

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
**ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
"РЯЗАНСКИЙ ГОСУДАРСТВЕННЫЙ РАДИОТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ
ИМЕНИ В.Ф. УТКИНА"**

СОГЛАСОВАНО
Зав. выпускающей кафедры

УТВЕРЖДАЮ

**Защита информации в автоматизированных
системах специального назначения
рабочая программа дисциплины (модуля)**

Закреплена за кафедрой	Вычислительной и прикладной математики
Учебный план	09.05.01_24_00.plx 09.05.01 Применение и эксплуатация автоматизированных систем специального назначения
Квалификация	инженер
Форма обучения	очная
Общая трудоемкость	6 ЗЕТ

Распределение часов дисциплины по семестрам

Семестр (<Курс>.<Семестр на курсе>)	9 (5.1)		Итого	
Неделя	16			
Вид занятий	УП	РП	УП	РП
Лекции	32	32	32	32
Лабораторные	32	32	32	32
Практические	32	32	32	32
Иная контактная работа	0,35	0,35	0,35	0,35
Консультирование перед экзаменом и практикой	2	2	2	2
Итого ауд.	98,35	98,35	98,35	98,35
Контактная работа	98,35	98,35	98,35	98,35
Сам. работа	64	64	64	64
Часы на контроль	53,65	53,65	53,65	53,65
Итого	216	216	216	216

г. Рязань

Программу составил(и):

к.т.н., доц., Швечкова Ольга Григорьевна

Рабочая программа дисциплины

Защита информации в автоматизированных системах специального назначения

разработана в соответствии с ФГОС ВО:

ФГОС ВО - специалитет по специальности 09.05.01 Применение и эксплуатация автоматизированных систем специального назначения (приказ Минобрнауки России от 02.04.2020 г. № 541дсп)

составлена на основании учебного плана:

09.05.01 Применение и эксплуатация автоматизированных систем специального назначения

утвержденного учёным советом вуза от 26.01.2024 протокол № 8.

Рабочая программа одобрена на заседании кафедры

Вычислительной и прикладной математики

Протокол от 19.06.2024 г. № 10

Срок действия программы: 2024-2028 уч.г.

Зав. кафедрой Овечкин Геннадий Владимирович

Визирование РПД для исполнения в очередном учебном году

Рабочая программа пересмотрена, обсуждена и одобрена для
исполнения в 2025-2026 учебном году на заседании кафедры
Вычислительной и прикладной математики

Протокол от ____ 2025 г. № ____

Зав. кафедрой _____

Визирование РПД для исполнения в очередном учебном году

Рабочая программа пересмотрена, обсуждена и одобрена для
исполнения в 2026-2027 учебном году на заседании кафедры
Вычислительной и прикладной математики

Протокол от ____ 2026 г. № ____

Зав. кафедрой _____

Визирование РПД для исполнения в очередном учебном году

Рабочая программа пересмотрена, обсуждена и одобрена для
исполнения в 2027-2028 учебном году на заседании кафедры
Вычислительной и прикладной математики

Протокол от ____ 2027 г. № ____

Зав. кафедрой _____

Визирование РПД для исполнения в очередном учебном году

Рабочая программа пересмотрена, обсуждена и одобрена для
исполнения в 2028-2029 учебном году на заседании кафедры

Вычислительной и прикладной математики

Протокол от ____ 2028 г. № ____

Зав. кафедрой _____

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)

1.1	Целью освоения дисциплины является приобретение базовых знаний и умений в соответствии с Федеральным государственным образовательным стандартом в сфере обеспечения безопасности информации и автоматизированных систем на базе современных информационных технологий, посредством обеспечения этапов формирования компетенций, предусмотренных ФГОС, в части представленных ниже знаний, умений и навыков.
1.2	Задачи:
1.3	• Изучение проблем защиты информации и поддерживающей ее инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, которые могут нанести ущерб владельцам или пользователям информации.
1.4	• Изучение угроз безопасности и ресурсам, причин и условий, способствующих нанесению финансового, материального и морального ущерба его интересам.
1.5	• Изучение механизмов и условий оперативного реагирования на угрозы безопасности и проявлению негативных тенденций в функционировании предприятия;
1.6	• Освоение основных методов и приемов построения защищенных автоматизированных систем, использования программных методов защиты информации. Использование современных алгоритмов криптографической защиты и механизмов цифровой подписи для реализации защищенного электронного документооборота.

2. МЕСТО ДИСЦИПЛИНЫ (МОДУЛЯ) В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Цикл (раздел) ОП:	
2.1	Требования к предварительной подготовке обучающегося:
2.1.1	Метрология, стандартизация и сертификация
2.1.2	Программирование специализированных вычислительных устройств
2.1.3	Технологическая (проектно-технологическая) практика
2.1.4	Архитектура промышленных автоматизированных систем
2.1.5	Корпоративные информационные системы
2.1.6	Надежность автоматизированных систем
2.1.7	Облачные вычисления
2.1.8	Предметно-ориентированные автоматизированные информационные системы
2.1.9	Системы цифровой обработки сигналов
2.1.10	Администрирование автоматизированных систем специального назначения
2.1.11	Компьютерная графика
2.1.12	Операционные системы
2.1.13	Сетевое администрирование
2.1.14	Сети и телекоммуникации
2.1.15	Администрирование в информационных системах
2.1.16	Базы данных и клиент-серверные приложения
2.1.17	Разработка и анализ требований к автоматизированным системам специального назначения
2.1.18	Организация ЭВМ, вычислительных комплексов и систем
2.1.19	Автоматизированные системы специального назначения
2.1.20	Алгоритмы и структуры данных
2.1.21	Машино-зависимые языки программирования
2.1.22	Инженерная графика
2.1.23	Ознакомительная практика
2.1.24	Учебная практика
2.1.25	Информатика
2.1.26	Информационные технологии
2.1.27	Архитектура промышленных автоматизированных систем
2.1.28	Сетевое администрирование
2.2	Дисциплины (модули) и практики, для которых освоение данной дисциплины (модуля) необходимо как предшествующее:
2.2.1	Научно-исследовательская работа
2.2.2	Подготовка к процедуре защиты и защита выпускной квалификационной работы
2.2.3	Преддипломная практика

