МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГРОЗНЕНСКИЙ ГОСУДАРСТВЕННЫЙ НЕФТЯНОЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ

имени академика М.Д. Миллионщикова

«УТВЕРЖДАЮ»

Первый проректор

И.Г. Гайрабеков

«02» 03 2021 г.

РАБОЧАЯ ПРОГРАММА

дисциплины

«Криптографические методы защиты и средства обеспечения информационной безопасности инфокоммуникаций»

Направление подготовки

11.03.02 Инфокоммуникационные технологии и системы связи

Направленность (профиль)

«Инфокоммуникационные сети и системы»

Квалификация

бакалавр

Год начала подготовки -2020

Грозный – 2021

1. Цели и задачи дисциплины

Целью изучения дисциплины «Криптографические методы защиты и средства обеспечения информационной безопасности инфокоммуникаций» является изучение технических средств и методов защиты информации автоматизированных систем обработки информации и управления, ремонту и техническому обслуживанию этой аппаратуры.

Задачи изучения дисциплины обеспечение конфиденциальности и защиты информационных данных компьютерных сетей в процессе передачи ее по сети между пользователями системы/

2. Место дисциплины в структуре образовательной программы

Дисциплина относится к части, формируемой участниками образовательных отношений программы бакалавриата сприсвоением квалификации «Бакалавр»по направлению подготовки 11.03.02 Инфокоммуникационные технологии и системы связи.

3. Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с индикаторами достижения компетенций

Таблица 1

Код по ФГОС	**Индикаторы достижения**	**Планируемые результаты обучения по дисциплине (ЗУВ)**
Профессиональные		
ПК-9 Способен к администрированию средств обеспечения безопасности удаленного доступа (операционных систем и специализированных протоколов)	**ПК-9.1.** Использует общие принципы функционирования и архитектуру аппаратных, программных и программно-аппаратных средств администрируемой сети; Протоколы канального, сетевого, транспортного и прикладного уровней модели взаимодействия открытых систем **ПК-9.2.** Подключает и настраивает современные средства обеспечения безопасности удаленного доступа (операционных систем и специализированных протоколов); работать с контрольно-измерительными аппаратными и программными средствами	**Знать:** **-** основы сетевых технологий и принципы работы сетевого оборудования, правила работы с различными инфокоммуникационными **Уметь:** **-** работать с различными инфокоммуникационными системами и базами данных, обрабатывать информацию о выполнения заявок на техподдержку оборудования с использованием современных технических средств **Владеть:** **-** навыками выбора и использования соответствующего тестового и измерительного оборудования, использования программного обеспечения оборудования

	ПК-9.3. Устанавливает дополнительные программные продукты для обеспечения безопасности удаленного доступа и их параметризация	при его настройке

4. Объем дисциплины и виды учебной работы

Таблица 2

Вид учебной работы		**Всего часов/ зач.ед.**		**Семестры**			
				6	**7**	**7**	**8**
		ОФО	**ЗФО**	**ОФО**		**ЗФО**	
Контактная работа (всего)		**132/3,7**	**32/0,9**	**64/1,7**	**68/1,8**	**16/0,4**	**16/0,4**
В том числе:							
Лекции		66/1,8	16/0,4	32/0,9	34/0,9	8/0,2	8/0,2
Практические занятия		-	-	-	-	-	-
Практическая подготовка		-	-	-	-	-	-
Лабораторные занятия		66/1,8	16/0,4	32/0,8	34/0,9	8/0,2	8/0,2
Самостоятельная работа (всего)		**156/4,3**	**256/7,1**	**80/2,2**	**76/2,1**	**128/3,5**	**128/3,5**
В том числе:							
Курсовая работа (проект)		36/1	36/1	-	36/1	-	36/1
Расчетно-графические работы		-	-	-	-	-	-
ИТР		-	-	-	-	-	-
Рефераты		-	-	-	-	-	-
Доклады		44/1,2	84/2,3	32/0,8	10/0,3	60/1,0	34/0,9
И (или) другие виды самостоятельной работы:							
Подготовка к лабораторным работам		40/1,1	82/2,2	30/0,8	12/0,33	50/1,4	30/0,8
Подготовка к практическим занятиям		-	-	-	-	-	-
Подготовка к зачету		18/0,5	18/0,5	18/0,5	-	18/1,6	-
Подготовка к экзамену		18/0,5	18/0,5	-	18/0,5	-	18/0,5
Вид отчетности				**зачет**	**экзамен**	**зачет**	**экзамен**
Общая трудоемкость дисциплины	**ВСЕГО в часах**	**288**	**288**	**144**	**144**	**144**	**144**
	ВСЕГО в зач. единицах	**8**	**8**	**4**	**4**	**4**	**4**

5. Содержание дисциплины

5.1. Разделы дисциплины и виды занятий

Таблица 3

№ п/п	Наименование раздела дисциплиныпо семестрам	Часы лекционных занятий		Часы лабораторных занятий		Часы практических (семинарских) занятий		Всего часов	
		ОФО	ЗФО	ОФО	ЗФО	ОФО	ЗФО	ОФО	ЗФО
1.	Введение	3	1	3	-	-	-	6	1
2.	Предмет и задачи криптографии	6	2	6	2	-	-	12	4
3.	Методы шифрования с закрытым ключом	13	2	13	2	-	-	26	4
4.	Криптографические алгоритмы с открытым ключом	6	2	6	2	-	-	12	4
5.	Электронная цифровая подпись	10	-	10	1	-	-	20	1
6.	Совершенно секретные системы	4	-	4	1	-	-	8	1
7.	Структура блочного алгоритма симметричного шифрования. Методы симметричного шифрования	4	2	4	2	-	-	8	4
8.	Основные понятия и классификация средств ассиметричной криптографической защиты информации	10	2	10	2	-	-	20	4
9.	Криптографические системы на эллиптических кривы	10	2	10	2	-	-	20	4

