

УДК 004.75

Б. О. ПАЛКОВСКИЙ (ЭС-31), *К. АДИБ МЕНЬКОВА* (МТ-56)

Научные руководители: ст. преп. *С. В. КИСЕЛЁВА*,

канд. техн. наук *В. О. МАТУСЕВИЧ*

МОДЕЛИРОВАНИЕ РАБОТЫ СЕТЕВЫХ УСТРОЙСТВ «ИНТЕРНЕТ ВЕЩЕЙ» (IoT)

Выполнен анализ архитектуры и принципов функционирования систем «Интернета вещей». Проведено имитационное моделирование автономной системы «Умный дом» с использованием шлюза. Рассмотрен стандарт связи NB-IoT, а также актуальные вопросы кибербезопасности IoT-устройств. Изучен вопрос кибербезопасности.

Концепция Интернета вещей (IoT) подразумевает подключение повседневных объектов и устройств к Интернету для сбора и обмена данными, что наделяет их свойствами «smart». Архитектура IoT включает в себя несколько уровней:

1 Уровень восприятия (Physical/Device Layer): «физический уровень», состоящий из датчиков, сенсоров и исполнительных механизмов, которые собирают данные (температура, влажность, движение) из окружающей среды.

2 Сетевой уровень (Network Layer): отвечает за безопасную передачу собранных данных в облако или на сервер.

3 Периферийный уровень (Edge/Gateway Layer): промежуточный уровень, где данные проходят первичную обработку (фильтрацию) ближе к источнику, прежде чем попасть в облако.

4 Уровень обработки/Облака (Processing/Cloud Layer): мощная платформа, где данные хранятся, анализируются и обрабатываются с помощью машинного обучения для принятия решений.

5 Прикладной уровень (Application Layer): конечный уровень, с которым взаимодействует пользователь: мобильные приложения, панели мониторинга и интерфейсы управления системами.

Классическое представление IoT системы – это «умный дом».

Умный дом – автономная система управления домом, способная принимать некоторые решения без участия человека. В дальнейшем рассмотрим пример автоматической системы полива и охлаждения помещения.

Концепция умного дома будет использована для опыта моделирования в Cisco Packet Tracer (рисунок 1).

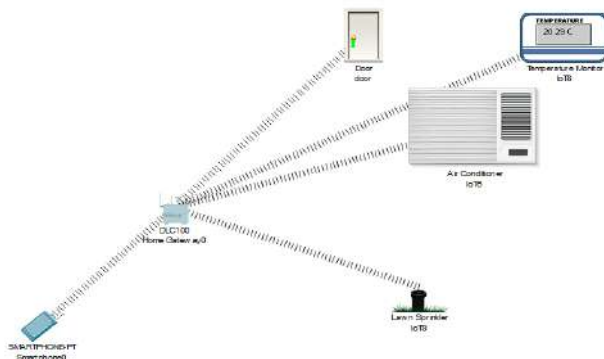


Рисунок 1 – Модель «Умный дом»

Модель (см. рисунок 1) включает в себя: уровень восприятия, состоящий из полива (Lawn Sprinkler), дверь (Door), кондиционер (Air Conditioner), монитор температуры (Temperature Monitor); периферийный уровень и уровень обработки, представленный шлюзом (DLC100) (рисунок 2); прикладной уровень представлен через смартфон (SMARTPHONE PT).



Рисунок 2 – Шлюз

В современных «умных домах» взаимодействие с прикладным уровнем осуществляется в основном через шлюз (см. рисунок 2) посредством голосового ввода, но и также допускается управление через персональное устройство.

Шлюз, представленный в примере, способен поддерживать различные форматы экосистем IoT (Apple, Яндекс и т. д.) и иметь одновременно до 32 «умных» устройств.

По мере развития и усовершенствование IoT-технологий возник новый стандарт – NB-IoT.

