МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ «ГРОЗНЕНСКИЙ ГОСУДАРСТВЕННЫЙ НЕФТЯНОЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТИМЕНИ АКАДЕМИКА М.Д.МИЛЛИОНЩИКОВА»

Информационные технологии

УТВЕРЖДЕН

на заседании кафедры
«22»____11____2023 г., протокол №_3_

_____ Заведующий кафедрой
_____ Н.А. Моисеенко

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ПО УЧЕБНОЙ ДИСЦИПЛИНЕ

«Методы и средства защиты компьютерной информации»

Направление подготовки
09.03.04 Программная инженерия

Направленность (профиль)
«Программная инженерия»

Квалификация
бакалавр

Составитель (и) _____ И.Р. Усамов

Грозный – 2023

ПАСПОРТ

ФОНДА ОЦЕНОЧНЫХ СРЕДСТВ ПО УЧЕБНОЙ ДИСЦИПЛИНЕ

«Методы и средства защиты компьютерной информации»

№ п/п	Контролируемые разделы (темы) дисциплины	Код контролируемойкомпетенции (или ее части)	Наименование оценочного средства
1.	Законодательные аспекты информационных технологий	ПК-4, ПК-6	Лабораторные работы Доклады с презентациями Письм. контрольная работа (аттестация) Экзамен
2.	Криптографические методы защиты	ПК-4, ПК-6	Лабораторные работы Доклады с презентациями Письм. контрольная работа (аттестация) Экзамен
3.	Безопасность современных сетевых технологий	ПК-4, ПК-6	Лабораторные работы Доклады с презентациями Письм. контрольная работа (аттестация) Экзамен
4.	Методы и средства встраивания скрытой служебной информации для управления правами доступа к информационным ресурсам.	ПК-4, ПК-6	Лабораторные работы Доклады с презентациями Письм. контрольная работа (аттестация) Экзамен

ПЕРЕЧЕНЬ ОЦЕНОЧНЫХ СРЕДСТВ

№ п/п	Наименование оценочного средства	Краткая характеристика оценочного средства	Представление оценочного средства в фонде
1.	Лабораторная работа	Задания, выполняемые с использованием изучаемого программного обеспечения с целью углубления и закрепления теоретических знаний и развития навыков самостоятельного проведения эксперимента	Комплект заданий для выполнения лабораторных работ
2.	Доклад с презентацией	Продукт самостоятельной работы студента, представляющий собой публичное выступление по определенной учебно-практической, исследовательской или научной теме	Темы докладов
3.	Письм. контрольная работа (аттестация)	Подведение итогов учебной деятельности студентов в течение семестра в письменной форме	Вопросы по темам / разделам дисциплины
4.	Зачет	Итоговая форма оценки знаний	Вопросы к зачету

КОМПЛЕКТ ЗАДАНИЙ ДЛЯ ВЫПОЛНЕНИЯ ЛАБОРАТОРНЫХ РАБОТ

Лабораторные работы организуются в компьютерных аудиториях и выполняются по заданию преподавателя с использованием изучаемого программного обеспечения.

Тема 1. Простые шифры: защита информации в КИС

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).

Подготовить для включения в отчет о лабораторной работе ответы на следующие вопросы:

- какие существуют простые шифры?
- в чем слабость простых шифров?
- как может быть повышена надежность простых шифров?
- какой может быть реакция системы на попытку подбора паролей?
- кому может быть разрешен доступ по чтению и по записи к базе учетных записей пользователей?
- как должны храниться простые шифры?

Тема 2. Реализация сложных шифров

Определение понятий (изучить, включить в отчет):

- сложный шифр;
- код нечетных чисел;
- журнал шифра;
- квантовые шифры;
- комбинированные шифры;
- шифры замены.

Порядок выполнения лабораторной работы заключается в следующем:

- ознакомиться с разделами методических указаний к данной лабораторной работе;
- получить у преподавателя вариант (варианты) заданий на исследование описанных выше шифров;
- составить контрольный пример;
- разработать и реализовать заданный(е) алгоритм(ы) шифрования/дешифрования;
- на контрольном примере проверить правильность работы алгоритмов шифрования и дешифрования;
- составить отчет.

