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

Методы и средства криптографической защиты информации

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 **9 ЗЕТ**

Распределение часов дисциплины по семестрам

Семестр (<Курс>.<Семестр на курсе>)	**6 (3.2)**		**7 (4.1)**		**8 (4.2)**		Итого	
Недель	16		16		16			
Вид занятий	УП	РП	УП	РП	УП	РП	УП	РП
Лекции	32	32	32	32	24	24	88	88
Лабораторные					24	24	24	24
Практические	16	16	32	32			48	48
Иная контактная работа	0,25	0,25	0,35	0,35	0,35	0,35	0,95	0,95
Консультирование перед экзаменом и практикой			2	2	2	2	4	4
Итого ауд.	48,25	48,25	66,35	66,35	50,35	50,35	164,95	164,95
Контактная работа	48,25	48,25	66,35	66,35	50,35	50,35	164,95	164,95
Сам. работа	15	15	33	33	4,3	4,3	52,3	52,3
Часы на контроль	8,75	8,75	44,65	44,65	53,35	53,35	106,75	106,75
Итого	72	72	144	144	108	108	324	324

г. Рязань

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

Рабочая программа дисциплины
Методы и средства криптографической 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 28.04.2023 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	Цель: получение обучающимися знаний в области защиты информационных систем с помощью криптографических методов защиты информации
1.2	Задачами освоения дисциплины являются:
1.3	- изучение стандартов в области криптографической защиты информации;
1.4	- изучение основных методов шифрования;
1.5	- изучение базовых алгоритмов, применяемых в криптосистемах;
1.6	- освоение основ криптоанализа;
1.7	- изучение системного подхода к организации защиты информации, передаваемой и обрабатываемой техническими средствами на основе применения криптографических методов.
2. МЕСТО ДИСЦИПЛИНЫ (МОДУЛЯ) В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ	
Цикл (раздел) ОП:	Б1.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-10.1. Применяет алгоритмы функционирования криптографических систем

Знать
основные виды симметричных и асимметричных криптографических алгоритмов; математические модели шифров
Уметь
корректно применять симметричные и асимметричные криптографические алгоритмы
Владеть
криптографической терминологией

ОПК-10.2. Применяет алгоритмы функционирования электронной подписи

Знать
основные алгоритмы электронной подписи
Уметь
работать со средствами создания электронной подписи
Владеть
навыками установки и настройки средств работы с электронной подписью

ОПК-10.5. Использует методы и средства криптографической защиты информации при решении задач профессиональной деятельности

Знать
принципы работы современных средств криптографической защиты информации
Уметь
производить установку, наладку, тестирование и обслуживание средств криптографической защиты информации
Владеть
навыками применения криптографических средств с учетом требований нормативных и правовых актов по защите информации

В результате освоения дисциплины (модуля) обучающийся должен

3.1	**Знать:**
3.1.1	современные средства криптографической защиты информации
3.2	**Уметь:**
3.2.1	выбирать средства криптографической защиты информации на основании требований нормативных и правовых актов по защите информации

3.3	**Владеть:**
3.3.1	использования средства 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/	6	0			
1.2	Основные понятия и определения. Основные этапы развития криптографии. Становление криптографии как науки /Лек/	6	2	ОПК-10.1-З ОПК-10.1-У ОПК-10.1-В ОПК-10.2-З ОПК-10.2-У ОПК-10.2-В ОПК-10.5-З ОПК-10.5-У ОПК-10.5-В	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Л2.7Л3.1 Л3.2 Л3.3 Л3.4 Л3.5 Л3.6 Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8	Конспект лекций.
1.3	Изучение конспекта лекций /Ср/	6	2	ОПК-10.1-З ОПК-10.1-У ОПК-10.1-В ОПК-10.2-З ОПК-10.2-У ОПК-10.2-В ОПК-10.5-З ОПК-10.5-У ОПК-10.5-В	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Л2.7Л3.1 Л3.2 Л3.3 Л3.4 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. Введение в криптографию					
2.1	Задачи криптографии /Тема/	6	0			
2.2	Основные задачи криптографии. Управление секретными ключами. Инфраструктура открытых ключей /Лек/	6	2	ОПК-10.1-З ОПК-10.1-У ОПК-10.1-В ОПК-10.2-З ОПК-10.2-У ОПК-10.2-В ОПК-10.5-З ОПК-10.5-У ОПК-10.5-В	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Л2.7Л3.1 Л3.2 Л3.3 Л3.4 Л3.6 Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8	Конспект лекций.
2.3	Модели открытых текстов. По-значная модель открытого текста. Вероятностная модель открытого текста. Критерии распознавания открытых текстов /Лек/	6	2	ОПК-10.1-З ОПК-10.1-У ОПК-10.1-В ОПК-10.2-З ОПК-10.2-У ОПК-10.2-В ОПК-10.5-З ОПК-10.5-У ОПК-10.5-В	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Л2.7Л3.1 Л3.2 Л3.3 Л3.4 Л3.6 Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8	Конспект лекций.

