МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение высшего образования
«Дальневосточный федеральный университет»
(ДВФУ)
ПОЛИТЕХНИЧЕСКИЙ ИНСТИТУТ

«СОГЛАСОВАНО»
Руководитель ОП
_____ ___ Л.Г. Стаценко ___
(подпись) (Ф.И.О.)
«_21__» ____апреля_____ 2021 г.

«УТВЕРЖДАЮ»
Директор департамента электроники,
телекоммуникации и приборостроения
_____ Л.Г. Стаценко __
(подпись) (Ф.И.О.)
«__21_» __апреля_____ 2021 г.

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

Методы и средства защиты информации

Направление подготовки 11.03.02 Инфокоммуникационные технологии и системы связи

профиль «Видеоинформационные технологии и цифровое вещание»

Форма подготовки очная

курс 3 семестр 5
лекции 36 час.
практические занятия 18 час.
лабораторные работы 18 час.
в том числе с использованием МАО лек. 0/пр. 0/лаб. 0 час.
всего часов аудиторной нагрузки 72 час.
в том числе с использованием МАО 0 час.
самостоятельная работа 9 час.
в том числе на подготовку к экзамену 5 час.
курсовая работа / курсовой проект не предусмотрены учебным планом
зачет не предусмотрен учебным планом
экзамен 5 семестр

Рабочая программа составлена в соответствии с требованиями Федерального государственного образовательного стандарта по направлению подготовки **11.03.02 Инфокоммуникационные технологии и системы связи** утвержденного приказом Министерства образования и науки РФ от 19.09.2017 г. №930.

Рабочая программа обсуждена на заседании департамента электроники, телекоммуникации и приборостроения
протокол № 11 от « 21 » апреля 20___ г.

Директор департамента Стаценко Л.Г. д. ф.-м.н., професоор
Составитель: Чусов А.А., доцент, к.т.н.

Владивосток
2021

I. Рабочая программа пересмотрена на заседании департамента:

Протокол от «_____» _____ 20___ г. № _____

Директор департамента _____ _____
(подпись) (И.О. Фамилия)

II. Рабочая программа пересмотрена на заседании департамента:

Протокол от «_____» _____ 20___ г. № _____

Директор департамента _____ _____
(подпись) (И.О. Фамилия)

III. Рабочая программа пересмотрена на заседании департамента:

Протокол от «_____» _____ 20___ г. № _____

Директор департамента _____ _____
(подпись) (И.О. Фамилия)

IV. Рабочая программа пересмотрена на заседании департамента:

Протокол от «_____» _____ 20___ г. № _____

Директор департамента _____ _____
(подпись) (И.О. Фамилия)

Цели и задачи освоения дисциплины:

Цель: раскрыть смысл ключевых понятий информационной безопасности в телекоммуникационных сетях, сформировать представление о методах и средствах технической защиты информации и сторон инфокоммуникационных протоколов.

Задачи:

- приобретение студентами базового набора представлений о целях и средствах защиты данных и участников телекоммуникационных протоколов, об угрозах безопасности и способах противодействия им.
- ознакомить студентов с элементарными и составными средствами криптографической и стенографической защиты данных и участников информационного обмена.

Для успешного изучения дисциплины «Методы и средства защиты информации» у обучающихся должны быть сформированы следующие предварительные компетенции:

- способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач (УК-1);
- способен осуществлять социальное взаимодействие и реализовывать свою роль в команде (УК-3);
- способен осуществлять деловую коммуникацию в устной и письменной формах на государственном языке Российской Федерации и иностранном(ых) языке(ах) (УК-4).

Планируемые результаты обучения по данной дисциплине (знания, умения, владения), соотнесенные с планируемыми результатами освоения образовательной программы, характеризуют этапы формирования следующих компетенций.

Общепрофессиональные компетенции выпускников и индикаторы их достижения

Наименование категории (группы) общепрофессиональных компетенций	Код и наименование общепрофессиональной компетенции (результат освоения)	Код и наименование индикатора достижения компетенции
	ОПК-1 Способен использовать положения, законы и методы естественных наук и математики для решения задач инженерной деятельности	ОПК-1.1 Выделяет известные физические и математические законы в явлениях окружающего мира
		ОПК-1.2 Применяет физические законы и математические методы для решения задач теоретического и прикладного характера

	ОПК-3 Способен применять методы поиска, хранения, обработки, анализа и представления в требуемом формате информации из различных источников и баз данных, соблюдая при этом основные требования информационной безопасности	ОПК-3.1 Применяет принципы, основные алгоритмы и устройства цифровой обработки сигналов
		ОПК-3.2 Решает задачи обработки данных с помощью современных средств цифровой вычислительной техники
		ОПК-3.3 Строит вероятностные модели для конкретных процессов, проводит необходимые расчеты в рамках построенной модели

Код и наименование индикатора достижения компетенции	Наименование показателя оценивания (результата обучения по дисциплине)
ОПК-1.1 Выделяет известные физические и математические законы в явлениях окружающего мира	Знает фундаментальное математическое и физическое обоснование защиты информации и данных, взаимодействия через инфокоммуникационный канал связи, заданный логическим или физическим представлением, математической моделью.
	Умеет выполнять обоснование задач информационной безопасности, основываясь на сформированном представлении о физике информации и каналов инфокоммуникации, на ее отображении на математическую модель.
	Владеет навыками реализации задач информационной безопасности и о методах ее реализации, опираясь на научное и формальное представление об информации, о физическое реализуемости сетей связи, методах их формального математического обоснования.
ОПК-1.2 Применяет физические законы и математические методы для решения задач теоретического и прикладного характера	Знает методы математического моделирования и обоснования эффективности
	Умеет выполнять формальное обоснование задачи информационной безопасности в терминах математических и физических закономерностей, информатики и информационной безопасности.
	Владеет представлением об информационной безопасности и о методах ее реализации, основываясь на фундаментальных законах математики, информатики и физики, методами обоснования задач предметной области на их основе.
ОПК-3.1 Применяет принципы, основные алгоритмы и устройства цифровой обработки сигналов	Знает основные формы представления информации и данных, а также защиты участников информационного обмена на основе положений теорий алгоритмов и сложности, релевантные положения дискретной математики, математического анализа и теории вероятности

Код и наименование индикатора достижения компетенции	Наименование показателя оценивания (результата обучения по дисциплине)
	Умеет обосновать задачу информационной безопасности в инфокоммуникационных сетях, построить ее математическую модель, использующую методы цифровой обработки сигналов, а также методов ее реализации в контексте требований к функциональной эффективности с использованием математического формализма и формальноязыковых средств.
	Владеет навыками адекватного описания задач и методов цифровой обработки сигналов для реализации задач информационной безопасности в привязке к выбранной системе показателей и критериев эффективности.
ОПК-3.2 Решает задачи обработки данных с помощью современных средств цифровой вычислительной техники	Знает методы априорной и апостериорной оценки информационной безопасности инфотелекоммуникационных систем, аспекты безопасности информационных систем, обусловленные их развертыванием, введением в эксплуатацию и передачей третьей стороне.
	Умеет выбирать и реализовывать основные методы обеспечения информационной безопасности посредством криптографических протоколов и алгоритмов.
	Владеет навыками реализации комплексных задач информационной безопасности, возникающих в профессиональной деятельности, опираясь на актуальные требования к стойкости, оперативности и ресурсоемкости, обоснования этих требований в контексте эффективности современной вычислительной техники.
ОПК-3.3 Строит вероятностные модели для конкретных процессов, проводит необходимые расчеты в рамках построенной модели	Знает методы построения и анализа математических вероятностных моделей информационных сетей и систем для реализации задач информационной безопасности.
	Умеет применять различные формы представления чувствительной информации в компьютерных устройствах и сетях, а также выполнять реализацию методов информационной безопасности в системах и сетях на основе положений теорий алгоритмов и сложности, релевантные положения дискретной математики, математического анализа и теории вероятности
	Владеет базовыми навыками анализа безопасности информационных систем и синтеза формальных вероятностных моделей систем информационной безопасности на основе определенных критериев информационной безопасности.

Трудоемкость освоения дисциплины составляет 3 зачетные единицы (108 часов), 1 зачетная единица соответствует 36 академическим часам. Дисциплина реализуется на 3 курсе в 5 семестре.

Видами учебных занятий и работы обучающегося по дисциплине могут являться:

Обозначение	Виды учебных занятий и работы обучающегося
Лек	Лекции
Лаб	Лабораторные работы
Пр	Практические занятия
ОК	Онлайн курс
СР	Самостоятельная работа обучающегося в период теоретического обучения
Контроль	Самостоятельная работа обучающегося и контактная работа обучающегося с преподавателем в период промежуточной аттестации

Структура дисциплины:

Форма обучения – очная.

№	Наименование раздела дисциплины	Семестр	Количество часов по видам учебных занятий и работы обучающегося						Формы промежуточной и текущей аттестации
			Лек	Лаб	Пр	ОК	СР	Контроль	
1	Распределенные информационные системы	3	36	18	18	0	9	27	Экзамен
	Итого:		36	18	18	0	9	27	

Для формирования вышеуказанных компетенций в рамках дисциплины «Основы информационной безопасности сетей связи» не применяются методы активного/ интерактивного обучения.

I. СТРУКТУРА И СОДЕРЖАНИЕ ТЕОРЕТИЧЕСКОЙ ЧАСТИ КУРСА (36 ЧАСОВ)

Тема 1. Политики и модели безопасности вычислительных сетей и систем (8 час)

Введение в курс. Основные понятия и определения. Угрозы, уязвимости телекоммуникационных сетей и систем. Задачи обеспечения информационной безопасности сетей. Понятие политики безопасности. Основные типы политики безопасности. Модели безопасности. Дискреционные модели распространения прав доступа. Мандатные модели распространения прав доступа. Модели безопасности основных операционных систем.

Тема 2. Требования к информационной безопасности телекоммуникационных сетей и систем (4 час)

Международные и государственные стандарты безопасности информации. Классификация автоматизированных систем и нормативные требования по обеспечению безопасности информации. Требования по обеспечению защиты от НСД.

Тема 3. Методы и средства защиты информации в телекоммуникационных сетях (8 час)

Классификация методов и средств защиты информации. Модель нарушителя и классификация средств криптографической защиты информации. Требования к программным и аппаратным компонентам информационной защиты.

Тема 4. Математическое обоснование методов и криптографических средств защиты информационной безопасности (4 час)

Классы вычислительных проблем. Теория сложности применительно к примитивам и системам информационной безопасности. Классы сложности, NP-полнота. Примеры сложных проблем. Понятие алгебраической группы, кольца и поля; операции над ними. Примеры групп перестановок применительно к анализу перестановочных шифров. Абелевы группы. Циклические группы. Поля Галуа.

Тема 5. Средства криптографической защиты информации в телекоммуникационных сетях (6 час)

Стандарт шифрования данных ГОСТ-28147-89. Назначение, алгоритм шифрования, основные режимы работы. Шифрование в режимах простой замены и гаммирования. Режим формирования и проверки имитовставки. Особенности аппаратной и программной реализации алгоритмов шифрования. Стандарт шифрования данных AES. Построение и использование криптографической хеш-функции. Принцип построение пошаговой хеш-функции. Анализ хеширующего преобразования. Применение асимметричной криптографии. Стандарт электронной цифровой подписи. Управление ключами в криптографических системах защиты информации. Назначение, классификация и требования к ключам. Генерация ключевой информации.

Хранение и распределение ключевой информации. Алгоритм RSA. Эллиптические кривые в криптографии.

Тема 6. Криптографические протоколы (6 часов)

Обзор атак на протоколы и методы противодействия им. Элементарные протоколы: протокол разделения секрета, протокол доказательства с нулевым разглашением, протокол подбрасывания честной монеты. Протоколы аутентификации участников протокола. Протоколы электронного голосования.

II. СОДЕРЖАНИЕ ПРАКТИЧЕСКОЙ ЧАСТИ КУРСА И САМОСТОЯТЕЛЬНОЙ РАБОТЫ

Практические занятия (18 часов)

Практическое занятие № 1. Математические основы криптографии (4 часа)

Алгебраические структуры: кольца, поля. Элементы алгебраических групп. Аддитивность и мультипликативность групп.

Классы и системы вычетов. Отображение целочисленных данных на кольца и поля. Поиск аддитивной и мультипликативной инверсии в кольцах. Расширенный алгоритм Евклида. Линейные диофантовы уравнения. Решение линейных алгебраических уравнений и систем уравнений над полями. Операции с матрицами с элементами, определенными на конечных кольцах.

Практическое занятие № 2. Традиционные шифры с симметричным ключом (2 часа)

Базовые протоколы использования симметричных шифров. Анализ протоколов распределения ключей симметричного шифрования. Аддитивные, мультипликативные и аффинные шифры и их анализ. Автоключевой шифр и его анализ. Шифр Виженера. Шифр Хилла. Шифр Плейфнера. Простые перестановочные шифры. Блочные шифры. Потоковые шифры с гаммированием.

Практическое занятие № 3. Оценка стойкости хеш-функций методом простого перебора и поиском коллизий (2 часа)

Оценить максимальное количество вычислений N-битовой хеш-функции для ее вскрытия, когда необходимо найти сообщение, которое производит

заданный хеш и когда необходимо найти пару сообщений, дающих одинаковый хеш. Привести сценарии, при котором вскрытие вторым способом будет иметь смысл.

Практическое занятие № 4. Методы ассиметричной криптографии (4 часа)

Описать протоколы шифрования и электронной цифровой подписи сообщений между двумя собеседниками. Проанализировать возможности атаки на телекоммуникационные системы, использующую ассиметричные методы, методом «человек-в-середине» и методом повторной отправки сообщения.

Пусть имеется система-получатель сообщений с автоматической отправкой подтверждения, автоматически и всегда верифицируя пришедшие данные, затем дешифруя их, затем шифруя результат собственным открытым ключом и подписывает, после чего осуществляет отправку сообщения обратно. Пусть используется примитив ассиметричной криптографии, такой как RSA, в котором операции шифрования и верификации, а также операции дешифрования и цифровой подписи попарно одинаковы. Проанализировать стойкость такой телекоммуникационной системы.

Сгенерировать пару ключей RSA и продемонстрировать работу шифра при шифровании своего имени и затем дешифровании результата, а также подписи и верификации.