Тема 3. Разграничение доступа к ресурсам в защищенных версиях операционной системы Windows

Подготовить для включения в отчет о лабораторной работе определения понятий:

- дискреционная политика безопасности;
- мандатная политика безопасности;
- субъект доступа;
- объект доступа;
- виды доступа;
- монитор обращений;
- монитор безопасности объектов;
- домен безопасности;
- реестр операционной системы;
- контроль целостности объектов;
- ключ симметричного шифрования;
- ключи асимметричного шифрования.

Подготовить для включения в отчет о лабораторной работе ответы на следующие вопросы:

- в чем достоинства и недостатки дискреционной политики безопасности?
- в чем достоинства и недостатки мандатной политики безопасности?
- в чем заключается тождественность объектов и тождественность субъектов компьютерной системы?
- кто определяет права доступа к папкам, файлам, принтерам при использовании дискреционной политики безопасности?
- каковы возможные пути нарушения политики безопасности в компьютерной системе?
- какие факторы влияют на определение размеров доменов безопасности?
- какая информация хранится в реестре Windows?

Тема 4. Использование программных средств контроля и анализа выполнения политики безопасности на примере операционной системы Windows XP/7

Подготовить для включения в отчет о лабораторной работе определения понятий:

- матрица доступа;
- дискреционный список контроля доступа;
- домен безопасности;
- журнал (файл) аудита;
- запись журнала аудита;
- стандарт безопасности.

Подготовить для включения в отчет о лабораторной работе ответы на следующие вопросы:

- что такое Trusted Computer System Evaluation Criteria (TCSEC)?
- какие основные категории требований к защищенности компьютерных систем предложены в TCSEC, в чем их смысл?
- какие требования к компьютерным системам предъявляются по классу защиты C2 TCSEC?
- кто управляет дискреционным списком контроля доступа к объектам в операционной системе Windows XP?
- как должны использоваться записи журнала аудита событий безопасности?
- какие права доступа к файлу аудита имеет по умолчанию администратор системы?
- что такое консольное приложение Windows?

Тема 5. Использование программных средств контроля и анализа выполнения политики безопасности на примере операционной системы Windows XP

Цель работы: освоение системных программ Windows XP, программ из комплекта Windows NT Resource Kit и других программных средств, предназначенных для:

- просмотра и управления разрешениями на доступ к конфиденциальным объектам компьютерной системы;
- просмотра и анализа записей аудита;
- анализа соответствия реализуемой в компьютерной системе политики безопасности требованиям стандартов безопасности;
- дополнительной защиты базы учетных записей пользователей компьютерной системы и используемых ими рабочих станций.

Подготовить для включения в отчет о лабораторной работе ответы на следующие вопросы:

- что такое Trusted Computer System Evaluation Criteria (TCSEC)?
- какие основные категории требований к защищенности компьютерных систем предложены в TCSEC, в чем их смысл?
- какие требования к компьютерным системам предъявляются по классу защиты C2 TCSEC?

- кто управляет дискреционным списком контроля доступа к объектам в операционной системе Windows XP?

- как должны использоваться записи журнала аудита событий безопасности?

- какие права доступа к файлу аудита имеет по умолчанию администратор системы?

- что такое консольное приложение Windows?

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.

ТЕМЫ ДОКЛАДОВ С ПРЕЗЕНТАЦИЯМИ

Подготовка презентации на 12-15 слайдов с устным докладом по заданной тематике:

Примерный перечень тем:

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.

Критерии оценки доклада с презентацией:

13-15 баллов выставляется студенту, если:

- проведенное исследование и изложенный в докладе материал соответствует заданной теме;
- представленные в докладе сведения отвечают требованиям актуальности и новизны;
- продумана структура и стиль сопроводительной презентации;
- студент способен ответить на вопросы преподавателя по теме доклада.

6-12 баллов:

- представленный в докладе материал соответствует заданной теме, однако присутствуют недостатки в связности изложения и структуре сопроводительной презентации;
- не все выводы носят аргументированный и доказательный характер.

1-5 баллов:

- студент способен изложить материал доклада, однако наблюдаются отклонения от заданной темы;
- сопроводительная презентация подготовлена, но плохо соотносится с представленным докладом.

