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

рабочая программа дисциплины (модуля)

Закреплена за кафедрой **Вычислительной и прикладной математики**

Учебный план 09.03.03_26_00.plx
09.03.03 Прикладная информатика

Квалификация **бакалавр**

Форма обучения **очная**

Общая трудоемкость **3 ЗЕТ**

Распределение часов дисциплины по семестрам

Семестр (<Курс>.<Семестр на курсе>)	**8 (4.2)**		Итого	
Недель	8			
Вид занятий	УП	РП	УП	РП
Лекции	16	16	16	16
Лабораторные	16	16	16	16
Практические	16	16	16	16
Иная контактная работа	0,25	0,25	0,25	0,25
Итого ауд.	48,25	48,25	48,25	48,25
Контактная работа	48,25	48,25	48,25	48,25
Сам. работа	51	51	51	51
Часы на контроль	8,75	8,75	8,75	8,75
Итого	108	108	108	108

г. Рязань

Программу составил(и):
к.т.н., доц., Крошилина С. В.

Рабочая программа дисциплины
Защита информации

разработана в соответствии с ФГОС ВО:
ФГОС ВО - бакалавриат по направлению подготовки 09.03.03 Прикладная информатика (приказ Минобрнауки России от 19.09.2017 г. № 922)

составлена на основании учебного плана:
09.03.03 Прикладная информатика
утвержденного учёным советом вуза от 24.04.2026 протокол № 10.

Рабочая программа одобрена на заседании кафедры
Вычислительной и прикладной математики

Протокол от 15.06.2026 г. № 7
Срок действия программы: 20262030 уч.г.
Зав. кафедрой Овечкин Геннадий Владимирович

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 _____

Визирование РПД для исполнения в очередном учебном году

Рабочая программа пересмотрена, обсуждена и одобрена для исполнения в 2029-2030 учебном году на заседании кафедры
Вычислительной и прикладной математики

Протокол от __ _____ 2029 г. № __

Зав. кафедрой _____

Визирование РПД для исполнения в очередном учебном году

Рабочая программа пересмотрена, обсуждена и одобрена для исполнения в 2030-2031 учебном году на заседании кафедры

Вычислительной и прикладной математики

Протокол от __ _____ 2030 г. № __

Зав. кафедрой _____

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)	
1.1	Целью освоения дисциплины является приобретение базовых знаний и умений в со-ответствии с Федеральным государственным образовательным стандартом в сфере обес-печения безопасности информации и информационных систем на базе современных ин-формационных 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 безопасно-сти и проявлению негативных тенденций в функционировании предприятия;
1.6	• Освоение основных методов и приемов построения защищенных информационных 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:	Б1.О
2.1	**Требования к предварительной подготовке обучающегося:**
2.1.1	Информатика
2.2	**Дисциплины (модули) и практики, для которых освоение данной дисциплины (модуля) необходимо как предшествующее:**
2.2.1	Выполнение и защита выпускной квалификационной работы

3. КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)

ОПК-3: Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности

ОПК-3.2. Понимает основные требования информационной безопасности

Знать
принципы информационной и библиографической куль-туры, методы и средства решения стандартных задач профес-сиональной деятельности с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.
Уметь
решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.
Владеть
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. Решает задачи профессиональной деятельности с применением информационно-коммуникационных технологий с учетом основных требований информационной безопасности

Знать
методы и средства решения стандартных задач профессиональной деятельности с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.
Уметь
решать стандартные задачи профессиональной деятельности с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.
Владеть
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.

