МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ

федеральное государственное автономное образовательное учреждение
высшего образования
«МОСКОВСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»
Факультет информационных технологий

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«Кибербезопасность систем интернета вещей и робототехники»

Направление подготовки
09.03.01 Информатика и вычислительная техника

Профиль
«Киберфизические системы»

Квалификация
Бакалавриат

Формы обучения
очная

Москва, 2023 г.

Разработчик(и):

Доцент, к.т.н.  /Д.Г. Демидов /

Согласовано:

Заведующий кафедрой
«Смарт-технологии»  /Е.В. Петрунина /

Содержание

1 Цели, задачи и планируемые результаты обучения по дисциплине

Целью освоения дисциплины является получение знаний о методах взлома устройств интернета вещей и робототехники, и противодействии таким атакам.

Задачи дисциплины:

- изучить методы моделирования угроз и методологию тестирования безопасности
- изучить работу протоколов и интерфейсов устройств интернета вещей
- освоить типовые схемы атак на устройства интернета вещей
- изучить аппаратное и программное обеспечение для реализации кибератак

Обучение по дисциплине «Кибербезопасность систем интернета вещей и робототехники» направлено на формирование у обучающихся следующих компетенций:

Код и наименование компетенций	Индикаторы достижения компетенции
ПК-3. Способен разрабатывать требования и проектировать программное обеспечение	ИПК-3.1. Знает принципы осуществления кибербезопасности смарт-устройств; основы безопасности систем интернета вещей; уязвимости аппаратного и программного обеспечения. ИПК-3.2. Умеет реализовывать атаки на сетевые протоколы, порты, интерфейсы, радиоканалы; анализировать сетевые протоколы; предотвращать взломы и атаки на системы IoT ИПК-3.3. Владеет навыками проведения аудита кибербезопасности смарт-устройств; моделирования угроз для смарт-устройств; методологией тестирования безопасности

В процессе освоения образовательной программы данные компетенции, в том числе их отдельные компоненты, формируются поэтапно в ходе освоения обучающимися дисциплин (модулей), практик в соответствии с учебным планом и календарным графиком учебного процесса.

2 Место дисциплины в структуре образовательной программы

Дисциплина относится к числу учебных дисциплин блока Б1 основной профессиональной образовательной программы.

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

- Теория вероятностей и математическая статистика;
- Проектная деятельность;
- Современные тенденции в сфере информационных технологий;
- Учебная (проектная) практика;
- Производственная (проектно-технологическая) практика;
- Производственная (преддипломная) практика

3 Структура и содержание дисциплины

Общая трудоемкость дисциплины составляет 2 зачетных единицы, т.е. 72 академических часа.

3.1 Виды учебной работы и трудоемкость (по формам обучения)

3.1.1 Очная форма обучения

№ п/п	Вид учебной работы	Количество часов	Семестры	
			6	
1	**Аудиторные занятия**	**36**	36	
	В том числе:			
1.1	Лекции	18	18	
1.2	Семинарские/практические занятия			
1.3	Лабораторные занятия	18	18	
2	**Самостоятельная работа**	**36**	36	
3	**Промежуточная аттестация**			
	Дифференцированные зачеты		Зачет	
	Итого:	**72**	72	

3.2 Тематический план изучения дисциплины (по формам обучения)

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	Безопасность систем интернета вещей	8	4		0		4
2	Сетевые угрозы	18	4		6		8
3	Уязвимости аппаратного обеспечения	22	4		6		12
4	Уязвимости радиоканалов	24	6		6		12
Итого		**72**	**18**		**18**		**36**

3.3 Содержание дисциплины

№	Темы лекций и лабораторных работ
1	Лекция 1. Безопасность систем интернета вещей
2	Лекция 2. Сетевые угрозы

