МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

«МОСКОВСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»

(МОСКОВСКИЙ ПОЛИТЕХ)

Факультет машиностроения

УТВЕРЖДАЮ

Декан

_____ /Е.В.Сафонов/

«27» апреля 2023 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Информационная безопасность

Специальность
11.05.01 Радиоэлектронные системы и комплексы

Профиль
Радиоэлектронные системы передачи информации

Квалификация
Инженер

Формы обучения
очная

Москва, 2023 г.

Разработчик(и):

Доцент кафедры «Автоматика и управление»,
к.т.н.  А.А. Филимонова/

Согласовано:
Заведующий кафедрой «Автоматика и управление»,
д.т.н., профессор  /А.А. Радионов/

Руководитель образовательной программы
д.т.н., профессор  /А.А. Радионов/

Содержание

1 Цели, задачи и планируемые результаты обучения по дисциплине

Целью дисциплины является получение обучающимися систематизированных теоретических знаний о базовых принципах и методах построения интернета вещей и возможностях обеспечения информационной безопасности, в том числе в радиотехнических системах.

Задачи дисциплины заключаются в освоении типовых приемов проектирования средств обеспечения информационной безопасности отдельных участков интернета вещей и принципов имитационного моделирования; привитии базовых навыков анализа и проектирования защищенных участков интернета вещей.

Обучение по дисциплине «Информационная безопасность» направлено на формирование у обучающихся следующих компетенций:

Код и наименование компетенций	Индикаторы достижения компетенции	Наименование показателя оценивания
ПК-5. Способен проектировать, устанавливать, настраивать и поддерживать в работоспособном состоянии компоненты системы обеспечения информационной безопасности в радиотехнических системах	ИПК-5.1. Проводит анализ угроз безопасности информации в радиотехнических системах в процессе их эксплуатации ИПК-5.2. Разрабатывает и выполняет мероприятия по защите информации в радиотехнических системах для обеспечения непрерывного функционирования в процессе их эксплуатации; ИПК-5.3. Применяет штатные средства защиты информации, администрирует и конфигурирует компоненты системы обеспечения безопасности в радиотехнических системах.	**Знать:** - методику анализа уязвимостей в подсистеме обеспечения безопасности стандартов в радиотехнических системах и сетях интернета вещей; - общие принципы функционирования и взаимодействия устройств в рамках основных информационных систем; - протоколы и алгоритмы взаимодействия в сетях интернета вещей; - источники и виды угроз безопасности в информационных системах и сетях интернета вещей; - основные подходы и методы оценки рисков информационной безопасности в сетях интернета вещей. **Уметь:** вырабатывать стратегию действий по защите информации в радиотехнических системах; осуществлять выбор наиболее подходящей для заданных условий конфигурации сети интернета вещей; - применять методику анализа уязвимостей в подсистеме

		обеспечения безопасности сети интернета вещей. **Владеть:** навыками работы по разработке планов и проведению мероприятий по организации защиты информации радиотехнических система и систем «Интернета вещей»; методами настройки встроенных механизмов защиты информационной системы; навыками применения стандартных средств защиты информации.

2 Место дисциплины в структуре образовательной программы

Дисциплина относится к части, формируемой участниками образовательных отношений блока Б1 «Дисциплины (модули)». Дисциплина непосредственно связана со следующими дисциплинами и практиками ООП:

Автоматизированные системы контроля и управления радиоэлектронными средствами
Интеллектуальный анализ данных
Информационные технологии
Кодирование и шифрование информации в радиоэлектронных системах
Компьютерные и промышленные интерфейсы и сети
Основы конструирования и технологии производства РЭС
Производственная практика (преддипломная)
Управление персоналом

3 Структура и содержание дисциплины

Общая трудоемкость дисциплины составляет 4 зачетные единицы (144 часа).

3.1 Виды учебной работы и трудоемкость

№ п/п	Вид учебной работы	Количество часов	Семестры
			10
1	**Аудиторные занятия**	**72**	**72**
	В том числе:		
1.1	Лекции	36	36
1.2	Семинарские/практические занятия	36	36
1.3	Лабораторные занятия	0	0
2	**Самостоятельная работа**	**72**	**72**
	В том числе:		
2.1	Подготовка к лекциям	18	18
2.2	Подготовка к семинарам	36	36
2.3	Подготовка к экзамену по дисциплине	18	18
3	**Промежуточная аттестация**		
	Зачет/диф.зачет/экзамен	-	Экзамен
	Итого	**144**	**144**

3.2 Тематический план изучения дисциплины

№ п/п	Разделы/темы дисциплины	Трудоемкость, час					
		Всего	Аудиторная работа				Самостоятельная работа
			Лекции	Семинарские/ практические занятия	Лабораторные занятия	Практическая подготовка	
1	**Раздел 1. Введение в информационную безопасность Интернета вещей**	**38**	**12**	**8**	**0**	**0**	**18**
1.1	Тема 1. Информационная безопасность киберфизических систем, кибербезопасность в интернете вещей: основные стандарты, понятия, определения.		4	0	0	0	4
1.2	Тема 2. Протоколы связи и аутентификации для киберфизических систем и «Интернет вещей»: обзор, особенности, проблемы безопасности.		4	4	0	0	8
1.3	Тема 3. Индустриальный Интернет вещей. Проблемы технологий индустриального Интернета вещей.		4	4	0	0	6
2	**Раздел 2. Анализ безопасности технологий Интернета вещей**	**46**	**14**	**12**	**0**	**0**	**20**
2.1	Тема 1. Проблемы безопасности Интернета вещей		4	0	0	0	4