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	Работать в средах программирования, ориентированных на соответствующие предметные области, разрабатывать и использовать специализированные программные средства.
3.3	**Владеть:**
3.3.1	Навыками применения математических методов и проектирования алгоритмов, обладать знаниями в области архитектуры информационных систем.
3.3.2	Навыками 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	Компетен-ции	Литература	Форма контроля
	Раздел 1. Базовые понятия области защиты информации и безопасности информационных систем.					
1.1	Проблема информационной безопасности общества. Основные термины и определения данной предметной области. Задачи по защите информации и информационных 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/	8	0			
1.2	Основные понятия защиты информации. /Лек/	8	2	ОПК-3.2-З ОПК-3.2-У ОПК-3.2-В ОПК-3.3-З ОПК-3.3-У ОПК-3.3-В	Л1.1 Л1.3 Л1.2Л2.1 Л2.8 Л2.2 Л2.3 Л2.4 Л2.6 Л2.9 Л2.10 Л2.5 Л2.11 Л2.7Л3.4 Л3.6 Л3.7 Л3.8 Л3.9 Л3.10 Л3.1 Л3.2 Л3.11 Л3.3 Л3.5 Э1 Э2	Зачет
1.3	Изучение понятия «информационная безопасность» в различных контекстах. Закон РФ «Об участии в международном ин-формационном обмене». Доктрина информационной безопасности Российской Федерации. По-нятие защиты информации как комплекса мероприятий, направленных на обеспечение информационной безопасности. Изучение законодательных ак-тов РФ в области защиты ин-формации и информационных систем от разрушающих про-граммных средств. Изучение различных видов разрушающих программных средств. /Пр/	8	2	ОПК-3.2-З ОПК-3.2-У ОПК-3.2-В ОПК-3.3-З ОПК-3.3-У ОПК-3.3-В	Л1.1 Л1.3 Л1.2Л2.1 Л2.8 Л2.2 Л2.3 Л2.4 Л2.6 Л2.9 Л2.10 Л2.5 Л2.11 Л2.7Л3.4 Л3.6 Л3.7 Л3.8 Л3.9 Л3.10 Л3.1 Л3.2 Л3.11 Л3.3 Л3.5 Э1 Э2	Зачет

1.4	Проблемы защиты информации для открытых информационных систем. Характеристики, влияющие на безопасность информации. /Ср/	8	6	ОПК-3.2-З ОПК-3.2-У ОПК-3.2-В ОПК-3.3-З ОПК-3.3-У ОПК-3.3-В	Л1.1 Л1.3 Л1.2Л2.1 Л2.8 Л2.2 Л2.3 Л2.4 Л2.6 Л2.9 Л2.10 Л2.5 Л2.11 Л2.7Л3.4 Л3.6 Л3.7 Л3.8 Л3.9 Л3.10 Л3.1 Л3.2 Л3.11 Л3.3 Л3.5 Э1 Э2	Зачет
	Раздел 2. Угрозы информационной безопасности					
2.1	Исследование причин нарушения безопасности. Понятие угрозы информационной безопасности. Классификация угроз по различным классифиационным признакам. Понятие уязвимости информации. Современные виды угроз. Понятие, виды, классификация, этапы реализации типовых сетевых атак. Технические каналы утечки информации. Каналы несанкционированного доступа к информации. /Тема/	8	0			
2.2	Исследование причин нарушения безопасности. Понятие угрозы информационной без-опасности. Классификация угроз по различным классифи-кационным признакам. Поня-тие уязвимости информации. Современные виды угроз. Понятие, виды, классификация, этапы реализации типовых сетевых атак. Технические каналы утечки информации. Каналы несанкционированного доступа к информации. /Лек/	8	2	ОПК-3.2-З ОПК-3.2-У ОПК-3.2-В ОПК-3.3-З ОПК-3.3-У ОПК-3.3-В	Л1.1 Л1.3 Л1.2Л2.1 Л2.8 Л2.2 Л2.3 Л2.4 Л2.6 Л2.9 Л2.10 Л2.5 Л2.11 Л2.7Л3.4 Л3.6 Л3.7 Л3.8 Л3.9 Л3.10 Л3.1 Л3.2 Л3.11 Л3.3 Л3.5 Э1 Э2	Зачет
2.3	Построение сценария функцио-нирования компьютерной си-стемы в среде реально суще-ствующих 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/	8	2	ОПК-3.2-З ОПК-3.2-У ОПК-3.2-В ОПК-3.3-З ОПК-3.3-У ОПК-3.3-В	Л1.1 Л1.3 Л1.2Л2.1 Л2.8 Л2.2 Л2.3 Л2.4 Л2.6 Л2.9 Л2.10 Л2.5 Л2.11 Л2.7Л3.4 Л3.6 Л3.7 Л3.8 Л3.9 Л3.10 Л3.1 Л3.2 Л3.11 Л3.3 Л3.5 Э1 Э2	Зачет

