

Документ подписан простой электронной подписью

Информация о владельце:

ФИО: Максимов Алексей Борисович

Должность: директор департамента по образовательной политике

Дата подписания: 12.10.2026 16:48:36

Уникальный идентификатор:

8db180d1a3f02ac9e60521a5672742735c18b1d6

**МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ**

**Федеральное государственное автономное образовательное учреждение
высшего образования**

«МОСКОВСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»

УТВЕРЖДАЮ

Декан факультета

«Информационных технологий»



 / Д.Г. Демидов /

« 26 » февраль 2026 г.

**РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
Безопасность интернета вещей**

Направление подготовки

09.03.01 Информатика и вычислительная техника

Профиль подготовки (образовательная программа)

«Информационные системы умных пространств»

Год начала обучения:

2026

Квалификация (степень) выпускника

Бакалавр

Форма обучения

Очная

Москва – 2026

Рабочая программа составлена на основе ФГОС ВО и учебного плана Московского политехнического университета по направлению (специальности) 09.03.01 Информатики и вычислительная техника, по профилю подготовки Информационные системы умных пространств.

Разработчик(и):

к. ф.-м. н., доцент кафедры



/ Т.Т. Идиатуллин /

Согласовано:

Заведующий кафедрой
«СМАРТ-технологии»,
к.т.н., доцент



/ Е.В. Петрунина /

Содержание

1. Цели, задачи и планируемые результаты обучения по дисциплине
2. Место дисциплины в структуре образовательной программы
3. Структура и содержание дисциплины
 - 3.1 Виды учебной работы и трудоемкость
 - 3.2 Тематический план изучения дисциплины (по формам обучения)
 - 3.3 Содержание дисциплины
 - 3.4 Тематика семинарских/практических и лабораторных занятий
 - 3.5 Тематика вопросов для самостоятельного изучения
4. Учебно-методическое и информационное обеспечение
 - 4.1 Нормативные документы и ГОСТы
 - 4.2. Основная литература
 - 4.3 Дополнительная литература
 - 4.4 Электронные образовательные ресурсы
 - 4.5 Лицензионное и свободно распространяемое программное обеспечение
 - 4.6 Современные профессиональные базы данных и информационные справочные системы
- 5 Материально-техническое обеспечение
- 6 Методические рекомендации
 - 6.1 Методические рекомендации для преподавателя по организации обучения
 - 6.2 Методические указания для обучающихся по освоению дисциплины
 - 6.3 Средства адаптации преподавания дисциплины к потребностям обучающихся инвалидов и лиц с ограниченными возможностями здоровья
- 7 Фонд оценочных средств
 - 7.1 Методы контроля и оценивания результатов обучения
 - 7.2 Шкала и критерии оценивания результатов обучения
- Приложение 1
- Приложение 2

1 Цели, задачи и планируемые результаты обучения по дисциплине

К основным целям освоения дисциплины «Безопасность интернета вещей» следует отнести:

- формирование у обучающихся системного представления об угрозах информационной безопасности систем Интернета вещей и методах защиты на всех уровнях их архитектуры;
- ознакомление обучающихся с нормативной базой, стандартами и лучшими практиками обеспечения безопасности устройств, сетей и платформ Интернета вещей;
- формирование навыков анализа защищенности, проектирования мер защиты и тестирования на проникновение применительно к системам Интернета вещей и умных пространств.

К основным задачам освоения дисциплины «Безопасность интернета вещей» следует отнести:

- изучение специфики угроз и модели нарушителя для устройств и систем Интернета вещей в отличие от традиционных информационных систем;
- изучение методов обеспечения безопасности на аппаратном уровне: защищенная загрузка, доверенное хранение ключей, защита от физического вмешательства;
- изучение криптографических примитивов и протоколов защиты каналов связи, применимых для устройств с ограниченными ресурсами;
- изучение угроз и мер защиты сетевого и прикладного уровней протокольного стека Интернета вещей;
- изучение угроз облачных и туманных платформ Интернета вещей, вопросов безопасности при агрегации и хранении данных;
- изучение методов управления идентификацией, доступом и жизненным циклом устройств, включая безопасное обновление программного обеспечения;
- приобретение навыков проведения анализа защищенности устройств и сетей Интернета вещей, включая элементы тестирования на проникновение;
- приобретение навыков разработки политики безопасности и модели угроз для проектируемой системы умного пространства.