2.2	Тема 2. Классификация угроз IoT		4	0	0	0	4
2.3	Тема 3. Проблемы безопасности технологий индустриального Интернета вещей		4	6	0	0	8
2.4	Тема 4. Классификация угроз индустриального Интернета вещей		2	6	0	0	4
3	**Раздел 3. Примеры угроз для устройств Интернета вещей в различных сферах**	**32**	**6**	**8**	**0**	**0**	**18**
3.1	Тема 1. Интеллектуальная транспортная система		2	0	0	0	4
3.2	Тема 2. Элементы методологии цифровой экспертизы		2	0	0	0	4
3.3	Тема 3. Примеры сценариев атак на устройства Интернета вещей		2	8	0	0	10
4	**Раздел 4. Разработка мер безопасности для устройств интернета вещей**	**28**	**4**	**8**	**0**	**0**	**16**
4.1	Тема 1. Анализ проблем обеспечения безопасности IoT-устройств		2	4	0	0	6
4.2	Тема 2. Меры по обеспечению безопасности устройств Интернета вещей		2	4	0	0	10
	Итого	**144**	**36**	**36**	**0**	**0**	**72**

3.3 Содержание дисциплины

Раздел 1. Введение в информационную безопасность Интернета вещей.

Информационная безопасность киберфизических систем, кибербезопасность в интернете вещей: основные стандарты, понятия, определения. Протоколы связи и аутентификации для киберфизических систем и «Интернет вещей»: обзор, особенности, проблемы безопасности. Индустриальный Интернет вещей. Введение в проблему информационной безопасности Интернета вещей, области применения, специфика требований. Жизненный цикл проекта Интернета вещей. Классификация систем Интернета вещей. Нормативно-правовое регулирование. Требования к обеспечению информационной безопасности.

Раздел 2. Анализ безопасности технологий Интернета вещей.

Проблемы безопасности Интернета вещей. Классификация угроз IoT. Проблемы безопасности технологий индустриального Интернета вещей. Классификация угроз индустриального Интернета вещей. Обзор существующих методов защиты систем промышленных предприятия, требования и особенности интеграции элементов и систем защиты информации.

Раздел 3. Примеры угроз для устройств Интернета вещей в различных сферах.

Интеллектуальная транспортная система. Элементы методологии цифровой экспертизы. Примеры сценариев атак на устройства Интернета вещей. Понятие модели нарушителя, отраслевые модели нарушителя. Влияние модели нарушителя на процесс разработки прикладного программного обеспечения

Раздел 4. Разработка мер безопасности для устройств интернета вещей.

Анализ проблем обеспечения безопасности IoT-устройств. Меры по обеспечению безопасности устройств Интернета вещей. Управление рисками в системах интернета вещей. Классификация рисков, построение модели угроз. Критерии достаточности в управлении рисками.

3.4 Тематика семинарских/практических и лабораторных занятий

3.4.1 Семинарские/практические занятия

Семинар 1. Основные типы систем Интернета вещей и требования, предъявляемые к ним

Семинар 2. Правовое обеспечение информационной безопасности на предприятии.

Семинар 3. Анализ и выбор протоколов безопасности устройств в проектируемой сети

Семинар 4. Требования по обеспечению безопасности при разработке элементов инфраструктуры Интернета вещей.

Семинар 5. Анализ типовых решений для Интернета вещей

Семинар 6. Анализ решений по защите систем Интернета вещей от различных производителей.

Семинар 7. Анализ требований по информационной безопасности систем Интернета вещей в зависимости от профиля их использования.

Семинар 8. Определение Риска сети Интернета вещей.

Семинар 9. Обзор программных средств и возможностей для создания имитационных моделей протоколов обеспечения безопасности Интернета вещей

3.4.2 Лабораторные занятия

Не предусмотрены

3.5 Тематика курсовых проектов (курсовых работ)

Не предусмотрены

4 Учебно-методическое и информационное обеспечение

4.1 Нормативные документы и ГОСТы

Не предусмотрены

4.2 Основная литература

1. Фот, Ю. Д. Стандарты информационной безопасности : учебное пособие / Ю. Д. Фот. — Оренбург : ОГУ, 2018. — 226 с. — ISBN 978-5-7410-2297-9. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/159804.

2. Никифоров, С. Н. Методы защиты информации. Защита от внешних вторжений / С. Н. Никифоров. — 5-е изд., стер. — Санкт-Петербург : Лань, 2023. — 96 с. — ISBN 978-5-507-45868-4. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/288974.