Практическое занятие № 5. Протоколы распределения симметричных ключей шифрования (1 час)

Составить диаграмму последовательностей, на которой показать возможные протоколы распределения ключей симметричного шифрования с помощью посредника.

Применить и проанализировать алгоритм Диффи-Хеллмана для распределения ключей шифрования с использованием простого дискретного логарифма в поле вычетов. Стоек ли метод, если подлинность коммутирующих сторон взаимно не подтверждена?

Практическое занятие № 6. Режимы работы блочных шифров на примере аффинного шифра (3 часа)

С помощью выбранного аффинного шифра (т.е. ключа) и произвольно выбранных дополнительных параметров (если требуются) зашифровать собственную фамилию в режимах ECB, CBC, PCBC, OFB, CFB и CTR. Пусть размер блока аффинного шифра соответствует трем символам входного открытого текста. Проанализировать возможные методы выравнивания входных данных с обеспечением обратимости операции.

Практическое занятие № 7. Методы получения имитовставки HMAC и CBC-MAC (2 часа)

Рассчитать значение функций HMAC и CBC-MAC над своей фамилией и с произвольно выбранным ключом. В качестве хеш-функции использовать функцию $h(X) = \bigoplus_{i=1}^{N} x'_i$, а в качестве блочного шифра – $E(x,k) = x \oplus k$, с размером блока и ключа, равным трем байтам. Один символ открытого текста должен быть умещаем в один байт. Для кодировки символов использовать предоставленную таблицу ANSI ASCII.

Лабораторные работы (18 часов)

Лабораторная работа №1. Комплекс решений для шифрования PGP и работа с ним с помощью OpenPGP (4 часа)

Разбиться на пары, затем используя программу GnuPG Kleopatra сгенерировать собственные сертификаты пользователя и осуществить передачу произвольных сообщений напарнику. Пришедшее сообщение расшифровать и верифицировать.

Лабораторная работа №2. Алгоритмическая и программная реализация алгоритма распределения Диффи-Хеллмана над точками выбранной эллиптической кривой. (9 час.)

С помощью заданного генератора синтезировать поле с характеристикой, не равной двум и трем. Записать алгоритм, принимающий на вход параметры эллиптической кривой и точку на ней, а также выполняющий умножение этой точки на натуральное число. Реализовать алгоритм на языке программирования C или C++. Показать реализацию распределения ключей симметричного шифрования и цифровой подписи, с использованием реализации.

Лабораторная работа №3. Реализация протокола «Ментальный покер» (1 час.)

Разбиться на пары и реализовать партию игры в покер, выполняя протокол Ментального покера на основе шифра RSA. Реализация шифра RSA предоставляется. Оценить возможности по обману собеседника.

Лабораторная работа №4. Реализация протокола доказательства с нулевым разглашением с помощью потокового шифра на основе линейного конгруэнтного генератора гаммы. (4 час.) Показать и реализовать протокол доказательства с нулевым разглашением, на основе шифрования случайных байтовых строк, и составляющие его алгоритмы потокового шифра. Реализовать линейный конгруэнтный генератор с

множителем 0x7FFFFFED и смещением 0x7FFFFFC3. Применить генератор для получения гаммы потокового шифра. Показать применение потокового шифра для реализации вышеупомянутого протокола доказательства с нулевым разглашением с использованием изменяемого состояния. Показать уязвимости протокола, без рассмотрения примененных примитивов.

Самостоятельная работа №1. Арифметика конечных полей характеристики 2 и их применение в задачах информационной безопасности.

Рассмотреть применение математики конечного поля для реализации функций информационной безопасности сетей связи. Рассмотреть использование определенных над этими полями арифметических операций сложения и вычитания, умножения, деления. Методы генерации элементов поля, вопросы обратимости элементов и их отображений, алгоритмы для вычисления таких отображений. Рассмотреть применение аффинных операций над скалярами и матрицами, определенными над конечным полем. Рассмотреть алгоритмы быстрой инверсии матриц и поиска решений СЛАУ для реализации симметричных блочных шифров на основе арифметики конечных полей.

Требования:

1. Знать элементарные методы и тождества модульной арифметики.
2. Уметь выполнять арифметические операции над полиномами.
3. Знать и понимать базовый и расширенный алгоритмы Эвклида и их применение для поиска мультипликативных инверсий и решений диофантовых уравнений первого порядка.
4. Знать аксиомы алгебраических колей и полей, критерии мультипликативной инвертируемости элемента целочисленного факторкольца.
5. Знать критерий существования корней полиномов в конечном поле.
6. Знать методы основных арифметических операций над матрицами: сложение/вычитание, умножение, правое и левое деление, Гауссово преобразование, триангуляция и LU-разложение.
7. Знать методы использования матричных операций над кольцами для осуществления аффинных преобразований данных и реализации блочного шифрования.

Темы для обсуждения

1. Аффинные шифры и аффинные преобразования, определенные над конечными кольцами.
2. Использование конечных полей в задачах криптографической

обработки бинарных данных.

3. Поиск мультипликативной инверсии элемента в конечном поле путем выполнения расширенного алгоритма Эвклида над этим элементом и неприводимым полиномом, определенным для поля.

4. Реализация аффинного шифра над скалярами, принадлежащими конечному полю, ключей, открытого текста и шифротекста. Пример выполнения операций шифрования и дешифрования. Пример атаки с известным открытым текстом.

5. Реализация блочного шифра, основанного на матричном аффинном преобразовании вектора открытого текста. Пример мультипликативной инверсии матрицы на основе LU-разложения. Реализация дешифрования. Пример шифрования и дешифрования трехбайтового блока данных и с использованием матрицы 3x3 в качестве мультипликативной части ключа.

6. Циклическая генерация элементов конечного поля.

7. Дискретное логарифмирование в конечном поле.

Самостоятельная работа №2. Функция и теорема Эйлера, ее применение для математического обоснования алгоритмов информационной безопасности, основанных на дискретном логарифмировании в конечном поле.

Функция Эйлера. Ее вывод и применение для оценки размера наибольшей мультипликативной подгруппы числового факторкольца. Теорема Лагранжа и ее вывод в терминах теории групп. Применение теоремы Лагранжа для обоснования и доказательства малой теоремы Ферма и теоремы Эйлера. Методы расчета показательной функции в факторкольце и мультипликативных группах. Применимость теоремы Лагранжа для реализации степенной функции над нечисловыми группами.

Алгоритмы асимметричной криптографии, основанные на операции возведения в степень в поле. Распределение ключей Диффи-Хеллмана. Алгоритм RSA и обратимость показательной функции.

Требования:

1. Уметь выполнять анализ счетных и конечных множеств и их отношений.

2. Знать аксиомы алгебраических групп, колец и полей. Знать условие мультипликативной обратимости в кольце и уметь генерировать циклические мультипликативные подгруппы.

3. Знать метод генерации ключей RSA и метода шифрования и дешифрования; уметь обосновать эти операции.

4. Умение обосновать реализуемость RSA для операций цифровой

подписи и шифрования с одной парой ключей.

5. Знать и уметь показать связь стойкости шифра RSA со сложностью разложения на простые сомножители.

6. Условия применения RSA и DSA со стойкой хеш-функцией.

Темы для обсуждения

1. Функция Эйлера и ее применение в задачах вычисления полиномиальной функции над конечным числовым полем.

2. Теорема Лагранжа и ее применение для увеличения оперативности вычисления целочисленной степени в группе.

3. Малая теорема Ферма и теорема Эйлера.

4. Доказательство обратимости операций шифрования/дешифрования RSA.

5. Вычисление степени в конечном поле и применимость RSA над конечным полем.

6. Электронная цифровая подпись RSA, RSA с хеш, DSA.

7. Распределение ключей Диффи-Хеллмана, определенных в конечном поле.

Самостоятельная работа №3. Критерий Эйлера и вычисление квадратичных вычетов в конечном поле.

Рассмотреть основные аспекты реализации проверки существования квадратного корня в мультипликативной группе и кольце, а также алгоритмы вычисления такого корня.

Требования:

1. Знать особенности вычисления показательных функций в группах и кольцах.

2. Знать методы генерации циклических групп и конечных полей.

3. Знать основные свойства показательной функции и арифметического корня.

Темы для обсуждения

1. Аналитическое обоснование критерия Эйлера.

2. Применение малой теоремы Ферма для вычисления квадратичного вычета в числовой мультипликативной группе с простым числом элементов.

3. Применение теорем Эйлера и Лагранжа для вычисления квадратичных вычетов в конечных группах общего вида.

Самостоятельная работа №4. Реализация эллиптической кривой, определенной над конечном поле, и ее применение для распределения ключей ECDH.

Рассмотреть понятие эллиптической кривой, определенной над полями действительных и комплексных чисел, а также над конечным полем. Рассмотреть метод выбора точек на эллиптической кривой, группу точек, с точкой в бесконечности, на эллиптической кривой над конечным полем, определение, обоснование и выполнение аксиом групповой операции над точками. Рассмотреть дополнительные требования к эллиптической кривой и полю, обеспечивающие реализуемость групповой операции для задач информационной безопасности. Рассмотреть примеры применения эллиптической кривой для решения криптографических задач, включая реализацию распределения ключей Диффи-Хеллмана.

Требования:

1. Уметь решать кубические и квадратичные уравнения.

2. Уметь выполнять основные арифметические операции в полях.

3. Знать методы нахождения точек пересечений прямой с кривыми, методы нахождения касательных и дифференцирования.

4. Уметь применять арифметику конечных полей и групп для реализации составных задач обработки данных, включая задачи информационной безопасности.

Темы для обсуждения

1. Метод построения и определения эллиптической кривой и ей уравнение.

2. Метод выбора произвольных (случайных) точек на заданной эллиптической кривой.

3. Групповая операция на множестве точек эллиптической кривой.

4. Аксиомы групповой операции.

5. Применение групп точек на эллиптической кривой для реализации задач информационной безопасности и стойкость дискретного логарифмирования в группе.

6. Требования к полю, на котором определена эллиптическая кривая с точки зрения реализуемости.

7. Требования к параметрам эллиптической кривой и определяющему ее конечному полу с точки зрения стойкости.

План-график выполнения самостоятельной работы по дисциплине

Очная форма обучения.

№ п/п	Дата/сроки выполнения	Вид самостоятельной работы	Примерные нормы времени на выполнение	Форма контроля

1.	4 неделя обучения	Арифметика конечных полей характеристики 2 и их применение в задачах информационной безопасности.	3 часа	Собеседование (УО-1)
2.	6 неделя обучения	Функция и теорема Эйлера, ее применение для математического обоснования алгоритмов информационной безопасности, основанных на дискретном логарифмировании в конечном поле.	3 часа	Собеседование (УО-1)
3.	6 неделя обучения	Критерий Эйлера и вычисление квадратичных вычетов в конечном поле.	2 часа	Собеседование (УО-1)
4.	6 неделя обучения	Реализация эллиптической кривой, определенной над конечном поле, и ее применение для распределения ключей ECDH.	1 час	Собеседование (УО-1)
13.	В течение семестра	Подготовка к экзамену	5 часов	Экзамен

III. УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ САМОСТОЯТЕЛЬНОЙ РАБОТЫ ОБУЧАЮЩИХСЯ

Учебно-методическое обеспечение самостоятельной работы обучающихся по дисциплине «Основы информационной безопасности сетей связи» включает в себя:

- план-график выполнения самостоятельной работы по дисциплине, в том числе примерные нормы времени на выполнение по каждому заданию;
- характеристика заданий для самостоятельной работы обучающихся и методические рекомендации по их выполнению;
- требования к представлению и оформлению результатов самостоятельной работы;
- критерии оценки выполнения самостоятельной работы.

Самостоятельные работы проводятся на рабочих местах с доступом к ресурсам Internet и в домашних условиях. Порядок выполнения

самостоятельной работы соответствует программе курса и контролируется в ходе аудиторных занятий. Самостоятельная работа подкрепляется учебно-методическим и информационным обеспечением, включающим рекомендованные учебники и учебно-методические пособия.

Самостоятельная работа считается выполненной, если в отчете по проделанной работе представлено письменные пояснения к полученным выводам и, если требуется, код программной реализации, компилируемый и выполняющий задачу корректно.

Проводится проверка правильности выполнения заданий по самостоятельной работе. Задание зачтено, если нет ошибок. По текущим ошибкам даются пояснения.

Методические рекомендации по выполнению заданий для самостоятельной работы и критерии оценки.

Самостоятельная работа №1. Для успешного выполнения работы от обучающегося требуется:

1) знать основные арифметические операции над конечными множествами целочисленных элементов;

2) знать методы и основные тождества модульной арифметики, ее применение для реализации аффинных шифров.

Выполнение самостоятельной работы должно быть основано на материале аудиторных занятий, проведенных к моменту выдачи задания, а также на информационных источниках, приведенных в разделе V.

Критерии оценки.

Оценка	Требования
«зачтено»	Студент умеет анализировать требования, предъявляемые заданием, выполнять формализацию знаний с помощью математического формализма и формулировать теоретическое обоснование используемых алгоритмических методов для решения задач обработки данных. Работа соответствует требованиям и выполнена в установленные сроки.
«не зачтено»	Не раскрыта структура и теоретическая составляющая темы. Студент не умеет анализировать требования, предъявляемые заданием, выполнять их формализацию и обоснование. Проект не выполнен.

Самостоятельная работа №2. Для успешного выполнения работы от обучающегося требуется:

1) знать принципы логического представления элементарных целочисленных данных в вычислительной технике и устройствах цифровой обработки сигналов и данных;

2) методы реализации основных арифметических операций в конечных кольцах и полях, реализуемых вычислительной техникой и устройствами цифровой обработки сигналов и данных;

3) знать методы анализа делимости чисел, применение базового и расширенного алгоритма Эвклида;

4) методы генерации циклических групп и подгрупп;

5) интерпретация теоремы Лагранжа для анализа алгебраических групп;

6) обратимость показательного преобразования.

Выполнение самостоятельной работы должно быть основано на материале аудиторных занятий, проведенных к моменту выдачи задания, а также на информационных источниках, приведенных в разделе V.

Критерии оценки.

