

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 z09.03.03_22_00.plx
09.03.03 Прикладная информатика
Квалификация **бакалавр**
Форма обучения **заочная**
Общая трудоемкость **3 ЗЕТ**

Распределение часов дисциплины по курсам

Курс	5		Итого	
	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 09.03.03 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 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: 2022-2026 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 соответствии с Федеральным государственным образовательным стандартом в сфере обеспечения безопасности информации и информационных 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 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	Научно-исследовательская работа
2.1.2	Учебная практика
2.1.3	Ознакомительная практика
2.1.4	Интегрированные информационные технологии общего назначения
2.2 Дисциплины (модули) и практики, для которых освоение данной дисциплины (модуля) необходимо как предшествующее:	

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 применять основные требования информационной безопасности.
Владеть	Владеть приемами реализации основных требований информационной безопасности.
ОПК-3.3. Решает задачи профессиональной деятельности с применением информационно-коммуникационных технологий с учетом основных требований информационной безопасности	
Знать	Знать методы решения задач профессиональной деятельности с учетом основных требований информационной безопасности.
Уметь	Уметь применять методы решения задач профессиональной деятельности с учетом основных требований информационной безопасности.
Владеть	Владеть методами решения задач профессиональной деятельности с учетом основных 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	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 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. 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. Оценка рисков в сфере информационной безопасности. Основные методы средства, механизмы защиты информации. /Лек/	5	2	ОПК-3.2-3 ОПК-3.2-У ОПК-3.2-В ОПК-3.3-3 ОПК-3.3-У ОПК-3.3-В	Л1.1 Л1.2Л2.1 Л2.2Л3.1 Л3.2	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 актов РФ в области защиты информации и информационных систем от разрушающих программных средств. Изучение различных видов разрушающих программных средств. /Пр/	5	2	ОПК-3.2-3 ОПК-3.2-У ОПК-3.2-В ОПК-3.3-3 ОПК-3.3-У ОПК-3.3-В	Л1.1 Л1.2Л2.1 Л2.2Л3.1 Л3.2	Защита практической работы
1.4	Проблемы защиты информации для открытых информационных систем. Характеристики, влияющие на безопасность информации. /Ср/	5	20	ОПК-3.2-3 ОПК-3.2-У ОПК-3.2-В ОПК-3.3-3 ОПК-3.3-У ОПК-3.3-В	Л1.1 Л1.2Л2.1 Л2.2Л3.1 Л3.2	Зачет

1.5	Методы контроля, обеспечения достоверности и защиты информации и программного обеспечения. Защита от разрушающих программных средств. /Лаб/	5	2	ОПК-3.2-3 ОПК-3.2-У ОПК-3.2-В ОПК-3.3-3 ОПК-3.3-У ОПК-3.3-В	Л1.1 Л1.2Л2.1 Л2.2Л3.1 Л3.2	Зачет
	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 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-3.2-3 ОПК-3.2-У ОПК-3.2-В ОПК-3.3-3 ОПК-3.3-У ОПК-3.3-В	Л1.1 Л1.2Л2.1 Л2.2Л3.1 Л3.2	Зачет
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/	5	2	ОПК-3.2-3 ОПК-3.2-У ОПК-3.2-В ОПК-3.3-3 ОПК-3.3-У ОПК-3.3-В	Л1.1 Л1.2Л2.1 Л2.2Л3.1 Л3.2	Защита практической работы
2.4	Возможности сети Интернет и проблемы безопасности. Угрозы и уязвимости корпоративных сетей и систем. /Ср/	5	18	ОПК-3.2-3 ОПК-3.2-У ОПК-3.2-В ОПК-3.3-3 ОПК-3.3-У ОПК-3.3-В	Л1.1 Л1.2Л2.1 Л2.2Л3.1 Л3.2	Зачет
2.5	Шифры перестановки, замены, гаммирования /Лаб/	5	2	ОПК-3.2-3 ОПК-3.2-У ОПК-3.2-В ОПК-3.3-3 ОПК-3.3-У ОПК-3.3-В	Л1.1 Л1.2Л2.1 Л2.2Л3.1 Л3.2	Защита лабораторной работы
2.6	Типовые решения по применению межсетевых экранов для защиты информационных ресурсов. /Ср/	5	10	ОПК-3.2-3 ОПК-3.2-У ОПК-3.2-В ОПК-3.3-3 ОПК-3.3-У ОПК-3.3-В	Л1.1 Л1.2Л2.1 Л2.2Л3.1 Л3.2	Зачет
2.7	Методы управления средствами сетевой безопасности. Освоение приемов противодействия разрушающим программным средствам. /Ср/	5	18	ОПК-3.2-3 ОПК-3.2-У ОПК-3.2-В ОПК-3.3-3 ОПК-3.3-У ОПК-3.3-В	Л1.1 Л1.2Л2.1 Л2.2Л3.1 Л3.2	Зачет