5.2. Лекционные занятия

Таблица 4

№ п/п	Наименование раздела дисциплины	Содержание раздела
1.	Введение	Предмет и основные разделы кибернетики. Предмет теории информации. Принцип управления.
2.	Предмет теории информации. Непрерывная и дискретная информация	Характеристики непрерывной и дискретной информации. Перевод непрерывной информации в дискретную. Кодирование информации.
		Частота дискретизации. Теорема Котельникова и ее применение
3.	Общая схема передачи информации	Схема передачи информации. Канал передачи информации. Скорость передачи информации.
		Аналоговые и цифровые преобразователи. Сущность АВМ и ЦВМ и их применение на практике.
4.	Измерение информации	Методы измерения информации. Вероятностный подход к измерению информации. Мера информации Шеннона.
		Понятие энтропии. Свойства количества информации и энтропии. Алфавитный подход к измерению информации.
5.	Кодирование информации	Постановка задачи кодирования. Кодирование информации при передаче без помех. Первая теорема Шеннона. Кодирование информации при передаче в канале с помехами.
		Вторая теорема Шеннона. Основные виды помехоустойчивых кодов. Практическая реализация помехоустойчивого кодирования.
6.	Основы преобразования информации	Сжатие информации, как основной аспект передачи данных. Пределы сжатия информации. Простейшие алгоритмы сжатия информации. Применение метода Шеннона-Фено для сжатия данных. Примеры.
		Метод Хаффмена. Применение метода Хаффмена для сжатия данных. Подстановочные или словарно-ориентированные методы сжатия данных. Арифметический метод сжатия данных
7.	Шифрование информации	Основные понятия классической криптографии. Классификация шифров. Шифры перестановки и шифры замены.
		Потоковые шифрующие системы. Симметричные блочные шифры. Шифры DES, AES. Асимметричные шифры. Шифр RSA.
8.	Криптографические алгоритмы с открытым ключом	Основные понятия и классификация средств ассиметричной криптографической защиты информации. Основные свойства асимметричных криптосистем.
		Предпосылки создания методов шифрования с открытым ключом и основные определения. Односторонние функции. Требования к алгоритмам шифрования с открытым ключом.

9.	Электронная цифровая подпись	История развития. Виды электронных подписей в Российской Федерации. Общая схема электронной цифровой подписи. Использование хеш-функций.
		Стандарты на алгоритмы цифровой подписи. Стандарт цифровой подписи ГОСТ Р34.10-94. Новый отечественный стандарт ЭЦП.Управление открытыми ключами.

5.3. Лабораторные занятия

Таблица 5

№ п/п	Наименование раздела дисциплины	Наименование лабораторных работ
1.	Криптографические алгоритмы с открытым ключом	Программная реализация алгоритма RSA.
2.	Криптографические системы на эллиптических кривы	Программная реализация криптографических протоколов.
3.	Электронная цифровая подпись	Программная реализация ЭЦП.
4.	Шифрование информации	Симметричные блочные шифры. Шифры DES, AES.

5.4. Практические (семинарские) занятия: нет

Обсуждение с преподавателем и размещение в портфолио докладов и презентаций, составленных по тематике лекционного курса. Обработка их в гипертексте и размещение в своем портфолио выполненных самостоятельно лабораторных работ

6. Самостоятельная работа студентов по дисциплине

6.1 Тематика докладов студентов:

Тематика докладов с презентациями:

1. Шифры одноалфавитной замены. Шифр Цезаря, квадрат «Полибия»
2. Ассиметричная криптография и электронная цифровая подпись. Понятия.
3. Аппаратное шифрование DES: структура, перестановки, сеть Файштеля, расширение ключа.
4. Шифры перестановки. Квадрат «Кардана».
5. TEA: структура, алгоритм, образующая функция, ключ.
6. Шифры многоалфавитной замены. Табло Виженера.
7. IDEA: структура, алгоритм, расширение ключа.
8. Шифровальный аппарат Вернама. Шифр Вернама (XOR).
9. Структура ГОСТ 28147-89: образующая функция, расширение ключа.
10. Шифр Плейфейера.
11. Классификация шифров по ключевой информации.
12. Конкурс AES: цели и условия конкурса, алгоритмы шифрования конкурса.
13. Шифр Хилла.
14. MARS структура: образующая функция, схемы входного и выходного

перемешивания.

15. Типы криптоанализа шифрованных сообщений. Понятие защищенности шифрованных сообщений.

16. Основные принципы ассиметричной криптографии.

17. Нелинейные поточные шифры. Фильтрующие шифры. Линейный регистр сдвига.

18. Комбинирующие поточные шифры. Корреляционно-стойкий комбинирующий шифр.