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

Код и наименование компетенций	Индикаторы достижения компетенции
ПК-3. Способен осуществлять концептуальное, функциональное и логическое проектирование систем среднего и крупного масштаба и сложности	ИПК-3.1. Знает принципы создания систем интернета вещей и интеллектуальных пространств ИПК-3.2. Умеет производить концептуальное, функциональное и логическое проектирование систем интернета вещей и интеллектуальных пространств ИПК-3.3. Имеет навыки применения ПО для концептуального, функционального и логического проектирования систем интернета вещей и интеллектуальных пространств

2 Место дисциплины в структуре образовательной программы

Дисциплина «Безопасность интернета вещей» относится к числу профессиональных учебных дисциплин базового цикла (Б1.2) части, формируемой участниками образовательных отношений основной образовательной программы бакалавриата по направлению подготовки 09.03.01 «Информатика и вычислительная техника», профиль «Информационные системы умных пространств».

Изучение дисциплины опирается на знания, умения и навыки, приобретенные в предшествующих дисциплинах: «Протоколы IoT», «Архитектура систем умных пространств», «Аппаратное обеспечение умных пространств», «Интеллектуальные интерфейсы в умных пространствах», «Операционные системы микроконтроллеров».

Дисциплина обеспечивает изучение дисциплины «Информационные системы умных пространств», а также выполнение курсовых работ и выпускной квалификационной работы.

3 Структура и содержание дисциплины

Общая трудоемкость дисциплины составляет 4 зачетные единицы, т.е. 144 академических часа, из них аудиторных — 54 часа, самостоятельная работа обучающихся — 90 часов. Форма промежуточной аттестации — зачет в 6 семестре.

3.1 Виды учебной работы и трудоемкость

(по очной форме обучения)

№ п/п	Вид учебной работы	Количество часов	Семестр 6
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
3	Промежуточная аттестация	зачет	зачет
	Итого:	144	144

3.2 Тематический план изучения дисциплины

(по очной форме обучения)

№ п/п	Разделы/темы дисциплины	Всего, час.	Лекции	Лабораторные занятия	Самостоятельная работа
1	Тема 1. Информационная безопасность Интернета вещей: специфика угроз и модель нарушителя	16	2	4	10
2	Тема 2. Безопасность аппаратного уровня и физическая защита устройств	16	2	4	10
3	Тема 3. Криптографические примитивы и протоколы защиты для ограниченных устройств	18	2	4	12
4	Тема 4. Безопасность беспроводных сетей и протоколов канального и сетевого уровня	18	2	4	12
5	Тема 5. Безопасность прикладных протоколов Интернета вещей	16	2	4	10

№ п/п	Разделы/темы дисциплины	Всего, час.	Лекции	Лабораторные занятия	Самостоятельная работа
6	Тема 6. Безопасность облачных и туманных платформ. Защита данных	16	2	4	10
7	Тема 7. Управление идентификацией, доступом и безопасное обновление устройств	18	2	4	12
8	Тема 8. Анализ защищенности, тестирование на проникновение и управление рисками	26	4	8	14
	Итого	144	18	36	90

3.3 Содержание дисциплины

3.3.1 Содержание лекционных занятий (18 часов)

Тема 1. Информационная безопасность Интернета вещей: специфика угроз и модель нарушителя (2 ч)

Основные понятия информационной безопасности: конфиденциальность, целостность, доступность применительно к системам Интернета вещей. Специфика Интернета вещей, отличающая его от традиционных информационных систем: масштаб, гетерогенность устройств, ограниченность ресурсов, физическая доступность устройств, длительный жизненный цикл. Классификация угроз безопасности Интернета вещей: угрозы устройствам, каналам связи, платформам и данным. Модель нарушителя: внешний и внутренний нарушитель, уровень квалификации и ресурсов, мотивация атак. Поверхность атаки распределенной системы умного пространства. Обзор известных инцидентов безопасности Интернета вещей и извлеченных уроков. Обзор нормативной базы и стандартов в области безопасности Интернета вещей, в том числе отечественных.

Тема 2. Безопасность аппаратного уровня и физическая защита устройств (2 ч)

Угрозы физического уровня: несанкционированный физический доступ к устройству, извлечение прошивки и ключей, атаки по побочным каналам. Защищенная загрузка (secure boot): проверка целостности и подлинности загружаемого программного обеспечения. Доверенная среда выполнения и

аппаратные модули безопасности, защищенное хранение ключей. Физически неклонировуемые функции (PUF) и их применение для идентификации устройств. Методы защиты от вмешательства (tamper detection и tamper response). Особенности обеспечения аппаратной безопасности для массовых недорогих устройств Интернета вещей. Требования к безопасности на этапе производства и поставки устройств, риски цепочки поставок.