0 баллов:

- материал не соответствует заданной теме;
- отсутствует сопроводительная презентация к докладу;
- студент не освоил материал полностью и не способен ответить на вопросы преподавателя по теме доклада.

ГРОЗНЕНСКИЙ ГОСУДАРСТВЕННЫЙ НЕФТЯНОЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТИМЕНИ АКАДЕМИКА М.Д.МИЛЛИОНЩИКОВА

Институт прикладных информационных технологий

Кафедра Информационные технологии

Вопросы к экзамену по дисциплине «Методы и средства защиты компьютерной информации»

Итоговая отчетность студентов по дисциплине принимается по билетам, с предоставлением времени на подготовку (20-30 мин.) и последующим устным ответом преподавателю. Состав билета на зачет – 2 вопроса.

Вопросы к зачету

К 1-ой рубежной аттестации:

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

23. Подстановочные и перестановочные шифры. Шифры Цезаря, Виженера, Вернома. Исследования Шеннона в области криптографии. Нераскрываемость шифра Вернома. (ПК-4, ПК-6)

24. Симметричные криптографические системы. (ПК-4, ПК-6)

25. Стандарт шифрования DES: алгоритм, скорость работы на различных платформах, режимы пользования, основные результаты по анализу стойкости. (ПК-4, ПК-6)

26. Стандарт шифрования данных ГОСТ 28147-89: алгоритм, скорость работы на различных платформах, режимы пользования. (ПК-4, ПК-6)

27. Блочные алгоритмы. Алгоритм Blowfish. Потоковые алгоритмы. Алгоритм PKZIP. (ПК-4, ПК-6)

28. Теоретическая и практическая стойкость. (ПК-4, ПК-6)

29. Системы с открытым ключом. (ПК-4, ПК-6)

30. Алгоритм шифрования RSA. Вычислительные аспекты реализации алгоритма RSA. Вопросы стойкости. (ПК-4, ПК-6)

31. Криптосистема Эль-Гамаля. Криптосистемы на основе эллиптических уравнений. (ПК-4, ПК-6)

32. Задача обмена ключами. (ПК-4, ПК-6)

33. Алгоритм Диффи-Хеллмана. Протоколы обмена ключами на основе алгоритма Диффи-Хеллмана: двусторонний и многосторонний протокол. (ПК-4, ПК-6)

34. Цифровая электронная подпись. (ПК-4, ПК-6)

35. Проблема аутентификации данных и электронная цифровая подпись. (ПК-4, ПК-6)

36. Однонаправленные хэш-функции. (ПК-4, ПК-6)

37. Алгоритм безопасного хэширования SHA. (ПК-4, ПК-6)

38. Однонаправленные хэш-функции на основе симметричных блочных алгоритмов. (ПК-4, ПК-6)

39. Отечественный стандарт хэш-функции. (ПК-4, ПК-6)

40. Электронная подпись на основе алгоритма RSA. (ПК-4, ПК-6)

41. Алгоритм цифровой подписи Эль-Гамаля (EGSA). (ПК-4, ПК-6)

42. Алгоритм цифровой подписи DSA. Отечественный стандарт цифровой подписи. (ПК-4, ПК-6)

Ко 2-ой рубежной аттестации:

1. Способы несанкционированного доступа к информации в компьютерных сетях. (ПК-4, ПК-6)

2. Классификация способов несанкционированного доступа и жизненный цикл атак. (ПК-4, ПК-6)

3. Способы противодействия несанкционированному межсетевому доступу. (ПК-4, ПК-6)

4. Функции межсетевого экранирования. (ПК-4, ПК-6)

5. Особенности межсетевого экранирования на различных уровнях модели OSI. (ПК-4, ПК-6)

6. Режим функционирования межсетевых экранов и их основные компоненты. (ПК-4, ПК-6)

7. Маршрутизаторы. (ПК-4, ПК-6)

8. Шлюзы сетевого уровня. (ПК-4, ПК-6)

9. Основные схемы сетевой защиты на базе межсетевых экранов. (ПК-4, ПК-6)

10. Применение межсетевых экранов для организации виртуальных корпоративных сетей. (ПК-4, ПК-6)

