DOI: https://doi.org/10.15276/ict.02.2025.30
УДК 004.056.5:004.8

Перспективи використання методів і технологій штучного інтелекту у системах мережевого захисту

Бірка Євген Геннадійович[1)]
Аспірант каф. Комп'ютерних систем
ORCID: https://orcid.org/0009-0008-4669-493X; rariwe@gmail.com
Стрельцов Олег Василійович[1)]
Канд. техніч., доцент каф. Комп'ютерних систем[1)]
ORCID: https://orcid.org/0000-0002-4691-5703, e-mail: streltsov.o.v@op.edu.ua
[1)] Національний університет «Одеська політехніка», пр. Шевченка, 1. Одеса, 65044, Україна

АНОТАЦІЯ

Сучасні виклики у секторі мережевої безпеки вимагають створення нових підходів та залучення нових засобів для підвищення ефективності кіберзахисту, що є актуальною проблемою і завданням сьогодення. Традиційні засоби боротьби з протиправним проникненням у приватні та корпоративні мережі, хмарні та серверні сховища данних, які засновуються на сигнатурних методах, не завжди є ефективним методом боротьби перед мережевими атаками нового типу. Саме тому залучення штучного інтелекту (ШІ) до боротьби з цими загрозами дає змогу підвисити якість відбиття атак та створити нові, сучасні засоби захисту, які є більш ефективними за переліком аспектів якості та відповідають сучасним критеріям. Світовому досвід масштабних кіберзлочинів та існуючих проектів з інтеграції штучного інтелекту у мережеву безпеку, дає змогу дійти висновку про можливості перспективи використання ШІ як унітарного засобу, так і комплексного інструменту у поєднанні з іншими технологіями.

Ключові слова: штучний інтелект; кіберзахист, машинне навчання; кіберзахист, кібератака

Вступ: Сучасний мережевий простір, як відкрита глобальна мережа, так і локальні або корпоративні мережі не є застрахованими від несанкціонованого проникнення та кіберзлочинів різного типу та цілей. Ця теза підтверджена сумним світовим глобальним досвідом та щоденними інцидентами у сфері мережевої безпеки. Для більш чіткого розуміння проблеми необхідно мати певне уявлення про сучасні кіберзагрози та їх класифікацію. Масштаб сучасних мережевих атак можливо класифікувати за величиною мережі, яку можна поділити на три рівні – локальний, корпоративний та глобальний. Цілі мережевих атак можуть бути різноманітними, але серед найпопулярніших можливо виділити такі, як; саботаж – атака направлена на вивід з ладу активного мережевого устаткування, фінансова атака – крадіжка коштів, даних за транзакціями, вимагання та шантаж, шпигунство – атаки, направлені на крадіжку конфіденційних даних, які відносяться більше до сфери кіберрозвідки, політичні та ідеологічні атаки – ставлять за мету створення зовнішнього інформаційного впливу та дезінформації, кіберзлочини проти звичайних осіб – крадіжка паролей, акаунтів, приватної особистої інформації. За рівнем наслідків результат атаки варіюється від непомітного до катастрофічного. Атака може створити короткий за терміном збій та втрату незначного обсягу інформації, може повністю зупинити певні сервіси, як і мережеві, так і соціальні. Наслідки звичайно оцінюють у грошовому та часовому еквіваленті, але масштаб наслідків може бути і катастрофічним на рівні цілої держави та суспільства.

Сучасні засоби боротьби із кіберзагрозами: На кожному рівні мережі існують власні засоби захисту. На рівні локальних мереж використовують базове антивірусне програмне забезпеяення, такі програмні продукти усім відомі, приклади – ESET, Windows Defender, тощо. Також це персональні фаєрволи, ціллю яких є контроль вхідного та вихідного трафіку. Популярними засобами є системи шифрування даних на базі передових криптографічних алгоритмів, двохфакторна аутентифікація та різноманітні засоби біометрії, така технологія як VPN та менеджери паролів. На корпоративному рівні використовуються більш стійкі методи захисту, слід відмітити такі, як інтелектуальні фаєрволи з глибинним аналізом пакетів (NGFW with DPI), системи розпізнавання та запобіганню загрозам (IDS/IPS), захист кінцевих пристроїв (EDR), мінімізація доступу до мережі та її сегментація з можливістю