2.4	Возможности сети Интернет и проблемы безопасности. Угрозы и уязвимости корпоративных сетей и систем. /Ср/	8	6	ОПК-3.2-З ОПК-3.2-У ОПК-3.2-В ОПК-3.3-З ОПК-3.3-У ОПК-3.3-В	Л1.1 Л1.3 Л1.2Л2.1 Л2.8 Л2.2 Л2.3 Л2.4 Л2.6 Л2.9 Л2.10 Л2.5 Л2.11 Л2.7Л3.4 Л3.6 Л3.7 Л3.8 Л3.9 Л3.10 Л3.1 Л3.2 Л3.11 Л3.3 Л3.5 Э1 Э2	Зачет
	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/	8	0			
3.2	Оценка рисков в сфере информационной безопасности. Основные методы средства, меха- низмы защиты информации. /Лек/	8	2	ОПК-3.2-З ОПК-3.2-У ОПК-3.2-В ОПК-3.3-З ОПК-3.3-У ОПК-3.3-В	Л1.1 Л1.3 Л1.2Л2.1 Л2.8 Л2.2 Л2.3 Л2.4 Л2.6 Л2.9 Л2.10 Л2.5 Л2.11 Л2.7Л3.4 Л3.6 Л3.7 Л3.8 Л3.9 Л3.10 Л3.1 Л3.2 Л3.11 Л3.3 Л3.5 Э1 Э2	Зачет
3.3	Методы контроля, обеспечения достоверности и защиты ин-формационного и программного обеспечения. Защита от разрушающих программных средств. /Лаб/	8	2	ОПК-3.2-З ОПК-3.2-У ОПК-3.2-В ОПК-3.3-З ОПК-3.3-У ОПК-3.3-В	Л1.1 Л1.3 Л1.2Л2.1 Л2.8 Л2.2 Л2.3 Л2.4 Л2.6 Л2.9 Л2.10 Л2.5 Л2.11 Л2.7Л3.4 Л3.6 Л3.7 Л3.8 Л3.9 Л3.10 Л3.1 Л3.2 Л3.11 Л3.3 Л3.5 Э1 Э2	Зачет
3.4	Изучение законодательных актов РФ в области защиты ин-формации и информационных систем от разрушающих про-граммных средств. Изучение различных видов разрушающих программных средств. /Пр/	8	2	ОПК-3.2-З ОПК-3.2-У ОПК-3.2-В ОПК-3.3-З ОПК-3.3-У ОПК-3.3-В	Л1.1 Л1.3 Л1.2Л2.1 Л2.8 Л2.2 Л2.3 Л2.4 Л2.6 Л2.9 Л2.10 Л2.5 Л2.11 Л2.7Л3.4 Л3.6 Л3.7 Л3.8 Л3.9 Л3.10 Л3.1 Л3.2 Л3.11 Л3.3 Л3.5 Э1 Э2	Зачет

3.5	Политика безопасности в сетях. Технологии безопасности данных. /Ср/	8	6	ОПК-3.2-З ОПК-3.2-У ОПК-3.2-В ОПК-3.3-З ОПК-3.3-У ОПК-3.3-В	Л1.1 Л1.3 Л1.2Л2.1 Л2.8 Л2.2 Л2.3 Л2.4 Л2.6 Л2.9 Л2.10 Л2.5 Л2.11 Л2.7Л3.4 Л3.6 Л3.7 Л3.8 Л3.9 Л3.10 Л3.1 Л3.2 Л3.11 Л3.3 Л3.5 Э1 Э2	Зачет
	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/	8	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/	8	2	ОПК-3.2-З ОПК-3.2-У ОПК-3.2-В ОПК-3.3-З ОПК-3.3-У ОПК-3.3-В	Л1.1 Л1.3 Л1.2Л2.1 Л2.8 Л2.2 Л2.3 Л2.4 Л2.6 Л2.9 Л2.10 Л2.5 Л2.11 Л2.7Л3.4 Л3.6 Л3.7 Л3.8 Л3.9 Л3.10 Л3.1 Л3.2 Л3.11 Л3.3 Л3.5 Э1 Э2	Зачет
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/	8	2	ОПК-3.2-З ОПК-3.2-У ОПК-3.2-В ОПК-3.3-З ОПК-3.3-У ОПК-3.3-В	Л1.1 Л1.3 Л1.2Л2.1 Л2.8 Л2.2 Л2.3 Л2.4 Л2.6 Л2.9 Л2.10 Л2.5 Л2.11 Л2.7Л3.4 Л3.6 Л3.7 Л3.8 Л3.9 Л3.10 Л3.1 Л3.2 Л3.11 Л3.3 Л3.5 Э1 Э2	Зачет
4.4	Типовые решения по применению межсетевых экранов для за щиты информационных ресурсов. /Ср/	8	6	ОПК-3.2-З ОПК-3.2-У ОПК-3.2-В ОПК-3.3-З ОПК-3.3-У ОПК-3.3-В	Л1.1 Л1.3 Л1.2Л2.1 Л2.8 Л2.2 Л2.3 Л2.4 Л2.6 Л2.9 Л2.10 Л2.5 Л2.11 Л2.7Л3.4 Л3.6 Л3.7 Л3.8 Л3.9 Л3.10 Л3.1 Л3.2 Л3.11 Л3.3 Л3.5 Э1 Э2	Зачет