11. Критерии оценки межсетевых экранов. (ПК-4, ПК-6)

12. Построение защищенных виртуальных сетей. (ПК-4, ПК-6)

13. Способы создания защищенных виртуальных каналов. Обзор протоколов. (ПК-4, ПК-6)

14. Безопасность в открытых сетях. (ПК-4, ПК-6)

15. Инфраструктура на основе криптографии с открытыми ключами (ИОК). (ПК-4, ПК-6)

16. Цифровые сертификаты. (ПК-4, ПК-6)

17. Управление цифровыми сертификатами. (ПК-4, ПК-6)

18. Компоненты ИОК и их функции. Центр Сертификации. Центр Регистрации. Конечные пользователи. Сетевой справочник. (ПК-4, ПК-6)

19. Использование ИОК в приложениях. Электронная почта и документооборот. Web-приложения. (ПК-4, ПК-6)

20. Стандарты в области ИОК. Стандарты PKIX. Стандарты, основанные на ИОК (S/MIME, SSL и TLS, SET, IPSEC). (ПК-4, ПК-6)

21. Методы и средства встраивания скрытой служебной информации для управления правами доступа к информационным ресурсам. (ПК-4, ПК-6)

22. Понятие стеганографии. (ПК-4, ПК-6)

23. Задача встраивания скрытой служебной информации (цифровых водяных знаков) в аудио и видеосигналы. (ПК-4, ПК-6)

24. Основные методы и алгоритмы встраивания и обнаружения водяных знаков. (ПК-4, ПК-6)

25. Встраивание водяных знаков и сжатие информации. (ПК-4, ПК-6)

26. Виды атак на информационные ресурсы, содержащие водяные знаки. (ПК-4, ПК-6)

При оценке ответа студента на экзамене учитываются:

- правильность ответа на вопрос;
- логика изложения материала вопроса;
- правильность ответа на дополнительные вопросы;
- умение увязывать теоретические и практические аспекты вопроса;
- культура устной речи студента.

В пределах допускаемых на экзамене 20 баллов студенту выставляется:

Более 15 баллов – студент показывает всестороннее глубокое систематическое знание учебно-методического материала, усвоил основную литературу и знаком с дополнительной литературой; самостоятельно, в логической последовательности и исчерпывающе отвечает на все вопросы билета; умеет анализировать, классифицировать, обобщать и систематизировать изученный материал, устанавливать причинно-следственные связи; увязывает теоретические аспекты предмета с практическими задачами.

От 6 до 15 баллов – студент обнаруживает, в основном, полное знание учебно-программного материала, успешно выполняет предусмотренные в программе задания; излагает ответы на поставленные вопросы систематизированно и последовательно, но

имеются пробелы знаний в некоторых разделах; демонстрирует умение анализировать материал, однако не все выводы носят аргументированный и доказательный характер; способен к самостоятельному пополнению и обновлению знаний в ходе дальнейшей учебной работы и профессиональной деятельности.

До 5 баллов – студент показывает знания основного учебно-программного материала в объеме, необходимом для дальнейшей учебы, знаком с основной литературой, рекомендованной программой, однако проявляет затруднения в самостоятельных ответах, оперирует неточными формулировками; в процессе ответов допускаются ошибки по существу вопросов. Студент способен решать лишь наиболее легкие задачи, владеет только обязательным минимумом практических навыков.

0 баллов – студент показывает существенные пробелы в знаниях основного учебного программного материала, допускает принципиальные ошибки в выполнении предусмотренных программой заданий; не способен ответить на вопросы билета даже при дополнительных наводящих вопросах преподавателя.

КОНТРОЛЬНО-ИЗМЕРИТЕЛЬНЫЕ МАТЕРИАЛЫ ПО ДИСЦИПЛИНЕ

«Методы и средства защиты компьютерной информации»

Билеты к рубежной аттестации

Грозненский государственный нефтяной технический университет им.акад. М.Д. Миллионщикова
Кафедра «Информационные технологии»
Группа "" Семестр "8"
1-я рубежная аттестация
Дисциплина "Методы и средства защиты компьютерной информации"
Билет № 1

1. Основные задачи обеспечения безопасности информации в компьютерных сетях.
2. Электронная подпись на основе алгоритма RSA.

