МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное учреждение высшего образования
«ТОМСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ СИСТЕМ
УПРАВЛЕНИЯ И РАДИОЭЛЕКТРОНИКИ»
(ТУСУР)

УТВЕРЖДАЮ
Проректор по УР
Сенченко П.В.
«22» _____ 02 _____ 2023 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

БЕЗОПАСНОСТЬ ИНТЕРНЕТА ВЕЩЕЙ И СЕНСОРНЫХ СИСТЕМ

Уровень образования: **высшее образование - специалитет**

Направление подготовки / специальность: **10.05.03 Информационная безопасность автоматизированных систем**

Направленность (профиль) / специализация: **Безопасность автоматизированных систем в кредитно-финансовой сфере**

Форма обучения: **очная**

Факультет: **Факультет безопасности (ФБ)**

Кафедра: **Кафедра комплексной информационной безопасности электронно-вычислительных систем (КИБЭВС)**

Курс: **5**

Семестр: **10**

Учебный план набора 2023 года

Объем дисциплины и виды учебной деятельности

Виды учебной деятельности	10 семестр	Всего	Единицы
Лекционные занятия	28	28	часов
Лабораторные занятия	40	40	часов
Самостоятельная работа	76	76	часов
Подготовка и сдача экзамена	36	36	часов
Общая трудоемкость	180	180	часов
(включая промежуточную аттестацию)	5	5	з.е.

Формы промежуточной аттестация	Семестр
Экзамен	10

Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Сенченко П.В.
Должность: Проректор по УР
Дата подписания: 22.02.2023
Уникальный программный ключ:
a1119608-cdff-4455-b54e-5235117c185c

Томск

1. Общие положения

1.1. Цели дисциплины

1. изучение основных направлений деятельности по обеспечению безопасности систем Интернета вещей.
2. изучение основных понятий в области безопасности Интернета вещей.
3. изучение основных угроз, уязвимостей, рисков в области безопасности Интернета вещей.
4. изучение основных требований нормативно-правовых документов по защите объектов критической информационной инфраструктуры.

1.2. Задачи дисциплины

1. научить студентов разрабатывать архитектуру систем «Интернета вещей», принимать решения по выбору используемых протоколов, технологий и архитектурных компонентов системы.
2. научить студентов анализировать риски в области безопасности систем «Интернета вещей».
3. научить студентов применять на практике полученные знания для противодействия сетевым атакам на системы «Интернет вещей».

2. Место дисциплины в структуре ОПОП

Блок дисциплин: Б1. Дисциплины (модули).

Часть блока дисциплин: Обязательная часть.

Модуль дисциплин: Модуль специальности (special hard skills - SHS).

Индекс дисциплины: Б1.О.03.36.

Реализуется с применением электронного обучения, дистанционных образовательных технологий.

3. Перечень планируемых результатов обучения по дисциплине, соотнесенных с индикаторами достижения компетенций

Процесс изучения дисциплины направлен на формирование следующих компетенций в соответствии с ФГОС ВО и основной образовательной программой (таблица 3.1):

Таблица 3.1 – Компетенции и индикаторы их достижения

Компетенция	Индикаторы достижения компетенции	Планируемые результаты обучения по дисциплине
Универсальные компетенции		
-	-	-
Общепрофессиональные компетенции		

ОПК-9. Способен решать задачи профессиональной деятельности с учетом текущего состояния и тенденций развития информационных технологий, средств технической защиты информации, сетей и систем передачи информации	ОПК-9.1. Знает основные программные и программно-аппаратные средства защиты информации телекоммуникационных систем от несанкционированного доступа и принципы работы этих средств	типичные средства и методы защиты информации в локальных и глобальных вычислительных сетях; требования НПА и стандартов по разработке моделей угроз информационной безопасности; наиболее распространенные уязвимости IoT-устройств и протоколов передачи данных; средства обеспечения информационной безопасности IoT-систем; принципы построения защищенных телекоммуникационных систем; механизмы реализации атак в сетях Интернета вещей;
	ОПК-9.2. Умеет настраивать типичные программные и программно-аппаратные средства защиты информации телекоммуникационных систем от несанкционированного доступа, определять наличие типичных технических каналов утечки информации на объектах информатизации	проводить первичную настройку и проверку функционирования СССЭ, средств и систем защиты СССЭ от НСД; обнаруживать типичные уязвимости IoT-систем; внедрять типичные решения по информационной безопасности IoT-систем; осуществлять меры противодействия нарушениям сетевой безопасности с использованием различных программных и аппаратных средств защиты в соответствии с требованиями нормативно правовых актов и нормативных методических документов; проводить анализ защищенности IoT-систем
	ОПК-9.3. Владеет методиками расчета и инструментального контроля показателей технической защиты информации на объектах информатизации, навыками проведения измерений при аттестации объектов информатизации по требованиям защиты информации	терминологией в области безопасности систем интернета вещей; методами защиты информации в IoT-системах; инструментами анализа защищенности IoT-систем; методикой анализа результатов работы средств обнаружения вторжений; навыками проверки работоспособности системы защиты информации автоматизированной системы; навыками первичной настройки и проверки функционирования программных, программно-аппаратных (в том числе криптографических) и технических средств и систем защиты СССЭ от НСД;

