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 протоколы

рабочая программа дисциплины (модуля)

Закреплена за кафедрой **Информационной безопасности**
Учебный план 10.05.01 _23_00.plx
10.05.01 - КОМПЬЮТЕРНАЯ БЕЗОПАСНОСТЬ

Квалификация **специалист по защите информации**
Форма обучения **очная**
Общая трудоемкость **4 ЗЕТ**

Распределение часов дисциплины по семестрам

Семестр (<Курс>.<Семестр на курсе>)	**9 (5.1)**		Итого	
Недель	16			
Вид занятий	УП	РП	УП	РП
Лекции	32	32	32	32
Практические	32	32	32	32
Иная контактная работа	0,25	0,25	0,25	0,25
Итого ауд.	64,25	64,25	64,25	64,25
Контактная работа	64,25	64,25	64,25	64,25
Сам. работа	62	62	62	62
Часы на контроль	17,75	17,75	17,75	17,75
Итого	144	144	144	144

г. Рязань

Программу составил(и):
ст. преп., Калинкина Т.И.

Рабочая программа дисциплины

Криптографические протоколы

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 28.04.2023 протокол № 11.

Рабочая программа одобрена на заседании кафедры

Информационной безопасности

Протокол от 05.07.2023 г. № 12
Срок действия программы: 2023-2029 уч.г.
Зав. кафедрой Пржегорлинский Виктор Николаевич

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 _____

Визирование РПД для исполнения в очередном учебном году

Рабочая программа пересмотрена, обсуждена и одобрена для исполнения в 2027-2028 учебном году на заседании кафедры
Информационной безопасности

Протокол от __ _____ 2027 г. № __

Зав. кафедрой _____

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)	
1.1	теоретическая и практическая подготовка специалистов к деятельности, связанной с анализом, синтезом и использованием для защиты информации криптографических протоколов.
1.2	

2. МЕСТО ДИСЦИПЛИНЫ (МОДУЛЯ) В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ	
Цикл (раздел) ОП:	Б1.О
2.1	**Требования к предварительной подготовке обучающегося:**
2.1.1	Методы и средства криптографической защиты информации
2.1.2	Криптографические средства защиты информации
2.2	**Дисциплины (модули) и практики, для которых освоение данной дисциплины (модуля) необходимо как предшествующее:**
2.2.1	Практика по получению профессиональных умений и опыта профессиональной деятельности
2.2.2	Производственная практика
2.2.3	Подготовка к процедуре защиты и процедура защиты выпускной квалификационной работы
2.2.4	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. Осуществляет анализ работы криптографических протоколов с использованием BAN - логики

Знать
постулаты и правила BAN-логики
Уметь
применять постулаты и правила BAN-логики
Владеть
анализом работы криптографических протоколов с использованием постулатов и правил BAN-логики

ОПК-10.4. Проводит анализ методов криптографической защиты информации, используемых в криптографическом протоколе

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

ОПК-10.6. Настраивает современные криптографические протоколы при сетевом взаимодействии

Знать
принципы работы современных криптографических протоколов при сетевом взаимодействии
Уметь
производить установку, наладку, тестирование и обслуживание криптографических протоколов при сетевом взаимодействии
Владеть

В результате освоения дисциплины (модуля) обучающийся должен

3.1	**Знать:**
3.1.1	современные криптографические протоколы
3.2	**Уметь:**
3.2.1	уметь настраивать криптографические протоколы при сетевом взаимодействии
3.3	**Владеть:**
3.3.1	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/	9	0			

