УДК 004.8(043.2)

О.В. Дубчак, Н.К. Гулак, к.т.н.
(Національний авіаційний університет, Україна)

Застосування AI в завданнях кібербезпеки

Анотація У роботі визначено вплив AI на сучасний стан кібербезпеки; розглянуто використання AI в інструментах кібербезпеки, зокрема таких, як системи виявлення та запобігання вторгненням, що забезпечують комплексний захист мереж від атак; проведено порівняльний аналіз систем IDS і IPS; визначено доцільність їхнього використання, спільні характеристики, переваги та недоліки

Відповідно до прогнозів WEF (The World Economic Forum, Всесвітній Економічний Форум) на найближчі кілька років і десятирічну перспективу, кіберзагрози та кіберінциденти посідатимуть восьме місце серед десяти найсерйозніших глобальних ризиків, таких як зміни клімату чи вимушені міграції. [1]

Зі збільшенням складності кіберзагроз, зокрема, завдяки використанню зловмисниками технологій AI (Artificial intelligence, штучний інтелект), для підтримки високого рівня захисту комунікаційних мереж вирішальне значення має створення ефективних рішень щодо протидії порушенням функціонування мереж і пом'якшення наслідків можливих атак.

Кібербезпека, яка містить у собі протоколи, технології, прилади, інструменти та методи для запобігання загрозам і захисту інформації, що циркулює мережами, є невід'ємною частиною комунікаційних мереж.

Відповіддю сфери кібербезпеки на виклики сучасних кіберзагроз стає впровадження алгоритмів AI щодо проведення: оцінювання ризиків; моніторингу підозрілої мережевої активності; миттєвого реагування на атаки; пошуку вразливостей тощо. Для проведення аналітичних дій з величезними наборами даних (Big Data, великі дані), виявлення певних поведінкових закономірностей або аномалій використовуються алгоритми машинного навчання та системи підтримки прийняття рішень. [2]

Для фахівців із кібербезпеки нагальною потребою стає інвестування в процес упровадження систем AI до механізмів випередження кібератак, у методи проведення яких зловмисники інтегрують алгоритми AI. За даними Spherical Insight & Consulting обсяги світового ринку AI в сфері кібербезпеки до 2032 року мають досягти 90,81 млрд доларів США за сукупного річного темпу зростання у 20,3%. [3]

Проблеми кібербезпеки, з якими щоденно стикаються мережеві адміністратори, не можуть бути успішно вирішені жодним додатком. Незважаючи на те, що захист мережевих пристроїв, контроль доступу та функції міжмережевого екрана є частиною правильно налаштованого убезпечення мережі, це не може гарантувати повноцінного захисту мереж від зловмисницьких впливів, що швидко розповсюджуються та постійно удосконалюються. Мережа має бути здатною миттєво розпізнавати кіберзагрози та зменшувати їхні наслідки.

Ускладненим є і завдання щодо стримування можливого вторгнення у декількох точках мережі, оскільки запобігання вторгненням необхідно у всій мережі для виявлення та зупинення атаки саме в кожній точці входу та виходу.

Задля підвищення ефективності інструментів кібербезпеки в деякі з них інтегруються системи AI, зокрема: міжмережеві екрани; рішення щодо убезпечення кінцевих точок; засоби захисту пристроїв Інтернету речей; системи виявлення та запобігання мережевим вторгненням тощо. [4]

Одним із економічно ефективних варіантів захисту від стрімких атак, що постійно удосконалюються та ускладнюються, є IDS (Intrusion Detection Systems, системи виявлення вторгнень) або більш масштабовані IPS (Intrusion Prevention Systems, системи запобігання вторгненням), в підґрунтя функціонування яких закладено системи AI.

IDS впроваджуються для пасивного моніторингу мережевого трафіку: копіює потік та аналізує відстежуваний трафік, а не фактичні перенаправлені пакети. Працюючи в автономному режимі, система порівнює захоплений потік з відомими шкідливими сигнатурами, аналогічно до програмного забезпечення, яке перевіряє наявність вірусів.

Перевага роботи з копією трафіку: IDS не спричиняє негативного впливу на фактичний потік пакетів трафіку, що пересилається; не впливає на продуктивність мережі, що, в свою чергу, не призводить до затримки або інших проблем трафіку. Крім того, якщо датчик виходить з ладу, це не впливає на функціональність мережі, а лише - на здатність IDS аналізувати дані.