ізоляція (Zero Trust system), системи запобігання витоку даних (DPL-системи), системи резервного копіювання, протидії фішингу та вже існуючим атакам методами соціальної інженерії. До цього переліку можливо додати використання глибинної аутентифікації за рахунок сучасних мережевих протоколів безпеки. Завдяки сучасним криптографічним алгоритмам, які були реалізовані у певних протоколах та засобах захисту мережі, трафік з корпоративних мереж, при передачі через глобальну мережу, наприклад між філіями, активно шифрується, таким чином при перехваті даних, мережеві пакети являють собою набір даних, які не піддаються аналізу. На глобальному рівні використовують комплексні системи захисту, такі як глобальні системи моніторингу загроз на сигнатурній базі (MITRE, IBM X-force), глобальні мережеві фільтри (приклад Google Safe Browsing), які відсіюють певний перелік ресурсів з потенційними загрозами, системи захисту критичної інфраструктури (приклад система SCADA). Дуже важливим є аналіз трафіку з боку провайдерів (ISP-level security), адже глобальний мережевий простір є простором компаній з бізнес-сегменту. На глобальному рівні системи захисту є більш різноманітними та об'єднуються у єдиний комплекс захисту та систему, яка контролює велику кількість аспектів.

Світовий досвід протистояння кіберзагрозам: Мережевий захист завжди йде на один крок позаду кіберзагроз. Особливої уваги потребують так звані атаки нульового дня (Zero day attacks). Цей тип атак полягає у використанні вразливостей програмного продукту, які не були виявлені на етапі тестування, і назва аргументується тим, що в розробників було 0 днів на можливість запобігти прояву вразливості. Більш відомий інцидент з атакою нульового дня, це сумнозвісний WannaCry – криптовірус-вимагач на базі невідомої вразливості у мережевому протоколі SMB. За рахунок цієї вразливості та з використання експлойтів вірус автоматично поширювався мережею без участі користувачів, все більше і більше заражаючи персональні пристрої [1]. За статистичними звітами вірус встиг заразити 230 тисяч пристроїв у 150 країнах світу, паралізувавши медичні структури, заводи та окремі банківські структури. Такий приклад атаки довів відповідність початкової тези та став прикладом величезних наслідків та потенціалу кіберзагроз. Саме тому розробка сучасних більш досконалих методів та засобів мережевого захисту є популярною галуззю розробки та експериментів, у тому числі із залученням штучного інтелекту.

