МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное автономное образовательное учреждение
высшего образования
«МОСКОВСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»
Факультет информационных технологий

**УТВЕРЖДАЮ**
Декан факультета
«Информационные технологии»
_____/Д.Г.Демидов/
«16» мая 2022

# РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

# «Безопасность интернета вещей»

Направление подготовки/специальность
**09.03.02 Информационные системы и технологии**
Профиль/специализация
**Информационные системы умных пространств**

Квалификация
**Бакалавр**

Форма обучения
**Очная**

Москва 2022 г.

**Разработчик(и):**

Заведующий кафедрой
«Информатика и информационные технологии»,
к.т.н.  / Е.В. Булатников /

**Согласовано:**

Заведующий кафедрой
«Информатика и информационные технологии»,
к.т.н.  / Е.В. Булатников /

# Содержание

## 1. Цели, задачи и планируемые результаты обучения по дисциплине

Целью данной дисциплины является освоение обучающимися навыков по проектированию, развертыванию и управлению безопасными системами интернета вещей, что в свою очередь способствует развитию безопасного и устойчивого цифрового мира.

Задачами дисциплины являются:

- Освоение анализа угроз и рисков;
- Приобретение практических навыков в проектировании безопасных систем;
- Освоение шифрования данных;
- Использование методов идентификации и аутентификации;
- Приобретение навыков управления доступом;
- Обнаружение и реагирование на инциденты;
- Соблюдение стандартов и нормативов.

Обучение по дисциплине «Безопасность интернета вещей» направлено на формирование у обучающихся следующих компетенций:

| Код и наименование компетенций | Индикаторы достижения компетенции |
|---|---|
| ПК-1. Способен разрабатывать требования и проектировать программное обеспечение | ИПК-1.1. Знает способы разработки требований и проектирования программного обеспечения в области интернет вещей и умного дома<br>ИПК-1.2. Умеет проектировать программное обеспечение с применением современных инструментальных средств в области интернет вещей и умного дома<br>ИПК-1.3. Имеет навыки разработки требований и проектирования программное обеспечение с применением современных инструментальных средств в области интернет вещей и умного дома |
| ПК-6. Способен предотвращать потери и повреждения данных | ИПК-6.1. Знает способы и методы резервного копирования и восстановления данных в проектах интернет вещей и умного дома<br>ИПК-6.2. Умеет, производить резервное копирование и восстановление данных в проектах интернет вещей и умного дома<br>ИПК-6.3. Имеет навыки разработки и применения программного обеспечения для резервного копирования и восстановления данных в проектах интернет вещей и умного дома |

## 2. Место дисциплины в структуре образовательной программы

Дисциплина относится к категории элективных Блока 1. Дисциплины (модули) учебного плана программы бакалавриата.

Дисциплина взаимосвязана логически и содержательно-методически со следующими дисциплинами и практиками ОПОП:

- Надежность, эргономика и качество систем управления;
- Распределенные системы;
- Учебная практика (проектная);

- Производственная практика (проектно-технологическая);
- Производственная практика (преддипломная);
- Выполнение и защита выпускной квалификационной работы.

## 3. Структура и содержание дисциплины

Общая трудоемкость дисциплины составляет 4 зачетных единицы, т.е. 144 академических часа.

### 3.1 Виды учебной работы и трудоемкость

3.1.1. Очная форма обучения

| № п/п | Вид учебной работы | Количество часов | Семестры |
|---|---|---|---|
| | | | 5 |
| **1** | **Аудиторные занятия** | **54** | **54** |
| | В том числе: | | |
| 1.1 | Лекции | 18 | 18 |
| 1.2 | Семинарские/практические занятия | | |
| 1.3 | Лабораторные занятия | 36 | 36 |
| **2** | **Самостоятельная работа** | **90** | **90** |
| | В том числе: | | |
| 2.1 | Подготовка и выполнение лабораторных работ | 90 | 90 |
| **3** | **Промежуточная аттестация** | | |
| | Экзамен/зачет/диф.зачет | | экзамен |
| | **Итого:** | **144** | **144** |

