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

ИНЖЕНЕРНАЯ ШКОЛА

«СОГЛАСОВАНО»
Руководитель ОП

_____ __ Л.Г. Стаценко ___
(подпись) (Ф.И.О. рук. ОП)
«29» 06 2016 г.

«УТВЕРЖДАЮ»
Заведующая кафедрой
Электроники и средств связи (ЭиСС)

_____ Л.Г. Стаценко _
(подпись) (Ф.И.О. зав. каф.)
«29» 06 2016 г.

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ
Методы и средства защиты информации
Направление подготовки 11.03.02 Инфокоммуникационные технологии и системы связи
профиль «Системы радиосвязи и радиодоступа»
Форма подготовки очная

курс 3 семестр 5
лекции 18 час.
практические занятия 36 час.
лабораторные работы не предусмотрены учебным планом.
в том числе с использованием МАО лек. 0/пр. 0/лаб. 0 час.
всего часов аудиторной нагрузки 54 час.
в том числе с использованием МАО 0 час.
самостоятельная работа 54 час.
в том числе на подготовку к экзамену 36 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 высшего образования Дальневосточного федерального университета, принятого решением Ученого совета ДВФУ, протокол от 25.02.2016 № 02-16, введен в действие приказом ректора ДВФУ от 10.03.2016 № 12-13-391

Рабочая программа обсуждена на заседании кафедры электроники и средств связи, протокол №21 от «29» июня 2016г.

Заведующая кафедрой Стаценко Л.Г. профессор каф. ЭиСС, д.ф.-м.н.
Составитель: Чусов А.А., доцент каф. ЭиСС, к.т.н.

I. Рабочая программа пересмотрена на заседании кафедры:

Протокол от «10» 07 2018 г. № 16

Заведующий кафедрой _____ _____
(подпись) (И.О. Фамилия)

II. Рабочая программа пересмотрена на заседании кафедры:

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

Заведующий кафедрой _____ _____
(подпись) (И.О. Фамилия)

ABSTRACT

Bachelor's degree in 11.03.02 Infocommunication Technologies and Systems

Study profile/ Specialization/ Bachelor's Program "Systems of radiocommunication and radio access"

Course title: Methods and means of information security

Variable part of Block 1, 4 credits

Instructor: *Chusov A.A.*

At the beginning of the course a student should be able to:

- communicate with others, both verbally and in the writing form, using the official state language of the Russian Federation and foreign languages in order to address professional problems (GC-12);
- work with computers and computer networks, perform computer simulation of hardware devices, systems and processes using packages of general-purpose software applications (GPC-4);
- study sources of scientific and technical information, perceive domestic and world experience of the research domain (PC-17);
- conduct and manage a practical use and application of research results (PC-20).

Learning outcomes:

General Professional Competence

GPC-1 – the ability to understand the nature and significance of information in development of modern society, understand dangers and threats of this process, to adhere basic requirements of information security, including the security of state secrets.

GPC-2 – the ability to address ordinary challenges of professional activity based on informational and bibliographical culture and with a use of information technologies taking into account basic principles of information security.

Professional Competence

PC-18 – the ability to exploit modern theoretical and experimental methods to create new innovative means of electric communications and informatics.

Course description.

The course covers the following topics.

Basics of information security in telecommunication systems.

Stenography and cryptography.

Mathematical foundations of cryptography.

Historical and modern cryptographic primitives.

Cryptographic protocols.

Means and tools for data and principal security in telecommunications.

Main course literature:

1. Petrov S.V. Informacionnaja bezopasnost' [Information Security]. – Saratov: IPR Books, 2015. – 326p. (rus).

2. Golikov A.M. Zashhita informacii ot utechki po tehnicheskim kanalam [Protection from leakage of information via technical channels]. – Tomsk: Tomsk State University of Control Systems and Radioelectronics, 2015. – 256p. (rus).

3. Skrypnikov A.V. Bezopasnost' sistem baz dannyh [Security of database systems]. – Voronezh: Voronezh State Agricultural University, 2015. – 144p. (rus)

4. Chujanov A. G. Problemy zashhishhennosti telekommunikacionnyh sistem [Security problems of telecommiunication systems]. – Omsk: Omsk academy of MIA of Russia, 2015. – 164p. (rus).