2.4	Формальные модели шифров. Алгебраическая модель шифра. Вероятностная модель шифра. /Лек/	6	2	ОПК-10.1-З ОПК-10.1-У ОПК-10.1-В ОПК-10.2-З ОПК-10.2-У ОПК-10.2-В ОПК-10.5-З ОПК-10.5-У ОПК-10.5-В	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Л2.7Л3.1 Л3.2 Л3.3 Л3.4 Л3.6 Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8	Конспект лекций.
2.5	Делимость и алгоритм Евклида. Сравнения /Пр/	6	4	ОПК-10.1-З ОПК-10.1-У ОПК-10.1-В ОПК-10.2-З ОПК-10.2-У ОПК-10.2-В ОПК-10.5-З ОПК-10.5-У ОПК-10.5-В	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Л2.7Л3.1 Л3.2 Л3.3 Л3.4 Л3.6 Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8	Устный опрос по теме. Решение задач. Проверка домашнего задания.
2.6	Изучение литературы, конспекта лекций и подготовка к практической работе /Ср/	6	2	ОПК-10.1-З ОПК-10.1-У ОПК-10.1-В ОПК-10.2-З ОПК-10.2-У ОПК-10.2-В ОПК-10.5-З ОПК-10.5-У ОПК-10.5-В	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Л2.7Л3.1 Л3.2 Л3.3 Л3.4 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. Основные классы шифров и их свойства					
3.1	Простейшие шифры /Тема/	6	0			
3.2	Классификация шифров. Поточные шифры замены. Шифры простой замены и их анализ /Лек/	6	2	ОПК-10.1-З ОПК-10.1-У ОПК-10.1-В ОПК-10.2-З ОПК-10.2-У ОПК-10.2-В ОПК-10.5-З ОПК-10.5-У ОПК-10.5-В	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Л2.7Л3.1 Л3.2 Л3.3 Л3.4 Л3.6 Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8	Конспект лекций.
3.3	Многоалфавитные шифры замены. Дисковые шифраторы. /Лек/	6	2	ОПК-10.1-З ОПК-10.1-У ОПК-10.1-В ОПК-10.2-З ОПК-10.2-У ОПК-10.2-В ОПК-10.5-З ОПК-10.5-У ОПК-10.5-В	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Л2.7Л3.1 Л3.2 Л3.3 Л3.4 Л3.6 Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8	Конспект лекций.

3.4	Шифры гаммирования. Использование неравновероятностной гаммы. Повторное использование гаммы. Криптоанализ шифра Вижинера /Лек/	6	2	ОПК-10.1-З ОПК-10.1-У ОПК-10.1-В ОПК-10.2-З ОПК-10.2-У ОПК-10.2-В ОПК-10.5-З ОПК-10.5-У ОПК-10.5-В	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Л2.7Л3.1 Л3.2 Л3.3 Л3.4 Л3.6 Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8	Конспект лекций.
3.5	Шифры перестановки. Разновидности шифров перестановки. Элементы криптоанализа шифров перестановки. /Лек/	6	4	ОПК-10.1-З ОПК-10.1-У ОПК-10.1-В ОПК-10.2-З ОПК-10.2-У ОПК-10.2-В ОПК-10.5-З ОПК-10.5-У ОПК-10.5-В	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Л2.7Л3.1 Л3.2 Л3.3 Л3.4 Л3.6 Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8	Конспект лекций.
3.6	Сравнения /Пр/	6	4	ОПК-10.1-З ОПК-10.1-У ОПК-10.1-В ОПК-10.2-З ОПК-10.2-У ОПК-10.2-В ОПК-10.5-З ОПК-10.5-У ОПК-10.5-В	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Л2.7Л3.1 Л3.2 Л3.3 Л3.4 Л3.6 Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8	Устный опрос по теме. Решение задач. Проверка домашнего задания.
3.7	Конечные поля и квадратичные вычеты. /Пр/	6	4	ОПК-10.1-З ОПК-10.1-У ОПК-10.1-В ОПК-10.2-З ОПК-10.2-У ОПК-10.2-В ОПК-10.5-З ОПК-10.5-У ОПК-10.5-В	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Л2.7Л3.1 Л3.2 Л3.3 Л3.4 Л3.6 Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8	Устный опрос по теме. Решение задач. Проверка домашнего задания.
3.8	Некоторые простые криптосистемы /Пр/	6	4	ОПК-10.1-З ОПК-10.1-У ОПК-10.1-В ОПК-10.2-З ОПК-10.2-У ОПК-10.2-В ОПК-10.5-З ОПК-10.5-У ОПК-10.5-В	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Л2.7Л3.1 Л3.2 Л3.3 Л3.4 Л3.6 Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8	Устный опрос по теме. Решение задач. Проверка домашнего задания.