Оценка	Требования
«зачтено»	Студент умеет анализировать требования, предъявляемые заданием, выполнять их формализацию, объяснять применение показательного преобразования в группах и конечных полях, объяснять проблему дискретного логарифмирования в контексте решения задач информационной безопасности. Работа соответствует требованиям и выполнена в установленные сроки.
«не зачтено»	Не раскрыта структура и теоретическая составляющая темы. Студент не умеет анализировать требования, предъявляемые заданием, выполнять их формализацию, интерпретировать и объяснять обратимость показательного преобразования в конечном поле, объяснять применение преобразования для реализации задач информационной безопасности в инфокоммуникационных протоколах, привязываясь в своем объяснении к проблемам поиска значения функции Эйлера, разложения на простые сомножители и дискретного логарифмирования. Проект не выполнен.

Самостоятельная работа №3. Для успешного выполнения работы от обучающегося требуется:

1) знать алгоритмическую реализацию возведения в целочисленную степень в конечных и счетных группах и кольцах на основе теоремы Лагранжа;

2) знать теоремы Ферми и Эйлера и использовать их для вычисления показательной функции в конечном поле или мультипликативной группе;

3) знать основные свойства показательной функции и арифметического корня;

4) знать и уметь применять арифметику циклических групп для поиска квадратичных вычетов в конечных мультипликативных группах.

Выполнение самостоятельной работы должно быть основано на материале аудиторных занятий, проведенных к моменту выдачи задания, а также на информационных источниках, приведенных в разделе V.

Критерии оценки.

Оценка	Требования
«зачтено»	Студент успешно применяет критерий Эйлера теста существования квадратичных вычетов для произвольных элементов числовых мультипликативных групп, объяснять его применение. Работа соответствует требованиям и выполнена в установленные сроки.
«не зачтено»	Студент в устных ответах не раскрывает суть критерия Эйлера, не может обосновать его формально, опираясь на теоремы Ферма и Эйлера. Студент не умеет вычислять квадратичный вычет в поле. Его

	работа не соответствует требованиям или не выполнена в установленные сроки.

Самостоятельная работа №4. Для успешного выполнения работы от обучающегося требуется:

1) знать методы проверки существования и поиска решения квадратичных уравнений в конечных мультипликативных группах;

2) уметь решать задачи поиска пересечений прямых с кривой;

3) уметь составляю уравнение касательной к кривой в точке;

4) уметь возводить элементы нечисловых групп в целочисленную степень и выполнять генерацию циклических подгрупп;

5) выполнять составные арифметические действия над элементами конечного поля.

Выполнение самостоятельной работы должно быть основано на материале аудиторных занятий, проведенных к моменту выдачи задания, а также на информационных источниках, приведенных в разделе V.

Критерии оценки.

Оценка	Требования
«зачтено»	Студент умеет выбирать произвольные точки на эллиптической кривой и решать квадратичные уравнения в конечном поле. Студент успешно генерирует циклическую подгруппу точек на эллиптической кривой, используя произвольный генератор. Студент умеет применять арифметику группы точек на эллиптической кривой для реализации распределения ключей, выполняя над точкой и показателями степени алгоритм Диффи-Хеллмана. Работа соответствует требованиям и выполнена в установленные сроки.
«не зачтено»	Не раскрыта структура и теоретическая составляющая темы. Студент не умеет выбирать произвольные точки на эллиптической кривой и решать квадратичные уравнения в конечном поле; или студент не может генерировать циклическую подгруппу точек на эллиптической кривой, используя произвольный генератор; или студент не умеет применять арифметику группы точек на эллиптической кривой для реализации распределения ключей, выполняя над точкой и показателями степени алгоритм Диффи-Хеллмана. Работа не соответствует требованиям или не выполнена в установленные сроки.

IV. КОНТРОЛЬ ДОСТИЖЕНИЯ ЦЕЛЕЙ КУРСА

№ п/п	Контролируемые модули/ разделы / темы дисциплины	Код индикатора достижения компетенции	Результаты обучения	Оценочные средства – наименование	
				текущий контроль	промежуточная аттестация
1	Политики и модели безопасности вычислительных сетей и систем	ОПК-1.1 Выделяет известные физические и математические законы в явлениях	Знает фундаментальное математическое и физическое обоснование защиты информации и данных, взаимодействия через инфокоммуникационный канал связи, заданный	Собеседование (УО-1); дискуссия (УО-4); лабораторная работа (ПР-6);	Экзаменационные вопросы 5, 7, 9, 10, 11, 13, 21, 23

		окружающего мира	логическим или физическим представлением, математической моделью.	конспект (ПР-7); разноуровневые задачи и задания (ПР-11).	
			Умеет выполнять обоснование задач информационной безопасности, основываясь на сформированном представлении о физике информации и каналов инфокоммуникации, на ее отображении на математическую модель.	Собеседование (УО-1); дискуссия (УО-4); лабораторная работа (ПР-6); конспект (ПР-7); разноуровневые задачи и задания (ПР-11).	Экзаменационные вопросы 5, 7, 9, 10, 11, 13, 21, 23
			Владеет навыками реализации задач информационной безопасности и о методах ее реализации, опираясь на научное и формальное представление об информации, о физическое реализуемости сетей связи, методах их формального математического обоснования.	Собеседование (УО-1); дискуссия (УО-4); лабораторная работа (ПР-6); конспект (ПР-7); разноуровневые задачи и задания (ПР-11).	Экзаменационные вопросы 5, 7, 9, 10, 11, 13, 21, 23
		ОПК-1.2 Применяет физические законы и математические методы для решения задач теоретического и прикладного характера	Знает методы математического моделирования и обоснования эффективности	Собеседование (УО-1); дискуссия (УО-4); лабораторная работа (ПР-6); конспект (ПР-7); разноуровневые задачи и задания (ПР-11).	Экзаменационные вопросы 2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32
			Умеет выполнять формальное обоснование задачи информационной безопасности в терминах математических и физических закономерностей, информатики и информационной безопасности.	Собеседование (УО-1); дискуссия (УО-4); лабораторная работа (ПР-6); конспект (ПР-7); разноуровневые задачи и задания (ПР-11).	Экзаменационные вопросы 2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32
			Владеет представлением об информационной безопасности и о методах ее реализации,	Собеседование (УО-1); дискуссия (УО-4);	Экзаменационные вопросы 2, 4, 6, 8, 10, 12, 14, 16, 18, 20,

			основываясь на фундаментальных законах математики, информатики и физики, методами обоснования задач предметной области на их основе.	лабораторная работа (ПР-6); конспект (ПР-7); разноуровневые задачи и задания (ПР-11).	22, 24, 26, 28, 30, 32
2	Требования к информационной безопасности телекоммуникационных сетей и систем	ОПК-1.1 Выделяет известные физические и математические законы в явлениях окружающего мира	Знает фундаментальное математическое и физическое обоснование защиты информации и данных, взаимодействия через инфокоммуникационный канал связи, заданный логическим или физическим представлением, математической моделью.	Собеседование (УО-1); дискуссия (УО-4); лабораторная работа (ПР-6); конспект (ПР-7); разноуровневые задачи и задания (ПР-11).	Экзаменационные вопросы 2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32
			Умеет выполнять обоснование задач информационной безопасности, основываясь на сформированном представлении о физике информации и каналов инфокоммуникации, на ее отображении на математическую модель.	Собеседование (УО-1); дискуссия (УО-4); лабораторная работа (ПР-6); конспект (ПР-7); разноуровневые задачи и задания (ПР-11).	Экзаменационные вопросы 2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32
			Владеет навыками реализации задач информационной безопасности и о методах ее реализации, опираясь на научное и формальное представление об информации, о физическое реализуемости сетей связи, методах их формального математического обоснования.	Собеседование (УО-1); дискуссия (УО-4); лабораторная работа (ПР-6); конспект (ПР-7); разноуровневые задачи и задания (ПР-11).	Экзаменационные вопросы 2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32
3	Методы и средства защиты информации в телекоммуникационных сетях	ОПК-3.3 Строит вероятностные модели для конкретных процессов, проводит необходимые расчеты в рамках построенной модели	Знает методы построения и анализа математических вероятностных моделей информационных сетей и систем для реализации задач информационной безопасности.	Собеседование (УО-1); дискуссия (УО-4); лабораторная работа (ПР-6); конспект (ПР-7); разноуровневые задачи и задания (ПР-11).	Экзаменационные вопросы 1, 5, 11, 15, 21.

			Умеет применять различные формы представления чувствительной информации в компьютерных устройствах и сетях, а также выполнять реализацию методов информационной безопасности в системах и сетях на основе положений теорий алгоритмов и сложности, релевантные положения дискретной математики, математического анализа и теории вероятности	Собеседование (УО-1); дискуссия (УО-4); лабораторная работа (ПР-6); конспект (ПР-7); разноуровневые задачи и задания (ПР-11).	Экзаменационные вопросы 1, 5, 11, 15, 21.
			Владеет базовыми навыками анализа безопасности информационных систем и синтеза формальных вероятностных моделей систем информационной безопасности на основе определенных критериев информационной безопасности.	Собеседование (УО-1); дискуссия (УО-4); лабораторная работа (ПР-6); конспект (ПР-7); разноуровневые задачи и задания (ПР-11).	Экзаменационные вопросы 1, 5, 11, 15, 21.
4	Математическое обоснование методов и криптографических средств защиты информационной безопасности	ОПК-1.2 Применяет физические законы и математические методы для решения задач теоретического и прикладного характера	Знает методы математического моделирования и обоснования эффективности	Собеседование (УО-1); дискуссия (УО-4); лабораторная работа (ПР-6); конспект (ПР-7); разноуровневые задачи и задания (ПР-11).	Экзаменационные вопросы 3, 12, 16, 17, 19, 25, 27, 29.
			Умеет выполнять формальное обоснование задачи информационной безопасности в терминах математических и физических закономерностей, информатики и информационной безопасности.	Собеседование (УО-1); дискуссия (УО-4); лабораторная работа (ПР-6); конспект (ПР-7); разноуровневые задачи и задания (ПР-11).	Экзаменационные вопросы 3, 12, 16, 17, 19, 25, 27, 29.
			Владеет представлением об информационной безопасности и о методах ее реализации, основываясь на фундаментальных	Собеседование (УО-1); дискуссия (УО-4);	Экзаменационные вопросы 3, 12, 16, 17, 19, 25, 27, 29.

			законах математики, информатики и физики, методами обоснования задач предметной области на их основе.	лабораторная работа (ПР-6); конспект (ПР-7); разноуровневые задачи и задания (ПР-11).	
		ОПК-3.1 Применяет принципы, основные алгоритмы и устройства цифровой обработки сигналов	Знает основные формы представления информации и данных, а также защиты участников информационного обмена на основе положений теорий алгоритмов и сложности, релевантные положения дискретной математики, математического анализа и теории вероятности	Собеседование (УО-1); дискуссия (УО-4); лабораторная работа (ПР-6); конспект (ПР-7); разноуровневые задачи и задания (ПР-11).	Экзаменационные вопросы 5, 7, 9, 10, 11, 13, 21, 23
			Умеет обосновать задачу информационной безопасности в инфокоммуникационных сетях, построить ее математическую модель, использующую методы цифровой обработки сигналов, а также методов ее реализации в контексте требований к функциональной эффективности с использованием математического формализма и формальноязыковых средств.	Собеседование (УО-1); дискуссия (УО-4); лабораторная работа (ПР-6); конспект (ПР-7); разноуровневые задачи и задания (ПР-11).	Экзаменационные вопросы 5, 7, 9, 10, 11, 13, 21, 23
			Владеет навыками адекватного описания задач и методов цифровой обработки сигналов для реализации задач информационной безопасности в привязке к выбранной системе показателей и критериев эффективности.	Собеседование (УО-1); дискуссия (УО-4); лабораторная работа (ПР-6); конспект (ПР-7); разноуровневые задачи и задания (ПР-11).	Экзаменационные вопросы 5, 7, 9, 10, 11, 13, 21, 23
		ОПК-3.3 Строит вероятностные модели для конкретных процессов, проводит необходимые расчеты в	Знает методы построения и анализа математических вероятностных моделей информационных сетей и систем для реализации задач информационной безопасности.	Собеседование (УО-1); дискуссия (УО-4); лабораторная работа (ПР-6); конспект (ПР-7);	Экзаменационные вопросы 2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32

		рамках построенной модели		разноуровневые задачи и задания (ПР-11).	
			Умеет применять различные формы представления чувствительной информации в компьютерных устройствах и сетях, а также выполнять реализацию методов информационной безопасности в системах и сетях на основе положений теорий алгоритмов и сложности, релевантные положения дискретной математики, математического анализа и теории вероятности	Собеседование (УО-1); дискуссия (УО-4); лабораторная работа (ПР-6); конспект (ПР-7); разноуровневые задачи и задания (ПР-11).	Экзаменационные вопросы 2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32
			Владеет базовыми навыками анализа безопасности информационных систем и синтеза формальных вероятностных моделей систем информационной безопасности на основе определенных критериев информационной безопасности.	Собеседование (УО-1); дискуссия (УО-4); лабораторная работа (ПР-6); конспект (ПР-7); разноуровневые задачи и задания (ПР-11).	Экзаменационные вопросы 2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32
5	Средства криптографической защиты информации в телекоммуникационных сетях	ОПК-3.1 Применяет принципы, основные алгоритмы и устройства цифровой обработки сигналов	Знает основные формы представления информации и данных, а также защиты участников информационного обмена на основе положений теорий алгоритмов и сложности, релевантные положения дискретной математики, математического анализа и теории вероятности	Собеседование (УО-1); дискуссия (УО-4); лабораторная работа (ПР-6); конспект (ПР-7); разноуровневые задачи и задания (ПР-11).	Экзаменационные вопросы 2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32
			Умеет обосновать задачу информационной безопасности в инфокоммуникационных сетях, построить ее математическую модель, использующую методы цифровой обработки сигналов, а также методов ее реализации в контексте требований к функциональной эффективности с использованием математического	Собеседование (УО-1); дискуссия (УО-4); лабораторная работа (ПР-6); конспект (ПР-7); разноуровневые задачи и задания (ПР-11).	Экзаменационные вопросы 2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32

