МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГРОЗНЕНСКИЙ ГОСУДАРСТВЕННЫЙ НЕФТЯНОЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ

имени академика М. Д. Миллионщикова

«УТВЕРЖДАЮ»
Первый проректор
И.Г.Гайрабеков
«01» 09 2023г.

РАБОЧАЯ ПРОГРАММА

дисциплины

«Криптографические методы защиты и средства обеспечения информационной безопасности инфокоммуникаций»

Направления подготовки

11.03.02 *Инфокоммуникационные технологии и системы связи*

Направленность (профиль)

«Инфокоммуникационные технологии и системы связи»

Квалификация

бакалавр

Год начала подготовки - 2023

Грозный – 2023

1. Цели и задачи дисциплины

Целями освоения учебной дисциплины является изучение методов и средств построения и эксплуатации программно-аппаратных технологий для обеспечения информационной безопасности на объекте, а также изучение основных подходов разработки, реализации, эксплуатации, анализу, сопровождению и совершенствованию технологий защиты передачи информации.

Приобретенные знания позволят студентам основывать свою профессиональную деятельность на построении, проектировании и эксплуатации программно-аппаратных технологий защиты передачи информации.

Задачами дисциплины являются:

- обучение студентов систематизированным представлениям о принципах построения, функционирования и применения аппаратных средств современной вычислительной техники;
- изложение основных теоретических концепций, положенных в основу построения современных компьютеров, вычислительных систем, сетей и телекоммуникаций;
- обучение основам защиты информации аппаратными и техническими средствами.
- изучение основ комплексного обеспечения защиты информации и информационной безопасности;
- изучение основ организационно-правового обеспечения защиты информации и информационной безопасности;
- изучение стандартов информационной безопасности.

2. Место дисциплины в структуре образовательной программы

Учебная дисциплина «Криптографические методы защиты и средства обеспечения информационной безопасности инфокоммуникаций» относится к дисциплинам по выбору ФГОС ВО по направлению подготовки 11.03.02 Инфокоммуникационные технологии и системы связи.

Предшествующие дисциплины, освоение которых необходимо для изучения данной дисциплины:

- Информационные системы и технологии;
- Теории передачи сигналов;
- Основы построения инфокоммуникационных систем и сетей;
- Компоненты электронной техники.

Помимо самостоятельного значения, данная дисциплина является предшествующей для дисциплин:

- Технология сетей абонентского доступа;
- Сети связи;
- Проектирование защищенных инфокоммуникационных систем.

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

Таблица 1

Код по ОП	**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. **ПК-9.3.** Устанавливает дополнительные программные продукты для обеспечения безопасности удаленного доступа и их параметризация.	**Знать:** - основные понятия информационной безопасности; - принципы, методы и средства решения стандартных задач информационной безопасности; - правовые нормы необходимые для осуществления профессиональной деятельности; - знать стандарты информационной безопасности; - знать программные и аппаратные механизмы защиты сетей; - знать криптографические методы защиты сетей. **Уметь:** - проводить анализ и оценку уязвимостей компьютерной системы; - применять меры информационной безопасности процедурного уровня; - осуществлять защиту информации от несанкционированного доступа; - настраивать безопасность почтового клиента; - настраивать параметры аутентификации пользователей; - осуществлять регистрацию и аудит информационной безопасности; - настраивать системы разграничения доступа; - применять

		криптографические методы и средства зашиты информации; - использовать средства антивирусной защиты; - использовать стандарты и спецификации информационной безопасности. **Владеть:** методами и средствами технической защиты информации; методами расчета и инструментального контроля показателей технической защиты информации