3. Никифоров, С. Н. Методы защиты информации. Защищенные сети : учебное пособие для вузов / С. Н. Никифоров. — 2-е изд., стер. — Санкт-Петербург : Лань, 2021. — 96 с. — ISBN 978-5-8114-8123-1. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/171868

4. Андреев, Ю. С. Промышленный интернет вещей : учебное пособие / Ю. С. Андреев, С. Д. Третьяков. — Санкт-Петербург : НИУ ИТМО, 2019. — 54 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/344408.

4.3 Дополнительная литература

1. Зенков, А. В. Основы информационной безопасности : учебное пособие / А. В. Зенков. — Вологда : Инфра-Инженерия, 2022. — 104 с. — ISBN 978-5-9729-0864-6. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/281195.

2. Колмогорова, С. С. Обработка данных алгоритмами искусственного интеллекта в системе интернета вещей / С. С. Колмогорова. — Санкт-Петербург : Лань, 2023. — 104 с. — ISBN 978-5-507-46186-8. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/327356.

3. Муромцев, Д. И. Интернет Вещей: Введение в программирование на arduino : учебно-методическое пособие / Д. И. Муромцев, В. Н. Шматков. — Санкт-Петербург : НИУ ИТМО, 2018. — 36 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/136448.

4.4 Электронные образовательные ресурсы

Не предусмотрены

4.5 Лицензионное и свободно распространяемое программное обеспечение

1. Microsoft-Office
2. Microsoft-Windows

4.6 Современные профессиональные базы данных и информационные справочные системы

1. Единое окно доступа к образовательным ресурсам Федеральный портал http://window.edu.ru

2. Компьютерные информационно-правовые системы «Консультант» http://www.consultant.ru, «Гарант» http://www.garant.ru

3. Официальный интернет-портал правовой информации http://pravo.gov.ru.

4. Научная электронная библиотека http://www.elibrary.ru

5. Российская государственная библиотека http://www.rsl.ru

6. ЭБС «Университетская библиотека онлайн» https://biblioclub.ru/index.php

5 Материально-техническое обеспечение

1. Компьютерный класс с предустановленным программным обеспечением, указанным в п. 4.5, мультимедийное оборудование (проектор, персональный компьютер преподавателя).

2. Аудитория для лекционных, практических занятий. Оборудование и аппаратура: аудиторная доска, возможность использования мультимедийного комплекса.

6 Методические рекомендации

6.1 Методические рекомендации для преподавателя по организации обучения

На первом занятии по дисциплине необходимо ознакомить студентов с порядком ее изучения (темами курса, формами занятий, текущего и промежуточного контроля), раскрыть место и роль дисциплины в системе наук, ее практическое значение, довести до студентов требования к форме отчетности и применения видов контроля. Выдаются задания для подготовки к практическим и семинарским занятиям.

При подготовке к семинарам по перечню объявленных тем преподавателю необходимо уточнить план их проведения, продумать формулировки и содержание учебных вопросов, выносимых на обсуждение, ознакомиться с перечнем тематических вопросов.

В ходе семинара во вступительном слове раскрыть практическую значимость темы, определить порядок занятия, время на обсуждение каждого учебного вопроса. Применяя фронтальный опрос дать возможность выступить всем студентам, присутствующим на занятии.

В заключительной части работы семинара подвести его итоги: дать оценку выступлений каждого студента и учебной группы в целом. Раскрыть положительные стороны и недостатки проведенной работы. Ответить на вопросы студентов. Выдать задания для самостоятельной работы по подготовке к следующему занятию.

Методика преподавания дисциплины «Информационная безопасность» и реализация компетентностного подхода в изложении и восприятии материала предусматривает использование следующих активных и интерактивных форм проведения групповых, индивидуальных, аудиторных занятий в сочетании с внеаудиторной работой с целью формирования и развития профессиональных навыков обучающихся:

– защита и обсуждение эссе в рамках семинаров;

– технологии анализа ситуаций для активного обучения, которые позволяют студентам соединить теорию и практику, представить примеры принимаемых решений и их последствий, демонстрировать различные позиции, формировать навыки оценки альтернативных вариантов в вероятностных условиях.

Обучение по дисциплине ведется с применением традиционных потоково-групповых информационно-телекоммуникационных технологий. При осуществлении образовательного процесса по дисциплине используются следующие информационно-телекоммуникационные технологии: презентации с применением проектора и программы PowerPoint.

6.2 Методические указания для обучающихся по освоению дисциплины

Самостоятельная работа студентов направлена на решение следующих задач:

Самостоятельная работа является одним из видов учебных занятий. Цель самостоятельной работы – практическое самостоятельное получение студентами навыков работы в программе математического моделирования, рассматриваемых в процессе изучения дисциплины.

Аудиторная самостоятельная работа по дисциплине выполняется на учебных занятиях под непосредственным руководством преподавателя и по его заданию.

Внеаудиторная самостоятельная работа выполняется студентом по заданию преподавателя, но без его непосредственного участия.