			формализма и формальноязыковых средств.		
			Владеет навыками адекватного описания задач и методов цифровой обработки сигналов для реализации задач информационной безопасности в привязке к выбранной системе показателей и критериев эффективности.	Собеседование (УО-1); дискуссия (УО-4); лабораторная работа (ПР-6); конспект (ПР-7); разноуровневые задачи и задания (ПР-11).	Экзаменационные вопросы 2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32
		ОПК-3.2 Решает задачи обработки данных с помощью современных средств цифровой вычислительной техники	Знает методы априорной и апостериорной оценки информационной безопасности инфотелекоммуникационных систем, аспекты безопасности информационных систем, обусловленные их развертыванием, введением в эксплуатацию и передачей третьей стороне.	Собеседование (УО-1); дискуссия (УО-4); лабораторная работа (ПР-6); конспект (ПР-7); разноуровневые задачи и задания (ПР-11).	Экзаменационные вопросы 1, 5, 11, 15, 21.
			Умеет выбирать и реализовывать основные методы обеспечения информационной безопасности посредством криптографических протоколов и алгоритмов.	Собеседование (УО-1); дискуссия (УО-4); лабораторная работа (ПР-6); конспект (ПР-7); разноуровневые задачи и задания (ПР-11).	Экзаменационные вопросы 1, 5, 11, 15, 21.
			Владеет навыками реализации комплексных задач информационной безопасности, возникающих в профессиональной деятельности, опираясь на актуальные требования к стойкости, оперативности и ресурсоемкости, обоснования этих требований в контексте эффективности современной вычислительной техники.	Собеседование (УО-1); дискуссия (УО-4); лабораторная работа (ПР-6); конспект (ПР-7); разноуровневые задачи и задания (ПР-11).	Экзаменационные вопросы 1, 5, 11, 15, 21.
		ОПК-3.3 Строит вероятностны	Знает методы построения и анализа математических	Собеседование (УО-1);	Экзаменационные вопросы 3,

		е модели для конкретных процессов, проводит необходимые расчеты в рамках построенной модели	вероятностных моделей информационных сетей и систем для реализации задач информационной безопасности.	дискуссия (УО-4); лабораторная работа (ПР-6); конспект (ПР-7); разноуровневые задачи и задания (ПР-11).	12, 16, 17, 19, 25, 27, 29.
			Умеет применять различные формы представления чувствительной информации в компьютерных устройствах и сетях, а также выполнять реализацию методов информационной безопасности в системах и сетях на основе положений теорий алгоритмов и сложности, релевантные положения дискретной математики, математического анализа и теории вероятности	Собеседование (УО-1); дискуссия (УО-4); лабораторная работа (ПР-6); конспект (ПР-7); разноуровневые задачи и задания (ПР-11).	Экзаменационные вопросы 3, 12, 16, 17, 19, 25, 27, 29.
			Владеет базовыми навыками анализа безопасности информационных систем и синтеза формальных вероятностных моделей систем информационной безопасности на основе определенных критериев информационной безопасности.	Собеседование (УО-1); дискуссия (УО-4); лабораторная работа (ПР-6); конспект (ПР-7); разноуровневые задачи и задания (ПР-11).	Экзаменационные вопросы 5, 7, 9, 10, 11, 13, 21, 23
6	Криптографические протоколы	ОПК-3.1 Применяет принципы, основные алгоритмы и устройства цифровой обработки сигналов	Знает основные формы представления информации и данных, а также защиты участников информационного обмена на основе положений теорий алгоритмов и сложности, релевантные положения дискретной математики, математического анализа и теории вероятности	Собеседование (УО-1); дискуссия (УО-4); лабораторная работа (ПР-6); конспект (ПР-7); разноуровневые задачи и задания (ПР-11).	Экзаменационные вопросы 5, 7, 9, 10, 11, 13, 21, 23
			Умеет обосновать задачу информационной безопасности в инфокоммуникационных сетях, построить ее математическую модель, использующую методы цифровой обработки	Собеседование (УО-1); дискуссия (УО-4); лабораторная работа (ПР-6);	Экзаменационные вопросы 5, 7, 9, 10, 11, 13, 21, 23

			сигналов, а также методов ее реализации в контексте требований к функциональной эффективности с использованием математического формализма и формальноязыковых средств.	конспект (ПР-7); разноуровневые задачи и задания (ПР-11).	
			Владеет навыками адекватного описания задач и методов цифровой обработки сигналов для реализации задач информационной безопасности в привязке к выбранной системе показателей и критериев эффективности.	Собеседование (УО-1); дискуссия (УО-4); лабораторная работа (ПР-6); конспект (ПР-7); разноуровневые задачи и задания (ПР-11).	Экзаменационные вопросы 2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32
		ОПК-3.2 Решает задачи обработки данных с помощью современных средств цифровой вычислительной техники	Знает методы априорной и апостериорной оценки информационной безопасности инфотелекоммуникационных систем, аспекты безопасности информационных систем, обусловленные их развертыванием, введением в эксплуатацию и передачей третьей стороне.	Собеседование (УО-1); дискуссия (УО-4); лабораторная работа (ПР-6); конспект (ПР-7); разноуровневые задачи и задания (ПР-11).	Экзаменационные вопросы 2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32
			Умеет выбирать и реализовывать основные методы обеспечения информационной безопасности посредством криптографических протоколов и алгоритмов.	Собеседование (УО-1); дискуссия (УО-4); лабораторная работа (ПР-6); конспект (ПР-7); разноуровневые задачи и задания (ПР-11).	Экзаменационные вопросы 2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32
			Владеет навыками реализации комплексных задач информационной безопасности, возникающих в профессиональной деятельности, опираясь на актуальные требования к стойкости, оперативности и ресурсоемкости, обоснования этих требований в контексте	Собеседование (УО-1); дискуссия (УО-4); лабораторная работа (ПР-6); конспект (ПР-7); разноуровневые задачи и задания (ПР-11).	Экзаменационные вопросы 5, 7, 9, 10, 11, 13, 21, 23

			эффективности современной вычислительной техники.		
		ОПК-3.3 Строит вероятностные модели для конкретных процессов, проводит необходимые расчеты в рамках построенной модели	Знает методы построения и анализа математических вероятностных моделей информационных сетей и систем для реализации задач информационной безопасности.	Собеседование (УО-1); дискуссия (УО-4); лабораторная работа (ПР-6); конспект (ПР-7); разноуровневые задачи и задания (ПР-11).	Экзаменационные вопросы 5, 7, 9, 10, 11, 13, 21, 23
			Умеет применять различные формы представления чувствительной информации в компьютерных устройствах и сетях, а также выполнять реализацию методов информационной безопасности в системах и сетях на основе положений теорий алгоритмов и сложности, релевантные положения дискретной математики, математического анализа и теории вероятности	Собеседование (УО-1); дискуссия (УО-4); лабораторная работа (ПР-6); конспект (ПР-7); разноуровневые задачи и задания (ПР-11).	Экзаменационные вопросы 5, 7, 9, 10, 11, 13, 21, 23
			Владеет базовыми навыками анализа безопасности информационных систем и синтеза формальных вероятностных моделей систем информационной безопасности на основе определенных критериев информационной безопасности.	Собеседование (УО-1); дискуссия (УО-4); лабораторная работа (ПР-6); конспект (ПР-7); разноуровневые задачи и задания (ПР-11).	Экзаменационные вопросы 2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32

Типовые контрольные задания, методические материалы, определяющие процедуры оценивания знаний, умений и навыков и (или) опыта деятельности, а также критерии и показатели, необходимые для оценки знаний, умений, навыков и характеризующие результаты обучения, представлены в Приложении.

V. СПИСОК УЧЕБНОЙ ЛИТЕРАТУРЫ И ИНФОРМАЦИОННО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Основная литература

(электронные и печатные издания)

1. Шаньгин В.Ф. Информационная безопасность и защита информации [Электронный ресурс]/ Шаньгин В.Ф.— Электрон. текстовые данные.— Саратов: Профобразование, 2017.— 702 с.— Режим доступа: http://www.iprbookshop.ru/63594.html .— ЭБС «IPRbooks»

2. Фороузан Бехроуз А. Криптография и безопасность сетей [Электронный ресурс]: учебное пособие/ Фороузан Бехроуз А.— Электрон. текстовые данные.— Москва, Саратов: Интернет-Университет Информационных Технологий (ИНТУИТ), Вузовское образование, 2017.— 782 с.— Режим доступа: http://www.iprbookshop.ru/72337.html .— ЭБС «IPRbooks»

3. Теоретико-числовые методы в криптографии [Электронный ресурс]: учебное пособие/ — Электрон. текстовые данные.— Ставрополь: Северо-Кавказский федеральный университет, 2017.— 107 с.— Режим доступа: http://www.iprbookshop.ru/75601.html .— ЭБС «IPRbooks»

4. Прокушев Я.Е. Программно-аппаратные средства защиты информации [Электронный ресурс]: учебное пособие/ Прокушев Я.Е.— Электрон. текстовые данные.— СПб.: Интермедия, 2017.— 160 с.— Режим доступа: http://www.iprbookshop.ru/66799.html .— ЭБС «IPRbooks»

5. Фаронов А.Е. Основы информационной безопасности при работе на компьютере [Электронный ресурс]: учебное пособие/ Фаронов А.Е.— Электрон. текстовые данные.— Москва, Саратов: Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2020.— 154 с.— Режим доступа: http://www.iprbookshop.ru/89453.html.— ЭБС «IPRbooks»

Дополнительная литература

(печатные и электронные издания)

1. Основы информационной безопасности [Электронный ресурс]: учебник для студентов вузов, обучающихся по направлению подготовки «Правовое обеспечение национальной безопасности»/ В.Ю. Рогозин [и др.].— Электрон. текстовые данные.— М.: ЮНИТИ-ДАНА, 2017.— 287 с.— Режим доступа: http://www.iprbookshop.ru/72444.html.— ЭБС «IPRbooks».

2. Галатенко В.А. Основы информационной безопасности [Электронный ресурс]/ Галатенко В.А.— Электрон. текстовые данные.— М.:

Интернет-Университет Информационных Технологий (ИНТУИТ), 2016.— 266 с.— Режим доступа: http://www.iprbookshop.ru/52209.html.— ЭБС «IPRbooks».

Перечень информационных технологий и программного обеспечения

1. Библиотека OpenPGP (реализация Gpg4win 2.3.3) и программа Kleopatra 2.2.

VI. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

Для достижения поставленных целей преподавания дисциплины реализуются следующие средства, способы и организационные мероприятия:

изучение теоретического материала дисциплины на лекциях с использованием компьютерных технологий;

самостоятельное изучение теоретического материала дисциплины с использованием Internet-ресурсов, методических разработок, специальной учебной и научной литературы;

закрепление теоретического материала при проведении лабораторных работ, выполнение проблемно-ориентированных, творческих заданий.

подготовка материалов для выступления на семинарах по темам курса, участие в дискуссиях.

Дисциплину рекомендуется изучать по плану занятий. Обучающийся должен своевременно выполнять задания, выданные на практических занятиях, и защищать их во время занятий или на консультациях.

При подготовке к лекциям обучающийся изучает план лекционного материала, рекомендованную и дополнительную литературу. Для подготовки к практическим занятиям и выполнения индивидуальных графических заданий требуется изучение лекционного материала.

Каждая лабораторная работа рассчитана на несколько аудиторных часов. Поскольку выполнение лабораторных работ опирается на лекционный материал. Для каждой лабораторной работы приведены контрольные вопросы. Для подготовки к практическим занятиям и лабораторным работам требуется изучение лекционного материала, уверенное знание ответов на контрольные вопросы для закрепления материала.

К зачету обучающийся должен отчитаться по всем практическим и лабораторным занятиям. Темы, рассмотренные на лекционных занятиях, но не

отраженные в лабораторных работах закрепляются обучающимся во время самостоятельной работы.

При подготовке к зачету необходимо повторить учебный материал, используя конспект лекций, основную и дополнительную литературу, при необходимости посещать консультации.

VII. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Лабораторные работы и практические занятия проводятся в компьютерном классе.

Материально-техническое и программное обеспечение дисциплины

Наименование специальных помещений и помещений для самостоятельной работы	Оснащенность специальных помещений и помещений для самостоятельной работы	Перечень лицензионного программного обеспечения. Реквизиты подтверждающего документа
690922, Приморский край, г. Владивосток, остров Русский, полуостров Саперный, поселок Аякс, 10, корпус Е, ауд. Е 727. Учебная аудитория для проведения занятий лекционного типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации	Помещение укомплектовано специализированной учебной мебелью (посадочных мест – 25) Оборудование: Моноблок Lenovo C360G-i34164G500UDK. Кодек видеоконференцсвязи LifeSizeExpress 220-Codeconly- Non-AES в составе:коде. Акустическая система для пото-лочного монтажа с низким профилем, Extron SI 3CT LP. Стол компьютерный СК-1. Мультимедийный проектор, Mitsubishi EW330U, 3000 ANSI Lumen, 1280x800.	1С Предприятие (8.2), 7-Zip, ABBYY Lingvo 12, Alice 3, Anaconda 3, Autodesk, CodeBlocks, CorelDRAW X7, Dia, Directum 4.8, DosBox-0.74, Farmanager, Firebird 2.5, FlameRobin, Foxit Reader, Free Pascal, Geany, Ghostscript, Git, Greenfoot, gsview, Inscape 0.91, Java, Java development Kit, Kaspersky, Lazarus, LibreOffice 4.4,MatLab R2017b, Maxima 5.37.2, Microsoft Expression, Microsoft Office 2013, Microsoft Silverlight Microsoft System Center, Microsoft Visual Studio 2017, MikTeX 2.9, MySQL, NetBeans, Notepad++, Oracle VM VirtualBox, PascalABC.NET, PostgreSQL 9.4, PTC Mathcad, Putty, PyQt GPL v5.4.1 for Python 3.4, Pyton2.7(3.4, 3.6), QGIS Brighton, RStudio, SAM CoDeC Pack, SharePoint,Strawberry Perl,Tecnomatix, TeXnicCenter, TortoiseSVN, Unity 2017.3.1f1,Veusz, Vim 8.1, Visual Paradigm CE, Windows Kits, Windows Phone SDK 8.1, Xilinx Design Tools, Acrobat Reader DC, Adobe Bridge CS3, Adobe Device Central CS3, Adobe Extend Script Toolkit 2,Adobe Photoshop CS3,DVD-студия Windows, Google Chrome, Internet Explorer, ITMOproctor, Mozilla Firefox, Windows Media Center, WinSCP