5. Gorjuhina E.Ju. Informacionnaja bezopasnost' [Information Security]. – Voronezh: FSBEI HE «VSUET», 2015. – 221p. (rus)

Form of final control: exam.

АННОТАЦИЯ

Рабочая программа дисциплины «Методы и средства защиты информации» разработана для студентов бакалавриата 3 курса, обучающихся по направлению 11.03.02 Инфокоммуникационные технологии и системы связи, профиль «Системы радиосвязи и радиодоступа».

Дисциплина «Методы и средства защиты информации» базируется на дисциплинах «Дискретная математика», «Информатика в инфокоммуникациях», «Линейная алгебра и аналитическая геометрия», «Алгоритмические языки программирования в задачах инфокоммуникаций», «Пакеты прикладных программ в инфокоммуникациях», изучаемых в бакалавриате.

Общая трудоемкость освоения дисциплины составляет 5 зачетных единиц (144 часов). Учебным планом предусмотрены лекционные занятия (18 час.), практические занятия (36 час.), самостоятельная работа студента (54 час.), подготовка к экзамену (36 час.). Данная дисциплина входит в вариативную часть блока дисциплин по выбору. Дисциплина реализуется на 3 курсе в 5 семестре.

Дисциплина «Методы и средства защиты информации» базируется на дисциплинах «Дискретная математика», «Информатика в инфокоммуникациях», «Линейная алгебра и аналитическая геометрия», «Алгоритмические языки программирования в задачах инфокоммуникаций», «Пакеты прикладных программ в инфокоммуникациях», изучаемых в бакалавриате.

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

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:

- способность к коммуникации в устной и письменной формах на русском и иностранном языках для решения задач межличностного и межкультурного взаимодействия (ОК-12);
- способность иметь навыки самостоятельной работы на компьютере и в компьютерных сетях, осуществлять компьютерное моделирование устройств, систем и процессов с использованием универсальных пакетов прикладных компьютерных программ (ОПК-1);
- готовность изучать научно-техническую информацию, отечественный и зарубежный опыт по тематике исследования (ПК-17);
- готовность к организации работ по практическому использованию и внедрению результатов исследований (ПК-20).

Планируемые результаты обучения по данной дисциплине (знания, умения, владения), соотнесенные с планируемыми результатами освоения образовательной программы, характеризуют этапы формирования следующих компетенций (общекультурные/ общепрофессиональные/ профессиональные компетенции (элементы компетенций)):

Код и формулировка компетенции	**Этапы формирования компетенции**	
ОПК-1 способностью понимать сущность и значение информации в развитии современного информационного общества, сознавать опасности и угрозы, возникающие в этом	Знает	основные формы представления информации в современных компьютерных устройствах и сетях, а также защиты участников информационного обмена в них с учетом основных требований информационной безопасности
	Умеет	применять различные формы представления чувствительной информации в компьютерных устройствах и сетях, а также защиты участников информационного обмена в них с учетом основных требований информационной безопасности

процессе, соблюдать основные требования информационной безопасности, в том числе защиты государственной тайны	Владеет	основными техническими средствами представления и управления чувствительной информацией в компьютерных устройствах и сетях, а также защиты участников информационного обмена в них с учетом основных требований информационной безопасности
ОПК-2 способностью решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением инфокоммуникационных технологий и с учетом основных требований информационной безопасности	Знает	стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением инфокоммуникационных технологий и с учетом основных требований информационной безопасности
	Умеет	решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением инфокоммуникационных технологий и с учетом основных требований информационной безопасности
	Владеет	способностью решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением инфокоммуникационных технологий и с учетом основных требований информационной безопасности
ПК-18 способностью применять современные теоретические и экспериментальные методы исследования с целью создания новых перспективных средств электросвязи и информатики	Знает	актуальные методы теоретико-экспериментальных исследований фундаментальных свойств информационных систем, их влияние и принципы использования для обеспечения защиты информации; обоснования методов защиты информации и информационных систем.
	Умеет	применять современные методы научного познания и исследований для проектирования распределенных информационных систем, удовлетворяющих известным и определенным для конкретных задач производства критериям.
	Владеет	базовыми навыками анализа безопасности информационных систем и синтеза архитектур систем на основе определенных критериев информационной безопасности.

