МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования

«Воронежский государственный технический университет»

УТВЕРЖДАЮ

Декан факультета ФИТКБ

_____/Гусев П.Ю./

_____ 202_ г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«Безопасность информационных систем и сетей интернета вещей»

Специальность 10.05.03 Информационная безопасность автоматизированных систем

Специализация специализация N 7 "Анализ безопасности информационных систем"

Квалификация выпускника специалист по защите информации

Нормативный период обучения 5 лет и 6 м.

Форма обучения очная

Год начала подготовки 2023

Автор программы _____ С.А. Ермаков

Заведующий кафедрой Систем информационной безопасности _____ А.Г. Остапенко

Руководитель ОПОП _____ А.Г. Остапенко

Воронеж 2023

1. ЦЕЛИ И ЗАДАЧИ ДИСЦИПЛИНЫ

1.1. Цели дисциплины

Формирование навыков оценки и регулирования рисков защищенности информационных систем и сетей интернета вещей.

1.2. Задачи освоения дисциплины

- изучить основы проектирования систем информационной безопасности в информационных системах и сетях интернета вещей;
- получить практических навыки анализа систем связи с точки зрения определения целей защиты и непосредственного внедрения алгоритмов защиты информации в информационных системах и сетях интернета вещей;
- изучить функциональные особенности современных стандартов информационных систем и сетей интернета вещей;
- изучить методологии анализа и оценки эффективности использования систем связи и передачи информации с учетом помехозащищенности, выбора метода шифрования и кодирования, объема и скорости передачи информации.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП

Дисциплина «Безопасность информационных систем и сетей интернета вещей» относится к дисциплинам части, формируемой участниками образовательных отношений (дисциплина по выбору) блока Б1.

3. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ

Процесс изучения дисциплины «Безопасность информационных систем и сетей интернета вещей» направлен на формирование следующих компетенций:

ПК-7.4 - Способен разрабатывать программные и программно-аппаратные средства для систем защиты информации автоматизированных систем

Компетенция	Результаты обучения, характеризующие сформированность компетенции
ПК-7.4	знать эталонную модель взаимодействия открытых систем, основные протоколы, последовательность и содержание этапов построения и функционирования современных локальных и глобальных компьютерных сетей; принципы построения компьютерных систем и сетей Интернета Вещей; модели безопасности компьютерных систем; виды политик безопасности компьютерных систем и сетей Интернета Вещей; методы, способы, средства, последовательность и содержание этапов разработки автоматизированных систем и систем защиты информации в автоматизированных системах

	уметь выявлять уязвимости информационно-технологических ресурсов автоматизированных систем, выполнять анализ безопасности компьютерных систем и разрабатывать рекомендации по эксплуатации системы защиты информации; разрабатывать предложения по устранению выявленных уязвимостей; оценивать информационные риски в автоматизированных системах Интернета Вещей и определять информационную инфраструктуру и информационные ресурсы, подлежащие защите.
	владеть навыками разработки предложений по совершенствованию системы управления информационной безопасностью автоматизированных систем, навыками определения угроз безопасности информации, реализация которых может привести к нарушению безопасности информации в компьютерной системе и сети Интернета вещей, навыками оценки рисков, связанных с осуществлением угроз безопасности в отношении компьютерных систем, навыками формирования требований по защите информации, включая использование математического аппарата для решения прикладных задач.

4. ОБЪЕМ ДИСЦИПЛИНЫ

Общая трудоемкость дисциплины «Безопасность информационных систем и сетей интернета вещей» составляет 6 з.е.

Распределение трудоемкости дисциплины по видам занятий

очная форма обучения

Виды учебной работы	Всего часов	Семестры
		8
Аудиторные занятия (всего)	54	54
В том числе:		
Лекции	36	36
Лабораторные работы (ЛР)	18	18
Самостоятельная работа	162	162
Виды промежуточной аттестации - зачет с оценкой	+	+
Общая трудоемкость:		