Тема 3. Криптографические примитивы и протоколы защиты для ограниченных устройств (2 ч)

Особенности применения криптографии на устройствах с ограниченными вычислительными ресурсами и энергопотреблением. Легковесная криптография: облегченные алгоритмы шифрования и хеширования, стандартизация легковесных криптографических примитивов. Симметричное и асимметричное шифрование, эллиптическая криптография как способ снижения вычислительной нагрузки. Протоколы защиты транспортного уровня TLS и DTLS для ограниченных устройств, профили для устройств Интернета вещей. Протокол OSCORE для сквозной защиты сообщений при наличии посредников. Управление криптографическими ключами: распределение, обновление, отзыв ключей в масштабе большого количества устройств. Постквантовая криптография и перспективы ее применения в системах Интернета вещей.

Тема 4. Безопасность беспроводных сетей и протоколов канального и сетевого уровня (2 ч)

Угрозы беспроводных технологий, применяемых в Интернете вещей: перехват трафика, атаки повторного воспроизведения, глушение канала связи (jamming). Уязвимости протоколов Wi-Fi, Bluetooth Low Energy, Zigbee, известные атаки и меры защиты. Безопасность технологий LPWAN: механизмы защиты в LoRaWAN и NB-IoT. Угрозы сетевого уровня: атаки на протокол маршрутизации RPL, атаки типа sinkhole и selective forwarding в сетях с потерями. Защита адаптационного уровня 6LoWPAN и обеспечение целостности маршрутизации. Сегментация сети и изоляция сегментов Интернета вещей от корпоративной сети. Обнаружение аномалий сетевого трафика устройств Интернета вещей.

Тема 5. Безопасность прикладных протоколов Интернета вещей (2 ч)

Угрозы безопасности протокола MQTT: отсутствие аутентификации по умолчанию, риски открытых брокеров, перехват и подмена сообщений. Механизмы защиты MQTT: аутентификация клиентов, авторизация по темам, применение TLS. Угрозы безопасности протокола CoAP и меры защиты

средствами DTLS и OSCORE. Безопасность протокола HTTP/REST и веб-интерфейсов управления устройствами: типовые уязвимости веб-приложений применительно к панелям управления устройствами. Безопасность протоколов автоматизации умного дома: угрозы стандарту Matter и экосистемам умного дома. Атаки на устройства через голосовых ассистентов и через мобильные приложения управления. Защита от подмены и повторного использования сообщений на прикладном уровне.

Тема 6. Безопасность облачных и туманных платформ. Защита данных (2 ч)

Модель разделения ответственности за безопасность между поставщиком платформы Интернета вещей и разработчиком решения. Угрозы облачных платформ Интернета вещей: неправильная настройка доступа, утечки данных, атаки на API управления устройствами. Безопасность граничных и туманных вычислительных узлов, риски компрометации шлюза. Защита данных при хранении: шифрование, разграничение доступа, анонимизация и псевдонимизация. Требования законодательства о персональных данных применительно к телеметрии умных пространств. Безопасность цифровых двойников и агрегированных данных умного пространства. Мониторинг безопасности платформы: журналирование событий, обнаружение аномалий, реагирование на инциденты.

Тема 7. Управление идентификацией, доступом и безопасное обновление устройств (2 ч)

Идентификация и аутентификация устройств: сертификаты, предустановленные ключи, аппаратные идентификаторы. Управление жизненным циклом идентификационных данных устройства: выпуск, ротация, отзыв. Модели управления доступом: ролевая, атрибутная модели применительно к устройствам и пользователям умного пространства. Единая точка входа и федеративная аутентификация пользователей платформы умного пространства. Безопасное обновление программного обеспечения устройств по воздуху (secure OTA): проверка подлинности, целостности и версии обновления, откат при неудачном обновлении. Управление конфигурацией большого парка устройств и обеспечение согласованности настроек безопасности. Вывод устройств из эксплуатации и безопасное удаление данных.

