Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Максимов Алексей Борисович
Должность: директор департамента по образовательной политике
Дата подписания: 14.07.2026 11:08:05
Уникальный программный ключ:
8db180d1a3f02ac9e60521a5672742735c18b1d6

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«МОСКОВСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»
(МОСКОВСКИЙ ПОЛИТЕХ)

Факультет информационных технологий

УТВЕРЖДАЮ
Декан факультета
«Информационных технологий»
_____ / Д.Г. Демидов /
«26» февраля 2026 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
«Защита встраиваемых систем и интернета вещей»

Направление подготовки 10.05.03
«Информационная безопасность автоматизированных систем»

Образовательная программа (профиль):
«Безопасность открытых информационных систем»

Квалификация (степень) выпускника
Специалист по защите информации

Формы обучения
Очная

Москва, 2026 г.

Разработчик(и):

Доцент, к.т.н., доцент  /И.В. Калуцкий/

Согласовано:
Заведующий кафедрой «Информационная безопасность»  И.В.Калуцкий

Содержание

1	Цели, задачи и планируемые результаты обучения по дисциплине	4
2	Место дисциплины в структуре образовательной программы	5
3	Структура и содержание дисциплины	5
3.1	Виды учебной работы и трудоемкость	5
3.2	Тематический план изучения дисциплины	6
3.3	Содержание дисциплины	7
3.4	Тематика семинарских/практических и лабораторных занятий	8
3.5	Тематика курсовых проектов (курсовых работ)	9
4	Учебно-методическое и информационное обеспечение	9
4.1	Нормативные документы и ГОСТы	9
4.2	Основная литература	10
4.3	Дополнительная литература	10
4.4	Электронные образовательные ресурсы	11
4.5	Лицензионное и свободно распространяемое программное обеспечение	11
4.6	Современные профессиональные базы данных и информационные справочные системы	11
5	Материально-техническое обеспечение	11
6	Методические рекомендации	11
6.1	Методические рекомендации для преподавателя по организации обучения	11
6.2	Методические указания для обучающихся по освоению дисциплины	11
7	Фонд оценочных средств	11
7.1	Методы контроля и оценивания результатов обучения	11
7.2	Шкала и критерии оценивания результатов обучения	12
7.3	Оценочные средства	13

1 Цели, задачи и планируемые результаты обучения по дисциплине

Целью освоения дисциплины «Защита встраиваемых систем и интернета вещей»»:

- сформировать у слушателей необходимый объем теоретических и практических знаний в области защиты встраиваемых систем и интернета вещей (IoT), умений и навыков по обеспечению безопасности таких систем, а также изучить инструментальные средства и методы для их практической реализации.

Задачи преподавания дисциплины:

- Рассмотреть архитектурные особенности и уязвимости типовых встраиваемых систем и IoT-устройств.
- Рассмотреть модели угроз и векторы атак на компоненты IoT-экосистемы (устройства, связи, облако, приложения).
- Рассмотреть методы и протоколы обеспечения конфиденциальности, целостности и аутентичности данных в беспроводных сетях IoT.
- Рассмотреть модели и механизмы управления доступом и идентификации в IoT-сетях.
- Рассмотреть практические методы анализа защищенности встраиваемых систем.
- Рассмотреть основы криптографических методов защиты и особенности их применения в ресурсо-ограниченных средах.
- Рассмотреть современные стандарты безопасности для интернета вещей.

В результате освоения дисциплины «Защита встраиваемых систем и интернета вещей» у обучающихся формируются следующие компетенции и должны быть достигнуты следующие результаты обучения как этап формирования соответствующих компетенций:

- способен разрабатывать и эксплуатировать системы защиты информации открытых информационных систем

- способен осуществлять контроль обеспечения информационной безопасности и проводить верификацию данных в открытых информационных системах..