ОПК-12. Способен применять знания в области безопасности вычислительных сетей, операционных систем и баз данных при разработке автоматизированных систем	ОПК-12.1. Знает классификацию компьютерных систем, виды информационного взаимодействия и обслуживания, основы построения автоматизированных систем, назначение, функции и обобщенную структуру операционных систем и типовые операционные системы, в том числе отечественного производства	стандарты реализации интерфейсов подключаемых устройств; стандарты информационного взаимодействия систем; существующие технологии в области Интернета вещей;
	ОПК-12.2. Умеет применять выбранные информационные технологии, программные средства системного и прикладного назначений для решения задач профессиональной деятельности, устранять выявленные уязвимости автоматизированной системы, приводящие к возникновению угроз безопасности информации	конфигурировать параметры системы защиты информации автоматизированной системы в соответствии с ее эксплуатационной документацией; работать с документацией, прилагаемой разработчиком устройства; разбираться в существующих IoT-технологиях и применять их к конкретным сценариям;
	ОПК-12.3. Владеет навыками осуществления автономной наладки технических и программных средств системы защиты информации автоматизированной системы	базовыми навыками по объединению конечных устройств в сеть; навыками реализации сетевых протоколов с помощью программных средств; навыками применения нормативно правовых актов и нормативных методических документов в области инфокоммуникационных систем; навыками поиска технической документации по используемым средствам и технологиям (языкам программирования, программным интерфейсам, протоколам передачи данных); навыками работы с технической документацией по целевому аппаратному средству
Профессиональные компетенции		
-	-	-

4. Объем дисциплины в зачетных единицах с указанием количества академических часов, выделенных на контактную работу обучающихся с преподавателем и на самостоятельную работу обучающихся

Общая трудоемкость дисциплины составляет 5 зачетных единиц, 180 академических часов.

Распределение трудоемкости дисциплины по видам учебной деятельности представлено в таблице 4.1.

Таблица 4.1 – Трудоемкость дисциплины по видам учебной деятельности

Виды учебной деятельности	Всего часов	Семестры
		10 семестр
Контактная аудиторная работа обучающихся с преподавателем, всего	68	68
Лекционные занятия	28	28
Лабораторные занятия	40	40
Самостоятельная работа обучающихся, в т.ч. контактная внеаудиторная работа обучающихся с преподавателем, всего	76	76
Подготовка к тестированию	28	28
Подготовка к лабораторной работе, написание отчета	48	48
Подготовка и сдача экзамена	36	36
Общая трудоемкость (в часах)	180	180
Общая трудоемкость (в з.е.)	5	5

5. Структура и содержание дисциплины

5.1. Разделы (темы) дисциплины и виды учебной деятельности

Структура дисциплины по разделам (темам) и видам учебной деятельности приведена в таблице 5.1.

Таблица 5.1 – Разделы (темы) дисциплины и виды учебной деятельности

Названия разделов (тем) дисциплины	Лек. зан., ч	Лаб. раб.	Сам. раб., ч	Всего часов (без экзамена)	Формируемые компетенции
10 семестр					
1 Угрозы безопасности Интернета Вещей	8	12	22	42	ОПК-12, ОПК-9
2 Уязвимости аппаратной части систем Интернета Вещей	6	8	16	30	ОПК-12, ОПК-9
3 Уязвимости беспроводных каналов передачи информации систем Интернета Вещей	10	20	34	64	ОПК-12, ОПК-9
4 Атаки на экосистемы Интернета вещей	4	-	4	8	ОПК-12, ОПК-9
Итого за семестр	28	40	76	144	
Итого	28	40	76	144	

5.2. Содержание разделов (тем) дисциплины

Содержание разделов (тем) дисциплины (в т.ч. по лекциям) приведено в таблице 5.2.