Для формирования вышеуказанных компетенций в рамках дисциплины «Методы и средства защиты информации» не применяются методы активного/ интерактивного обучения.

I. СТРУКТУРА И СОДЕРЖАНИЕ ТЕОРЕТИЧЕСКОЙ ЧАСТИ КУРСА (18 ЧАСОВ)

Тема 1. Политики и модели безопасности вычислительных сетей и систем (4 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.

Тема 2. Методы и средства защиты информации в телекоммуникационных сетях (4 час)

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

Тема 3. 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 4. Средства криптографической защиты информации в телекоммуникационных сетях (4 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. Применение асимметричной криптографии. Стандарт электронной цифровой подписи. Управление ключами в криптографических системах защиты информации. Назначение, классификация и требования к ключам. Генерация ключевой информации.

Тема 5. Криптографические протоколы (2 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. СТРУКТУРА И СОДЕРЖАНИЕ ПРАКТИЧЕСКОЙ ЧАСТИ КУРСА

Практические занятия (36 часов)

Практическое занятие № 1. Математические основы криптографии (8 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 (4 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 (4 часа)

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 (4 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 (4 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.

Практическое занятие № 8. Реализация алгоритма RSA на примере малых простых чисел (2 часа)

Сгенерировать собственные малые ключи RSA и выполнить с их помощью коммуникацию с выбранным собеседником, осуществляя подписание и шифрование сообщения.

III. УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ САМОСТОЯТЕЛЬНОЙ РАБОТЫ ОБУЧАЮЩИХСЯ

Учебно-методическое обеспечение самостоятельной работы обучающихся по дисциплине «Методы и средства защиты информации» представлено в Приложении 1 и 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.

IV. КОНТРОЛЬ ДОСТИЖЕНИЯ ЦЕЛЕЙ КУРСА

№ п/п	Контролируемые разделы / темы дисциплины	Коды и этапы формирования компетенций		Оценочные средства	
				текущий контроль	промежуточная аттестация
1	Политики и модели безопасности компьютерных сетей	ОПК-1 ОПК-2 ПК-18	знает	Устный опрос (УО-1); тесты (ПР-1)	Экзаменационные вопросы 1, 5, 11, 15, 21.
			умеет	Устный опрос (УО-1); контрольная работа (ПР-2)	Экзаменационные вопросы 1, 5, 11, 15, 21.
			владеет	Контрольная работа (ПР-2); тесты (ПР-1)	Экзаменационные вопросы 1, 5, 11, 15, 21.

2	Требования к защите информации в телекоммуникационных сетях	ОПК-1 ОПК-2 ПК-18	знает	Устный опрос (УО-1); тесты (ПР-1)	Экзаменационные вопросы 3, 12, 16, 17, 19, 25, 27, 29.
			умеет	Устный опрос (УО-1); контрольная работа (ПР-2)	Экзаменационные вопросы 3, 12, 16, 17, 19, 25, 27, 29.
			владеет	Контрольная работа (ПР-2); тесты (ПР-1)	Экзаменационные вопросы 3, 12, 16, 17, 19, 25, 27, 29.
3	Методы и средства защиты информации в телекоммуникационных сетях	ОПК-1 ОПК-2 ПК-18	знает	Устный опрос (УО-1); тесты (ПР-1)	Экзаменационные вопросы 5, 7, 9, 10, 11, 13, 21, 23
			умеет	Устный опрос (УО-1); контрольная работа (ПР-2)	Экзаменационные вопросы 5, 7, 9, 10, 11, 13, 21, 23
			владеет	Контрольная работа (ПР-2); тесты (ПР-1)	Экзаменационные вопросы 5, 7, 9, 10, 11, 13, 21, 23
4	Средства криптографической защиты информации в телекоммуникационных сетях	ОПК-1 ОПК-2 ПК-18	знает	Устный опрос (УО-1); тесты (ПР-1)	Экзаменационные вопросы 2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32
			умеет	Устный опрос (УО-1); контрольная работа (ПР-2)	Экзаменационные вопросы 2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32
			владеет	Контрольная работа (ПР-2); тесты (ПР-1)	Экзаменационные вопросы 2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32
5	Криптографические протоколы	ОПК-1 ОПК-2 ПК-18	знает	Устный опрос (УО-1); тесты (ПР-1)	Экзаменационные вопросы 2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32
			умеет	Устный опрос (УО-1); контрольная работа (ПР-2)	Экзаменационные вопросы 2, 4, 6, 8, 10, 12, 14, 16, 18, 20,

					22, 24, 26, 28, 30, 32
			владеет	Контрольная работа (ПР-2); тесты (ПР-1)	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 этапы формирования компетенций в процессе освоения образовательной программы, представлены в Приложении 2.