академические часы	216	216
зач.ед.	6	6

5. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

5.1 Содержание разделов дисциплины и распределение трудоемкости по видам занятий

очная форма обучения

№ п/п	Наименование темы	Содержание раздела	Лекц	Лаб. зан.	СРС	Всего, час
1	Основы построения беспроводных сетей	Цели и задачи курса. Предмет, структура и краткое содержание курса. Краткий экскурс в историю беспроводной связи. Основные термины и понятия. Постановка задачи распределенной обработки данных. Классификация сетей по способам распределения данных, сравнительная характеристика различных типов сетей. Основные сетевые стандарты и протоколы. Сетевые операционные системы. Средства взаимодействия процессов в сетях. Распределенная обработка информации в системах клиент-сервер, одноранговые сети, локальные и глобальные сети. Неоднородные вычислительные сети.	8	6	46	60
2	Технологии обеспечения безопасности в информационных системах и сетях интернета вещей	Основы классификации сетевых угроз и атак. Примеры типовых атак и рекомендации по построению систем защиты. Влияние человеческого фактора на сетевую безопасность. Маршрутизаторы, межсетевые экраны (МЭ). Основные механизмы применения МЭ. Абонентское шифрование. Виртуальные частные сети. Защита компонентов сети от НСД. Безопасность ресурсов сети: средства идентификации и аутентификации, методы разделения ресурсов и технологии разграничения доступа. Электронная цифровая подпись и пакетное шифрование. Криптографические сетевые протоколы. Управление ключами. Защита от сбоев электропитания, аппаратного и программного обеспечения. Контроль и распределение нагрузки на вычислительную сеть. Стандарты безопасности вычислительных сетей и их компонентов. Правовые основы защиты информации в сетях.	10	3	34	47
3	Проектирование защищенных сетей интернета вещей	Понятие политики безопасности. Типовые элементы политики безопасности. Рекомендации по построению политики безопасности. Основные шаги по реализации политики безопасности. Основные критерии анализа сетевой безопасности. Общая процедура анализа. Классификация беспроводных систем, анализ состава и архитектурных особенностей построения сетей интернета вещей, изучение функциональных особенностей современных стандартов	6	5	43	54

		сетей интернета вещей.				
4	Методы и алгоритмы прогнозирования эффективности защиты информационных систем и сетей интернета вещей	Постановка задачи оценки эффективности наборов средств защиты беспроводных сетей. Оценка эффективности системы обеспечения безопасности информационной системы и сети интернета вещей. Организация и управление экспертной системой для оценки основных показателей защищенности сети интернета вещей. Методический подход к оптимизации выбора мер и средств защиты информационной системы и сети интернета вещей.	12	4	39	55
		Итого	**36**	**18**	**162**	**216**

5.2 Перечень лабораторных работ

1. Принципы построения беспроводных сетей связи. Монтаж, настройка и защита беспроводной сети – 3 ч.
   - настройка сети со статическим адресом беспроводного клиента;
   - настройка сети с динамическим адресом беспроводного клиента.
2. Технологии обеспечения безопасности в информационных системах и сетях интернета вещей. Подключение к беспроводной сети – 5 ч.
   - организация одноранговой (ad hoc) сети;
   - перехват пакетов беспроводной сети.
3. Проектирование защищенных сетей интернета вещей – 4 ч.
   - настройка системы защиты точки доступа через web-интерфейс;
   - анализ и выбор протоколов безопасности устройств в проектируемой сети.
4. Методы и алгоритмы прогнозирования эффективности защиты информационных систем и сетей интернета вещей – 3 ч.
   - анализ эффективности сети интернета вещей при использовании различных протоколов безопасности;
   - выработка рекомендаций к построению эффективной сети интернета вещей.
5. Модели прогнозной оценки риска в сетях интернета вещей – 3 ч.
   - овладение навыками моделирования сети интернета вещей;
   - механизм нечетко-множественной оценки риска безопасности сети интернета вещей.

6. ПРИМЕРНАЯ ТЕМАТИКА КУРСОВЫХ ПРОЕКТОВ (РАБОТ) И КОНТРОЛЬНЫХ РАБОТ

В соответствии с учебным планом освоение дисциплины не предусматривает выполнение курсового проекта (работы) или контрольной работы.

7. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ДЛЯ ПРОВЕДЕНИЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО

ДИСЦИПЛИНЕ

7.1. Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания

7.1.1 Этап текущего контроля

Результаты текущего контроля знаний и межсессионной аттестации оцениваются по следующей системе:

«аттестован»;

«не аттестован».