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

Код и наименование компетенций	Индикаторы достижения компетенции
ОПК-5.2. способен разрабатывать и эксплуатировать системы защиты информации открытых информационных систем	ИОПК-5.2.1 Выполняет обследование объекта защиты, обосновывает необходимость создания системы защиты информации, разрабатывает техническое задание на создание подсистемы информационной безопасности для открытой информационной системы; ИОПК-5.2.2 На основе требований к открытой информационной системе (технического, программного, информационного обеспечения и технологии обработки (передачи) информации) разрабатывает организационно-технические мероприятия по защите информации организационно-распорядительные документы по обеспечению информационной безопасности; ИОПК-5.2.3 Проводит опытную эксплуатацию средств защиты

	информации в комплексе с другими техническими и программными средствами открытой информационной системы, разрабатывает методики и документы приемо-сдаточных испытаний средств защиты информации
ОПК-5.3. способен осуществлять контроль обеспечения информационной безопасности и проводить верификацию данных в открытых информационных системах.	ОПК-5.3.1 Понимает значение контроля информационной безопасности, применяет различные виды контроля обеспечения информационной безопасности; ОПК-5.3.2 Проводит контроль эффективности защиты информации (организационный и технический) в открытых информационных системах ОПК-5.3.3 Определяет виды и категории данных, подлежащих обработке в открытой информационной системе, их объемы, структуру, технологии обработки и передачи, методы верификации и контроля целостности; проводит верификацию и контроль целостности данных

2 Место дисциплины в структуре образовательной программы

Дисциплина «Защита встраиваемых систем и интернета вещей» относится к числу учебных дисциплин обязательной части (Б1.1) основной образовательной программы (Б1.1.45).

Изучение дисциплины опирается на знания, умения и навыки, приобретенные в предшествующих дисциплинах: «Основы информационной безопасности», «Сети и системы передачи информации», «Безопасность систем баз данных», «Электроника и самотехника».

3 Структура и содержание дисциплины

Общая трудоемкость дисциплины составляет 4 зачетные единицы, т.е. 144 часа (лабораторные занятия – 72 часа, самостоятельная работа - 72 часа, форма контроля – экзамен) в 9 семестре.

Структура и содержание дисциплины «Защита встраиваемых систем и интернета вещей» по срокам и видам работы отражены в приложении

3.1 Виды учебной работы и трудоемкость

(по формам обучения)

3.1.1 Очная форма обучения

№ п/п	Вид учебной работы	Количество часов	Семестры	
			9	
1	**Аудиторные занятия**	**72**	72	

	В том числе:			
1.1	Лекции			
1.2	Семинарские/практические занятия			
1.3	Лабораторные занятия	72	72	
2	**Самостоятельная работа**	**72**	72	
	В том числе:			
2.1	…			
3	**Промежуточная аттестация**			
	Зачет/диф.зачет/экзамен		экзамен	
	Итого	**144**		

3.1.2 Очно-заочная форма обучения
Не предусмотрена

3.1.3 Заочная форма обучения
Не предусмотрена

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	
1.1	Тема 1. Безопасность интернета вещей.	16			8		8
1.2	Тема 2. Моделирование угроз.	24			12		12
1.3	Тема 3. Методология тестирования безопасности.	16			8		8
1.4	Тема 4. Взлом сети.	24			12		12
1.5	Тема 5. Взлом аппаратной части системы.	24			12		12
1.6	Тема 6. Взлом радиоканалов.	16			8		8
1.7	Тема 7. Атаки на экосистему IoT.	24			12		12
Итого		**144**			**72**		**72**

3.2.2 Очно-заочная форма обучения
Не предусмотрена.