V. СПИСОК УЧЕБНОЙ ЛИТЕРАТУРЫ И ИНФОРМАЦИОННО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Основная литература

(электронные и печатные издания)

1. Петров С.В. Информационная безопасность [Электронный ресурс]: учебное пособие/ Петров С.В., Кисляков П.А.— Электрон. текстовые данные.— Саратов: Ай Пи Ар Букс, 2015.— 326 с.— Режим доступа: http://www.iprbookshop.ru/33857.html.— ЭБС «IPRbooks».

2. Голиков А.М. Защита информации от утечки по техническим каналам [Электронный ресурс]: учебное пособие/ Голиков А.М.— Электрон. текстовые данные.— Томск: Томский государственный университет систем управления и радиоэлектроники, 2015.— 256 с.— Режим доступа: http://www.iprbookshop.ru/72090.html.— ЭБС «IPRbooks».

3. Безопасность систем баз данных [Электронный ресурс]: учебное пособие/ А.В. Скрыпников [и др.].— Электрон. текстовые данные.— Воронеж: Воронежский государственный университет инженерных технологий, 2015.—

144 с.— Режим доступа: http://www.iprbookshop.ru/50628.html.— ЭБС «IPRbooks»

4. Чуянов А. Г. Проблемы защищенности телекоммуникационных систем [Электронный ресурс]: учебное пособие/ Чуянов А. Г.— Электрон. текстовые данные.— Омск: Омская академия МВД России, 2015.— 164 с.— Режим доступа: http://www.iprbookshop.ru/61873.html.— ЭБС «IPRbooks».

5. Горюхина Е.Ю. Информационная безопасность [Электронный ресурс]: учебное пособие/ Горюхина Е.Ю., Литвинова Л.И., Ткачева Н.В.— Электрон. текстовые данные.— Воронеж: Воронежский Государственный Аграрный Университет им. Императора Петра Первого, 2015.— 221 с.— Режим доступа: http://www.iprbookshop.ru/72672.html.— ЭБС «IPRbooks».

Дополнительная литература

(печатные и электронные издания)

1. Шелухин О.И. Основы стеганографии. Часть 1. Скрытие данных в аудио- и текстовых файлах [Электронный ресурс]: учебное пособие/ Шелухин О.И., Бен Режеб Т.Б.К.— Электрон. текстовые данные.— М.: Московский технический университет связи и информатики, 2015.— 129 с.— Режим доступа: http://www.iprbookshop.ru/61517.html.— ЭБС «IPRbooks».

2. Влацкая И.В. Проектирование и реализация прикладного программного обеспечения [Электронный ресурс]: учебное пособие/ Влацкая И.В., Заельская Н.А., Надточий Н.С.— Электрон. текстовые данные.— Оренбург: Оренбургский государственный университет, ЭБС АСВ, 2015.— 119 с.— Режим доступа: http://www.iprbookshop.ru/54145.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 изучения дисциплины «Методы и средства защиты информации» обучающемуся предлагаются лекционные и практические занятия. Обязательным элементом является также самостоятельная работа. Из 144 общих учебных часов 54 часов отводится на самостоятельную работу студента. В рамках часов, выделенных на самостоятельную работу, студент должен производить подготовку к рейтинговым и зачетным проверкам, а также изучать темы, отведенные преподавателем на самостоятельное изучение. Помимо различных методических указаний и списка рекомендуемой литературы обучающийся должен обсуждать возникающие у него вопросы на консультациях, назначаемых преподавателем.