Компе-тенция	Результаты обучения, характеризующие сформированность компетенции	Критерии оценивания	Аттестован	Не аттестован
ПК-7.4	знать эталонную модель взаимодействия открытых систем, основные протоколы, последовательность и содержание этапов построения и функционирования современных локальных и глобальных компьютерных сетей; принципы построения компьютерных систем и сетей Интернета Вещей; модели безопасности компьютерных систем; виды политик безопасности компьютерных систем и сетей Интернета Вещей; методы, способы, средства, последовательность и содержание этапов разработки автоматизированных систем и систем защиты информации в автоматизированных системах	Знание учебного материала и использование учебного материала в процессе выполнения заданий	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	уметь выявлять уязвимости информационно-технологических ресурсов автоматизированных систем, выполнять анализ безопасности компьютерных систем и разрабатывать рекомендации по эксплуатации системы защиты информации; разрабатывать предложения по устранению выявленных уязвимостей; оценивать информационные риски в автоматизированных системах Интернета Вещей и определять информационную инфраструктуру и информационные ресурсы, подлежащие защите.	Умение использоват учебный материал в процессе выполнения лабораторных работ	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	владеть навыками разработки предложений по совершенствованию системы управления информационной безопасностью автоматизированных систем, навыками определения угроз безопасности информации, реализация которых может привести к нарушению безопасности информации в компьютерной системе и сети Интернета вещей, навыками оценки рисков, связанных с осуществлением угроз безопасности в отношении компьютерных систем, навыками формирования требований по защите	Применение учебного материала в рамках конкретных прикладных заданий	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах

	информации, включая использование математического аппарата для решения прикладных задач.			

7.1.2 Этап промежуточного контроля знаний

Результаты промежуточного контроля знаний оцениваются в 8 семестре для очной формы обучения по четырехбалльной системе:

«отлично»;

«хорошо»;

«удовлетворительно»;

«неудовлетворительно».

Компе-тенция	Результаты обучения, характеризующие сформированность компетенции	Критерии оценивания	Отлично	Хорошо	Удовл.	Неудовл.
ПК-7.4	знать эталонную модель взаимодействия открытых систем, основные протоколы, последовательность и содержание этапов построения и функционирования современных локальных и глобальных компьютерных сетей; принципы построения компьютерных систем и сетей Интернета Вещей; модели безопасности компьютерных систем; виды политик безопасности компьютерных систем и сетей Интернета Вещей; методы, способы, средства, последовательность и содержание этапов разработки автоматизированных систем и систем защиты информации в автоматизированных системах	Тест	Выполнение теста на 90- 100%	Выполнение теста на 80-90%	Выполнение теста на 70-80%	В тесте менее 70% правильных ответов
	уметь выявлять уязвимости информационно-технологических ресурсов автоматизированных систем, выполнять анализ безопасности компьютерных систем и разрабатывать рекомендации по эксплуатации системы защиты информации; разрабатывать предложения по устранению выявленных уязвимостей; оценивать информационные риски в автоматизированных системах Интернета Вещей и определять информационную инфраструктуру и информационные ресурсы, подлежащие защите.	Решение стандартных практических задач	Задачи решены в полном объеме и получены верные ответы	Продемонстр ирован верный ход решения всех, но не получен верный ответ во всех задачах	Продемонстр ирован верный ход решения в большинстве задач	Задачи не решены
	владеть навыками разработки предложений по совершенствованию системы управления информационной безопасностью автоматизированных систем,	Решение прикладных задач в конкретной предметной области	Задачи решены в полном объеме и получены верные	Продемонстр ирован верный ход решения всех, но не получен	Продемонстр ирован верный ход решения в большинстве задач	Задачи не решены

	навыками определения угроз безопасности информации, реализация которых может привести к нарушению безопасности информации в компьютерной системе и сети Интернета вещей, навыками оценки рисков, связанных с осуществлением угроз безопасности в отношении компьютерных систем, навыками формирования требований по защите информации, включая использование математического аппарата для решения прикладных задач.		ответы	верный ответ во всех задачах		

7.2 Примерный перечень оценочных средств (типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности)

7.2.1 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.

7.2.2 Примерный перечень заданий для решения стандартных задач

Не предусмотрен учебным планом

7.2.3 Примерный перечень заданий для решения прикладных задач

Не предусмотрен учебным планом

7.2.4 Примерный перечень вопросов для подготовки к зачету

Билет 1

1. Цели и задачи курса. Предмет, структура и краткое содержание курса.
2. Рекомендации по построению политики безопасности. Основные шаги по реализации политики безопасности. Поддержание и модификация политики безопасности.

Билет 2

1. Стандарты беспроводной передачи данных.
2. Критерии оценки безопасности сетевых ОС.

Билет 3

1. Параметры связи: скорость передачи данных, диапазон частот, метод модуляции сигнала и т.д.
2. Основные критерии анализа сетевой безопасности. Общая процедура анализа. Методика подготовки экспертного заключения.

Билет 4

1. Современные стандарты, используемые в сетях интернета вещей.
2. Регламентирующие документы в области безопасности вычислительных сетей Стандарты безопасности вычислительных сетей и их компонентов. Правовые основы защиты информации в сетях.