2.2.4	Производственная практика
3. КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)	
ОПК-3: Способен применять методы поиска, хранения, обработки, анализа и представления в требуемом формате информации из различных источников и баз данных, соблюдая при этом основные требования информационной безопасности	
ОПК-3.1. Использует современные информационные технологии и программные средства при решении задач профессиональной деятельности	
Знать современные информационные технологии и программные средства при решении задач профессиональной деятельности Уметь применять современные информационные технологии и программные средства при решении задач профессиональной деятельности Владеть навыками работы с современными информационными технологиями и программными средствами при решении задач профессиональной деятельности	
ОПК-3.2. Применяет методы поиска, хранения, обработки, анализа и представления информации из различных источников и баз данных в различных форматах	
Знать Знает принципы информационной и библиографической культуры, методы и средства решения стандартных задач профессиональной деятельности с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности. Уметь Умеет решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности. Владеть Владеет методами поиска и анализа информации для подготовки документов, обзоров, рефератов, докладов, публикаций, на основе информационной и библиографической культуры, с учетом соблюдения авторского права и требований информационной безопасности данных с помощью средств вычислительной техники.	
ОПК-3.3. Соблюдает основные требования информационной безопасности при поиске, хранении, обработке, анализе и представлении информации из различных источников и баз данных	
Знать Знает методы и средства решения стандартных задач профессиональной деятельности с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности. Уметь Уметь решать стандартные задачи профессиональной деятельности с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности. Владеть Владеет методами поиска информации и приемами организации электронного документооборота на основе новых информационных технологий, с учетом соблюдения авторского права и требований информационной безопасности с помощью средств вычислительной техники.	
ОПК-4: Способен применять современные информационно коммуникационные технологии для подготовки текстовой и конструкторско-технологической документации с учетом требований нормативных документов в своей профессиональной деятельности	
ОПК-4.1. Учитывает основные требования стандартов при оформлении технической документации в сфере профессиональной деятельности	
Знать основные требования стандартов при оформлении технической документации в сфере профессиональной деятельности Уметь применять основные требования стандартов при оформлении технической документации в сфере профессиональной деятельности Владеть навыками применения основных требований стандартов при оформлении технической документации в сфере профессиональной деятельности	
ПК-1: Способен выполнять постановку задач, обосновывать технические условия и задания на проектирование автоматизированных систем с учетом требований к автоматизированным системам специального назначения	
ПК-1.1. Выявляет и определяет требования к автоматизированным системам специального назначения и возможностей их реализации, формулирует цель и ставит задачи проектирования	

Знать

требования к автоматизированным системам специального назначения и возможностей их реализации, цели и задачи проектирования

Уметь

выявлять и определять требования к автоматизированным системам специального назначения и возможностей их реализации, формулировать цель и ставить задачи проектирования

Владеть

навыками определения цели и задачи проектирования

В результате освоения дисциплины (модуля) обучающийся должен

3.1	Знать:
3.1.1	Основные понятия базовых разделов высшей математики, дискретной математики, информатики, теории вероятности.
3.1.2	Принципы, приемы, методы объектно-ориентированного программирования, основы современных информационных технологий.
3.2	Уметь:
3.2.1	Применять свои знания при решении различных предметных задач.
3.2.2	Уметь работать в средах программирования, ориентированных на соответствующие предметные области, разрабатывать и использовать специализированные программные средства.
3.3	Владеть:
3.3.1	Иметь навыки применения математических методов и проектирования алгоритмов, обладать знаниями в области архитектуры информационных систем.
3.3.2	Иметь опыт применения методов и приемов разработки и использования специализированных программных средств.

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Код занятия	Наименование разделов и тем /вид занятия/	Семестр / Курс	Часов	Компетенции	Литература	Форма контроля
	Раздел 1. Базовые понятия области защиты информации и безопасности автоматизированных систем.					
1.1	Проблема информационной безопасности общества. Основные термины и определения данной предметной области. Задачи по защите информации и автоматизированных систем. Уровни формирования режима информационной безопасности. Обзор нормативно-правовых документов в области защиты информации. Государственные стандарты РФ – руководящие документы Гостехкомиссии России по защите информации. /Тема/	9	0			
1.2	Основные понятия защиты информации. /Лек/	9	4	ОПК-3.1-3 ОПК-3.1-У ОПК-3.1-В ОПК-3.2-3 ОПК-3.2-У ОПК-3.2-В ОПК-3.3-3 ОПК-3.3-У ОПК-3.3-В ОПК-4.1-3 ОПК-4.1-У ОПК-4.1-В ПК-1.1-3 ПК-1.1-У ПК-1.1-В	Л1.1 Л1.3 Л1.2Л2.2 Л2.1Л3.5 Л3.4 Л3.6 Л3.2 Л3.3 Л3.1	Экзамен