Примерное распределение часов самостоятельной работы, которые студент должен отводить на тот или иной вид занятий: закрепление лекционного материала – 24 ч., подготовка к практическим занятиям – 30 ч., подготовка к экзамену – 36 ч. Тем не менее, учитывая особенности каждого студента, указанные часы могут варьироваться.

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

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.

К экзамену 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 экзамену необходимо повторить учебный материал, используя конспект лекций, основную и дополнительную литературу, при необходимости посещать консультации. Экзамен проставляется по результатам рейтинга и экзамена.

VII. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Практические занятия проводятся в компьютерном классе.

№	Наименование	Кол-во
1	Библиотечный фонд ДВФУ	
2	Учебные классы ДВФУ С общим количеством: - посадочных мест - рабочих мест (компьютер+монитор) - проекторов, экранов	1 31 16 3
3	Рабочие места с выходом в интернет	16

Приложение 1

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

ИНЖЕНЕРНАЯ ШКОЛА

УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ САМОСТОЯТЕЛЬНОЙ РАБОТЫ ОБУЧАЮЩИХСЯ

по дисциплине «Методы и средства защиты информации»

Направление подготовки 11.03.02 Инфокоммуникационные технологии и системы связи

профиль «Системы радиосвязи и радиодоступа»

Форма подготовки очная

Владивосток
2016

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.	2 неделя обучения	Разработка программного обеспечения асимметричного шифра RSA с использованием своих или сторонних библиотек для работы с длинным целыми и с использованием собственной реализации теста Рабина-Миллера.	4 часа	Проект
2.	2 неделя обучения	Разработка программного обеспечения контроля целостности на основе хеш функций SHA-512/T, SHA-224 и SHA-384.	4 часа	Проект
2.	2 неделя обучения	Абстрактная алгебра и алгебраические структуры в криптографии. Аддитивные и мультипликативные группы. Генерация циклических групп. Кольца и поля.	2 часа	Собеседование
3.	2 неделя обучения	Шифр DES.	2 часа	Собеседование
4.	2 неделя обучения	Шифр AES.	2 часа	Собеседование
5.	4 неделя обучения	Разработка программного обеспечения алгоритмов электронно-цифровой подписи DSA, ГОСТ 34.10.-2001, ГОСТ 34.11-94.	4 часа	Проект
6.	4 неделя обучения	Реализация криптографической защиты на сетевом и прикладном уровнях OSI.	4 часа	Собеседование
7.	6 неделя обучения	Библиотека cryptlib.	4 часа	Собеседование
8.	8 неделя обучения	Китайская теорема об остатках. Доказательство и применение в криптографии.	4 часа	Собеседование

9.	10 неделя обучения	Криптографические генераторы псевдослучайных последовательностей NIST SP 800-90.	4 часа	Проект
10.	10 неделя обучения	Тесты качества псевдослучайных генераторов Diehard.	4 часа	Собеседование
11.	10 неделя обучения	Информационная безопасность в мобильных сетях. Потоковые шифры A5 (история и современное состояние) и методов аутентификации и генерации сеансовых ключей A3/A8.	4 часа	Собеседование
12.	10 неделя обучения	Линейные сдвиговые регистры с обратной связью. Их использование для генерации гаммы в потоковых шифрах.	4 часа	Собеседование
13.	10 неделя обучения	Протокол «Мысленный покер».	4 часа	Проект
14.	10 неделя обучения	Криптография на основе эллиптических кривых	4 часа	Собеседование
15.	В течение семестра	Подготовка к экзамену	36 часов	Экзамен

Характеристика заданий для самостоятельной работы обучающихся и методические рекомендации по их выполнению

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.

Требования к представлению и оформлению результатов самостоятельной работы

Самостоятельная работа считается выполненной, в отчете по проделанной работе представлено письменные пояснения к полученным выводам и, если

требуется, код программной реализации, компилируемый и выполняющий задачу корректно.