Билет 5

1. Типовые угрозы безопасности. Основы классификации сетевых угроз и атак. Примеры типовых атак и рекомендации по построению систем защиты.
2. Анализ возможных сценариев атак.

Билет 6

1. Защита топологии сети. Маршрутизаторы, межсетевые экраны (МЭ). Основные механизмы применения МЭ. Абонентское шифрование.
2. Анализ характерных уязвимостей сетей интернета вещей.

Билет 7

1. Виртуальные частные сети.
2. Прогнозирование эффективности системы обеспечения безопасности сети интернета вещей.

Билет 8

1. Защита сетевого трафика и компонентов сети.
2. Модели принятия решений в условиях неопределенности.

Билет 9

1. Защита компонентов сети от НСД. Безопасность ресурсов сети: средства идентификации и аутентификации, методы разделения ресурсов и технологии разграничения доступа.
2. Архитектура системы безопасности в сетях интернета вещей.

Билет 10

1. Электронная цифровая подпись и пакетное шифрование. Криптографические сетевые протоколы. Управление ключами.
2. Модель безопасности в сетях интернета вещей. Типовые атаки в сетях интернета вещей.

Билет 11

1. Понятие политики безопасности. Типовые элементы политики безопасности.
2. Вероятностный подход к анализу рисков сетей интернета вещей.

Билет 12

1. Методика выбора мер и средств защиты информационной системы и сети интернета вещей.
2. Экспертный подход к анализу рисков сетей интернета вещей.

7.2.5 Примерный перечень заданий для подготовки к экзамену

Не предусмотрен учебным планом

7.2.6. Методика выставления оценки при проведении

промежуточной аттестации

Зачёт с оценкой проводится по тест-билетам, каждый из которых содержит 10 вопросов и задачу. Каждый правильный ответ на вопрос в тесте оценивается 1 баллом, задача оценивается в 10 баллов (5 баллов верное решение и 5 баллов за верный ответ). Максимальное количество набранных баллов – 20.

1. Оценка «Неудовлетворительно» ставится в случае, если студент набрал менее 6 баллов.

2. Оценка «Удовлетворительно» ставится в случае, если студент набрал от 6 до 10 баллов

3. Оценка «Хорошо» ставится в случае, если студент набрал от 11 до 15 баллов.

4. Оценка «Отлично» ставится, если студент набрал от 16 до 20 баллов.

7.2.7 Паспорт оценочных материалов

№ п/п	Контролируемые разделы (темы) дисциплины	Код контролируемой компетенции	Наименование оценочного средства
1	Основы построения беспроводных сетей	ПК-7.4	Тест, выполнение лабораторных работ
2	Технологии обеспечения безопасности в информационных системах и сетях интернета вещей	ПК-7.4	Тест, выполнение лабораторных работ
3	Проектирование защищенных сетей интернета вещей	ПК-7.4	Тест, выполнение лабораторных работ
4	Методы и алгоритмы прогнозирования эффективности защиты информационных систем и сетей интернета вещей	ПК-7.4	Тест, выполнение лабораторных работ

7.3. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности

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.

Выполнение лабораторных работ осуществляется согласно учебного плана в соответствии с методическими указаниями к выполнению лабораторных работ № 1 – 3 для студентов специальности 10.05.03 «Информационная безопасность автоматизированных систем» очной формы обучения и методическими указаниями к выполнению лабораторных работ № 4-5 для студентов специальности 10.05.03 «Информационная безопасность автоматизированных систем».

8 УЧЕБНО МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ)

8.1 Перечень учебной литературы, необходимой для освоения дисциплины

Основная:

1. Олифер В.Г., Олифер Н. А. Компьютерные сети. Принципы, технологии, протоколы. Учебник : учебник для вузов – 6-е изд. – СПб.: Питер, 2020 – 1008 с. ISBN 978-5-4461-1426-9.
2. Щербаков В.Б., Ермаков С.А., Коленбет Н.С. Риск-анализ атакуемых беспроводных сетей; под ред. чл.-корр. РАН Д.А. Новикова: Монография – Воронеж : Издательство «Научная книга», 2013 – 160 с. ISBN 978-5-98222-847-5.
3. Щербаков В.Б., Ермаков С.А. Безопасность беспроводных сетей: стандарт IEEE 802.11; под ред. В.И. Борисова. – М. : Радио-Софт, 2010. – 256 с. ISBN 978-5-93274-020-0.

