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

Криптографические средства защиты информации

рабочая программа дисциплины (модуля)

Закреплена за кафедрой **Информационной безопасности**
Учебный план 10.05.01 _20_00.plx
10.05.01 - КОМПЬЮТЕРНАЯ БЕЗОПАСНОСТЬ

Квалификация **специалист по защите информации**
Форма обучения **очная**
Общая трудоемкость **2 ЗЕТ**

Распределение часов дисциплины по семестрам

Семестр (<Курс>.<Семестр на курсе>)	**7 (4.1)**		Итого	
Недель	16			
Вид занятий	УП	РП	УП	РП
Лекции	32	32	32	32
Иная контактная работа	0,25	0,25	0,25	0,25
Итого ауд.	32,25	32,25	32,25	32,25
Контактная работа	32,25	32,25	32,25	32,25
Сам. работа	31	31	31	31
Часы на контроль	8,75	8,75	8,75	8,75
Итого	72	72	72	72

г. Рязань

Программу составил(и):
ст. преп., Калинкина Татьяна Ивановна

Рабочая программа дисциплины
Криптографические средства защиты информации
разработана в соответствии с ФГОС ВО:
ФГОС ВО - специалитет по специальности 10.05.01 Компьютерная безопасность (приказ Минобрнауки России от 26.11.2020 г. № 1459)
составлена на основании учебного плана:
10.05.01 КОМПЬЮТЕРНАЯ БЕЗОПАСНОСТЬ
утвержденного учёным советом вуза от 28.01.2022 протокол № 6.

Рабочая программа одобрена на заседании кафедры
Информационной безопасности
Протокол от 29.06.2022 г. № 12
Срок действия программы: 2020-2026 уч.г.
Зав. кафедрой Пржегорлинский Виктор Николаевич

Визирование РПД для исполнения в очередном учебном году

Рабочая программа пересмотрена, обсуждена и одобрена для исполнения в 2023-2024 учебном году на заседании кафедры
Информационной безопасности

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
Информационной безопасности

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
Информационной безопасности

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
Информационной безопасности

Протокол от __ _____ 2026 г. № __

Зав. кафедрой _____

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)	
1.1	Целью изучения дисциплины является обучение студентов методам и механизмам, лежащим в основе построения современных криптографических средств защиты информации, основам построения современных криптографических систем и практическому использованию криптографических средств защиты информации.

2. МЕСТО ДИСЦИПЛИНЫ (МОДУЛЯ) В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ	
Цикл (раздел) ОП:	ФТД.О
2.1	**Требования к предварительной подготовке обучающегося:**
2.2	**Дисциплины (модули) и практики, для которых освоение данной дисциплины (модуля) необходимо как предшествующее:**
2.2.1	Криптографические протоколы
2.2.2	Практика по получению профессиональных умений и опыта профессиональной деятельности
2.2.3	Производственная практика
2.2.4	Подготовка к процедуре защиты и процедура защиты выпускной квалификационной работы
2.2.5	Преддипломная практика

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

ОПК-10: Способен анализировать тенденции развития методов и средств криптографической защиты информации, использовать средства криптографической защиты информации при решении задач профессиональной деятельности;

ОПК-10.3. Применяет алгоритмы функционирования криптографических систем

Знать
основные виды симметричных и асимметричных криптографических алгоритмов,математические модели шифров, постулаты и правила BAN-логики
Уметь
корректно применять симметричные и асимметричные криптографические алгоритмы, применять постулаты и правила BAN-логики
Владеть
криптографической терминологией, анализом работы криптографических протоколов с использованием постулатов и правил BAN-логики

ОПК-10.4. Применяет алгоритмы функционирования электронной подписи

Знать
методы криптографической защиты информации, используемые в криптографическом протоколе
Уметь
определять методы криптографической защиты информации, используемые в криптографическом протоколе
Владеть
навыками анализа методов криптографической защиты информации, используемых в криптографическом протоколе