Критерии оценки выполнения самостоятельной работы

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

Приложение 2

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

ИНЖЕНЕРНАЯ ШКОЛА

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

по дисциплине «Методы и средства защиты информации»

Направление подготовки 11.03.02 Инфокоммуникационные технологии и системы связи
профиль «Системы радиосвязи и радиодоступа»
Форма подготовки очная

Владивосток
2016

Паспорт ФОС

Код и формулировка компетенции	Этапы формирования компетенции	
ОПК-1 понимать сущность и значение информации в развитии современного информационного общества, сознавать опасности и угрозы, возникающие в этом процессе, соблюдать основные требования информационной безопасности, в том числе защиты государственной тайны	Знает	основные формы представления информации в современных компьютерных устройствах и сетях, а также защиты участников информационного обмена в них с учетом основных требований информационной безопасности
	Умеет	применять различные формы представления чувствительной информации в компьютерных устройствах и сетях, а также защиты участников информационного обмена в них с учетом основных требований информационной безопасности
	Владеет	основными техническими средствами представления и управления чувствительной информацией в компьютерных устройствах и сетях, а также защиты участников информационного обмена в них с учетом основных требований информационной безопасности
ОПК-2 способностью решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением инфокоммуникационных технологий и с учетом основных требований информационной безопасности	Знает	стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением инфокоммуникационных технологий и с учетом основных требований информационной безопасности
	Умеет	решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением инфокоммуникационных технологий и с учетом основных требований информационной безопасности
	Владеет	способностью решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением инфокоммуникационных технологий и с учетом основных требований информационной безопасности
ПК-18 способностью применять современные теоретические и экспериментальные методы исследования с целью создания новых перспективных	Знает	актуальные методы теоретико-экспериментальных исследований фундаментальных свойств информационных систем, их влияние и принципы использования для обеспечения защиты информации; обоснования методов защиты информации и информационных систем.
	Умеет	применять современные методы научного познания и исследований для проектирования

средств электросвязи и информатики		распределенных информационных систем, удовлетворяющих известным и определенным для конкретных задач производства критериям.
	Владеет	базовыми навыками анализа безопасности информационных систем и синтеза архитектур систем на основе определенных критериев информационной безопасности.

№ п/п	Контролируемые разделы / темы дисциплины	Коды и этапы формирования компетенций		Оценочные средства	
				текущий контроль	промежуточная аттестация
1	Политики и модели безопасности компьютерных сетей	ОПК-1 ОПК-2 ПК-18	знает	Устный опрос (УО-1); тесты (ПР-1)	Экзаменационные вопросы 1, 5, 11, 15, 21.
			умеет	Устный опрос (УО-1); контрольная работа (ПР-2)	Экзаменационные вопросы 1, 5, 11, 15, 21.
			владеет	Контрольная работа (ПР-2); тесты (ПР-1)	Экзаменационные вопросы 1, 5, 11, 15, 21.
2	Требования к защите информации в телекоммуникационных сетях	ОПК-1 ОПК-2 ПК-18	знает	Устный опрос (УО-1); тесты (ПР-1)	Экзаменационные вопросы 3, 12, 16, 17, 19, 25, 27, 29.
			умеет	Устный опрос (УО-1); контрольная работа (ПР-2)	Экзаменационные вопросы 3, 12, 16, 17, 19, 25, 27, 29.
			владеет	Контрольная работа (ПР-2); тесты (ПР-1)	Экзаменационные вопросы 3, 12, 16, 17, 19, 25, 27, 29.
3	Методы и средства защиты информации в телекоммуникационных сетях	ОПК-1 ОПК-2 ПК-18	знает	Устный опрос (УО-1); тесты (ПР-1)	Экзаменационные вопросы 5, 7, 9, 10, 11, 13, 21, 23
			умеет	Устный опрос (УО-1); контрольная работа (ПР-2)	Экзаменационные вопросы 5, 7, 9, 10, 11, 13, 21, 23
			владеет	Контрольная работа (ПР-2); тесты (ПР-1)	Экзаменационные вопросы 5, 7, 9, 10, 11, 13, 21, 23
4	Средства криптографической защиты информации в	ОПК-1 ОПК-2 ПК-18	знает	Устный опрос (УО-1); тесты (ПР-1)	Экзаменационные вопросы 2, 4, 6, 8, 10, 12, 14, 16, 18, 20,