Тема 8. Анализ защищенности, тестирование на проникновение и управление рисками (4 ч)

Методология анализа защищенности систем Интернета вещей: анализ по уровням архитектуры (устройство, сеть, платформа, приложение). Моделирование угроз: методики построения модели угроз, применение матриц угроз для систем Интернета вещей. Методы и инструменты тестирования на проникновение устройств: анализ прошивки, анализ радиоинтерфейсов, анализ мобильных приложений и облачных API. Классификации уязвимостей Интернета вещей, использование открытых баз данных уязвимостей. Оценка рисков информационной безопасности: вероятность реализации угрозы и величина ущерба, приоритизация мер защиты. Разработка политики безопасности и требований безопасности в техническом задании на систему. Организационные меры обеспечения безопасности: обучение персонала, регламенты реагирования на инциденты. Тенденции развития угроз и средств защиты Интернета вещей.

3.3.2 Содержание лабораторных занятий (36 часов)

Лабораторная работа № 1. Построение модели угроз для системы умного пространства (4 ч)

Выбор объекта умного пространства и описание его архитектуры по уровням. Идентификация активов, подлежащих защите, и потенциальных нарушителей. Построение модели угроз для выбранной системы с использованием изученной методики. Оформление документа «Модель угроз».

Лабораторная работа № 2. Анализ и настройка защищенной загрузки и хранения ключей (4 ч)

Изучение механизма проверки целостности загружаемого программного обеспечения на отладочном модуле. Настройка защищенного хранения ключевой информации средствами доступного аппаратного модуля безопасности или программной эмуляции. Исследование поведения устройства при попытке загрузки модифицированного образа программного обеспечения. Оформление отчета с описанием реализованных мер защиты.

Лабораторная работа № 3. Настройка защищенного канала связи для ограниченного устройства (4 ч)

Настройка защищенного соединения по протоколу DTLS между устройством и сервером с использованием общего ключа и с использованием сертификатов. Измерение накладных расходов защищенного соединения по времени установления и объему трафика на ограниченном устройстве. Анализ перехваченного трафика для оценки отсутствия утечки данных в открытом виде. Сравнение результатов для разных режимов аутентификации.

Лабораторная работа № 4. Анализ уязвимостей беспроводной сети и сети с протоколом маршрутизации (4 ч)

Перехват и анализ трафика беспроводной сети лабораторного стенда, выявление отсутствия шифрования или слабых механизмов защиты. Моделирование атаки на протокол маршрутизации в сети с потерями (например, sinkhole) на программном симуляторе и анализ ее последствий. Разработка и проверка мер обнаружения подобной атаки. Оформление отчета с рекомендациями по защите сети.

Лабораторная работа № 5. Анализ защищенности протокола MQTT (4 ч)

Развертывание брокера MQTT с настройками по умолчанию и демонстрация возможности несанкционированного подключения и перехвата сообщений. Настройка аутентификации клиентов, авторизации по темам и защищенного соединения по TLS. Повторная проверка защищенности брокера после внесения изменений. Оформление сравнительного отчета «до» и «после» применения мер защиты.

Лабораторная работа № 6. Анализ безопасности облачной платформы и API управления устройствами (6 ч)

Изучение модели разграничения доступа выбранной платформы Интернета вещей. Выявление типовых ошибок конфигурации доступа к ресурсам платформы на учебном примере. Анализ защищенности прикладного программного интерфейса (API) управления устройствами: проверка аутентификации запросов и корректности обработки ошибочных данных. Разработка рекомендаций по усилению защиты облачного компонента системы.

Лабораторная работа № 7. Управление идентификацией устройств и безопасное обновление программного обеспечения (6 ч)

Настройка выпуска и применения сертификатов для идентификации устройств в учебном стенде. Реализация процедуры проверки подлинности и целостности обновления программного обеспечения перед его установкой на устройство. Моделирование ситуации неудачного обновления и проверка механизма отката к предыдущей версии. Оформление отчета с описанием реализованной процедуры безопасного обновления.

Лабораторная работа № 8. Комплексный анализ защищенности макета умного пространства и защита проекта (4 ч)

Проведение комплексного анализа защищенности собранного в течение семестра макета системы умного пространства по уровням архитектуры.

Формирование перечня выявленных уязвимостей и оценка связанных с ними рисков. Разработка итоговых рекомендаций и плана мероприятий по устранению выявленных недостатков. Публичная защита выполненной работы с обоснованием предложенных мер защиты.