3.2.2 Заочная форма обучения
Не предусмотрена

3.3 Содержание дисциплины

№ п/п	Раздел (тема) дисциплины	Содержание
1.1	Тема 1. Безопасность интернета вещей.	Основные понятия и принципы безопасности IoT. Особенности архитектуры интернета вещей, уязвимости устройств и сетей. Методы защиты данных и каналов связи. Риски, связанные с массовым внедрением IoT в бытовую и промышленную среду. Современные стандарты и подходы к кибербезопасности IoT.
1.2	Тема 2. Моделирование угроз.	Понятие угрозы информационной безопасности. Классификация угроз и уязвимостей в системах IoT. Методологии моделирования угроз (STRIDE, DREAD, PASTA и др.). Определение активов, потенциальных атакующих и сценариев атак. Построение моделей рисков и оценка вероятности реализации угроз.
1.3	Тема 3. Методология тестирования безопасности.	Подходы к тестированию безопасности IoT-систем. Этапы и методы проведения анализа: тестирование на проникновение, аудит конфигураций, анализ исходного кода и сетевого трафика. Используемые инструменты и фреймворки. Формирование отчетов о результатах тестирования и рекомендации по устранению уязвимостей.
1.4	Тема 4. Взлом сети.	Типовые методы атак на сетевую инфраструктуру IoT. Анализ сетевого взаимодействия и протоколов. Перехват, подмена и анализ данных в сетях. Использование инструментов для взлома Wi-Fi, Bluetooth и других сетевых интерфейсов. Практические аспекты обнаружения и предотвращения сетевых атак.
1.5	Тема 5. Взлом аппаратной части системы.	Физический доступ и исследование устройств IoT. Методы анализа аппаратной части: JTAG, UART, SPI, I²C, NAND и др. Извлечение прошивки, анализ содержимого памяти, обратная разработка. Аппаратные закладки, побочные каналы, защита от несанкционированного доступа и модификации.
1.6	Тема 6. Взлом радиоканалов.	Особенности беспроводной связи в IoT. Уязвимости радиоинтерфейсов: RFID, NFC, ZigBee, LoRaWAN, BLE. Методы анализа радиотрафика, перехват и декодирование сигналов. Инструменты и оборудование для тестирования радиоканалов. Меры защиты и шифрования данных в беспроводных системах.
1.7	Тема 7. Атаки на экосистему IoT.	Комплексные атаки на инфраструктуру интернета вещей. Компрометация облачных сервисов, мобильных приложений, шлюзов и пользовательских устройств. Масштабные ботнеты и DDoS-атаки с использованием IoT. Анализ инцидентов и стратегия построения устойчивой экосистемы безопасности.

3.4 Тематика семинарских/практических и лабораторных занятий

3.4.1 Семинарские/практические занятия

Не предусмотрены учебным планом.

3.4.2 Лабораторные занятия

№	Наименование лабораторной работы	Объем, час.
1	Выполнение работы №1 «MQTT-симулятор»	8
2	Выполнение работы №2 «Улучшение MQTT-системы: мониторинг, шифрование и безопасность»	12
3	Выполнение работы №3 «Анализ сетевого трафика (pcap) и построение карты устройств»	8
4	Выполнение работы №4 «Byte-at-a-time decryption»	12
5	Выполнение работы №5 «Работа с учебным стендом»	12
6	Выполнение работы №6 «Packet Tracer. Подключение устройств IoT и мониторинг их работы»	8
7	Выполнение работы №7 «Packet Tracer. Управление IoT-устройствами»	12
Итого		72

3.5 Тематика курсовых проектов (курсовых работ)

Курсовое проектирование по данной дисциплине учебным планом не запланировано.

4 Учебно-методическое и информационное обеспечение

4.1 Нормативные документы и ГОСТы

1. Программа составлена в соответствии с Федеральным государственным образовательным стандартом высшего образования по направлению подготовки бакалавров 10.05.03 «Информационная безопасность автоматизированных систем».

4.2 Основная литература

1. «Архитектура операционных систем мобильных устройств» (Архитектура операционных систем мобильных устройств : учебное пособие / И. В. Синицын, С. М. Трушин, Ю. А. Воронцов, Е. К. Михайлова. — Москва : РТУ МИРЭА, 2022. — 343 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/265724 (Дата обращения 10.08.2025).
2. Белоус, А. И. Основы кибербезопасности. Стандарты, концепции, методы и средства обеспечения : энциклопедия / А. И. Белоус, В. А. Солодуха. — Москва : Техносфера, 2021. — 482 с. — ISBN 978-5-94836-612-8. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/181222 (Дата обращения 10.08.2025).
3. «Принципы построения и функционирования аппаратно-программных средств телекоммуникационных систем: Часть 2: Сетевые операционные системы и принципы обеспечения информационной безопасности в сетях» (Макаренко, С. И. Принципы построения