4. Объем дисциплины и виды учебной работы

Таблица 2

Вид учебной работы	**Всего часов/ зач.ед.**			
	ОФО	**ОФО**	**ЗФО**	**ЗФО**
	6 семестр	**7 семестр**	**6 семестр**	**7 семестр**
Аудиторные занятия (всего)	**132/3,6**		**32/0,9**	
В том числе:				
Лекции	32/0,9	34/0,9	8/0,22	8/0,22
Практические занятия				
Семинары				
Лабораторные работы	32/0,9	34/0,9	8/0,22	8/0,22
Самостоятельная работа (всего)	**156/4,4**		**256/7,1**	
В том числе:				
Доклады	39/1,1		64/1,8	
Презентации	39/1,1		64/1,8	
И (или) другие виды самостоятельной работы:				
Подготовка к лабораторным работам	39/1,1		64/1,8	
Подготовка к экзамену	39/1,1		64/1,8	
Вид отчетности	**зачет**	**зкзамен**	**зачет**	**зкзамен**
Общая трудоемкость дисциплины	**288**		**288**	
	8		**8**	

5. Содержание дисциплины

5.1. Разделы дисциплины и виды занятий

Таблица 3

№ п/п	Наименование раздела дисциплины по семестрам	Лекц. зан. часы		Лаб. зан. часы		Всего часов	
		ОФО	ЗФО	ОФО	ЗФО	ОФО	ЗФО
6-7семестр ОФО; 6-7 семестр ЗФО							
1.	Основные понятия и анализ угроз информационной безопасности: политика безопасности	17	4	17	4	34	8
2.	Стандарты и спецификации в области информационной безопасности	17	4	17	4	34	8
3.	Угроза вредоносных программ и защита от них	16	4	16	4	32	8
4.	Безопасность вычислительных сетей	16	4	16	4	32	8

5.2. Лекционные занятия

Таблица 4

№ п/п	Наименование раздела дисциплины	Содержание раздела
6-7 семестр ОФО; 6-7 семестр ЗФО		
1.	Основные понятия и анализ угроз информационной безопасности: политика безопасности	Понятие «Информационная безопасность». Составляющие информационной безопасности. Классификация угроз «информационной безопасности». Система формирования режима информационной безопасности. Административный уровень обеспечения информационной безопасности. Нормативно-правовые основы информационной безопасности в РФ.
2.	Стандарты и спецификации в области информационной безопасности	Стандарты информационной безопасности: «Общие критерии». Стандарты информационной безопасности распределенных систем. Стандарты информационной безопасности в РФ.
3.	Угроза вредоносных программ и защита от них	Вирусы как угроза информационной безопасности. Классификация компьютерных вирусов. Характеристика «вирусоподобных» программ. Антивирусные программы. Профилактика компьютерных вирусов. Обнаружение неизвестного вируса.

4.	Безопасность вычислительных сетей	Информационная безопасность вычислительных сетей. Механизмы обеспечения «информационной безопасности». Межсетевые экраны.

5.3. Лабораторный практикум

Таблица 5

№ п/п	Наименование раздела дисциплины	Наименование лабораторных работ
6-7 семестр ОФО; 6-7 семестр ЗФО		
1.	Основные понятия и анализ угроз информационной безопасности: политика безопасности	**Лабораторная работа №1.** Разграничение прав пользователей
2.	Основные понятия и анализ угроз информационной безопасности: политика безопасности	**Лабораторная работа №2.** Реализация политики безопасности в защищенных версиях операционной системы Windows
3.	Стандарты и спецификации в области информационной безопасности	**Лабораторная работа №3.** Разграничение доступа к ресурсам в защищенных версиях операционной системы Windows
4.	Безопасность вычислительных сетей	**Лабораторная работа №4.** Использование программных средств контроля и анализа выполнения политики безопасности на примере операционной системы Windows XP/7
5.	Угроза вредоносных программ и защита от них	**Лабораторная работа №5.** Использование программного продукта Acronis. Восстановление данных. Создание резервной копии пространства памяти
6.	Угроза вредоносных программ и защита от них	**Лабораторная работа №6.** Использование программного продукта Acronis. Восстановление данных. Создание резервной копии пространства памяти

5.4. Практические занятия (семинары): планом не предусмотрены

6. Самостоятельная работа студентов по дисциплине

6.1. Тематика и формы самостоятельной работы студентов

Подготовить доклад и презентацию по выбранной теме в области информационной безопасности (российский, зарубежный). Примерный перечень тем докладов:

1. ГОСТ Р ИСО/МЭК 15408 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий» Части 1, 2, 3