В результате освоения дисциплины (модуля) обучающийся должен

3.1	**Знать:**
3.1.1	современные криптографические протоколы
3.2	**Уметь:**
3.2.1	настраивать криптографические протоколы при сетевом взаимодействии
3.3	**Владеть:**
3.3.1	навыками использования криптографических протоколов в средствах криптографической защиты информации

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Код занятия	Наименование разделов и тем /вид занятия/	Семестр / Курс	Часов	Компетен-ции	Литература	Форма контроля
	Раздел 1. Введение					
1.1	Введение /Тема/	7	0			

1.2	Основные понятия и определения. Основные этапы развития криптографии. Становление криптографии как науки. Применение методов криптографии в современной деятельности человека /Лек/	7	2	ОПК-10.3-З ОПК-10.3-У ОПК-10.3-В ОПК-10.4-З ОПК-10.4-У ОПК-10.4-В	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л1.7 Л1.8 Л1.9 Л1.10 Л1.11 Л1.12 Л1.13 Л1.14 Л1.15 Л1.16 Л1.17 Л1.18Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Л2.7 Л2.8 Л2.9 Л2.10 Л2.11 Л2.12 Л2.13Л3.1 Л3.2 Л3.3 Л3.4 Л3.5 Л3.6 Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8	Конспект лекций.
1.3	Изучение литературы и конспекта лекций /Ср/	7	2	ОПК-10.3-З ОПК-10.3-У ОПК-10.3-В ОПК-10.4-З ОПК-10.4-У ОПК-10.4-В	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л1.7 Л1.8 Л1.9 Л1.10 Л1.11 Л1.12 Л1.14 Л1.15 Л1.16 Л1.17 Л1.18Л2.1 Л2.3 Л2.5 Л2.7 Л2.8 Л2.9 Л2.10 Л2.11 Л2.12 Л2.13Л3.1 Л3.2 Л3.3 Л3.4 Л3.5 Л3.6 Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8	Подготовка конспекта по вопросам темы. Краткий опрос по теме на консультации к зачету.
	Раздел 2. Стандарты информационной безопасности					
2.1	Международные стандарты информационной безопасности /Тема/	7	0			
2.2	Международные стандарты по информационной безопасности. /Лек/	7	2	ОПК-10.3-З ОПК-10.3-У ОПК-10.3-В ОПК-10.4-З ОПК-10.4-У ОПК-10.4-В	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л1.7 Л1.8 Л1.9 Л1.10 Л1.11 Л1.12 Л1.14 Л1.15 Л1.16 Л1.17 Л1.18Л2.1 Л2.3 Л2.5 Л2.7 Л2.8 Л2.9 Л2.10 Л2.11 Л2.12 Л2.13Л3.1 Л3.2 Л3.3 Л3.4 Л3.5 Л3.6 Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8	Конспект лекций.