	Лабораторная работа 1. Исследование уязвимостей сетевых протоколов *Цель*: Формирование у студентов практических навыков анализа безопасности сетевых протоколов, применяемых в системах Интернета вещей (IoT) и робототехнике. Развитие компетенций в области выявления уязвимостей, разработки инструментов анализа трафика и реализации атак на типовые протоколы. *Содержание и порядок выполнения лабораторной работы*: • Реализовать атаку на VLAN (VLAN Hopping) • Реализовать атаку на MQTT • Разработать диссектор Wireshark для протокола DICOM • Создать диссектор C-ECHO для протокола DICOM • Разработать сканер служб DICOM для механизма сценариев Nmap • Реализовать атаку против UPnP *Результаты выполнения лабораторной работы*: • Отчет о проделанной лабораторной работе
3	Лекция 3. Уязвимости аппаратного обеспечения Лабораторная работа 2. Формирование у студентов практических навыков исследования аппаратных уязвимостей в устройствах Интернета вещей (IoT) и робототехнических систем. Развитие компетенций в области физического доступа к устройствам, извлечения прошивки и эксплуатации уязвимостей последовательных интерфейсов. *Содержание и порядок выполнения лабораторной работы*: • Осуществить взлом устройства с помощью UART и SWD • Извлечь содержимое микросхемы флеш-памяти EEPROM с SPI • Осуществить атаку на I2C с помощью Bus Pirate. *Результаты выполнения лабораторной работы*: • Отчет о проделанной лабораторной работе
4	Лекция 4. Уязвимости радиоканалов Лабораторная работа 3. Формирование у студентов практических навыков анализа безопасности беспроводных технологий, широко используемых в системах Интернета вещей (IoT) и робототехнике. Развитие компетенций в области эксплуатации уязвимостей в протоколах RFID, Bluetooth Low Energy (BLE), Wi-Fi и LoRa/LoRaWAN. *Содержание и порядок выполнения лабораторной работы*: • Реализовать атаку на RFID-систему с помощью Proxmark3 • Осуществить взлом устройства с BLE • Осуществить атаку на точку доступа Wi-Fi • Осуществить захват трафика LoRa • Реализовать атаку на LoRaWAN *Результаты выполнения лабораторной работы*: • Отчет о проделанной лабораторной работе

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. Приказ Минобрнауки России от 19.09.2017 N 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. N 48489).

3. Академический учебный план Направление подготовки: 09.03.01 Информатика и вычислительная техника Профиль: Киберфизические системы. Форма обучения: очная.

4. 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).

4.2 Основная литература

1. Чанцис Ф., Стаис И., Кальдерон П., Деирменцоглу Е., Вудс Б. Практический хакинг интернета вещей / пер. с англ. Л. Н. Акулич. – М.: ДМК Пресс, 2022. – 480 с.: ил.

2. Щербак, А. В. Информационная безопасность : учебник для вузов / А. В. Щербак. — 2-е изд. — Москва : Издательство Юрайт, 2025. — 252 с. — (Высшее образование). — ISBN 978-5-9916-4299-6. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/569267 (дата обращения: 18.05.2025).

4.3 Дополнительная литература

1. Внуков, А. А. Защита информации : учебник для вузов / А. А. Внуков. — 3-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2025. — 161 с. — (Высшее образование). — ISBN 978-5-534-07248-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/561313 (дата обращения: 18.05.2025).

2. Мельников, Е. В. Основы микропроцессорной техники : лабораторный практикум / Е. В. Мельников. — Самара : Самарский государственный технический университет, ЭБС АСВ, 2020. — 47 с. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/105222.html (дата обращения: 18.05.2025).

4.4 Электронные образовательные ресурсы

Курс ЭОР Кибербезопасность систем интернета вещей и робототехники https://online.mospolytech.ru/course/view.php?id= 15260

4.5 Лицензионное и свободно распространяемое программное обеспечение

1. Не требуется

5 Материально-техническое обеспечение

5.1 Требования к оборудованию и помещению для занятий

Лабораторные работы и самостоятельная работа студентов должны проводиться в специализированной аудитории, оснащенной современной оргтехникой и персональными компьютерами с программным обеспечением в соответствии с тематикой изучаемого материала. Число рабочих мест в аудитории должно быть достаточным для обеспечения индивидуальной работы студентов. Рабочее место преподавателя должно быть оснащены современным компьютером с подключенным к нему проектором на настенный экран, или иным аналогичным по функциональному назначению оборудованием.