1.2	Основные понятия и определения. Функции — сервисы безопасности. Понятие криптографического протокола. Конфиденциальность Целостность. Аутентификация. Невозможность отказа от авторства (электронная подпись) /Лек/	9	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 ОПК-10.6-З ОПК-10.6-У ОПК-10.6-В	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л1.7 Л1.8Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Л2.7Л3.1 Л3.2 Л3.4 Л3.5 Э1 Э2 Э3 Э5 Э6 Э7 Э8	Конспект лекций.
1.3	Изучение литературы и конспекта лекций /Ср/	9	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 ОПК-10.6-З ОПК-10.6-У ОПК-10.6-В	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л1.7 Л1.8Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Л2.7Л3.1 Л3.2 Л3.4 Л3.5 Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8	Подготовка конспекта по вопросам темы. Краткий опрос по теме на консультации к зачету.
	Раздел 2. Общие сведения о криптографических протоколах					
2.1	Безопасность криптографических протоколов /Тема/	9	0			
2.2	Свойства, характеризующие безопасность протоколов. Основные атаки на безопасность протоколов /Лек/	9	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 ОПК-10.6-З ОПК-10.6-У ОПК-10.6-В	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л1.7 Л1.8Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Л2.7Л3.1 Л3.2 Л3.3 Л3.4 Л3.5 Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8	Конспект лекций.
2.3	Изучение литературы, конспекта лекций. /Ср/	9	1	ОПК-10.3-З ОПК-10.3-У ОПК-10.3-В ОПК-10.4-З ОПК-10.4-У ОПК-10.4-В ОПК-10.6-З ОПК-10.6-У ОПК-10.6-В	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л1.7 Л1.8Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Л2.7Л3.1 Л3.2 Л3.4 Л3.5 Э1 Э2 Э3 Э5 Э6 Э7	Подготовка конспекта по вопросам темы. Краткий опрос по теме на консультации к зачету.
2.4	Виды криптографических протоколов /Тема/	9	0			

2.5	Основные виды криптографических протоколовФормальные методы анализа криптопротоколов /Лек/	9	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 ОПК-10.6-З ОПК-10.6-У ОПК-10.6-В	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л1.7 Л1.8Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Л2.7Л3.1 Л3.2 Л3.4 Л3.5 Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8	Конспект лекций.
2.6	Изучение литературы, конспекта лекций и подготовка к практической работе /Ср/	9	3	ОПК-10.3-З ОПК-10.3-У ОПК-10.3-В ОПК-10.4-З ОПК-10.4-У ОПК-10.4-В ОПК-10.6-З ОПК-10.6-У ОПК-10.6-В	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л1.7 Л1.8Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Л2.7Л3.1 Л3.2 Л3.4 Л3.5 Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8	Подготовка конспекта по вопросам темы. Краткий опрос по теме на консультации к зачету.
2.7	Методы анализа криптопротоколов /Пр/	9	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 ОПК-10.6-З ОПК-10.6-У ОПК-10.6-В	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л1.7 Л1.8Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Л2.7Л3.1 Л3.2 Л3.4 Л3.5 Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8	Устный опрос по теме. Решение задач. Проверка домашнего задания.
	Раздел 3. Криптографические хеш-функции и коды аутентификации					
3.1	Криптографические хеш-функции. /Тема/	9	0			
3.2	Требования к криптографическим хеш-функциям. Бесключевые хеш-функции. /Лек/	9	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 ОПК-10.6-З ОПК-10.6-У ОПК-10.6-В	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л1.7 Л1.8Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Л2.7Л3.1 Л3.2 Л3.4 Л3.5 Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8	Конспект лекций.

3.3	Основы построения хеш-функций. Хеш-функция на основе блочного алгоритма. Хеш-функция MD4 и MD5 /Лек/	9	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 ОПК-10.6-З ОПК-10.6-У ОПК-10.6-В	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л1.7 Л1.8Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Л2.7Л3.1 Л3.2 Л3.4 Л3.5 Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8	Конспект лекций.
3.4	Стандарты на хеш-функции. Хеш-функции, задаваемые ключом. /Лек/	9	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 ОПК-10.6-З ОПК-10.6-У ОПК-10.6-В	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л1.7 Л1.8Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Л2.7Л3.1 Л3.2 Л3.4 Л3.5 Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8	Конспект лекций.
3.5	Изучение литературы, конспекта лекций и подготовка к практической работе /Ср/	9	10	ОПК-10.3-З ОПК-10.3-У ОПК-10.3-В ОПК-10.4-З ОПК-10.4-У ОПК-10.4-В ОПК-10.6-З ОПК-10.6-У ОПК-10.6-В	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л1.7 Л1.8Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Л2.7Л3.1 Л3.2 Л3.4 Л3.5 Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8	Подготовка конспекта по вопросам темы. Краткий опрос по теме на консультации к зачету.
3.6	Криптографические хеш-функции /Пр/	9	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 ОПК-10.6-З ОПК-10.6-У ОПК-10.6-В	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л1.7 Л1.8Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Л2.7Л3.1 Л3.2 Л3.4 Л3.5 Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8	Устный опрос по теме. Решение задач. Проверка домашнего задания.
3.7	Коды аутентификации /Тема/	9	0			
3.8	Коды аутентификации сообщений – MAC. /Лек/	9	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 ОПК-10.6-З ОПК-10.6-У ОПК-10.6-В	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л1.7 Л1.8Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Л2.7Л3.1 Л3.2 Л3.4 Л3.5	Конспект лекций.

