МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГРОЗНЕНСКИЙ ГОСУДАРСТВЕННЫЙ НЕФТЯНОЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ

имени академика М. Д. Миллионщикова

«УТВЕРЖДАЮ»
Первый проректор
[illegible]
_____
«22»_____ 2023 г.

РАБОЧАЯ ПРОГРАММА

дисциплины

«Методы и средства защиты компьютерной информации»

Направления подготовки

09.03.04 *Программная инженерия*

Направленность (профиль)

«Программная инженерия»

Квалификация

бакалавр

Год начала подготовки - 2024

Грозный – 2023

1. Цели и задачи дисциплины

Целью преподавания дисциплины является ознакомление с организационными, техническими, алгоритмическими и другими методами и средствами защиты компьютерной информации, с законодательством и стандартами в этой области, с современными криптосистемами.

Задачи изучения дисциплины:

1. Сформировать взгляд на криптографию и защиту информации как на систематическую научно-практическую деятельность, носящую прикладной характер.

2. Сформировать базовые теоретические понятия (возможно, на элементарном уровне), лежащие в основе процесса защиты информации.

3. Дать представление о роли компьютера, как о центральном месте в области криптографии, взявшем на себя большинство функций традиционной компьютерной деятельности, включающей реализацию криптографических алгоритмов, проверку их качества, генерацию и распределение ключей, автоматизацию работы по анализу перехвата и раскрытию шифров.

4. Научить использованию криптографических алгоритмов в широко распространенных программных продуктах.

2. Место дисциплины в структуре образовательной программы

Учебная дисциплина «Методы и средства защиты компьютерной информации» относится к части, формируемая участниками образовательных отношений профессионального цикла ФГОС ВО по направлению подготовки 09.03.04 Программная инженерия.

Предшествующие дисциплины, освоение которых необходимо для изучения данной дисциплины:

- Безопасность информационных технологий и систем;
- Операционные системы и среды;
- Современные информационные технологии;
- Основы программной инженерии.

Помимо самостоятельного значения, данная дисциплина является предшествующей для дисциплин:

- Преддипломная практика (Научно-исследовательская работа);
- Анализ больших данных;
- Выполнение и защита выпускной квалификационной работы.

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-4. Способен выполнять концептуально-логическое проектирование системы и	**ПК 4.1.** Выявляет требования к Системе и проектные решения по Системе **ПК 4.2.** Выполняет обследования текущей	**Знать:** - правовые основы защиты компьютерной информации, математические основы криптографии, организационные, технические и программные методы

сопровождать разработанные проектные решения	ситуации **ПК 4.3.** Умеет проводить концептуально-логическое проектирование системы **ПК 4.4.** Участвует в разработке технического задания на систему	защиты информации в современных компьютерных системах и сетях, стандарты. **Уметь:** - применять известные методы и средства поддержки информационной безопасности в компьютерных системах. **Владеть:** - методами и средствами технической защиты информации; методами расчета и инструментального контроля показателей технической защиты информации
ПК-6. Способен создавать информационные технологии нового поколения.	**ПК 6.1.** Умеет выявлять, формировать и согласовывать требования к результатам аналитических работ с применением технологий больших данных. **ПК 6.2.** Умеет планировать и организовывать аналитические работы с использованием технологий больших данных. **ПК 6.3.** Умеет подготавливать данные для проведения аналитических работ по исследованию больших данных.	**Знать:** **-** методы шифрования, методы идентификации пользователей, методы защиты программ от вирусов, основы инфраструктуры систем, построенных с с использованием публичных и секретных ключей. **Уметь:** **-** проводить сравнительный анализ, выбирать методы и средства, оценивать уровень защиты информационных ресурсов в прикладных системах. **Владеть:** - навыками проведения сравнительного анализа, выбора методов и средств разработки безопасной системы.