Задачи самостоятельной работы студента:

- развитие навыков самостоятельной учебной работы;

- освоение содержания дисциплины;
- углубление содержания и осознание основных понятий дисциплины;
- использование материала, собранного и полученного в ходе самостоятельных занятий для эффективной подготовки к экзамену.

Виды внеаудиторной самостоятельной работы:
- самостоятельное изучение отдельных тем дисциплины;
- подготовка к семинарам;
- написание эссе по темам семинаров и подготовка к их защите;

Для выполнения любого вида самостоятельной работы необходимо пройти следующие этапы:
- определение цели самостоятельной работы;
- конкретизация познавательной задачи;
- самооценка готовности к самостоятельной работе;
- выбор адекватного способа действия, ведущего к решению задачи;
- планирование работы (самостоятельной или с помощью преподавателя) над заданием;
- осуществление в процессе выполнения самостоятельной работы самоконтроля (промежуточного и конечного) результатов работы и корректировка выполнения работы;
- рефлексия;
- презентация работы.

7 Фонд оценочных средств

В процессе обучения используются следующие оценочные формы самостоятельной работы студентов, оценочные средства текущего контроля успеваемости и промежуточных аттестаций:
- защита эссе по теме семинара;
- контрольные работы;
- тестирование;
- экзамен.

Оценочные средства текущего контроля успеваемости включают контрольные задания индивидуально для каждого обучающегося.

В результате освоения дисциплины (модуля) формируются следующие компетенции:

Код компетенции	**Наименование компетенции выпускника**
ПК-5	Способен проектировать, устанавливать, настраивать и поддерживать в работоспособном состоянии компоненты системы обеспечения информационной безопасности в радиотехнических системах

7.1 Методы контроля и оценивания результатов обучения

Перечень оценочных средств по дисциплине «Информационная безопасность».

№ п/п	Вид контроля результатов обучения	Наименование контроля результатов обучения	Краткая характеристика контроля результатов обучения
1	Текущий	Эссе	Эссе готовится каждым студентом индивидуально за неделю до проводимого семинара по соответствующей теме. Авторы лучших эссе приглашаются для выступления на семинарском занятии с докладом.
2	Текущий	Тестирование	Тестирование проводится на последнем занятии изучаемой темы. Тестирование осуществляется, либо при помощи компьютерной системы тестирования, либо с использованием выданных тест-заданий на бумажном носителе. В рамках тестирования проверяется владение терминологией и знание теоретической базы.
3	Текущий	Контрольная работа	Решение контрольной работы осуществляется на последнем занятии изучаемого раздела. Контрольная работа выполняется индивидуально каждым студентом. При проверке преподаватель оценивает правильность произведенных расчетов, алгоритмов, использования терминологии и выводы.
4	Промежуточный	Экзамен	Промежуточная аттестация обучающихся в форме экзамена 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 «отлично», «хорошо», «удовлетворительно» или «неудовлетворительно». Экзамен проводится в устной форме. В аудитории находится преподаватель и не более 5 человек из числа студентов. Во время проведения экзамена его участникам запрещается иметь при себе и использовать

			средства связи (сотовые телефоны, микрофоны и пр.). Студенту выдается билет с тремя вопросами. Количество дополнительных вопросов – не более двух. Количество дополнительных вопросов зависит от полноты ответа студента. Длительность экзамена 2 часа (120 минут). К промежуточной аттестации допускаются только студенты, выполнившие все виды учебной работы, предусмотренные рабочей программой по дисциплине «Информационная безопасность».

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).

Показатель	**Критерии оценивания**			
	2	**3**	**4**	**5**
Знать: - методику анализа уязвимостей в подсистеме обеспечения безопасности стандартов в радиотехнических системах и сетях интернета вещей; - общие принципы функционирования и взаимодействия устройств в рамках основных информационных систем; - протоколы и алгоритмы взаимодействия в сетях интернета вещей; - источники и виды угроз безопасности в информационных системах и сетях интернета вещей; - основные подходы и методы оценки рисков информационной безопасности в сетях интернета вещей.	Обучающийся демонстрирует полное отсутствие или недостаточное соответствие следующих знаний: - методику анализа уязвимостей в подсистеме обеспечения безопасности стандартов в радиотехнических системах и сетях интернета вещей; - общие принципы функционирования и взаимодействия устройств в рамках основных информационных систем; - протоколы и алгоритмы взаимодействия в сетях интернета вещей; - источники и виды угроз безопасности в информационных системах и сетях интернета вещей; - основные подходы и методы оценки рисков	Обучающийся демонстрирует неполное соответствие следующих знаний: - методику анализа уязвимостей в подсистеме обеспечения безопасности стандартов в радиотехнических системах и сетях интернета вещей; - общие принципы функционирования и взаимодействия устройств в рамках основных информационных систем; - протоколы и алгоритмы взаимодействия в сетях интернета вещей; - источники и виды угроз безопасности в информационных системах и сетях интернета вещей; - основные подходы и методы оценки рисков информационной	Обучающийся демонстрирует частичное соответствие следующих знаний: - методику анализа уязвимостей в подсистеме обеспечения безопасности стандартов в радиотехнических системах и сетях интернета вещей; - общие принципы функционирования и взаимодействия устройств в рамках основных информационных систем; - протоколы и алгоритмы взаимодействия в сетях интернета вещей; - источники и виды угроз безопасности в информационных системах и сетях интернета вещей; - основные подходы и методы оценки рисков информационной	Обучающийся демонстрирует полное соответствие следующих знаний: - методику анализа уязвимостей в подсистеме обеспечения безопасности стандартов в радиотехнических системах и сетях интернета вещей; - общие принципы функционирования и взаимодействия устройств в рамках основных информационных систем; - протоколы и алгоритмы взаимодействия в сетях интернета вещей; - источники и виды угроз безопасности в информационных системах и сетях интернета вещей; - основные подходы и методы оценки рисков информационной