690922, Приморский край, г. Владивосток, остров Русский, полуостров Саперный, поселок Аякс, 10, корпус Е, мультимедийные аудитории Е 725-728	Экран с электроприводом 236*147 см Trim Screen Line; Проектор DLP, 3000 ANSI Lm, WXGA 1280x800, 2000:1 EW330U Mitsubishi; Подсистема специализированных креплений оборудования CORSA-2007 Tuarex; Подсисте-ма видеокоммутации; Подсистема аудиокоммутации и звукоусиления; акустическая система для потолочного монтажа SI 3CT LP Extron; цифровой аудиопроцессор DMP 44 LC Extron; беспроводные ЛВС для обучающихся обеспечены системой на базе точек доступа 802.11a/b/g/n 2x2 MIMO(2SS).	1С Предприятие (8.2), 7-Zip, ABBYY Lingvo 12, Alice 3, Anaconda 3, Autodesk, CodeBlocks, CorelDRAW X7, Dia, Directum 4.8, DosBox-0.74, Farmanager, Firebird 2.5, FlameRobin, Foxit Reader, Free Pascal, Geany, Ghostscript, Git, Greenfoot, gsview, Inscape 0.91, Java, Java development Kit, Kaspersky, Lazarus, LibreOffice 4.4,MatLab R2017b, Maxima 5.37.2, Microsoft Expression, Microsoft Office 2013, Microsoft Silverlight Microsoft System Center, Microsoft Visual Studio 2017, MikTeX 2.9, MySQL, NetBeans, Notepad++, Oracle VM VirtualBox, PascalABC.NET, PostgreSQL 9.4, PTC Mathcad, Putty, PyQt GPL v5.4.1 for Python 3.4, Pyton2.7(3.4, 3.6), QGIS Brighton, RStudio, SAM CoDeC Pack, SharePoint,Strawberry Perl,Tecnomatix, TeXnicCenter, TortoiseSVN, Unity 2017.3.1f1,Veusz, Vim 8.1, Visual Paradigm CE, Windows Kits, Windows Phone SDK 8.1, Xilinx Design Tools, Acrobat Reader DC, Adobe Bridge CS3, Adobe Device Central CS3, Adobe Extend Script Toolkit 2,Adobe Photoshop CS3,DVD-студия Windows, Google Chrome, Internet Explorer, ITMOproctor, Mozilla Firefox, Windows Media Center, WinSCP
690922, Приморский край, г. Владивосток, остров Русский, полуостров Саперный, поселок Аякс, 10, корпус Е, ауд. Е 726, Е728, Е729. учебные лаборатории электроники и средств связи на 20 человек, общей площадью 50 м^2.	Моноблок Lenovo C360G-i34164G500UDK, Кодек видеоконференцсвязи LifeSizeExpress 220-Codeconly- Non-AES в составе:коде, Акустическая система для потолочного монтажа с низким профилем, Extron SI 3CT LP, стол компьютерный СК-1, Мультимедийный проектор, Mitsubishi EW330U, 3000 ANSI Lumen, 1280x800, Цифровой аудиопроцессор, Extron DMP 44 LC, Матричный коммутатор DVI 4x4.	1С Предприятие (8.2), 7-Zip, ABBYY Lingvo 12, Alice 3, Anaconda 3, Autodesk, CodeBlocks, CorelDRAW X7, Dia, Directum 4.8, DosBox-0.74, Farmanager, Firebird 2.5, FlameRobin, Foxit Reader, Free Pascal, Geany, Ghostscript, Git, Greenfoot, gsview, Inscape 0.91, Java, Java development Kit, Kaspersky, Lazarus, LibreOffice 4.4,MatLab R2017b, Maxima 5.37.2, Microsoft Expression, Microsoft Office 2013, Microsoft Silverlight Microsoft System Center, Microsoft Visual Studio 2017, MikTeX 2.9, MySQL, NetBeans, Notepad++, Oracle VM VirtualBox, PascalABC.NET, PostgreSQL 9.4, PTC Mathcad, Putty, PyQt GPL v5.4.1 for Python 3.4, Pyton2.7(3.4, 3.6), QGIS Brighton, RStudio, SAM CoDeC Pack, SharePoint,Strawberry Perl,Tecnomatix, TeXnicCenter, TortoiseSVN, Unity 2017.3.1f1,Veusz, Vim 8.1, Visual Paradigm CE, Windows Kits, Windows Phone SDK 8.1, Xilinx Design Tools, Acrobat Reader DC, Adobe Bridge CS3, Adobe Device Central CS3, Adobe Extend Script Toolkit 2,Adobe Photoshop CS3,DVD-студия Windows, Google Chrome, Internet Explorer, ITMOproctor, Mozilla Firefox, Windows Media Center, WinSCP

	Extron DXP 44 DVI PRO, Сетевая видеокамера Multipix MP-HD718, Документ-камера Avervision CP355AF, Доска ученическая двусторонняя магнитная, для письма мелом и маркером, Стойка металлическая для ЖК-дисплея У SMS Flatscreen FH T1450	
690922, Приморский край, г. Владивосток, остров Русский, полуостров Саперный, поселок Аякс, 10, корпус А, уровень 10.	Моноблок HP ProOne 400 All-in-One 19,5 (1600x900), Core i3-4150T, 4GB DDR3-1600 (1x4GB), 1TB HDD 7200 SATA, DVD+/-RW,GigEth,Wi-Fi,BT,usb kbd/mse,Win7Pro (64-bit)+Win8.1Pro(64-bit),1-1-1 Wty Скорость доступа в Интернет 500 Мбит/сек. Рабочие места для людей с ограниченными возможностями здоровья оснащены дисплеями и принтерами Брайля; оборудованы: портативными устройствами для чтения плоскопечатных текстов, сканирующими и читающими машинами видеоувеличителем с возможностью регуляции цветовых спектров; увеличивающими электронными лупами и ультразвуковыми маркировщиками	1С Предприятие (8.2), 7-Zip, ABBYY Lingvo 12, Alice 3, Anaconda 3, Autodesk, CodeBlocks, CorelDRAW X7, Dia, Directum 4.8, DosBox-0.74, Farmanager, Firebird 2.5, FlameRobin, Foxit Reader, Free Pascal, Geany, Ghostscript, Git, Greenfoot, gsview, Inscape 0.91, Java, Java development Kit, Kaspersky, Lazarus, LibreOffice 4.4,MatLab R2017b, Maxima 5.37.2, Microsoft Expression, Microsoft Office 2013, Microsoft Silverlight Microsoft System Center, Microsoft Visual Studio 2017, MikTeX 2.9, MySQL, NetBeans, Notepad++, Oracle VM VirtualBox, PascalABC.NET, PostgreSQL 9.4, PTC Mathcad, Putty, PyQt GPL v5.4.1 for Python 3.4, Pyton2.7(3.4, 3.6), QGIS Brighton, RStudio, SAM CoDeC Pack, SharePoint,Strawberry Perl,Tecnomatix, TeXnicCenter, TortoiseSVN, Unity 2017.3.1f1,Veusz, Vim 8.1, Visual Paradigm CE, Windows Kits, Windows Phone SDK 8.1, Xilinx Design Tools, Acrobat Reader DC, Adobe Bridge CS3, Adobe Device Central CS3, Adobe Extend Script Toolkit 2,Adobe Photoshop CS3,DVD-студия Windows, Google Chrome, Internet Explorer, ITMOproctor, Mozilla Firefox, Windows Media Center, WinSCP

Лекции проводятся с использованием проектора и внутренней системы портала ДВФУ. Лабораторные занятия проходят в аудиториях, оборудованных компьютерами типа Lenovo C360G-i34164G500UDK с лицензионными программами Microsoft Visual Studio 2017 и аудиовизуальными средствами проектор Panasonic DLPProjectorPT-D2110XE, плазма LG FLATRON M4716CCBAM4716CJ. Для выполнения самостоятельной работы студенты в жилых корпусах ДВФУ обеспечены Wi-Fi.

Для проведения учебных занятий по дисциплине, а также для организации самостоятельной работы студентам доступно специализированные кабинеты, соответствующие действующим санитарным и противопожарным нормам, а также требованиям техники безопасности при проведении учебных и научно-производственных работ.

В целях обеспечения специальных условий обучения инвалидов и лиц с ограниченными возможностями здоровья в ДВФУ все здания оборудованы пандусами, лифтами, подъемниками, специализированными местами, оснащенными туалетными комнатами, табличками информационно-навигационной поддержки.

VIII. ФОНДЫ ОЦЕНОЧНЫХ СРЕДСТВ

Фонды оценочных средств представлены в приложении.

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение высшего образования
«Дальневосточный федеральный университет»
(ДВФУ)

ПОЛИТЕХНИЧЕСКИЙ ИНСТИТУТ (ШКОЛА)

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

по дисциплине «Методы и средства защиты информации»
Направление подготовки 11.03.02 Инфокоммуникационные технологии и системы связи
Профиль «Видеоинформационные технологии и цифровое вещание»
Форма подготовки очная

Владивосток
2021

ПЕРЕЧЕНЬ ФОРМ ОЦЕНИВАНИЯ, ПРИМЕНЯЕМЫХ НА РАЗЛИЧНЫХ ЭТАПАХ ФОРМИРОВАНИЯ КОМПЕТЕНЦИЙ В ХОДЕ ОСВОЕНИЯ ДИСЦИПЛИНЫ

№ п/п	Контролируемые модули/ разделы / темы дисциплины	Код индикатора достижения компетенции	Результаты обучения	Оценочные средства – наименование	
				текущий контроль	промежуточная аттестация
1	Политики и модели безопасности вычислительных сетей и систем	ОПК-1.1 Выделяет известные физические и математические законы в явлениях окружающего мира	Знает фундаментальное математическое и физическое обоснование защиты информации и данных, взаимодействия через инфокоммуникационный канал связи, заданный логическим или физическим представлением, математической моделью.	Собеседование (УО-1); дискуссия (УО-4); лабораторная работа (ПР-6); конспект (ПР-7); разноуровневые задачи и задания (ПР-11).	Экзаменационные вопросы 5, 7, 9, 10, 11, 13, 21, 23
			Умеет выполнять обоснование задач информационной безопасности, основываясь на сформированном представлении о физике информации и каналов инфокоммуникации, на ее отображении на математическую модель.	Собеседование (УО-1); дискуссия (УО-4); лабораторная работа (ПР-6); конспект (ПР-7); разноуровневые задачи и задания (ПР-11).	Экзаменационные вопросы 5, 7, 9, 10, 11, 13, 21, 23
			Владеет навыками реализации задач информационной безопасности и о методах ее реализации, опираясь на научное и формальное представление об информации, о физическое реализуемости сетей связи, методах их формального математического обоснования.	Собеседование (УО-1); дискуссия (УО-4); лабораторная работа (ПР-6); конспект (ПР-7); разноуровневые задачи и задания (ПР-11).	Экзаменационные вопросы 5, 7, 9, 10, 11, 13, 21, 23
		ОПК-1.2 Применяет физические законы и математические методы для решения задач теоретического и	Знает методы математического моделирования и обоснования эффективности	Собеседование (УО-1); дискуссия (УО-4); лабораторная работа (ПР-6); конспект (ПР-7); разноуровневые задачи и	Экзаменационные вопросы 2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32

		прикладного характера		задания (ПР-11).	
			Умеет выполнять формальное обоснование задачи информационной безопасности в терминах математических и физических закономерностей, информатики и информационной безопасности.	Собеседование (УО-1); дискуссия (УО-4); лабораторная работа (ПР-6); конспект (ПР-7); разноуровневые задачи и задания (ПР-11).	Экзаменационные вопросы 2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32
			Владеет представлением об информационной безопасности и о методах ее реализации, основываясь на фундаментальных законах математики, информатики и физики, методами обоснования задач предметной области на их основе.	Собеседование (УО-1); дискуссия (УО-4); лабораторная работа (ПР-6); конспект (ПР-7); разноуровневые задачи и задания (ПР-11).	Экзаменационные вопросы 2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32
2	Требования к информационной безопасности телекоммуникационных сетей и систем	ОПК-1.1 Выделяет известные физические и математические законы в явлениях окружающего мира	Знает фундаментальное математическое и физическое обоснование защиты информации и данных, взаимодействия через инфокоммуникационный канал связи, заданный логическим или физическим представлением, математической моделью.	Собеседование (УО-1); дискуссия (УО-4); лабораторная работа (ПР-6); конспект (ПР-7); разноуровневые задачи и задания (ПР-11).	Экзаменационные вопросы 2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32
			Умеет выполнять обоснование задач информационной безопасности, основываясь на сформированном представлении о физике информации и каналов инфокоммуникации, на ее отображении на математическую модель.	Собеседование (УО-1); дискуссия (УО-4); лабораторная работа (ПР-6); конспект (ПР-7); разноуровневые задачи и задания (ПР-11).	Экзаменационные вопросы 2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32
			Владеет навыками реализации задач информационной безопасности и о методах ее реализации, опираясь на научное и формальное представление об информации, о физическое	Собеседование (УО-1); дискуссия (УО-4); лабораторная работа (ПР-6); конспект (ПР-7);	Экзаменационные вопросы 2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32

			реализуемости сетей связи, методах их формального математического обоснования.	разноуровневые задачи и задания (ПР-11).	
3	Методы и средства защиты информации в телекоммуникационных сетях	ОПК-3.3 Строит вероятностные модели для конкретных процессов, проводит необходимые расчеты в рамках построенной модели	Знает методы построения и анализа математических вероятностных моделей информационных сетей и систем для реализации задач информационной безопасности.	Собеседование (УО-1); дискуссия (УО-4); лабораторная работа (ПР-6); конспект (ПР-7); разноуровневые задачи и задания (ПР-11).	Экзаменационные вопросы 1, 5, 11, 15, 21.
			Умеет применять различные формы представления чувствительной информации в компьютерных устройствах и сетях, а также выполнять реализацию методов информационной безопасности в системах и сетях на основе положений теорий алгоритмов и сложности, релевантные положения дискретной математики, математического анализа и теории вероятности	Собеседование (УО-1); дискуссия (УО-4); лабораторная работа (ПР-6); конспект (ПР-7); разноуровневые задачи и задания (ПР-11).	Экзаменационные вопросы 1, 5, 11, 15, 21.
			Владеет базовыми навыками анализа безопасности информационных систем и синтеза формальных вероятностных моделей систем информационной безопасности на основе определенных критериев информационной безопасности.	Собеседование (УО-1); дискуссия (УО-4); лабораторная работа (ПР-6); конспект (ПР-7); разноуровневые задачи и задания (ПР-11).	Экзаменационные вопросы 1, 5, 11, 15, 21.
4	Математическое обоснование методов и криптографических средств защиты информационной безопасности	ОПК-1.2 Применяет физические законы и математические методы для решения задач теоретического и прикладного характера	Знает методы математического моделирования и обоснования эффективности	Собеседование (УО-1); дискуссия (УО-4); лабораторная работа (ПР-6); конспект (ПР-7); разноуровневые задачи и задания (ПР-11).	Экзаменационные вопросы 3, 12, 16, 17, 19, 25, 27, 29.

