Стецюк М.В., PhD, ст. викладач
Заставна Я.В., здобувач
Тімош В.Л., здобувач
Хмельницицький національний університет

СИСТЕМА ПОВЕДІНКОВОГО АНАЛІЗУ ДЛЯ ВИЯВЛЕННЯ ЗАГРОЗ В IOT-МЕРЕЖАХ

Інтернет речей (IoT) швидко змінює спосіб взаємодії людей із технікою, проте водночас стає вразливим до кіберзагроз, таких як DDoS-атаки, експлойти та брутфорс-атаки. Традиційні методи захисту, що базуються на статичних правилах, часто неефективні перед новими загрозами, тому ефективним рішенням є системи виявлення загроз на основі поведінкового аналізу. Вони здійснюють моніторинг активності пристроїв у реальному часі, дозволяючи виявляти аномалії, що можуть свідчити про атаку.[1]

Формування нормального профілю роботи пристроїв є важливим етапом у побудові ефективної системи поведінкового аналізу. Нормальний профіль визначає стандартні параметри функціонування IoT-пристрою та використовується для виявлення аномальних відхилень. Для кожного пристрою формується індивідуальний профіль, що включає його типову активність, середні значення мережевої взаємодії, рівень енергоспоживання, частоту обміну даними та інші показники. Це дозволяє системі адаптуватися до змін у роботі пристроїв без необхідності ручного налаштування для кожного окремого випадку.

Контролерна частина формує нормальний профіль підключеного пристрою, спостерігаючи за його роботою у звичайному режимі. Протягом певного періоду вона збирає дані та створює модель типової поведінки.[2] Ця модель включає такі параметри, як допустимий обсяг трафіку, інтенсивність запитів, рівень споживаної енергії та типові мережеві підключення. Після цього контролер починає порівнювати поточну активність пристрою з нормальним профілем. Якщо значення будь-якого показника виходить за встановлені межі, це вважається потенційною загрозою, і дані передаються на сервер для подальшого аналізу.

Серверна частина використовує отримані від контролера дані для перевірки аномалій і прийняття рішень щодо реагування. Сервер не лише перевіряє отримані показники на відповідність нормальному профілю, а й проводить аналіз за допомогою алгоритмів поведінкового моделювання.[4] Якщо аномалія підтверджується, сервер ініціює відповідні заходи безпеки, такі як генерація сповіщення, блокування підозрілого пристрою або оновлення політик контролера. Використання серверних обчислень дозволяє швидко обробляти великі обсяги даних і виявляти складні загрози, які можуть залишатися непомітними на рівні окремих пристроїв.

Контролерна частина виконує первинний аналіз та передає підозрілі події на сервер. Її робота включає кілька основних етапів. Спочатку контролер здійснює збір параметрів пристрою, включаючи рівень енергоспоживання, мережеві підключення та структуру переданого трафіку. Далі отримані дані порівнюються з нормальним профілем пристрою. Якщо значення параметрів виходять за межі встановлених норм, система визначає рівень відхилень і оцінює, чи є вони критичними.[5] У разі виявлення підозрілої активності контролер передає відповідні дані на сервер для подальшого аналізу. Після завершення аналізу сервер надсилає оновлені політики безпеки, які контролер інтегрує у свою роботу. Це дозволяє забезпечити адаптивний захист та динамічне оновлення норм поведінки пристроїв. На рисунку 1 представлено алгоритм роботи контролерної частини

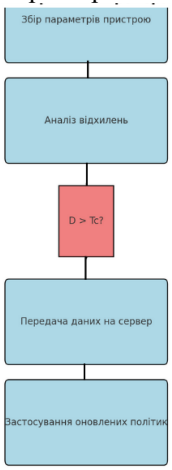

Рис. 1. Алгоритм роботи конролерної частини системи виявлення загроз

Серверна частина відповідає за глибший аналіз отриманих даних та прийняття рішень щодо можливих загроз. Після отримання інформації від контролера сервер застосовує алгоритми поведінкового аналізу для перевірки можливих аномалій. Якщо відхилення підтверджується, система генерує тривожний сигнал та ініціює заходи безпеки. Це може включати блокування пристрою, обмеження його мережевої активності або оновлення безпекових правил для всіх контролерів у системі. Сервер також веде журнал загроз, що дозволяє проводити подальший аналіз атак та вдосконалювати алгоритми виявлення аномалій.

На рисунку 2 представлено блок-схему алгоритму роботи серверної частини.

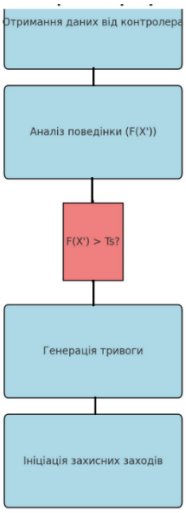

Рисунок 2 – Алгоритм роботи серверної частини системи виявлення загроз

Контролерна та серверна частини працюють у взаємодії через захищений канал зв’язку, що дозволяє здійснювати безперервний моніторинг і реагування на потенційні загрози. Контролери збирають дані та передають їх на сервер, який аналізує ситуацію і приймає рішення про необхідність втручання. Завдяки такій архітектурі система забезпечує виявлення та блокування загроз у режимі реального часу без необхідності попереднього знання про конкретний тип атак.

Список використаних джерел:

1. Булдаков О. В., Ковальов Г. П. Методи виявлення аномалій у трафіку IoT-пристроїв. *Комп’ютерні системи та мережі*. 2021. Т. 49, № 2. С. 112–121.
2. Anderson J., McCarthy B. Behavioral Analysis for IoT Security. *Journal of Cybersecurity Research*. 2020. Vol. 7, No. 1. P. 88–97.
3. Марченко Р. М., Коваленко А. А., Знайдюк В. Г. Аналіз методів виявлення аномального трафіку в мережах IoT. *Системи управління, навігації та зв'язку*. 2024. №1. С. 133–140.
4. IoT Analytics. State of IoT—Spring 2022. *IoT Analytics*. 2022. URL: https://iot-analytics.com/product/state-of-iot-spring-2022 (дата звернення: 10.03.2024).