Таблица 5.2 – Содержание разделов (тем) дисциплины (в т.ч. по лекциям)

Названия разделов (тем) дисциплины	Содержание разделов (тем) дисциплины (в т.ч. по лекциям)	Трудоемкость (лекционные занятия), ч	Формируемые компетенции
10 семестр			

1 Угрозы безопасности Интернета Вещей	Интернет вещей: технологии, рынок, развитие;	2	ОПК-9, ОПК-12
	Анализ угроз безопасности и классификация уязвимостей систем Интернета Вещей	2	ОПК-9, ОПК-12
	Моделирование угроз для систем Интернета Вещей	2	ОПК-9, ОПК-12
	Методология и инструменты тестирования безопасности систем Интернета Вещей	2	ОПК-9, ОПК-12
	Итого	8	
2 Уязвимости аппаратной части систем Интернета Вещей	Аппаратные механизмы обеспечения безопасности систем Интернета Вещей	2	ОПК-9, ОПК-12
	Уязвимости аппаратной части систем Интернета Вещей	2	ОПК-9, ОПК-12
	Взлом прошивки устройств систем Интернета Вещей	2	ОПК-9, ОПК-12
	Итого	6	
3 Уязвимости беспроводных каналов передачи информации систем Интернета Вещей	Оценка безопасности сети Интернета Вещей	2	ОПК-9, ОПК-12
	Анализ сетевых протоколов используемых в системах Интернета Вещей	2	ОПК-9, ОПК-12
	Безопасность беспроводных каналов ближнего радиуса действия	2	ОПК-9, ОПК-12
	Безопасность беспроводных каналов среднего радиуса действия	2	ОПК-9, ОПК-12
	Безопасность беспроводных каналов дальнего радиуса действия	2	ОПК-9, ОПК-12
	Итого	10	
4 Атаки на экосистемы Интернета вещей	Угрозы в мобильных приложениях интернета вещей	2	ОПК-9, ОПК-12
	Инструменты анализа приложений для iOS и Android	2	ОПК-9, ОПК-12
	Итого	4	
Итого за семестр		28	
Итого		28	

5.3. Практические занятия (семинары)

Не предусмотрено учебным планом

5.4. Лабораторные занятия

Наименование лабораторных работ приведено в таблице 5.4.

Таблица 5.4 – Наименование лабораторных работ

Названия разделов (тем) дисциплины	Наименование лабораторных работ	Трудоемкость, ч	Формируемые компетенции
10 семестр			

1 Угрозы безопасности Интернета Вещей	Работа с поисковыми системами Интернета вещей	4	ОПК-9, ОПК-12
	Построение модели угроз системы Интернета Вещей	4	ОПК-9, ОПК-12
	Моделирование атак на LoRa	4	ОПК-9, ОПК-12
	Итого	12	
2 Уязвимости аппаратной части систем Интернета Вещей	Получение доступа к целевому устройству через отладочные интерфейсы	8	ОПК-9, ОПК-12
	Итого	8	
3 Уязвимости беспроводных каналов передачи информации систем Интернета Вещей	Исследование узлов сети	4	ОПК-9, ОПК-12
	Моделирование атак на RFID	4	ОПК-9, ОПК-12
	Моделирование атак на BLE	4	ОПК-9, ОПК-12
	Моделирование атак на Wi-Fi	4	ОПК-9, ОПК-12
	Сниффинг BLE-трафика	4	ОПК-9, ОПК-12
	Итого	20	
Итого за семестр		40	
Итого		40	

5.5. Курсовой проект / курсовая работа

Не предусмотрено учебным планом

5.6. Самостоятельная работа

Виды самостоятельной работы, трудоемкость и формируемые компетенции представлены в таблице 5.6.

Таблица 5.6. – Виды самостоятельной работы, трудоемкость и формируемые компетенции

Названия разделов (тем) дисциплины	Виды самостоятельной работы	Трудоемкость, ч	Формируемые компетенции	Формы контроля
10 семестр				
1 Угрозы безопасности Интернета Вещей	Подготовка к тестированию	8	ОПК-9, ОПК-12	Тестирование
	Подготовка к лабораторной работе, написание отчета	14	ОПК-9, ОПК-12	Лабораторная работа
	Итого	22		
2 Уязвимости аппаратной части систем Интернета Вещей	Подготовка к лабораторной работе, написание отчета	10	ОПК-9, ОПК-12	Лабораторная работа
	Подготовка к тестированию	6	ОПК-9, ОПК-12	Тестирование
	Итого	16		
3 Уязвимости беспроводных каналов передачи информации систем Интернета Вещей	Подготовка к тестированию	10	ОПК-9, ОПК-12	Тестирование
	Подготовка к лабораторной работе, написание отчета	24	ОПК-9, ОПК-12	Лабораторная работа
	Итого	34		

4 Атаки на экосистемы Интернета вещей	Подготовка к тестированию	4	ОПК-9, ОПК-12	Тестирование
	Итого	4		
	Итого за семестр	76		
	Подготовка и сдача экзамена	36		Экзамен
	Итого	112		

5.7. Соответствие компетенций, формируемых при изучении дисциплины, и видов учебной деятельности

Соответствие компетенций, формируемых при изучении дисциплины, и видов учебной деятельности представлено в таблице 5.7.