	телекоммуникационных сетях				22, 24, 26, 28, 30, 32
			умеет	Устный опрос (УО-1); контрольная работа (ПР-2)	Экзаменационные вопросы 2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32
			владеет	Контрольная работа (ПР-2); тесты (ПР-1)	Экзаменационные вопросы 2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32
5	Криптографические протоколы	ОПК-1 ОПК-2 ПК-18	знает	Устный опрос (УО-1); тесты (ПР-1)	Экзаменационные вопросы 2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32
			умеет	Устный опрос (УО-1); контрольная работа (ПР-2)	Экзаменационные вопросы 2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32
			владеет	Контрольная работа (ПР-2); тесты (ПР-1)	Экзаменационные вопросы 2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32

Шкала оценивания уровня сформированности компетенций

Код и формулировка компетенции	**Этапы формирования компетенции**		**критерии**	**показатели**
ОПК-1 понимать сущность и значение информации в развитии современного информационного	знает (пороговый уровень)	основные формы представления информации в современных компьютерных устройствах и сетях, а также защиты участников информационного обмена в них	Знание способов представления информации в современных компьютерных устройствах и сетях, а также защиты участников информационного обмена в них с учетом	Знание критериев адекватного метода представления данных при защищенном информационном обмене средствами криптографии, а также целей и

общества, сознавать опасности и угрозы, возникающие в этом процессе, соблюдать основные требования информационной безопасности, в том числе защиты государственной тайны		с учетом основных требований информационной безопасности	основных требований информационной безопасности	задач защиты информации и принципалов
	умеет (продвинутый)	выбирать адекватные формы представления информации в современных компьютерных устройствах и сетях, а также защиты участников информационного обмена в них с учетом основных требований информационной безопасности	Умение анализировать и осуществлять выбор и адекватное применение методов и адекватные форм представления информации в современных компьютерных устройствах и сетях, а также защиты участников информационного обмена в них с учетом основных требований информационной безопасности	Способность обосновать выбор корректных протоколов, алгоритмов защиты информации в соответствии с требованиями и ограничениями телекоммуникационной системы и среды передачи данных
	владеет (высокий)	основными техническими средствами представления и управления чувствительной информацией в компьютерных устройствах и сетях, а также защиты участников информационного обмена в них с учетом основных требований информационной безопасности	Владение техническими средствами представления и управления чувствительной информацией в компьютерных устройствах и сетях, а также защиты участников информационного обмена в них с учетом основных требований информационной безопасности	Способность решать основные задачи защиты информации и узлов телекоммуникационных систем.
ОПК-2 способностью решать	знает (пороговый уровень)	стандартные задачи профессиональной деятельности	Знание основных задач профессиональной деятельности	Знание критериев выбора адекватных

стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением инфокоммуникационных технологий и с учетом основных требований информационной безопасности		на основе информационной и библиографической культуры с применением инфокоммуникационных технологий и с учетом основных требований информационной безопасности	на основе информационной и библиографической культуры с применением инфокоммуникационных технологий и с учетом основных требований информационной безопасности	средств информационных систем для решения стандартных задач профессиональной деятельности
	умеет (продвинутый)	решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением инфокоммуникационных технологий и с учетом основных требований информационной безопасности	Умение решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением инфокоммуникационных технологий и с учетом основных требований информационной безопасности	Умение корректно проанализировать поставленную задачу, составить алгоритм ее решения и оценить эффективность с точки зрения требований к безопасности передаваемых данных и участников информационного обмена
	владеет (высокий)	способностью решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением инфокоммуникационных технологий и с учетом основных требований	Владение способностью решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением инфокоммуникационных технологий и с учетом основных	Основными методами решения задач обеспечения защиты информации в телекоммуникационных системах, включая шифрование данных, авторизацию и аутентификацию сторон информационного обмена и сообщений.