Подпись преподавателя_____ **Подпись заведующего кафедрой**_____

Грозненский государственный нефтяной технический университет им.акад. М.Д. Миллионщикова
Кафедра «Информационные технологии»
Группа "" Семестр "8"
1-я рубежная аттестация
Дисциплина "Методы и средства защиты компьютерной информации"
Билет № 2

1. Теоретическая и практическая стойкость.
2. Системы с открытым ключом.

Подпись преподавателя_____ **Подпись заведующего кафедрой**_____

Грозненский государственный нефтяной технический университет им.акад. М.Д. Миллионщикова
Кафедра «Информационные технологии»
Группа "" Семестр "8"
1-я рубежная аттестация
Дисциплина "Методы и средства защиты компьютерной информации"
Билет № 3

1. Законодательство Российской Федерации в области информационной безопасности.
2. Блочные алгоритмы. Алгоритм Blowfish. Потоковые алгоритмы. Алгоритм PKZIP.

Подпись преподавателя_____ **Подпись заведующего кафедрой**_____

Грозненский государственный нефтяной технический университет им.акад. М.Д. Миллионщикова
Кафедра «Информационные технологии»
Группа "" Семестр "8"
1-я рубежная аттестация
Дисциплина "Методы и средства защиты компьютерной информации"
Билет № 4

1. Отечественный стандарт хэш-функции.
2. Компьютерные преступления и особенности их расследования.

Подпись преподавателя_____ **Подпись заведующего кафедрой**_____

Грозненский государственный нефтяной технический университет им.акад. М.Д. Миллионщикова
Кафедра «Информационные технологии»
Группа "" Семестр "8"
1-я рубежная аттестация
Дисциплина "Методы и средства защиты компьютерной информации"
Билет № 5

1. Асимметричная криптография.
2. Датчики ПСЧ.

Подпись преподавателя_____ **Подпись заведующего кафедрой**_____

Грозненский государственный нефтяной технический университет им.акад. М.Д. Миллионщикова
Кафедра «Информационные технологии»
Группа "" Семестр "8"
1-я рубежная аттестация
Дисциплина "Методы и средства защиты компьютерной информации"
Билет № 6

1. Алгоритм Диффи-Хеллмана. Протоколы обмена ключами на основе алгоритма Диффи-Хеллмана: двусторонний и многосторонний протокол.
2. Цифровая электронная подпись.

Подпись преподавателя_____ Подпись заведующего кафедрой_____

Грозненский государственный нефтяной технический университет им.акад. М.Д. Миллионщикова
Кафедра «Информационные технологии»
Группа "" Семестр "8"
1-я рубежная аттестация
Дисциплина "Методы и средства защиты компьютерной информации"
Билет № 7

1. Стандарт шифрования DES: алгоритм, скорость работы на различных платформах, режимы пользования, основные результаты по анализу стойкости.
2. Основные средства защиты информации в современных компьютерных системах и сетях.

Подпись преподавателя_____ Подпись заведующего кафедрой_____

Грозненский государственный нефтяной технический университет им.акад. М.Д. Миллионщикова
Кафедра «Информационные технологии»
Группа "" Семестр "8"
1-я рубежная аттестация
Дисциплина "Методы и средства защиты компьютерной информации"
Билет № 8

1. Подстановочные и перестановочные шифры. Шифры Цезаря, Виженера, Вернома. Исследования Шеннона в области криптографии. Нераскрываемость шифра Вернома.
2. Электронная подпись на основе алгоритма RSA.

Подпись преподавателя_____ Подпись заведующего кафедрой_____

Грозненский государственный нефтяной технический университет им.акад. М.Д. Миллионщикова
Кафедра «Информационные технологии»
Группа "" Семестр "8"
1-я рубежная аттестация
Дисциплина "Методы и средства защиты компьютерной информации"
Билет № 9

1. Электронная подпись на основе алгоритма RSA.
2. Основные задачи защиты информации.