4. Объем дисциплины и виды учебной работы

Таблица 2

Вид учебной работы	**Всего часов/ зач.ед.**
	ОФО
	8 семестр
Аудиторные занятия (всего)	**48/1,33**
В том числе:	
Лекции	16/0,44
Практические занятия	
Семинары	
Лабораторные работы	32/0,87
Самостоятельная работа (всего)	**96/2,67**
В том числе:	
Доклады	24/0,67
Презентации	24/0,67

И (или) другие виды самостоятельной работы:	
Подготовка к лабораторным работам	24/0,67
Подготовка к зачету	24/0,67
Вид отчетности	**зачет**
Общая трудоемкость дисциплины	**144**
	4

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	ОФО	ОФО
8 семестр ОФО				
1.	Законодательные аспекты информационных технологий	6		6
2.	Криптографические методы защиты	6	24	30
3.	Безопасность современных сетевых технологий	6		6
4.	Методы и средства встраивания скрытой служебной информации для управления правами доступа к информационным ресурсам.	6		6

5.2. Лекционные занятия

Таблица 4

№ п/п	Наименование раздела дисциплины	Содержание раздела
6 семестр ОФО; 6 семестр ЗФО		
1.	Законодательные аспекты информационных технологий	Законодательство Российской Федерации в области информационной безопасности. Информация как объект юридической и физической защиты. Государственные информационные ресурсы. Защита государственной тайны как особого вида защищаемой информации. Защита конфиденциальной информации, в том числе интеллектуальной собственности и коммерческой тайны. Нормативно-правовая база защиты компьютерных сетей от несанкционированного доступа. Компьютерные преступления и особенности их расследования.

2.	Криптографические методы защиты	Основные понятия и определения. Понятие криптографического протокола. Основные типы протоколов. Классы преобразований: подстановки, перестановки, гаммирование, блочные шифры. Датчики ПСЧ. Симметричная криптография. Асимметричная криптография. Цифровой дайджест и хэш-функция. Подстановочные и перестановочные шифры. Шифры Цезаря, Виженера, Вернома. Исследования Шеннона в области криптографии. Нераскрываемость шифра Вернома.
3.	Безопасность современных сетевых технологий	Способы несанкционированного доступа к информации в компьютерных сетях. Классификация способов несанкционированного доступа и жизненный цикл атак. Способы противодействия несанкционированному межсетевому доступу. Функции межсетевого экранирования. Особенности межсетевого экранирования на различных уровнях модели OSI. Режим функционирования межсетевых экранов и их основные компоненты. Маршрутизаторы. Шлюзы сетевого уровня. Основные схемы сетевой защиты на базе межсетевых экранов. Применение межсетевых экранов для организации виртуальных корпоративных сетей. Критерии оценки межсетевых экранов. Построение защищенных виртуальных сетей. Способы создания защищенных виртуальных каналов. Обзор протоколов.
4.	Методы и средства встраивания скрытой служебной информации для управления правами доступа к информационным ресурсам.	Понятие стеганографии. Задача встраивания скрытой служебной информации (цифровых водяных знаков) в аудио и видеосигналы. Основные методы и алгоритмы встраивания и обнаружения водяных знаков. Встраивание водяных знаков и сжатие информации Виды атак на информационные ресурсы, содержащие водяные знаки.

5.3. Лабораторный практикум

Таблица 5

№ п/п	**Наименование раздела дисциплины**	**Наименование лабораторных работ**
8 семестр		

1.	Криптографические методы защиты	**Лабораторная работа №1.** Простые шифры. Разработка и анализ простых криптографических алгоритмов на основе методов перестановок и подстановок. **Лабораторная работа №2.** Генерация псевдослучайных последовательностей чисел в системах защиты информации. Оценка статистических характеристик датчика псевдослучайных чисел с заданным законом распределения. **Лабораторная работа №3.** Симметричная криптография. Разработка и реализация варианта симметричного криптографического алгоритма с DES – подобной структурой. Оценка скорости работы алгоритма. **Лабораторная работа №4.** Разработка алгоритма и программная реализация атаки на симметричную криптографическую систему. **Лабораторная работа №5.** Программная реализация алгоритма RSA **Лабораторная работа №6.** Разработка и программная реализация протокола обмена симметричными ключами на основе алгоритма Diffyie-Hellman **Лабораторная работа №7.** Разработка и программная реализация алгоритма вычисления цифрового дайджеста сообщения. **Лабораторная работа №8.** Программная реализация алгоритмов цифровой подписи

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. Определение информации, ее классификация. Основные определения и термины при защите информации.
2. Основные термины криптографии.
3. Методы шифрования в криптографии: перестановок, замены, гаммирования.
4. Методы стеганографии в защите информации.
5. Хеш-функции в задачах защиты информации.
6. Аппаратные и программные методы и средства защиты информации при электронной обработке данных.
7. Аппаратные и программные методы и средства парольной защиты.

8. Атаки на протоколы идентификации.