2. Анализ методов повышения надежности хранения информации на жестких магнитных дисках

3. Анализ средств защиты от спама

4. Анализ методов обеспечения безопасности домашней сети

5. Анализ методов изучения поведения нарушителей безопасности компьютерных систем

6. Анализ методов перехвата паролей пользователей компьютерных систем и методов противодействия им

7. Сравнительный анализ антивирусных пакетов

8. Анализ методов обеспечения безопасности электронного магазина

9. Анализ методов организации антивирусной защиты компьютерных систем

10. Сравнительный анализ систем обнаружения атак

11. Анализ средств безопасности в пакете Microsoft Office

12. ГОСТ Р ИСО/МЭК ТО 15446 «Информационная технология. Методы и средства обеспечения безопасности. Руководство по разработке профилей защиты и заданий по безопасности»

13. Сравнительный анализ средств защиты электронной почты

14. ГОСТ Р ИСО/МЭК ТО 19791 «Информационная технология. Методы и средства обеспечения безопасности. Оценка безопасности автоматизированных систем».

6.2. Учебно-методическое обеспечение для самостоятельной работы студентов:

1. Мельников, В.П. Информационная безопасность и защита информации: учеб. пособие для студ. высших учебных заведений [Текст] / В.П. Мельников, С.А. Клейменов, А.М, Петраков; под ред. С.А. Клейменова – М.: Издательский центр «Академия», 2008. – 336 с. *(www.library-it.ru)*

2. Шаньгин, В.Ф. Информационная безопасность компьютерных систем и сетей: учеб. пособие [Текст] / В.Ф. Шаньгин. - М.: ИД «ФОРУМ»: ИНФРА-М, 2008. - 416 с.: ил. *(библиотека ГГНТУ)*

7. Фонды оценочных средств

7.1. Вопросы к рубежным аттестациям

***Вопросы к 1 рубежной аттестации**:*

1. Основные понятия защиты информации и информационной безопасности
2. Базовые свойства информации применительно к ИБ
3. Идентификация, аутентификация, авторизация
4. Анализ угроз ИБ
5. Признаки классификации угроз
6. НСД к информации. Способы получения НСД
7. Общие критерии безопасности
8. Концепции общих критериев
9. Политика безопасности организации
10. Распределение ролей и обязанностей администраторов и пользователей сети
11. Структура политики безопасности
12. Уровни политики безопасности

13. Процедуры безопасности

Вопросы ко 2 рубежной аттестации:

1. Основные понятия криптографической защиты информации
2. Симметричные криптосистемы шифрования
3. Ассиметричные криптосистемы шифрования
4. Электронная цифровая подпись и функция хэширования
5. Аутентификация, авторизация и администрирование действий пользователей
6. Аутентификация на основе паролей
7. Угрозы безопасности ОС
8. Понятие защищенной ОС
9. Основные функции подсистемы защиты ОС
10. Разграничение доступа к объектам ОС
11. Аудит
12. Технология межсетевых экранов
13. Функции МЭ
14. Дополнительные возможности МЭ
15. Проблемы безопасности МЭ.

Образцы билетов рубежной аттестации:

МИНИСТЕРСТВО НАУКИ И ВАЫСШЕГО ОБРАЗОВАНИЯ РФ
Грозненский Государственный Нефтяной Технический Университет
им. акад. М.Д. Миллионщикова
Кафедра «Информационные технологии»
Дисциплина «Криптографические методы защиты и средства обеспечения информационной безопасности инфокоммуникаций»
1-я рубежная аттестация
Группа: **Семестр:**

Билет 1

1. Основные понятия защиты информации и информационной безопасности.
2. Разграничение доступа к объектам ОС.

Преподаватель_____Усамов И.Р.

МИНИСТЕРСТВО НАУКИ И ВАЫСШЕГО ОБРАЗОВАНИЯ РФ
Грозненский Государственный Нефтяной Технический Университет
им. акад. М.Д. Миллионщикова
Кафедра «Информационные технологии»
Дисциплина «Криптографические методы защиты и средства обеспечения информационной безопасности инфокоммуникаций»
2-я рубежная аттестация
Группа: **Семестр:**

Билет 1

1. Аутентификация на основе паролей
2. Функции МЭ.