NB-IoT – это технология передачи данных, использующая узкий частотный диапазон. Это обеспечивает высокую проникающую способность, низкое энергопотребление и работу с небольшими объемами данных. Показатель эффективности – это постоянный рост использования датчиков NB-IoT на рынке датчиков IoT.

На рисунке 3 показаны особенность и удобство для датчиков применения узкополосного сигнала (NB).

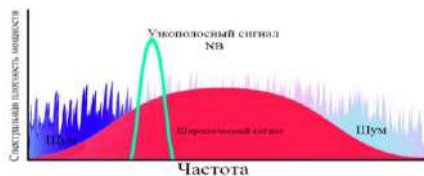


Рисунок 3 – График узкополосного сигнала

Технология NB-IoT также позволяет использовать такие же диапазоны частот, как и для технологий 2G/3G/4G(LTE) [1]. Основной же особенностью является многократное увеличение срока эксплуатации IoT-датчиков в отдельных случаях до 10 лет. Также NB-IoT осуществляет передачу данных посредством лицензируемого диапазона частот сотового оператора [1].



Рисунок 4 – Пример модуля NB-IoT

В настоящий момент технология NB-IoT позволила масштабироваться с отдельных объектов до квартирных комплексов, автоматизировав сбор сч-счетчиков воды и т. д., в дальнейшем эту технологию можно расширить до «Smart-city». Несмотря на то, что Интернет вещей зародился только в 2010-х, по данным IoT Analytic, к 2035 году объем IoT-устройств достигнет свыше 50 млрд (рисунок 5).

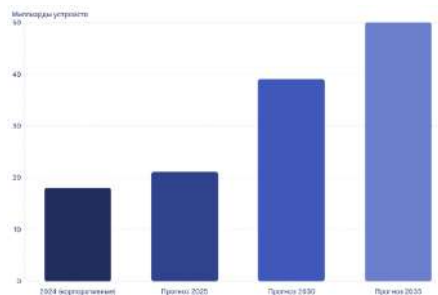


Рисунок 5 – Прогноз количества IoT-устройств к 2035 году

Из-за быстрого роста количества устройств и направленности на скорость и эффективность передачи информации, а не на безопасность, зачастую IoT-устройства не шифруют свой трафик, что привело к тому, что большинство из них «заражены». В настоящий момент большинство кибератак производят с помощью IoT-устройств. Ботнеты стали основой 90 % сложных многовекторных атак 2025 года, количество IoT-устройств в ботнетах, осуществляющих DDoS-атаки, выросло в пять раз (с 200 000 до 1 000 000). Для безопасности необходимо:

- 1 Сегментирование сети, т. е. изолирование от общей сети.
- 2 Замена стандартных логинов и паролей.
- 3 Мониторинг трафика.
- 4 Своевременные обновления.

Таким образом, развитие технологии «Интернет вещей» и увеличение количества IoT-устройств привело к тому, что вопрос кибербезопасности стал одним из главных, в настоящий момент нет единого протокола шифрования, который мог бы сбалансировать скорость передачи информации и ее защиту.

СПИСОК ЛИТЕРАТУРЫ

1 NB-IoT: как он работает? Ч. 1. // ХАБР. – URL: https://habr.com/ru/companies/ru_mts/articles/430496/ (дата обращения: 29.04.2026).

Получено 29.05.2026

ISSN 2227-1155. Сборник студенческих научных работ.
Вып. 31. Гомель, 2026

УДК 624.159.2

П. А. ПЕТРОВЕЦ (ПСм-22)

Научный руководитель – канд. техн. наук *В. В. ТАЛЕЦКИЙ*

СРАВНЕНИЕ ОСАДКИ ФУНДАМЕНТОВ, РАССЧИТАННОЙ РАЗНЫМИ МЕТОДАМИ

Рассмотрены варианты определения осадки ленточных фундаментов на слоистом основании методом послойного суммирования и методом эквивалентного слоя. Рекомендуется в сложных грунтовых условиях применять метод послойного суммирования, а для предварительных проработок и простых случаев – метод эквивалентного слоя, как более простой при расчете.