УДК 004.8:004.056

РОЛЬ ШТУЧНОГО ІНТЕЛЕКТУ ТА МАШИННОГО НАВЧАННЯ У ВИЯВЛЕННІ ТА ЗАПОБІГАННІ АТАКАМ НА БЕЗПРОВІДНІ МЕРЕЖІ ІНТЕРНЕТУ РЕЧЕЙ

Стрименешенко О.С.,
Науковий керівник – д. т. н., проф. Агеєв Д. В.
Харківський національний університет радіоелектроніки
(61166, Харків, пр. Науки, 14, каф. Інфокомунікаційної інженерії ім.Поповського В.В.,
e-mail: oleksandr.strymeneshenko@nure.ua

The modern world is becoming increasingly dependent on Internet of Things (IoT) technologies, which are implemented in various areas of life: from industry to home devices. However, as the IoT grows in popularity, so does the threat to cybersecurity, especially with wireless networks being more vulnerable to attack. We now consider the role of artificial intelligence (AI) and machine learning (ML) in detecting and preventing attacks on IoT wireless networks.

Штучний інтелект (ШІ) та машинне навчання (МН) відіграють важливу роль у забезпеченні кібербезпеки в контексті Інтернету речей (IoT). Вони дозволяють системам автоматично виявляти аномалії, атаки та інші загрози безпеки у безпровідних мережах та вчасно реагувати на них. Ось кілька способів, які використовуються у ролі ШІ та МН для захисту безпровідних мереж IoT:

- Виявлення аномалій. Системи на основі МН виявляють аномалії у безпровідних мережах IoT, аналізуючи трафік та виявляючи відхилення від типових патернів передачі даних. Це досягається за допомогою алгоритмів, які навчаються розпізнавати нормальну поведінку мережі на основі історичних даних. Наприклад, якщо система виявляє, що зазвичай певний пристрій відправляє дані з певною частотою або обсягом, але виявляється зміна у цих параметрах, це може вказувати на підозрілу активність, таку як атака або несанкціонований доступ. Системи виявлення аномалій можуть навіть автоматично навчатися адаптуватися до нових шаблонів поведінки мережі з часом, щоб покращити точність виявлення аномалій;
- прогнозування ризиків. Штучний інтелект (ШІ) використовується для аналізу даних про попередні атаки та аномальні події у безпровідних мережах IoT з метою прогнозування майбутніх ризиків. ШІ може аналізувати великі обсяги даних для виявлення шаблонів та ознак, що передують атакам або іншим загрозам кібербезпеки. Наприклад, якщо історичні дані показують, що певні типи атак зазвичай відбуваються після певних подій або мають певні характеристики трафіку, ШІ може використовувати цю інформацію для прогнозування майбутніх ризиків та розробки ефективних стратегій захисту;

- автоматизована відповідь. Системи на основі ШІ можуть автоматично реагувати на виявлені загрози у безпровідних мережах IoT, забезпечуючи швидку та ефективну відповідь. Це може включати автоматичне блокування атак, ізоляцію вразливих пристроїв або розробку власних стратегій оборони. Наприклад, якщо система виявляє атаку на певний пристрій, вона може автоматично відключити його від мережі, щоб запобігти подальшим атакам або поширенню інфекції.

На сьогоднішній день вже існують різні системи та продукти, які використовують ШІ та МН для захисту безпровідних мереж IoT. Наприклад, Cisco IoT Threat Defense або Darktrace Industrial.

Cisco IoT Threat Defense - це рішення, розроблене компанією Cisco для захисту безпровідних мереж Інтернету речей (IoT) від кіберзагроз. Це комплексна платформа, яка використовує розумний аналіз даних, машинне навчання та штучний інтелект для виявлення, моніторингу та запобігання різним видам кібератак. Ця платформа аналізує трафік у безпровідних мережах IoT з використанням розумних алгоритмів машинного навчання для виявлення аномальних або підозрілих активностей. Вона враховує різні параметри, такі як типова поведінка підключених пристроїв, характеристики трафіку та інші фактори, щоб виявити відхилення від норми, які можуть вказувати на потенційні загрози. Також вона легко інтегрується з іншими рішеннями безпеки Cisco, такими як Cisco Umbrella, Cisco Identity Services Engine та інші. Це дозволяє створити єдину систему безпеки для всієї інфраструктури організації, включаючи безпровідні мережі IoT.[1]

Darktrace Industrial - це рішення з кібербезпеки, призначене для захисту промислових систем та безпровідних мереж Інтернету речей (IoT) від кіберзагроз. Ця платформа використовує штучний інтелект та алгоритми машинного навчання для виявлення аномалій та вчасного реагування на потенційні загрози. Вона є потужним інструментом для захисту промислових систем та безпровідних мереж IoT від кіберзагроз. Її здатність виявляти аномалії, прогнозувати ризики та автоматично реагувати на загрози допомагає забезпечити надійний рівень безпеки в промислових середовищах.

Список використаних джерел:

1. Cisco IoT Threat Defense. (2022). Cisco IoT Threat Defense: Overview. Retrieved from URL: https://www.cisco.com/c/en/us/solutions/collateral/internet-of-things/iot-threat-defense-smart-building-aag.html