УДК 332.1

М. В. Гаврилов, здобувач третього (освітньо-наукового) рівня вищої освіти
Тернопільський національний технічний університет ім. І. Пулюя, Україна
Науковий керівник: І. С. Скарга-Бандурова, докт.техн.наук, проф.

ВИЯВЛЕННЯ ЗАГРОЗ В ІОТ ПРИСТРОЯХ: ВИКЛИКИ ТА СУЧАСНІ ПІДХОДИ

M. Havrylov, the third (educational and scientific) level of higher education applicant
Ternopil Ivan Puluj National Technical University, Ukraine
I. Skarga-Bandurova, Dr.Sc., Prof., scientific supervisor

THREAT DETECTION IN IOT DEVICES: CHALLENGES AND MODERN APPROACHES

Інтернет речей є однією з ключових складових цифрової трансформації сучасного суспільства. Ця технологія інтегрує фізичні пристрої, датчики, програмне забезпечення та мережеві технології в єдину екосистему, що дозволяє автоматизувати процеси, підвищувати ефективність роботи та надавати нові сервіси у різних галузях, таких як охорона здоров'я, промисловість, транспорт, «розумні» міста та сільське господарство. Проте стрімке впровадження IoT супроводжується значними викликами у сфері інформаційної безпеки, що зумовлює необхідність розробки сучасних технологій для виявлення загроз.

IoT пристрої є привабливою ціллю для зловмисників через їхні численні уразливості. Серед основних проблем – недостатній рівень захисту даних, обмежені ресурси для впровадження традиційних механізмів безпеки, а також висока гетерогенність екосистем. Найбільш поширеними загрозами є атаки на конфіденційність даних, перехоплення або несанкціонований доступ до інформації, атаки типу DoS/DDoS, які виводять пристрої з ладу через перенавантаження системи, використання зловмисного програмного забезпечення для створення ботнетів, а також маніпуляція фізичними процесами, що може призвести до серйозних наслідків, таких як аварії в промисловості. [1]

Для забезпечення захисту IoT пристроїв активно розробляються сучасні технології виявлення загроз. Одним із найбільш перспективних підходів є використання систем на основі штучного інтелекту, які дозволяють аналізувати великі обсяги даних у реальному часі, виявляючи аномалії в поведінці пристроїв. Методи аналізу поведінки із застосуванням машинного навчання дозволяють визначати відхилення від звичайного трафіку пристроїв. Системи виявлення вторгнень моніторять мережевий трафік для ідентифікації підозрілих дій, а технології на основі великих даних аналізують потоки інформації, виявляючи шаблони, характерні для атак. Важливим напрямом є також використання блокчейну, який забезпечує захист даних та підтвердження автентичності транзакцій у розподілених IoT екосистемах. [2]

Разом із тим, впровадження цих технологій супроводжується значними викликами. Зокрема, обмежені апаратні ресурси більшості IoT пристроїв ускладнюють реалізацію складних алгоритмів шифрування та аналізу поведінки. Відсутність стандартизації та висока гетерогенність пристроїв перешкоджають створенню універсальних рішень, а масштабування систем безпеки стає дедалі складнішим через зростання кількості пристроїв.

Майбутнє IoT безпеки лежить у розробці гібридних систем виявлення загроз, які поєднують методи машинного навчання, блокчейн і традиційні підходи до інформаційної безпеки. Важливу роль відіграє також створення глобальних стандартів захисту, що враховують специфіку IoT пристроїв та мереж. Інтеграція ефективних технологій захисту є критично важливою не лише для зменшення ризиків для користувачів, але й для забезпечення стабільного розвитку цифрової економіки в умовах глобальної цифровізації. [3]

Одним із перспективних напрямів є створення децентралізованих систем виявлення загроз, що комбінують штучний інтелект із розподіленими технологіями, такими як блокчейн. Це дозволяє уникнути централізованих точок відмови, забезпечуючи високу

надійність і прозорість роботи систем. Крім того, нові стандарти в галузі IoT безпеки, такі як ISO/IEC 30141, спрямовані на вирішення проблем, пов'язаних із масштабуванням захисту пристроїв у гетерогенних екосистемах.

Варто також зазначити, що освітні кампанії та підвищення обізнаності користувачів щодо основ безпеки IoT мають суттєвий вплив на зменшення ризиків. Наприклад, дослідження показали, що правильна конфігурація пристроїв та оновлення їх програмного забезпечення можуть знизити ризик атак на 45% [2]. Таким чином, індивідуальний підхід до забезпечення безпеки, який включає як технологічні, так і організаційні заходи, є ключем до успішного управління загрозами.

Інтеграція ефективних технологій захисту є критично важливою не лише для зменшення ризиків для користувачів, але й для забезпечення стабільного розвитку цифрової економіки в умовах глобальної цифровізації. Тільки завдяки комплексному підходу, який включає інноваційні технології, стандартизацію та просвітницьку діяльність, можна забезпечити безпеку IoT пристроїв і впевнено рухатись до майбутнього цифрового суспільства. Одним важливим аспектом забезпечення безпеки IoT є розвиток методів активного моніторингу загроз у реальному часі. Використання алгоритмів обчислювального інтелекту, зокрема глибокого навчання, дозволяє автоматично ідентифікувати не лише відомі типи атак, але й раніше невідомі загрози. Наприклад, аналіз поведінкових моделей пристроїв у поєднанні з аналізом мережевого трафіку створює можливість для динамічної адаптації захисних систем. Такий підхід дозволяє значно скоротити час реакції на атаки та знизити ризик їхнього поширення в межах IoT екосистем.

Література

1. Abomhara, M., & Køien, G. M. (2015). Security and privacy in the Internet of Things: Current status and open issues. Computers & Security, 52, 1-25.
2. Sicari, S., Rizzardi, A., Grieco, L. A., & Coen-Porisini, A. (2015). Security, privacy and trust in Internet of Things: The road ahead. Computer Networks, 76, 146-164.
3. Alaba, F. A., Othman, M., Hashem, I. A. T., & Alotaibi, F. (2017). Internet of Things security: A survey. Journal of Network and Computer Applications, 88, 10-28.