Таблица 5.7 – Соответствие компетенций, формируемых при изучении дисциплины, и видов занятий

Формируемые компетенции	Виды учебной деятельности			Формы контроля
	Лек. зан.	Лаб. раб.	Сам. раб.	
ОПК-9	+	+	+	Лабораторная работа, Тестирование, Экзамен
ОПК-12	+	+	+	Лабораторная работа, Тестирование, Экзамен

6. Рейтинговая система для оценки успеваемости обучающихся

6.1. Балльные оценки для форм контроля

Балльные оценки для форм контроля представлены в таблице 6.1.

Таблица 6.1 – Балльные оценки

Формы контроля	Максимальный балл на 1-ую КТ с начала семестра	Максимальный балл за период между 1КТ и 2КТ	Максимальный балл за период между 2КТ и на конец семестра	Всего за семестр
10 семестр				
Лабораторная работа	14	28	21	63
Тестирование	2	2	3	7
Экзамен				30
Итого максимум за период	16	30	24	100
Нарастающим итогом	16	46	70	100

6.2. Пересчет баллов в оценки за текущий контроль

Пересчет баллов в оценки за текущий контроль представлен в таблице 6.2.

Таблица 6.2 – Пересчет баллов в оценки за текущий контроль

Баллы на дату текущего контроля	Оценка
≥ 90% от максимальной суммы баллов на дату ТК	5
От 70% до 89% от максимальной суммы баллов на дату ТК	4
От 60% до 69% от максимальной суммы баллов на дату ТК	3
< 60% от максимальной суммы баллов на дату ТК	2

6.3. Пересчет суммы баллов в традиционную и международную оценку

Пересчет суммы баллов в традиционную и международную оценку представлен в таблице 6.3.

Таблица 6.3 – Пересчет суммы баллов в традиционную и международную оценку

Оценка	Итоговая сумма баллов, учитывает успешно сданный экзамен	Оценка (ECTS)
5 (отлично) (зачтено)	90 – 100	A (отлично)
4 (хорошо) (зачтено)	85 – 89	B (очень хорошо)
	75 – 84	C (хорошо)
	70 – 74	D (удовлетворительно)
3 (удовлетворительно) (зачтено)	65 – 69	E (посредственно)
	60 – 64	
2 (неудовлетворительно) (не зачтено)	Ниже 60 баллов	F (неудовлетворительно)

7. Учебно-методическое и информационное обеспечение дисциплины

7.1. Основная литература

1. Ли, П. Архитектура интернета вещей / П. Ли ; перевод с английского М. А. Райтман. Москва : ДМК Пресс, 2019. — 454 с. — ISBN 978-5-97060-672-8. — Текст : электронный // Лань : электронно-библиотечная система. - Режим доступа: для авториз. пользователей [Электронный ресурс]: — Режим доступа: <https://e.lanbook.com/book/112923>.

7.2. Дополнительная литература

1. Диогенес, Ю. Кибербезопасность. стратегия атак и обороны / Ю. Диогенес, Э. Озкайя ; перевод с английского Д. А. Беликова. — Москва : ДМК Пресс, 2020. — 326 с. — ISBN 978-5-97060-709-1. — Текст : электронный // Лань : электронно-библиотечная система. — Режим доступа: для авториз. пользователей. [Электронный ресурс]: — Режим доступа: <https://e.lanbook.com/book/131717>.

2. Нестеров, С. А. Основы информационной безопасности / С. А. Нестеров. — 2-е изд., стер. — Санкт-Петербург : Лань, 2023. — 324 с. — ISBN 978-5-507-48149-1. — Текст : электронный // Лань : электронно-библиотечная система. — Режим доступа: для авториз. пользователей. [Электронный ресурс]: — Режим доступа: <https://e.lanbook.com/book/341267>.

3. Безопасность беспроводных локальных сетей : учебное пособие / М. М. Ковцур, Д. В. Юркин, Е. Ю. Герлинг, К. А. Ахрамеева. — Санкт-Петербург : СПбГУТ им. М.А. Бонч-Бруевича, 2021. — 71 с. — ISBN 978-5-89160-227-4. — Текст : электронный // Лань : электронно-библиотечная система. — Режим доступа: для авториз. пользователей. [Электронный ресурс]: — Режим доступа: <https://e.lanbook.com/book/279623>.