5.2 Требования к программному обеспечению

Для выполнения лабораторных работ и самостоятельной работы необходимо следующее программное обеспечение:

1. Microsoft Windows.
2. Офисные приложения, Microsoft Office.
3. Веб-браузер, Chrome.
4. Microsoft Visio.

6 Методические рекомендации

6.1 Методические рекомендации для преподавателя по организации обучения

1. При подготовке к занятиям следует предварительно проработать материал занятия, предусмотрев его подачу точно в отведенное для этого время занятия. Следует подготовить необходимые материалы – теоретические сведения, задачи и др. При проведении занятия следует контролировать подачу материала и решение заданий с учетом учебного времени, отведенного для занятия.

2. При проверке работ и отчетов следует учитывать не только правильность выполнения заданий, но и оптимальность выбранных методов решения, правильность выполнения всех его шагов.

6.2 Методические указания для обучающихся по освоению дисциплины

Изучение дисциплины осуществляется в строгом соответствии с целевой установкой в тесной взаимосвязи учебным планом. Основой теоретической подготовки студентов являются аудиторные занятия, семинары и практики.

В процессе самостоятельной работы студенты закрепляют и углубляют знания, полученные во время аудиторных занятий, дорабатывают конспекты и записи, готовятся к промежуточной аттестации, а также самостоятельно изучают отдельные темы учебной программы.

На занятиях студентов, в том числе предполагающих практическую деятельность, осуществляется закрепление полученных, в том числе и в процессе самостоятельной работы, знаний. Особое внимание обращается на развитие умений и навыков установления связи положений теории с профессиональной деятельностью будущего специалиста.

Самостоятельная работа осуществляется индивидуально. Контроль самостоятельной работы организуется в двух формах:

- самоконтроль и самооценка студента;
- контроль со стороны преподавателей (текущий и промежуточный).

Текущий контроль осуществляется на аудиторных занятиях, промежуточный контроль осуществляется на зачете в письменной (устной) форме.

Критериями оценки результатов самостоятельной работы студента являются:

- уровень освоения студентом учебного материала;
- умения студента использовать теоретические знания при выполнении практических задач;
- сформированность компетенций;
- оформление материала в соответствии с требованиями.

7 Фонд оценочных средств

7.1 Методы контроля и оценивания результатов обучения

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

- 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.

Показатель	**Критерии оценивания**			
	2	**3**	**4**	**5**
ПК-3. Способен разрабатывать требования и проектировать программное обеспечение				
ИПК-3.1. Знает принципы осуществления кибербезопасности смарт-устройств; основы безопасности систем интернета вещей; уязвимости аппаратного и программного обеспечения. ИПК-3.2. Умеет реализовывать атаки на сетевые протоколы, порты, интерфейсы, радиоканалы;	Обучающийся демонстрирует полное отсутствие или недостаточное соответствие материалу дисциплины знаний, указанных в индикаторах компетенций дисциплины.	Обучающийся демонстрирует неполное соответствие следующих знаний, указанных в индикаторах компетенций дисциплины. Допускаются значительные ошибки, проявляется недостаточность знаний, по ряду показателей, обучающийся испытывает значительные затруднения	Обучающийся демонстрирует частичное соответствие следующих знаний, указанных в индикаторах компетенций дисциплины. Но допускаются незначительные ошибки, неточности, затруднения при аналитических операциях.	Обучающийся демонстрирует полное соответствие следующих знаний, указанных в индикаторах компетенций дисциплины. Свободно оперирует приобретенными знаниями.

анализировать сетевые протоколы; предотвращать взломы и атаки на системы IoT ИПК-3.3. Владеет навыками проведения аудита кибербезопасности смарт-устройств; моделирования угроз для смарт-устройств; методологией тестирования безопасности		при оперировании знаниями при их переносе на новые ситуации.		

Шкала оценивания результатов промежуточной аттестации и её описание

Форма промежуточной аттестации: экзамен.