2.3	Изучение литературы и конспекта лекций /Ср/	7	2	ОПК-10.3-З ОПК-10.3-У ОПК-10.3-В ОПК-10.4-З ОПК-10.4-У ОПК-10.4-В	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л1.7 Л1.8 Л1.9 Л1.10 Л1.11 Л1.12 Л1.14 Л1.15 Л1.16 Л1.17 Л1.18Л2.1 Л2.3 Л2.5 Л2.7 Л2.8 Л2.9 Л2.10 Л2.11 Л2.12 Л2.13Л3.1 Л3.2 Л3.3 Л3.4 Л3.5 Л3.6 Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8	Подготовка конспекта по вопросам темы. Краткий опрос по теме на консультации к зачету.
2.4	Российские стандарты информационной безопасности /Тема/	7	0			
2.5	Российские нормативно-правовые документы по защите информации. /Лек/	7	2	ОПК-10.3-З ОПК-10.3-У ОПК-10.3-В ОПК-10.4-З ОПК-10.4-У ОПК-10.4-В	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л1.7 Л1.8 Л1.9 Л1.10 Л1.11 Л1.12 Л1.14 Л1.15 Л1.16 Л1.17 Л1.18Л2.1 Л2.3 Л2.5 Л2.7 Л2.8 Л2.9 Л2.10 Л2.11 Л2.12 Л2.13Л3.1 Л3.2 Л3.3 Л3.4 Л3.5 Л3.6 Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8	Конспект лекций.
2.6	Российские нормативно-правовые документы по криптографической защите информации /Лек/	7	2	ОПК-10.3-З ОПК-10.3-У ОПК-10.3-В ОПК-10.4-З ОПК-10.4-У ОПК-10.4-В	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л1.7 Л1.8 Л1.9 Л1.10 Л1.11 Л1.12 Л1.14 Л1.15 Л1.16 Л1.17 Л1.18Л2.1 Л2.3 Л2.5 Л2.7 Л2.8 Л2.9 Л2.10 Л2.11 Л2.12 Л2.13Л3.1 Л3.2 Л3.3 Л3.4 Л3.5 Л3.6 Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8	Конспект лекций.

2.7	Изучение литературы и конспекта лекций /Ср/	7	4	ОПК-10.3-З ОПК-10.3-У ОПК-10.3-В ОПК-10.4-З ОПК-10.4-У ОПК-10.4-В	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л1.7 Л1.8 Л1.9 Л1.10 Л1.11 Л1.12 Л1.14 Л1.15 Л1.16 Л1.17 Л1.18Л2.1 Л2.3 Л2.5 Л2.7 Л2.8 Л2.9 Л2.10 Л2.11 Л2.12 Л2.13Л3.1 Л3.2 Л3.3 Л3.4 Л3.5 Л3.6 Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8	Подготовка конспекта по вопросам темы. Краткий опрос по теме на консультации к зачету.
	Раздел 3. Криптографическая защита информации					
3.1	Криптографические системы /Тема/	7	0			
3.2	Симметричные и ассиметричные криптосистемы /Лек/	7	2	ОПК-10.3-З ОПК-10.3-У ОПК-10.3-В ОПК-10.4-З ОПК-10.4-У ОПК-10.4-В	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л1.7 Л1.8 Л1.9 Л1.10 Л1.11 Л1.12 Л1.14 Л1.15 Л1.16 Л1.17 Л1.18Л2.1 Л2.3 Л2.5 Л2.7 Л2.8 Л2.9 Л2.10 Л2.11 Л2.12 Л2.13Л3.1 Л3.2 Л3.3 Л3.4 Л3.5 Л3.6 Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8	Конспект лекций.
3.3	Изучение литературы и конспекта лекций. /Ср/	7	2	ОПК-10.3-З ОПК-10.3-У ОПК-10.3-В ОПК-10.4-З ОПК-10.4-У ОПК-10.4-В	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л1.7 Л1.8 Л1.9 Л1.10 Л1.11 Л1.12 Л1.14 Л1.15 Л1.16 Л1.17 Л1.18Л2.1 Л2.3 Л2.5 Л2.7 Л2.8 Л2.9 Л2.10 Л2.11 Л2.12 Л2.13Л3.1 Л3.2 Л3.3 Л3.4 Л3.5 Л3.6 Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8	Подготовка конспекта по вопросам темы. Краткий опрос по теме на консультации к зачету.
3.4	Электронная подпись /Тема/	7	0			