### 3.2Тематический план изучения дисциплины

3.2.1 Очная форма обучения

| № п/п | Разделы/темы дисциплины | Трудоемкость, час | | | | | |
|---|---|---|---|---|---|---|---|
| | | Всего | Аудиторная работа | | | | Самостоятельная работа |
| | | | Лекции | Семинарские/практические занятия | Лабораторные занятия | Практическая подготовка | |
| 1 | Лекция 1. Анализ угроз и рисков. Идентификация типичных угроз безопасности. Оценка рисков и их воздействия на системы IoT. | 7 | 2 | | | | 5 |
| 1.1 | Лабораторная работа 1. Проведение анализа угроз для конкретного устройства IoT. Оценка рисков и разработка стратегии по их снижению. | 9 | | | 4 | | 5 |
| 2 | Лекция 2. Шифрование данных в IoT Применение криптографии для защиты данных. Обзор современных алгоритмов | 7 | 2 | | | | 5 |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | шифрования и их применение в IoT. | | | | | | |
| 2.1 | Лабораторная работа 2.<br>Реализация примера протокола шифрования для безопасной передачи данных между устройствами.<br>Оценка производительности и стойкости к атакам. | 9 | | | 4 | | 5 |
| 3 | Лекция 3. Идентификация и аутентификация устройств<br>Разработка механизмов идентификации устройств и пользователей.<br>Защита от несанкционированного доступа. | 7 | 2 | | | | 5 |
| 3.1 | Лабораторная работа 3.<br>Создание механизмов идентификации и аутентификации для устройств IoT.<br>Практическое тестирование с использованием симуляции атак. | 9 | | | 4 | | 5 |
| 4 | Лекция 4. Управление доступом в IoT<br>Создание систем контроля доступа для управления правами пользователей и устройств.<br>Ограничение доступа к чувствительным данным и функциям. | 7 | 2 | | | | 5 |
| 4.1 | Лабораторная работа 4.<br>Разработка и реализация системы контроля доступа для устройств.<br>Тестирование различных уровней доступа и правил. | 9 | | | 4 | | 5 |
| 5 | Лекция 5. Обнаружение и реагирование на инциденты<br>Разработка средств обнаружения аномалий и необычного поведения.<br>Стратегии реагирования на инциденты безопасности в IoT. | 7 | 2 | | | | 5 |
| 5.1 | Лабораторная работа 5.<br>Создание механизмов обнаружения аномалий в поведении устройств.<br>Разработка плана реагирования на инциденты безопасности. | 9 | | | 4 | | 5 |
| 6 | Лекция 6. Безопасность беспроводных сетей IoT<br>Защита от угроз в беспроводных коммуникациях.<br>Стандарты безопасности для беспроводных протоколов. | 7 | 2 | | | | 5 |
| 6.1 | Лабораторная работа 6.<br>Настройка и тестирование | 9 | | | 4 | | 5 |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | безопасных беспроводных соединений между устройствами. Исследование мер безопасности протоколов беспроводной связи. | | | | | | |
| 7 | Лекция 7. Безопасность встроенных систем<br>Защита от вредоносного программного обеспечения и атак на встроенные устройства. Проектирование безопасных встроенных систем. | 7 | 2 | | | | 5 |
| 7.1 | Лабораторная работа 7.<br>Анализ безопасности встроенных устройств и разработка мер по их улучшению. Тестирование устройств на устойчивость к вредоносному программному обеспечению. | 9 | | | 4 | | 5 |
| 8 | Лекция 8. Безопасность облачных сервисов IoT<br>Защита данных и коммуникаций в облачных средах. Обзор принципов безопасности облачных сервисов для IoT. | 7 | 2 | | | | 5 |
| 8.1 | Лабораторная работа 8.<br>Подключение устройства к облачному сервису с использованием безопасных протоколов. Анализ политик безопасности облачных сервисов. | 9 | | | 4 | | 5 |
| 9 | Лекция 9. Обновление и управление жизненным циклом безопасности<br>Стратегии обновления программного обеспечения и внедрения патчей. Управление безопасностью в течение жизненного цикла продукта IoT. | 7 | 2 | | | | 5 |
| 9.1 | Лабораторная работа 9.<br>Разработка процедур обновления программного обеспечения для устройств IoT. Тестирование процесса обновления и внедрение патчей. | 9 | | | 4 | | 5 |
| | **Итого** | **144** | **18** | | **36** | | **90** |

## 3.3 Содержание разделов дисциплины

**1. Анализ угроз и рисков**

Идентификация типичных угроз безопасности. Оценка рисков и их воздействия на системы IoT.

