Крім того, модульна архітектура розробленого рішення дозволяє нарощувати пропускну здатність кластера або підмінювати окремі компоненти (наприклад, додати контрастивний препроцесинг чи LLM-класифікатор) без переробки всієї системи. У тестовій інфраструктурі з навантаженням понад 300 000 запитів/хв. рішення зберегло стабільний час реакції, а кількість хибнопозитивів залишилася нижчою, ніж у класичних сигнатурних або чисто частотних методів. Таким чином, запропонована система відповідає сучасним вимогам до реального сектору: швидке розгортання, пояснювані результати й можливість поступово інтегрувати більш складні ML-та DL-модулі у міру розвитку загроз.

1. Verizon. 2024 Data Breach Investigations Report. New York : Verizon, 2024. 114 p.
2. Cost of a Data Breach Report 2024. USA : IBM Security, 2024. 87 p.
3. Barr J. Access Logs for Elastic Load Balancers [Electronic resource]. AWS News Blog. 2014. Access mode: https://aws.amazon.com/blogs/aws/access-logs-for-elastic-load-balancers/ (date of access: 22.04.2025).

Використання NetLogo для моделювання кібератак на IoT системи

УДК 004.2

Юрій Підлісний
Національний університет «Чернігівська політехніка», ypodlesny@ukr.net

Інтернет речей (IoT) є однією з найбільш перспективних технологій сучасності, що знаходить застосування у розумних містах, промислових системах та охороні здоров'я. Проте зростаюча кількість IoT-пристроїв робить їх привабливою ціллю для зловмисників. Одним з ефективних методів аналізу вразливостей IoT-мереж є мультиагентне моделювання, яке дозволяє досліджувати динаміку атак і механізми їхнього виявлення.

У цій статті розглядається використання NetLogo для моделювання кібератак на IoT [1].

Модель у NetLogo створена для симуляції взаємодії між різними агентами в мережі IoT, зокрема пристроями, хакерами та захисниками [2]. Вона включає три основних *типи агентів:*

- *Пристрої (devices)* – елементи IoT-мережі, які можуть бути вразливими до атак.
- *Хакери (hackers)* – атакувальні агенти, що намагаються інфікувати пристрої.
- *Захисники (defenders)* – агенти, які виявляють і нейтралізують загрози.

Агенти мають наступні властивості:

Пристрої (devices):

- infected? – статус пристрою (інфікований чи ні).
- security-level – рівень безпеки (від 0 до 100).
- update-readiness – готовність до оновлень, що покращують захист.

Хакери (hackers):

- attack-power – потужність атаки, що визначає ефективність зламування пристроїв.
- preferred-target – стратегія вибору цілі, яка може бути спрямована на пристрої з низьким рівнем захисту або на критично важливі елементи мережі.

Захисники (defenders):

- detection-radius – радіус виявлення загроз.
- response-time – час реакції на атаку.

Візуалізація моделі представлена на Рисунку 1:

1) *Пристрої (Devices):*Вони відображаються як зелені квадрати (або прямокутники).
2) *Хакери (Hackers):*Хакери відображаються як червоні фігури людини.
3) *Захисники (Defenders):*Захисники відображаються як блакитні кола.

Опис взаємодії агентів: Пристрої можуть рухатися по мережі (повертатися і рухатися вперед, а хакери здійснюють атаки на пристрої з низьким рівнем безпеки або пристрої, що мають високу цінність. Захисники намагаються знайти інфіковані пристрої в радіусі своєї виявлення і відновити їх.

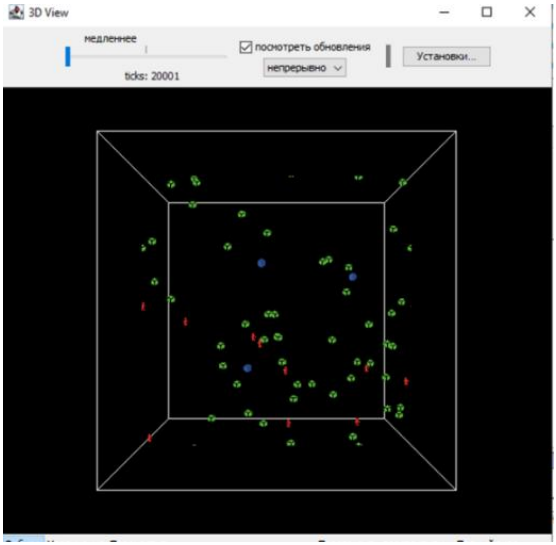

Рис 1. Візуалізація кібератаки на мережу IoT за допомогою NetLogo

Зміни в кольорі:

- *Зелені пристрої* — це здорові пристрої, які не інфіковані.
- *Червоні пристрої* — це пристрої, які були інфіковані хакерами.
- *Червоні хакери* — ці агенти здійснюють атаки на пристрої.
- *Сині захисники* — вони працюють на відновлення пристроїв.

У процесі симуляції ми бачимо як хакери атакують пристрої, як захисники реагують на ці атаки, і як пристрої можуть оновлюватися, щоб підвищити свій рівень захисту. Така 3D візуалізація допомагає краще уявити, як ці агенти працюють в реальному часі, спостерігаючи за змінами в мережі і рухами агентів, що дає вам наочне розуміння того, як працює механізм атаки та захисту.

1. Alrawi, C. Lever, M. Antonakakis, F. Monrose, Security of the Internet of Things: Vulnerabilities, Attacks and Countermeasures. November 2019IEEE Communications Surveys & Tutorials 22(1):616-644 DOI:10.1109/COMST.2019.2953364

2. Seth Tisue, Uri Wilensky. NetLogo: Design and Implementation of a Multi-Agent Modeling Environment. Center for Connected Learning and Computer-Based Modeling Northwestern University, Evanston, Illinois,

Розробка алгоритму детекції шкідливого програмного забезпечення на основі поведінкового аналізу

УДК 004.056.5 (043.2)

Артем Повозніков[1], Наталья Козаченко [2]

Національний університет «Одеська Політехніка»,

[1]9560415@stud.op.edu.ua, [2]kozachenko.n.h@op.edu.ua

В умовах стрімкого зростання кількості та складності кіберзагроз традиційні антивірусні рішення стають менш ефективними. Це обумовлює потребу у впровадженні нових методів виявлення шкідливого програмного забезпечення (ШПЗ), зокрема заснованих на поведінковому аналізі.

Мета роботи – розробка алгоритму детекції ШПЗ, який базується на аналізі аномальної поведінки програм, а не лише на сигнатурних базах.

Сигнатурні антивірусні системи залежать від оновлення баз даних загроз і часто не здатні розпізнати нові або модифіковані варіанти шкідливих програм. Натомість поведінковий аналіз орієнтується на виявлення відхилень у звичних сценаріях роботи програм, таких як аномальні зміни реєстру, нетипові запити до мережі або небажаний доступ до критичних системних ресурсів. У рамках дослідження розглянуто існуючі методи детекції шкідливого ПЗ(таблиця 1).

Таблиця 1

Порівняння методів детекції шкідливого програмного забезпечення

Критерій/ Метод	**Сигнатурний аналіз**	**Евристичний аналіз**	**Поведінковий аналіз**	**Машинне навчання**
Виявлення нових загроз	Низьке	Середнє	Високе	Високе
Рівень хибних спрацьовувань	Низький	Середній	Середній	Може бути високим