

БЕЗОПАСНОСТЬ ПЕРЕДАЧИ ДАННЫХ ДЛЯ УСТРОЙСТВ ИНТЕРНЕТА ВЕЩЕЙ
DATA TRANSFER SECURITY FOR INTERNET OF THINGS DEVICES

УДК 654.9: 656.05

СОРОКИН Иван Александрович (кандидат технических наук), **ЧЕСНОКОВ Александр Дмитриевич**,
РОМАНОВ Павел Николаевич, **ГАНИН Дмитрий Владимирович** (кандидат экономических наук),
ШАХТАНОВ Сергей Валентинович (кандидат технических наук)
(Нижегородский государственный инженерно-экономический университет)

Анализ, классификация и методы обнаружения атак в беспроводных сенсорных сетях являются важными аспектами обеспечения их безопасности. Анализ атак включает в себя анализ уязвимостей сети и устройств, которые могут быть использованы для атаки.

Классификация атак может быть основана на их характеристиках (пассивные или активные) и на целях (конфиденциальность данных или доступность сети). Это помогает определять специфические методы обнаружения вторжения и защиты от них.

Методы обнаружения атак включают использование правил, определяющих аномальное поведение сети, использование интеллектуальных алгоритмов машинного обучения для обнаружения аномалий в поведении узлов и сети.

В статье исследуются общие аспекты, влияющие на безопасность Интернета вещей в существующих и перспективных сетях, включая проблемы, ориентированные на человека и механизмы. Выделены основные сферы, оказывающие влияние на безопасность Интернета вещей в современных беспроводных сетях, включая новые отрасли хозяйствования, такие как сфера ЖКХ, энергетика, транспорт и относительно пока слабо развитое в сфере цифровизации сельское хозяйство. Предлагаются возможности исследования в области конфиденциальности и безопасности Интернета вещей для следующего поколения сетевых технологий.

Analysis, classification and methods for detecting attacks in wireless sensor networks are important aspects of ensuring their security. Attack analysis involves analyzing the vulnerabilities of the network and devices that can be used for attack.

The classification of attacks can be based on their characteristics (passive or active attacks) and on the attack targets (data confidentiality or network availability). This helps define specific intrusion detection and defense methods.

Attack detection methods include the use of rules that define anomalous network behavior, the use of intelligent machine learning algorithms to detect anomalies in the behavior of nodes and the network.

The article examines the general aspects affecting the security of the Internet of Things in existing and future networks, including human- and machine-centric issues. The main areas that influence the security of the Internet of things in modern wireless networks are identified, including new sectors of the economy, such as housing and communal services, energy, transport and agriculture, which is still relatively poorly developed in the field of digitalization. Research opportunities in the areas of Internet of Things privacy and security are proposed for the next generation of networking technologies.

Ключевые слова: информационная безопасность, беспроводная сенсорная сеть, сетевые атаки, обнаружение сетевых атак, система обнаружения вторжений.

Keywords: information security, wireless sensor network, network attacks, network attack detection, intrusion detection system.

Литература

1. Верещагина Е.А., Капецкий И.О., Ярмонов А.С. Проблемы безопасности Интернета вещей: Учебное пособие. — М.: Мир науки. 2021. С. 35 — 47.
2. Обзор интернета вещей. Рекомендация МСЭ-Т Y.2060./ Серия Y: Глобальная информационная инфраструктура, аспекты протокола Интернет и сети последующих поколений. Сети последующих поколений. Структура и функциональные модели архитектуры. 06/2021. [Электронный ресурс]. Дата обращения: 28.08.2023 г.
3. Росляков А.В., Ваняшин С.В., Гребешков А.Ю. Интернет вещей: Учебное пособие по направлению подготовки “Инфокоммуникационные технологии и системы связи”. — Самара: ПГУТИ. 2015. 136 с.
4. Цветков В.Я. Интернет вещей как глобальная инфраструктура для информационного общества// Современные технологии управления. 2017. № 6. С. 28.
5. Ярмонов А.С., Остяков А.В. Использование протокола маршрутизации для обеспечения безопасности сенсорной сети/ Материалы региональной научно-практической конференции студентов, аспирантов и молодых ученых по естественным наукам. Владивосток. 11 — 30 апреля 2017 г. — Владивосток: Дальневосточный федеральный университет. 2017. С. 76 — 78.
6. Затраты государства и бизнеса в РФ на внедрение М2М и IoT составили почти 114 млрд рублей/ ТАСС. 21 февраля 2023. [Электронный ресурс]. Дата обращения: 28.08.2023 г.
7. Исакова Т. 41,6 млрд могут вложить в российские технологии интернета вещей/ Ведомости. 22 марта 2021. [Электронный ресурс]. Дата обращения: 28.08.2023 г.
8. Вещам заморозили поддержку/ Коммерсантъ. 30.11.2023. [Электронный ресурс]. Дата обращения: 28.08.2023 г.