**2. Шифрование данных в IoT**

Применение криптографии для защиты данных. Обзор современных алгоритмов шифрования и их применение в IoT.

3. **Идентификация и аутентификация устройств**

Разработка механизмов идентификации устройств и пользователей. Защита от несанкционированного доступа.

4. **Управление доступом в IoT**

Создание систем контроля доступа для управления правами пользователей и устройств. Ограничение доступа к чувствительным данным и функциям.

5. **Обнаружение и реагирование на инциденты**

Разработка средств обнаружения аномалий и необычного поведения. Стратегии реагирования на инциденты безопасности в IoT.

6. **Безопасность беспроводных сетей IoT**

Защита от угроз в беспроводных коммуникациях. Стандарты безопасности для беспроводных протоколов.

7. **Безопасность встроенных систем**

Защита данных и коммуникаций в облачных средах. Обзор принципов безопасности облачных сервисов для IoT.

8. **Безопасность облачных сервисов IoT**

Защита данных и коммуникаций в облачных средах. Обзор принципов безопасности облачных сервисов для IoT.

9. **Обновление и управление жизненным циклом безопасности**

Стратегии обновления программного обеспечения и внедрения патчей. Управление безопасностью в течение жизненного цикла продукта IoT.

## 3.4 Тематика семинарских/практических и лабораторных занятий

3.4.1 Семинарские/практические занятия

Семинарские и практические занятия не предусмотрены.

3.4.2 Лабораторные занятия

**Лабораторная работа 1**. Проведение анализа угроз для конкретного устройства IoT. Оценка рисков и разработка стратегии по их снижению.

**Лабораторная работа 2**. Реализация примера протокола шифрования для безопасной передачи данных между устройствами. Оценка производительности и стойкости к атакам.

**Лабораторная работа 3**. Создание механизмов идентификации и аутентификации для устройств IoT. Практическое тестирование с использованием симуляции атак.

**Лабораторная работа 4**. Разработка и реализация системы контроля доступа для устройств. Тестирование различных уровней доступа и правил.

**Лабораторная работа 5**. Создание механизмов обнаружения аномалий в поведении устройств. Разработка плана реагирования на инциденты безопасности.

**Лабораторная работа 6**. Настройка и тестирование безопасных беспроводных соединений между устройствами. Исследование мер безопасности протоколов беспроводной связи.

**Лабораторная работа 7**. Защита от вредоносного программного обеспечения и атак на встроенные устройства. Проектирование безопасных встроенных систем.

**Лабораторная работа 8**. Подключение устройства к облачному сервису с использованием безопасных протоколов. Анализ политик безопасности облачных сервисов.

**Лабораторная работа 9**. Разработка процедур обновления программного обеспечения для устройств IoT. Тестирование процесса обновления и внедрение патчей.

## 3.5 Тематика курсовых проектов (курсовых работ)

Курсовые проекты не предусмотрены.

## 4. Учебно-методическое и информационное обеспечение

### 4.1 Нормативные документы и ГОСТы

1. https://fgos.ru/fgos/fgos-01-03-02-prikladnaya-matematika-i-informatika-9/ 2. "Положения об организации образовательного процесса в Московском Политехническом университете"

### 4.2 Основная литература


1. Прохорова, О.В. Информационная безопасность и защита информации : учебник / О.В. Прохорова ; Министерство образования и науки РФ, Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования «Самарский государственный архитектурно-строительный университет». - Самара : Самарский государственный архитектурно-строительный университет, 2014. - [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=438331
2. Загинайлов, Ю.Н. Теория информационной безопасности и методология защиты информации : учебное пособие / Ю.Н. Загинайлов. - Москва ; Берлин : Директ-Медиа, 2015. - [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=276557


### 4.3 Дополнительная литература

Не предусмотрена.

### 4.4 Электронные образовательные ресурсы

ЭОР разрабатывается.

### 4.5 Лицензионное и свободно распространяемое программное обеспечение

Для успешного освоения дисциплины, студент использует следующие программные средства:

- Cooja Simulator;
- IoT-Lab;
- OpenIoT;
- OWASP IoT Security Project.