7.3. Учебно-методические пособия

7.3.1. Обязательные учебно-методические пособия

1. Поздняк, И. С. Обеспечение безопасности в беспроводных сетях : методические указания / И. С. Поздняк, Н. В. Киреева, О. А. Караулова. — Самара : ПГУТИ, 2019. — 22 с. — Текст : электронный // Лань : электронно-библиотечная система. — Режим доступа: для авториз. пользователей. [Электронный ресурс]: — Режим доступа: <https://e.lanbook.com/book/223310>.

2. Информационная безопасность интернета вещей: Учебно-методическое пособие / О. В. Пехов - 2022. 34 с. [Электронный ресурс]: — Режим доступа: <https://edu.tusur.ru/publications/9998>.

7.3.2. Учебно-методические пособия для лиц с ограниченными возможностями здоровья и инвалидов

Учебно-методические материалы для самостоятельной и аудиторной работы обучающихся из числа лиц с ограниченными возможностями здоровья и инвалидов предоставляются в формах, адаптированных к ограничениям их здоровья и восприятия информации.

Для лиц с нарушениями зрения:

- в форме электронного документа;
- в печатной форме увеличенным шрифтом.

Для лиц с нарушениями слуха:

- в форме электронного документа;

– в печатной форме.

Для лиц с нарушениями опорно-двигательного аппарата:

– в форме электронного документа;

– в печатной форме.

7.4. Современные профессиональные базы данных и информационные справочные системы

1. При изучении дисциплины рекомендуется обращаться к современным базам данных, информационно-справочным и поисковым системам, к которым у ТУСУРа открыт доступ: <https://lib.tusur.ru/ru/resursy/bazy-dannyh>.

8. Материально-техническое и программное обеспечение дисциплины

8.1. Материально-техническое и программное обеспечение для лекционных занятий

Для проведения занятий лекционного типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации используется учебная аудитория с достаточным количеством посадочных мест для учебной группы, оборудованная доской и стандартной учебной мебелью. Имеются мультимедийное оборудование и учебно-наглядные пособия, обеспечивающие тематические иллюстрации по лекционным разделам дисциплины.

8.2. Материально-техническое и программное обеспечение для лабораторных работ

Лаборатория защиты информации в системах Интернета вещей: учебная аудитория для проведения занятий практического типа, учебная аудитория для проведения занятий лабораторного типа; 634045, Томская область, г. Томск, ул. Красноармейская, д. 146, 707 ауд.

Описание имеющегося оборудования:

- Интерактивная доска Samsung LH75QBHRTBC/CI;
- Модуль UMDK-RFU адаптера внешних датчиков;
- Модем радиосети LoRa;
- Модуль UMDK-LIT датчика естественной освещенности;
- Модуль UMDK-THP датчика температуры, влажности, давления воздуха;
- Модуль UMDK-6FET управления нагрузками постоянного тока;
- Источник питания 12 В 1,5А;
- Источник питания 5В 2А;
- Модуль UMDK-LMT внешних термодатчиков;
- Модуль UMDK-SOUND датчика звукового давления;
- Мультиметр UT-139C;
- Универсальная лаборатория Analog Discovery 2;
- UMDK-PIR;
- STM32F0DISCOVERY;
- Отладочная плата на базе MCU STM32F051R8T6 (ARM Cortex-M0), ST-LINK/V;
- Комплект специализированной учебной мебели;
- Рабочее место преподавателя.

Программное обеспечение:

- ОС Ubuntu 16.04;

8.3. Материально-техническое и программное обеспечение для самостоятельной работы

Для самостоятельной работы используются учебные аудитории (компьютерные классы), расположенные по адресам:

- 634050, Томская область, г. Томск, Ленина проспект, д. 40, 233 ауд.;
- 634045, Томская область, г. Томск, ул. Красноармейская, д. 146, 209 ауд.;
- 634034, Томская область, г. Томск, Вершинина улица, д. 47, 126 ауд.;
- 634034, Томская область, г. Томск, Вершинина улица, д. 74, 207 ауд.

Описание имеющегося оборудования:

- учебная мебель;
- компьютеры;
- компьютеры подключены к сети «Интернет» и обеспечивают доступ в электронную

информационно-образовательную среду ТУСУРа.

Перечень программного обеспечения:

- Microsoft Windows;
- OpenOffice;
- Kaspersky Endpoint Security 10 для Windows;
- 7-Zip;
- Google Chrome.

8.4. Материально-техническое обеспечение дисциплины для лиц с ограниченными возможностями здоровья и инвалидов

Освоение дисциплины лицами с ограниченными возможностями здоровья и инвалидами осуществляется с использованием средств обучения общего и специального назначения.

