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
Проректор по УР

А.В. Корячко

Защита информации

рабочая программа дисциплины (модуля)

Закреплена за кафедрой **Вычислительная и прикладная математика**

Учебный план z09.03.02_21_00.plx
09.03.02 Информационные системы и технологии

Квалификация **бакалавр**

Форма обучения **заочная**

Общая трудоемкость **3 ЗЕТ**

Распределение часов дисциплины по курсам

Курс	**5**		Итого	
Вид занятий	УП	РП		
Лекции	6	6	6	6
Лабораторные	6	6	6	6
Практические	6	6	6	6
Иная контактная работа	0,25	0,25	0,25	0,25
Итого ауд.	18,25	18,25	18,25	18,25
Контактная работа	18,25	18,25	18,25	18,25
Сам. работа	76	76	76	76
Часы на контроль	3,75	3,75	3,75	3,75
Контрольная работа заочники	10	10	10	10
Итого	108	108	108	108

г. Рязань

Программу составил(и):
к.т.н., доц., Швечкова Ольга Григорьевна

Рабочая программа дисциплины
Защита информации

разработана в соответствии с ФГОС ВО:
ФГОС ВО - бакалавриат по направлению подготовки 09.03.02 Информационные системы и технологии (приказ Минобрнауки России от 19.09.2017 г. № 926)

составлена на основании учебного плана:
09.03.02 Информационные системы и технологии
утвержденного учёным советом вуза от 28.01.2022 протокол № 6.

Рабочая программа одобрена на заседании кафедры
Вычислительная и прикладная математика

Протокол от 14.06.2022 г. № 10
Срок действия программы: 2021-2026 уч.г.
Зав. кафедрой Овечкин Геннадий Владимирович

Визирование РПД для исполнения в очередном учебном году

Рабочая программа пересмотрена, обсуждена и одобрена для исполнения в 2023-2024 учебном году на заседании кафедры
Вычислительная и прикладная математика

Протокол от __ _____ 2023 г. № __

Зав. кафедрой _____

Визирование РПД для исполнения в очередном учебном году

Рабочая программа пересмотрена, обсуждена и одобрена для исполнения в 2024-2025 учебном году на заседании кафедры
Вычислительная и прикладная математика

Протокол от __ _____ 2024 г. № __

Зав. кафедрой _____

Визирование РПД для исполнения в очередном учебном году

Рабочая программа пересмотрена, обсуждена и одобрена для исполнения в 2025-2026 учебном году на заседании кафедры
Вычислительная и прикладная математика

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

Вычислительная и прикладная математика

Протокол от __ _____ 2026 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 информа-ции.
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
Знать основные требования информационной безопасности
Уметь
Уметь поддерживать основные требования информационной безопасности
Владеть
Владеть приемами обеспечения основных требований информационной безопасности

ОПК-3.3. Решает задачи профессиональной деятельности с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности

Знать
Знать методы решения задач профессиональной деятельности с применением информационно-коммуникационных технологий с учетом требований информационной безопасности
Уметь
Уметь применять методы решения задач профессиональной деятельности с применением информационно-коммуникационных технологий с учетом требований информационной безопасности
Владеть
Владеть методами решения задач профессиональной деятельности с применением информационно-коммуникационных технологий с учетом требований информационной безопасности

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	
3.1.3	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/	5	0			
1.2	Проблема информационной безопасности общества. Основ-ные 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. Оценка рисков в сфере информационной безопасности. Ос-новные методы средства, меха-низмы защиты информации. /Лек/	5	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 Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.1 Л2.1 Л2.3 Л2.4 Л2.5 Л2.6 Л2.7 Л2.8 Л2.9Л3.3 Л3.4 Л3.5 Л3.7 Л3.8 Л3.9 Л3.10 Л3.11 Л3.12 Л3.13 Л3.14	Зачет
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 ак-тов РФ в области защиты ин-формации и информационных систем от разрушающих программных средств. Изучение различных видов разрушающих программных средств. /Пр/	5	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 Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.1 Л3.5 Л2.1 Л2.3 Л2.4 Л2.5 Л2.6 Л2.7 Л3.10 Л2.8 Л2.9Л3.3 Л3.4 Л3.7 Л3.8 Л3.9 Л3.11 Л3.12 Л3.13 Л3.14	Защита практической работы