Шкала оценивания	**Описание**
Зачтено	Выполнены все **обязательные условия подготовки студента к промежуточной аттестации**, предусмотренные программой дисциплины. Обучающийся демонстрирует соответствие знаний, умений, навыков заявленным индикаторам, оперирует приобретенными знаниями, умениями, навыками. При этом могут быть допущены незначительные ошибки, неточности, затруднения при аналитических операциях, переносе знаний и умений на новые, нестандартные ситуации.
Не зачтено	Не выполнены обязательные **условия подготовки студента к промежуточной аттестации**, предусмотренные программой дисциплины, ИЛИ обучающийся демонстрирует неполное соответствие знаний, умений, навыков заявленным индикаторам и допускает значительные ошибки при оперировании знаниями и умениями и применении приобретенных навыков в стандартных ситуациях

7.3 Оценочные средства

7.3.1 Перечень оценочных средств

№ ОС	Наименование оценочного средства	Краткая характеристика оценочного средства	Представление оценочного средства в ФОС
1	Устный опрос / собеседование,	Средство контроля, организованное как презентация обучающимся результатов выполнения проекта с демонстрацией наглядных материалов и ответов на вопросы на тему доклада, теме, проблеме и т.п.	Контрольные вопросы
2	Тест	Система стандартизированных заданий, позволяющая автоматизировать процедуру измерения уровня знаний и умений обучающегося.	Фонд тестовых заданий

7.3.2 Контрольные вопросы

1. Какие особенности архитектуры IoT-систем создают уникальные риски с точки зрения кибербезопасности?
2. Почему традиционные подходы к ИБ часто неприменимы к IoT-устройствам?
3. Какие принципы «безопасности по умолчанию» (security by default) должны соблюдаться при разработке IoT-устройств?
4. Что такое «поверхность атаки» в контексте IoT и как её минимизировать?
5. Как обеспечивается аутентификация и авторизация устройств в распределённой IoT-инфраструктуре?
6. Какие стандарты и регламенты существуют для обеспечения безопасности IoT (например, ETSI EN 303 645, NISTIR 8200)?
7. Какие типы данных, собираемых IoT-устройствами, требуют особой защиты?
8. Как организуется безопасное обновление прошивки (OTA — over-the-air) в IoT-устройствах?
9. Какие методы используются для защиты конфиденциальности пользователей в IoT-системах?
10. Какие последствия могут возникнуть при компрометации умного дома или промышленного IoT-решения?
11. 2. Сетевые угрозы
12. Какие типы сетевых атак наиболее характерны для IoT-устройств (DDoS, MITM, подмена DNS и др.)?
13. Почему IoT-устройства часто становятся частью ботнетов (например, Mirai)?
14. Как работает атака типа «человек посередине» (MITM) в IoT-сетях и как её предотвратить?
15. Какие протоколы передачи данных (MQTT, CoAP, HTTP, LoRaWAN) используются в IoT и какие у них уязвимости?
16. Как обеспечивается шифрование трафика между IoT-устройством и облаком?
17. Что такое «zero-trust архитектура» и как она применима к IoT?
18. Какие угрозы возникают при использовании публичных Wi-Fi сетей для подключения IoT-устройств?

19. Какие меры защиты применяются на сетевом уровне (межсетевые экраны, IDS/IPS, сегментация сети)?
20. Как организуется безопасная интеграция IoT-устройств с корпоративной ИТ-инфраструктурой?
21. Какие риски связаны с использованием облачных платформ для хранения и обработки данных IoT?
22. 3. Уязвимости аппаратного обеспечения
23. Какие типы аппаратных уязвимостей характерны для микроконтроллеров и SoC в IoT и робототехнике?
24. Что такое side-channel атаки и как они применяются к IoT-устройствам?
25. Как осуществляется реверс-инжиниринг аппаратного обеспечения и как ему противодействовать?
26. Какие меры защиты встраиваются в чипы для предотвращения несанкционированного доступа (secure boot, TPM, TrustZone)?
27. Что такое JTAG/SWD-интерфейсы и какие риски они несут с точки зрения безопасности?
28. Как обеспечивается защита ключей шифрования в аппаратных модулях (HSM, secure element)?
29. Какие угрозы связаны с использованием компонентов от недобросовестных поставщиков («аппаратные закладки»)?
30. Какие методы применяются для физической защиты IoT-устройств от вскрытия и модификации?
31. Как влияет отсутствие аппаратной поддержки криптографии на безопасность устройства?
32. Какие примеры известных аппаратных уязвимостей (Spectre, Meltdown, Rowhammer) применимы к IoT-системам?
33. 4. Уязвимости радиоканалов
34. Какие беспроводные технологии используются в IoT (Wi-Fi, Bluetooth, Zigbee, Z-Wave, LoRa, NB-IoT) и какие у них уязвимости?
35. Как осуществляется перехват и анализ радиотрафика (например, с помощью SDR)?
36. Что такое атака повтора (replay attack) в беспроводных IoT-сетях и как её предотвратить?
37. Какие меры защиты применяются для шифрования радиоканалов (например, AES в Zigbee)?
38. Какие риски связаны с использованием устаревших протоколов (например, WEP, Bluetooth 2.0)?
39. Как работает атака типа «глушение сигнала» (jamming) и как обеспечить отказоустойчивость канала?
40. Что такое spoofing в радиоканале и как его обнаружить?
41. Какие особенности безопасности у технологий LPWAN (LoRaWAN, Sigfox)?
42. Как организуется безопасная аутентификация устройств при подключении по радиоканалу?
43. Какие угрозы возникают при использовании незащищённых beacon-сообщений или служебных пакетов?
44. Дополнительные вопросы по интеграции тем (IoT + робототехника)
45. Какие особенности безопасности характерны для автономных роботизированных систем (дроны, AGV, сервисные роботы)?
46. Какие угрозы возникают при дистанционном управлении роботами через интернет?
47. Как обеспечивается целостность сенсорных данных в робототехнических системах?
48. Какие риски связаны с использованием компьютерного зрения и ИИ в роботах с точки зрения безопасности?