3.9	Изучение литературы, конспекта лекций и подготовка к практической работе /Ср/	9	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 ОПК-10.6-З ОПК-10.6-У ОПК-10.6-В	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л1.7 Л1.8Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Л2.7Л3.1 Л3.2 Л3.4 Л3.5	Подготовка конспекта по вопросам темы. Краткий опрос по теме на консультации к зачету.
3.10	Коды аутентификации. /Пр/	9	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 ОПК-10.6-З ОПК-10.6-У ОПК-10.6-В	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л1.7 Л1.8Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Л2.7Л3.1 Л3.2 Л3.4 Л3.5	Устный опрос по теме. Решение задач. Проверка домашнего задания.
	Раздел 4. Схемы электронных подписей					
4.1	Алгоритмы электронных подписей /Тема/	9	0			
4.2	Определение схемы электронной подписи. Алгоритм цифровой подписи RSA /Лек/	9	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 ОПК-10.6-З ОПК-10.6-У ОПК-10.6-В	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л1.7 Л1.8Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Л2.7Л3.1 Л3.2 Л3.4 Л3.5 Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8	Конспект лекций.
4.3	Изучение конспекта лекций. /Ср/	9	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 ОПК-10.6-З ОПК-10.6-У ОПК-10.6-В	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л1.7 Л1.8Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Л2.7Л3.1 Л3.2 Л3.4 Л3.5 Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8	Подготовка конспекта по вопросам темы. Краткий опрос по теме на консультации к зачету.
4.4	Семейство схем типа Эль-Гамаля. Схема подписи Fiat-Shamir /Лек/	9	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 ОПК-10.6-З ОПК-10.6-У ОПК-10.6-В	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л1.7 Л1.8Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Л2.7Л3.1 Л3.2 Л3.4 Л3.5 Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8	Конспект лекций.

4.5	Инфраструктура открытых ключей PKI. Рекомендации X.509. /Лек/	9	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 ОПК-10.6-З ОПК-10.6-У ОПК-10.6-В	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л1.7 Л1.8Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Л2.7Л3.1 Л3.2 Л3.4 Л3.5 Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8	Конспект лекций.
4.6	Электронные подписи с дополнительными функциональными свойствами /Ср/	9	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 ОПК-10.6-З ОПК-10.6-У ОПК-10.6-В	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л1.7 Л1.8Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Л2.7Л3.1 Л3.2 Л3.4 Л3.5 Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8	Подготовка конспекта по вопросам темы. Краткий опрос по теме на консультации к зачету.
4.7	Подготовка к практическим занятиям /Ср/	9	10	ОПК-10.3-З ОПК-10.3-У ОПК-10.3-В ОПК-10.4-З ОПК-10.4-У ОПК-10.4-В ОПК-10.6-З ОПК-10.6-У ОПК-10.6-В	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л1.7 Л1.8Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Л2.7Л3.1 Л3.2 Л3.4 Л3.5 Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8	Подготовка конспекта по вопросам темы. Краткий опрос по теме на консультации к зачету.
4.8	Электронные подписи типа Эль-Гамаля. Схема подписи Fiat-Shamir. Электронные подписи с дополнительными функциональными свойствами. /Пр/	9	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 ОПК-10.6-З ОПК-10.6-У ОПК-10.6-В	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л1.7 Л1.8Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Л2.7Л3.1 Л3.2 Л3.4 Л3.5 Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8	Устный опрос по теме. Решение задач. Проверка домашнего задания.
	Раздел 5. Протоколы идентификации и аутентификации					
5.1	Протоколы аутентификации. /Тема/	9	0			