			Умеет выполнять формальное обоснование задачи информационной безопасности в терминах математических и физических закономерностей, информатики и информационной безопасности.	Собеседование (УО-1); дискуссия (УО-4); лабораторная работа (ПР-6); конспект (ПР-7); разноуровневые задачи и задания (ПР-11).	Экзаменационные вопросы 3, 12, 16, 17, 19, 25, 27, 29.
			Владеет представлением об информационной безопасности и о методах ее реализации, основываясь на фундаментальных законах математики, информатики и физики, методами обоснования задач предметной области на их основе.	Собеседование (УО-1); дискуссия (УО-4); лабораторная работа (ПР-6); конспект (ПР-7); разноуровневые задачи и задания (ПР-11).	Экзаменационные вопросы 3, 12, 16, 17, 19, 25, 27, 29.
		ОПК-3.1 Применяет принципы, основные алгоритмы и устройства цифровой обработки сигналов	Знает основные формы представления информации и данных, а также защиты участников информационного обмена на основе положений теорий алгоритмов и сложности, релевантные положения дискретной математики, математического анализа и теории вероятности	Собеседование (УО-1); дискуссия (УО-4); лабораторная работа (ПР-6); конспект (ПР-7); разноуровневые задачи и задания (ПР-11).	Экзаменационные вопросы 5, 7, 9, 10, 11, 13, 21, 23
			Умеет обосновать задачу информационной безопасности в инфокоммуникационных сетях, построить ее математическую модель, использующую методы цифровой обработки сигналов, а также методов ее реализации в контексте требований к функциональной эффективности с использованием математического формализма и формальноязыковых средств.	Собеседование (УО-1); дискуссия (УО-4); лабораторная работа (ПР-6); конспект (ПР-7); разноуровневые задачи и задания (ПР-11).	Экзаменационные вопросы 5, 7, 9, 10, 11, 13, 21, 23
			Владеет навыками адекватного описания задач и методов цифровой обработки сигналов для реализации задач информационной	Собеседование (УО-1); дискуссия (УО-4);	Экзаменационные вопросы 5, 7, 9, 10, 11, 13, 21, 23

			безопасности в привязке к выбранной системе показателей и критериев эффективности.	лабораторная работа (ПР-6); конспект (ПР-7); разноуровневые задачи и задания (ПР-11).	
		ОПК-3.3 Строит вероятностные модели для конкретных процессов, проводит необходимые расчеты в рамках построенной модели	Знает методы построения и анализа математических вероятностных моделей информационных сетей и систем для реализации задач информационной безопасности.	Собеседование (УО-1); дискуссия (УО-4); лабораторная работа (ПР-6); конспект (ПР-7); разноуровневые задачи и задания (ПР-11).	Экзаменационные вопросы 2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32
			Умеет применять различные формы представления чувствительной информации в компьютерных устройствах и сетях, а также выполнять реализацию методов информационной безопасности в системах и сетях на основе положений теорий алгоритмов и сложности, релевантные положения дискретной математики, математического анализа и теории вероятности	Собеседование (УО-1); дискуссия (УО-4); лабораторная работа (ПР-6); конспект (ПР-7); разноуровневые задачи и задания (ПР-11).	Экзаменационные вопросы 2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32
			Владеет базовыми навыками анализа безопасности информационных систем и синтеза формальных вероятностных моделей систем информационной безопасности на основе определенных критериев информационной безопасности.	Собеседование (УО-1); дискуссия (УО-4); лабораторная работа (ПР-6); конспект (ПР-7); разноуровневые задачи и задания (ПР-11).	Экзаменационные вопросы 2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32
5	Средства криптографической защиты информации в телекоммуникационных сетях	ОПК-3.1 Применяет принципы, основные алгоритмы и устройства цифровой обработки сигналов	Знает основные формы представления информации и данных, а также защиты участников информационного обмена на основе положений теорий алгоритмов и сложности, релевантные положения	Собеседование (УО-1); дискуссия (УО-4); лабораторная работа (ПР-6); конспект (ПР-7);	Экзаменационные вопросы 2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32

			дискретной математики, математического анализа и теории вероятности	разноуровневые задачи и задания (ПР-11).	
			Умеет обосновать задачу информационной безопасности в инфокоммуникационных сетях, построить ее математическую модель, использующую методы цифровой обработки сигналов, а также методов ее реализации в контексте требований к функциональной эффективности с использованием математического формализма и формальноязыковых средств.	Собеседование (УО-1); дискуссия (УО-4); лабораторная работа (ПР-6); конспект (ПР-7); разноуровневые задачи и задания (ПР-11).	Экзаменационные вопросы 2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32
			Владеет навыками адекватного описания задач и методов цифровой обработки сигналов для реализации задач информационной безопасности в привязке к выбранной системе показателей и критериев эффективности.	Собеседование (УО-1); дискуссия (УО-4); лабораторная работа (ПР-6); конспект (ПР-7); разноуровневые задачи и задания (ПР-11).	Экзаменационные вопросы 2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32
		ОПК-3.2 Решает задачи обработки данных с помощью современных средств цифровой вычислительной техники	Знает методы априорной и апостериорной оценки информационной безопасности инфотелекоммуникационных систем, аспекты безопасности информационных систем, обусловленные их развертыванием, введением в эксплуатацию и передачей третьей стороне.	Собеседование (УО-1); дискуссия (УО-4); лабораторная работа (ПР-6); конспект (ПР-7); разноуровневые задачи и задания (ПР-11).	Экзаменационные вопросы 1, 5, 11, 15, 21.
			Умеет выбирать и реализовывать основные методы обеспечения информационной безопасности посредством криптографических протоколов и алгоритмов.	Собеседование (УО-1); дискуссия (УО-4); лабораторная работа (ПР-6); конспект (ПР-7); разноуровневые задачи и задания (ПР-11).	Экзаменационные вопросы 1, 5, 11, 15, 21.

			Владеет навыками реализации комплексных задач информационной безопасности, возникающих в профессиональной деятельности, опираясь на актуальные требования к стойкости, оперативности и ресурсоемкости, обоснования этих требований в контексте эффективности современной вычислительной техники.	Собеседование (УО-1); дискуссия (УО-4); лабораторная работа (ПР-6); конспект (ПР-7); разноуровневые задачи и задания (ПР-11).	Экзаменационные вопросы 1, 5, 11, 15, 21.
		ОПК-3.3 Строит вероятностные модели для конкретных процессов, проводит необходимые расчеты в рамках построенной модели	Знает методы построения и анализа математических вероятностных моделей информационных сетей и систем для реализации задач информационной безопасности.	Собеседование (УО-1); дискуссия (УО-4); лабораторная работа (ПР-6); конспект (ПР-7); разноуровневые задачи и задания (ПР-11).	Экзаменационные вопросы 3, 12, 16, 17, 19, 25, 27, 29.
			Умеет применять различные формы представления чувствительной информации в компьютерных устройствах и сетях, а также выполнять реализацию методов информационной безопасности в системах и сетях на основе положений теорий алгоритмов и сложности, релевантные положения дискретной математики, математического анализа и теории вероятности	Собеседование (УО-1); дискуссия (УО-4); лабораторная работа (ПР-6); конспект (ПР-7); разноуровневые задачи и задания (ПР-11).	Экзаменационные вопросы 3, 12, 16, 17, 19, 25, 27, 29.
			Владеет базовыми навыками анализа безопасности информационных систем и синтеза формальных вероятностных моделей систем информационной безопасности на основе определенных критериев информационной безопасности.	Собеседование (УО-1); дискуссия (УО-4); лабораторная работа (ПР-6); конспект (ПР-7); разноуровневые задачи и задания (ПР-11).	Экзаменационные вопросы 5, 7, 9, 10, 11, 13, 21, 23
6	Криптографические протоколы	ОПК-3.1 Применяет	Знает основные формы представления	Собеседование (УО-1);	Экзаменационные вопросы 5,

		принципы, основные алгоритмы и устройства цифровой обработки сигналов	информации и данных, а также защиты участников информационного обмена на основе положений теорий алгоритмов и сложности, релевантные положения дискретной математики, математического анализа и теории вероятности	дискуссия (УО-4); лабораторная работа (ПР-6); конспект (ПР-7); разноуровневые задачи и задания (ПР-11).	7, 9, 10, 11, 13, 21, 23
			Умеет обосновать задачу информационной безопасности в инфокоммуникационных сетях, построить ее математическую модель, использующую методы цифровой обработки сигналов, а также методов ее реализации в контексте требований к функциональной эффективности с использованием математического формализма и формальноязыковых средств.	Собеседование (УО-1); дискуссия (УО-4); лабораторная работа (ПР-6); конспект (ПР-7); разноуровневые задачи и задания (ПР-11).	Экзаменационные вопросы 5, 7, 9, 10, 11, 13, 21, 23
			Владеет навыками адекватного описания задач и методов цифровой обработки сигналов для реализации задач информационной безопасности в привязке к выбранной системе показателей и критериев эффективности.	Собеседование (УО-1); дискуссия (УО-4); лабораторная работа (ПР-6); конспект (ПР-7); разноуровневые задачи и задания (ПР-11).	Экзаменационные вопросы 2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32
		ОПК-3.2 Решает задачи обработки данных с помощью современных средств цифровой вычислительной техники	Знает методы априорной и апостериорной оценки информационной безопасности инфотелекоммуникационных систем, аспекты безопасности информационных систем, обусловленные их развертыванием, введением в эксплуатацию и передачей третьей стороне.	Собеседование (УО-1); дискуссия (УО-4); лабораторная работа (ПР-6); конспект (ПР-7); разноуровневые задачи и задания (ПР-11).	Экзаменационные вопросы 2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32
			Умеет выбирать и реализовывать основные методы обеспечения информационной безопасности посредством криптографических	Собеседование (УО-1); дискуссия (УО-4); лабораторная работа (ПР-6);	Экзаменационные вопросы 2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32

			протоколов и алгоритмов.	конспект (ПР-7); разноуровневые задачи и задания (ПР-11).	
			Владеет навыками реализации комплексных задач информационной безопасности, возникающих в профессиональной деятельности, опираясь на актуальные требования к стойкости, оперативности и ресурсоемкости, обоснования этих требований в контексте эффективности современной вычислительной техники.	Собеседование (УО-1); дискуссия (УО-4); лабораторная работа (ПР-6); конспект (ПР-7); разноуровневые задачи и задания (ПР-11).	Экзаменационные вопросы 5, 7, 9, 10, 11, 13, 21, 23
		ОПК-3.3 Строит вероятностные модели для конкретных процессов, проводит необходимые расчеты в рамках построенной модели	Знает методы построения и анализа математических вероятностных моделей информационных сетей и систем для реализации задач информационной безопасности.	Собеседование (УО-1); дискуссия (УО-4); лабораторная работа (ПР-6); конспект (ПР-7); разноуровневые задачи и задания (ПР-11).	Экзаменационные вопросы 5, 7, 9, 10, 11, 13, 21, 23
			Умеет применять различные формы представления чувствительной информации в компьютерных устройствах и сетях, а также выполнять реализацию методов информационной безопасности в системах и сетях на основе положений теорий алгоритмов и сложности, релевантные положения дискретной математики, математического анализа и теории вероятности	Собеседование (УО-1); дискуссия (УО-4); лабораторная работа (ПР-6); конспект (ПР-7); разноуровневые задачи и задания (ПР-11).	Экзаменационные вопросы 5, 7, 9, 10, 11, 13, 21, 23
			Владеет базовыми навыками анализа безопасности информационных систем и синтеза формальных вероятностных моделей систем информационной безопасности на основе определенных критериев	Собеседование (УО-1); дискуссия (УО-4); лабораторная работа (ПР-6); конспект (ПР-7);	Экзаменационные вопросы 2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32

			информационной безопасности.	разноуровневые задачи и задания (ПР-11).	

Для дисциплины «Методы и средства защиты информации» используются следующие оценочные средства.

Устный опрос:

1) устный опрос (УО-1);

2) дискуссия (УО-4);

Письменные работы:

1) тесты (ПР-1);

2) лабораторная работа (ПР-6);

3) конспект (ПР-7);

4) разноуровневые задачи и задания (ПР-11);

5) кейс-задачи (ПР-14).

Методические рекомендации, определяющие процедуры оценивания результатов освоения дисциплины

Для дисциплины «Основы информационной безопасности сетей связи» используются следующие оценочные средства.

Устный опрос:

1) собеседование (УО-1);

2) дискуссия (УО-4);

Письменные работы:

1) лабораторная работа (ПР-6);

2) конспект (ПР-7);

3) разноуровневые задачи и задания (ПР-11).

Устный опрос

Устный опрос позволяет оценить знания студента, умение устно обосновать и сформулировать ответ, используя термины и понятия предметной области.

Обучающая функция состоит в выявлении деталей, которые по каким-то причинам оказались недостаточно осмысленными в ходе учебных занятий по дисциплине.

Собеседование (УО-1) – средство контроля, организованное как специальная беседа преподавателя с обучающимся на темы, связанные с изучаемой дисциплиной, и рассчитанное на выяснение объема знаний обучающегося по определенному разделу, теме, проблеме и т.п.

Дискуссия (УО-4) – оценочное средство, позволяющее включить

обучающихся в процесс обсуждения спорного вопроса, проблемы и оценить их умение аргументировать собственную точку зрения.

Письменные работы

Письменный ответ прививает навыки формального, точного и лаконичного выражения мысленных идей и сформированных студентом в ходе изучения материала дисциплины когнитивных структур.

Лабораторная работа (ПР-6) – средство для закрепления и практического освоения материала по определенному разделу.

Конспект (ПР-7) – продукт самостоятельной работы обучающегося, отражающий основные идеи заслушанной лекции, сообщения и т.д.

Проект (ПР-9) – конечный продукт, получаемый в результате планирования и выполнения комплекса учебных и исследовательских заданий, который позволяет оценить умения обучающихся самостоятельно конструировать свои знания в процессе решения практических задач и проблем, ориентироваться в информационном пространстве и уровень сформированности аналитических, исследовательских навыков, навыков практического и творческого мышления; может выполняться в индивидуальном порядке или группой обучающихся.