	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/	8	0			
5.2	Обзор проблем безопасности наиболее популярных Internet-сервисов. Задачи обеспечения информационной безопасности сетей. Комплексный подход к реализации основных функцио-нальных компонентов безопас-ности сетевых систем обработки информации с использованием методов и средств криптографии, механизмов аутентификации и авторизации, антивирусных средств, межсетевого экранирования. /Лек/	8	2	ОПК-3.2-З ОПК-3.2-У ОПК-3.2-В ОПК-3.3-З ОПК-3.3-У ОПК-3.3-В	Л1.1 Л1.3 Л1.2Л2.1 Л2.8 Л2.2 Л2.3 Л2.4 Л2.6 Л2.9 Л2.10 Л2.5 Л2.11 Л2.7Л3.4 Л3.6 Л3.7 Л3.8 Л3.9 Л3.10 Л3.1 Л3.2 Л3.11 Л3.3 Л3.5 Э1 Э2	Зачет
5.3	Шифры перестановки, замены, гаммирования /Лаб/	8	2	ОПК-3.2-З ОПК-3.2-У ОПК-3.2-В ОПК-3.3-З ОПК-3.3-У ОПК-3.3-В	Л1.1 Л1.3 Л1.2Л2.1 Л2.8 Л2.2 Л2.3 Л2.4 Л2.6 Л2.9 Л2.10 Л2.5 Л2.11 Л2.7Л3.4 Л3.6 Л3.7 Л3.8 Л3.9 Л3.10 Л3.1 Л3.2 Л3.11 Л3.3 Л3.5 Э1 Э2	Зачет
5.4	Методы управления средствами сетевой безопасности /Ср/	8	6	ОПК-3.2-З ОПК-3.2-У ОПК-3.2-В ОПК-3.3-З ОПК-3.3-У ОПК-3.3-В	Л1.1 Л1.3 Л1.2Л2.1 Л2.8 Л2.2 Л2.3 Л2.4 Л2.6 Л2.9 Л2.10 Л2.5 Л2.11 Л2.7Л3.4 Л3.6 Л3.7 Л3.8 Л3.9 Л3.10 Л3.1 Л3.2 Л3.11 Л3.3 Л3.5 Э1 Э2	Зачет
	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/	8	0			

6.2	Функции и назначение межсетевых экранов. Требования к межсетевым экранам. Классификация межсетевых экранов. Механизмы построения виртуальных защищенных сетей (VPN-технологии). /Лек/	8	2	ОПК-3.2-З ОПК-3.2-У ОПК-3.2-В ОПК-3.3-З ОПК-3.3-У ОПК-3.3-В	Л1.1 Л1.3 Л1.2Л2.1 Л2.8 Л2.2 Л2.3 Л2.4 Л2.6 Л2.9 Л2.10 Л2.5 Л2.11 Л2.7Л3.4 Л3.6 Л3.7 Л3.8 Л3.9 Л3.10 Л3.1 Л3.2 Л3.11 Л3.3 Л3.5 Э1 Э2	Зачет
6.3	Системы с открытым ключом. Алгоритм RSA. Схема шифрования Полига – Хеллмана. /Лаб/	8	4	ОПК-3.2-З ОПК-3.2-У ОПК-3.2-В ОПК-3.3-З ОПК-3.3-У ОПК-3.3-В	Л1.1 Л1.3 Л1.2Л2.1 Л2.8 Л2.2 Л2.3 Л2.4 Л2.6 Л2.9 Л2.10 Л2.5 Л2.11 Л2.7Л3.4 Л3.6 Л3.7 Л3.8 Л3.9 Л3.10 Л3.1 Л3.2 Л3.11 Л3.3 Л3.5 Э1 Э2	Зачет
6.4	Типовые решения по применению межсетевых экранов для защиты информационных ресурсов /Ср/	8	2	ОПК-3.2-З ОПК-3.2-У ОПК-3.2-В ОПК-3.3-З ОПК-3.3-У ОПК-3.3-В	Л1.1 Л1.3 Л1.2Л2.1 Л2.8 Л2.2 Л2.3 Л2.4 Л2.6 Л2.9 Л2.10 Л2.5 Л2.11 Л2.7Л3.4 Л3.6 Л3.7 Л3.8 Л3.9 Л3.10 Л3.1 Л3.2 Л3.11 Л3.3 Л3.5 Э1 Э2	Зачет
	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/	8	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/	8	2	ОПК-3.2-З ОПК-3.2-У ОПК-3.2-В ОПК-3.3-З ОПК-3.3-У ОПК-3.3-В	Л1.1 Л1.3 Л1.2Л2.1 Л2.8 Л2.2 Л2.3 Л2.4 Л2.6 Л2.9 Л2.10 Л2.5 Л2.11 Л2.7Л3.4 Л3.6 Л3.7 Л3.8 Л3.9 Л3.10 Л3.1 Л3.2 Л3.11 Л3.3 Л3.5 Э1 Э2	Зачет