При занятиях с обучающимися с **нарушениями слуха** предусмотрено использование звукоусиливающей аппаратуры, мультимедийных средств и других технических средств приема/передачи учебной информации в доступных формах, мобильной системы преподавания для обучающихся с инвалидностью, портативной индукционной системы. Учебная аудитория, в которой занимаются обучающиеся с нарушением слуха, оборудована компьютерной техникой, аудиотехникой, видеотехникой, электронной доской, мультимедийной системой.

При занятиях с обучающимися с **нарушениями зрения** предусмотрено использование в лекционных и учебных аудиториях возможности просмотра удаленных объектов (например, текста на доске или слайда на экране) при помощи видеоувеличителей для комфортного просмотра.

При занятиях с обучающимися с **нарушениями опорно-двигательного аппарата** используются альтернативные устройства ввода информации и другие технические средства приема/передачи учебной информации в доступных формах, мобильной системы обучения для людей с инвалидностью.

9. Оценочные материалы и методические рекомендации по организации изучения дисциплины

9.1. Содержание оценочных материалов для текущего контроля и промежуточной аттестации

Для оценки степени сформированности и уровня освоения закрепленных за дисциплиной компетенций используются оценочные материалы, представленные в таблице 9.1.

Таблица 9.1 – Формы контроля и оценочные материалы

Названия разделов (тем) дисциплины	Формируемые компетенции	Формы контроля	Оценочные материалы (ОМ)
1 Угрозы безопасности Интернета Вещей	ОПК-12, ОПК-9	Лабораторная работа	Темы лабораторных работ
		Тестирование	Примерный перечень тестовых заданий
		Экзамен	Перечень экзаменационных вопросов
2 Уязвимости аппаратной части систем Интернета Вещей	ОПК-12, ОПК-9	Лабораторная работа	Темы лабораторных работ
		Тестирование	Примерный перечень тестовых заданий
		Экзамен	Перечень экзаменационных вопросов

3 Уязвимости беспроводных каналов передачи информации систем Интернета Вещей	ОПК-12, ОПК-9	Лабораторная работа	Темы лабораторных работ
		Тестирование	Примерный перечень тестовых заданий
		Экзамен	Перечень экзаменационных вопросов
4 Атаки на экосистемы Интернета вещей	ОПК-12, ОПК-9	Тестирование	Примерный перечень тестовых заданий
		Экзамен	Перечень экзаменационных вопросов

Шкала оценки сформированности отдельных планируемых результатов обучения по дисциплине приведена в таблице 9.2.

Таблица 9.2 – Шкала оценки сформированности планируемых результатов обучения по дисциплине

Оценка	Баллы за ОМ	Формулировка требований к степени сформированности планируемых результатов обучения		
		знать	уметь	владеть
2 (неудовлетворительно)	< 60% от максимальной суммы баллов	отсутствие знаний или фрагментарные знания	отсутствие умений или частично освоенное умение	отсутствие навыков или фрагментарные применение навыков
3 (удовлетворительно)	от 60% до 69% от максимальной суммы баллов	общие, но не структурированные знания	в целом успешно, но не систематически осуществляемое умение	в целом успешное, но не систематическое применение навыков
4 (хорошо)	от 70% до 89% от максимальной суммы баллов	сформированные, но содержащие отдельные проблемы знания	в целом успешное, но содержащие отдельные пробелы умение	в целом успешное, но содержащие отдельные пробелы применение навыков
5 (отлично)	≥ 90% от максимальной суммы баллов	сформированные систематические знания	сформированное умение	успешное и систематическое применение навыков

Шкала комплексной оценки сформированности компетенций приведена в таблице 9.3.

Таблица 9.3 – Шкала комплексной оценки сформированности компетенций

Оценка	Формулировка требований к степени компетенции
2 (неудовлетворительно)	Не имеет необходимых представлений о проверяемом материале или Знать на уровне ориентирования , представлений. Обучающийся знает основные признаки или термины изучаемого элемента содержания, их отнесенность к определенной науке, отрасли или объектам, узнает в текстах, изображениях или схемах и знает, к каким источникам нужно обращаться для более детального его усвоения.

3 (удовлетворительно)	Знать и уметь на репродуктивном уровне. Обучающихся знает изученный элемент содержания репродуктивно: произвольно воспроизводит свои знания устно, письменно или в демонстрируемых действиях.
4 (хорошо)	Знать, уметь, владеть на аналитическом уровне. Зная на репродуктивном уровне, указывать на особенности и взаимосвязи изученных объектов, на их достоинства, ограничения, историю и перспективы развития и особенности для разных объектов усвоения.
5 (отлично)	Знать, уметь, владеть на системном уровне. Обучающийся знает изученный элемент содержания системно, произвольно и доказательно воспроизводит свои знания устно, письменно или в демонстрируемых действиях, учитывая и указывая связи и зависимости между этим элементом и другими элементами содержания дисциплины, его значимость в содержании дисциплины.