6.2 Тематика курсовых проектов студентов 8 семестр:

1. Система нормативных актов РФ в области защиты от НСД
2. Угрозы и уязвимости современных автоматизированных систем
3. Классы защищённости современных автоматизированных систем и программно-аппаратных средств
4. Авторизация как процесс доступа
5. Реализация механизмов парольной защиты для организации банковского сектора
6. Межсетевые экраны как средство защиты информации от несанкционированного доступа
7. Анализ рынка средств усиления парольной защиты
8. Реализация добавочных механизмов усиления парольной защиты
9. Разработка политики информационной государственной организации безопасности
10. Разработка политики информационной безопасности для организации оборонно-промышленного комплекса
11. Архитектура корпоративной системы машиностроительного предприятия защиты
12. Анализ современных способов разграничения доступа
13. Анализ защищённости внутренней информации инфраструктуры государственной организации сети
14. Анализ защищённости внутренней инфраструктуры сети коммерческой организации
15. Применения инструментальных средств анализа защищённости внутренней инфраструктуры сети
16. Анализ рынка программно-аппаратных средств защиты информации от несанкционированного доступа
17. Технико-экономическая оценка комплексирования средств защиты информации на примере коммерческой организации
18. Разработка модели угроз безопасности информации коммерческой фирмы
19. Разработка модели угроз безопасности информации государственной организации
20. Анализ рынка биометрических средств ввода пароля

Учебно-методическое обеспечение для самостоятельной работы студентов:

Велигоша А.В. Общая теория связи [Электронный ресурс]: учебное пособие / Велигоша А.В. - Электрон. текстовые данные. – Ставрополь: СКФУ, 2018. - 240 с- Режим доступа: https://www.directmedia.ru/book_457770_obschaya_teoriya_svyazi/ - ЭБС «Direct-Media»

7. Оценочные средства

7.1. Вопросы к рубежным аттестациям

7 семестр

Вопросы к 1 рубежной аттестации:

1. Алгоритм Эль Гамаль (асимметричная криптография).
2. Комбинирующий поточный шифр с элементом памяти.
3. Код аутентификации сообщения (MAC). Способы построения MAC. HMAC.
4. Динамический поточный шифр.
5. Определение блочного шифрования. Блок информации. Ключ алгоритма.
6. Абсолютно симметричный блочный шифр.
7. Аутентификация пользователя. Типы систем аутентификации (на симметричных и асимметричных криптосистемах, на сертификатах).
8. Обратимые операции в блочном шифровании.
9. Kerberos. Протокол распределения ключей.
10. Необратимые операции в блочном шифровании.
11. Распространение ключей. Протоколы, основанные на использовании симметрич-ной криптосистемы и случайных параметров.
12. Сети блочных шифров, ветви сети, раунд сети, образующая функция. SP-сеть, KASLT-сеть.
13. Распространение ключей. 3-х этапный протокол Шамира (Shamir).
14. Классическая структура сети Фейстеля. Ветви сети, материал ключа, раунд сети, образующая функция.
15. Распространение ключей. Протокол Needham-Schroeder.
16. Абсолютно симметричная сеть Фейстеля. Модификация сети Фейстеля для большего числа ветвей: тип 1 – размер блока, ветви сети, материал ключа, раунд сети, образующая функция.
17. Распространение ключей. Протоколы на основе асимметричных криптосистем.
18. Алгоритм RSA (асимметричная криптография).

Вопросы ко 2-ой рубежной аттестации:

1. Исторические шифры. Шифр сдвига. Шифр замены. Полиалфавитный шифр. Шифр
2. Виженера. Шифр Вернама. Недостатки исторических шифров. (Информационная стойкость).

3. Информационная стойкость криптографических систем Вычислительно защищенная криптосистема. Основные проблемы вычислительно защищенной криптосистемы. Абсолютнотстойкая (совершенная) криптосистема.
4. К какому классу криптосистем - вычислительно защищенной или абсолютно стойкой относятся следующие криптосистемы: Шифр сдвига. Шифр замены. Шифр Виженера. Шифр Вернама?
5. Энтропия случайной величины. Свойства энтропии. совместная энтропия двух случайных величин. Условная энтропия двух случайных величин. Неопределенность ключа.
6. Энтропия естественного языка. Расстояние единственности шифра.
7. Криптосистема с секретным ключом. Принцип Керкхоффа. Поточные и блочные шифры.
8. Поточные шифры. Генератор ключевого потока. Свойства генератора ключевого потока. Генератор псевдослучайных чисел, основанный на использовании алгебраических свойств М-последовательностей.
9. Статистические тесты генераторов ключевого потока.
10. Блочные шифры. Алгоритм DES. Перестановки. Раунды. Алгоритм Фейстеля при шифровании и дешифровании.
11. Сравнение блочных и поточных шифров. Методы организации процедуры исправления ошибок.
12. Статичный ключ. Эфемерный ключ. Распределение ключей. Основные пути решения проблемы распределения ключей. (физические методы, Протоколы с секретным ключом, Протоколы с открытым ключом, современные физические методы).
13. Разделение секрета. Схема порогового разделения секрета. (T, W) - пороговая схема Шамира.
14. Протоколы распределения секретных ключей. Основные цели протокола распределения ключей. Протокол Барроуза.
15. Протоколы распределения секретных ключей. Основные цели протокола распределения ключей. Протокол Нидхейма-Шредера.

8 семестр

Вопросы к 1-ой рубежной аттестации:

1. Основные понятия, обозначения и задачи криптографии.
2. Исторические примеры криптосистем.
3. Основные принципы криптографической защиты информации. Общая схема системы защиты информации.
4. Функции шифрования. Односторонние функции. Простейшие шифры и их классификация.
5. Основные требования к шифрам, к криптографическим системам.
6. Абсолютно стойкие (совершенные) шифры. Криптостойкость алгоритма шифрования. Особенности симметричных криптосистем.
7. Метод простой подстановки (замены).
8. Метод перестановки.
9. Метод блочных шифров.