7.3	Схема шифрования Эль-Гамаля /Лаб/	8	2	ОПК-3.2-З ОПК-3.2-У ОПК-3.2-В ОПК-3.3-З ОПК-3.3-У ОПК-3.3-В	Л1.1 Л1.3 Л1.2Л2.1 Л2.8 Л2.2 Л2.3 Л2.4 Л2.6 Л2.9 Л2.10 Л2.5 Л2.11 Л2.7Л3.4 Л3.6 Л3.7 Л3.8 Л3.9 Л3.10 Л3.1 Л3.2 Л3.11 Л3.3 Л3.5 Э1 Э2	Зачет
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. Основ-ной механизм заражения вирусом, макровирусом. Методы обнаружения макровируса. Методы обезвреживания макровируса /Пр/	8	4	ОПК-3.2-З ОПК-3.2-У ОПК-3.2-В ОПК-3.3-З ОПК-3.3-У ОПК-3.3-В	Л1.1 Л1.3 Л1.2Л2.1 Л2.8 Л2.2 Л2.3 Л2.4 Л2.6 Л2.9 Л2.10 Л2.5 Л2.11 Л2.7Л3.4 Л3.6 Л3.7 Л3.8 Л3.9 Л3.10 Л3.1 Л3.2 Л3.11 Л3.3 Л3.5 Э1 Э2	Зачет
7.5	Освоение приемов противодействия разрушающим программным средствам. /Ср/	8	8	ОПК-3.2-З ОПК-3.2-У ОПК-3.2-В ОПК-3.3-З ОПК-3.3-У ОПК-3.3-В	Л1.1 Л1.3 Л1.2Л2.1 Л2.8 Л2.2 Л2.3 Л2.4 Л2.6 Л2.9 Л2.10 Л2.5 Л2.11 Л2.7Л3.4 Л3.6 Л3.7 Л3.8 Л3.9 Л3.10 Л3.1 Л3.2 Л3.11 Л3.3 Л3.5 Э1 Э2	Зачет
	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. Законода-тельные 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/	8	0			