Недолік: IDS не може зупинити шкідливі поодинокі пакети від досягнення пункту призначення, перш ніж надійде відповідь на атаку, для чого IDS часто вимагає допомоги від інших мережевих пристроїв, таких як маршрутизатори та міжмережеві екрани. [5]

Більш оптимальним варіантом убезпечення мережі є реалізація рішення IPS, що виявляє та, за необхідності, негайно усуває мережеву проблему.

Власне, технологія IPS заснована на технології IDS. Але, на відміну від IDS, система IPS реалізована в убудованому режимі, тобто весь вхідний та вихідний трафік проходить через неї для опрацювання. Лише проведення попереднього аналізу системою IPS дозволить пакетам входити в довірену частину мережі. Отже, мережева проблема може бути виявленою та негайно вирішеною.

Перевага роботи в убудованому режимі: IPS може зупинити атаки окремих пакетів до цільової системи. Недолік: неналежним чином налаштована система IPS або недоречне рішення IPS можуть негативно вплинути на потік пакетів трафіку, що пересилається. Крім того, помилки, збої та переповнення датчика IPS надто великим трафіком можуть негативно вплинути на продуктивність мережі. Системі IPS належить мати відповідні розміри та бути реалізованою таким чином, щоб чутливі до часу застосунки, такі як VoIP (Voice over IP, IP-телефонія), не зазнавали негативного впливу.

Системи IDS та IPS мають кілька спільних характеристик, а саме: використовуються як датчики; використовують сигнатури для виявлення випадків небажаного мережевого трафіку, завдяки яким можуть бути виявлені серйозні порушення безпеки, загальні мережеві атаки та збирання інформації;

можуть виявляти атомарні шаблони сигнатур (single-packet, один пакет) або складені шаблони сигнатур (multi-packet, кілька пакетів).

Найсуттєвіша відмінність між IDS та IPS полягає в тому, що IPS відповідає негайно і не пропускає будь-який шкідливий трафік, тоді як IDS може пропускати небажаний трафік до надання належної відповіді. [5]

Слід зазначити, що використання однієї з розглянутих технологій не скасовує використання іншої. Фактично, технології IDS і IPS можуть доповнювати одна одну, коли, наприклад, IDS реалізований для перевірки роботи IPS, оскільки IDS можна налаштувати для більш глибокої перевірки пакетів в автономному режимі, що надає можливість IPS зосередитись на меншій кількості, але більш важливих шаблонів трафіку.

Беззаперечною перевагою IDS і IPS є те, що архітектура мережі інтегрує ці рішення саме в точки входу та виходу мережі.

Висновок

Ураховуючи темпи зростання кількості кіберзагроз із використанням AI, інтеграція систем AI у сферу кібербезпеки стає стратегічним завданням. Підвищуючи можливості виявлення та попередження кіберзагроз, а також зменшуючи час реагування на них, системи AI сприяють перетворенню кібербезпеки в потужний механізм захисту критично важливих активів і об'єктів. Прискіплива увага до вирішення проблем кібербезпеки та захисту інформації забезпечує, крім іншого, і безперервність бізнесу та зводить до мінімуму ефект вторгнень, що можуть призвести до дороговартісних наслідків.

Технології AI, впроваджені в інструменти відстеження мережевого трафіку, такі як IDS і IPS, дозволяють прискорити опрацювання даних з метою виявлення та блокування кібератак.

Список літератури

1. The Global Risks Report 2023 [Електронний ресурс] - Режим доступу: https://www3.weforum.org/docs/WEF_Global_Risks_Report_2023.pdf
2. Гулак Н.К. Алгоритм організації функціонування розподіленої СППР в умовах великого навантаження/Н.К. Гулак, О.В. Дубчак // Scientific Periodical Journal "SWorldJournal" (ISSN 2663-5712, DOI: 10.30888/2663-5712.2024-24-00) / SWorld & D.A. Tsenov Academy of Economics, Svishtov, Bulgaria, - 2024. – Issue 24 (Part 1, March 2024). – P.111 – 119.
3. Global AI in Cybersecurity [Електронний ресурс] - Режим доступу: https://finance.yahoo.com/news/global-artificial-intelligence-cybersecurity-market-130000866.html
4. What is AI for Cyber Security? [Електронний ресурс] - Режим доступу: https://www.microsoft.com/uk-ua/security/business/security-101/what-is-ai-for-cybersecurity#heading-ocafd6
5. Network Security. Cisco Networking Academy [Електронний ресурс] - Режим доступу: https://www.netacad.com/