9.1.1. Примерный перечень тестовых заданий

- Какая из данных технологий способна образовывать самоорганизующуюся ячеистую сеть(mesh-сеть) по умолчанию, без дополнительных усилий?
 - WiFi
 - ZigBee
 - Bluetooth
 - LoRa
- В каком формате сообщение будет иметь наименьший объем, если считать посимвольно при прочих равных условиях?
 - HTML
 - YAML
 - JSON
 - XML
- Допустим, что вы конструируете устройство, которое должно знать о том, открыта ли дверь. Какой механизм протокола MQTT стоит использовать, чтобы новые подписчики сразу узнавали статус двери?
 - Retain
 - Network Pipe
 - Last Will
 - QoS
- Для чего используется механизм MQTT, называемый “Завещание” (“Last Will”)?
 - Уведомить подписчиков о том, что есть проблема на стороне издателя
 - Оставить сообщение “до востребования”, то есть сделать его доступным для новых подписчиков
 - Гарантировать доставку сообщения
 - Уведомить издателя о проблеме с сетью
- Что нужно сделать подписчику чтобы получить “Завещание” (“Last Will”)?
 - Установить флаг “Last Will”
 - Подписаться на топик с качеством обслуживания не ниже 1
 - Установить флаг “Retain”
 - Ничего специально делать не нужно, письмо придёт автоматически
- Для решения какой задачи вы точно не будете использовать технологию LoRa?
 - Измерение температуры тела коровы
 - Снятие показаний электронных счетчиков ЖКХ
 - Отслеживание местоположения транспорта в реальном времени
 - Экологический мониторинг реки на предмет слива промышленных отходов
- Как достигается уникальность идентификатора устройства (DevEUI) в сетях LoRa?
 - Производитель конечных устройств назначает идентификатор из диапазона разрешённых адресов
 - Никак не достигается, идентификатор можно свободно менять

- в) Производитель приёмопередатчиков LoRa, компания Semtech, присваивает идентификатор каждому чипу
- г) Проектировщик конкретной системы назначает адреса устройствам
- 8. Почему не стоит делать период опроса датчиков меньше 1 минуты, если мы работаем с системой LoRa?
 - а) Отправка и пересылка сообщений занимает слишком много времени, поэтому это создаст “затор” в сети
 - б) Период менее 1 минуты не поддерживается RIOT OS
 - в) Архитектура микроконтроллера не позволяет назначить период дробным числом
 - г) Датчик не успевает оцифровать показания
- 9. Какой протокол используется на транспортном уровне в протоколе MQTT-SN (Sensor Networks)?
 - а) UDP
 - б) UDP-Lite
 - в) SCTP
 - г) TCP
- 10. В каком радиодиапазоне работает WiFi?
 - а) 915 МГц
 - б) 108 МГц
 - в) 868 МГц
 - г) 2450 МГц

9.1.2. Перечень экзаменационных вопросов

1. Типы объектов защиты информации и их определения.
2. Свойства информации, обеспечиваемые при её защите.
3. Категории доступа к информации. Степени секретности сведений, составляющих государственную тайну.
4. Виды информации, относящейся к сведениям конфиденциального характера.
5. Понятие «нарушение информационной безопасности». Примеры атак на информационные системы.

9.1.3. Темы лабораторных работ

1. Работа с поисковыми системами Интернета вещей
2. Построение модели угроз системы Интернета Вещей
3. Моделирование атак на LoRa
4. Получение доступа к целевому устройству через отладочные интерфейсы
5. Исследование узлов сети
6. Моделирование атак на RFID
7. Моделирование атак на BLE
8. Моделирование атак на Wi-Fi
9. Сниффинг BLE-трафика

9.2. Методические рекомендации

Учебный материал излагается в форме, предполагающей самостоятельное мышление студентов, самообразование. При этом самостоятельная работа студентов играет решающую роль в ходе всего учебного процесса.

Начать изучение дисциплины необходимо со знакомства с рабочей программой, списком учебно-методического и программного обеспечения. Самостоятельная работа студента включает работу с учебными материалами, выполнение контрольных мероприятий, предусмотренных учебным планом.

В процессе изучения дисциплины для лучшего освоения материала необходимо регулярно обращаться к рекомендуемой литературе и источникам, указанным в учебных материалах; пользоваться через кабинет студента на сайте Университета образовательными ресурсами электронно-библиотечной системы, а также общедоступными интернет-порталами, содержащими научно-популярные и специализированные материалы, посвященные различным аспектам учебной дисциплины.