		информационной безопасности	требований информационной безопасности.	
ПК-18 способностью применять современные теоретические и экспериментальные методы исследования с целью создания новых перспективных средств электросвязи и информатики	знает (пороговый уровень)	актуальные методы и современные средства анализа безопасности инфотелекоммуникационных систем, требования к безопасности систем, моделирования и проектирования систем на основе заданных критериев информационной безопасности.	Знает средства и методы оценки стойкости информационных систем, основные известные на текущий момент потенциальные уязвимости информационных систем, методы реализаций безопасных протоколов взаимодействия и политик безопасности информационных систем на основе существующих примитивов реализации информационной безопасности.	Знает основные фундаментальные положения математики и информатики, ограничивающие вычислительные возможности злоумышленника, принципы оценки стойкости информационных систем к вскрытию с учетом технического и технологического прогресса, основные известные пути вскрытия телекоммуникационных протоколов взаимодействия подсистем информационной системы через незащищенные каналы связи.
	умеет (продвинутый)	выполнять оценку стойкости информационный и телекоммуникационных систем к вскрытию в различных сценариях существования и взаимодействия систем; выбирать адекватные сегодня и в	Умеет осуществлять и обосновывать выбор адекватных методов и средств реализации информационной безопасности инфотелекоммуникационных систем на основе требований ку этим системам в различных сценариях	Умеет приводить обоснованный с теоретической точки зрения выбор адекватных методов защиты информации и инфотелекоммуникационных систем для заданных требований к безопасности. Умеет формулировать

		будущем методы и средства реализации информационной безопасности на основе выбранных требований к критерию информационной безопасности.	использования и задач, решаемых в предметной области.	требования и критерий безопасности инфотелекоммуникационных систем для решения типичных задач телекоммуникации и взаимодействия информационных систем.
	владеет (высокий)	навыками реализации информационной безопасности инфотелекоммуникационных систем, дизайна систем безопасности систем и выбора адекватных примитивных средств информационной безопасности.	Владеет навыками реализации методов информационной безопасности на основе выбранных требований к критерию информационной безопасности, а также формального описания и обоснования этих требований в типичных сценариях развертывания и реализации инфотелекоммуникационных систем.	Владеет навыками реализации телекоммуникационных криптопротоколов и выбора адекватных примитивов криптографической защиты информации и принципалов инфотелекоммуникационных систем, а также навыками элементарного анализа безопасности информационных и телекоммуникационных систем и формулировки требований к ней.

Методические рекомендации, определяющие процедуры оценивания результатов освоения дисциплины

Оценочные средства для промежуточной аттестации

Для допуска к экзамену студент должен привести обоснование решений представленных практических заданий.

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

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 А 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 В не доверяет А и желает убедиться в том, что решение проблемы действительно существует. При этом сторона А также не доверяет В 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.

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.

Оценочные средства для текущей аттестации

Перечень дискуссионных тем для дискуссии

по дисциплине «Методы и средства защиты информации»

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.

Критерии оценки:

✓ 100-85 баллов выставляется студенту, если ответ показывает прочные знания основных процессов изучаемой предметной области, отличается глубиной и полнотой раскрытия темы; владение терминологическим аппаратом; умение объяснять сущность, явлений, процессов, событий, делать выводы и обобщения, давать аргументированные ответы, приводить примеры; свободное владение монологической речью, логичность и последовательность ответа; умение приводить примеры современных проблем изучаемой области.

✓ 85-76 баллов выставляется студенту, если ответ, обнаруживающий прочные знания основных процессов изучаемой предметной области, отличается глубиной и полнотой раскрытия темы; владение терминологическим аппаратом; умение объяснять сущность, явлений, процессов, событий, делать выводы и обобщения, давать аргументированные ответы, приводить примеры; свободное владение монологической речью, логичность и последовательность ответа. Однако допускается одна - две неточности в ответе.

✓ 75-61 баллов выставляется студенту, если оценивается ответ, свидетельствующий в основном о знании процессов изучаемой предметной области, отличающийся недостаточной глубиной и полнотой раскрытия темы;

знанием основных вопросов теории; слабо сформированными навыками анализа явлений, процессов, недостаточным умением давать аргументированные ответы и приводить примеры; недостаточно свободным владением монологической речью, логичностью и последовательностью ответа. Допускается несколько ошибок в содержании ответа; неумение привести пример развития ситуации, провести связь с другими аспектами изучаемой области.

✓ 60-50 баллов выставляется студенту, если ответ, обнаруживающий незнание процессов изучаемой предметной области, отличающийся неглубоким раскрытием темы; незнанием основных вопросов теории, несформированными навыками анализа явлений, процессов; неумением давать аргументированные ответы, слабым владением монологической речью, отсутствием логичности и последовательности. Допускаются серьезные ошибки в содержании ответа; незнание современной проблематики изучаемой области.