9. Методы «запрос-ответ» при идентификации. Биометрическая идентификация.

10. Основные определения и механизмы информационной безопасности.

11. Система охраны периметра траектории с компьютерными системами.

12. Система видеонаблюдения для обеспечения информационной безопасности.

13. Назначение и роль охранной (пожарной) сигнализации в защите информации.

14. Назначение и сущность цифровой подписи.

15. Межсетевые экраны с контролем соединений.

16. Атаки некорректными сетевыми пакетами типа Nuke. Защита протоколов сетевой безопасности.

17. Основные методы информационной безопасности.

18. Dos-атаки. Методы защиты.

19. Понятие компьютерного вируса. Признаки. Методы обнаружения. Способы борьбы.

20. Методы защиты от компьютерных вирусов.

21. Автоматизированные средства безопасности. Антивирусы.

22. Методы удаления последствий заражения компьютерными вирусами.

23. Основные механизмы ввода пароля.

24. Угрозы преодоления парольной защиты.

25. Защита от атак на web-сайты и web-браузеры.

26. Сигнатурный метод защиты информации при сетевых атаках типа Teardrop.

6.2. Учебно-методическое обеспечение для самостоятельной работы студентов:

1. Костин В.Н. Методы и средства защиты компьютерной информации: аппаратные и программные средства защиты информации : учебное пособие / Костин В.Н.. - Москва : Издательский Дом МИСиС, 2018. - 21 с. - ISBN 978-5-906953-22-3. - Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. - URL: https://www.iprbookshop.ru/98199.html

2. Шаньгин В.Ф. Защита компьютерной информации. Эффективные методы и средства / В.Ф. Шаньгин. - Саратов: Профобразование, 2019. - 543 с. - ISBN 978-5-4488-0074-0. - Текст: электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. - URL: https://www.iprbookshop.ru/87992.html

7. Фонды оценочных средств

7.1. Вопросы к рубежным аттестациям

Вопросы к 1 рубежной аттестации*:*

1. Основные задачи защиты информации.

2. Теоретические основы защиты информации.

3. Основные понятия криптографии: терминология.

4. Криптография и криптоанализ.

5. Требования к криптосистемам.

6. Проблемы защиты информации в компьютерных системах.

7. Основные средства защиты информации в современных компьютерных системах и сетях.

8. Основные задачи обеспечения безопасности информации в компьютерных сетях.

9. Законодательство Российской Федерации в области информационной безопасности.

10. Информация как объект юридической и физической защиты.

11. Государственные информационные ресурсы.

12. Защита государственной тайны как особого вида защищаемой информации.

13. Защита конфиденциальной информации, в том числе интеллектуальной собственности и коммерческой тайны.

14. Нормативно-правовая база защиты компьютерных сетей от несанкционированного доступа.

15. Компьютерные преступления и особенности их расследования.

16. Понятие криптографического протокола.

17. Основные типы протоколов.

18. Классы преобразований: подстановки, перестановки, гаммирование, блочные шифры.

19. Датчики ПСЧ.

20. Симметричная криптография.

21. Асимметричная криптография.

22. Цифровой дайджест и хэш-функция.

23. Подстановочные и перестановочные шифры. Шифры Цезаря, Виженера, Вернома. Исследования Шеннона в области криптографии. Нераскрываемость шифра Вернома.

24. Симметричные криптографические системы.

25. Стандарт шифрования DES: алгоритм, скорость работы на различных платформах, режимы пользования, основные результаты по анализу стойкости.

26. Стандарт шифрования данных ГОСТ 28147-89: алгоритм, скорость работы на различных платформах, режимы пользования.

27. Блочные алгоритмы. Алгоритм Blowfish. Потоковые алгоритмы. Алгоритм PKZIP.

28. Теоретическая и практическая стойкость.

29. Системы с открытым ключом.

30. Алгоритм шифрования RSA. Вычислительные аспекты реализации алгоритма RSA. Вопросы стойкости.

31. Криптосистема Эль-Гамаля. Криптосистемы на основе эллиптических уравнений.

32. Задача обмена ключами.

33. Алгоритм Диффи-Хеллмана. Протоколы обмена ключами на основе алгоритма Диффи-Хеллмана: двусторонний и многосторонний протокол.

34. Цифровая электронная подпись.

35. Проблема аутентификации данных и электронная цифровая подпись.

36. Однонаправленные хэш-функции.