3.9	Изучение литературы, конспекта лекций и подготовка к практическим работам /Ср/	6	5	ОПК-10.1-З ОПК-10.1-У ОПК-10.1-В ОПК-10.2-З ОПК-10.2-У ОПК-10.2-В ОПК-10.5-З ОПК-10.5-У ОПК-10.5-В	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Л2.7Л3.1 Л3.2 Л3.3 Л3.4 Л3.6 Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8	Подготовка конспекта по вопросам темы. Краткий опрос по теме на консультации к зачету.
3.10	Блочные шифры /Тема/	6	0			
3.11	Блочные шифры. Блочные шифры простой замены. Шифры Плейфера и Хилла. Архитектура современных блочных шифров: сеть Фейстеля. /Лек/	6	4	ОПК-10.1-З ОПК-10.1-У ОПК-10.1-В ОПК-10.2-З ОПК-10.2-У ОПК-10.2-В ОПК-10.5-З ОПК-10.5-У ОПК-10.5-В	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Л2.7Л3.1 Л3.2 Л3.3 Л3.4 Л3.6 Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8	Конспект лекций.
3.12	Режимы использования блочных шифров. Российский блочный шифр «Магма». Криптоалгоритмы: RINJDAEL и IDEA. /Лек/	6	2	ОПК-10.1-З ОПК-10.1-У ОПК-10.1-В ОПК-10.2-З ОПК-10.2-У ОПК-10.2-В ОПК-10.5-З ОПК-10.5-У ОПК-10.5-В	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Л2.7Л3.1 Л3.2 Л3.3 Л3.4 Л3.6 Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8	Конспект лекций.
3.13	Методы анализа алгоритмов блочного шифрования. Рекомендации по практическому применению алгоритмов блочного шифрования. /Лек/	6	2	ОПК-10.1-З ОПК-10.1-У ОПК-10.1-В ОПК-10.2-З ОПК-10.2-У ОПК-10.2-В ОПК-10.5-З ОПК-10.5-У ОПК-10.5-В	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Л2.7Л3.1 Л3.2 Л3.3 Л3.4 Л3.6 Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8	Конспект лекций.
3.14	Системы шифрования с открытым ключом. Принцип ассиметричного шифрования /Лек/	6	2	ОПК-10.1-З ОПК-10.1-У ОПК-10.1-В ОПК-10.2-З ОПК-10.2-У ОПК-10.2-В ОПК-10.5-З ОПК-10.5-У ОПК-10.5-В	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Л2.7Л3.1 Л3.2 Л3.3 Л3.4 Л3.6 Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8	Конспект лекций.

3.15	Практические аспекты использования криптосистем с открытым ключом. /Лек/	6	2	ОПК-10.1-З ОПК-10.1-У ОПК-10.1-В ОПК-10.2-З ОПК-10.2-У ОПК-10.2-В ОПК-10.5-З ОПК-10.5-У ОПК-10.5-В	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Л2.7Л3.1 Л3.2 Л3.3 Л3.4 Л3.6 Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8	Конспект лекций.
3.16	Изучение литературы и конспекта лекций /Ср/	6	6	ОПК-10.1-З ОПК-10.1-У ОПК-10.1-В ОПК-10.2-З ОПК-10.2-У ОПК-10.2-В ОПК-10.5-З ОПК-10.5-У ОПК-10.5-В	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Л2.7Л3.1 Л3.2 Л3.3 Л3.4 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. Надежность шифров					
4.1	Надежность шифроы /Тема/	7	0			
4.2	Криптографическая стойкость шифров. Теоретическая и практическая стойкость шифров. /Лек/	7	2	ОПК-10.1-З ОПК-10.1-У ОПК-10.1-В ОПК-10.2-З ОПК-10.2-У ОПК-10.2-В ОПК-10.5-З ОПК-10.5-У ОПК-10.5-В	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Л2.7Л3.1 Л3.2 Л3.3 Л3.4 Л3.6 Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8	Конспект лекций.
4.3	Подходы к определению криптографической стойкости шифров. Подходы к определению практической стойкости шифров. /Лек/	7	2	ОПК-10.1-З ОПК-10.1-У ОПК-10.1-В ОПК-10.2-З ОПК-10.2-У ОПК-10.2-В ОПК-10.5-З ОПК-10.5-У ОПК-10.5-В	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Л2.7Л3.1 Л3.2 Л3.3 Л3.4 Л3.6 Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8	Конспект лекций.
4.4	Имитостойкость шифров. Имитозащита. Характеристики имитостойкости шифров и их оценки /Лек/	7	2	ОПК-10.1-З ОПК-10.1-У ОПК-10.1-В ОПК-10.2-З ОПК-10.2-У ОПК-10.2-В ОПК-10.5-З ОПК-10.5-У ОПК-10.5-В	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Л2.7Л3.1 Л3.2 Л3.3 Л3.4 Л3.6 Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8	Конспект лекций.