Разноуровневые задачи и задания (ПР-11) реконструктивного уровня, позволяющие оценивать и диагностировать умения синтезировать, анализировать, обобщать фактический и теоретический материал с формулированием конкретных выводов, установлением причинно-следственных связей.

Для допуска к экзамену студент должен выполнить все представленные в разделе II лабораторные работы, привести обоснование решений представленных в разделе II практических заданий.

Методические рекомендации, определяющие процедуры оценивания результатов освоения дисциплины

Итоговая оценка промежуточной аттестации выставляется согласно рейтинг-плану, который включает в себя оценочные мероприятия, в том числе и экзамен/зачет, и весовые коэффициенты. Преподаватель знакомит студентом с рейтинг-планом в начале семестра.

Оценочные средства для текущей аттестации

Текущая аттестация студентов по дисциплине проводится в соответствии с локальными нормативными актами ДВФУ и является обязательной.

Текущая аттестация проводится в форме контрольных мероприятий (собеседования, дискуссии, лабораторные работы, конспекты лекций,

проекты, разноуровневые задачи реконструктивного уровня) по оцениванию фактических результатов обучения студентов и осуществляется ведущим преподавателем.

Объектами оценивания выступают:

− учебная дисциплина (активность на занятиях, своевременность выполнения различных видов заданий, посещаемость всех видов занятий по аттестуемой дисциплине);

− степень усвоения теоретических знаний;

− уровень овладения практическими умениями и навыками по всем видам учебной работы;

− результаты самостоятельной работы

Проводится проверка отчетов по лабораторным работам и собеседования, в рамках которых студенты устно объясняют результаты измерений. Аналогично проводится проверка правильности выполнения заданий по самостоятельной работе. Задание зачтено, если нет ошибок. По текущим ошибкам даются пояснения.

Вопросы для собеседования

1. Задачи информационной безопасности сетей связи и методы их решения.
2. Инструменты криптографической защиты информации и узлов сетей связи.
3. Стоимость информации, информационной системы и стойкость методов защиты.
4. Международные и государственные стандарты безопасности информации.
5. Криптографические инфокоммуникационные протоколы.
6. Модели распределения прав доступа в информационных системах.
7. Криптографические алгоритмы на основе сетей Фейстеля и на основе подстановочно-перестановочных сетей.
8. Оценка стойкости крипторафических псевдослучайных генераторов.
9. Энтропия Реньи и ее применение в задачах защиты информации.
10. Китайская теорема об остатках.

Перечень тем для дискуссии

1. Аффинные шифры и аффинные преобразования, определенные над конечными кольцами.
2. Использование конечных полей в задачах криптографической обработки бинарных данных.

3. Поиск мультипликативной инверсии элемента в конечном поле путем выполнения расширенного алгоритма Эвклида над этим элементом и неприводимым полиномом, определенным для поля.

4. Реализация аффинного шифра над скалярами, принадлежащими конечному полю, ключей, открытого текста и шифротекста. Пример выполнения операций шифрования и дешифрования. Пример атаки с известным открытым текстом.

5. Реализация блочного шифра, основанного на матричном аффинном преобразовании вектора открытого текста. Пример мультипликативной инверсии матрицы на основе LU-разложения. Реализация дешифрования. Пример шифрования и дешифрования трехбайтового блока данных и с использованием матрицы 3x3 в качестве мультипликативной части ключа.

6. Циклическая генерация элементов конечного поля.

7. Дискретное логарифмирование в конечном поле.

8. Функция Эйлера и ее применение в задачах вычисления полиномиальной функции над конечным числовым полем.

9. Теорема Лагранжа и ее применение для увеличения оперативности вычисления целочисленной степени в группе.

10. Малая теорема Ферма и теорема Эйлера.

11. Доказательство обратимости операций шифрования/дешифрования RSA.

12. Вычисление степени в конечном поле и применимость RSA над конечным полем.

13. Электронная цифровая подпись RSA, RSA с хеш, DSA.

14. Распределение ключей Диффи-Хеллмана, определенных в конечном поле.

15. Аналитическое обоснование критерия Эйлера.

16. Применение малой теоремы Ферма для вычисления квадратичного вычета в числовой мультипликативной группе с простым числом элементов.

17. Применение теорем Эйлера и Лагранжа для вычисления квадратичных вычетов в конечных группах общего вида.

18. Метод построения и определения эллиптической кривой и ей уравнение.

19. Метод выбора произвольных (случайных) точек на заданной эллиптической кривой.

20. Групповая операция на множестве точек эллиптической кривой.

21. Аксиомы групповой операции.

22. Применение групп точек на эллиптической кривой для реализации задач информационной безопасности и стойкость дискретного логарифмирования в группе.

23. Требования к полю, на котором определена эллиптическая кривая с точки зрения реализуемости.

24. Требования к параметрам эллиптической кривой и определяющему ее конечному полу с точки зрения стойкости.

Критерии оценивания

Оценка	Требования
«зачтено»	Студент умеет аргументированно обосновать свою точку зрения на рассматриваемый вопрос, используя термины и определения предметной области дисциплины, опираясь на законы и формальное математическое обоснование, приведенное в лекциях и полученное в ходе выполнения практических работ.
«не зачтено»	Студент демонстрирует незнание вопроса, неумение аргументированно обосновать свою точку зрения.

Тематика лабораторных работ

1. Комплекс решений для шифрования PGP и работа с ним с помощью OpenPGP.
2. Алгоритмическая и программная реализация алгоритма распределения Диффи-Хеллмана над точками выбранной эллиптической кривой.
3. Реализация протокола «Ментальный покер».
4. Реализация протокола доказательства с нулевым разглашением с помощью потокового шифра на основе линейного конгруэнтного генератора гаммы.

Критерии оценивания

Оценка	Требования
«зачтено»	Студент выполняет лабораторную работу в полном объёме с приведением необходимого обоснования метода реализации в соответствии с заданием на лабораторную и соблюдением последовательности действий, правильно и самостоятельно определяет цель работы, определяет области применимости своего решения, правильно формулирует выводы, точно и аккуратно выполняет все записи, приводит таблицы, рисунки, графики, умеет обобщать фактический материал. Допускается два/три недочёта или одна негрубая ошибка и один недочёт.
«не зачтено»	Студент выполнил работу не полностью, не определяет самостоятельно цель работы; в ходе работы допускает одну и более ошибок, которые студент не в состоянии самостоятельно обнаружить и исправить в течение десяти минут, не может обосновать приведенное

	решение и наблюдаемые результаты; не умеет обобщать фактический материал. Лабораторная работа не выполнена.

Перечень тем лекционных занятий, отражение которых в конспекте обязательно

1. Политики и модели безопасности вычислительных сетей и систем.
2. Требования к информационной безопасности телекоммуникационных сетей и систем.
3. Методы и средства защиты информации в телекоммуникационных сетях.
4. Математическое обоснование методов и криптографических средств защиты информационной безопасности.
5. Средства криптографической защиты информации в телекоммуникационных сетях.
6. Криптографические протоколы.

Критерии оценивания

Оценка	Требования
«зачтено»	Конспект выполнен аккуратно, в нем приведены все основные постулаты лекции, кратко описано их обоснование. Где, в соответствии с лекцией, необходимо, приведено оформление материала лекций в виде рисунков, таблиц и графиков.
«не зачтено»	Конспект не выполнен, не отражает материал лекции или отражает его не более чем на 70%, приведены не все выводы и постулаты лекции, материал, где необходимо, не сопровождается рисунками, графиками и таблицами, или они не в полной мере, неадекватно отражают обсуждаемый вопрос, выполнены не аккуратно.

Разноуровневые задачи и задания реконструктивного уровня

1. Математические основы криптографии. Обоснование методов криптографии и математических методов информационной безопасности с помощью алгебры конечных групп, колец и полей.
2. Применение и использование традиционных шифров с симметричным ключом.
3. Оценка стойкости хеш-функций методом простого перебора и поиском коллизий.
4. Выполнение преобразований асимметричной криптографии. Экспоненциальные функции и дискретное логарифмирование в алгебраических группах и конечных полях.
5. Протоколы распределения симметричных ключей шифрования. Применение протоколов с посредником и арбитром. Применение

асимметричных методов для распределения ключей. Генерация сеансовых ключей симметричного шифрования на основе проблемы дискретного логарифмирование.

6. Режимы работы блочных шифров на примере аффинного преобразованиями вектора данных размером 3 байт, определенного над конечным полем.

7. Методы получения имитовставки HMAC и CBC-MAC.

Критерии оценивания

Оценка	Требования
«зачтено»	Задача выполнена полностью в соответствии с заданием. Метод ее реализации обоснован, принятые решения по выбору метода приводятся студентом на основе требований к реализуемости, и оперативности вычислений, требуемых для реализации задачи.
«не зачтено»	Задача не выполнена, не соответствует заданию или соответствует ему не полностью.

Оценочные средства для промежуточной аттестации

Промежуточная аттестация студентов по дисциплине «Основы информационной безопасности сетей связи» проводится в соответствии с локальными нормативными актами ДВФУ и является обязательной. Форма отчётности по дисциплине – экзамен (5-й, осенний семестр). Экзамен по дисциплине включает ответы на 3 вопроса, как минимум один из которых направлен на оценку общих теоретических знаний по предмету, и как минимум один – на решение конкретной задачи по реализации цифровой обработки данных в сетях связи или по анализу предоставленной реализации.

Критерии выставления оценки студенту на экзамене

Баллы (рейтинговой оценки)	**Оценка экзамена** (стандартная)	**Требования к сформированным компетенциям**
86-100	«отлично»	Оценка «отлично» выставляется студенту, если он глубоко и прочно усвоил программный материал, исчерпывающе, последовательно, четко и логически стройно его излагает, умеет тесно увязывать теорию с практикой, свободно справляется с задачами, вопросами и другими видами применения знаний, причем не затрудняется с ответом при видоизменении заданий, правильно обосновывает принятое решение, владеет разносторонними навыками и приемами выполнения практических задач.

76-85	«хорошо»	Оценка «хорошо» выставляется студенту, если он твердо знает материал, грамотно и по существу излагает его, не допуская существенных неточностей в ответе на вопрос, правильно применяет теоретические положения при решении практических вопросов и задач, владеет необходимыми навыками и приемами их выполнения.
61-75	«удовлетворительно»	Оценка «удовлетворительно» выставляется студенту, если он имеет знания только основного материала, но не усвоил его деталей, допускает неточности, недостаточно правильные формулировки, нарушения логической последовательности в изложении программного материала, испытывает затруднения при выполнении практических работ.
0-60	«неудовлетворительно»	Оценка «неудовлетворительно» выставляется студенту, который не знает значительной части программного материала, допускает существенные ошибки, неуверенно, с большими затруднениями выполняет практические работы. Как правило, оценка «неудовлетворительно» ставится студентам, которые не могут продолжить обучение без дополнительных занятий по соответствующей дисциплине.

Методические указания по сдаче экзамена

Экзамен принимается ведущим преподавателем. При большом количестве групп у одного преподавателя или при большой численности потока по распоряжению директора департамента (заместителя директора по учебной и воспитательной работе) допускается привлечение в помощь ведущему преподавателю других преподавателей. В первую очередь привлекаются преподаватели, которые проводили лабораторные занятия по дисциплине в группах.

В исключительных случаях, по согласованию с заместителем директора института по учебной и воспитательной работе, директор департамента имеет право принять экзамен в отсутствие ведущего преподавателя.

Форма проведения экзамена (устная, письменная и др.) утверждается на заседании департамента по согласованию с руководителем в соответствии с рабочей программой дисциплины.

Во время проведения экзамена студенты могут пользоваться рабочей программой дисциплины, а также с разрешения преподавателя, проводящего экзамен, справочной литературой и другими пособиями (учебниками, учебными пособиями, рекомендованной литературой и т.п.).

Время, предоставляемое студенту на подготовку к ответу на экзамене, должно составлять не более 90 минут. По истечении данного времени студент должен быть готов к ответу.

Присутствие на экзамене посторонних лиц (кроме лиц, осуществляющих проверку) без разрешения соответствующих лиц (ректора либо проректора по учебной и воспитательной работе, директора института, руководителя ОПОП или директора департамента) не допускается. Инвалиды и лица с ограниченными возможностями здоровья, не имеющие возможности самостоятельного передвижения, допускаются на экзамен с сопровождающими.

При промежуточной аттестации обучающимся устанавливается оценка «неудовлетворительно», «удовлетворительно» «хорошо» или «отлично».

Запись «неудовлетворительно» вносится только в экзаменационную ведомость. При неявке студента на экзамен в ведомости делается запись «не явился».

Вопросы к экзамену

1. Криптография и стеганография. Задачи криптографии и криптоанализа. Принцип Керкгоффса.
2. Разделить секрет, коим является номер зачетной книжки, на секреты не меньшей длины: а) на две части б) на три части. Прилагается таблица ANSI ASCII шестнадцатеричной кодировки кириллических символов.
3. Симметричные шифры.
4. Пусть задан блочный шифр $E(x,k) = x \oplus k$ с длиной блока B = 32 бит, а также схема PKCS7 дополнения данных до размера последнего блока шифра. Для приложенной таблицы кодировки Windows-1251 символов зашифруйте свое имя в режиме ECB, используя в качестве ключа K = {6B 3D 10 58}. Значение задано в шестнадцатеричной системе счисления.
5. Распределение ключей в криптографии.
6. Пусть задан блочный шифр $E(x,k) = x \oplus k$ с длиной блока B = 24 бит, а также схема ISO/IEC 7816-4 дополнения данных до размера последнего блока шифра. Для приложенной таблицы двухбайтовой кодировки символов (UTF-8, Little-Endian) расшифруйте текст {48 38 4e 5e 06 0b 1a 38 44 5e 7e 0b 62 38 3a 5e bc 0f} в режиме ECB, используя в качестве ключа K = {5A 3C 0F}. Значения заданы в шестнадцатеричной системе счисления.
7. Асимметричные шифры. Применение.

8.Пусть задан блочный шифр $E(x,k) = x \oplus k$ с длиной блока B = 24 бит, а также схема ISO 10126 дополнения данных до размера последнего блока шифра. Для приложенной таблицы двухбайтовой кодировки символов (UTF-8, Little-Endian) расшифруйте текст {81 26 40 df 29 4b bb 11 45} в режиме CBC, используя в качестве ключа K = {5A 3C 0F}, а в качестве вектора инициализации значение {CB 1E 74}. Значения заданы в шестнадцатеричной системе счисления.