37. Алгоритм безопасного хэширования SHA.

38. Однонаправленные хэш-функции на основе симметричных блочных алгоритмов.

39. Отечественный стандарт хэш-функции.

40. Электронная подпись на основе алгоритма RSA.

41. Алгоритм цифровой подписи Эль-Гамаля (EGSA).

42. Алгоритм цифровой подписи DSA. Отечественный стандарт цифровой подписи.

Вопросы ко 2 рубежной аттестации:

1. Способы несанкционированного доступа к информации в компьютерных сетях.

2. Классификация способов несанкционированного доступа и жизненный цикл атак.

3. Способы противодействия несанкционированному межсетевому доступу.

4. Функции межсетевого экранирования.

5. Особенности межсетевого экранирования на различных уровнях модели OSI.

6. Режим функционирования межсетевых экранов и их основные компоненты.

7. Маршрутизаторы.

8. Шлюзы сетевого уровня.

9. Основные схемы сетевой защиты на базе межсетевых экранов.

10. Применение межсетевых экранов для организации виртуальных корпоративных сетей.

11. Критерии оценки межсетевых экранов.

12. Построение защищенных виртуальных сетей.

13. Способы создания защищенных виртуальных каналов. Обзор протоколов.

14. Безопасность в открытых сетях.

15. Инфраструктура на основе криптографии с открытыми ключами (ИОК).

16. Цифровые сертификаты.

17. Управление цифровыми сертификатами.

18. Компоненты ИОК и их функции. Центр Сертификации. Центр Регистрации. Конечные пользователи. Сетевой справочник.

19. Использование ИОК в приложениях. Электронная почта и документооборот. Web-приложения.

20. Стандарты в области ИОК. Стандарты PKIX. Стандарты, основанные на ИОК (S/MIME, SSL и TLS, SET, IPSEC).

21. Методы и средства встраивания скрытой служебной информации для управления правами доступа к информационным ресурсам.

22. Понятие стеганографии.

23. Задача встраивания скрытой служебной информации (цифровых водяных знаков) в аудио и видеосигналы.

24. Основные методы и алгоритмы встраивания и обнаружения водяных знаков.

25. Встраивание водяных знаков и сжатие информации.

26. Виды атак на информационные ресурсы, содержащие водяные знаки.

Образцы билетов рубежной аттестации:

МИНИСТЕРСТВО НАУКИ И ВАЫСШЕГО ОБРАЗОВАНИЯ РФ
Грозненский Государственный Нефтяной Технический Университет
им. акад. М.Д. Миллионщикова
Кафедра «Информационные технологии»
Дисциплина «Методы и средства защиты компьютерной информации»
1-я рубежная аттестация
Группа: **Семестр:**

Билет 1

1. Компьютерные преступления и особенности их расследования.
2. Понятие криптографического протокола.

Преподаватель_____Усамов И.Р.

МИНИСТЕРСТВО НАУКИ И ВАЫСШЕГО ОБРАЗОВАНИЯ РФ
Грозненский Государственный Нефтяной Технический Университет
им. акад. М.Д. Миллионщикова
Кафедра «Информационные технологии»
Дисциплина «Методы и средства защиты компьютерной информации»
2-я рубежная аттестация
Группа: **Семестр:**

Билет 1

1. Построение защищенных виртуальных сетей.
2. Способы создания защищенных виртуальных каналов. Обзор протоколов.

Преподаватель_____Усамов И.Р.

7.2. Вопросы к зачету / экзамену

Вопросы к зачету:

1. Основные задачи защиты информации.
2. Теоретические основы защиты информации.
3. Основные понятия криптографии: терминология.
4. Криптография и криптоанализ.
5. Требования к криптосистемам.
6. Проблемы защиты информации в компьютерных системах.
7. Основные средства защиты информации в современных компьютерных системах и сетях.
8. Основные задачи обеспечения безопасности информации в компьютерных сетях.
9. Законодательство Российской Федерации в области информационной безопасности.
10. Информация как объект юридической и физической защиты.
11. Государственные информационные ресурсы.
12. Защита государственной тайны как особого вида защищаемой информации.
13. Защита конфиденциальной информации, в том числе интеллектуальной собственности и коммерческой тайны.
14. Нормативно-правовая база защиты компьютерных сетей от несанкционированного доступа.
15. Компьютерные преступления и особенности их расследования.
16. Понятие криптографического протокола.
17. Основные типы протоколов.
18. Классы преобразований: подстановки, перестановки, гаммирование, блочные шифры.
19. Датчики ПСЧ.
20. Симметричная криптография.
21. Асимметричная криптография.
22. Цифровой дайджест и хэш-функция.
23. Подстановочные и перестановочные шифры. Шифры Цезаря, Виженера, Вернома. Исследования Шеннона в области криптографии. Нераскрываемость шифра Вернома.
24. Симметричные криптографические системы.

