

**МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ**  
**БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ**  
**ФАКУЛЬТЕТ ПРИКЛАДНОЙ МАТЕМАТИКИ И ИНФОРМАТИКИ**  
Кафедра математического моделирования и анализа данных

**КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ДАННЫХ В IoT  
СИСТЕМАХ**

Курсовая работа

Шиляева Ивана Владимировича  
студента 4 курса, 9 группы  
специальность  
«компьютерная безопасность»

Научный руководитель:  
ассистент  
М.А. Казловский

Минск, 2021

# Оглавление

<b>Введение</b>	<b>3</b>
<b>1 Анализ литературы</b>	<b>4</b>
1.1 Используемые протоколы . . . . .	4
1.1.1 ZigBee . . . . .	5
1.1.2 Z-Wave . . . . .	5
1.1.3 Wi-Fi . . . . .	5
<b>Заключение</b>	<b>6</b>
<b>Список использованных источников</b>	<b>7</b>

# Введение

Термин «Интернет вещей» («Internet of Things») появился более 20 лет назад, а история развития технологии насчитывает почти два столетия. Среди множества определений термина можно выделить следующее. Интернет вещей — это глобальная сеть объектов, подключённых к интернету, которые взаимодействуют между собой и обмениваются данными без вмешательства человека.

Основными компонентами IoT систем являются объекты, или «вещи», данные, которыми они обмениваются, и инфраструктура, с помощью которой осуществляется взаимодействие. К последнему пункту можно отнести разнообразные виды соединения и каналы связи, программные средства и протоколы. Именно этот пункт будет интересовать нас больше всего в рамках данной работы.

Говоря о практическом применении Интернета вещей, многие отрасли выигрывают при использовании этой технологии. И в каждой из этих отраслей необходимо думать о безопасности и защите данных. В связи с этим возникают задачи актуализации знаний об алгоритмах и протоколах, применяемых в данной сфере, их сравнении и реализации в рамках программного обеспечения, а также рассмотрения вариантов модификации и улучшения этих протоколов с применением белорусской криптографии. Эти задачи и легли в основу данной работы. В соответствии с задачами были поставлены следующие цели:

1. ...
2. ...
3. ...
4. ...

Данная работа состоит из ... глав, в которых последовательно раскрываются все перечисленные выше вопросы.

# Глава 1

## Анализ литературы

### 1.1 Используемые протоколы

Существует множество разнообразных способов взаимодействия умных устройств между собой. Поэтому при выборе протоколов для Интернета вещей часто возникает вопрос: есть ли реальная необходимость разработки новых решений, когда хорошо зарекомендовавшие себя протоколы сети Интернет уже используются повсеместно десятилетиями? Причина для этого кроется в том, что существующие протоколы часто оказываются недостаточно эффективными и слишком энергоёмкими для работы с возникающими IoT технологиями. Поэтому речь пойдёт об альтернативных решениях, посвящённых именно IoT системам.

Одна из возможных классификаций разбивает все протоколы на три группы: ближнего, среднего и дальнего действия. Наиболее ярким представителем первой группы является Bluetooth, который несмотря на свою повсеместную распространённость остаётся далеко не лучшим решением, особенно при передаче больших объёмов данных. К последней группе относят такие протоколы как NB-IoT, LTE Cat-M1, LoRa WAN и SigFox. Эти решения являются весьма современными и продвинутыми, однако используются часто в масштабах предприятий. Наша же цель заключается в изучении решений, применимых к простым пользователям IoT систем, поэтому данный раздел будет преимущественно сконцентрирован вокруг второй группы, а именно протоколов средней зоны действия.

1.1.1 ZigBee

1.1.2 Z-Wave

1.1.3 Wi-Fi

# Заключение

# Литература