10. Метод гаммирования.
11. Метод шифрования на основе теоремы Эйлера-Ферма.
12. Композиция шифров.
13. Стандарт криптосистемы США DES.
14. Стандарт криптосистемы России – ГОСТ 28147-89. Системы защиты с открытым ключом.
15. Криптосистема RSA.
16. Теоретико-числовые алгоритмы и их сложность. Методы дискретного логарифмирования.
17. Система защиты Диффи-Хеллмана. Система защиты информации на основе заданного рюкзака.

Вопросы ко 2-ой рубежной аттестации:

1. Протоколы распределения секретных ключей. Основные цели протокола распре-деления ключей. Протокол Отвэй-Риса.
2. Протоколы распределения секретных ключей. Основные цели протокола распре-деления ключей. Цербер.
3. Арифметика остатков. Сравнение по модулю. Решение уравнения ax = b (mod N).
4. Функция Эйлера. Мультипликативные обратные по модулю N. Теорема Лагранжа. Малая теорема Ферма. Применение в криптографии.
5. Алгоритм Евклида. Китайская теорема об остатках. Расширенный алгоритм Евклида. Применение в криптографии.
6. Криптосистема с открытым ключом. Криптографическая односторонняя функция. Важнейшие криптографические односторонние функции.
7. Оценка сложности задач. Сложность алгоритма: Полиноминальная, экспоненци-альная, субэкспоненциальная Оракул. Сравнительный анализ сложности крипто-графических алгоритмов (без доказательства).
8. Алгоритм RSA. Шифрование в RSA. Дешифрование в RSA. Доказательство алго-ритма.
9. Алгоритм RSA. Задача криптоаналитика. Криптостойкость RSA
10. Криптосистема Эль-Гамаль. Параметры домена. Шифрование. Дешифрование.
11. Криптосистема Рабина. Алгоритм. Шифрование. Дешифрование.
12. Простые числа. Важность проблемы тестирования простых чисел. Пробное деле-ние.
13. Распределение ключей Диффи ? Хеллмана. Алгоритм. Стойкость. Атака человек посередине. Необходимость использования цифровой подписи.
14. Алгоритмом цифровой подписи RSA.
15. Криптографическая Хэш-функция. Свойства криптографической хэш-функции. Свойство односторонности Защищенность от повторений, защищенностью от вто-рых прообразов.
16. Алгоритмом цифровой подписи DSA.
17. Отечественный стандарт цифровой подписи ГОСТ Р 34.10-94.
18. Квантовая криптография.
19. Передача секретных ключей по радиоканалу.

Помимо проверки знания теоретического материала, на аттестации / экзамене студентам предлагаются практические задания по разделам дисциплины.

Образец билетов рубежной аттестации:

Грозненский Государственный Нефтяной Технический Университет
им. акад. М.Д. Миллионщикова
Кафедра «Сети связи и системы коммутации»
Дисциплина «Криптографические методы защиты и средства обеспечения информационной безопасности инфокоммуникаций»
1-я рубежная аттестация
Группа: _____ Семестр: _____
Билет №

1. Классическая структура сети Фейстеля. Ветви сети, материал ключа, раунд сети, образующая функция
2.Алгоритм RSA (асимметричная криптография).

Преподаватель_____

Грозненский Государственный Нефтяной Технический Университет
им. акад. М.Д. Миллионщикова
Кафедра «Сети связи и системы коммутации»
Дисциплина «Криптографические методы защиты и средства обеспечения информационной безопасности инфокоммуникаций»
2-я рубежная аттестация
Группа: _____ Семестр: _____
Билет №

1.Протоколы распределения секретных ключей. Основные цели протокола распределения ключей. Протокол Барроуза.
2.Сравнение блочных и поточных шифров. Методы организации процедуры исправления ошибок.

Преподаватель_____

Грозненский Государственный Нефтяной Технический Университет
им. акад. М.Д. Миллионщикова
Кафедра «Сети связи и системы коммутации»
Дисциплина «Криптографические методы защиты и средства обеспечения информационной безопасности инфокоммуникаций»
1-я рубежная аттестация
Группа: _____ Семестр: _____
Билет №

1. Квантовая криптография.
2. Криптосистема Рабина. Алгоритм. Шифрование. Дешифрование.

Преподаватель_____

Грозненский Государственный Нефтяной Технический Университет
им. акад. М.Д. Миллионщикова
Кафедра «Сети связи и системы коммутации»
Дисциплина «Криптографические методы защиты и средства обеспечения информационной безопасности инфокоммуникаций»
2-я рубежная аттестация

Группа: СК-19 **Семестр: 8 Группа: _____**

Семестр: _____

Билет №

1. Квантовая криптография
2. Криптосистема Рабина. Алгоритм. Шифрование. Дешифрование.