Дополнительная:

1. Зараменских Е.П., Артемьев И.Е. Интернет вещей. Исследования и область применения [Электронный ресурс]: Монография / М.: НИЦ ИНФРА-М, 2015. – 200 с. Режим доступа: http://znanium.com/catalog.php?bookinfo=526946
2. Росляков А.В., Ваняшин С.В., Гребешков А.Ю. Интернет вещей: учебное пособие – Самара: ПГУТИ, 2015 – 200с.

Методические разработки:

1. Беспроводные системы связи и их безопасность: методические указания к выполнению лабораторных работ № 1 - 3 для студентов специальности 10.05.02 «Информационная безопасность телекоммуникационных систем» очной формы обучения / ФГБОУ ВПО «Воронежский государственный технический университет»; сост.: С. А. Ермаков. Воронеж, 2021. 38 с.
2. Беспроводные системы связи и их безопасность: методические указания к выполнению лабораторных работ № 4-5 для студентов специальности 10.05.02 «Информационная безопасность телекоммуникационных систем» очной формы обучения / ФГБОУ ВО «Воронежский государственный технический университет»; сост.: С. А. Ермаков. Воронеж: Изд-во ВГТУ, 2021. 29 с.

8.2 Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень лицензионного программного обеспечения, ресурсов информационно-телекоммуникационной сети «Интернет», современных профессиональных баз данных и информационных справочных систем:

http://eios.vorstu.ru/
http://www.studentlibrary.ru/

http://znanium.com/
http://e.lanbook.com/
http://www.iprbookshop.ru/
http://www.kit-e.ru/
GNU Octave – свободная система для математических вычислений
Mathworks Matlab&Simulink – среда технических вычислений/визуального имитационного моделирования

9 МАТЕРИАЛЬНО-ТЕХНИЧЕСКАЯ БАЗА, НЕОБХОДИМАЯ ДЛЯ ОСУЩЕСТВЛЕНИЯ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА

Специализированная лекционная аудитория, оснащенная оборудованием для лекционных демонстраций и проекционной аппаратурой.

Дисплейный класс, оснащенный компьютерными программами для проведения лабораторных занятий.

10. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ (МОДУЛЯ)

По дисциплине «Безопасность информационных систем и сетей интернета вещей» читаются лекции, проводятся лабораторные работы.

Основой изучения дисциплины являются лекции, на которых излагаются наиболее существенные и трудные вопросы, а также вопросы, не нашедшие отражения в учебной литературе.

Лабораторные работы выполняются на лабораторном оборудовании в соответствии с методиками, приведенными в указаниях к выполнению работ.

Вид учебных занятий	Деятельность студента
Лекция	Написание конспекта лекций: кратко, схематично, последовательно фиксировать основные положения, выводы, формулировки, обобщения; помечать важные мысли, выделять ключевые слова, термины. Проверка терминов, понятий с помощью энциклопедий, словарей, справочников с выписыванием толкований в тетрадь. Обозначение вопросов, терминов, материала, которые вызывают трудности, поиск ответов в рекомендуемой литературе. Если самостоятельно не удается разобраться в материале, необходимо сформулировать вопрос и задать преподавателю на лекции или на практическом занятии.
Лабораторная работа	Лабораторные работы позволяют научиться применять теоретические знания, полученные на лекции при решении конкретных задач. Чтобы наиболее рационально и полно использовать все возможности лабораторных для подготовки к ним необходимо: следует разобрать лекцию по соответствующей теме, ознакомится с соответствующим разделом учебника, проработать дополнительную литературу и источники, решить задачи и выполнить другие письменные задания.
Самостоятельная работа	Самостоятельная работа студентов способствует глубокому

	усвоения учебного материала и развитию навыков самообразования. Самостоятельная работа предполагает следующие составляющие: - работа с текстами: учебниками, справочниками, дополнительной литературой, а также проработка конспектов лекций; - выполнение домашних заданий и расчетов; - работа над темами для самостоятельного изучения; - участие в работе студенческих научных конференций, олимпиад; - подготовка к промежуточной аттестации.
Подготовка к промежуточной аттестации	Готовиться к промежуточной аттестации следует систематически, в течение всего семестра. Интенсивная подготовка должна начаться не позднее, чем за месяц-полтора до промежуточной аттестации. Данные перед зачетом с оценкой три дня эффективнее всего использовать для повторения и систематизации материала.

ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ

№ п/п	Перечень вносимых изменений	Дата внесения изменений	Подпись заведующего кафедрой, ответственной за реализацию ОПОП
1			