5.2	Протоколы аутентификации на основе паролей. /Лек/	9	1	ОПК-10.3-З ОПК-10.3-У ОПК-10.3-В ОПК-10.4-З ОПК-10.4-У ОПК-10.4-В ОПК-10.6-З ОПК-10.6-У ОПК-10.6-В	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л1.7 Л1.8Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Л2.7Л3.1 Л3.2 Л3.4 Л3.5 Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8	Конспект лекций.
5.3	Протоколы аутентификации на основе паролей. /Пр/	9	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 ОПК-10.6-З ОПК-10.6-У ОПК-10.6-В	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л1.7 Л1.8Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Л2.7Л3.1 Л3.2 Л3.4 Л3.5 Э1 Э2 Э3 Э5 Э6 Э7 Э8	Устный опрос по теме. Решение задач. Проверка домашнего задания.
5.4	Изучение литературы, конспекта лекций и подготовка к практической работе. /Ср/	9	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 ОПК-10.6-З ОПК-10.6-У ОПК-10.6-В	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л1.7 Л1.8Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Л2.7Л3.1 Л3.2 Л3.4 Л3.5 Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8	Подготовка конспекта по вопросам темы. Краткий опрос по теме на консультации к зачету.
5.5	Протоколы идентификации. /Тема/	9	0			
5.6	Протоколы идентификации типа «запрос-ответ» и рукопожатие. Понятие проколов интерактивного доказательства и доказательства знания. /Лек/	9	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 ОПК-10.6-З ОПК-10.6-У ОПК-10.6-В	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л1.7 Л1.8Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Л2.7Л3.1 Л3.2 Л3.4 Л3.5	Конспект лекций.
5.7	Протоколы с нулевым разглашением. Протоколы Фиата-Шамира, Гиллу-Кискатра и Шнорра. Протоколы с самосертифицируемыми ключами /Лек/	9	3	ОПК-10.3-З ОПК-10.3-У ОПК-10.3-В ОПК-10.4-З ОПК-10.4-У ОПК-10.4-В ОПК-10.6-З ОПК-10.6-У ОПК-10.6-В	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л1.7 Л1.8Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Л2.7Л3.1 Л3.2 Л3.4 Л3.5	Конспект лекций.

5.8	Протоколы идентификации типа «запрос-ответ» и рукопожатие. Протоколы с самосертифицируемыми ключами /Пр/	9	6	ОПК-10.3-З ОПК-10.3-У ОПК-10.3-В ОПК-10.4-З ОПК-10.4-У ОПК-10.4-В ОПК-10.6-З ОПК-10.6-У ОПК-10.6-В	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л1.7 Л1.8Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Л2.7Л3.1 Л3.2 Л3.4 Л3.5	Устный опрос по теме. Решение задач. Проверка домашнего задания.
5.9	Изучение литературы, конспекта лекций и подготовка к практической работе /Ср/	9	10	ОПК-10.3-З ОПК-10.3-У ОПК-10.3-В ОПК-10.4-З ОПК-10.4-У ОПК-10.4-В ОПК-10.6-З ОПК-10.6-У ОПК-10.6-В	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л1.7 Л1.8Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Л2.7Л3.1 Л3.2 Л3.4 Л3.5	Подготовка конспекта по вопросам темы. Краткий опрос по теме на консультации к зачету.
	Раздел 6. Протоколы распределения ключей					
6.1	Протоколы передачи ключей /Тема/	9	0			
6.2	Протоколы генерации и передачи ключей. Примеры протоколов передачи ключей на основе симметричного и открытого шифрования. Двух и трех сторонние протоколы, Kerberos. Функции доверенной третьей стороны. Передача ключей с исполь-зованием асимметричного шифрования. /Лек/	9	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 ОПК-10.6-З ОПК-10.6-У ОПК-10.6-В	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л1.7 Л1.8Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Л2.7Л3.1 Л3.2 Л3.4 Л3.5 Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8	Конспект лекций.
6.3	Двух и трех сторонние протоколы, Ker-beros. Функции доверенной третьей стороны. /Пр/	9	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 ОПК-10.6-З ОПК-10.6-У ОПК-10.6-В	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л1.7 Л1.8Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Л2.7Л3.1 Л3.2 Л3.4 Л3.5 Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8	Устный опрос по теме. Решение задач. Проверка домашнего задания.
6.4	Изучение литературы, конспекта лекций и подготовка к практической работе. /Ср/	9	7	ОПК-10.3-З ОПК-10.3-У ОПК-10.3-В ОПК-10.4-З ОПК-10.4-У ОПК-10.4-В ОПК-10.6-З ОПК-10.6-У ОПК-10.6-В	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л1.7 Л1.8Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Л2.7Л3.1 Л3.2 Л3.4 Л3.5 Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8	Подготовка конспекта по вопросам темы. Краткий опрос по теме на консультации к зачету.