Преподаватель_____

7.2. Вопросы к зачету/ экзамену

7 семестр

Вопросы к зачету:

1. Алгоритм Эль Гамаль (асимметричная криптография).
2. Комбинирующий поточный шифр с элементом памяти.
3. Код аутентификации сообщения (MAC). Способы построения MAC. HMAC.
4. Динамический поточный шифр.
5. Определение блочного шифрования. Блок информации. Ключ алгоритма.
6. Абсолютно симметричный блочный шифр.
7. Аутентификация пользователя. Типы систем аутентификации (на симметричных и асимметричных криптосистемах, на сертификатах).
8. Обратимые операции в блочном шифровании.
9. Kerberos. Протокол распределения ключей.
10. Необратимые операции в блочном шифровании.
11. Распространение ключей. Протоколы, основанные на использовании симметричной
12. криптосистемы и случайных параметров.
13. Сети блочных шифров, ветви сети, раунд сети, образующая функция. SP-сеть,
14. KASLT-сеть.
15. Распространение ключей. 3-х этапный протокол Шамира (Shamir).
16. Классическая структура сети Фейстеля. Ветви сети, материал ключа, раунд сети, образующая функция.
17. Распространение ключей. Протокол Needham-Schroeder.
18. Абсолютно симметричная сеть Фейстеля. Модификация сети Фейстеля для
19. большего числа ветвей: тип 1 – размер блока, ветви сети, материал ключа, рунд сети, образующая функция.
20. Распространение ключей. Протоколы на основе асимметричных криптосистем.
21. Алгоритм RSA (асимметричная криптография).
22. Видовые демаскирующие признаки.
23. Сигнальные демаскирующие признаки.
24. Демаскирующие признаки веществ.
25. Состав и характеристики видовых, сигнальных признаков, признаков веществ.
26. Классификация демаскирующих признаков.

8 семестр

Вопросы к экзамену:

1. Основные понятия, обозначения и задачи криптографии.
2. Исторические примеры криптосистем.
3. Основные принципы криптографической защиты информации. Общая схема системы защиты информации.
4. Функции шифрования. Односторонние функции. Простейшие шифры и их клас-сификация.
5. Основные требования к шифрам, к криптографическим системам.
6. Абсолютно стойкие (совершенные) шифры. Криптостойкость алгоритма шифро-вания. Особенности симметричных криптосистем.
7. Метод простой подстановки (замены). Метод перестановки. Метод блочных шифров.
8. Метод гаммирования. Метод шифрования на основе теоремы Эйлера-Ферма.
9. Композиция шифров.
10. Стандарт криптосистемы США DES.
11. Стандарт криптосистемы России – ГОСТ 28147-89. Системы защиты с открытым ключом.
12. Криптосистема RSA.
13. Теоретико-числовые алгоритмы и их сложность. Методы дискретного логариф-мирования.
14. Система защиты Диффи-Хеллмана. Система защиты информации на основе за-данного рюкзака.
15. Протоколы распределения секретных ключей. Основные цели протокола распре-деления ключей. Протокол Отвэй-Риса.
16. Протоколы распределения секретных ключей. Основные цели протокола распре-деления ключей. Цербер.
17. Арифметика остатков. Сравнение по модулю. Решение уравнения $ax = b \pmod N$.
18. Функция Эйлера. Мультипликативные обратные по модулю N. Теорема Лагранжа. Малая теорема Ферма. Применение в криптографии.
19. Алгоритм Евклида. Китайская теорема об остатках. Расширенный алгоритм Евклида. Применение в криптографии.
20. Криптосистема с открытым ключом. Криптографическая односторонняя функция. Важнейшие криптографические односторонние функции.
21. Оценка сложности задач. Сложность алгоритма: Полиноминальная, экспоненци-альная, субэкспоненциальная Оракул. Сравнительный анализ сложности криптографических алгоритмов (без доказательства).
22. Алгоритм RSA. Шифрование в RSA. Дешифрование в RSA. Доказательство алго-ритма.
23. Алгоритм RSA. Задача криптоаналитика. Криптостойкость RSA
24. Криптосистема Эль-Гамаль. Параметры домена. Шифрование. Дешифрование.
25. Криптосистема Рабина. Алгоритм. Шифрование. Дешифрование.
26. Простые числа. Важность проблемы тестирования простых чисел. Пробное деле-ние.

27. Распределение ключей Диффи ? Хеллмана. Алгоритм. Стойкость. Атака человек посередине. Необходимость использования цифровой подписи.

28. Алгоритмом цифровой подписи RSA.

29. Криптографическая Хэш-функция. Свойства криптографической хэш-функции. Свойство односторонности Защищенность от повторений, защищенностью от вторых прообразов.

30. Алгоритмом цифровой подписи DSA.

31. Отечественный стандарт цифровой подписи ГОСТ Р 34.10-94.

32. Квантовая криптография.

Образец билета к зачету:

Грозненский Государственный Нефтяной Технический Университет
им. акад. М.Д. Миллионщикова
Кафедра «Сети связи и системы коммутации»
Дисциплина «Криптографические методы защиты и средства обеспечения информационной безопасности инфокоммуникаций»
Группа: _____ Семестр: _____
Билет №
1. Стандарт криптосистемы России – ГОСТ 28147-89. Системы защиты с открытым ключом.
2. Метод простой подстановки (замены).
Подпись преподавателя_____ Подпись заведующего кафедрой_____

Образец билета к экзамену:

Грозненский Государственный Нефтяной Технический Университет
им. акад. М.Д. Миллионщикова
Кафедра «Сети связи и системы коммутации»
Дисциплина «Криптографические методы защиты и средства обеспечения информационной безопасности инфокоммуникаций»
Группа: _____ Семестр: _____
Билет №
1.Протоколы распределения секретных ключей. Основные цели протокола распределения ключей. Протокол Отвэй-Риса.
2. Простые числа. Важность проблемы тестирования простых чисел. Пробное деление.
3. Квантовая криптография.