При самостоятельном изучении тем следуйте рекомендациям:

– чтение или просмотр материала осуществляйте со скоростью, достаточной для индивидуального понимания и освоения материала, выделяя основные идеи; на основании изученного составить тезисы. Освоив материал, попытаться соотнести теорию с примерами из практики;

– если в тексте встречаются незнакомые или малознакомые термины, следует выяснить их значение для понимания дальнейшего материала;

– осмысливайте прочитанное и изученное, отвечайте на предложенные вопросы.

Студенты могут получать индивидуальные консультации, в т.ч. с использованием средств телекоммуникации.

По дисциплине могут проводиться дополнительные занятия, в т.ч. в форме вебинаров. Расписание вебинаров и записи вебинаров публикуются в электронном курсе / электронном журнале по дисциплине.

9.3. Требования к оценочным материалам для лиц с ограниченными возможностями здоровья и инвалидов

Для лиц с ограниченными возможностями здоровья и инвалидов предусмотрены дополнительные оценочные материалы, перечень которых указан в таблице 9.4.

Таблица 9.4 – Дополнительные материалы оценивания для лиц с ограниченными возможностями здоровья и инвалидов

Категории обучающихся	Виды дополнительных оценочных материалов	Формы контроля и оценки результатов обучения
С нарушениями слуха	Тесты, письменные самостоятельные работы, вопросы к зачету, контрольные работы	Преимущественно письменная проверка
С нарушениями зрения	Собеседование по вопросам к зачету, опрос по терминам	Преимущественно устная проверка (индивидуально)
С нарушениями опорно-двигательного аппарата	Решение дистанционных тестов, контрольные работы, письменные самостоятельные работы, вопросы к зачету	Преимущественно дистанционными методами
С ограничениями по общемедицинским показаниям	Тесты, письменные самостоятельные работы, вопросы к зачету, контрольные работы, устные ответы	Преимущественно проверка методами, определяющимися исходя из состояния обучающегося на момент проверки

9.4. Методические рекомендации по оценочным материалам для лиц с ограниченными возможностями здоровья и инвалидов

Для лиц с ограниченными возможностями здоровья и инвалидов предусматривается доступная форма предоставления заданий оценочных средств, а именно:

- в печатной форме;
- в печатной форме с увеличенным шрифтом;
- в форме электронного документа;
- методом чтения ассистентом задания вслух;
- предоставление задания с использованием сурдоперевода.

Лицам с ограниченными возможностями здоровья и инвалидам увеличивается время на подготовку ответов на контрольные вопросы. Для таких обучающихся предусматривается доступная форма предоставления ответов на задания, а именно:

- письменно на бумаге;
- набор ответов на компьютере;
- набор ответов с использованием услуг ассистента;
- представление ответов устно.

Процедура оценивания результатов обучения лиц с ограниченными возможностями

здоровья и инвалидов по дисциплине предусматривает предоставление информации в формах, адаптированных к ограничениям их здоровья и восприятия информации:

Для лиц с нарушениями зрения:

- в форме электронного документа;
- в печатной форме увеличенным шрифтом.

Для лиц с нарушениями слуха:

- в форме электронного документа;
- в печатной форме.

Для лиц с нарушениями опорно-двигательного аппарата:

- в форме электронного документа;
- в печатной форме.

При необходимости для лиц с ограниченными возможностями здоровья и инвалидов процедура оценивания результатов обучения может проводиться в несколько этапов.

ЛИСТ СОГЛАСОВАНИЯ

Рассмотрена и одобрена на заседании кафедры КИБЭВС
протокол № 1 от «24» 1 2023 г.

СОГЛАСОВАНО:

Должность	Инициалы, фамилия	Подпись
Заведующий выпускающей каф. КИБЭВС	А.А. Шелупанов	Согласовано, c53e145e-8b20-45aa- 9347-a5e4dbb90e8d
Заведующий обеспечивающей каф. КИБЭВС	А.А. Шелупанов	Согласовано, c53e145e-8b20-45aa- 9347-a5e4dbb90e8d
И.О. начальника учебного управления	И.А. Лариошина	Согласовано, c3195437-a02f-4972- a7c6-ab6ee1f21e73

ЭКСПЕРТЫ:

Доцент, каф. КИБЭВС	А.А. Конев	Согласовано, 81687a04-85ce-4835- 9e1e-9934a6085fdd
Доцент, каф. КИБЭВС	А.Ю. Якимук	Согласовано, 4ffdf265-fb78-4863- b293-f03438cb07cc

РАЗРАБОТАНО:

Старший преподаватель, каф. КИБЭВС	О.В. Пехов	Разработано, 20c0ed46-bc2c-48e8- a44a-b830ba556cfd
------------------------------------	------------	--