6.5	Протоколы распределения ключей /Тема/	9	0			
6.6	Открытое распределение ключей. Протокол Диффи-Хеллмана и его модификации. Схемы предварительного распределения ключей. Групповые протоколы. Протоколы разделения секрета и распределения ключей для конференцсвязи. Способы установления ключей для конференцсвязи. /Лек/	9	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 ОПК-10.6-З ОПК-10.6-У ОПК-10.6-В	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л1.7 Л1.8Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Л2.7Л3.1 Л3.2 Л3.4 Л3.5 Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8	Конспект лекций.
6.7	Передача ключей с использованием асимметричного шифрования. Открытое распределение ключей. Протокол Диффи-Хеллмана и его модификации /Пр/	9	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 ОПК-10.6-З ОПК-10.6-У ОПК-10.6-В	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л1.7 Л1.8Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Л2.7Л3.1 Л3.2 Л3.4 Л3.5 Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8	Устный опрос по теме. Решение задач. Проверка домашнего задания.
6.8	Изучение литературы, конспекта лекций и подготовка к практической работе. /Ср/	9	7	ОПК-10.3-З ОПК-10.3-У ОПК-10.3-В ОПК-10.4-З ОПК-10.4-У ОПК-10.4-В ОПК-10.6-З ОПК-10.6-У ОПК-10.6-В	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л1.7 Л1.8Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Л2.7Л3.1 Л3.2 Л3.4 Л3.5 Э1 Э2 Э3 Э5 Э6 Э7 Э8	Подготовка конспекта по вопросам темы. Краткий опрос по теме на консультации к зачету.
	Раздел 7. ИКР					
7.1	ИКР /Тема/	9	0			
7.2	Прием зачета с оценкой /ИКР/	9	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 ОПК-10.6-З ОПК-10.6-У ОПК-10.6-В	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л1.7 Л1.8Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Л2.7Л3.1 Л3.2 Л3.4 Л3.5	Ответы на Контрольные вопросы Результаты решения задач. Ответы на дополнительные вопросы. Результаты тестирования.
	Раздел 8. Контроль					
8.1	Контроль /Тема/	9	0			

8.2	Подготовка к приему зачета с оценкой /ЗаО/	9	17,75	ОПК-10.3-З ОПК-10.3-У ОПК-10.3-В ОПК-10.4-З ОПК-10.4-У ОПК-10.4-В ОПК-10.6-З ОПК-10.6-У ОПК-10.6-В	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л1.7 Л1.8Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Л2.7Л3.1 Л3.2 Л3.4 Л3.5	Задачи к зачету. 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 протоколы")

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	Лапонина О. Р.	Основы сетевой безопасности. Криптографические алгоритмы и протоколы взаимодействия	Москва: Интернет-Университет Информационных Технологий (ИНТУИТ), 2016, 242 с.	5-9556-00020-5, http://www.iprbookshop.ru/52217.html
Л1.2	Ожиганов А. А.	Криптографические системы с секретным и открытым ключом : учебное пособие	Санкт-Петербург: Университет ИТМО, 2015, 66 с.	2227-8397, http://www.iprbookshop.ru/67230.html
Л1.3	Лапонина О. Р.	Межсетевое экранирование : учебное пособие	Москва, Саратов: Интернет-Университет Информационных Технологий (ИНТУИТ), Вузовское образование, 2017, 344 с.	978-5-4487-0078-1, http://www.iprbookshop.ru/67391.html
Л1.4	Ожиганов А. А.	Основы криптоанализа симметричных шифров : учебное пособие	Санкт-Петербург: Университет ИТМО, 2008, 44 с.	2227-8397, http://www.iprbookshop.ru/67479.html
Л1.5	Ожиганов А. А.	Теория автоматов : учебное пособие	Санкт-Петербург: Университет ИТМО, 2013, 86 с.	2227-8397, http://www.iprbookshop.ru/68172.html