4.5	Изучение литературы и конспекта лекций /Ср/	7	6	ОПК-10.1-З ОПК-10.1-У ОПК-10.1-В ОПК-10.2-З ОПК-10.2-У ОПК-10.2-В ОПК-10.5-З ОПК-10.5-У ОПК-10.5-В	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Л2.7Л3.1 Л3.2 Л3.3 Л3.4 Л3.6 Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8	Подготовка конспекта по вопросам темы. Краткий опрос по теме на консультации к экзамену.
	Раздел 5. Методы синтеза и анализа симметричных криптосистем.					
5.1	Поточные криптосистемы /Тема/	7	0			
5.2	Принципы построения алгоритмов поточного шифрования. Строение поточных криптосистем. /Лек/	7	2	ОПК-10.1-З ОПК-10.1-У ОПК-10.1-В ОПК-10.2-З ОПК-10.2-У ОПК-10.2-В ОПК-10.5-З ОПК-10.5-У ОПК-10.5-В	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Л2.7Л3.1 Л3.2 Л3.3 Л3.4 Л3.6 Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8	Конспект лекций.
5.3	Генераторы псевдослучайных последовательностей. Конгруэнтные генераторы. Генераторы Фибоначчи. Генераторы, основанные на сложности решения задач теории чисел. Генераторы на основе линейных регистров сдвига. /Лек/	7	6	ОПК-10.1-З ОПК-10.1-У ОПК-10.1-В ОПК-10.2-З ОПК-10.2-У ОПК-10.2-В ОПК-10.5-З ОПК-10.5-У ОПК-10.5-В	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Л2.7Л3.1 Л3.2 Л3.3 Л3.4 Л3.6 Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8	Конспект лекций.
5.4	Методы анализа криптографических алгоритмов. Классификация методов анализа криптографических алгоритмов. Методы нахождения ключей криптографических алгоритмов: алгоритмические методы, алгебраические методы, статистические методы. /Лек/	7	6	ОПК-10.1-З ОПК-10.1-У ОПК-10.1-В ОПК-10.2-З ОПК-10.2-У ОПК-10.2-В ОПК-10.5-З ОПК-10.5-У ОПК-10.5-В	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Л2.7Л3.1 Л3.2 Л3.3 Л3.4 Л3.6 Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8	Конспект лекций.
5.5	Криптографические системы /Пр/	7	8	ОПК-10.1-З ОПК-10.1-У ОПК-10.1-В ОПК-10.2-З ОПК-10.2-У ОПК-10.2-В ОПК-10.5-З ОПК-10.5-У ОПК-10.5-В	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Л2.7Л3.1 Л3.2 Л3.3 Л3.4 Л3.6 Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8	Устный опрос по теме. Решение задач. Проверка домашнего задания.

5.6	«Изучение классических симметричных шифров» /Пр/	7	4	ОПК-10.1-З ОПК-10.1-У ОПК-10.1-В ОПК-10.2-З ОПК-10.2-У ОПК-10.2-В ОПК-10.5-З ОПК-10.5-У ОПК-10.5-В	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Л2.7Л3.1 Л3.2 Л3.3 Л3.4 Л3.6 Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8	Устный опрос по теме. Решение задач. Проверка домашнего задания.
5.7	Реализация симметричной криптосистемы с использованием блочного алгоритма шифрования /Пр/	7	4	ОПК-10.1-З ОПК-10.1-У ОПК-10.1-В ОПК-10.2-З ОПК-10.2-У ОПК-10.2-В ОПК-10.5-З ОПК-10.5-У ОПК-10.5-В	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Л2.7Л3.1 Л3.2 Л3.3 Л3.4 Л3.6 Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8	Устный опрос по теме. Решение задач. Проверка домашнего задания.
5.8	Изучение литературы и конспекта лекций. Подготовка к практическим работам /Ср/	7	15	ОПК-10.1-З ОПК-10.1-У ОПК-10.1-В ОПК-10.2-З ОПК-10.2-У ОПК-10.2-В ОПК-10.5-З ОПК-10.5-У ОПК-10.5-В	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Л2.7Л3.1 Л3.2 Л3.3 Л3.4 Л3.6 Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8	Подготовка конспекта по вопросам темы. Краткий опрос по теме на консультации к экзамену.
	Раздел 6. Криптографические хеш-функции.					
6.1	Криптографические хеш-функции /Тема/	7	0			
6.2	Общие сведения о хеш-функциях. Криптографические хеш-функции. Ключевые и бесключевые хеш-функции. Итеративные способы по-строения хеш-функций. Понятие о стойкости хеш-функций /Лек/	7	8	ОПК-10.1-З ОПК-10.1-У ОПК-10.1-В ОПК-10.2-З ОПК-10.2-У ОПК-10.2-В ОПК-10.5-З ОПК-10.5-У ОПК-10.5-В	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Л2.7Л3.1 Л3.2 Л3.3 Л3.4 Л3.6 Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8	Конспект лекций.
6.3	Использование криптографических хеш-функций /Пр/	7	8	ОПК-10.1-З ОПК-10.1-У ОПК-10.1-В ОПК-10.2-З ОПК-10.2-У ОПК-10.2-В ОПК-10.5-З ОПК-10.5-У ОПК-10.5-В	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Л2.7Л3.1 Л3.2 Л3.3 Л3.4 Л3.6 Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8	Устный опрос по теме. Решение задач. Проверка домашнего задания.