Преподаватель_____Усамов И.Р.

7.2. Вопросы к зачету / экзамену

Вопросы к зачету:

1. Основные понятия защиты информации и информационной безопасности
2. Базовые свойства информации применительно к ИБ
3. Идентификация, аутентификация, авторизация
4. Анализ угроз ИБ
5. Признаки классификации угроз
6. НСД к информации. Способы получения НСД
7. Общие критерии безопасности
8. Концепции общих критериев
9. Политика безопасности организации
10. Распределение ролей и обязанностей администраторов и пользователей сети
11. Структура политики безопасности
12. Уровни политики безопасности
13. Процедуры безопасности
14. Основные понятия криптографической защиты информации
15. Симметричные криптосистемы шифрования
16. Ассиметричные криптосистемы шифрования
17. Электронная цифровая подпись и функция хэширования
18. Аутентификация, авторизация и администрирование действий пользователей
19. Аутентификация на основе многоразовых паролей
20. Аутентификация на основе одноразовых паролей
21. Аутентификация на основе PIN-кода
22. Угрозы безопасности ОС
23. Понятие защищенной ОС
24. Основные функции подсистемы защиты ОС
25. Разграничение доступа к объектам ОС
26. Аудит
27. Технология межсетевых экранов
28. Функции МЭ
29. Дополнительные возможности МЭ

Образец билета к зачету:

МИНИСТЕРСТВО НАУКИ И ВАЫСШЕГО ОБРАЗОВАНИЯ РФ
Грозненский Государственный Нефтяной Технический Университет
им. акад. М.Д. Миллионщикова
Кафедра «Информационные технологии»
Дисциплина «Криптографические методы защиты и средства обеспечения информационной безопасности инфокоммуникаций»
Группа: **Семестр:**

Билет 1

1. Основные понятия защиты информации и информационной безопасности
2. Разграничение доступа к объектам ОС.

Преподаватель_____**Усамов И.Р.**
Зав. кафедрой_____**Моисеенко Н.А.**

7.3. Текущий контроль

Образец типового задания для лабораторных занятий

Лабораторная работа 1. Защита информации в КИС (4 часа)

Цель работы, сделать обзор существующих методов и средств защиты информации в корпоративных информационных системах, используя информационные ресурсы сети Internet.

Задание

a. Проанализировать средства антивирусной защиты и описать конфигурацию антивирусного пакета.

b. Описать:

- классификацию вирусов и средств защиты;
- виды антивирусных программных продуктов;
- характеристики наиболее популярных антивирусных пакетов.

Методические указания по выполнению задания

1. Определите на вашем рабочем месте установленный антивирусный пакет. Просмотрите его настройки и опишите его конфигурацию (используйте экранные копии изображений).
2. Загрузите браузер для работы в сети Internet (например, InternetExplorer, Opera).
3. В адресной строке наберите адрес любой поисковой системы (например, www.yandex.ru, www.google.ru, www.poisk.com).
4. В поисковую строку введите ключевые слова для поиска.
5. Поочередно нажимая на ссылки из полученного списка ресурсов, найдите нужную информацию.
6. Используя буфер обмена, скопируйте информацию в текстовый редактор MSWord.
7. Систематизируйте полученную информацию и подготовьте отчет по лабораторной работе.

Контрольные вопросы

1. Информационная безопасность.
2. Угроза информационной безопасности.
3. Подходы к классификации угроз информационной безопасности.
4. Способы воздействия угроз на объекты информационной безопасности.
5. Политика безопасности.
6. Методы обеспечения безопасности.
7. Средства обеспечения безопасности.
8. Средства анализа защищенности.
9. Системы обнаружения атак.
10. Правовое обеспечение безопасности информационных систем.