	информационной безопасности в сетях интернета вещей.	безопасности в сетях интернета вещей. Допускаются значительные ошибки, проявляется недостаточность знаний, по ряду показателей, обучающийся испытывает значительные затруднения при оперировании знаниями при их переносе на новые ситуации.	безопасности в сетях интернета вещей. Допускаются незначительные ошибки, неточности, затруднения при аналитических операциях.	безопасности в сетях интернета вещей. Свободно оперирует приобретенными знаниями.
Уметь: вырабатывать стратегию действий по защите информации в радиотехнических системах; осуществлять выбор наиболее подходящей для заданных условий конфигурации сети интернета вещей; - применять методику анализа уязвимостей в подсистеме обеспечения безопасности сети интернета вещей.	Обучающийся не умеет или в недостаточной степени умеет: вырабатывать стратегию действий по защите информации в радиотехнических системах; осуществлять выбор наиболее подходящей для заданных условий конфигурации сети интернета вещей; - применять методику анализа уязвимостей в подсистеме обеспечения безопасности сети интернета вещей.	Обучающийся демонстрирует неполное соответствие следующих умений: вырабатывать стратегию действий по защите информации в радиотехнических системах; осуществлять выбор наиболее подходящей для заданных условий конфигурации сети интернета вещей; - применять методику анализа уязвимостей в подсистеме обеспечения безопасности сети интернета вещей. Допускаются значительные ошибки, проявляется недостаточность умений, по ряду показателей, обучающийся испытывает значительные затруднения при оперировании умениями при их переносе на новые ситуации.	Обучающийся демонстрирует частичное соответствие следующих умений: вырабатывать стратегию действий по защите информации в радиотехнических системах; осуществлять выбор наиболее подходящей для заданных условий конфигурации сети интернета вещей; - применять методику анализа уязвимостей в подсистеме обеспечения безопасности сети интернета вещей. Умения освоены, но допускаются незначительные ошибки, неточности, затруднения при аналитических операциях, переносе умений на новые, нестандартные ситуации.	Обучающийся демонстрирует полное соответствие следующих умений: вырабатывать стратегию действий по защите информации в радиотехнических системах; осуществлять выбор наиболее подходящей для заданных условий конфигурации сети интернета вещей; - применять методику анализа уязвимостей в подсистеме обеспечения безопасности сети интернета вещей. Свободно оперирует приобретенными умениями, применяет их в ситуациях повышенной сложности.
Владеть: навыками работы по разработке планов и проведению мероприятий по организации защиты информации радиотехнических	Обучающийся не владеет или в недостаточной степени владеет - навыками работы по разработке планов и проведению мероприятий по	Обучающийся в недостаточной степени владеет: - навыками работы по разработке планов и проведению мероприятий по организации защиты	Обучающийся частично владеет - навыками работы по разработке планов и проведению мероприятий по организации защиты информации	Обучающийся в полном объеме владеет: навыками работы по разработке планов и проведению мероприятий по

система и систем «Интернета вещей»; методами настройки встроенных механизмов защиты информационной системы; навыками применения стандартных средств защиты информации.	организации защиты информации радиотехнических система и систем «Интернета вещей»; методами настройки встроенных механизмов защиты информационной системы; навыками применения стандартных средств защиты информации.	информации радиотехнических система и систем «Интернета вещей»; методами настройки встроенных механизмов защиты информационной системы; навыками применения стандартных средств защиты информации. Обучающийся испытывает значительные затруднения при применении навыков в новых ситуациях.	радиотехнических система и систем «Интернета вещей»; методами настройки встроенных механизмов защиты информационной системы; навыками применения стандартных средств защиты информации. Навыки освоены, но допускаются незначительные ошибки, неточности, затруднения при аналитических операциях, переносе умений на новые, нестандартные ситуации.	организации защиты информации радиотехнических система и систем «Интернета вещей»; методами настройки встроенных механизмов защиты информационной системы; навыками применения стандартных средств защиты информации. Свободно применяет полученные навыки в ситуациях повышенной сложности.

Шкала оценивания промежуточной аттестации: экзамена.