и функционирования аппаратно-программных средств телекоммуникационных систем : учебное пособие / С. И. Макаренко, А. А. Ковальский, С. А. Краснов. — Санкт-Петербург : , 2020 — Часть 2 : Сетевые операционные системы и принципы обеспечения информационной безопасности в сетях — 2020. — ISBN 978-5-6044429-8-2. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/329378

4. Паршин, К. А. Методы и средства проектирования информационных систем и технологий : учебно-методическое пособие / К. А. Паршин. — Екатеринбург : , 2018. — 129 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/121337 (дата обращения: 01.02.2022). — Режим доступа: для авториз. пользователей. — С. 1.

4.3 Дополнительная литература

1. OASIS. MQTT Version 3.1.1 Plus Errata 01. — (Официальная спецификация протокола MQTT.) [Электронный ресурс]. — Режим доступа: https://mqtt.org/mqtt-specification/ (Дата обращения 10.08.2025).

2. Eclipse Foundation. paho-mqtt — Python Client Library Documentation. — (Документация по библиотеке Paho MQTT для Python.) [Электронный ресурс]. — Режим доступа: https://www.eclipse.org/paho/index.php?page=clients/python/index.php (Дата обращения 10.08.2025).

3. Docker, Inc. Docker Documentation. — (Официальное руководство по Docker и Docker Compose.) [Электронный ресурс]. — Режим доступа: https://docs.docker.com/ (Дата обращения 10.08.2025).

4. Mosquitto MQTT Broker. Eclipse Mosquitto Documentation. — (Описание установки и настройки брокера MQTT Mosquitto.) [Электронный ресурс]. — Режим доступа: https://mosquitto.org/documentation/ (Дата обращения 10.08.2025).

5. InfluxData. InfluxDB Documentation. — (Руководство по работе с базой данных временных рядов InfluxDB.) [Электронный ресурс]. — Режим доступа: https://docs.influxdata.com/influxdb/ (Дата обращения 10.08.2025).

6. InfluxData. Telegraf Documentation. — (Описание агента для сбора метрик и интеграции с MQTT и InfluxDB.) [Электронный ресурс]. — Режим доступа: https://docs.influxdata.com/telegraf/ (Дата обращения 10.08.2025).

7. Grafana Labs. Grafana Documentation. — [Электронный ресурс]. — Режим доступа: https://grafana.com/docs/ (Дата обращения 10.08.2025).

8. Wireshark Foundation. Wireshark User’s Guide. — [Электронный ресурс]. — Режим доступа: https://www.wireshark.org/docs/ (Дата обращения 10.08.2025).

9. Сандерс, К. Практический анализ пакетов: использование Wireshark для решения реальных проблем в сетях / К. Сандерс ; [пер. с англ.]. — 3-е изд. — Сан-Франциско : No Starch Press, 2017. — 467 с.

10. O’Reilly Media. Мониторинг сетевой безопасности с помощью Wireshark и tcpdump / O’Reilly Media. — [б. м.] : O’Reilly, 2020. — 289 с.

11. NIST. FIPS 197 — Advanced Encryption Standard (AES) [Электронный ресурс]. — Режим доступа: https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.197.pdf, свободный. — Загл. с экрана. — Яз. англ. (Дата обращения 10.08.2025)

12. RSA Laboratories. PKCS #7: Cryptographic Message Syntax Standard [Электронный ресурс]. — Режим доступа: https://www.rfc-editor.org/rfc/rfc2315, свободный. — Загл. с экрана. — Яз. англ. (Дата обращения 10.08.2025)

13. Демиденко, А. MQTT и CoAP для начинающих: Протоколы для умного дома / А. Демиденко. — Москва : [б. и.], 2022. — 156 с.