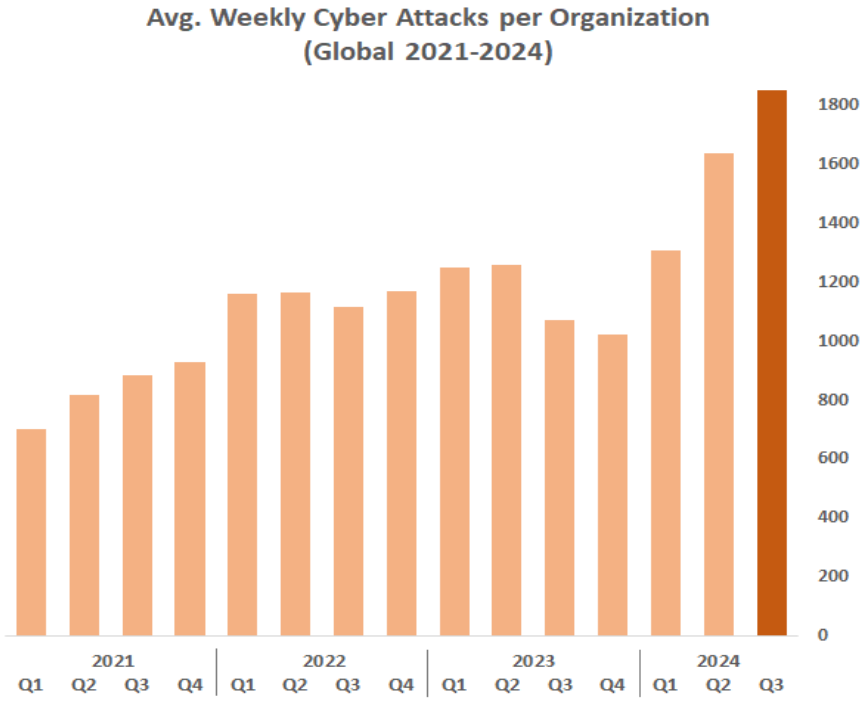

Рис.1. Графік **кількості мережевих атак у середньому на 1 організацію у бізнес-сегменті за різними кварталами починаючи з 2021-го року.**

Динаміка кібератак має інтенсивність до постійного зросту, що демонструється на графіку (рис. 1) [2]. Аналіз статистичних показників останніх 4-х років дає можливість дійти висновку, що рівень кіберзлочинів зріс у двічі, кількість подій щодня вимірюється на орієнтовній позначці у 2200 кібератак [3]. Час виявлення та аналізу місця атаки залишається досить великим, так може тривати до кількох місяців. Особливо популярним та старим методом залишаються атаки через електрону пошту за рахну підробних адресів та хибних посиланнь для крадіжки даних про обліковий засіб. Зазвичай, причинно-наслідковим з'вязком є те, що користувачі за рахунок неуважності чи недбалого ставлення не сприймають підробний лист за загрозу. Особливо вразливим залишається корпоративний сегмент, де засоби мережевої безпеки відсіюють лише малу частину підроблених листів. У першій половині 2025-го року було порушено конфіденційність чи вкрадено даних з 93.6 млн. облікових записів користувачів [4]. Найпопулярнішим вектором атак є використання скомпрометованих облікових засобів за рахунок фішингу. Парадоксальним є те, що кількість та складність загроз виросла непропорційно за рахунок використання засобів ШІ та швидкої автоматизації.

Штучний інтелект у секторі кібербезпеки: Не зважаючи на те, що ШІ доволі давно використовується у секторі безпеки, особливого розвитку він набув на початку 2020-х. У 2000-х роках на практиці почали використовувати алгоритми кластерізації та нейронні мережі для аналізу спаму та мережевого трафіку, У 2010-х роках з'явились перші компанії, які почали інтегрувати ШІ у системи захисту на фоні популяризації хмарних сервісів. Але у 2020-х роках з появою глибинного навчання (Deep learning) відкрився горизонт не тільки для виявлення, а ще й для прогнозування мережевих атак. Характерною ознакою певного прориву стало різке підвищення можливостей ШІ. Це дало змогу у короткі терміни зробити великий обсяг симуляцій з використанням так званих великих мовних моделей (LLM) для автоматизації виявлення загроз та їх прогнозування. У перспективі можливе створення повної автономної системи захисту з можливістю самонавчання та самовдосконалення, ретельного аналізу та прийняття рішення, а особливо важливо – у режимі реального часу, та поєднання у стек з іншими технологіями, доповнюючи переваги одна одної.

Перспективи та результати є багатообіцяючими, але є ряд проблемних аспектів, які сповільнюють розвиток. По-перше, глибинне навчання автономних систем безпеки з використання штучного інтелекту потребує надмірно великої кількості даних, які потрібно оброблювати на надпотужних серверах, що створює очевидну проблему фінансування. Додатково, те, що є характерним для систем захисту, які базуються на сигнатурних базах – хибні спрацювання, усе одно можливі і нікуди не зникнуть. Неможливо створити систему з абсолютним показником ефективності вірних спрацювань. Додатковою проблемою є те, що певні атаки усе одно залишаються не поміченими за рахунок використання методів соціальної інженерії. Навіть передові системи, які базуються на кластерному зборі інформації та створенні матриць поведінки користувачів, усе одно не зможуть виявити приховану атаку, якщо вона не буде випадати з типового сценарію, таким чином зловмисники можуть обійти навіть передові системи захисту, які є зараз. Раніше згаданий парадокс також присутній, коли сучасні системи захисту з ШІ можуть бути обійдені за рахунок використання також штучного інтелекту.