1.3	Изучение понятия «информационная безопасность» в различных контекстах. Закон РФ «Об участии в международном информационном обмене». Доктрина информационной безопасности Российской Федерации. Понятие защиты информации как комплекса мероприятий, направленных на обеспечение информационной безопасности. Изучение законодательных актов РФ в области защиты информации и автоматизированных систем от разрушающих программных средств. Изучение различных видов разрушающих программных средств. /Пр/	9	4	ОПК-3.1-З ОПК-3.1-У ОПК-3.1-В ОПК-3.2-З ОПК-3.2-У ОПК-3.2-В ОПК-3.3-З ОПК-3.3-У ОПК-3.3-В ОПК-4.1-З ОПК-4.1-У ОПК-4.1-В ПК-1.1-З ПК-1.1-У ПК-1.1-В	Л1.1 Л1.3 Л1.2Л2.2 Л2.1Л3.5 Л3.4 Л3.6 Л3.2 Л3.3 Л3.1	Защита практической работы
1.4	Проблемы защиты информации для открытых автоматизированных систем. Характеристики, влияющие на безопасность информации. /Ср/	9	6	ОПК-3.1-З ОПК-3.1-У ОПК-3.1-В ОПК-3.2-З ОПК-3.2-У ОПК-3.2-В ОПК-3.3-З ОПК-3.3-У ОПК-3.3-В ОПК-4.1-З ОПК-4.1-У ОПК-4.1-В ПК-1.1-З ПК-1.1-У ПК-1.1-В	Л1.1 Л1.3 Л1.2Л2.2 Л2.1Л3.5 Л3.4 Л3.6 Л3.2 Л3.3 Л3.1	Экзамен
	Раздел 2. Угрозы информационной безопасности					
2.1	Исследование причин нарушения безопасности. Понятие угрозы информационной безопасности. Классификация угроз по различным классификационным признакам. Понятие уязвимости информации. Современные виды угроз. Понятие, виды, классификация, этапы реализации типовых сетевых атак. Технические каналы утечки информации, каналы ПЭМИН. Каналы несанкционированного доступа к информации(НСД). /Тема/	9	0			
2.2	Исследование причин нарушения безопасности. Понятие угрозы информационной безопасности. Классификация угроз по различным классификационным признакам. Понятие уязвимости информации. Современные виды угроз. Понятие, виды, классификация, этапы реализации типовых сетевых атак. Технические каналы утечки информации. Каналы несанкционированного доступа к информации. /Лек/	9	4	ОПК-3.1-З ОПК-3.1-У ОПК-3.1-В ОПК-3.2-З ОПК-3.2-У ОПК-3.2-В ОПК-3.3-З ОПК-3.3-У ОПК-3.3-В ОПК-4.1-З ОПК-4.1-У ОПК-4.1-В ПК-1.1-З ПК-1.1-У ПК-1.1-В	Л1.1 Л1.3 Л1.2Л2.2 Л2.1Л3.5 Л3.4 Л3.6 Л3.2 Л3.3 Л3.1	Экзамен

2.3	Построение сценария функционирования компьютерной системы в среде реально существующих угроз с учетом ролей всех участников процесса обработки и потребления информации позволяет определить механизмы построения защищенной системы обработки информации и свести к минимуму ущерб от возможных нарушений. /Пр/	9	4	ОПК-3.1-З ОПК-3.1-У ОПК-3.1-В ОПК-3.2-З ОПК-3.2-У ОПК-3.2-В ОПК-3.3-З ОПК-3.3-У ОПК-3.3-В ОПК-4.1-З ОПК-4.1-У ОПК-4.1-В ПК-1.1-З ПК-1.1-У ПК-1.1-В	Л1.1 Л1.3 Л1.2Л2.2 Л2.1Л3.5 Л3.4 Л3.6 Л3.2 Л3.3 Л3.1	Защита практической работы
2.4	Возможности сети Интернет и проблемы безопасности. Угрозы и уязвимости корпоративных сетей и систем. /Ср/	9	6	ОПК-3.1-З ОПК-3.1-У ОПК-3.1-В ОПК-3.2-З ОПК-3.2-У ОПК-3.2-В ОПК-3.3-З ОПК-3.3-У ОПК-3.3-В ОПК-4.1-З ОПК-4.1-У ОПК-4.1-В ПК-1.1-З ПК-1.1-У ПК-1.1-В	Л1.1 Л1.3 Л1.2Л2.2 Л2.1Л3.5 Л3.4 Л3.6 Л3.2 Л3.3 Л3.1	Экзамен
	Раздел 3. Общие подходы к проблеме защиты информации. Основные методы и средства защиты безопасности					
3.1	Оценка рисков в сфере информационной безопасности. Основные методы средства, механизмы защиты информации. /Тема/	9	0			
3.2	Оценка рисков в сфере информационной безопасности. Основные методы средства, механизмы защиты информации. /Лек/	9	4	ОПК-3.1-З ОПК-3.1-У ОПК-3.1-В ОПК-3.2-З ОПК-3.2-У ОПК-3.2-В ОПК-3.3-З ОПК-3.3-У ОПК-3.3-В ОПК-4.1-З ОПК-4.1-У ОПК-4.1-В ПК-1.1-З ПК-1.1-У ПК-1.1-В	Л1.1 Л1.3 Л1.2Л2.2 Л2.1Л3.5 Л3.4 Л3.6 Л3.2 Л3.3 Л3.1	Экзамен
3.3	Методы контроля, обеспечения достоверности и защиты информационного и программного обеспечения автоматизированных систем. Защита от разрушающих программных средств. /Лаб/	9	4	ОПК-3.1-З ОПК-3.1-У ОПК-3.1-В ОПК-3.2-З ОПК-3.2-У ОПК-3.2-В ОПК-3.3-З ОПК-3.3-У ОПК-3.3-В ОПК-4.1-З ОПК-4.1-У ОПК-4.1-В ПК-1.1-З ПК-1.1-У ПК-1.1-В	Л1.1 Л1.3 Л1.2Л2.2 Л2.1Л3.5 Л3.4 Л3.6 Л3.2 Л3.3 Л3.1	Защита лабораторной работы

