

ИНТЕРНЕТ ВЕЩЕЙ (IOT): ВОЗМОЖНОСТИ И УГРОЗЫ

Пидгурская Е.С., студент 3 курса факультет технологии и
оборудования машиностроительных производств
Научный руководитель - Пидгурский С.Н. гл. метролог УУАЗ
ФГБОУ ВО «ИРНИТУ»

Ключевые слова: интернет вещей, IoT, архитектура интернета вещей

Интернет вещей (IoT) — это сеть объектов с датчиками и ПО, позволяющими обмениваться данными. Он изменяет взаимодействие людей с миром, но угрожает безопасности и приватности

Введение. Интернет вещей (IoT) объединяет миллиарды физических объектов с сенсорами и программным обеспечением для обмена данными и принятия решений в реальном времени. IoT находит применение в различных отраслях, включая умные дома, города, промышленность и здравоохранение.

Однако с ростом популярности технологий IoT возникают серьезные угрозы, такие как уязвимости в безопасности, проблемы с конфиденциальностью данных и риск кибератак. Понимание возможностей и рисков IoT является ключевым для успешной интеграции этой технологии в повседневную жизнь и бизнес.

Целью данной работы является анализ возможностей и угроз, связанных с использованием IoT-устройств, а также оценка безопасности конкретного устройства — умного термостата. Мы стремимся выявить, как такие устройства могут улучшить качество жизни пользователей и какие меры предосторожности необходимо принимать для защиты их данных [1].

Результаты исследования

1. Возможности IoT:

- Умные дома: Устройства IoT, такие как термостаты и системы безопасности, позволяют удаленно управлять домом, что способствует экономии энергии и повышению комфорта.

- **Здравоохранение:** Умные часы и фитнес-трекеры помогают пользователям отслеживать здоровье в реальном времени, улучшая качество медицинского обслуживания [2].

- **Умные города:** IoT оптимизирует городскую инфраструктуру, улучшая управление ресурсами и транспортом.

- **Промышленность 4.0:** В производстве IoT повышает эффективность процессов и предотвращает сбои оборудования.

2. Угрозы IoT:

- **Безопасность данных:** Слабая защита устройств делает их уязвимыми для хакерских атак.

- **Приватность:** Сбор данных о пользователях может привести к нарушениям приватности.

- **Отказ в обслуживании (DoS):** Атаки могут отключить критически важные системы [3].

- **Зависимость от технологий:** Чрезмерная зависимость от устройств может вызвать проблемы при их сбое.

3. Практическая часть:

- Проведено исследование умного термостата с акцентом на его возможности и безопасность.

- Оценены функции автоматического регулирования температуры и удаленного управления.

- Проведены тесты на уязвимость и проверка настроек безопасности.

Выводы

- Умные термостаты значительно упрощают управление температурой в доме и могут привести к экономии энергии.

- Тем не менее, они представляют собой потенциальную угрозу для безопасности и приватности пользователей, если не принять соответствующие меры предосторожности.

- Важно не только пользоваться преимуществами IoT-устройств, но и быть осведомленным о рисках и способах их минимизации. Принятие мер по обеспечению безопасности данных является необходимым условием для безопасного использования технологий IoT.

Библиографический список:

1. Довгаль Виталий Анатольевич, Довгаль Дмитрий Витальевич Интернет вещей: концепции, приложения и задачи // Вестник Адыгейского государственного университета. Серия 4: Естественно-математические и технические науки. 2018. №1 (212). URL: <https://cyberleninka.ru/article/n/internet-veschey-kontseptsiya-prilozheniya-i-zadachi>(дата обращения: 06.02.2025).
2. Утегенов Н. Б. Интернет вещей (iot) и информационные системы // Universum: технические науки. 2023. №7-1 (112). URL: <https://cyberleninka.ru/article/n/internet-veschey-iot-i-informatsionnye-sistemy> (дата обращения: 06.02.2025).
3. Шилина М.Г. Интернет коммуникация в инфосфере: Монография. - Москва: 2013. - 231 с. (дата обращения: 06.02.2025).

INTERNET OF THINGS (IOT): OPPORTUNITIES AND THREATS

Pidgurskaya E.S.

Scientific supervisor - Pidgurskiy S.N.

IRNITU

Keywords: *Internet of Things, IoT, IoT architecture, IoT vision, WSN*

The Internet of Things (IoT) is a network of objects equipped with sensors and software that enable data exchange. It transforms the way people interact with the world but poses threats to security and privacy.