25. Стандарт шифрования DES: алгоритм, скорость работы на различных платформах, режимы пользования, основные результаты по анализу стойкости.

26. Стандарт шифрования данных ГОСТ 28147-89: алгоритм, скорость работы на различных платформах, режимы пользования.

27. Блочные алгоритмы. Алгоритм Blowfish. Потоковые алгоритмы. Алгоритм PKZIP.

28. Теоретическая и практическая стойкость.

29. Системы с открытым ключом.

30. Алгоритм шифрования RSA. Вычислительные аспекты реализации алгоритма RSA. Вопросы стойкости.

31. Криптосистема Эль-Гамаля. Криптосистемы на основе эллиптических уравнений.

32. Задача обмена ключами.

33. Алгоритм Диффи-Хеллмана. Протоколы обмена ключами на основе алгоритма Диффи-Хеллмана: двусторонний и многосторонний протокол.

34. Цифровая электронная подпись.

35. Проблема аутентификации данных и электронная цифровая подпись.

36. Однонаправленные хэш-функции.

37. Алгоритм безопасного хэширования SHA.

38. Однонаправленные хэш-функции на основе симметричных блочных алгоритмов.

39. Отечественный стандарт хэш-функции.

40. Электронная подпись на основе алгоритма RSA.

41. Алгоритм цифровой подписи Эль-Гамаля (EGSA).

42. Алгоритм цифровой подписи DSA. Отечественный стандарт цифровой подписи.

43. Способы несанкционированного доступа к информации в компьютерных сетях.

44. Классификация способов несанкционированного доступа и жизненный цикл атак.

45. Способы противодействия несанкционированному межсетевому доступу.

46. Функции межсетевого экранирования.

47. Особенности межсетевого экранирования на различных уровнях модели OSI.

48. Режим функционирования межсетевых экранов и их основные компоненты.

49. Маршрутизаторы.

50. Шлюзы сетевого уровня.

51. Основные схемы сетевой защиты на базе межсетевых экранов.

52. Применение межсетевых экранов для организации виртуальных корпоративных сетей.

53. Критерии оценки межсетевых экранов.

54. Построение защищенных виртуальных сетей.

55. Способы создания защищенных виртуальных каналов. Обзор протоколов.

56. Безопасность в открытых сетях.

57. Инфраструктура на основе криптографии с открытыми ключами (ИОК).

58. Цифровые сертификаты.

59. Управление цифровыми сертификатами.

60. Компоненты ИОК и их функции. Центр Сертификации. Центр Регистрации. Конечные пользователи. Сетевой справочник.

61. Использование ИОК в приложениях. Электронная почта и документооборот. Web-приложения.

62. Стандарты в области ИОК. Стандарты PKIX. Стандарты, основанные на ИОК (S/MIME, SSL и TLS, SET, IPSEC).

63. Методы и средства встраивания скрытой служебной информации для управления правами доступа к информационным ресурсам.

64. Понятие стеганографии.

65. Задача встраивания скрытой служебной информации (цифровых водяных знаков) в аудио и видеосигналы.

66. Основные методы и алгоритмы встраивания и обнаружения водяных знаков.

67. Встраивание водяных знаков и сжатие информации.

68. Виды атак на информационные ресурсы, содержащие водяные знаки.

Образец билета к зачету:

МИНИСТЕРСТВО НАУКИ И ВАЫСШЕГО ОБРАЗОВАНИЯ РФ
Грозненский Государственный Нефтяной Технический Университет
им. акад. М.Д. Миллионщикова
Кафедра «Информационные технологии»
Дисциплина «Методы и средства защиты компьютерной информации»
Группа: **Семестр:**

Билет 1

1. Однонаправленные хэш-функции
2. Управление цифровыми сертификатами.

Преподаватель_____Усамов И.Р.
Зав. кафедрой_____Моисеенко Н.А.