49. Как организуется безопасное взаимодействие робота с облачной платформой и другими устройствами?
50. Какие принципы «безопасности на всех этапах жизненного цикла» применимы к IoT и робототехнике?

7.3.3 Образцы тестовых заданий

::ТЗ :: Что такое интернет вещей (IoT)?
{
~Сеть компьютеров, соединенных друг с другом
=Сеть устройств, способных обмениваться данными и взаимодействовать друг с другом
~Система для управления умным домом
~Технология для создания виртуальной реальности
}

::ТЗ :: Какие основные угрозы безопасности существуют для устройств IoT?
{
=Физический доступ, кибератаки, вредоносное ПО
~Только физический доступ
~Только кибератаки
~Только вредоносное ПО
}

::ТЗ :: Что такое уязвимость нулевого дня?
{
~Известная уязвимость, для которой уже существует патч
=Новая уязвимость, для которой еще не существует патча
~Уязвимость в программном обеспечении, которая была устранена
~Уязвимость, связанная с физическим доступом к устройству
}

::ТЗ :: Что такое атака “человек посередине” (Man-in-the-Middle)?
{
~Атака на физическое местоположение устройства
=Атака, при которой злоумышленник перехватывает и изменяет данные
~Атака с использованием вредоносного ПО
~Атака на сетевую инфраструктуру
}

::ТЗ :: Какую роль играет шифрование в обеспечении безопасности IoT?
{
~Увеличение скорости передачи данных
=Защита данных при передаче и хранении
~Уменьшение энергопотребления устройства
~Улучшение физической защиты устройства
}

::ТЗ :: Что такое защищенный протокол в контексте IoT?
{
~Протокол, который не использует шифрование

=Протокол, использующий шифрование для защиты данных
~Протокол для управления умным домом
~Протокол для передачи видеоданных
}

::ТЗ :: Какую функцию выполняет аутентификация в IoT?
{
=Подтверждение подлинности устройства и пользователя
~Шифрование данных
~Защита от физических атак
~Управление энергопотреблением
}

::ТЗ :: Что такое атака отказа в обслуживании (Denial of Service)?
{
~Физическое повреждение устройства
=Перегрузка сети или устройства запросами, что делает его недоступным
~Кража данных с устройства
~Изменение данных в процессе передачи
}

::ТЗ :: Какую роль играют регулярные обновления программного обеспечения в обеспечении безопасности IoT?
{
~Повышение производительности устройства
=Исправление известных уязвимостей и внедрение улучшений безопасности
~Снижение энергопотребления
~Улучшение пользовательского интерфейса
}

::ТЗ :: Что такое сегментация сети в контексте безопасности IoT?
{
~Объединение всех устройств в одну сеть
=Разделение сети на изолированные сегменты для минимизации риска распространения атаки
~Использование одного пароля для всех устройств
~Увеличение пропускной способности сети
}