6.4	Изучение литературы и конспекта лекций. Подготовка к практической работе /Ср/	7	6	ОПК-10.1-З ОПК-10.1-У ОПК-10.1-В ОПК-10.2-З ОПК-10.2-У ОПК-10.2-В ОПК-10.5-З ОПК-10.5-У ОПК-10.5-В	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Л2.7Л3.1 Л3.2 Л3.3 Л3.4 Л3.6 Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8	Подготовка конспекта по вопросам темы. Краткий опрос по теме на консультации к экзамену.
	Раздел 7. Электронная подпись					
7.1	Электронная подпись /Тема/	7	0			
7.2	Понятие электронной подписи. Электронные подписи на основе шифрсистем с открытыми ключами. Электронная подпись Фиата-Шамира. /Лек/	7	2	ОПК-10.1-З ОПК-10.1-У ОПК-10.1-В ОПК-10.2-З ОПК-10.2-У ОПК-10.2-В ОПК-10.5-З ОПК-10.5-У ОПК-10.5-В	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Л2.7Л3.1 Л3.2 Л3.3 Л3.4 Л3.6 Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8	Конспект лекций.
7.3	Электронная подпись Эль-Гамаля. Одноразовые электронные подписи. /Лек/	7	2	ОПК-10.1-З ОПК-10.1-У ОПК-10.1-В ОПК-10.2-З ОПК-10.2-У ОПК-10.2-В ОПК-10.5-З ОПК-10.5-У ОПК-10.5-В	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Л2.7Л3.1 Л3.2 Л3.3 Л3.4 Л3.6 Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8	Конспект лекций.
7.4	Нормативные документы, регулирующие использование электронной подписи /Лек/	6	2	ОПК-10.1-З ОПК-10.1-У ОПК-10.1-В ОПК-10.2-З ОПК-10.2-У ОПК-10.2-В ОПК-10.5-З ОПК-10.5-У ОПК-10.5-В	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Л2.7Л3.1 Л3.2 Л3.3 Л3.4 Л3.6 Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8	Конспект лекций.
7.5	Использование электронных подписей /Пр/	7	8	ОПК-10.1-З ОПК-10.1-У ОПК-10.1-В ОПК-10.2-З ОПК-10.2-У ОПК-10.2-В ОПК-10.5-З ОПК-10.5-У ОПК-10.5-В	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Л2.7Л3.1 Л3.2 Л3.3 Л3.4 Л3.6 Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8	Устный опрос по теме. Решение задач. Проверка домашнего задания.

7.6	Изучение литературы и конспекта лекций. Подготовка к практическим занятиям. /Ср/	7	6	ОПК-10.1-З ОПК-10.1-У ОПК-10.1-В ОПК-10.2-З ОПК-10.2-У ОПК-10.2-В ОПК-10.5-З ОПК-10.5-У ОПК-10.5-В	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Л2.7Л3.1 Л3.2 Л3.3 Л3.4 Л3.6 Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8	Подготовка конспекта по вопросам темы. Краткий опрос по теме на консультации к экзамену.
	Раздел 8. Средства криптографической защиты информации					
8.1	Нормативные документы, регламентирующие использование СКЗИ /Тема/	8	0			
8.2	Требования НТД к эксплуатации СКЗИ /Лек/	8	2	ОПК-10.1-З ОПК-10.1-У ОПК-10.1-В ОПК-10.2-З ОПК-10.2-У ОПК-10.2-В ОПК-10.5-З ОПК-10.5-У ОПК-10.5-В	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Л2.7Л3.1 Л3.2 Л3.3 Л3.4 Л3.6 Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8	Конспект лекций.
8.3	Сертификация СКЗИ. Классы СКЗИ. /Лек/	8	2	ОПК-10.1-З ОПК-10.1-У ОПК-10.1-В ОПК-10.2-З ОПК-10.2-У ОПК-10.2-В ОПК-10.5-З ОПК-10.5-У ОПК-10.5-В	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Л2.7Л3.1 Л3.2 Л3.3 Л3.4 Л3.6 Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8	Конспект лекций.
8.4	Изучение литературы и конспекта лекций /Ср/	8	1,3	ОПК-10.1-З ОПК-10.1-У ОПК-10.1-В ОПК-10.2-З ОПК-10.2-У ОПК-10.2-В ОПК-10.5-З ОПК-10.5-У ОПК-10.5-В	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Л2.7Л3.1 Л3.2 Л3.3 Л3.4 Л3.6 Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8	Подготовка конспекта по вопросам темы. Краткий опрос по теме на консультации к экзамену.
8.5	Средства защиты от несанкционированного доступа к информации, передаваемой по каналам связи /Тема/	8	0			