2.8	Основные принципы работы алгоритмов отечественной цифровой подписи. /Ср/	5	10	ОПК-3.2-3 ОПК-3.2-У ОПК-3.2-В ОПК-3.3-3 ОПК-3.3-У ОПК-3.3-В	Л1.1 Л1.2Л2.1 Л2.2Л3.1 Л3.2	Зачет
Раздел 3. Подготовка к зачету						
3.1	Подготовка к зачету /Тема/	5	0			
3.2	Подготовка к зачету /ИКР/	5	0,25	ОПК-3.2-3 ОПК-3.2-У ОПК-3.2-В ОПК-3.3-3 ОПК-3.3-У ОПК-3.3-В	Л1.1 Л1.2Л2.1 Л2.2Л3.1 Л3.2	Зачет
3.3	Контрольная работа /КрЗ/	5	10	ОПК-3.2-3 ОПК-3.2-У ОПК-3.2-В ОПК-3.3-3 ОПК-3.3-У ОПК-3.3-В	Л1.1 Л1.2Л2.1 Л2.2Л3.1 Л3.2	Защита контрольной работы
3.4	Зачет /Зачёт/	5	3,75	ОПК-3.2-3 ОПК-3.2-У ОПК-3.2-В ОПК-3.3-3 ОПК-3.3-У ОПК-3.3-В	Л1.1 Л1.2Л2.1 Л2.2Л3.1 Л3.2	Зачет
Раздел 4. Общие подходы к проблеме защиты информации. Основные методы и средства защиты безопасности						
4.1	Общие подходы к проблеме защиты информации. Основные методы и средства защиты безопасности /Тема/	5	0			
4.2	Теоретические основы информации 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/	5	2	ОПК-3.2-У ОПК-3.2-В ОПК-3.3-3 ОПК-3.3-У ОПК-3.3-В ОПК-3.2-3	Л1.1 Л1.2Л2.1 Л2.2Л3.1 Л3.2	Зачет
4.3	Алгоритмы электронной цифровой подписи. Схема ГОСТ, алгоритм Шнорра. /Лаб/	5	2	ОПК-3.2-3 ОПК-3.2-У ОПК-3.2-В ОПК-3.3-3 ОПК-3.3-У ОПК-3.3-В	Л1.1 Л1.2Л2.1 Л2.2Л3.1 Л3.2	Защита лабораторной работы
4.4	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-3.2-3 ОПК-3.2-У ОПК-3.2-В ОПК-3.3-3 ОПК-3.3-У ОПК-3.3-В	Л1.1 Л1.2Л2.1 Л2.2Л3.1 Л3.2	Защита практической работы

5. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ПО ДИСЦИПЛИНЕ (МОДУЛЮ)

Оценочные материалы приведены в приложении к рабочей программе дисциплины (см. документ «Оценочные материалы по дисциплине «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	Башлы П. Н., Бабаш А. В., Баранова Е. К.	Информационная безопасность и защита информации : учебное пособие	Москва: Евразийский открытый институт, 2012, 311 с.	978-5-374-00301-7, http://www.iprbookshop.ru/10677.html
Л1.2	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

6.1.2. Дополнительная литература

№	Авторы, составители	Заглавие	Издательство, год	Количество/название ЭБС
Л2.1	Нерсисянц А. А.	Защита информации : учебное пособие	Ростов-на-Дону: Северо-Кавказский филиал Московского технического университета связи и информатики, 2010, 61 с.	2227-8397, http://www.iprbookshop.ru/61295.html
Л2.2	Омарова С. А., Исакова К. А., Тойганбаева Н. А.	Информационная безопасность и защита информации : учебно-методический комплекс	Алматы: Нур-Принт, 2012, 98 с.	9965-756-05-8, http://www.iprbookshop.ru/67055.html

6.1.3. Методические разработки

№	Авторы, составители	Заглавие	Издательство, год	Количество/название ЭБС
Л3.1	Каторин Ю. Ф., Разумовский А. В., Спивак А. И., Каторин Ю. Ф.	Техническая защита информации : лабораторный практикум	Санкт-Петербург: Университет ИТМО, 2013, 113 с.	2227-8397, http://www.iprbookshop.ru/68715.html
Л3.2	Малинин Ю.И.	Информационная безопасность и защита информации : Методические указания	Рязань: РИЦ РГРТУ, 2009,	https://elib.rsre.ru/ebs/download/851

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
Adobe Acrobat Reader	Свободное ПО
LibreOffice	Свободное ПО
VirtualBox	Свободное ПО
OpenOffice	Свободное ПО
Python	Свободное ПО

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 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	110 учебно-административный корпус. Аудитория для самостоятельной работы 20 мест Проектор: НІТАСНІ СР-Х400 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.)
3	206-2 учебно-административный корпус. Аудитория для самостоятельной работы 18 мест, Телевизор PHILIPS 46PFL3208T/60; документ-камера: AverVisionF33 POE7D; 20 ПК с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду: ЦП: Intel Pentium II/III class 2327 ОЗУ: 2 Гб ПЗУ: 80 Гб (1 шт.) ЦП: Intel Pentium III 2992 ОЗУ: 1,5 Гб ПЗУ: 150 Гб (1 шт.) ЦП: Intel Pentium III 2660 ОЗУ: 2 Гб ПЗУ: 80 Гб (9 шт.) ЦП: Intel Pentium III 2793 ОЗУ: 2 Гб ПЗУ: 100 Гб (1 шт.) ЦП: Intel Pentium II/III class 2660 ОЗУ: 1 Гб ПЗУ: 50 Гб (1 шт.) ЦП: Intel Pentium III 2527 ОЗУ: 2 Гб ПЗУ: 100 Гб (1 шт.) ЦП: Intel Pentium III 3158 ОЗУ: 2 Гб ПЗУ: 50 Гб (3 шт.) ЦП: Intel Pentium III 2826 ОЗУ: 2 Гб ПЗУ: 100 Гб (2 шт.) ЦП: Intel Pentium III 2693 ОЗУ: 1,5 Гб ПЗУ: 100 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
24.11.2022 16:17 (MSK), Простая подпись

Подписано заведующим выпускающей кафедры

ФГБОУ ВО "РГРТУ", РГРТУ, Овечкин Геннадий Владимирович, Заведующий кафедрой
24.11.2022 16:18 (MSK), Простая подпись

Подписано проректором по УР

ФГБОУ ВО "РГРТУ", РГРТУ, Корячко Алексей Вячеславович, Проректор по учебной работе
29.11.2022 10:42 (MSK), Простая подпись