Шкала оценивания	Описание
Отлично	Выполнены все виды учебной работы, предусмотренные учебным планом. Студент демонстрирует соответствие знаний, умений, навыков приведенным в таблицах показателям, оперирует приобретенными знаниями, умениями, навыками, применяет их в ситуациях повышенной сложности, не испытывает затруднений при аналитических операциях, переносе знаний и умений на новые, нестандартные ситуации.
Хорошо	Выполнены все виды учебной работы, предусмотренные учебным планом. Студент демонстрирует частичное соответствие знаний, умений, навыков приведенным в таблицах показателям, 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.
Удовлетворительно	Выполнены все виды учебной работы, предусмотренные учебным планом. Студент демонстрирует неполное соответствие знаний, умений, навыков приведенным в таблицах показателям, 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.
Неудовлетворительно	Не выполнен один или более видов учебной работы, предусмотренных учебным планом. Студент демонстрирует полное отсутствие или недостаточное соответствие знаний, умений, навыков приведенным в таблицах показателям, допускаются значительные ошибки, проявляется отсутствие знаний, умений,

	навыков по ряду показателей, студент не может оперировать знаниями и умениями при их переносе на новые ситуации.

Шкала оценивания текущего контроля.

Наименование контроля результатов обучения	Шкала оценивания	Описание
Выполнение и защита эссе по теме семинара	Зачтено: набрано 3 и более баллов Незачтено: набрано 2 и менее баллов Критерии оценивания Общий балл при оценке складывается из следующих показателей: - приведены формулировка проблемы, обзор действующих ограничений на выбор решения – 1 балл; приведено обоснование выбора методов решения, выбранное решение структурно описано. – 1 балл - выводы логичны и обоснованы – 1 балл - оформление работы соответствует требованиям – 1 балл - выполнен доклад на семинарском занятии.	По каждой из тем 1-6 необходимо подготовить задание, ответ оформить в письменном виде в формате эссе, сдать не позднее указанного срока (не более 2х недель): Для получения оценки «зачтено» эссе на каждую тему, соответствующую разделам дисциплины должно быть выполнено и отправлено в сроки изучения темы. Каждый студент формулирует задачу в рамках изучаемой темы. Формулировка согласовывается с преподавателем, при необходимости, преподаватель корректирует/уточняет постановку задачи. Требования к представлению результатов. Результаты выполненных заданий оформляются в формате эссе. Эссе необходимо представить: формулировку проблемы; обзор действующих ограничений на выбор решения; обоснование выбора методов решения; структурное описания выбранного решения. Длительность доклада не превышает 5 минут.
Контрольная работа по теме раздела	Отлично - Работа высокого качества, уровень выполнения отвечает всем требованиям, теоретическое содержание курса освоено полностью, без пробелов, необходимые практические навыки работы с освоенным материалом сформированы, все предусмотренные программой обучения учебные задания выполнены, либо некоторые из	Защита темы включает решение задач в аудитории в течение одной пары и проходит после изучения соответствующего раздела. Билеты состоят из вопросов, позволяющих оценить сформированность компетенций. На ответы отводится 1,5 часа.

	выполненных заданий содержат незначительные ошибки Хорошо - Уровень выполнения работы отвечает большинству основных требований, теоретическое содержание курса освоено частично, но пробелы не носят существенного характера, необходимые практические навыки работы с освоенным материалом в основном сформированы, некоторые виды заданий выполнены с ошибками. Удовлетворительно - Теоретическое содержание курса освоено частично, необходимые практические навыки работы не сформированы, большинство предусмотренных программой заданий не выполнено; при дополнительной самостоятельной работе над материалом курса возможно повышение качества выполнения учебных заданий. Неудовлетворительно - Теоретическое содержание курса не освоено, необходимые практические навыки работы не сформированы, предусмотренные программой задания не выполнены	
Тестирование по пройденной теме	Тест содержит 20 заданий, правильный ответ на 1 задание соответствует 1 баллу. Время тестирования - 30 минут. Студенту предоставляется две попытки для прохождения теста. Максимальная оценка за тест - 20 баллов. Тест считается успешно пройденным, если студент дал не менее 60% правильных ответов (набрал не менее 12 баллов).	Тестирование осуществляется, либо при помощи компьютерной системы тестирования, либо с использованием выданных тест-заданий на бумажном носителе. Время тестирования 30 мин. Затем осуществляется проверка теста экзаменатором и выставляется оценка согласно методики выставления оценки при проведении промежуточной аттестации.

7.3 Оценочные средства

7.3.1 Текущий контроль

Вопросы для подготовки эссе к Семинару 1 «Основные типы систем Интернета вещей и требования, предъявляемые к ним».

1. Перечислите основные типы систем Интернета вещей?
2. Выделите ключевые требования, предъявляемые к основным типам систем Интернета вещей (три типа систем на выбор).
3. К таким типам систем Интернета вещей относятся системы технологического управления в концепции «Индустрия 4.0», Умный дом, системы управления агрегатами и режимами работы автомобиля и др.

Вопросы для подготовки эссе к Семинару 2 «Правовое обеспечение информационной безопасности на предприятии».

1. Аспекты информационной системы
2. Правовые основы защиты информации
3. Уровни правового обеспечения информационной безопасности информации
4. Правовые основы информационной безопасности

Вопросы для подготовки эссе к Семинару 3 «Анализ и выбор протоколов безопасности устройств в проектируемой сети».