3.5	Инфраструктура открытых ключей PKI. /Лек/	7	2	ОПК-10.3-З ОПК-10.3-У ОПК-10.3-В ОПК-10.4-З ОПК-10.4-У ОПК-10.4-В	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л1.7 Л1.8 Л1.9 Л1.10 Л1.11 Л1.12 Л1.14 Л1.15 Л1.16 Л1.17 Л1.18Л2.1 Л2.3 Л2.5 Л2.7 Л2.8 Л2.9 Л2.10 Л2.11 Л2.12 Л2.13Л3.1 Л3.2 Л3.3 Л3.4 Л3.5 Л3.6 Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8	Конспект лекций.
3.6	Электронная подпись и ее применение /Лек/	7	2	ОПК-10.3-З ОПК-10.3-У ОПК-10.3-В ОПК-10.4-З ОПК-10.4-У ОПК-10.4-В	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л1.7 Л1.8 Л1.9 Л1.10 Л1.11 Л1.12 Л1.14 Л1.15 Л1.16 Л1.17 Л1.18Л2.1 Л2.3 Л2.5 Л2.7 Л2.8 Л2.9 Л2.10 Л2.11 Л2.12 Л2.13Л3.1 Л3.2 Л3.3 Л3.4 Л3.5 Л3.6 Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8	Конспект лекций.
3.7	Технологии аутентификации /Лек/	7	2	ОПК-10.3-З ОПК-10.3-У ОПК-10.3-В ОПК-10.4-З ОПК-10.4-У ОПК-10.4-В	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л1.7 Л1.8 Л1.9 Л1.10 Л1.11 Л1.12 Л1.14 Л1.15 Л1.16 Л1.17 Л1.18Л2.1 Л2.3 Л2.5 Л2.7 Л2.8 Л2.9 Л2.10 Л2.11 Л2.12 Л2.13Л3.1 Л3.2 Л3.3 Л3.4 Л3.5 Л3.6 Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8	Конспект лекций.

3.8	Изучение литературы и конспекта лекций /Ср/	7	8	ОПК-10.3-З ОПК-10.3-У ОПК-10.3-В ОПК-10.4-З ОПК-10.4-У ОПК-10.4-В	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л1.7 Л1.8 Л1.9 Л1.10 Л1.11 Л1.12 Л1.14 Л1.15 Л1.16 Л1.17 Л1.18Л2.1 Л2.3 Л2.5 Л2.7 Л2.8 Л2.9 Л2.10 Л2.11 Л2.12 Л2.13Л3.1 Л3.2 Л3.3 Л3.4 Л3.5 Л3.6 Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8	Подготовка конспекта по вопросам темы. Краткий опрос по теме на консультации к зачету.
	Раздел 4. Средства криптографической защиты информации					
4.1	Средства шифрования информации на жестких дисках /Тема/	7	0			
4.2	Средство шифрования информации на жестких дисках Secret Disk /Лек/	7	4	ОПК-10.3-З ОПК-10.3-У ОПК-10.3-В ОПК-10.4-З ОПК-10.4-У ОПК-10.4-В	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л1.7 Л1.8 Л1.9 Л1.10 Л1.11 Л1.12 Л1.14 Л1.15 Л1.16 Л1.17 Л1.18Л2.1 Л2.3 Л2.5 Л2.7 Л2.8 Л2.9 Л2.10 Л2.11 Л2.12 Л2.13Л3.1 Л3.2 Л3.3 Л3.4 Л3.5 Л3.6 Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8	Конспект лекций.
4.3	Изучение литературы и конспекта лекций /Ср/	7	2	ОПК-10.3-З ОПК-10.3-У ОПК-10.3-В ОПК-10.4-З ОПК-10.4-У ОПК-10.4-В	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л1.7 Л1.8 Л1.9 Л1.10 Л1.11 Л1.12 Л1.14 Л1.15 Л1.16 Л1.17 Л1.18Л2.1 Л2.3 Л2.5 Л2.7 Л2.8 Л2.9 Л2.10 Л2.11 Л2.12 Л2.13Л3.1 Л3.2 Л3.3 Л3.4 Л3.5 Л3.6 Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8	Подготовка конспекта по вопросам темы. Краткий опрос по теме на консультации к зачету.
4.4	Средства шифрования при передаче информации в вычислительных сетях /Тема/	7	0			