### 4.6 Современные профессиональные базы данных и информационные справочные системы

1. https://urait.ru/
2. https://www.iprbookshop.ru/
3. https://e.lanbook.com/

## 5. Материально-техническое обеспечение

Для проведения лабораторных работ необходим компьютерный класс (не менее 30 посадочных мест) с установленным программным обеспечением и подключенным интернет-соединением.

## 6. Методические рекомендации

### 6.1 Методические рекомендации для преподавателей по организации обучения

Для проведения занятий преподаватель пользуется учебником, по читаемому курсу, конспектом лекций, компьютерными презентациями для более наглядного изложения читаемого курса лекций.
Программа составлена в соответствии с Федеральным государственным образовательным стандартом высшего образования по направлению подготовки бакалавров 09.03.02.- Информационные системы и технологии.

## 6.2 Методические указания для обучающихся по освоению дисциплины

Для студентов подготовлены и используются учебник по дисциплине; методические указания по выполнению лабораторных работ.

## 7. Фонд оценочных средств

## 9.1 Методы контроля и оценивания результатов обучения

В процессе обучения используются следующие оценочные формы самостоятельной работы студентов, оценочные средства текущего контроля успеваемости и промежуточных аттестаций:

– подготовка к выполнению лабораторных работ и их защита;

– экзамен.

Оценочные средства текущего контроля успеваемости включают контрольные вопросы.

## 7.2 Шкала и критерии оценивания результатов обучения

Промежуточная аттестация обучающихся в форме экзамена проводится по результатам выполнения всех видов учебной работы, предусмотренных учебным планом по данной дисциплине, при этом учитываются результаты текущего контроля успеваемости в течение семестра. Оценка степени достижения обучающимися планируемых результатов обучения по дисциплине проводится преподавателем, ведущим занятия по дисциплине (модулю) методом экспертной оценки. По итогам промежуточной аттестации по дисциплине выставляется оценка «отлично», «хорошо», «удовлетворительно» или «неудовлетворительно».
К промежуточной аттестации допускаются только студенты, выполнившие все виды учебной работы, предусмотренные рабочей программой (прошли промежуточный контроль, выполнили лабораторные работы.)

| **Шкала оценивания** | **Описание** |
|---|---|
| Отлично | Выполнены все виды учебной работы, предусмотренные учебным планом. Студент демонстрирует соответствие знаний, умений, навыков приведенным в таблицах показателей, оперирует приобретенными знаниями, умениями, навыками, применяет их в ситуациях повышенной сложности. При этом могут быть допущены незначительные ошибки, неточности, затруднения при аналитических операциях, переносе знаний и умений на новые, нестандартные ситуации. |
| Хорошо | Выполнены все виды учебной работы, предусмотренные учебным планом. Студент демонстрирует соответствие знаний, умений, навыков приведенным в таблицах показателей, оперирует приобретенными знаниями, умениями, навыками, применяет их в ситуациях повышенной сложности, допускает мелкие неточности. При этом могут быть допущены |

| | |
|---|---|
| | незначительные ошибки, неточности, затруднения при аналитических операциях, переносе знаний и умений на новые, нестандартные ситуации. |
| Удовлетворительно | Выполнены все виды учебной работы, предусмотренные учебным планом. Студент демонстрирует неполное соответствие знаний, умений, навыков приведенным в таблицах показателей, оперирует приобретенными знаниями, умениями, навыками, применяет их в ситуациях повышенной сложности, допускает ошибки. При этом могут быть допущены ошибки, неточности, затруднения при аналитических операциях, переносе знаний и умений на новые, нестандартные ситуации. |
| Неудовлетворительно | Не выполнен один или более видов учебной работы, предусмотренных учебным планом. Студент демонстрирует неполное соответствие знаний, умений, навыков приведенным в таблицах показателей, допускаются значительные ошибки, проявляется отсутствие знаний, умений, навыков по ряду показателей, студент испытывает значительные затруднения при оперировании знаниями и умениями при их переносе на новые ситуации. |