Але проте є і велика кількість переваг, як самостійне тестування та самоаналіз, що веде до постійного розширення бібліотеки сталих сигнатур, так і скорочення часу реагування на невідому атаку і переривання її у максимально короткий термін. Додатково ШІ у перспективі значно спрощує пошук джерела атаки, локалізацію та ізоляцію сегмента мережі, який вже був вражений.

Практичне втілення ідей є у конкретних відомих технологіях, наприклад – Deep Instinct. Технологія використовує інноваційні глибинні нейронні мережі для передбачення кібеатак, крім того, вона стала здатна виявляти абсолютне різноманітне шкідливе програмне забезпечення, та так звані чорні ходи (прогалини у системі безпеки), за рахунок великої кількості годин тренування на шкідливому коді, заявлений час реагування складає 20 мс [5].

Уваги заслуговує Blackberry Cylance UES – система захисту кінцевого типу, яка аналізує процеси та файли у режимі реального часу без використання взагалі будь-яких сигнатур [6]. Велику увагу звертає на себе проект Azure Sentinel, як рішення для корпоративного кіберзахисту. Це система як і збору, так і використання даних для кореляції подій, що дозволяє виявляти складні багатоступеневі масштабні атаки різного рівня та цілей.

У найближчий перспективі почне розвиватися розробка автономних систем захисту на основі нейромережі у поєднанні з блокчейном, на базисі нетипової логіки квантових обчислень, які нівелюють потребу у великих ресурсах для глибинного навчання [7]. Також великий потенціал у підвищенні рівню ефективності використання ШІ за рахунок створення пояснювальних моделей, що дозволяє запобігти так званої чорної скриньки нейромережі, коли кінцеве рішення є непрозорим для розуміння. Інший показник – адаптивність та гнучкість таких засобів захисту.

Ознаки системи захисту нового покоління на основі штучного інтелекту: Такі системи захисту будуть більш «свідомими» та ефективними, та в результаті, будуть мати перелік особливих характеристик на фоні існуючих систем.

Мультизахист та мультикомплекс – одна комплексна система, яка буде залучати у себе апаратні та програмні засоби на місцях, зможе цілеспрямовано охоплювати різні рівні, як логічний мережевий та прикладний, так і фізичний, захищаючи усю мережу в цілому завдяки можливості до масштабування.

Уникнення парадоксу штучного інтелекту – за рахунок реагування у режимі реального часу та зазначених аспектів самонавчання та адаптивності, засоби нового покоління зможуть бути стійкими до атак, створених іншим штучним інтелектом та атак на сам ШІ, як ядро безпеки.

Мультиметричність до самоаналізу – системи нового зразку зможуть базуватись на аналізі багатьох метрик, як інформативні логі, поведінкові матриці, та постійне самотестування для побудови цілостної безпекової картини.

Пояснювальність та проактивність – людське регулювання усе одно потрібне, тому рішення з запобігання атак та їх передбачання повинні бути прозорими. Усі рішення, які приймаються на базисі вхідних даних, повинні бути зрозумілими для можливості зовнішнього впливу, адже автономність не є повним автоматизмом. Особливо це важливо для фактору довіри фахівців, які будуть інтегрувати подібні системи та регулювати їх. Саме тому системи безпеки нового покоління будуть містити моделі-спрощувачі, аналітику ознак та матриці важливості ознак для доступності взаємодії з боку користувача.

Загальний висновок: Ретельно проаналізувавши стан у галузі мережевої безпеки, автори дійшли висновку, що ризик зростання та ускладнення протидії кіберзагрозам є невирішеною проблемою, яка все більш активно впливає на різні показники якості існування людини. Наявність такої проблеми призводить до проблем з інтернет-сервісами, порушує приватність особистої інформації, більш того, призводить до колапсів певних соціальних секторів наприклад, як міжнародні авіаперевезення, сектор державної медицини, тощо, та мають тенденції до безмежного руйнівного впливу. Фінансові звіти є тому підвердженням, кіберзлочинність стала великою проблемою сьогодення і стан справ не має тенденції до покращення.