4.5	Средство защиты информации СКЗИ КриптоПроCSP /Лек/	7	4	ОПК-10.3-З ОПК-10.3-У ОПК-10.3-В ОПК-10.4-З ОПК-10.4-У ОПК-10.4-В	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л1.7 Л1.8 Л1.9 Л1.10 Л1.11 Л1.12 Л1.14 Л1.15 Л1.16 Л1.17 Л1.18Л2.1 Л2.3 Л2.5 Л2.7 Л2.8 Л2.9 Л2.10 Л2.11 Л2.12 Л2.13Л3.1 Л3.2 Л3.3 Л3.4 Л3.5 Л3.6 Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8	Конспект лекций.
4.6	Продукты серии VipNet /Лек/	7	4	ОПК-10.3-З ОПК-10.3-У ОПК-10.3-В ОПК-10.4-З ОПК-10.4-У ОПК-10.4-В	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л1.7 Л1.8 Л1.9 Л1.10 Л1.11 Л1.12 Л1.14 Л1.15 Л1.16 Л1.17 Л1.18Л2.1 Л2.3 Л2.5 Л2.7 Л2.8 Л2.9 Л2.10 Л2.11 Л2.12 Л2.13Л3.1 Л3.2 Л3.3 Л3.4 Л3.5 Л3.6 Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8	Конспект лекций.
4.7	Межсетевые экраны. СКЗИ «Континент». /Лек/	7	4	ОПК-10.3-З ОПК-10.3-У ОПК-10.3-В ОПК-10.4-З ОПК-10.4-У ОПК-10.4-В	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л1.7 Л1.8 Л1.9 Л1.10 Л1.11 Л1.12 Л1.14 Л1.15 Л1.16 Л1.17 Л1.18Л2.1 Л2.3 Л2.5 Л2.7 Л2.8 Л2.9 Л2.10 Л2.11 Л2.12 Л2.13Л3.1 Л3.2 Л3.3 Л3.4 Л3.5 Л3.6 Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8	Конспект лекций.

4.8	Изучение литературы и конспекта лекций. /Ср/	7	11	ОПК-10.3-З ОПК-10.3-У ОПК-10.3-В ОПК-10.4-З ОПК-10.4-У ОПК-10.4-В	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л1.7 Л1.8 Л1.9 Л1.10 Л1.11 Л1.12 Л1.14 Л1.15 Л1.16 Л1.17 Л1.18Л2.1 Л2.3 Л2.5 Л2.7 Л2.8 Л2.9 Л2.10 Л2.11 Л2.12 Л2.13Л3.1 Л3.2 Л3.3 Л3.4 Л3.5 Л3.6 Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8	Подготовка конспекта по вопросам темы. Краткий опрос по теме на консультации к зачету.
	Раздел 5. Иная контактная работа					
5.1	Иная контактная работа /Тема/	7	0			
5.2	Прием зачета. /ИКР/	7	0,25	ОПК-10.3-З ОПК-10.3-У ОПК-10.3-В ОПК-10.4-З ОПК-10.4-У ОПК-10.4-В	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л1.7 Л1.8 Л1.9 Л1.10 Л1.11 Л1.12 Л1.14 Л1.15 Л1.16 Л1.17 Л1.18Л2.1 Л2.3 Л2.5 Л2.7 Л2.8 Л2.9 Л2.10 Л2.11 Л2.12 Л2.13Л3.1 Л3.2 Л3.3 Л3.4 Л3.5 Л3.6	Ответы на Контрольные вопросы. Ответы на дополнительные вопросы. Результаты тестирования.
	Раздел 6. Контроль					
6.1	Подготовка к зачету, зачет /Тема/	7	0			
6.2	Подготовка к зачету. /Зачёт/	7	8,75	ОПК-10.3-З ОПК-10.3-У ОПК-10.3-В ОПК-10.4-З ОПК-10.4-У ОПК-10.4-В	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л1.7 Л1.8 Л1.9 Л1.10 Л1.11 Л1.12 Л1.14 Л1.15 Л1.16 Л1.17 Л1.18Л2.1 Л2.3 Л2.5 Л2.7 Л2.8 Л2.9 Л2.10 Л2.11 Л2.12 Л2.13Л3.1 Л3.2 Л3.3 Л3.4 Л3.5 Л3.6	Билеты к зачету. Тесты к зачету.

5. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ПО ДИСЦИПЛИНЕ (МОДУЛЮ)

Оценочные материалы приведены в приложении к рабочей программе дисциплины (см. документ "Оценочные материалы по дисциплине "Криптографические средства защиты 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	Калмыков И. А., Науменко Д. О., Гиш Т. А.	Криптографические методы защиты информации : лабораторный практикум	Ставрополь: Северо-Кавказский федеральный университет, 2015, 109 с.	2227-8397, http://www.iprbookshop.ru/63099.html
Л1.2	Алферов А.П., Зубов А.Ю., Кузьмин А.С., Черемушкин А.В.	Основы криптографии : Учеб.пособие	М.:Гелиос АРВ, 2001, 479с.	5-85438-019-6, 20
Л1.3	Соколов А.В., Шаньгин В.Ф.	Защита информации в распределенных корпоративных сетях и системах	М.:ДМК Пресс, 2002, 655с.	5-94074-172-X, 20
Л1.4	Дшхунян В.Л., Шаньгин В.Ф.	Электронная идентификация. Бесконтактные электронные идентификаторы и смарт-карты	М.: АСТ, 2004, 696с.; прил.	5-17-026327-9, 20
Л1.5	Фомина К.Ю., Кураксин В.А.	Методы и средства защиты информации : метод. указ. к лаб. работам	Рязань, 2018, 48с.; прил.	, 20
Л1.6	Титов А. А.	Инженерно-техническая защита информации	Москва: ТУСУ, 2010, 197 с.	, http://e.lanbook.com/books/element.php?pl1_cid=25&pl1_id=4959
Л1.7	Фомин Д. В.	Информационная безопасность и защита информации: специализированные аттестованные программные и программно-аппаратные средства	Благовещенск: АмГУ, 2017, 240 с.	, https://e.lanbook.com/book/156494
Л1.8	Костин, В. Н.	Методы и средства защиты компьютерной информации: аппаратные и программные средства защиты информации : учебное пособие	Москва: Издательский Дом МИСиС, 2018, 21 с.	978-5-906953-22-3, http://www.iprbookshop.ru/98199.html
Л1.9	Костин, В. Н.	Методы и средства защиты компьютерной информации: информационная безопасность компьютерных сетей : учебное пособие	Москва: Издательский Дом МИСиС, 2018, 31 с.	978-5-906953-53-7, http://www.iprbookshop.ru/98200.html
Л1.10	Громов Ю.Ю., Драчев В.О., Иванова О.Г., Шахов Н.Г.	Основы информационной безопасности : учеб. пособие	Старый Оскол: ТНТ, 2019, 381с.; прил.	978-5-94178-216-1, 15
Л1.11	Гатченко Н. А., Исаев А. С., Яковлев А. Д.	Криптографическая защита информации	Санкт-Петербург: Университет ИТМО, 2012, 142 с.	2227-8397, http://www.iprbookshop.ru/68658.html