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

Таблица 6

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-9. Способен к администрированию средств обеспечения безопасности удаленного доступа (операционных систем и специализированных протоколов)					
Знать: основные понятия информационной безопасности; принципы, методы и средства решения стандартных задач информационной безопасности; правовые нормы необходимые для осуществления профессиональной деятельности; знать стандарты информационной безопасности; знать программные и аппаратные механизмы защиты сетей; знать криптографические методы защиты сетей.	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: проводить анализ и оценку уязвимостей компьютерной системы; применять меры информационной безопасности процедурного уровня; осуществлять защиту информации от несанкционированного доступа; настраивать системы разграничения доступа; применять криптографические методы и средства зашиты информации; использовать средства антивирусной защиты; использовать стандарты и спецификации информационной безопасности.	Частичные умения	Неполные умения	Умения полные, допускаются небольшие ошибки	Сформированные умения	

Владеть: методами и средствами технической защиты информации; методами расчета и инструментального контроля показателей технической защиты информации	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. Малюк, А.А. Введение в информационную безопасность. Учебное пособие для вузов [Текст] / А.А. Малюк, В.И. Королев, В.М. Фомичев; Под ред. В.С. Горбатов. – М.: Горячая линия-Телеком, 2014. – 290 с.: ил. (библиотека ГГНТУ)

2. Мельников, В.П. Информационная безопасность и защита информации: учеб. пособие для студ. высших учебных заведений [Текст] / В.П. Мельников, С.А. Клейменов, А.М, Петраков; под ред. С.А. Клейменова - М.: Издательский центр «Академия», 2008. – 336 с. (библиотека ГГНТУ)

3. Шаньгин, В.Ф. Информационная безопасность компьютерных систем и сетей. Учебное пособие [Текст] / В.Ф. Шаньгин. – М.: ИД «ФОРУМ»: ИНФРА-М, 2008. – 416 с.: ил. (библиотека ГГНТУ)

4. Грибунин, В.Г. Комплексная система защиты информации на предприятии. Учебное пособие [Текст] / В.Г. Грибунин, В.В. Чудовский - М.: Издательский центр «Академия», 2009. - 416 с. (библиотека ГГНТУ)

5. Стрельцов, А.А. Организационно-правовое обеспечение информационной безопасности. Учебное пособие для вузов [Текст] / А.А. Стрельцов, В.С. Горбатов, Т.А.Полякова, Т.А. Кондратьева, О. В. Дамаскин, Е. Б. Белов, С. Ю. Савин - М.: Академия, 2008. - 256 с. (библиотека ГГНТУ)

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;
- мультимедийный проектор;
- настенный экран;

10.2. Помещения для самостоятельной работы

Учебная аудитория для самостоятельной работы – 4-06.

Методические указания по освоению дисциплины «Безопасность информационных технологий и систем»

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 4 связанных между собою 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, докладам и иным формам письменных работ, индивидуальная консультация с преподавателем).
3. Интерактивные формы проведения занятий (коллоквиум, лекция-дискуссия и др.формы).

Учебный материал структурирован и изучение дисциплины производится в тематической последовательности. Каждой лабораторно работе 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. Многие проблемы, изучаемые в курсе, носят дискуссионный характер, что предполагает интерактивный характер проведения занятий на конкретных примерах.

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 библиотеке (по 1 часу).

4. При подготовке к лабораторному занятию 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 практические ситуации (лаб.работы).

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.

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 практическим/семинарским 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 семинарских занятий.

Студенту рекомендуется следующая схема подготовки к семинарскому занятию:

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

В процессе подготовки к практическим 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;

4. Ответить на вопросы плана лабораторного занятия;
5. Выполнить домашнее задание;
6. Проработать тестовые задания и задачи;
7. При затруднениях сформулировать вопросы к преподавателю.

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

3. Методические указания обучающимся по организации самостоятельной работы.

Цель организации самостоятельной работы по дисциплине «Криптографические методы защиты и средства обеспечения информационной безопасности инфокоммуникаций» - это углубление и расширение знаний в безопасность информационных технологий и систем, 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.

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)

Доклад

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), практик, к изданиям электронных библиотечных систем.

Составитель:
Старший преподаватель кафедры
«Информационные технологии» / Усамов И.Р. /

Согласовано:
Зав. выпускающей кафедры
«Информационные технологии» / Моисеенко Н.А./

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

Директор ДУМР / Магомаева М.А. /