7.3. Текущий контроль

Образец типового задания для лабораторных занятий

Лабораторная работа 1. Простые шифры: защита информации в КИС (4 часа)

Цель работы:

Ознакомление с историей становления криптографии, освоение алгоритма шифрования «двойными перестановками», криптоанализа сообщений, зашифрованных указанным алгоритмом.

Задание на лабораторную работу:

1.Зашифровать предложение из 16 символов методом двойной перестановки и показать преподавателю.

2. Произвести криптоанализ перехваченного сообщения (выдает преподаватель).

3. Сравнить полученный и исходные ключи.

4. Разработать программы, позволяющие максимально автоматизировать процесс криптоанализа (автоматизированное рабочее место криптоаналитика).

Содержание отчета

Цель работы.

Результаты выполнения пунктов задания на лабораторную работу.

Схемы алгоритмов для автоматизированного рабочего места криптоаналитика, листинги разработанных программ.

Выводы по работе.

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 (удовлетворитель	61-80 баллов (хорошо)	81-100 баллов (отлично)	
ПК-4. Способен выполнять концептуально-логическое проектирование системы и сопровождать разработанные проектные решения					
Знать: правовые основы защиты компьютерной информации, математические основы криптографии, организационные, технические и программные методы защиты информации в современных компьютерных системах и сетях, стандарты	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: применять известные методы и средства поддержки информационной безопасности в компьютерных системах	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	
ПК-6. Способен создавать информационные технологии нового поколения.					
Знать: методы шифрования, методы идентификации пользователей, методы защиты программ от вирусов, основы инфраструктуры систем, построенных с использованием публичных и секретных ключей	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 сравнительный анализ, выбирать методы и средства, оценивать уровень защиты информационных ресурсов в прикладных системах	Частичные умения	Неполные умения	Умения полные, допускаются небольшие ошибки	Сформированные умения	
Владеть: навыками проведения сравнительного анализа, выбора методов и средств разработки безопасной системы	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;

1) 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);

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

3) 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. Костин В.Н. Методы и средства защиты компьютерной информации: аппаратные и программные средства защиты информации : учебное пособие / Костин В.Н.. - Москва : Издательский Дом МИСиС, 2018. - 21 с. - ISBN 978-5-906953-22-3. - Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. - URL: https://www.iprbookshop.ru/98199.html

2. Шаньгин В.Ф. Защита компьютерной информации. Эффективные методы и средства / В.Ф. Шаньгин. - Саратов: Профобразование, 2019. - 543 с. - ISBN 978-5-4488-0074-0. - Текст: электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. - URL: https://www.iprbookshop.ru/87992.html

3. Кирпичников А.П. Криптографические методы защиты компьютерной информации : учебное пособие / А.П. Кирпичников, З.М. Хайбуллина. - Казань : Казанский национальный исследовательский технологический университет, 2016. -100 с. - ISBN 978-5-7882-2052-9. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/79313.html

4. Международная информационная безопасность: теория и практика: в трех томах. Т.3: сборник документов (на английском языке). / А. В. Крутских, А. В. Бирюков, С. М. Бойко [и др.]; под редакцией А. В. Крутских; составители М. Б. Алборова, Е. С. Михалева, А. В. Макарычева. - 2-е изд. - Москва: Аспект Пресс, 2021. - 626 с. - ISBN 978-5-7567-1097-7 (т.3), 978-5-7567-1100-4. - Текст: электронный // Цифровой образовательный ресурс IPR SMART: [сайт]. - URL: https://www.iprbookshop.ru/104466.html

5. Сычев Ю.Н. Основы информационной безопасности: учебно-методический комплекс / Ю.Н. Сычев. - Москва: Евразийский открытый институт, 2012. - 342 с. - ISBN 978-5-374-00602-5. - Текст: электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. - URL: https://www.iprbookshop.ru/14642.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;
- мультимедийный проектор;
- настенный экран;

10.2. Помещения для самостоятельной работы

Учебная аудитория для самостоятельной работы – 4-06.

Методические указания по освоению дисциплины «Методы и средства защиты компьютерной информации»

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 «Методы и средства защиты компьютерной информации» состоит из 4 связанных между собою разделов, обеспечивающих последовательное изучение материала.

Обучение по дисциплине «Методы и средства защиты компьютерной информации» 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 «Методы и средства защиты компьютерной информации» - 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 работыявляется 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./

Директор ДУМР / Магомаева М.А. /