№	Авторы, составители	Заглавие	Издательство, год	Количество/ название ЭБС
Л1.12	Горюхина Е. Ю., Литвинова Л. И., Ткачева Н. В.	Информационная безопасность : учебное пособие	Воронеж: Воронежский Государственный Аграрный Университет им. Императора Петра Первого, 2015, 221 с.	2227-8397, http://www.iprbookshop.ru/72672.html
Л1.13	Фомин Д. В.	Информационная безопасность : учебно-методическое пособие для студентов заочной формы обучения направления подготовки 38.03.05 «бизнес-информатика»	Саратов: Вузовское образование, 2018, 125 с.	978-5-4487-0299-0, http://www.iprbookshop.ru/77318.html
Л1.14	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
Л1.15	Шаньгин В. Ф.	Информационная безопасность и защита информации	Саратов: Профобразование, 2019, 702 с.	978-5-4488-0070-2, http://www.iprbookshop.ru/87995.html
Л1.16	Литвинов Р. В., Волегов К. А., Бацула А. П.	Технические средства защиты информации. Часть 1 : курс лекций	Томск: Томский государственный университет систем управления и радиоэлектроники, 2006, 170 с.	2227-8397, http://www.iprbookshop.ru/14027.html
Л1.17	Мартемьянов Ю. Ф., Яковлев А. В., Яковлев А. В.	Операционные системы. Концепции построения и обеспечения безопасности	Москва: Горячая линия-Телеком, 2011, 332 с.	978-5-9912-0128-5, http://e.lanbook.com/books/element.php?pl1_cid=25&pl1_id=5176
Л1.18	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, 20

6.1.2. Дополнительная литература

№	Авторы, составители	Заглавие	Издательство, год	Количество/ название ЭБС
Л2.1	Аверченков В. И.	Аудит информационной безопасности : учебное пособие для вузов	Брянск: Брянский государственный технический университет, 2012, 268 с.	978-89838-487-6, http://www.iprbookshop.ru/6991.html

№	Авторы, составители	Заглавие	Издательство, год	Количество/ название ЭБС
Л2.2	Трушин В. А., Котов Ю. А., Левин Л. С., Донской К. А.	Введение в информационную безопасность и защиту информации : учебное пособие	Новосибирск: Новосибирский государственный технический университет, 2017, 132 с.	978-5-7782-3233-4, http://www.iprbookshop.ru/91329.html
Л2.3	Котов Ю. А.	Криптографические методы защиты информации. Шифры : учебное пособие	Новосибирск: Новосибирский государственный технический университет, 2016, 59 с.	978-5-7782-2959-4, http://www.iprbookshop.ru/91377.html
Л2.4	Фороузан, Б. А., Берлина, А. Н.	Криптография и безопасность сетей : учебное пособие	Москва: Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2021, 776 с.	978-5-4497-0946-2, http://www.iprbookshop.ru/102017.html
Л2.5	Иванов, Д. А., Макаренко, М. М., Пушкарев, В. В., Русскевич, Е. А.	Расследование преступлений, совершенных с использованием криптовалюты : учебное пособие	Москва: Ай Пи Ар Медиа, 2021, 80 с.	978-5-4497-1036-9, http://www.iprbookshop.ru/107712.html
Л2.6	Аверченков В. И., Рытов М. Ю., Гайнулин Т. Р.	Защита персональных данных в организации : монография	Брянск: Брянский государственный технический университет, 2012, 124 с.	5-89838-382-4, http://www.iprbookshop.ru/6993.html
Л2.7	Аверченков В. И., Ваинмаер Е. Е.	Инновационный менеджмент : учебное пособие для вузов	Брянск: Брянский государственный технический университет, 2012, 293 с.	5-89838-134-1, http://www.iprbookshop.ru/6995.html
Л2.8	Аверченков В. И., Рытов М. Ю., Кондрашин Г. В., Рудановский М. В.	Системы защиты информации в ведущих зарубежных странах : учебное пособие для вузов	Брянск: Брянский государственный технический университет, 2012, 224 с.	978-89838-488-3, http://www.iprbookshop.ru/7007.html
Л2.9	Аверченков В. И., Ерохин В. В., Рытов М. Ю., Голембиовская О. М.	Структура системы обеспечения безопасности Российской Федерации : учебное пособие	Брянск: Брянский государственный технический университет, 2012, 140 с.	978-5-89838-503-3, http://www.iprbookshop.ru/7011.html