№	Авторы, составители	Заглавие	Издательство, год	Количество/ название ЭБС
Л1.6	Жиль Земор, Шуликовская В. В.	Курс криптографии	Москва, Ижевск: Регулярная и хаотическая динамика, Институт компьютерных исследований, 2019, 256 с.	978-5-4344-0770-0, http://www.ipr bookshop.ru/91941.html
Л1.7	Глухов М. М., Круглов И. А., Пичкур А. Б., Черемушкин А. В.	Введение в теоретико-числовые методы криптографии	Санкт-Петербург: Лань, 2011, 400 с.	978-5-8114-1116-0, https://e.lanbook.com/books/element.php?pl1_id=68466
Л1.8	Косолапов, Ю. В.	Криптографические протоколы на основе линейных кодов : учебное пособие	Ростов-на-Дону, Таганрог: Издательство Южного федерального университета, 2020, 98 с.	978-5-9275-3316-9, http://www.ipr bookshop.ru/100176.html
6.1.2. Дополнительная литература				
№	Авторы, составители	Заглавие	Издательство, год	Количество/ название ЭБС
Л2.1	Земор Ж., Шуликовская В. В.	Курс криптографии	Москва, Ижевск: Регулярная и хаотическая динамика, Ижевский институт компьютерных исследований, 2006, 256 с.	5-93972-510-4, http://www.ipr bookshop.ru/16547.html
Л2.2	Кукина Е. Г., Романьков В. А.	Введение в криптографию : сборник задач и упражнений	Омск: Омский государственный университет им. Ф.М. Достоевского, 2013, 91 с.	978-5-7779-1588-7, http://www.ipr bookshop.ru/24876.html
Л2.3	Семенова Т. И., Кравченко О. М., Шакин В. Н.	Вычислительные модели и алгоритмы решения задач численными методами : учебное пособие	Москва: Московский технический университет связи и информатики, 2017, 83 с.	2227-8397, http://www.ipr bookshop.ru/92423.html
Л2.4	Апарина О. Ю., Попова Л. А., Семенов В. Е.	История государства и права России : учебное пособие (практикум)	Ставрополь: Северо-Кавказский федеральный университет, 2018, 197 с.	2227-8397, http://www.ipr bookshop.ru/92694.html

№	Авторы, составители	Заглавие	Издательство, год	Количество/ название ЭБС
Л2.5	Семенов Ю. А.	Процедуры, диагностики и безопасность в Интернет : учебное пособие	Москва: Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2020, 581 с.	978-5-4497-0560-0, http://www.iprbookshop.ru/94863.html
Л2.6	Семенов Ю. А.	Алгоритмы телекоммуникационных сетей. Часть 1. Алгоритмы и протоколы каналов и сетей передачи данных : учебное пособие	Москва: Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2020, 757 с.	978-5-4497-0541-9, http://www.iprbookshop.ru/94844.html
Л2.7	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

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 Эль-Гамаля : Методические указания	Рязань: РИЦ РГРТУ, 2013,	, https://elib.rsreu.ru/ebs/download/1031
Л3.5	Швечков В.А., Швечкова О.Г.	Методы контроля, обеспечения достоверности и защиты информационного и программного обеспечения. Схемы электронной цифровой подписи. Алгоритм Шнорра : метод. указ. к лаб. работе	Рязань, 2014, 20с.	, 20

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
OpenOffice	Свободное ПО
VMware Player	Свободное ПО
Операционная система Windows XP/Vista/7/8/10	Microsoft Imagine: Номер подписки 700102019, бессрочно
Kaspersky Endpoint Security	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	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	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.
3	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.
4	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.

8. МЕТОДИЧЕСКИЕ МАТЕРИАЛЫ ПО ДИСЦИПЛИНЕ (МОДУЛЮ)

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