3.3.3 Содержание самостоятельной работы обучающихся (90 часов)

Самостоятельная работа обучающихся включает следующие виды деятельности:

- проработка конспектов лекций и изучение разделов дисциплины, вынесенных на самостоятельное изучение, по рекомендованной литературе и электронным образовательным ресурсам;
- изучение стандартов и рекомендаций в области безопасности Интернета вещей, а также баз данных уязвимостей, в том числе на английском языке;
- подготовка к выполнению и защите лабораторных работ, оформление отчетов;
- выполнение сквозного индивидуального задания по анализу защищенности и разработке политики безопасности для заданной системы умного пространства;
- разбор известных инцидентов безопасности Интернета вещей по открытым источникам и подготовка их анализа;
- подготовка обзора (реферата) по современным угрозам и средствам защиты систем Интернета вещей;
- подготовка к тестированию и к зачету.

4 Учебно-методическое и информационное обеспечение

4.1 Нормативные документы и ГОСТы

1. Федеральный закон от 29.12.2012 № 273-ФЗ «Об образовании в Российской Федерации».
2. Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации».
3. Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных».
4. Приказ Минобрнауки России от 19.09.2017 № 929 (ред. от 08.02.2021) «Об утверждении федерального государственного образовательного стандарта высшего образования — бакалавриат по направлению

подготовки 09.03.01 Информатика и вычислительная техника» (Зарегистрировано в Минюсте России 10 октября 2017 г. № 48489).

5. Академический учебный план. Направление подготовки: 09.03.01 Информатика и вычислительная техника. Профиль: Информационные системы умных пространств. Форма обучения: очная.
6. Положение о проведении текущего контроля успеваемости и промежуточной аттестации обучающихся федерального государственного автономного образовательного учреждения высшего образования «Московский политехнический университет» (утверждено приказом Московского Политеха от 01.12.2022 № 1375ОД).
7. ГОСТ Р 59026-2020. Информационные технологии. Интернет вещей. Термины и определения.
8. ГОСТ Р 56939-2016. Защита информации. Разработка безопасного программного обеспечения. Общие требования.
9. ГОСТ Р ИСО/МЭК 27001-2021. Информационная безопасность, кибербезопасность и защита персональных данных. Требования.
10. ГОСТ Р 70262-2022. Информационная безопасность. Безопасность устройств Интернета вещей. Общие требования.
11. ГОСТ Р 71199-2023. Защита информации. Устройства Интернета вещей. Требования безопасности.

4.2 Основная литература

1. Столлинкс, В. Основы защиты сетей. Приложения и стандарты / В. Столлинкс. — Москва : Вильямс, 2002. — 432 с.
2. Шаньгин, В. Ф. Информационная безопасность и защита информации / В. Ф. Шаньгин. — Москва : ДМК Пресс, 2017. — 702 с.
3. Росляков, А. В. Интернет вещей : учебное пособие / А. В. Росляков, С. В. Ваняшин, А. Ю. Гребешков. — Самара : ПГУТИ, 2015. — 200 с.
4. Бирюков, А. А. Информационная безопасность. Защита и нападение / А. А. Бирюков. — Москва : ДМК Пресс, 2017. — 434 с.
5. Олифер, В. Г. Компьютерные сети. Принципы, технологии, протоколы : учебник для вузов / В. Г. Олифер, Н. А. Олифер. — 6-е изд. — Санкт-Петербург : Питер, 2020. — 1008 с.

4.3 Дополнительная литература

1. Куроуз, Дж. Компьютерные сети. Нисходящий подход / Дж. Куроуз, К. Росс. — Москва : Эксмо, 2016. — 912 с.
2. Гриценко, В. Основы криптографии : учебное пособие / В. Гриценко, В. Ковтун. — Санкт-Петербург : Лань, 2020. — 240 с.
3. Складов, Д. В. Искусство защиты и взлома информации / Д. В. Складов. — Санкт-Петербург : БХВ-Петербург, 2004. — 288 с.
4. Запечников, С. В. Информационная безопасность открытых систем : учебник / С. В. Запечников, Н. Г. Милославская, А. И. Толстой, Д. В. Ушаков. — Москва : Горячая линия — Телеком, 2018. — 536 с.
5. Сомов, А. М. Спутниковые системы связи и сети Интернета вещей : учебное пособие / А. М. Сомов. — Москва : Горячая линия — Телеком, 2019. — 244 с.