Подпись преподавателя_____ Подпись заведующего кафедрой_____

7.3. Текущий контроль

Образец типового задания для лабораторных занятий

Лабораторная работа

«Программная реализация криптографических протоколов»

Цель работы: получение студентами навыков работы с аппаратурой защиты речевой информации в телефонных линиях.

Краткие теоретические сведения:

7.4.Критерии оценивания текущей, рубежной и промежуточной аттестации

Наивысшая оценка лабораторной работы предусматривается в диапазоне от 2 до 5 баллов, в зависимости от сложности задания.

При оценке работы студента учитываются:

- уверенность действий при работе с изучаемым программным обеспечением;
- правильность выполнения необходимых шагов в лабораторной работе и адекватность / корректность полученного результата;
- умение самостоятельно находить способы решения возникающих проблем с помощью изучаемого программного обеспечения;
- способность ответить на вопросы преподавателя о последовательности выполненных шагов для получения результата.

При оценке работы студента на рубежной аттестации учитываются:

- правильность ответа на вопрос;
- логика изложения материала вопроса;
- выполнение практического задания.

7.5. Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкалы оценивания

Таблица 7

Планируемые результаты освоения компетенции	Критерии оценивания результатов обучения				Наименование оценочного средства
	менее 41 баллов (неудовлетворительно)	**41-60 баллов (удовлетворительно)**	**61-80 баллов (хорошо)**	**81-100 баллов (отлично)**	
ПК-3 Способен осуществлять монтаж, наладку, настройку, регулировку, опытную проверку работоспособности, испытания и сдачу в эксплуатацию сооружений, средств и оборудования сетей					
Знать: - основы сетевых технологий и принципы работы сетевого оборудования, правила работы с различными инфокоммуникационными	Фрагментарные знания	Неполные знания	Сформированные, но содержащие отдельные пробелы знания	Сформированные систематические знания	Комплект заданий для выполнения лабораторных работ, темы докладов с презентациями, вопросы по темам / разделам дисциплины
Уметь: - работать с различными инфокоммуникационными системами и базами данных, обрабатывать информацию о выполнения заявок на техподдержку оборудования с использованием современных технических средств	Частичные умения	Неполные умения	Умения полные, допускаются небольшие ошибки	Сформированные умения	
Владеть: - навыками выбора и использования соответствующего тестового и измерительного оборудования, использования программного обеспечения оборудования при его настройке	Частичное владение навыками	Несистематическое применение навыков	В систематическом применении навыков допускаются пробелы	Успешное и систематическое применение навыков	

8. Особенности реализации дисциплины для инвалидов и лиц с ограниченными возможностями здоровья

Для осуществления процедур текущего контроля успеваемости и промежуточной аттестации обучающихся созданы фонды оценочных средств, адаптированные для инвалидов и лиц с ограниченными возможностями здоровья и позволяющие оценить достижение ими запланированных в основной образовательной программе результатов обучения и уровень сформированности всех компетенций, заявленных в образовательной программе. Форма проведения текущей аттестации для студентов-инвалидов устанавливается с учетом индивидуальных психофизических особенностей (устно, письменно на бумаге, письменно на компьютере, в форме тестирования и т.п.). При тестировании для слабовидящих студентов используются фонды оценочных средств с укрупненным шрифтом. На экзамен приглашается сопровождающий, который обеспечивает техническое сопровождение студенту. При необходимости студенту-инвалиду предоставляется дополнительное время для подготовки ответа на экзамене (или зачете). Обучающиеся с ограниченными возможностями здоровья и обучающиеся инвалиды обеспечиваются печатными и электронными образовательными ресурсами (программы, учебные пособия для самостоятельной работы и т.д.) в формах, адаптированных к ограничениям их здоровья и восприятия информации:

1) для инвалидов и лиц с ограниченными возможностями здоровья **по зрению:**

- для слепых: задания для выполнения на семинарах и практических занятиях оформляются рельефно-точечным шрифтом Брайля или в виде электронного документа, доступного с помощью компьютера со специализированным программным обеспечением для слепых, либо зачитываются ассистентом; письменные задания выполняются на бумаге рельефно-точечным шрифтом Брайля или на компьютере со специализированным программным обеспечением для слепых либо надиктовываются ассистенту; обучающимся для выполнения задания при необходимости предоставляется комплект письменных принадлежностей и бумага для письма рельефно-точечным шрифтом Брайля, компьютер со специализированным программным обеспечением для слепых;

- для слабовидящих: обеспечивается индивидуальное равномерное освещение не менее 300 люкс; обучающимся для выполнения задания при необходимости предоставляется увеличивающее устройство; возможно также использование собственных увеличивающих устройств; задания для выполнения заданий оформляются увеличенным шрифтом;

2) для инвалидов и лиц с ограниченными возможностями здоровья **по слуху:**

- **для глухих и слабослышащих:** обеспечивается наличие звукоусиливающей аппаратуры коллективного пользования, при необходимости обучающимся предоставляется звукоусиливающая аппаратура индивидуального пользования; предоставляются услуги сурдопереводчика;

- **для слепоглухих** допускается присутствие ассистента, оказывающего услуги тифлосурдопереводчика (помимо требований, выполняемых соответственно для слепых и глухих);

3) для лиц с тяжелыми нарушениями речи, глухих, слабослышащих лекции и семинары, проводимые в устной форме, проводятся в письменной форме;

4) для инвалидов и лиц с ограниченными возможностями здоровья, **имеющих**

нарушения опорно-двигательного аппарата:

- для лиц с нарушениями опорно-двигательного аппарата, нарушениями двигательных функций верхних конечностей или отсутствием верхних конечностей: письменные задания выполняются на компьютере со специализированным программным обеспечением или надиктовываются ассистенту; выполнение заданий (тестов, контрольных работ), проводимые в письменной форме, проводятся в устной форме путем опроса, беседы с обучающимся.