Подпись преподавателя_____ Подпись заведующего кафедрой_____

Грозненский государственный нефтяной технический университет им.акад. М.Д. Миллионщикова
Кафедра «Информационные технологии»
Группа "" Семестр "8"
1-я рубежная аттестация
Дисциплина "Методы и средства защиты компьютерной информации"
Билет № 10

1. Основные задачи защиты информации.
2. Проблемы защиты информации в компьютерных системах.

Подпись преподавателя_____ Подпись заведующего кафедрой_____

Грозненский государственный нефтяной технический университет им.акад. М.Д. Миллионщикова
Кафедра «Информационные технологии»
Группа "" Семестр "8"
2-я рубежная аттестация
Дисциплина "Методы и средства защиты компьютерной информации"
Билет № 1

1. Шлюзы сетевого уровня.
2. Основные методы и алгоритмы встраивания и обнаружения водяных знаков.

Подпись преподавателя_____ Подпись заведующего кафедрой_____

Грозненский государственный нефтяной технический университет им.акад. М.Д. Миллионщикова
Кафедра «Информационные технологии»
Группа "" Семестр "8"
2-я рубежная аттестация
Дисциплина "Методы и средства защиты компьютерной информации"
Билет № 2

1. Стандарты в области ИОК. Стандарты PKIX. Стандарты, основанные на ИОК (S/MIME, SSL и TLS, SET, IPSEC).
2. Управление цифровыми сертификатами.

Подпись преподавателя_____ Подпись заведующего кафедрой_____

Грозненский государственный нефтяной технический университет им.акад. М.Д. Миллионщикова
Кафедра «Информационные технологии»
Группа "" Семестр "8"
2-я рубежная аттестация
Дисциплина "Методы и средства защиты компьютерной информации"
Билет № 3

1. Виды атак на информационные ресурсы, содержащие водяные знаки.
2. Понятие стеганографии.

Подпись преподавателя_____ Подпись заведующего кафедрой_____

Грозненский государственный нефтяной технический университет им.акад. М.Д. Миллионщикова
Кафедра «Информационные технологии»
Группа "" Семестр "8"
2-я рубежная аттестация
Дисциплина "Методы и средства защиты компьютерной информации"
Билет № 4

1. Использование ИОК в приложениях. Электронная почта и документооборот. Web-приложения.
2. Способы противодействия несанкционированному межсетевому доступу.

Подпись преподавателя_____ Подпись заведующего кафедрой_____

Грозненский государственный нефтяной технический университет им.акад. М.Д. Миллионщикова
Кафедра «Информационные технологии»
Группа "" Семестр "8"
2-я рубежная аттестация
Дисциплина "Методы и средства защиты компьютерной информации"
Билет № 5

1. Классификация способов несанкционированного доступа и жизненный цикл атак.
2. Безопасность в открытых сетях.

Подпись преподавателя_____ Подпись заведующего кафедрой_____

Грозненский государственный нефтяной технический университет им.акад. М.Д. Миллионщикова
Кафедра «Информационные технологии»
Группа "" Семестр "8"
2-я рубежная аттестация
Дисциплина "Методы и средства защиты компьютерной информации"

Билет № 6

1. Управление цифровыми сертификатами.
2. Задача встраивания скрытой служебной информации (цифровых водяных знаков) в аудио и видеосигналы.

Подпись преподавателя_____ Подпись заведующего кафедрой_____

Грозненский государственный нефтяной технический университет им.акад. М.Д. Миллионщикова
Кафедра «Информационные технологии»
Группа "" Семестр "8"
2-я рубежная аттестация
Дисциплина "Методы и средства защиты компьютерной информации"
Билет № 7

1. Задача встраивания скрытой служебной информации (цифровых водяных знаков) в аудио и видеосигналы.
2. Классификация способов несанкционированного доступа и жизненный цикл атак.

Подпись преподавателя_____ Подпись заведующего кафедрой_____

Грозненский государственный нефтяной технический университет им.акад. М.Д. Миллионщикова
Кафедра «Информационные технологии»
Группа "" Семестр "8"
2-я рубежная аттестация
Дисциплина "Методы и средства защиты компьютерной информации"
Билет № 8

1. Стандарты в области ИОК. Стандарты PKIX. Стандарты, основанные на ИОК (S/MIME, SSL и TLS, SET, IPSEC).
2. Понятие стеганографии.