4.4 Электронные образовательные ресурсы

1. Курс в ЛМС Московского политехнического университета. — <https://lms.mospolytech.ru/>
2. Проект Open Web Application Security Project, раздел по безопасности Интернета вещей (OWASP IoT Top 10). — <https://owasp.org/www-project-internet-of-things/>
3. База данных общеизвестных уязвимостей CVE (Common Vulnerabilities and Exposures). — <https://cve.mitre.org/>
4. Документы RFC организации IETF по безопасности ограниченных устройств (RFC 8613 OSCORE, RFC 9147 DTLS 1.3). — <https://www.rfc-editor.org/>
5. Материалы Национального координационного центра по компьютерным инцидентам (НКЦКИ). — <https://safe-surf.ru/>
6. Информационная система «Техэксперт»: нормативно-техническая документация. — <https://cntd.ru/>
7. Электронно-библиотечная система «Лань». — <https://e.lanbook.com/>
8. Электронно-библиотечная система «Юрайт». — <https://urait.ru/>

4.5 Лицензионное и свободно распространяемое программное обеспечение

1. Операционная система Windows 10 (или выше) — Microsoft Open License.

2. Офисные приложения Microsoft Office 2016 (или выше) — Microsoft Open License.
3. Анализатор сетевого трафика Wireshark — свободно распространяемое ПО (лицензия GPL).
4. Брокер сообщений Eclipse Mosquitto — свободно распространяемое ПО (лицензия EPL).
5. Средство сканирования уязвимостей сети Nmap — свободно распространяемое ПО.
6. Программно-определяемая радиосистема и инструменты анализа радиоэфира (GNU Radio) — свободно распространяемое ПО.
7. Библиотеки криптографии OpenSSL и mbedTLS — свободно распространяемое ПО.
8. Дистрибутив для тестирования на проникновение Kali Linux (в учебных целях, изолированный стенд) — свободно распространяемое ПО.
9. Система контроля версий Git — свободно распространяемое ПО (лицензия GPL).

5 Материально-техническое обеспечение

Для проведения всех видов занятий необходимо презентационное оборудование (мультимедийный проектор, компьютер, экран) — 1 комплект.

Для проведения лабораторных занятий необходимо наличие компьютерного класса, оборудованного современной вычислительной техникой из расчета одно рабочее место на одного обучающегося, объединенного в изолированную учебную сеть без доступа к внешним ресурсам во время выполнения работ по анализу защищенности, а также следующего оборудования:

- отладочные модули с беспроводными интерфейсами и аппаратными модулями безопасности — из расчета один комплект на одно-два рабочих места;
- изолированная лабораторная беспроводная сеть для проведения учебного анализа трафика и моделирования атак;
- серверное оборудование или виртуальная инфраструктура для развертывания брокеров сообщений, облачной платформы Интернета вещей и учебных уязвимых сервисов;
- средства анализа сетевого трафика и программно-определяемая радиосистема для учебного исследования радиоэфира;

- средства измерений и отладки: мультиметры, логические анализаторы, программаторы для работы с прошивками устройств.

6 Методические рекомендации

6.1 Методические рекомендации для преподавателя по организации обучения

При подготовке к занятиям следует предварительно проработать материал занятия, предусмотрев его подачу точно в отведенное для этого время занятия. Следует подготовить необходимые материалы — примеры реальных инцидентов, техническую документацию, задания для лабораторных работ, а также заранее развернуть и проверить изолированный лабораторный стенд для проведения работ, связанных с моделированием атак.

Все работы, связанные с анализом уязвимостей и моделированием атак, необходимо проводить исключительно в изолированной учебной среде без доступа к внешним сетям и системам; преподавателю следует явно разъяснять обучающимся правовые и этические границы применения полученных знаний и навыков.

Лабораторный практикум целесообразно организовать как сквозной проект: обучающиеся проходят полный цикл анализа защищенности одной выбранной системы умного пространства — от построения модели угроз до итогового комплексного анализа и разработки рекомендаций.

При проверке работ и отчетов следует учитывать не только формальное обнаружение уязвимости, но и корректность оценки связанного с ней риска, обоснованность предложенных мер защиты и умение обучающегося сопоставить их со стоимостью и удобством эксплуатации системы.

6.2 Методические указания для обучающихся по освоению дисциплины

Изучение дисциплины осуществляется в строгом соответствии с целевой установкой в тесной взаимосвязи с учебным планом. Основой теоретической подготовки обучающихся являются лекции.