9. Учебно-методическое и информационное обеспечение дисциплины

1. Рагозин Ю. Н. Инженерно-техническая защита информации: учебное пособие по физическим основам образования технических каналов утечки информации и по практикуму оценки их опасности / Ю. Н. Рагозин ; под редакцией Т. С. Кулакова. — Санкт-Петербург: Интермедия, 2018. — 168 c. — ISBN 978-5-4383-0161-5. — Текст: электронный // Электронно-библиотечная система IPR BOOKS: [сайт]. — URL: https://www.iprbookshop.ru/73641.html
2. Лабораторный практикум по дисциплине Программно-аппаратные средства защиты информации / составители И. А. Денисов. — Москва : Московский технический университет связи и информатики, 2016. — 31 с. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: https://www.iprbookshop.ru/61529.html
3. Учебно-методическое пособие по выполнению лабораторных работ по дисциплине Технологии программной защиты информации в интернете / составители А. Г. Симонян, В. В. Барков. — Москва : Московский технический университет связи и информатики, 2016. — 54 с. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: https://www.iprbookshop.ru/61565.html.

10.Материально-техническое обеспечение дисциплины

10.1. Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине

Перечень материально-технических средств учебной аудитории для проведения занятий по дисциплине:

- учебная аудитория, доска;
- стационарные компьютеры;
- мультимедийный проектор;
- настенный экран.

10.2. Помещения для самостоятельной работы

Учебная аудитория для самостоятельной работы – 2-23.

Методические указания по освоению дисциплины
«Криптографические методы защиты и средства обеспечения информационной безопасности инфокоммуникаций»

1. Методические указания для обучающихся по планированию и организации времени, необходимого для освоения дисциплины

Изучение рекомендуется начать с ознакомления с рабочей программой дисциплины, ее структурой и содержанием разделов (модулей), фондом оценочных средств, ознакомиться с учебно-методическим и информационным обеспечением дисциплины.

Дисциплина «Криптографические методы защиты и средства обеспечения

информационной безопасности инфокоммуникаций» состоит из девяти связанных между собой разделов, обеспечивающих последовательное изучение материала.

Обучение по дисциплине «Криптографические методы защиты и средства обеспечения

информационной безопасности инфокоммуникаций» осуществляется в следующих формах:

1. Аудиторные занятия (лекции, лабораторные занятия).
2. Самостоятельная работа студента (подготовка к лекциям, лабораторным занятиям, доклады с презентациями, индивидуальная консультация с преподавателем).

Учебный материал структурирован и изучение дисциплины производится в тематической последовательности. Каждому лабораторному занятию и самостоятельному изучению материала предшествует лекция по данной теме. Обучающиеся самостоятельно проводят предварительную подготовку к занятию, принимают активное и творческое участие в обсуждении теоретических вопросов, разборе проблемных ситуаций и поисков путей их решения.

Описание последовательности действий обучающегося:

При изучении курса следует внимательно слушать и конспектировать материал, излагаемый на аудиторных занятиях. Для его понимания и качественного усвоения рекомендуется следующая последовательность действий:

1. После окончания учебных занятий для закрепления материала просмотреть и обдумать текст лекции, прослушанной сегодня, разобрать рассмотренные примеры (10-15 минут).
2. При подготовке к лекции следующего дня повторить текст предыдущей лекции, подумать о том, какая может быть следующая тема (10-15 минут).
3. В течение недели выбрать время для работы с литературой в электронной библиотечной системе (по 1 часу).

4. При подготовке к лабораторному занятию повторить основные понятия по теме, изучить примеры. Решая конкретную ситуацию, – предварительно понять, какой теоретический материал нужно использовать. Наметить план решения, попробовать на его основе решить 1-2 задачи.

2. Методические указания по работе обучающихся во время проведения лекций

Лекции дают обучающимся систематизированные знания по дисциплине, концентрируют их внимание на наиболее сложных и важных вопросах. Лекции обычно

излагаются в традиционном или в проблемном стиле. Для студентов в большинстве случаев в проблемном стиле. Проблемный стиль позволяет стимулировать активную познавательную деятельность обучающихся и их интерес к дисциплине, формировать творческое мышление, прибегать к противопоставлениям и сравнениям, делать обобщения, активизировать внимание обучающихся путем постановки проблемных вопросов, поощрять дискуссию.

Во время лекционных занятий рекомендуется вести конспектирование учебного материала, обращать внимание на формулировки и категории, раскрывающие суть того или иного явления, выводы и практические рекомендации.

Конспект лекции лучше подразделять на пункты, соблюдая красную строку. Этому в большой степени будут способствовать вопросы плана лекции, предложенные преподавателям. Следует обращать внимание на акценты, выводы, которые делает преподаватель, отмечая наиболее важные моменты в лекционном материале замечаниями «важно», «хорошо запомнить» и т.п. Можно делать это и с помощью разноцветных маркеров или ручек, подчеркивая термины и определения.

Целесообразно разработать собственную систему сокращений, аббревиатур и символов. Однако при дальнейшей работе с конспектом символы лучше заменить обычными словами для быстрого зрительного восприятия текста.