8.6	Функции, выполняемые СКЗИ VipNET. Основные компоненты СКЗИ VipNET. Особенности и требования к эксплуатации СКЗИ VipNET /Лек/	8	4	ОПК-10.1-З ОПК-10.1-У ОПК-10.1-В ОПК-10.2-З ОПК-10.2-У ОПК-10.2-В ОПК-10.5-З ОПК-10.5-У ОПК-10.5-В	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Л2.7Л3.1 Л3.2 Л3.3 Л3.4 Л3.6 Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8	Конспект лекций.
8.7	ПАК "С-Терра". Функции, выполняемые ПАК "С-Терра". Основные компоненты ПАК "С-Терра". Особенности и требования к эксплуатации ПАК "С-Терра" /Лек/	8	4	ОПК-10.1-З ОПК-10.1-У ОПК-10.1-В ОПК-10.2-З ОПК-10.2-У ОПК-10.2-В ОПК-10.5-З ОПК-10.5-У ОПК-10.5-В	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Л2.7Л3.1 Л3.2 Л3.3 Л3.4 Л3.6 Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8	Конспект лекций.
8.8	АПКШ «Континент». Функции, выполняемые АПКШ «Континент». Основные компоненты АПКШ. Особенности и требования к эксплуатации АПКШ. /Лек/	8	4	ОПК-10.1-З ОПК-10.1-У ОПК-10.1-В ОПК-10.2-З ОПК-10.2-У ОПК-10.2-В ОПК-10.5-З ОПК-10.5-У ОПК-10.5-В	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Л2.7Л3.1 Л3.2 Л3.3 Л3.4 Л3.6 Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8	Конспект лекций.
8.9	Работа с СКЗИ «VipNet» /Лаб/	8	10	ОПК-10.1-З ОПК-10.1-У ОПК-10.1-В ОПК-10.2-З ОПК-10.2-У ОПК-10.2-В ОПК-10.5-З ОПК-10.5-У ОПК-10.5-В	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Л2.7Л3.1 Л3.2 Л3.3 Л3.4 Л3.6 Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8	Выполнение ЛР. Отчет по ЛР. Защита ЛР.
8.10	Работа с ПАК "С-Терра" /Лаб/	8	10	ОПК-10.1-З ОПК-10.1-У ОПК-10.1-В ОПК-10.2-З ОПК-10.2-У ОПК-10.2-В ОПК-10.5-З ОПК-10.5-У ОПК-10.5-В	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Л2.7Л3.1 Л3.2 Л3.3 Л3.4 Л3.6 Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8	Выполнение ЛР. Отчет по ЛР. Защита ЛР.

8.11	Изучение литературы и конспекта лекций. Подготовка к лабораторным работам. /Ср/	8	1,5	ОПК-10.1-З ОПК-10.1-У ОПК-10.1-В ОПК-10.2-З ОПК-10.2-У ОПК-10.2-В ОПК-10.5-З ОПК-10.5-У ОПК-10.5-В	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Л2.7Л3.1 Л3.2 Л3.3 Л3.4 Л3.6 Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8	Подготовка конспекта по вопросам темы. Краткий опрос по теме на консультации к экзамену.
8.12	Средства обеспечения достоверности и юридической значимости информации, неотказуемости от информации /Тема/	8	0			
8.13	СКЗИ КриптоПро. Функции, выполняемые СКЗИ КриптоПро. Основные компоненты СКЗИ КриптоПро. Особенности и требования к эксплуатации СКЗИ КриптоПро. /Лек/	8	4	ОПК-10.1-З ОПК-10.1-У ОПК-10.1-В ОПК-10.2-З ОПК-10.2-У ОПК-10.2-В ОПК-10.5-З ОПК-10.5-У ОПК-10.5-В	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Л2.7Л3.1 Л3.2 Л3.3 Л3.4 Л3.6 Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8	Конспект лекций.
8.14	СКЗИ «Верба-OW». Функции, выполняемые СКЗИ «Верба-OW». Основные компоненты СКЗИ «Верба-OW». Особенности и требования к эксплуатации СКЗИ «Верба-OW» /Лек/	8	4	ОПК-10.1-З ОПК-10.1-У ОПК-10.1-В ОПК-10.2-З ОПК-10.2-У ОПК-10.2-В ОПК-10.5-З ОПК-10.5-У ОПК-10.5-В	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Л2.7Л3.1 Л3.2 Л3.3 Л3.4 Л3.6 Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8	Конспект лекций.
8.15	Лабораторная работа "Электронная подпись" /Лаб/	8	4	ОПК-10.1-З ОПК-10.1-У ОПК-10.1-В ОПК-10.2-З ОПК-10.2-У ОПК-10.2-В ОПК-10.5-З ОПК-10.5-У ОПК-10.5-В	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Л2.7Л3.1 Л3.2 Л3.3 Л3.4 Л3.6 Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8	Выполнение ЛР. Отчет по ЛР. Защита ЛР.
8.16	Изучение литературы и конспекта лекций, подготовка к лабораторным работам /Ср/	8	1,5	ОПК-10.1-З ОПК-10.1-У ОПК-10.1-В ОПК-10.2-З ОПК-10.2-У ОПК-10.2-В ОПК-10.5-З ОПК-10.5-У ОПК-10.5-В	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Л2.7Л3.1 Л3.2 Л3.3 Л3.4 Л3.6 Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8	Подготовка конспекта по вопросам темы. Краткий опрос по теме на консультации к экзамену.
	Раздел 9. Иная контактная работа.					
9.1	ИКР /Тема/	8	0			