1.4	Проблемы защиты информации для открытых информационных систем. Характеристики, влияющие на безопасность информации. /Ср/	5	20	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 Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.1 Л2.1 Л2.3 Л2.4 Л2.5 Л2.6 Л2.7 Л2.8 Л2.9Л3.3 Л3.4 Л3.5 Л3.7 Л3.8 Л3.9 Л3.10 Л3.11 Л3.12 Л3.13 Л3.14	Зачет
1.5	Методы контроля, обеспечения достоверности и защиты ин-формационного и программного обеспечения. Защита от разрушающих программных средств. /Лаб/	5	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	Л2.1 Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л1.1 Л3.3 Л3.4 Л2.3 Л2.4 Л2.5 Л2.6 Л2.7 Л2.8 Л2.9Л2.1 Л3.5 Л3.7 Л3.8 Л3.9 Л3.10 Л3.11 Л3.12 Л3.13 Л3.14	Защита лабораторной работы
	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/	5	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/	5	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 Л3.5 Л2.1 Л1.1 Л1.2 Л3.10 Л1.3 Л1.4Л2.1 Л2.2 Л2.1 Л2.3 Л2.4 Л2.5 Л2.6 Л2.7 Л2.8 Л2.9Л3.3 Л3.4 Л3.7 Л3.8 Л3.9 Л3.11 Л3.12 Л3.13 Л3.14	Зачет

2.3	Построение сценария функцио-нирования компьютерной си-стемы в среде реально существующих угроз с учетом ролей всех участников процесса обработки и потребления информации. /Пр/	5	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	Л2.1 Л2.2 Л1.1 Л2.1 Л1.1 Л2.5 Л1.2 Л2.7 Л1.3 Л1.4Л2.1 Л2.3 Л2.4 Л2.6 Л2.8 Л2.9Л3.3 Л3.4 Л3.5 Л3.7 Л3.8 Л3.9 Л3.10 Л3.11 Л3.12 Л3.13 Л3.14	Защита практической работы
2.4	Возможности сети Интернет и проблемы безопасности. Угрозы и уязвимости корпоративных сетей и систем. /Ср/	5	18	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 Л1.1 Л2.4 Л2.5 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.1 Л3.7 Л2.3 Л2.6 Л2.7 Л2.8 Л2.9Л2.1 Л3.3 Л3.4 Л3.5 Л3.8 Л3.9 Л3.10 Л3.11 Л3.12 Л3.13 Л3.14	Зачет
2.5	Шифры перестановки, замены, гаммирования /Лаб/	5	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	Л3.7 Л2.3 Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л3.3 Л3.4 Л2.1 Л2.4 Л2.5 Л2.6 Л2.7 Л2.8 Л2.9Л1.1 Л2.1 Л3.5 Л3.8 Л3.9 Л3.10 Л3.11 Л3.12 Л3.13 Л3.14	Защита лабораторной работы
2.6	Типовые решения по применению межсетевых экранов для защиты информационных ресурсов. /Ср/	5	10	ОПК-3.2-З ОПК-3.2-У ОПК-3.2-В ОПК-3.3-З ОПК-3.3-У ОПК-3.3-В	Л2.1 Л2.2 Л1.1 Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.1 Л2.3 Л2.4 Л2.5 Л2.6 Л2.7 Л2.8 Л2.9Л3.3 Л3.4 Л3.5 Л3.7 Л3.8 Л3.9 Л3.10 Л3.11 Л3.12 Л3.13 Л3.14	Зачет