Работая над конспектом лекций, необходимо использовать не только основную литературу, но и ту литературу, которую дополнительно рекомендовал преподаватель. Именно такая серьезная, кропотливая работа с лекционным материалом позволит глубоко овладеть теоретическим материалом.

Тематика лекций дается в рабочей программе дисциплины.

3. Методические указания обучающимся по подготовке к лабораторным занятиям

На лабораторных занятиях приветствуется активное участие в обсуждении конкретных ситуаций, способность на основе полученных знаний находить наиболее эффективные решения поставленных проблем, уметь находить полезный дополнительный материал по тематике занятий.

Студенту рекомендуется следующая схема подготовки к лабораторному занятию:

1. Ознакомиться с планом занятия, который отражает содержание предложенной темы.
2. Проработать конспект лекций.
3. Прочитать основную и дополнительную литературу.

В процессе подготовки к лабораторным занятиям, необходимо обратить особое внимание на самостоятельное изучение рекомендованной литературы. При всей полноте конспектирования лекции в ней невозможно изложить весь материал из-за лимита аудиторных часов. Поэтому самостоятельная работа с учебниками, учебными пособиями, научной, справочной литературой, материалами периодических изданий и Интернета является наиболее эффективным методом получения дополнительных знаний, позволяет значительно активизировать процесс овладения информацией, способствует более глубокому усвоению изучаемого материала, формирует у студентов отношение к конкретной проблеме. Все новые понятия по изучаемой теме необходимо выучить наизусть и внести в глоссарий, который целесообразно вести с самого начала изучения курса.

1. Ответить на вопросы плана лабораторного занятия.

2. Выполнить домашнее задание.

3. При затруднениях сформулировать вопросы к преподавателю.

Результат такой работы должен проявиться в способности студента свободно ответить на теоретические вопросы, выступать и участвовать в коллективном обсуждении вопросов изучаемой темы, правильно выполнять практические задания, которые даются в фонде оценочных средств дисциплины.

4. Методические указания обучающимся по организации самостоятельной работы

Цель организации самостоятельной работы по дисциплине «Основы организации научных исследований» – это углубление и расширение знаний в области научной исследовательской деятельности; формирование навыка и интереса к самостоятельной познавательной деятельности.

Самостоятельная работа обучающихся является важнейшим видом освоения содержания дисциплины, подготовки к практическим занятиям и к контрольной работе. Сюда же относятся и самостоятельное углубленное изучение тем дисциплины. Самостоятельная работа представляет собой постоянно действующую систему, основу образовательного процесса и носит исследовательский характер, что послужит в будущем основанием для написания выпускной квалификационной работы, практического применения полученных знаний.

Организация самостоятельной работы обучающихся ориентируется на активные методы овладения знаниями, развитие творческих способностей, переход от поточного к индивидуализированному обучению, с учетом потребностей и возможностей личности.

Правильная организация самостоятельных учебных занятий, их систематичность, целесообразное планирование рабочего времени позволяет студентам развивать умения и навыки в усвоении и систематизации приобретаемых знаний, обеспечивать высокий уровень успеваемости в период обучения, получить навыки повышения профессионального уровня.

Подготовка к лабораторному занятию включает, кроме проработки конспекта и презентации лекции, поиск литературы (по рекомендованным спискам и самостоятельно), подготовку заготовок для выступлений по вопросам, выносимым для обсуждения по конкретной теме. Такие заготовки могут включать цитаты, факты, сопоставление различных позиций, собственные мысли. Если проблема заинтересовала обучающегося, он может подготовить реферат и выступить с ним на практическом занятии. Лабораторное занятие – это, прежде всего, дискуссия, обсуждение конкретной ситуации, то есть предполагает умение внимательно слушать членов малой группы и модератора, а также стараться высказать свое мнение, высказывать собственные идеи и предложения, уточнять и задавать вопросы коллегам по обсуждению.

При подготовке к контрольной работе (рубежной аттестации) обучающийся должен повторять пройденный материал в строгом соответствии с учебной программой, используя конспект лекций и литературу, рекомендованную преподавателем. При необходимости можно обратиться за консультацией и методической помощью к преподавателю.

Самостоятельная работа реализуется:

– непосредственно в процессе аудиторных занятий – на лекциях, лабораторных занятиях;

– в контакте с преподавателем вне рамок расписания – на консультациях по учебным вопросам, в ходе творческих контактов, при ликвидации задолженностей, при выполнении индивидуальных заданий и т.д.

– в библиотеке, дома, на кафедре при выполнении обучающимся учебных и практических задач.

Виды СРС и критерии оценок

(по балльно-рейтинговой системе ГГНТУ, СРС оценивается в 15 баллов)

1. Доклад с презентацией
2. Подготовка к лабораторным занятиям

Темы для самостоятельной работы прописаны в рабочей программе дисциплины. Эффективным средством осуществления обучающимся самостоятельной работы является электронная информационно-образовательная среда университета, которая обеспечивает доступ к учебным планам, рабочим программам дисциплин (модулей), лабораторных, к изданиям электронных библиотечных систем.

Составитель:

Старший преподаватель кафедры
«Сети связи и системы коммутации»  / Доудов Х.А. /

СОГЛАСОВАНО:

И.о. зав. выпускающей кафедры
«Сети связи и системы коммутации»  / Пашаев М.Я. /

Директор ДУМР  / Магомаева М.А. /