Сучасні звичайні засоби боротьби з мережевими загрозами якщо і є ефективними, лише перед відомими атаками та засновані на сигнатурних базах, і лише питання часу, коли з’явиться загроза, яка зможе подолати цей бар’єр. Тому зважаючи на важливість вірішення такого складного питання, розвиток нових систем захисту з новою логікою обчислення та застосування штучного інтелекту є надважливим.

Тому у якості загального висновку слід зазначити, що зважаючи на усі тендеції з погіршення ситуації з кіберзлочинністю, розвиток галузі мережевої безпеки, особливо з залученням нових засобів, як штучний інтелект, є неминучім. Створення систем нового покоління є життєвоважливим кроком для мережевого простору та суспільства в цілому. У найбліжчі роки процесс розробки таких систем буде активним з використанням

нетрадиційних підходів у базовій логіці роботи подібних систем, що буде супроводжуватись ще й розвитком інших технологій. Потенційно все призведе до комбінаційного стеку безпеки.

СПИСОК ЛІТЕРАТУРИ

1. “WannaCry ransomware attack”. – URL: https://en.wikipedia.org/wiki/WannaCry_ransomware_attack.

2. “A Closer Look at Q3 2024: 75% Surge in Cyber Attacks Worldwide”. – URL: https://blog.checkpoint.com/research/a-closer-look-at-q3-2024-75-surge-in-cyber-attacks-worldwide.

3. “Data breaches statistics”. – URL: https://blog.xposedornot.com/data-breaches-statistics.

4. “300 Cyber Security Statistics & Trends (Updated August 2025)”. – URL: https://keepnetlabs.com/blog/cyber-security-statistics-and-trends.

5. “Deep Instinct Pioneers Deep-Learning Malware Prevention to Protect Mission Critical Business Applications at Scale”. – URL: https://www.deepinstinct.com/news/deep-instinct-pioneers-deep-learning-malware-prevention.

6. “BlackBerry Cylance vs.Traditional Security Approaches”. – URL: https://s7d2.scene7.com/is/content/cylance/prod/cylance-web/en-us/resources/knowledge-center/resource-library/white-papers/CylanceVsTraditionalSecurityApproaches.pdf.

7. “What is quantum computing?” – URL: https://www.ibm.com/think/topics/quantum-computing.

DOI: https://doi.org/10.15276/ict.02.2025.30
UDC 004.056.5:004.8

Prospects of using artificial intelligence methods and technologies in network security systems

Yevhen H. Birka[1)]
PhD Student of the Department of Computer Systems
ORCID: https://orcid.org/0009-0008-4669-493X, e-mail: rariwe@gmail.com
Oleh V. Streltsov[1)]
PhD, Associate Professor of the Department of Computer Systems
ORCID: https://orcid.org/0000-0002-4691-5703; streltsov.o.v@op.edu.ua
[1)] Odesa Polytechnic National University, 1 Shevchenko Ave. Odesa, 65044, Ukraine

ABSTRACT

Modern challenges in the field of network security require the development of new approaches and the implementation of advanced tools to enhance cybersecurity effectiveness, which is an urgent problem today. Traditional means of countering unauthorized access to private and corporate networks, as well as to cloud and server data storages, which are based on signature methods, are not always effective against new types of network attacks. Therefore, the integration of artificial intelligence (AI) into cybersecurity makes it possible to improve the efficiency of attack detection and mitigation, as well as to develop modern protective solutions that are more effective in terms of quality criteria and compliance with current standards. Global experience of large-scale cybercrimes and ongoing projects integrating AI into network security confirms the prospects of using AI both as a standalone tool and as a part of complex systems combined with other technologies.

Keywords: artificial intelligence,,cybersecurity, machine learning, cyber defense, cyberattack