2.7	Методы управления средствами сетевой безопасности. Освоение приемов противодействия разрушающим программным средствам. /Ср/	5	18	ОПК-3.2-З ОПК-3.2-У ОПК-3.2-В ОПК-3.3-З ОПК-3.3-У ОПК-3.3-В	Л2.1 Л2.2 Л1.1 Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л3.3 Л3.4 Л2.1 Л2.3 Л2.4 Л2.5 Л2.6 Л2.7 Л2.8 Л2.9Л3.5 Л3.7 Л3.8 Л3.9 Л3.10 Л3.11 Л3.12 Л3.13 Л3.14	Зачет
2.8	Основные принципы работы алгоритмов отечественной цифровой подписи. /Ср/	5	10	ОПК-3.2-З ОПК-3.2-У ОПК-3.2-В ОПК-3.3-З ОПК-3.3-У ОПК-3.3-В	Л2.1 Л2.2 Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л3.3 Л2.1 Л2.3 Л2.4 Л2.5 Л2.6 Л2.7 Л2.8 Л2.9Л1.1 Л3.4 Л3.5 Л3.7 Л3.8 Л3.9 Л3.10 Л3.11 Л3.12 Л3.13 Л3.14	Зачет
	Раздел 3. Общие подходы к проблеме защиты информации. Основные методы и средства защиты безопасности					
3.1	Общие подходы к проблеме защиты информации. Основные методы и средства защиты безопасности /Тема/	5	0			
3.2	Теоретические основы инфор-мационной безопасности. Понятия «объект», «субъект», «сущность», «процесс». Поня-тие модели безопасности. Виды моделей безопасности в зависимости от реализуемых функций защиты. Понятие политики безопасности. Мандатная, дискреционная, ролевая политики безопасности. /Лек/	5	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 Л2.3 Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.4 Л2.5 Л2.6 Л2.7 Л2.8 Л2.9Л2.1 Л3.3 Л3.4 Л3.5 Л2.1 Л3.7 Л3.8 Л3.9 Л3.10 Л3.11 Л3.12 Л3.13 Л3.14	Зачет
3.3	Алгоритмы электронной цифровой подписи. Схема ГОСТ, алгоритм Шнорра. /Лаб/	5	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 Л2.1 Л2.3 Л1.1 Л1.2 Л3.10 Л1.3 Л1.4Л2.1 Л2.2 Л2.1 Л2.4 Л2.5 Л2.6 Л2.7 Л2.8 Л2.9Л3.3 Л3.4 Л3.5 Л3.7 Л3.8 Л3.9 Л3.11 Л3.12 Л3.13 Л3.14	Защита лабораторной работы

3.4	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/	5	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	Л2.1 Л2.2 Л1.1 Л1.1 Л2.6 Л1.2 Л2.7 Л1.3 Л1.4Л2.1 Л2.1 Л2.3 Л2.4 Л2.5 Л2.8 Л2.9Л3.3 Л3.4 Л3.5 Л3.7 Л3.8 Л3.9 Л3.10 Л3.11 Л3.12 Л3.13 Л3.14	Защита практической работы
	Раздел 4. Промежуточная аттестация					
4.1	Промежуточная аттестация /Тема/	5	0			
4.2	Сдача зачета /ИКР/	5	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 Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.1 Л2.3 Л2.4 Л2.5 Л2.6 Л2.7 Л2.8 Л2.9Л3.3 Л3.4 Л3.5 Л2.1 Л3.7 Л3.8 Л3.9 Л3.10 Л3.11 Л3.12 Л3.13 Л3.14	Зачет
4.3	Контрольная работа /КрЗ/	5	10	ОПК-3.2-З ОПК-3.2-У ОПК-3.2-В ОПК-3.3-З ОПК-3.3-У ОПК-3.3-В	Л2.1 Л1.1 Л2.5 Л2.6 Л1.2 Л1.3 Л1.4Л2.2 Л1.1 Л2.1 Л2.3 Л2.4 Л2.7 Л2.8 Л2.9 Л3.12 Л3.13Л2.1 Л3.3 Л3.4 Л3.5 Л3.7 Л3.8 Л3.9 Л3.10 Л3.11 Л3.14	Защита контрольной работы
4.4	Подготовка к зачету /Зачёт/	5	3,75	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 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л1.1 Л2.3 Л2.4 Л2.5 Л2.6 Л2.7 Л2.8 Л2.9Л2.1 Л3.3 Л3.4 Л3.5 Л2.1 Л3.7 Л3.8 Л3.9 Л3.10 Л3.11 Л3.12 Л3.13 Л3.14	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	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
Л1.2	Швечкова О.Г.	Алгоритмы стеганографической защиты информации : Методические указания	Рязань: РИЦ РГРТУ, 2017,	, https://elib.rsreu.ru/ebs/download/1318
Л1.3	Швечкова О.Г.	Методы и средства защиты информации : Метод.указ.к лаб.работам	Рязань, 2003, 32с.	, 1
Л1.4	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
Л1.5	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	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
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
Л2.3	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
Л2.4	Шаньгин В. Ф.	Информационная безопасность и защита информации	Саратов: Профобразование, 2019, 702 с.	978-5-4488-0070-2, http://www.iprbookshop.ru/87995.html
Л2.5	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