8.2	Понятие криптографических методов защиты информации. Классификация криптографических методов. Простейшие шифры и их свойства. Оценка криптостойкости шифров. Системы шифрования с симмет-ричным и открытым ключом. Современные алгоритмы шифрования. Понятие электронной цифровой подписи. Законодательные акты, регламентирующие использование электрон-ной цифровой подписи при реализации электронного документооборота. Процедуры постановки и проверки электронной цифровой подписи. Понятие и свойства хэш-функции. Современные алгоритмы электронной цифровой подписи /Лек/	8	2	ОПК-3.2-З ОПК-3.2-У ОПК-3.2-В ОПК-3.3-З ОПК-3.3-У ОПК-3.3-В	Л1.1 Л1.3 Л1.2Л2.1 Л2.8 Л2.2 Л2.3 Л2.4 Л2.6 Л2.9 Л2.10 Л2.5 Л2.11 Л2.7Л3.4 Л3.6 Л3.7 Л3.8 Л3.9 Л3.10 Л3.1 Л3.2 Л3.11 Л3.3 Л3.5 Э1 Э2	Зачет
8.3	Потоковый шифр RC4. Алгоритмы электронной цифровой подписи. Схема DSA. Алгоритмы электронной цифровой подписи. Схема ГОСТ, алгоритм Шнорра. /Лаб/	8	6	ОПК-3.2-З ОПК-3.2-У ОПК-3.2-В ОПК-3.3-З ОПК-3.3-У ОПК-3.3-В	Л1.1 Л1.3 Л1.2Л2.1 Л2.8 Л2.2 Л2.3 Л2.4 Л2.6 Л2.9 Л2.10 Л2.5 Л2.11 Л2.7Л3.4 Л3.6 Л3.7 Л3.8 Л3.9 Л3.10 Л3.1 Л3.2 Л3.11 Л3.3 Л3.5 Э1 Э2	Зачет
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/	8	4	ОПК-3.2-З ОПК-3.2-У ОПК-3.2-В ОПК-3.3-З ОПК-3.3-У ОПК-3.3-В	Л1.1 Л1.3 Л1.2Л2.1 Л2.8 Л2.2 Л2.3 Л2.4 Л2.6 Л2.9 Л2.10 Л2.5 Л2.11 Л2.7Л3.4 Л3.6 Л3.7 Л3.8 Л3.9 Л3.10 Л3.1 Л3.2 Л3.11 Л3.3 Л3.5 Э1 Э2	Зачет
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/	8	11	ОПК-3.2-З ОПК-3.2-У ОПК-3.2-В ОПК-3.3-З ОПК-3.3-У ОПК-3.3-В	Л1.1 Л1.3 Л1.2Л2.1 Л2.8 Л2.2 Л2.3 Л2.4 Л2.6 Л2.9 Л2.10 Л2.5 Л2.11 Л2.7Л3.4 Л3.6 Л3.7 Л3.8 Л3.9 Л3.10 Л3.1 Л3.2 Л3.11 Л3.3 Л3.5 Э1 Э2	Зачет
	Раздел 9. Промежуточная аттестация					
9.1	Промежуточная аттестация /Тема/	8	0			

9.2	Сдача зачета /ИКР/	8	0,25	ОПК-3.2-З ОПК-3.2-У ОПК-3.2-В ОПК-3.3-З ОПК-3.3-У ОПК-3.3-В	Л1.1 Л1.3 Л1.2Л2.1 Л2.8 Л2.2 Л2.3 Л2.4 Л2.6 Л2.9 Л2.10 Л2.5 Л2.11 Л2.7Л3.4 Л3.6 Л3.7 Л3.8 Л3.9 Л3.10 Л3.1 Л3.2 Л3.11 Л3.3 Л3.5 Э1 Э2	Зачет
9.3	Подготовка к зачету /Зачёт/	8	8,75	ОПК-3.2-З ОПК-3.2-У ОПК-3.2-В ОПК-3.3-З ОПК-3.3-У ОПК-3.3-В	Л1.1 Л1.3 Л1.2Л2.1 Л2.8 Л2.2 Л2.3 Л2.4 Л2.6 Л2.9 Л2.10 Л2.5 Л2.11 Л2.7Л3.4 Л3.6 Л3.7 Л3.8 Л3.9 Л3.10 Л3.1 Л3.2 Л3.11 Л3.3 Л3.5 Э1 Э2	Зачет

5. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ПО ДИСЦИПЛИНЕ (МОДУЛЮ)

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

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	Евдокимова Л.М., Корябкин В.В., Пылькин А.Н., Швечкова О.Г.	Электронный документооборот и обеспечение безопасности стандартными средствами WINDOWS : учеб. пособие	М.: КУРС, 2017, 294с.; прил.	978-5-906923-24-0,978-5-16-012741-5, 1
Л1.2	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
Л1.3	Швечкова О.Г., Пылькин А.Н., Марчев Д.В.	Базовые криптографические алгоритмы защиты информации : учеб. пособие	М.: КУРС, 2018, 168с.	978-5-906923-83-7, 1

6.1.2. Дополнительная литература

№	Авторы, составители	Заглавие	Издательство, год	Количество/ название ЭБС
Л2.1	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