В процессе самостоятельной работы обучающиеся закрепляют и углубляют знания, полученные во время аудиторных занятий, дорабатывают конспекты лекций, изучают стандарты и открытые базы данных уязвимостей, готовятся к защите лабораторных работ и к зачету, а также самостоятельно изучают отдельные темы учебной программы.

Особое внимание при подготовке следует уделять анализу реальных инцидентов безопасности Интернета вещей: рекомендуется для каждого изученного класса угроз находить и разбирать соответствующий известный пример из практики. Все практические навыки анализа защищенности допускается применять только на собственных учебных стендах и с явного разрешения владельца системы.

7 Фонд оценочных средств

7.1 Методы контроля и оценивания результатов обучения

В процессе обучения используются следующие оценочные формы самостоятельной работы обучающихся, оценочные средства текущего контроля успеваемости и промежуточной аттестации:

- подготовка к решению прикладных задач;
- выполнение и защита лабораторных работ, оформление отчетов;
- выполнение сквозного индивидуального задания по анализу защищенности и его защита;
- подготовка обзора (реферата) по современным угрозам и средствам защиты Интернета вещей;
- тест;
- зачет.

7.2 Шкала и критерии оценивания результатов обучения

Показателем оценивания компетенций на различных этапах их формирования является достижение обучающимися планируемых результатов обучения по дисциплине (модулю).

ПК-3. Способен осуществлять концептуальное, функциональное и логическое проектирование систем среднего и крупного масштаба и сложности

Показатель	2	3	4	5
знать: специфику угроз и модель нарушителя для систем Интернета вещей, методы защиты аппаратного, сетевого, прикладного уровней и облачных платформ	Обучающийся демонстрирует полное отсутствие или недостаточное соответствие указанных знаний	Обучающийся демонстрирует неполное соответствие указанных знаний, освещена основная, наиболее важная часть материала,	Обучающийся демонстрирует частичное соответствие указанных знаний, допускаются 2—3 несущественные ошибки и неточности	Обучающийся демонстрирует полное соответствие указанных знаний, свободно оперирует материалом дисциплины

Показатель	2	3	4	5
		допущена одна значительная ошибка или неточность		
уметь: строить модель угроз, настраивать средства криптографической защиты каналов связи, выявлять и анализировать уязвимости устройств, сетей и платформ Интернета вещей	Обучающийся не умеет или в недостаточной степени умеет выполнять указанные действия	Обучающийся демонстрирует неполное соответствие указанных умений, испытывает значительные затруднения при переносе умений на новые ситуации	Обучающийся демонстрирует частичное соответствие указанных умений, допускает незначительные ошибки и неточности	Обучающийся демонстрирует полное соответствие указанных умений, уверенно применяет их в нестандартных ситуациях
владеть: навыками проведения анализа защищенности и элементов тестирования на проникновение, разработки политики безопасности и оценки рисков для системы умного пространства	Обучающийся не владеет или в недостаточной степени владеет указанными навыками	Обучающийся владеет указанными навыками, но допускаются значительные ошибки, проявляется недостаточность навыков по ряду показателей	Обучающийся частично владеет указанными навыками, допускаются незначительные ошибки и затруднения при аналитических операциях	Обучающийся в полном объеме владеет указанными навыками, свободно оперирует приобретенными знаниями

Шкалы оценивания результатов промежуточной аттестации и их описание:

Форма промежуточной аттестации: зачет.

Промежуточная аттестация обучающихся в форме зачета проводится по результатам выполнения всех видов учебной работы, предусмотренных учебным планом по данной дисциплине (модулю), при этом учитываются результаты текущего контроля успеваемости в течение семестра. Оценка степени достижения обучающимися планируемых результатов обучения по дисциплине (модулю) проводится преподавателем, ведущим занятия по дисциплине (модулю), методом экспертной оценки. По итогам промежуточной аттестации по дисциплине (модулю) выставляется оценка «зачтено» или «не зачтено».