## 7.3 Оценочные средства

Вопросы к экзамену

1. Что такое IoT (Интернет вещей)?
2. Перечислите основные компоненты архитектуры IoT.
3. Какие проблемы безопасности связаны с развитием IoT?
4. Какие угрозы могут возникнуть из-за уязвимостей в устройствах IoT?
5. Чем безопасность IoT отличается от безопасности традиционных компьютерных сетей?
6. Какие методы криптографии могут использоваться для обеспечения безопасности данных в IoT?
7. Объясните принципы работы алгоритмов шифрования на примере использования в IoT.
8. Какие меры обеспечивают конфиденциальность данных в передаче между устройствами IoT?
9. Почему важна идентификация и аутентификация в сети IoT?
10. Какие механизмы аутентификации могут быть использованы для устройств IoT?
11. В чем заключается система контроля доступа в сфере IoT?
12. Какие меры обеспечивают управление доступом в системах IoT?
13. Какие протоколы безопасности используются в сетях IoT?
14. Объясните, как работает TLS/SSL в контексте безопасности IoT.
15. Какие угрозы безопасности связаны с беспроводными сетями IoT?
16. Какие стандарты безопасности существуют для беспроводных протоколов в IoT?
17. Какие основные угрозы могут воздействовать на встроенные системы в устройствах IoT?
18. Какие методы обеспечивают защиту от вредоносного программного обеспечения в устройствах IoT?
19. Какие меры обеспечивают обнаружение аномалий в работе систем IoT?
20. Что включает в себя план реагирования на инциденты в контексте IoT?
21. Какие угрозы связаны с облачными сервисами в контексте IoT?
22. Как обеспечивается безопасность данных, передаваемых в облачных средах IoT?

23. Почему важно обеспечивать безопасность в течение жизненного цикла продукта IoT?
24. Какие шаги следует предпринять для обеспечения безопасного обновления программного обеспечения в устройствах IoT?
25. Какие этические вопросы возникают в сфере IoT и безопасности?
26. Какие законодательные нормы и стандарты регулируют безопасность в сети IoT?
27. Какие угрозы могут воздействовать на безопасность умных домов и потребительских устройств IoT?
28. Какие специфические меры безопасности требуются для промышленных систем IoT?
29. Какие международные стандарты используются в области безопасности IoT?
30. Как соблюдение стандартов способствует обеспечению безопасности в IoT?
31. Какие правовые вопросы могут возникнуть в связи с безопасностью IoT?
32. Какие нормативы регулируют обработку данных в IoT?
33. Какие тенденции в развитии технологий могут повлиять на безопасность IoT в будущем?
34. Какие вызовы могут возникнуть в связи с развитием новых технологий IoT?
35. Расскажите о конкретной угрозе безопасности в сети IoT и способах ее предотвращения.
36. Какие шаги вы предпримете в случае обнаружения уязвимости в устройстве IoT?
37. Какие протоколы обеспечивают защиту приватности данных в системах IoT?
38. Расскажите о сценарии атаки на сеть IoT и мерах по ее предотвращению.
39. Как провести аудит безопасности системы IoT?
40. Какие инструменты используются для тестирования безопасности устройств IoT?
41. Какие стандарты безопасности существуют для критически важных промышленных систем IoT?
42. Какие требования предъявляются к безопасности в промышленных средах?
43. Приведите примеры успешных решений в области безопасности IoT.
44. Какие уроки можно извлечь из известных случаев нарушения безопасности в IoT?
45. Какие программы обучения и сертификации существуют для специалистов по безопасности IoT?
46. Каковы лучшие методы обучения персонала по вопросам безопасности IoT?
47. Какие факторы следует учитывать при внедрении безопасных систем IoT?
48. Какие лучшие практики следует соблюдать при обслуживании устройств IoT?
49. Какие экологические проблемы могут возникнуть в связи с использованием устройств IoT?
50. Какие меры могут быть предприняты для минимизации экологического воздействия IoT?
51. Какие социальные проблемы связаны с распространением IoT?
52. Как улучшить осведомленность и образование об обеспечении безопасности IoT в обществе?
53. Как искусственный интеллект влияет на безопасность систем IoT?
54. Каким образом можно использовать искусственный интеллект для обеспечения безопасности в IoT?
55. Какие инновации в области безопасности IoT могут ожидаться в ближайшие годы?
56. Как инновации могут улучшить безопасность устройств IoT?
57. Какие вызовы представляют собой "умные города" в контексте безопасности IoT?
58. Как можно балансировать между уровнем безопасности и удобством использования в системах IoT?
59. Какие этические проблемы могут возникнуть из-за использования технологий IoT?
60. Как ученые и инженеры могут учесть этические аспекты при разработке систем IoT?