№	Авторы, составители	Заглавие	Издательство, год	Количество/ название ЭБС
Л2.2	Швечкова О.Г.	Методы и средства защиты информации : Метод.указ.к лаб.работам	Рязань, 2003, 32с.	, 1
Л2.3	Швечкова О.Г., Блинов А.В., Смирнов В.А.	Методы защиты информационных систем : метод. указ. к лаб. работам	Рязань, 2009, 48с.	, 1
Л2.4	Швечкова О.Г., Москвитина О.А., Курдюков Н.С.	Современные алгоритмы криптографической защиты информации : Методические указания	Рязань: РИЦ РГРТУ, 2012,	, https://elib.rsreu.ru/ebs/download/1027
Л2.5	Швечкова О.Г., Москвитина О.А., Курдюков Н.С.	Основы теории и практики реализации криптографических алгоритмов защиты информации : Методические указания	Рязань: РИЦ РГРТУ, 2012,	, https://elib.rsreu.ru/ebs/download/1028
Л2.6	Швечкова О.Г., Блинов А.В., Смирнов В.А.	Методы защиты информационных систем : Методические указания	Рязань: РИЦ РГРТУ, 2009,	, https://elib.rsreu.ru/ebs/download/1259
Л2.7	Шаньгин В.Ф.	Защита компьютерной информации.Эффективные методы и средства : Учеб.пособие	М.:ДМК Пресс, 2008, 544с.	5-94074-383-8, 1
Л2.8	Демидов Д.Г., Швечкова О.Г., Москвитина О.А., Пылькин А.Н., Майков К.А., Смирнова Г.К.	Защита информации с использованием механизмов электронной цифровой подписи : Учебное пособие	Рязань: РИЦ РГРТУ, 2014,	, https://elib.rsreu.ru/ebs/download/1316
Л2.9	Швечкова О.Г., Москвитина О.А., Курдюков Н.С.	Современные алгоритмы криптографической защиты информации : метод. указ. к лаб. работам	Рязань, 2012, 40с.	, 1
Л2.10	Шаньгин В. Ф.	Информационная безопасность и защита информации	Саратов: Профобразование, 2019, 702 с.	978-5-4488-0070-2, http://www.iprbookshop.ru/87995.html
Л2.11	Романец Ю.В., Тимофеев П.А., Шаньгин В.Ф.	Защита информации в компьютерных системах и сетях	М.:Радио и связь, 1999, 328с.	5-256-01436-6, 1
6.1.3. Методические разработки				
№	Авторы, составители	Заглавие	Издательство, год	Количество/ название ЭБС
Л3.1	Соколов А.В., Шаньгин В.Ф.	Защита информации в распределенных корпоративных сетях и системах	М.:ДМК Пресс, 2002, 655с.	5-94074-172-X, 1

№	Авторы, составители	Заглавие	Издательство, год	Количество/ название ЭБС
Л3.2	Романец Ю.В., Тимофеев П.А., Шаньгин В.Ф.	Защита информации в компьютерных системах и сетях	М.:Радио и связь, 2001, 376с.	5-256-01518-4, 1
Л3.3	Гашков С.Б., Применко Э.А., Черепнев М.А.	Криптографические методы защиты информации : учеб. пособие	М.: Академия, 2010, 304с.	978-5-7695-4962-5, 1
Л3.4	Швечкова О.Г., Бурдина Л.В., Бусловаев М.А., Блинов А.В., Смирнов В.А.	Основы теории и практики реализации механизмов информационной безопасности : метод. указ. к лаб. работам	Рязань, 2008, 40с.	, 1
Л3.5	Швечкова О.Г., Москвитина О.А., Курдюков Н.С.	Основы теории и практики реализации криптографических алгоритмов защиты информации : метод. указ. к лаб. работам	Рязань, 2012, 47с.	, 1
Л3.6	Швечкова О.Г., Москвитина О.А.	Алгоритмы электронной цифровой подписи. Схема DSA : Методические указания	Рязань: РИЦ РГРТУ, 2013,	, https://elib.rsreu.ru/ebs/download/1029
Л3.7	Швечков В.А., Швечкова О.Г.	Методы контроля, обеспечения достоверности и защиты информационного и программного обеспечения. Защита от разрушающих программных средств : метод. указ. к лаб. работе	Рязань, 2014, 16с.	, 1
Л3.8	Швечкова О.Г., Москвитина О.А.	Алгоритмы электронной цифровой подписи. Схема ГОСТ Р 34.10-2001 : Методические указания	Рязань: РИЦ РГРТУ, 2013,	, https://elib.rsreu.ru/ebs/download/1030
Л3.9	Швечкова О.Г., Москвитина О.А.	Алгоритмы электронной цифровой подписи. Схема Эль-Гамаля : Методические указания	Рязань: РИЦ РГРТУ, 2013,	, https://elib.rsreu.ru/ebs/download/1031
Л3.10	Швечков В.А., Швечкова О.Г.	Методы контроля, обеспечения достоверности и защиты информационного и программного обеспечения. Защита от разрушающих программных средств : Методические указания	Рязань: РИЦ РГРТУ, 2014,	, https://elib.rsreu.ru/ebs/download/1260
Л3.11	Швечков В.А., Швечкова О.Г.	Методы контроля, обеспечения достоверности и защиты информационного и программного обеспечения. Схемы электронной цифровой подписи. Алгоритм Шнорра : Методические указания	Рязань: РИЦ РГРТУ, 2014,	, https://elib.rsreu.ru/ebs/download/1261

