Фігурняк В.Р., гр. КІСП-22
Науковий керівник – Пуйда В.Я.

Програмна система виявлення та запобігання атак у розумному будинку

Стан проблеми. Розумні будинки стають все більш популярними завдяки зручності автоматизації побутових процесів та енергоефективності. Однак зростання кількості підключених IoT-пристроїв створює нові вектори кібератак [1]. Основними загрозами є несанкціонований доступ до системи, DDoS-атаки, перехоплення даних та компрометація приватності користувачів. Дослідження показують, що понад 560 тисяч IoT-пристроїв є вразливими до атак через слабкі паролі та відсутність належного захисту [1].

Традиційні методи захисту, розроблені для класичних мереж, часто неефективні для екосистем розумних будинків через обмежені обчислювальні ресурси пристроїв, гетерогенність протоколів зв'язку та динамічну топологію мережі. Оскільки сучасні системи розумного будинку підключені до Інтернету, атаки можуть проводитися дистанційно або за допомогою прямого доступу до мережевих інтерфейсів управління [2]. Це актуалізує потребу у спеціалізованих системах безпеки, адаптованих до особливостей IoT-середовища.

Постановка задачі. Розробити програмну систему виявлення та запобігання атак для екосистеми розумного будинку, яка здатна в реальному часі аналізувати мережевий трафік, виявляти аномальну поведінку пристроїв та автоматично реагувати на потенційні загрози. Система повинна забезпечувати мінімальний вплив на продуктивність IoT-пристроїв, підтримувати найпоширеніші протоколи зв'язку (MQTT, Zigbee, Z-Wave, Wi-Fi) та надавати зручний інтерфейс моніторингу для користувача. Розробити алгоритм класифікації загроз та механізм автоматичного реагування на інциденти безпеки з використанням методів машинного навчання [3].

Розв'язання задачі. Розроблена система базується на гібридному підході до виявлення загроз, що поєднує сигнатурний аналіз та методи машинного навчання для детекції аномалій. Архітектура системи включає три основні компоненти: модуль збору даних, модуль аналізу та модуль реагування.

Модуль збору даних здійснює моніторинг мережевого трафіку через центральний шлюз розумного будинку, використовуючи бібліотеку Scapy для перехоплення пакетів. Система збирає метадані про з'єднання, частоту запитів, обсяги переданих даних та профілі поведінки кожного пристрою. Реалізовано безперервний моніторинг мережі для виявлення незвичних подій або тенденцій у реальному часі [4].

Модуль аналізу реалізовано з використанням алгоритму Isolation Forest для виявлення аномалій у поведінці пристроїв. Алгоритми машинного навчання можуть аналізувати великі обсяги даних і виявляти аномалії швидше й точніше, дозволяючи організаціям швидко реагувати на потенційні загрози [5]. Додатково застосовується база сигнатур відомих атак (CVE для IoT-пристроїв), що забезпечує швидке розпізнавання типових загроз. Система аналізує наступні параметри: відхилення від нормального трафіку, спроби доступу до незвичайних портів, підозрілу частоту запитів, аномальне споживання ресурсів.

Використання методів глибинного навчання стало ключовим компонентом систем виявлення вторгнень, оскільки ідентифікація шкідливого трафіку дозволяє виявляти як відомі, так і раніше невідомі загрози [3]. Система відслідковує критичні характеристики мережі, включаючи обсяг трафіку, використання смуги пропускання та використання протоколів [4].

Модуль реагування забезпечує автоматичні відповіді на виявлені загрози відповідно до визначеного рівня критичності. Для високоризикових інцидентів застосовується ізоляція скомпрометованого пристрою від мережі, для середнього рівня загроз -- обмеження пропускної здатності або блокування специфічних з'єднань. Користувач отримує сповіщення через мобільний додаток з детальною інформацією про інцидент та рекомендаціями.

Програмна реалізація виконана на мові Python з використанням фреймворку Flask для веб-інтерфейсу та бібліотеки scikit-learn для алгоритмів машинного навчання. Система розгорнута на одноплатному комп'ютері Raspberry Pi 4, що виконує функції захищеного шлюзу. Використано основні способи захисту інформації, що доцільно впроваджувати в мережах розумного будинку - VPN, брандмауер, ACL та паролі для надійного захисту [6].

Для верифікації системи розроблено тестове середовище, що імітує екосистему розумного будинку з 15 IoT-пристроїв. Проведено тестування з використанням набору атак: брутфорс-атаки на автентифікацію, DDoS-атаки, MITM-атаки та експлуатація відомих вразливостей.

Експериментальні дослідження показали наступні результати:

Таблиця 1. Ефективність виявлення атак

Тип атаки	Точність виявлення, %	Час реакції, с
Брутфорс	98.5	0.3
DDoS	96.2	0.8
MITM	94.7	1.2
Експлуатація вразливостей	92.3	0.5
Аномальна поведінка	89.1	1.5

Система продемонструвала низький рівень хибнопозитивних спрацювань (4.2%) та мінімальний вплив на продуктивність мережі (додаткова затримка не перевищує 15 мс). Навантаження на процесор шлюзу в режимі активного моніторингу становить 18-22%.

Висновки. Розроблена програмна система виявлення та запобігання атак забезпечує ефективний захист екосистеми розумного будинку від широкого спектру кіберзагроз. Гібридний підхід, що поєднує сигнатурний аналіз та методи машинного навчання, дозволяє виявляти як відомі, так і нові типи атак. Система характеризується високою точністю детекції, низьким рівнем хибних спрацювань та мінімальним впливом на продуктивність мережі, що підтверджує її практичну придатність для реальних умов експлуатації.

Література

1. Бєлова А., Оніщенко В. Методи забезпечення безпеки розумного будинку // Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка». -- 2019. -- №2(6). -- С. 134-141.

2. Загрози і вразливості безпеки розумного будинку / Всеукраїнська практично-пізнавальна інтернет-конференція. [Електронний ресурс]. -- Режим доступу: https://naukam.triada.in.ua

3. Кочергіна І.О., Курбанова Е.І. Виявлення мережевих аномалій з використанням алгоритмів нейронних мереж // Телекомунікаційні та інформаційні технології. -- 2023. -- №2. -- С. 87-94.

4. Виявлення аномалій у мережевій поведінці [Електронний ресурс] // Вікіпедія. -- Режим доступу: https://uk.wikipedia.org/wiki/Виявлення_аномалій_у_мережевій_поведінці

5. Машинне навчання для виявлення аномалій у кібербезпеці [Електронний ресурс]. -- TS2 SPACE, 2023. -- Режим доступу: https://ts2.space/uk/

6. Захищена система розумного будинку з використанням Internet of Things / Репозиторій Національного університету. [Електронний ресурс]. -- Режим доступу: http://ir.stu.cn.ua/handle/123456789/21279