1. Протоколы безопасности устройств сети Интернета вещей.
2. Методы оценки риска для устройств, использующих разные протоколы безопасности и работающих на одной и той же беспроводной технологии.
3. Анализ эффективности сети интернета вещей при использовании различных протоколов безопасности.

Вопросы для подготовки эссе к Семинару 4 «Требования по обеспечению безопасности при разработке элементов инфраструктуры Интернета вещей».

1. Требования, рекомендации по разработке элементов инфраструктуры Интернета вещей.
2. Базовые требования по обеспечению безопасности.
3. Предложить варианты решения.

Вопросы для подготовки эссе к Семинару 5 «Анализ типовых решений для Интернета вещей».

1. Типовые решений для Интернета вещей, основные характеристики.
2. Основные риски типовых решений для Интернета вещей.

Вопросы для подготовки эссе к Семинару 6 «Анализ решений по защите систем Интернета вещей от различных производителей».

1. Решения по защите систем Интернета вещей от различных производителей: Cisco Systems, Infoteks, Positive Technology и др. Основные характеристики.

Вопросы для подготовки эссе к Семинару 7 «Анализ требований по информационной безопасности систем Интернета вещей в зависимости от профиля их использования».

1. Проблемы безопасности технологий индустриального Интернета вещей.
2. Требования по информационной безопасности систем Интернета вещей.

Вопросы для подготовки эссе к Семинару 8 «Определение Риска сети Интернета вещей».

1. Исследование угроз безопасности на примере умных часов
2. Основные виды рисков сети Интернета вещей.

Вопросы для подготовки эссе к Семинару 9 «Обзор программных средств и возможностей для создания имитационных моделей протоколов обеспечения безопасности Интернета вещей».

1. Анализ методов безопасной разработки программного обеспечения для систем Интернета вещей
2. Определить основные типы бизнес-процессов безопасной разработки программного обеспечения.
3. Обзор существующих программных средств для создания имитационных моделей протоколов обеспечения безопасности Интернета вещей.

Примерный перечень заданий для подготовки к тестированию.

1. Защита информации это: (отметьте один правильный вариант ответа)

а. совокупность правил, регламентирующих порядок и условия доступа субъекта к информации и ее носителям;

б. преобразование информации, в результате которого содержание информации становится непонятным для субъекта, не имеющего доступа;

в. деятельность по предотвращению утечки информации, несанкционированных и непреднамеренных воздействий на нее.

2. К недостаткам WLAN-сетей относят: (отметьте все правильные варианты ответа)

а. подверженность влиянию помех;

б. как правило, меньшая скорость по сравнению с обычными проводными LAN-сетями;

в. простая схема обеспечения безопасности передаваемой информации.

3. Для доступа к беспроводной сети адаптер может устанавливать связь через точку доступа. Такой режим называется: (отметьте один правильный вариант ответа)

а. инфраструктурным;

б. ad hoc;

в. подчиненный объект.

4. Что является наилучшим описанием количественного анализа рисков: (отметьте один правильный вариант ответа)

а. метод, используемый для точной оценки потенциальных потерь, вероятности потерь и рисков;

б. метод, сопоставляющий денежное значение с каждым компонентом оценки рисков;

в. анализ, основанный на сценариях, предназначенный для выявления различных угроз безопасности.

5. Почему при проведении анализа информационных рисков следует привлекать к этому специалистов из различных подразделений компании: (отметьте один правильный вариант ответа)

а. поскольку специалисты лучше понимают риски в своих подразделениях и смогут предоставить максимально полную и достоверную информацию для анализа;

б. поскольку люди в различных подразделениях сами являются одной из причин рисков, они должны быть ответственны за их оценку;

в. чтобы убедиться, что проводится справедливая оценка.

6. Что из перечисленного нельзя отнести к характеристикам интернета вещей: (отметьте один правильный вариант ответа)

а. невысокие скорости передачи данных;

б. фокусировка на обслуживании запросов людей;

в. необходимость создания новой инфраструктуры.

7. В какой из перечисленных рекомендаций ITU описана эталонная модель для интернета вещей: (отметьте один правильный вариант ответа)

а. Y.2060;

б. 802.3cd;

в. RFC 4960.

8. Что из перечисленного не является базовым уровнем эталонной модели интернета вещей, описанной в рекомендации ITU: (отметьте один правильный вариант ответа)

а. уровень приложений интернета вещей;

б. уровень ядра сети;

в. уровень поддержки приложений и услуг;

г. сетевой уровень.

9. Верно ли, что для сетей интернета вещей необходимо использовать только статическую маршрутизацию для организации связи между устройствами: (отметьте один правильный вариант ответа)

а. да;

б. нет;

в. да, но только для IPv6

10.TDM определяет: (отметьте один правильный вариант ответа)

а. уплотнение с частотным разделением;

б. уплотнение с временным разделением;

в. квадратурную амплитудную модуляцию.