9. Назначение и применение хеш функций. Вскрытие хеш функций.

10. Пусть задан блочный шифр $E(x,k) = x \oplus k$ с длиной блока B = 24 бит, а также схема PKCS7 дополнения данных до размера последнего блока шифра. Для приложенной таблицы двухбайтовой кодировки символов (UTF-8, Little-Endian) расшифруйте текст {8e 26 3b cf 20 70 d7 26 4e c8 1d 77} в режиме OFB, используя в качестве ключа K = {5A 3C 0F}, а в качестве вектора инициализации значение {CB 1E 74}. Значения заданы в шестнадцатеричной системе счисления.

11. Шифры DES, DESX и 3DES.

12. Пусть задан блочный шифр $E(x,k) = x \oplus k$ с длиной блока B = 24 бит, а также схема ISO 10126 дополнения данных до размера последнего блока шифра. Для приложенной таблицы двухбайтовой кодировки символов (UTF-8, Little-Endian) расшифруйте текст {b9 26 43 cf 5a 70 d1 26 45 cf 88 76} в режиме PCBC, используя в качестве ключа K = {5A 3C 0F}, а в качестве вектора инициализации значение {CB, 1E, 74}. Значения заданы в шестнадцатеричной системе счисления.

13. Шифр RSA.

14. Для алгоритма хеширования $h(X) = \bigoplus_{i=1}^{N} x'_i$ с размером блока B = 6 байт и ключом K = {87 10 3E} вычислить код аутентификации сообщения HMAC для своего имени. В качестве схемы дополнения данных до блока хеш-функции используйте ISO/IEC 7816-4.

Таблица кодировки CP866 символов прилагается.

15. Шифр AES.

16. Пусть имеется изображение размером 4x4 пиксела. Растр изображения представлен в формате RGB24. Для блочного алгоритма шифрования $E(x,k) = x \oplus k$ с длиной блока B = 24 бит и ключом k = {5A 3C 0F} вычислить шифротекст для режимов ECB, CBC и CTR. Значения вектора инициализации и NONCE выбрать самостоятельно.

FFFFFF FFFFFF FFFFFF 000000

000000 FFFFFF 000000 FF2222
000000 000000 FF2222 FF2222
FF2222 FF2222 FF2222 FF2222
17. Хеш-алгоритмы SHA.
18. Пусть задан блочный шифр $E(x,k) = x \oplus k$ с длиной блока B = 24 бит, а также схема дополнения последнего блока до нужной длины одним установленным битом слева и необходимым количеством сброшенных бит: (например, для B = 4 бит и x = {b1 b2 b3}: x' = Padd(x) = {b1 b2 b3 1 0 0 0 0}). Для приложенной таблицы кодировки символов зашифруйте свое имя, используя в качестве ключа K = {5A 3C 0F}. Значение задано в шестнадцатеричной системе счисления. Имя задается в кодировке UTF-8, Little-Endian. Таблица кодировки приложена.
19.Ключи шифрования – генерация, стойкость.
20. Пусть задан блочный шифр с длиной блока B = 24 бит, а также схема ISO 10126 дополнения данных до размера последнего блока шифра. В режиме OFB с одним и тем же ключом K = {5A 3C 0F} и вектором инициализации {CB, 1E, 74} проведите шифрование своего имени (в кодировке Windows-1251, таблица прилагается) дважды E(E(M)). Объясните природу эффекта. Наблюдается ли эффект в режимах CFB и CTR?
21. Классы вычислительной сложности.
22. Сгенерировать пару ключей RSA и зашифровать текст «Секрет» в кодировке CP-866, таблица прилагается. Продемонстрировать процедуру дешифрования текста.
23. Блочные шифры. Режимы шифрования.
24. Сгенерировать пару ключей RSA и продемонстрировать процедуры цифровой подписи и верификации сообщения «Данные» в кодировке CP-866, таблица прилагается.
25. Потоковые шифры и гаммирование.
26. Пусть задана стойкая 256-битовая хеш-функция h(M) и известно ее значение D для некоторого сообщения X. Определите количество итераций, необходимых при осуществлении атаки грубой силой, с тем чтобы с вероятностью 50% было найдено такое значение X', при котором h(X') = D. Определите количество итераций, при котором с 50%-ой вероятностью будут найдены любые два значения Y и Y', для которых значения хеш будут одинаковыми.
27. Цели и виды криптоанализа.
28. Определить стойкость шифра (Ax+b) mod m, если мощность алфавита x равна m.
29. Криптографические протоколы. Роли сторон. Типы протоколов.

30. Определить операцию дешифрования, обратную функции (Ax+b) mod m, где x – байт данных, A = 223, b = 100, m = 256.
31. Атака «человек-в-середине». Методы защиты от атаки.
32. Вскрыть аффинный шифр (знаки препинания и пробелы сохранены) с помощью частотного анализа:
ПЯАЮПФГФЪЁЬЬЯО НА, ГЗЬЯЛЗЖФАЙЗ З ЯБСНЛЯСЗЖФАЙЗ ПЯАЮПФГФЪОО ПЯРНСК ЮН ПЯЦЪЗЖЬКЛ ЛЯЧЗЬЯЛ АЗАСФЛК ГЪО НРПЯРНСЙЗ, ЦЯАСЯБЪОФС ЬЯРНП АФСФБКД ЛЯЧЗЬ НРПЯРЯСКБЯСЫ ЗЬУНПЛЯХЗЭ ЮЯПЯЪЪФЪЫЬН. ЮНЪЫЦНБЯСФЪЫ ПЯАЮПФГФЪЁЬЬНШ НА, БННРИФ ТНБНПО, ЬФ ЗЛФФС АБФГФЬЗШ Н СНЛ, ЬЯ ЙЯЙНШ ЛЯЧЗЬФ БКЮНЪЬОФСАО ФТН ПЯРНСЯ.
ПЯАЮПФГФЪЁЬЬЯО НА АВИФАСБВФС ЙЯЙ ФГЗЬЯО НЮФПЯХЗНЬЬЯО АЗАСФЛЯ Б ЛЯАЧСЯРЯД БКЖЗАЪЗСФЪЫЬНШ АЗАСФЛК. ЙЯЕГКШ ЙНЛЮЫЭСФП АФСЗ, ПЯРНСЯЭИФШ ЮНГ ВЮПЯБЪФЬЗФЛ ПЯАЮПФГФЪЁЬЬНШ НА, БКЮНЪЬОФС ЖЯАСЫ УВЬЙХЗШ МСНШ ТЪНРЯЪЫЬНШ НА. ПЯАЮПФГФЪЁЬЬЯО НА НРЩФГЗЬОФС БАФ ЙНЛЮЫЭСФПК АФСЗ Б СНЛ АЛКАЪФ, ЖСН НЬЗ ПЯРНСЯЭС Б СФАЬНШ ЙННЮФПЯХЗЗ ГПВТ А ГПВТНЛ ГЪО МУУФЙСЗБЬНТН ЗАЮНЪЫЦНБЯЬЗО БАФД ПФАВПАНБ ЙНЛЮЫЭСФПЬНШ АФСЗ.
Таблица частот прилагается.
33. Пусть сторона A знает эффективный алгоритм решения некоторой сложной проблемы (напр., она нашла полиномиальный алгоритм разложения чисел на сомножители). За это решение ей полагается премия в миллион долларов. Однако выдающее премию лицо B не доверяет A и желает убедиться в том, что решение проблемы действительно существует. При этом сторона A также не доверяет B и не желает раскрывать решения до получения премии.
Сформулировать эвристический протокол действий сторон в этих условиях.
34. Вскрыть аффинный шифр ТЙСЗМЧ, если известно, что открытому тексту АЯ соответствует шифротекст ЩВ.
35. Генерация случайных последовательностей. Оценка «случайности».
36. Используя автоключевой шифр зашифровать сообщение «АВТОРИЗАЦИЯ» для заданного начального смещения.
37. Протоколы распределения ключей с помощью посредника и ассиметричных методов.
38. С помощью шифра Виженера зашифровать собственное имя, используя фамилию в качестве ключа.
39. Протокол доказательства с нулевым разглашением.

40. Оценить сложность вскрытия шифра перестановки, который посимвольно записывает открытый текст в таблицу – строка за строкой – и генерирует шифротекст, последовательно составленный из символов столбцов таблицы.
41. Протоколы подбрасывания честной монеты и мысленного покера.
42. Описать протокол цифровой подписи данных с помощью хеш-функций и показать его стойкость. Расширить на произвольное число подписантов.
43. Криптография и стеганография. Задачи криптографии и криптоанализа. Принцип Керкгоффса.
44. Существует некоторый центр хранения данных, (интернет) адрес которого известен и априори является подлинным только при регистрации клиентов. Создать возможные протоколы аутентификации клиентов серверу.
45. Распределение ключей в криптографии.
46. Используя ключ шифрования {65 67 25 8B 05 15 97 03 11}, расшифровать сообщение {35 b1 b9 bb 77 43 97 8b ff} используя шифр Хилла. Шифрование и дешифрование производится по столбцам. Кодировка символов – Windows-1251, прилагается.
47. Ключи шифрования – генерация, стойкость.
48. Предположим, две стороны хотят подписать данные, но ни одна не желает ставить свою подпись первой. Проанализируйте возможные выходы из ситуации и предложите протокол.
49. Цели и виды криптоанализа.
50. Определить тип атаки на секретную информацию в каждом из следующих случаев: (1) студент проникает в преподавательскую и крадет ответы к экзаменационным билетам; (2) студент каждый день многократно пытается пересдать долг, беря преподавателя на измор и отнимая время на проведение некоторого учебного мероприятия; (3) студент просит своего более способного товарища написать ответы на свой билет.
51. С общих позиций рассмотреть области применимости, достоинства и недостатки симметричных и асимметричных шифров. Указать методы реализации инфокоммуникационных протоколов со смешанным применением симметричных и асимметричных шифров.
52. Найти частное и общее решение линейных диофантовых уравнений в целых числах или доказать отсутствие решений:

$$25x + 10y = 15;$$
$$40x + 16y = 88;$$
$$40x + 30y = 98.$$

53. Спроектировать потоковый шифр с генератором гаммы на основе трех сдвиговых регистров с обратной связью с соответствующими характеристическими полиномами $x^{10} + x^3 + 1$, $x^9 + x + 1$, $x^8 + x^4 + x^3 + x + 1$.

Проинициализировав эти регистры значениями 0x23C, 0x122 и 0x10F соответственно, показать шестнадцать первых псевдослучайных бит результирующей гаммы.

54. Пусть имеется некоторая вычислительная сеть, число узлов в которой равно n. Связь в этой сети осуществляется только с шифрованием передаваемых данных симметричными методами, но при этом ни один из узлов не доверяет всем остальным узлам, и коммуникация между парой узлов должна быть защищена от наблюдения всеми остальными узлами. Определить необходимое количество ключей шифрования в такой сети.

Далее пусть в такую сеть добавлен специальный узел, играющий в инфокоммуникационных протоколах роль посредника, которому абсолютно доверяют все без исключения остальные узлы. Определить минимально возможное количество ключей симметричного шифрования в этом случае.

Отдельно определить количество ключей, если посредник берет на себя роль генератора временны̀х ключей шифрования для коммуникации между двумя любыми узлами по запросу от них.

55. Пусть $\mathbb{Z}_{15} = [0;\ 15) \subset \mathbb{Z}$, и $\forall z \in \mathbb{Z}_{15}^*: \gcd(z, 15) = 1, \mathbb{Z}_{15}^* \subset \mathbb{Z}$, где $\mathbb{Z}$– множество целых чисел. Пусть $\forall x, y \in \mathbb{Z}_{15}: x \circ y = (x + y) \bmod 15$ и $\forall x, y \in \mathbb{Z}_{15}^*: x * y = (xy) \bmod 15$. Найти все подгруппы групп $G_+ = \langle \mathbb{Z}_{15}, \circ \rangle$ и $G_* = \langle \mathbb{Z}_{15}^*, * \rangle$.

56. Разделить число x на y, где x = 0xA1 и y = 0x13, если $x, y \in GF(2^8)$ с неприводимым полиномом $x^8 + x^4 + x^3 + x + 1$.

57. Сгенерировать элементы поля $GF(2^5)$ с неприводимым полиномом $x^5 + x^2 + 1$.

58. Известно, что в результате единичного преобразования SubBytes шифра AES байт шифруемых данных x подвергается аффинному преобразованию в байт c: $c = Ax + B$, где A и B – определенные в AES инвариантные матрицы

$$= \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \end{pmatrix}, B = \begin{pmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix},$$

а операции сложения и восьмибитовых матричных элементов определяются для поля Галуа $GF(2^8)$ с неприводимым полиномом $x^8 + x^4 + x^3 + x + 1$. Определить обратное преобразование, осуществляемое при дешифровании.

59. Построить таблицу результатов преобразований шестибитовых значений 000000 и 111111 каждым из восьми блоков подстановки шифра DES. Таблицы подстановок приведены в приложении.

Критерии оценки устного ответа

✓ 100-86 баллов - если ответ показывает глубокое и систематическое знание всего программного материала и структуры конкретного вопроса, а также основного содержания и новаций лекционного курса по сравнению с учебной литературой. Студент демонстрирует отчетливое и свободное владение концептуально-понятийным аппаратом, научным языком и терминологией соответствующей научной области. Знание основной литературы и знакомство с дополнительно рекомендованной литературой. Логически корректное и убедительное изложение ответа.

✓ 85-76 - баллов - знание узловых проблем программы и основного содержания лекционного курса; умение пользоваться концептуально-понятийным аппаратом в процессе анализа основных проблем в рамках данной темы; знание важнейших работ из списка рекомендованной литературы. В целом логически корректное, но не всегда точное и аргументированное изложение ответа.

✓ 75-61 - балл – фрагментарные, поверхностные знания важнейших разделов программы и содержания лекционного курса; затруднения с использованием научно-понятийного аппарата и терминологии учебной дисциплины; неполное знакомство с рекомендованной литературой; частичные затруднения с выполнением предусмотренных программой заданий; стремление логически определенно и последовательно изложить ответ.

✓ 60-50 баллов – незнание, либо отрывочное представление о данной проблеме в рамках учебно-программного материала; неумение использовать понятийный аппарат; отсутствие логической связи в ответе.