3.4	Изучение законодательных актов РФ в области защиты информации и автоматизированных систем от разрушающих программных средств. Изучение различных видов разрушающих программных средств. /Пр/	9	4	ОПК-3.1-З ОПК-3.1-У ОПК-3.1-В ОПК-3.2-З ОПК-3.2-У ОПК-3.2-В ОПК-3.3-З ОПК-3.3-У ОПК-3.3-В ОПК-4.1-З ОПК-4.1-У ОПК-4.1-В ПК-1.1-З ПК-1.1-У ПК-1.1-В	Л1.1 Л1.3 Л1.2Л2.2 Л2.1Л3.5 Л3.4 Л3.6 Л3.2 Л3.3 Л3.1	Защита практической работы
3.5	Политика безопасности в сетях. Технологии безопасности данных. /Ср/	9	6	ОПК-3.1-З ОПК-3.1-У ОПК-3.1-В ОПК-3.2-З ОПК-3.2-У ОПК-3.2-В ОПК-3.3-З ОПК-3.3-У ОПК-3.3-В ОПК-4.1-З ОПК-4.1-У ОПК-4.1-В ПК-1.1-З ПК-1.1-У ПК-1.1-В	Л1.1 Л1.3 Л1.2Л2.2 Л2.1Л3.5 Л3.4 Л3.6 Л3.2 Л3.3 Л3.1	Экзамен
	Раздел 4. Основные понятия теории защиты информации					
4.1	Теоретические основы информационной безопасности. Понятия «объект», «субъект», «сущность», «процесс». Понятие модели безопасности. Виды моделей безопасности в зависимости от реализуемых функций защиты. Понятие политики безопасности. Мандатная, дискреционная, ролевая политики безопасности. /Тема/	9	0			
4.2	Теоретические основы информационной безопасности. Понятия «объект», «субъект», «сущность», «процесс». Понятие модели безопасности. Виды моделей безопасности в зависимости от реализуемых функций защиты. Понятие политики безопасности. Мандатная, дискреционная, ролевая политики безопасности. /Лек/	9	4	ОПК-3.1-З ОПК-3.1-У ОПК-3.1-В ОПК-3.2-З ОПК-3.2-У ОПК-3.2-В ОПК-3.3-З ОПК-3.3-У ОПК-3.3-В ОПК-4.1-З ОПК-4.1-У ОПК-4.1-В ПК-1.1-З ПК-1.1-У ПК-1.1-В	Л1.1 Л1.3 Л1.2Л2.2 Л2.1Л3.5 Л3.4 Л3.6 Л3.2 Л3.3 Л3.1	Экзамен

4.3	Системно-концептуальный подход при решении задачи защиты информации в КС. Сущность концептуального подхода. Обеспечение безопасности данных. Критерии безопасности данных. Основные функции обеспечения безопасности данных. Принципы создания систем информационной безопасности. /Пр/	9	4	ОПК-3.1-З ОПК-3.1-У ОПК-3.1-В ОПК-3.2-З ОПК-3.2-У ОПК-3.2-В ОПК-3.3-З ОПК-3.3-У ОПК-3.3-В ОПК-4.1-З ОПК-4.1-У ОПК-4.1-В ПК-1.1-З ПК-1.1-У ПК-1.1-В	Л1.1 Л1.3 Л1.2Л2.2 Л2.1Л3.5 Л3.4 Л3.6 Л3.2 Л3.3 Л3.1	Защита практической работы
4.4	Типовые решения по применению межсетевых экранов для защиты информационных ресурсов. /Ср/	9	6	ОПК-3.1-З ОПК-3.1-У ОПК-3.1-В ОПК-3.2-З ОПК-3.2-У ОПК-3.2-В ОПК-3.3-З ОПК-3.3-У ОПК-3.3-В ОПК-4.1-З ОПК-4.1-У ОПК-4.1-В ПК-1.1-З ПК-1.1-У ПК-1.1-В	Л1.1 Л1.3 Л1.2Л2.2 Л2.1Л3.5 Л3.4 Л3.6 Л3.2 Л3.3 Л3.1	Экзамен
	Раздел 5. Понятие информационного сервиса безопасности					
5.1	Обзор проблем безопасности наиболее популярных Internet-сервисов. Задачи обеспечения информационной безопасности сетей. Комплексный подход к реализации основных функциональных компонентов безопасности сетевых систем обработки информации с использованием методов и средств криптографии, механизмов аутентификации и авторизации, антивирусных средств, межсетевого экранирования. /Тема/	9	0			
5.2	Обзор проблем безопасности наиболее популярных Internet-сервисов. Задачи обеспечения информационной безопасности сетей. Комплексный подход к реализации основных функциональных компонентов безопасности сетевых систем обработки информации с использованием методов и средств криптографии, механизмов аутентификации и авторизации, антивирусных средств, межсетевого экранирования. /Лек/	9	2	ОПК-3.1-З ОПК-3.1-У ОПК-3.1-В ОПК-3.2-З ОПК-3.2-У ОПК-3.2-В ОПК-3.3-З ОПК-3.3-У ОПК-3.3-В ОПК-4.1-З ОПК-4.1-У ОПК-4.1-В ПК-1.1-З ПК-1.1-У ПК-1.1-В	Л1.1 Л1.3 Л1.2Л2.2 Л2.1Л3.5 Л3.4 Л3.6 Л3.2 Л3.3 Л3.1	Экзамен

