуються у цьому типі атак, виникають зазвичай у обладнання чи хмарних застосунків, що пропускають через себе L3 чи L7-трафік. Недосконаліть захищеності алгоритмів маршрутизації чи фільтрації трафіку можуть призводити до можливості виконання довільного коду. Такі вразливості як правило рідкісні. Маршрутизація та фільтрація трафіку зазвичай відбувається на рівні ядра операційної системи. У обладнанні що працює на базі ОС GNU/Linux цей фактор може бути мінімізований завдяки своєчасному оновленню ядра Linux та мережевих сервісів. Однак у деяких L3-комутаторів маршрутизація може здійснюватись у спеціальному високопродутивному процесорі маршрутизації. Якщо у такому процесорі виявиться апаратна вразливість - без заміни обладнання її усунути не вдастся.
- інтерфейси управління (MGMT). У даному випадку несанкціонований доступ може відбуватись у двох випадках: компрометація авторизованого доступу чи експлуатація вразливості. Компрометації доступу може виникати при використанні дефолтних паролів чи взломі суміжних систем, які мали доступ до обладнання. Взлом обладнання найчастіше відбувається через протоколи Telnet, SSH, HTTP, SNMP [8] чи API-доступ.

Обидва типи атак стануть більш відчутними з ростом керованими штучним інтелектом атак. Це зумовлено тим, що одні лише кращі безпекові практики конфігурування перестануть бути дієвим способом для захисту від взломів [9]. Багато вразливостей софту та обладнання буде стрімко виявлено зростаючими можливостями систем штучного інтелекту, що скоріше за все і буде використано зловмисниками.

Висновки

Прихід AI-технологій у телекомунікаційну сферу та IT-безпеки вже стрімко відбувається і з часом він привнесе зміни у дуже консервативний світ мережевих технологій. Найшвидше вони впроваджуються у фільтруванні, балансуванні та аналізі L7-трафіку. Тектонічні зсуви у IT-безпеці телекомунікаційної інфраструктури пришвидшать AI-революцію у цій царині. На даний момент найбільш швидко впроваджувати інформаційний захист на базі AI-технологій можливо завдяки технології SD-WAN.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Yampolskiy, Roman V., ed. Artificial intelligence safety and security. CRC Press, 2018.
2. 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: 07.06.2023).
3. Domingos, Pedro. The master algorithm: How the quest for the ultimate learning machine will remake our world. Basic Books, 2015.
4. Perner, Petra, Atsushi Imiya. Machine learning and data mining in pattern recognition. Springer-Verlag Berlin Heidelberg, 2011.
5. 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: 07.06.2023).
6. Куперштейн Л. М. Нечіткий підхід до оцінки ризиків безпеки бездротових мереж [Електронний ресурс] / Л. М. Куперштейн, О. П. Войтович, А. Є. Татарчук // Матеріали XIV міжнародної конференції "Контроль і управління в складних системах (КУСС-2018)", м. Вінниця, 15-17 жовтня 2018 р. – Електрон. текст. дані. – Вінниця : ВНТУ, 2018. – Режим доступу: http://ir.lib.vntu.edu.ua/handle/123456789/22729.
7. 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: 07.06.2023).
8. Маліній П. П. Негативні безпекові чинники у локальних Ethernet-мережах та абонентських мереж останньої милі [Електронний ресурс] / П. П. Маліній, І. П. Маліній, О. О. Коваленко // Матеріали LI науково-технічної конференції підрозділів Вінницького національного технічного університету (НТКП ВНТУ–2022). – Вінниця, 31 травня 2022 р. – Електрон. текст. дані. – 2022. – Режим доступу: https://conferences.vntu.edu.ua/index.php/all-fitki/all-fitki-2022/paper/view/15614.
9. 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: 07.06.2023).

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

Крещенко Марина Сергіївна — студентка групи ТКС-22м, факультет Інформаційних електронних систем, Вінницький національний технічний університет

Маліній Ілля Павлович — асистент кафедри Комп’ютерних наук, Вінницький національний технічний університет