14. Practical Internet of ThingsSecurity Drew Van Duren 2016 Packt Publishing — Яз. англ. — BIRMINGHAM - MUMBAI: Packt Publishing, 2016. – 480 с.

15. Практический хакинг интернета вещей Полное руководство по атакам на устройства интернета вещей Фотиос Чанцис, Иоаннис Стаис, Паулино Кальдерон, Евангелос Деирменцоглу, Бо Вудс; [пер. с англ. Л. Н. Акулич.] — Москва: ДМК Пресс, 2022. – 313 с.

16. Хиллар, Г. С. MQTT Essentials - A Lightweight IoT Protocol: The preferred IoT publish-subscribe lightweight messaging protocol / Г. С. Хиллар. — [б. м.] : Packt Publishing, 2017. — 314 с. (Дата обращения 10.08.2025)

17. Коуп, С. The Mosquitto Broker For Complete Beginners / С. Коуп. — [б. м.] : Independently published, 2021. — 189 с.

18. Пульвер, Т. Hands-On Internet of Things with MQTT / Т. Пульвер. — [б. м.] : Packt Publishing, 2019. — 278 с.

19. Гондособрото, Р. Internet of Things from Scratch / Р. Гондособрото. — [б. м.] : Packt Publishing, 2023. — 402 с.

20. The CryptoPals Challenges [Электронный ресурс]. — Режим доступа: https://cryptopals.com/sets/2, свободный. — Загл. с экрана. — Яз. англ. (Дата обращения 10.08.2025).

4.4 Электронные образовательные ресурсы

1. Документация Yandex Cloud [Электронный ресурс] — URL: https://cloud.yandex.ru/docs (дата обращения: 01.02.2022).
2. ЭОР https://online.mospolytech.ru/course/view.php?id=15791

4.5 Лицензионное и свободно распространяемое программное обеспечение

1. Операционная система Microsoft Windows от 7 версии и выше; Microsoft Office или Open Office, браузер (Firefox/Google Chrome /Explorer).

4.6 Современные профессиональные базы данных и информационные справочные системы

1. Документация Yandex Cloud [Электронный ресурс] — URL: https://cloud.yandex.ru/docs (дата обращения: 01.02.2022).

5 Материально-техническое обеспечение

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

Для проведения лабораторных занятий необходимо наличие компьютерных классов оборудованных современной вычислительной техникой из расчета одно рабочее место на одного обучаемого.

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 и практической подготовки студентов являются лекции и лабораторные работы.

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

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:

- проведение лабораторных работ (практических занятий с использованием спецтехники) и их защита;
- самостоятельная подготовка и проведение презентаций по темам дисциплины;
- экзамен.

7.2 Шкала и критерии оценивания результатов обучения

Форма промежуточной аттестации: экзамен.

По итогам промежуточной аттестации по дисциплине (модулю) выставляется оценка «отлично», «хорошо», «удовлетворительно» или «неудовлетворительно».

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 неполное, правильное соответствие знаний, умений, навыков приведенным в таблицах

	показателей, либо если при этом были допущены 2-3 несущественные ошибки.
Удовлетворительно	Выполнены все виды учебной работы, предусмотренные учебным планом. Студент демонстрирует соответствие знаний, в котором освещена основная, наиболее важная часть материала, но при этом допущена одна значительная ошибка или неточность.
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

7.3.1 Текущий контроль

Оценочные средства для текущей аттестации

- Защита отчетов о выполнении лабораторных работ

7.3.2 Промежуточная аттестация

Оценочные средства для промежуточной аттестации

- Экзамен

Список вопросов для экзамена по дисциплине:

1. Интернет вещей: понятие, принципы функционирования и структура.
2. Особенности IoT-устройств по сравнению с традиционными ИТ-системами
3. Типы коммуникационных протоколов, используемых в IoT, и их особенности
4. Основные подходы к обеспечению безопасности систем интернета вещей
5. Проблемы жизненного цикла IoT-устройств и их влияние на безопасность
6. Риски для общества и личности при нарушении безопасности IoT
7. Роль потребителей, производителей и международных организаций в обеспечении безопасности IoT
8. Законодательное регулирование и правовые аспекты хакинга IoT
9. Экономические и технические факторы, влияющие на безопасность IoT
10. Этические и правовые проблемы эксплуатации IoT-устройств
11. Понятие моделирования угроз, его значение и этапы
12. Модель STRIDE: назначение, классификация угроз и шаги моделирования
13. Система оценки рисков DREAD: суть и показатели, ранжирование угроз
14. Подходы к моделированию угроз: программно-ориентированный, ресурсный, ориентированный на злоумышленника; альтернативные модели (PASTA, Trike, OCTAVE, VAST)

15. Визуальные средства моделирования угроз: диаграммы потоков данных, UML, диаграммы состояний
16. Использование деревьев атак (attack trees) для анализа угроз
17. Распространённые угрозы и типы атак на IoT-системы (подавление сигнала, воспроизведение, вмешательство в настройки, клонирование узлов)
18. Нарушения безопасности и конфиденциальности данных в IoT
19. Проблемы осведомленности пользователей как фактор киберрисков
20. Атаки на сетевые протоколы и службы, методы анализа трафика и выявления уязвимых каналов
21. Тестирование безопасности беспроводных протоколов: Wi-Fi, Bluetooth, SDR
22. Оценка безопасности веб-приложений, API и взаимодействия между устройством и облаком
23. Контроль доступа, аутентификация и управление сервисами в IoT-среде
24. Проверка ввода данных и защита от внедрения кода (SQLi, XSS, XXE)
25. Аппаратный уровень IoT-систем: уязвимости, периферийные интерфейсы (UART, JTAG, SWD, SPI, I2C) и методы их проверки
26. Методы получения, анализа и эмуляции прошивки (binwalk, firmwalker, FIRMADYNE)
27. Методы внедрения и тестирования бэкдоров в прошивке
28. Тестирование физической устойчивости и атак по побочным каналам
29. Принцип работы RFID-систем, типы меток (активные, пассивные, полупассивные) и их классификация
30. Структура памяти RFID-метки и уязвимости, механизмы защиты и методы атак
31. Архитектура и особенности BLE (GAP, GATT), рекламные пакеты и поверхность атаки
32. Принцип работы Wi-Fi Direct, уязвимости WPS и методы взлома WPA/WPA2
33. Особенности LPWAN, LoRaWAN: структура сети, процедуры присоединения, типичные атаки и меры защиты
34. Основные проблемы безопасности мобильных приложений Android и iOS
35. Распространённые типы атак на мобильные приложения IoT (MITM, установка приложений из сторонних источников, утечки данных)
36. Методы статического и динамического анализа мобильных приложений, выявление hardcoded-данных, проверка защищённости памяти и файлов
37. Принципы реверс-инжиниринга мобильных приложений (Radare2, jadx, dex2jar, lldb)
38. Уязвимости WebView, SQL-инъекции и XSS, перехват и расшифровка HTTPS-трафика
39. Особенности защиты Keychain (iOS) и SharedPreferences (Android), обход джейлбрейка и root-прав
40. Средства аппаратной защиты и безопасного хранения ключей (Secure Enclave, Titan M, TrustZone, SGX)
41. Подходы к моделированию угроз для мобильных приложений: архитектурный, компонентный, атакующий устройств IoT: пароли по умолчанию, раскрытие уязвимостей, обновления.

Пример билета.

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

«МОСКОВСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»
(МОСКОВСКИЙ ПОЛИТЕХ)

Факультет информационных технологий
Кафедра: Информационная безопасность
Дисциплина: Защита встраиваемых систем и интернета вещей
Специалисты. Курс 5, семестр 9

ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ № 1

1. Модель STRIDE: назначение, классификация угроз и шаги моделирования
2. Распространённые угрозы и типы атак на IoT-системы
3. Контроль доступа, аутентификация и управление сервисами в IoT-среде
4. Распространённые типы атак на мобильные приложения IoT

Преподаватель _____ / Калуцкий И.В. /