5.3	Шифры перестановки, замены, гаммирования /Лаб/	9	2	ОПК-3.1-З ОПК-3.1-У ОПК-3.1-В ОПК-3.2-З ОПК-3.2-У ОПК-3.2-В ОПК-3.3-З ОПК-3.3-У ОПК-3.3-В ОПК-4.1-З ОПК-4.1-У ОПК-4.1-В ПК-1.1-З ПК-1.1-У ПК-1.1-В	Л1.1 Л1.3 Л1.2Л2.2 Л2.1Л3.5 Л3.4 Л3.6 Л3.2 Л3.3 Л3.1	Защита лабораторной работы
5.4	Методы управления средствами сетевой безопасности /Ср/	9	6	ОПК-3.1-З ОПК-3.1-У ОПК-3.1-В ОПК-3.2-З ОПК-3.2-У ОПК-3.2-В ОПК-3.3-З ОПК-3.3-У ОПК-3.3-В ОПК-4.1-З ОПК-4.1-У ОПК-4.1-В ПК-1.1-З ПК-1.1-У ПК-1.1-В	Л1.1 Л1.3 Л1.2Л2.2 Л2.1Л3.5 Л3.4 Л3.6 Л3.2 Л3.3 Л3.1	Экзамен
	Раздел 6. Защита интернет–подключений.					
6.1	Функции и назначение межсетевых экранов. Требования к межсетевым экранам. Классификация межсетевых экранов. Механизмы построения виртуальных защищенных сетей (VPN-технологии). /Тема/	9	0			
6.2	Функции и назначение межсетевых экранов. Требования к межсетевым экранам. Классификация межсетевых экранов. Механизмы построения виртуальных защищенных сетей (VPN-технологии). /Лек/	9	4	ОПК-3.1-З ОПК-3.1-У ОПК-3.1-В ОПК-3.2-З ОПК-3.2-У ОПК-3.2-В ОПК-3.3-З ОПК-3.3-У ОПК-3.3-В ОПК-4.1-З ОПК-4.1-У ОПК-4.1-В ПК-1.1-З ПК-1.1-У ПК-1.1-В	Л1.1 Л1.3 Л1.2Л2.2 Л2.1Л3.5 Л3.4 Л3.6 Л3.2 Л3.3 Л3.1	Экзамен
6.3	Системы с открытым ключом. Алгоритм RSA. Схема шифрования Полига – Хеллмана. /Лаб/	9	8	ОПК-3.1-З ОПК-3.1-У ОПК-3.1-В ОПК-3.2-З ОПК-3.2-У ОПК-3.2-В ОПК-3.3-З ОПК-3.3-У ОПК-3.3-В ОПК-4.1-З ОПК-4.1-У ОПК-4.1-В ПК-1.1-З ПК-1.1-У ПК-1.1-В	Л1.1 Л1.3 Л1.2Л2.2 Л2.1Л3.5 Л3.4 Л3.6 Л3.2 Л3.3 Л3.1	Защита лабораторной работы

6.4	Типовые решения по применению межсетевых экранов для защиты информационных ресурсов /Ср/	9	11	ОПК-3.1-З ОПК-3.1-У ОПК-3.1-В ОПК-3.2-З ОПК-3.2-У ОПК-3.2-В ОПК-3.3-З ОПК-3.3-У ОПК-3.3-В ОПК-4.1-З ОПК-4.1-У ОПК-4.1-В ПК-1.1-З ПК-1.1-У ПК-1.1-В	Л1.1 Л1.3 Л1.2Л2.2 Л2.1Л3.5 Л3.4 Л3.6 Л3.2 Л3.3 Л3.1	Экзамен
	Раздел 7. Разрушающие программные средства. Вирусы, троянские программы					
7.1	Вредоносные программы как угроза информационной безопасности. Хронология и классификация вредоносного программного обеспечения. Антивирусные программы, особенности, качество их работы. Методы защиты от вредоносных программ. /Тема/	9	0			
7.2	Вредоносные программы как угроза информационной безопасности. Хронология и классификация вредоносного программного обеспечения. Антивирусные программы, особенности, качество их работы. Методы защиты от вредоносных программ. /Лек/	9	6	ОПК-3.1-З ОПК-3.1-У ОПК-3.1-В ОПК-3.2-З ОПК-3.2-У ОПК-3.2-В ОПК-3.3-З ОПК-3.3-У ОПК-3.3-В ОПК-4.1-З ОПК-4.1-У ОПК-4.1-В ПК-1.1-З ПК-1.1-У ПК-1.1-В	Л1.1 Л1.3 Л1.2Л2.2 Л2.1Л3.5 Л3.4 Л3.6 Л3.2 Л3.3 Л3.1	Экзамен
7.3	Схема шифрования Эль-Гамала /Лаб/	9	6	ОПК-3.1-З ОПК-3.1-У ОПК-3.1-В ОПК-3.2-З ОПК-3.2-У ОПК-3.2-В ОПК-3.3-З ОПК-3.3-У ОПК-3.3-В ОПК-4.1-З ОПК-4.1-У ОПК-4.1-В ПК-1.1-З ПК-1.1-У ПК-1.1-В	Л1.1 Л1.3 Л1.2Л2.2 Л2.1Л3.5 Л3.4 Л3.6 Л3.2 Л3.3 Л3.1	Защита лабораторной работы