11.SSID определяет: (отметьте один правильный вариант ответа)

а. беспроводную распределенную сеть;

б. идентификатор зоны обслуживания;

в. зону обслуживания

Примерный перечень вопросов для подготовки к контрольным работам.

1. Рекомендации по построению политики безопасности. Основные шаги по реализации политики безопасности. Поддержание и модификация политики безопасности.
2. Стандарты беспроводной передачи данных.
3. Критерии оценки безопасности сетевых ОС.
4. Параметры связи: скорость передачи данных, диапазон частот, метод модуляции сигнала и т.д.

5. Основные критерии анализа сетевой безопасности. Общая процедура анализа. Методика подготовки экспертного заключения.

6. Современные стандарты, используемые в сетях интернета вещей.

7. Регламентирующие документы в области безопасности вычислительных сетей. Стандарты безопасности вычислительных сетей и их компонентов. Правовые основы защиты информации в сетях.

8. Типовые угрозы безопасности. Основы классификации сетевых угроз и атак. Примеры типовых атак и рекомендации по построению систем защиты.

9. Анализ возможных сценариев атак.

10 Защита топологии сети. Маршрутизаторы, межсетевые экраны (МЭ). Основные механизмы применения МЭ. Абонентское шифрование.

11. Анализ характерных уязвимостей сетей интернета вещей.

12. Виртуальные частные сети.

13. Прогнозирование эффективности системы обеспечения безопасности сети интернета вещей.

14. Защита сетевого трафика и компонентов сети.

15. Модели принятия решений в условиях неопределенности.

16. Защита компонентов сети от НСД. Безопасность ресурсов сети: средства идентификации и аутентификации, методы разделения ресурсов и технологии разграничения доступа.

17. Архитектура системы безопасности в сетях интернета вещей.

18. Электронная цифровая подпись и пакетное шифрование. Криптографические сетевые протоколы. Управление ключами.

19. Модель безопасности в сетях интернета вещей. Типовые атаки в сетях интернета вещей.

20. Понятие политики безопасности. Типовые элементы политики безопасности.

21. Вероятностный подход к анализу рисков сетей интернета вещей.

22. Методика выбора мер и средств защиты телекоммуникационной системы и сети интернета вещей.

23. Экспертный подход к анализу рисков сетей интернета вещей.

7.3.2 Промежуточная аттестация

Вопросы к экзамену

1. Причины уязвимости систем класса интернета вещей.	ПК-5
2. Интернет вещей, - основные виды уязвимостей компонентов.	ПК-5
3. Требования к безопасности информационным системам, основные нормативно-правовые акты.	ПК-5
4. Требования к безопасности информационным системам, нормативно-правовые акты в области криптографической защиты.	ПК-5
5. Являются ли системы интернета вещей ключевыми? Приведение обоснование.	ПК-5
6. Жизненный цикл проекта Интернета вещей, характеристика этапов с точки зрения информационной безопасно.	ПК-5
7. Влияние принципов SDLC на проект Интернета вещей.	ПК-5
8. Понятие информационной безопасности в системах интернета вещей.	ПК-5

9. Определение приоритетной задачи безопасности для систем интернета вещей.	ПК-5
10. Типовые архитектуры безопасности для интернета вещей.	ПК-5
11. Основные методы управления рисками.	ПК-5
12. Особенности модели угроз для интернета вещей.	ПК-5
13. Назначение модели угроз.	ПК-5
14. Основные принципы управления рисками.	ПК-5
15. Роль модели угроз при разработке программного обеспечения.	ПК-5
16. Понятие безопасной разработки программного обеспечения.	ПК-5
17. Роль модели нарушителя при разработке программного обеспечения	ПК-5
18. Состав раздела пользовательской документации по требованиям безопасности.	ПК-5
19. Включение элементов интернета вещей в комплексные информационные системы, формирование требований по безопасности.	ПК-5
20. Особенности интеграции сторонних решений в критическое программное обеспечение.	ПК-5
21. Роль модели нарушителя при разработке безопасного программного обеспечения.	ПК-5
22. Включение элементов интернета вещей в комплексные информационные системы.	ПК-5
23. Влияние модели нарушителя компонента на политику безопасности комплексной системы.	ПК-5
24. Понятие технических условий безопасного использование компонентов.	ПК-5
25. Источники информации для построения модели нарушителя.	ПК-5
26. Роль эксперта в процессе разработки модели нарушителя.	ПК-5
27. Управление рисками в системах интернета вещей.	ПК-5
28. Классификация рисков для систем интернета вещей.	ПК-5
29. Методики построения модели угроз.	ПК-5
30. Критерии достаточности в управлении рисками.	ПК-5
31. Управление рисками в системах интернета вещей как услуга: критерии качества.	ПК-5
32. Влияние модели нарушителя на процесс разработки прикладного программного обеспечения.	ПК-5
33. Критерии достаточности при анализе безопасности прикладного программного обеспечения.	ПК-5
34. Понятие безопасной разработки программного обеспечения.	ПК-5
35. Состав типовой СЗИ для интернета вещей.	ПК-5
36. Методы управления процессами обмена информацией в системах интернета вещей.	ПК-5