6.2. Перечень ресурсов информационно-телекоммуникационной сети "Интернет"

Э1	Электронная библиотека РГРТУ http://elib.rsreu.ru/
Э2	Электронная библиотека IPRBooks http://iprbookshop.ru/

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

Pyton	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	Справочная правовая система «КонсультантПлюс» (договор об информационной поддержке №1342/455-100 от 28.10.2011 г.)
6.3.2.2	Система КонсультантПлюс http://www.consultant.ru
6.3.2.3	Информационно-правовой портал ГАРАНТ.РУ http://www.garant.ru

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 36 мест (+17 мест за компьютерными столами) проектор BENQ 10 ПК с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду: ЦП: intel i3 3220, ОЗУ: 4 Gb, ПЗУ: 320-500 Gb (9 шт.) ЦП: intel i5 6500, ОЗУ: 8 Gb, ПЗУ: 500 Gb (1 шт. преподавательский)
2	106 учебно-административный корпус. Аудитория для самостоятельной работы 36 мест (+17 мест за компьютерными столами) проектор BENQ 10 ПК с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду: ЦП: intel i3 3220, ОЗУ: 4 Gb, ПЗУ: 320-500 Gb (9 шт.) ЦП: intel i5 6500, ОЗУ: 8 Gb, ПЗУ: 500 Gb (1 шт. преподавательский)
3	106а учебно-административный корпус. Учебная аудитория для проведения занятий лекционного и семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации 42 места (+15 мест за компьютерными столами) проектор BENQ 16 ПК с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду: ЦП: intel i3 3220, ОЗУ: 4 Gb, ПЗУ: 320-500 Gb (15 шт.) ЦП: intel i5 6500, ОЗУ: 8 Gb, ПЗУ: 500 Gb (1 шт. преподавательский)
4	110 учебно-административный корпус. Учебная аудитория для проведения занятий лекционного и семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации 20 мест (+20 мест за компьютерными столами) Проектор: HITACHI CP-X400 3LCD 21 ПК с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду: ЦП: Intel i5-12400 ОЗУ: 16 Гб ПЗУ: ssd 512 Гб (20 шт. моноблок + 1шт. преподавательский)

5	110 учебно-административный корпус. Аудитория для самостоятельной работы 20 мест (+20 мест за компьютерными столами) Проектор: HITACHI CP-X400 3LCD 21 ПК с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду: ЦП: Intel i5-12400 ОЗУ: 16 Гб ПЗУ: ssd 512 Гб (20 шт. моноблок + 1шт. преподавательский)

8. МЕТОДИЧЕСКИЕ МАТЕРИАЛЫ ПО ДИСЦИПЛИНЕ (МОДУЛЮ)

Методическое обеспечение дисциплины приведено в приложении к рабочей программе дисциплины (см. документ «Методические указания дисциплины «Защита информации»»)

Оператор ЭДО ООО "Компания "Тензор"

ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ

ПОДПИСАНО ЗАВЕДУЮЩИМ КАФЕДРЫ — **ФГБОУ ВО "РГРТУ", РГРТУ,** Овечкин Геннадий Владимирович, Заведующий кафедрой ВПМ — **12.10.26** 08:32 (MSK) — Простая подпись

ПОДПИСАНО ЗАВЕДУЮЩИМ ВЫПУСКАЮЩЕЙ КАФЕДРЫ — **ФГБОУ ВО "РГРТУ", РГРТУ,** Овечкин Геннадий Владимирович, Заведующий кафедрой ВПМ — **12.10.26** 08:33 (MSK) — Простая подпись