7.4	Понятие компьютерного вируса. Классификация вирусов по различным признакам. Изучение алгоритмов работы резидентных вирусов, вирусов, использующих стелс-алгоритмы, полиморфичность. Анализ деструктивных, разрушительных возможностей разрушающих программных средств. Основной механизм заражения вирусом, макровирусом. Методы обнаружения макровируса. Методы обезвреживания макровируса /Пр/	9	8	ОПК-3.1-З ОПК-3.1-У ОПК-3.1-В ОПК-3.2-З ОПК-3.2-У ОПК-3.2-В ОПК-3.3-З ОПК-3.3-У ОПК-3.3-В ОПК-4.1-З ОПК-4.1-У ОПК-4.1-В ПК-1.1-З ПК-1.1-У ПК-1.1-В	Л1.1 Л1.3 Л1.2Л2.2 Л2.1Л3.5 Л3.4 Л3.6 Л3.2 Л3.3 Л3.1	Защита практической работы
7.5	Освоение приемов противодействия разрушающим программным средствам. /Ср/	9	12	ОПК-3.1-З ОПК-3.1-У ОПК-3.1-В ОПК-3.2-З ОПК-3.2-У ОПК-3.2-В ОПК-3.3-З ОПК-3.3-У ОПК-3.3-В ОПК-4.1-З ОПК-4.1-У ОПК-4.1-В ПК-1.1-З ПК-1.1-У ПК-1.1-В	Л1.1 Л1.3 Л1.2Л2.2 Л2.1Л3.5 Л3.4 Л3.6 Л3.2 Л3.3 Л3.1	Экзамен
	Раздел 8. Криптографические методы защиты информации. Электронная цифровая подпись					
8.1	Понятие криптографических методов защиты информации. Классификация криптографических методов. Простейшие шифры и их свойства. Оценка криптостойкости шифров. Системы шифрования с симметричным и открытым ключом. Современные алгоритмы шифрования. Понятие электронной цифровой подписи. Законодательные акты, регламентирующие использование электронной цифровой подписи при реализации электронного документооборота. Процедуры постановки и проверки электронной цифровой подписи. Понятие и свойства хэш-функции. Современные алгоритмы электронной цифровой подписи /Тема/	9	0			
8.2	Понятие криптографических методов защиты информации. Классификация криптографических методов. Простейшие шифры и их свойства. Оценка криптостойкости шифров. Системы шифрования с симметричным и открытым ключом. Современные алгоритмы шифрования. Понятие электронной цифровой подписи. Законодательные акты, регламентирующие использование электронной цифровой подписи при реализации электронного документооборота. Процедуры постановки и проверки электронной цифровой подписи. Понятие и свойства хэш-функции. Современные алгоритмы электронной цифровой подписи /Лек/	9	4	ОПК-3.1-З ОПК-3.1-У ОПК-3.1-В ОПК-3.2-З ОПК-3.2-У ОПК-3.2-В ОПК-3.3-З ОПК-3.3-У ОПК-3.3-В ОПК-4.1-З ОПК-4.1-У ОПК-4.1-В ПК-1.1-З ПК-1.1-У ПК-1.1-В	Л1.1 Л1.3 Л1.2Л2.2 Л2.1Л3.5 Л3.4 Л3.6 Л3.2 Л3.3 Л3.1	Экзамен