Шкала оценивания	Описание
зачтено	Выполнены все виды учебной работы, предусмотренные учебным планом. Обучающийся демонстрирует соответствие знаний, умений, навыков приведенным в таблицах показателей, оперирует

Шкала оценивания	Описание
	приобретенными знаниями, умениями и навыками, применяет их в ситуациях повышенной сложности. При этом могут быть допущены несущественные ошибки, исправленные обучающимся самостоятельно. Все лабораторные работы выполнены и защищены, индивидуальное задание сдано. Присутствовал более чем на $\frac{1}{2}$ занятий по дисциплине.
не зачтено	Не выполнен один или более видов учебной работы, предусмотренных учебным планом. Обучающийся демонстрирует неполное соответствие знаний, умений, навыков приведенным в таблицах показателей, допускаются значительные ошибки, проявляется отсутствие знаний, умений, навыков по ряду показателей, обучающийся испытывает значительные затруднения при оперировании знаниями и умениями при их переносе на новые ситуации.

7.3 Оценочные средства

7.3.1 Список вопросов для зачета

1. Конфиденциальность, целостность, доступность применительно к системам Интернета вещей.
2. Специфика Интернета вещей, отличающая его от традиционных информационных систем с точки зрения безопасности.
3. Классификация угроз безопасности Интернета вещей по уровням архитектуры.
4. Модель нарушителя: типы нарушителей, уровень квалификации и мотивация атак.
5. Поверхность атаки распределенной системы умного пространства.
6. Угрозы физического уровня и атаки по побочным каналам.
7. Защищенная загрузка (secure boot): назначение и принцип работы.
8. Доверенная среда выполнения и аппаратные модули безопасности.
9. Физически неклонируемые функции (PUF) и их применение.
10. Методы защиты от физического вмешательства (tamper detection).
11. Риски цепочки поставок устройств Интернета вещей.
12. Особенности применения криптографии на устройствах с ограниченными ресурсами.
13. Легковесная криптография: назначение и примеры алгоритмов.

14. Протоколы TLS и DTLS для защиты каналов связи ограниченных устройств.
15. Протокол OSCORE и его назначение при наличии посредников.
16. Управление криптографическими ключами в масштабе большого количества устройств.
17. Угрозы беспроводных технологий: перехват, повтор, глушение канала.
18. Уязвимости протоколов Wi-Fi, Bluetooth Low Energy и Zigbee.
19. Механизмы защиты в технологиях LoRaWAN и NB-IoT.
20. Атаки на протокол маршрутизации RPL: sinkhole, selective forwarding.
21. Защита адаптационного уровня 6LoWPAN.
22. Сегментация сети и изоляция сегментов Интернета вещей.
23. Угрозы безопасности протокола MQTT и меры защиты.
24. Угрозы безопасности протокола CoAP и меры защиты средствами DTLS и OSCORE.
25. Типовые уязвимости веб-интерфейсов управления устройствами.
26. Угрозы протоколам и экосистемам умного дома.
27. Модель разделения ответственности за безопасность облачной платформы.
28. Угрозы облачных платформ Интернета вещей.
29. Безопасность граничных и туманных вычислительных узлов.
30. Защита данных при хранении: шифрование, разграничение доступа, анонимизация.
31. Требования законодательства о персональных данных применительно к телеметрии умных пространств.
32. Мониторинг безопасности платформы и реагирование на инциденты.
33. Идентификация и аутентификация устройств Интернета вещей.
34. Модели управления доступом: ролевая и атрибутная модели.
35. Безопасное обновление программного обеспечения устройств по воздуху (secure OTA).
36. Управление конфигурацией парка устройств и вывод устройств из эксплуатации.
37. Методология анализа защищенности систем Интернета вещей по уровням архитектуры.
38. Методики построения модели угроз.

39. Методы и инструменты тестирования на проникновение устройств Интернета вещей.
40. Оценка рисков информационной безопасности и приоритизация мер защиты.

7.3.2 Примерные темы индивидуальных заданий и обзоров

- Разработка модели угроз для системы умного дома с голосовым управлением.
- Анализ защищенности брокера MQTT в типовой конфигурации платформы Интернета вещей.
- Обзор известных инцидентов безопасности Интернета вещей и извлеченных уроков.
- Разработка политики безопасности для системы видеонаблюдения умного пространства.
- Сравнительный анализ механизмов защиты в LoRaWAN и NB-IoT.
- Анализ рисков при использовании облачных платформ Интернета вещей для хранения телеметрии.
- Проектирование процедуры безопасного обновления программного обеспечения парка устройств.
- Обзор легковесных криптографических алгоритмов для устройств с ограниченными ресурсами.
- Анализ угроз системам контроля доступа умного здания.
- Разработка рекомендаций по повышению защищенности типового домашнего маршрутизатора и подключенных устройств.