№	Авторы, составители	Заглавие	Издательство, год	Количество/ название ЭБС
Л2.10	Пушкарев В. П., Пушкарев В. В.	Защита информационных процессов в компьютерных системах : учебное пособие	Томск: Томский государственный университет систем управления и радиоэлектроники, 2012, 131 с.	2227-8397, http://www.iprbookshop.ru/13929.html
Л2.11	Петров С. В., Кисляков П. А.	Информационная безопасность : учебное пособие	Саратов: Ай Пи Ар Букс, 2015, 326 с.	978-5-906-17271-6, http://www.iprbookshop.ru/33857.html
Л2.12	Петров А. А.	Компьютерная безопасность. Криптографические методы защиты	Саратов: Профобразование, 2019, 446 с.	978-5-4488-0091-7, http://www.iprbookshop.ru/87998.html
Л2.13	Котов Ю. А.	Криптографические методы защиты информации. Стандартные шифры. Шифры с открытым ключом : учебное пособие	Новосибирск: Новосибирский государственный технический университет, 2017, 67 с.	978-5-7782-3411-6, http://www.iprbookshop.ru/91227.html

6.1.3. Методические разработки

№	Авторы, составители	Заглавие	Издательство, год	Количество/ название ЭБС
Л3.1	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
Л3.2	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
Л3.3	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
Л3.4	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
Л3.5	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
Л3.6	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	1. Электронно-библиотечная система «Лань». – Режим доступа: с любого компьютера РГРТУ без пароля.
Э2	2. Электронно-библиотечная система «IPRbooks». – Режим доступа: с любого компьютера РГРТУ без пароля, из сети Интернет по паролю
Э3	3. Электронная библиотека РГРТУ
Э4	4. Научная электронная библиотека eLibrary
Э5	5. Библиотека и форум по программированию
Э6	6. Национальный открытый университет ИНТУИТ
Э7	7. Информационно-справочная система
Э8	8. Научная электронная библиотека КиберЛенинка

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
Adobe Acrobat Reader	Свободное ПО
LibreOffice	Свободное ПО
7 Zip	Свободное ПО
K-Lite Codec Pack	Свободное ПО
Kaspersky Endpoint Security	Коммерческая лицензия
Операционная система Windows XP/Vista/7/8/10	Microsoft Imagine: Номер подписки 700102019, бессрочно
Операционная система Ubuntu	Свободное ПО
Microsoft Office	Коммерческая лицензия

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	264 учебно-административный корпус. учебная аудитория для проведения учебных занятий Специализированная мебель (16 посадочных мест), 5 рабочих мест (стол), магнитно-маркерная доска.
2	268 учебно-административный корпус. компьютерный класс для проведения учебных занятий Специализированная мебель (20 компьютерных столов), 20 персональных компьютеров. Возможность подключения к сети Интернет и обеспечением доступа в электронную информационно-образовательную среду РГРТУ.
3	270 учебно-административный корпус. учебная аудитория для проведения учебных занятий. Специализированная мебель (42 посадочных места), магнитно-маркерная доска. Мультимедиа проектор, 1 экран. Рабочее место (2 стола), 1 персональный компьютер, 1 ноутбук.
4	266 а учебно-административный корпус. компьютерный класс для проведения учебных занятий, самостоятельной работы обучающихся Специализированная мебель (14 компьютерных столов), 14 персональных компьютеров. Возможность подключения к сети Интернет и обеспечением доступа в электронную информационно-образовательную среду РГРТУ.

8. МЕТОДИЧЕСКИЕ МАТЕРИАЛЫ ПО ДИСЦИПЛИНЕ (МОДУЛЮ)

Методическое обеспечение дисциплины приведено в приложении к рабочей программе дисциплины (см. документ "Методические указания дисциплины "Криптографические средства защиты информации")