8.3	Потоковый шифр RC4. Алгоритмы электронной цифровой подписи. Схема DSA. Алгоритмы электронной цифровой подписи. Схема ГОСТ, алгоритм Шнорра. /Лаб/	9	12	ОПК-3.1-З ОПК-3.1-У ОПК-3.1-В ОПК-3.2-З ОПК-3.2-У ОПК-3.2-В ОПК-3.3-З ОПК-3.3-У ОПК-3.3-В ОПК-4.1-З ОПК-4.1-У ОПК-4.1-В ПК-1.1-З ПК-1.1-У ПК-1.1-В	Л1.1 Л1.3 Л1.2Л2.2 Л2.1Л3.5 Л3.4 Л3.6 Л3.2 Л3.3 Л3.1	Защита лабораторной работы
8.4	Основные понятия и определения электронной цифровой подписи. Основные алгоритмы электронной цифровой подписи. Виды атак на электронную цифровую подпись. Математическая и программная реализация алгоритмов электронной цифровой подписи. /Пр/	9	8	ОПК-3.1-З ОПК-3.1-У ОПК-3.1-В ОПК-3.2-З ОПК-3.2-У ОПК-3.2-В ОПК-3.3-З ОПК-3.3-У ОПК-3.3-В ОПК-4.1-З ОПК-4.1-У ОПК-4.1-В ПК-1.1-З ПК-1.1-У ПК-1.1-В	Л1.1 Л1.3 Л1.2Л2.2 Л2.1Л3.5 Л3.4 Л3.6 Л3.2 Л3.3 Л3.1	Защита практической работы
8.5	Основные понятия и определения электронной цифровой подписи. Основные алгоритмы электронной цифровой подписи. Виды атак на электронную цифровую подпись. Математическая и программная реализация алгоритмов электронной цифровой подписи. /Ср/	9	11	ОПК-3.1-З ОПК-3.1-У ОПК-3.1-В ОПК-3.2-З ОПК-3.2-У ОПК-3.2-В ОПК-3.3-З ОПК-3.3-У ОПК-3.3-В ОПК-4.1-З ОПК-4.1-У ОПК-4.1-В ПК-1.1-З ПК-1.1-У ПК-1.1-В	Л1.1 Л1.3 Л1.2Л2.2 Л2.1Л3.5 Л3.4 Л3.6 Л3.2 Л3.3 Л3.1	Экзамен
	Раздел 9. Подготовка к экзамену					
9.1	Подготовка к экзамену /Тема/	9	0			
9.2	Сдача экзамена /ИКР/	9	0,35	ОПК-3.1-З ОПК-3.1-У ОПК-3.1-В ОПК-3.2-З ОПК-3.2-У ОПК-3.2-В ОПК-3.3-З ОПК-3.3-У ОПК-3.3-В ОПК-4.1-З ОПК-4.1-У ОПК-4.1-В ПК-1.1-З ПК-1.1-У ПК-1.1-В	Л1.1 Л1.3 Л1.2Л2.2 Л2.1Л3.5 Л3.4 Л3.6 Л3.2 Л3.3 Л3.1	Экзамен

9.3	Консультация перед экзаменом /Кнс/	9	2	ОПК-3.1-З ОПК-3.1-У ОПК-3.1-В ОПК-3.2-З ОПК-3.2-У ОПК-3.2-В ОПК-3.3-З ОПК-3.3-У ОПК-3.3-В ОПК-4.1-З ОПК-4.1-У ОПК-4.1-В ПК-1.1-З ПК-1.1-У ПК-1.1-В	Л1.1 Л1.3 Л1.2Л2.2 Л2.1Л3.5 Л3.4 Л3.6 Л3.2 Л3.3 Л3.1	Экзамен
9.4	Подготовка к экзамену /Экзамен/	9	53,65	ОПК-3.1-З ОПК-3.1-У ОПК-3.1-В ОПК-3.2-З ОПК-3.2-У ОПК-3.2-В ОПК-3.3-З ОПК-3.3-У ОПК-3.3-В ОПК-4.1-З ОПК-4.1-У ОПК-4.1-В ПК-1.1-З ПК-1.1-У ПК-1.1-В	Л1.1 Л1.3 Л1.2Л2.2 Л2.1Л3.5 Л3.4 Л3.6 Л3.2 Л3.3 Л3.1	Экзамен

5. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ПО ДИСЦИПЛИНЕ (МОДУЛЮ)

Оценочные материалы приведены в приложении к рабочей программе дисциплины (см. документ «Оценочные материалы дисциплины «Защита информации в автоматизированных системах специального назначения»»)

6. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

6.1. Рекомендуемая литература

6.1.1. Основная литература

№	Авторы, составители	Заглавие	Издательство, год	Количество/название ЭБС
Л1.1	Швечкова О.Г., Бабаев С.И.	Информационная безопасность: в 2 ч.: учеб. Ч.1. Теоретические основы : Учебник	Рязань: КУРС, 2022,	, https://elib.rsreu.ru/ebs/download/3176
Л1.2	Швечкова О.Г., Бабаев С.И.	Информационная безопасность: в 2 ч.: учеб. Ч.2. Стандарты и документы : Учебник	Рязань: КУРС, 2023,	, https://elib.rsreu.ru/ebs/download/3645
Л1.3	Швечкова О.Г., Пылькин А.Н., Марчев Д.В.	Базовые криптографические алгоритмы защиты информации: учеб. пособие : Учебное пособие	Рязань: КУРС, 2023,	, https://elib.rsreu.ru/ebs/download/3643

6.1.2. Дополнительная литература

№	Авторы, составители	Заглавие	Издательство, год	Количество/название ЭБС
---	---------------------	----------	-------------------	-------------------------

№	Авторы, составители	Заглавие	Издательство, год	Количество/название ЭБС
Л2.1	Шаньгин В. Ф.	Информационная безопасность и защита информации	Саратов: Профобразование, 2019, 702 с.	978-5-4488-0070-2, http://www.iprbookshop.ru/87995.html
Л2.2	Шаньгин В. Ф.	Защита компьютерной информации. Эффективные методы и средства	Саратов: Профобразование, 2019, 543 с.	978-5-4488-0074-0, http://www.iprbookshop.ru/87992.html