№	Авторы, составители	Заглавие	Издательство, год	Количество/ название ЭБС
Л2.6	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
Л2.7	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
Л2.8	Соколов А.В., Шаньгин В.Ф.	Защита информации в распределенных корпоративных сетях и системах	М.:ДМК Пресс, 2002, 655с.	5-94074-172-X, 1
Л2.9	Шаньгин В.Ф.	Защита компьютерной информации.Эффективные методы и средства : Учеб.пособие	М.:ДМК Пресс, 2008, 544с.	5-94074-383-8, 1
Л2.10	Швечкова О.Г., Москвитина О.А., Курдюков Н.С.	Современные алгоритмы криптографической защиты информации : метод. указ. к лаб. работам	Рязань, 2012, 40с.	, 1
Л2.11	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

6.1.3. Методические разработки

№	Авторы, составители	Заглавие	Издательство, год	Количество/ название ЭБС
Л3.1	Швечкова О.Г., Блинов А.В., Смирнов В.А.	Методы защиты информационных систем : метод. указ. к лаб. работам	Рязань, 2009, 48с.	, 1
Л3.2	Швечкова О.Г., Москвитина О.А.	Алгоритмы электронной цифровой подписи. Схема Эль-Гамаля : метод. указ. к лаб. работам	Рязань, 2013, 15с.	, 1
Л3.3	Швечкова О.Г., Москвитина О.А.	Алгоритмы электронной цифровой подписи. Схема DSA : метод. указ. к лаб. работам	Рязань, 2013, 16с.	, 1
Л3.4	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
Л3.5	Швечкова О.Г.	Алгоритмы стеганографической защиты информации : метод. указ. к лаб. работам	Рязань, 2017, 32с.	, 1

№	Авторы, составители	Заглавие	Издательство, год	Количество/ название ЭБС
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	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
Л3.8	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
Л3.9	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
Л3.10	Швечкова О.Г.	Криптографические методы защиты информации : Метод.указ.к лаб.работам N1-8	Рязань, 2004, 40с.	, 1
Л3.11	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

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
Kaspersky Endpoint Security	Коммерческая лицензия
LibreOffice	Свободное ПО
Adobe Acrobat Reader	Свободное ПО
OpenOffice	Свободное ПО
Pyton	Свободное ПО
Node.js. VisualStudioCode	Свободное ПО
Visual studio community	Свободное ПО
Chrome	Свободное ПО
Firefox	Свободное ПО
7 Zip	Свободное ПО
PyCharm Community	Свободное ПО
Delphi Community Edition	Свободное ПО
Adobe Acrobat Reader DC	Свободное ПО
Интерпретатор Python	Свободное ПО
Kaspersky Endpoint Security	Коммерческая лицензия
Операционная система Windows XP	Microsoft Imagine, номер подписки 700102019, бессрочно
Продукты Microsoft по программе DreamSpark Membership ID 700565239 (операционные системы семейства Windows)	Коммерческая лицензия
Microsoft Project 2010 - Microsoft DreamSpark Membership ID 700565239	

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.)

8. МЕТОДИЧЕСКИЕ МАТЕРИАЛЫ ПО ДИСЦИПЛИНЕ (МОДУЛЮ)

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

Подписано заведующим кафедры	**ФГБОУ ВО "РГРТУ", РГРТУ,** Овечкин Геннадий Владимирович, Заведующий кафедрой **11.12.2022** 19:34 (MSK), Простая подпись
Подписано заведущим выпускающей кафедры	**ФГБОУ ВО "РГРТУ", РГРТУ,** Холопов Сергей Иванович, Декан **13.12.2022** 13:36 (MSK), Простая подпись
Подписано проректором по УР	**ФГБОУ ВО "РГРТУ", РГРТУ,** Корячко Алексей Вячеславович, Проректор по учебной работе **13.12.2022** 15:29 (MSK), Простая подпись