9.2	Прием зачета /ИКР/	6	0,25	ОПК-10.1-З ОПК-10.1-У ОПК-10.1-В ОПК-10.2-З ОПК-10.2-У ОПК-10.2-В ОПК-10.5-З ОПК-10.5-У ОПК-10.5-В	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Л2.7Л3.1 Л3.2 Л3.3 Л3.4 Л3.6	Ответы на контрольные вопросы. Ответы на дополнительные вопросы.
9.3	Прием экзамена /ИКР/	7	0,35	ОПК-10.1-З ОПК-10.1-У ОПК-10.1-В ОПК-10.2-З ОПК-10.2-У ОПК-10.2-В ОПК-10.5-З ОПК-10.5-У ОПК-10.5-В	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Л2.7Л3.1 Л3.2 Л3.3 Л3.4 Л3.6	Ответы на контрольные вопросы. Ответы на дополнительные вопросы.
9.4	Прием экзамена /ИКР/	8	0,35	ОПК-10.1-З ОПК-10.1-У ОПК-10.1-В ОПК-10.2-З ОПК-10.2-У ОПК-10.2-В ОПК-10.5-З ОПК-10.5-У ОПК-10.5-В	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Л2.7Л3.1 Л3.2 Л3.3 Л3.4 Л3.6	Ответы на контрольные вопросы. Ответы на дополнительные вопросы.
	Раздел 10. Контроль					
10.1	Контроль /Тема/	8	0			
10.2	Подготовка к зачету /Зачёт/	6	8,75	ОПК-10.1-З ОПК-10.1-У ОПК-10.1-В ОПК-10.2-З ОПК-10.2-У ОПК-10.2-В ОПК-10.5-З ОПК-10.5-У ОПК-10.5-В	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Л2.7Л3.1 Л3.2 Л3.3 Л3.4 Л3.6	Задачи к зачету. Билеты к зачету. Тесты к зачету.
10.3	Подготовка к экзамену /Экзамен/	7	44,65	ОПК-10.1-З ОПК-10.1-У ОПК-10.1-В ОПК-10.2-З ОПК-10.2-У ОПК-10.2-В ОПК-10.5-З ОПК-10.5-У ОПК-10.5-В	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Л2.7Л3.1 Л3.2 Л3.3 Л3.4 Л3.6	Задачи к экзамену. Билеты к экзамену.

10.4	Подготовка к экзамену /Экзамен/	8	53,35	ОПК-10.1-З ОПК-10.1-У ОПК-10.1-В ОПК-10.2-З ОПК-10.2-У ОПК-10.2-В ОПК-10.5-З ОПК-10.5-У ОПК-10.5-В	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Л2.7Л3.1 Л3.2 Л3.3 Л3.4 Л3.6	Задачи к экзамену. Билеты к экзамену.
	Раздел 11. Консультации					
11.1	Консультирование перед экзаменом и практикой /Тема/	8	0			
11.2	Консультирование перед экзаменом и практикой /Кнс/	7	2	ОПК-10.1-З ОПК-10.1-У ОПК-10.1-В ОПК-10.2-З ОПК-10.2-У ОПК-10.2-В ОПК-10.5-З ОПК-10.5-У ОПК-10.5-В	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Л2.7Л3.1 Л3.2 Л3.3 Л3.4 Л3.6	Вопросы к экзамену. Решение типовых задач. Ответы на вопросы.
11.3	Консультирование перед экзаменом и практикой /Кнс/	8	2	ОПК-10.1-З ОПК-10.1-У ОПК-10.1-В ОПК-10.2-З ОПК-10.2-У ОПК-10.2-В ОПК-10.5-З ОПК-10.5-У ОПК-10.5-В	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Л2.7Л3.1 Л3.2 Л3.3 Л3.4 Л3.6	Вопросы к экзамену. Решение типовых задач. Ответы на вопросы.

5. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ПО ДИСЦИПЛИНЕ (МОДУЛЮ)

Оценочные материалы приведены в приложении к рабочей программе дисциплины (см. документ "Оценочные материалы по дисциплине "Методы и средства криптографической 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	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.iprbookshop.ru/24876.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

№	Авторы, составители	Заглавие	Издательство, год	Количество/ название ЭБС
Л1.3	Ожиганов А. А.	Основы криптоанализа симметричных шифров : учебное пособие	Санкт-Петербург: Университет ИТМО, 2008, 44 с.	2227-8397, http://www.iprbookshop.ru/67479.html
Л1.4	Басалова Г. В.	Основы криптографии : учебное пособие	Москва, Саратов: Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2020, 282 с.	978-5-4497-0340-8, http://www.iprbookshop.ru/89455.html
Л1.5	Гатченко Н. А., Исаев А. С., Яковлев А. Д.	Криптографическая защита информации : учебное пособие	Санкт-Петербург: НИУ ИТМО, 2012, 142 с.	, http://e.lanbook.com/books/element.php?pl1_id=40849
Л1.6	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

6.1.2. Дополнительная литература

№	Авторы, составители	Заглавие	Издательство, год	Количество/ название ЭБС
Л2.1	Романьков В. А.	Алгебраическая криптография : монография	Омск: Омский государственный университет им. Ф.М. Достоевского, 2013, 136 с.	978-5-7779-1600-6, http://www.iprbookshop.ru/24868.html
Л2.2	Гультяева Т. А.	Основы теории информации и криптографии : конспект лекций	Новосибирск: Новосибирский государственный технический университет, 2010, 88 с.	978-5-7782-1425-5, http://www.iprbookshop.ru/44987.html
Л2.3	Аграновский А. В., Хади Р. А.	Практическая криптография: алгоритмы и их программирование	Москва: СОЛОН-Пресс, 2016, 256 с.	5-98003-002-6, http://www.iprbookshop.ru/90248.html
Л2.4	Гультяева Т. А.	Основы защиты информации : учебное пособие	Новосибирск: Новосибирский государственный технический университет, 2018, 83 с.	978-5-7782-3641-7, http://www.iprbookshop.ru/91638.html

№	Авторы, составители	Заглавие	Издательство, год	Количество/ название ЭБС
Л2.5	Гультяева Т. А.	Основы информационной безопасности : учебное пособие	Новосибирск: Новосибирский государственный технический университет, 2018, 79 с.	978-5-7782-3640-0, http://www.iprbookshop.ru/91640.html
Л2.6	Долозов Н. Л., Гультяева Т. А.	Программные средства защиты информации : конспект лекций	Новосибирск: Новосибирский государственный технический университет, 2015, 63 с.	978-5-7782-2753-8, http://www.iprbookshop.ru/91683.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	Калинкина Т.И., Пржегорлинский В.Н.	Криптографические методы защиты информации : Методические указания	Рязань: РИЦ РГРТУ, 2014,	, https://elib.rsreu.ru/ebs/download/787
Л3.2	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
Л3.3	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	Швечкова О.Г.	Криптографические методы защиты информации : Метод.указ.к лаб.работам N1-8	Рязань, 2004, 40с.	, 20
6.2. Перечень ресурсов информационно-телекоммуникационной сети "Интернет"				
Э1	Электронно-библиотечная система «Лань». – Режим доступа: с любого компьютера РГРТУ без пароля			

Э2	Электронно-библиотечная система «IPRbooks». – Режим доступа: с любого компьютера РГРТУ без пароля, из сети Интернет по паролю
Э3	Электронная библиотека РГРТУ
Э4	Научная электронная библиотека eLibrary
Э5	Библиотека и форум по программированию
Э6	Национальный открытый университет ИНТУИТ
Э7	Информационно-справочная система
Э8	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
Kaspersky Endpoint Security	Коммерческая лицензия
LibreOffice	Свободное ПО
7 Zip	Свободное ПО
Операционная система Windows XP/Vista/7/8/10	Microsoft Imagine: Номер подписки 700102019, бессрочно

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	264 учебно-административный корпус. учебная аудитория для проведения учебных занятий Специализированная мебель (16 посадочных мест), 5 рабочих мест (стол), магнитно-маркерная доска.
2	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.
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	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 "Методы и средства криптографической зашиты информации")