6.1.3. Методические разработки

№	Авторы, составители	Заглавие	Издательство, год	Количество/название ЭБС
Л3.1	Швечкова О.Г.	Обеспечение безопасности информации собственными средствами Windows. Темы 3-4: метод. указ. к практ. работам : Методические указания	Рязань: , 2022,	, https://elib.rsreu.ru/ebs/download/3378
Л3.2	Швечкова О.Г.	Основы теории криптографических методов защиты информации: метод. указ. к лаб. и практ. работам : Методические указания	Рязань: , 2022,	, https://elib.rsreu.ru/ebs/download/3375
Л3.3	Швечкова О.Г.	Обеспечение безопасности информации собственными средствами Windows. Темы 1-2: метод. указ. к практ. работам : Методические указания	Рязань: , 2022,	, https://elib.rsreu.ru/ebs/download/3377
Л3.4	Швечкова О.Г.	Теоретические основы криптографических методов защиты информации: метод. указ. к лаб. и практ. работам : Методические указания	Рязань: , 2021,	, https://elib.rsreu.ru/ebs/download/2860
Л3.5	Швечкова О.Г.	Криптографические методы защиты информации. Шифры замены: метод. указ. к лаб. работам : Методические указания	Рязань: , 2021,	, https://elib.rsreu.ru/ebs/download/2859
Л3.6	Швечкова О.Г.	Блок оценочных средств дисциплины «Защита информации»: метод. указ. к практ. и лаб. работам : Методические указания	Рязань: , 2022,	, https://elib.rsreu.ru/ebs/download/3374

6.3 Перечень программного обеспечения и информационных справочных систем

6.3.1 Перечень лицензионного и свободно распространяемого программного обеспечения, в том числе отечественного производства

Наименование	Описание
Операционная система Windows	Коммерческая лицензия
Adobe Acrobat Reader	Свободное ПО
LibreOffice	Свободное ПО
Python	Свободное ПО
OpenOffice	Свободное ПО
Chrome	Свободное ПО
Delphi Community Edition	Свободное ПО
Интерпретатор Python	Свободное ПО
Операционная система Windows XP	Microsoft Imagine, номер подписки 700102019, бессрочно
Kaspersky Endpoint Security	Коммерческая лицензия

7Zip-Manager	Свободное ПО
Microsoft Visual Studio 12.0	Microsoft Imagine, номер подписки 700102019
6.3.2 Перечень информационных справочных систем	
6.3.2.1	Информационно-правовой портал ГАРАНТ.РУ http://www.garant.ru
6.3.2.2	Система КонсультантПлюс http://www.consultant.ru
6.3.2.3	Справочная правовая система «КонсультантПлюс» (договор об информационной поддержке №1342/455-100 от 28.10.2011 г.)

7. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)	
1	106 учебно-административный корпус. Учебная аудитория для проведения занятий лекционного и семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации 30 мест проектор BENQ 11 ПК с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду: ЦП: AMD 3411, ОЗУ: 4Гб, ПЗУ:780 Гб (4 штук); ЦП: AMD 3013, ОЗУ: 4 Гб, ПЗУ: 780 Гб (3 штук); ЦП: Intel Pentium 4 class 2659, ОЗУ: 1 Гб, ПЗУ: 50 Гб (4 штук).
2	106 учебно-административный корпус. Аудитория для самостоятельной работы 30 мест проектор BENQ 11 ПК с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду: ЦП: AMD 3411, ОЗУ: 4Гб, ПЗУ:780 Гб (4 штук); ЦП: AMD 3013, ОЗУ: 4 Гб, ПЗУ: 780 Гб (3 штук); ЦП: Intel Pentium 4 class 2659, ОЗУ: 1 Гб, ПЗУ: 50 Гб (4 штук).
3	106а учебно-административный корпус. Учебная аудитория для проведения занятий лекционного и семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации 42 мест проектор BENQ 15 ПК с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду: ЦП: 2x Intel Pentium II/III class 2126, ОЗУ: 2 Гб, ПЗУ: 74 Гб (1 шт) ЦП: Intel Pentium II/III class 3192, ОЗУ: 4 Гб, ПЗУ: 200 Гб (13 шт.) ЦП: Intel Pentium II/III class 2128, ОЗУ: 2 Гб ПЗУ: 74 Гб (1 шт.)
4	110 лабораторный корпус. Учебная аудитория для проведения учебных занятий лекционного и семинарского типа, практических занятий, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации Специализированная мебель (60 мест), доска.
5	110 учебно-административный корпус. Учебная аудитория для проведения занятий лекционного и семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации 20 мест Проектор: HITACHI CP-X400 3LCD 21 ПК с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду: ЦП: Intel Core i5-4570 ОЗУ: 8 Гб ПЗУ: 1 Тб (1 шт.)

8. МЕТОДИЧЕСКИЕ МАТЕРИАЛЫ ПО ДИСЦИПЛИНЕ (МОДУЛЮ)	
Методическое обеспечение дисциплины приведено в приложении к рабочей программе дисциплины (см. документ «Методические указания дисциплины «Защита информации в автоматизированных системах специального назначения»»)	

Оператор ЭДО ООО "Компания "Тензор"

ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ

ПОДПИСАНО
ЗАВЕДУЮЩИМ
КАФЕДРЫ**ФГБОУ ВО "РГРТУ", РГРТУ**, Овечкин Геннадий
Владимирович, Заведующий кафедрой ВПМ**03.09.24** 12:37 (MSK)

Простая подпись

ПОДПИСАНО
ЗАВЕДУЮЩИМ
ВЫПУСКАЮЩЕЙ
КАФЕДРЫ**ФГБОУ ВО "РГРТУ", РГРТУ**, Овечкин Геннадий
Владимирович, Заведующий кафедрой ВПМ**03.09.24** 12:38 (MSK)

Простая подпись

ПОДПИСАНО
НАЧАЛЬНИКОМ УРОП**ФГБОУ ВО "РГРТУ", РГРТУ**, Ерзылёва Анна
Александровна, Начальник УРОП**04.09.24** 11:07 (MSK)

Простая подпись