Подпись преподавателя_____ Подпись заведующего кафедрой_____

Грозненский государственный нефтяной технический университет им.акад. М.Д. Миллионщикова
Кафедра «Информационные технологии»
Группа "" Семестр "8"
2-я рубежная аттестация
Дисциплина "Методы и средства защиты компьютерной информации"
Билет № 9

1. Управление цифровыми сертификатами.
2. Особенности межсетевого экранирования на различных уровнях модели OSI.

Подпись преподавателя_____ Подпись заведующего кафедрой_____

Грозненский государственный нефтяной технический университет им.акад. М.Д. Миллионщикова
Кафедра «Информационные технологии»
Группа "" Семестр "8"
2-я рубежная аттестация
Дисциплина "Методы и средства защиты компьютерной информации"
Билет № 10

1. Инфраструктура на основе криптографии с открытыми ключами (ИОК).
2. Режим функционирования межсетевых экранов и их основные компоненты.

Подпись преподавателя_____ Подпись заведующего кафедрой_____

ЗАЧЕТНО-ЭКЗАМЕНАЦИОННЫЕ МАТЕРИАЛЫ

8 СЕМЕСТР, ЗАЧЕТ

Грозненский государственный нефтяной технический университет им.акад. М.Д. Миллионщикова
Кафедра «Информационные технологии»
Группа "" Семестр "8"
Дисциплина "Методы и средства защиты компьютерной информации"
Билет № 1

1. Основные задачи обеспечения безопасности информации в компьютерных сетях.
2. Электронная подпись на основе алгоритма RSA.

Подпись преподавателя_____ Подпись заведующего кафедрой_____

Грозненский государственный нефтяной технический университет им.акад. М.Д. Миллионщикова
Кафедра «Информационные технологии»
Группа "" Семестр "8"
Дисциплина "Методы и средства защиты компьютерной информации"
Билет № 2

1. Теоретическая и практическая стойкость.
2. Системы с открытым ключом.

Подпись преподавателя_____ Подпись заведующего кафедрой_____

Грозненский государственный нефтяной технический университет им.акад. М.Д. Миллионщикова
Кафедра «Информационные технологии»
Группа "" Семестр "8"
Дисциплина "Методы и средства защиты компьютерной информации"
Билет № 3

1. Законодательство Российской Федерации в области информационной безопасности.
2. Блочные алгоритмы. Алгоритм Blowfish. Потоковые алгоритмы. Алгоритм PKZIP.

Подпись преподавателя_____ Подпись заведующего кафедрой_____

Грозненский государственный нефтяной технический университет им.акад. М.Д. Миллионщикова
Кафедра «Информационные технологии»
Группа "" Семестр "8"
Дисциплина "Методы и средства защиты компьютерной информации"
Билет № 4

1. Отечественный стандарт хэш-функции.
2. Компьютерные преступления и особенности их расследования.

Подпись преподавателя_____ Подпись заведующего кафедрой_____

Грозненский государственный нефтяной технический университет им.акад. М.Д. Миллионщикова
Кафедра «Информационные технологии»
Группа "" Семестр "8"
Дисциплина "Методы и средства защиты компьютерной информации"
Билет № 5

1. Асимметричная криптография.
2. Датчики ПСЧ.

Подпись преподавателя_____ Подпись заведующего кафедрой_____

Грозненский государственный нефтяной технический университет им.акад. М.Д. Миллионщикова
Кафедра «Информационные технологии»
Группа "" Семестр "8"
Дисциплина "Методы и средства защиты компьютерной информации"
Билет № 6

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

2. Цифровая электронная подпись.

Подпись преподавателя_____ Подпись заведующего кафедрой_____

Грозненский государственный нефтяной технический университет им.акад. М.Д. Миллионщикова
Кафедра «Информационные технологии»
Группа "" Семестр "8"
Дисциплина "Методы и средства защиты компьютерной информации"
Билет № 7

1. Стандарт шифрования DES: алгоритм, скорость работы на различных платформах, режимы пользования, основные результаты по анализу стойкости.
2. Основные средства защиты информации в современных компьютерных системах и сетях.

Подпись преподавателя_____ Подпись заведующего кафедрой_____

Грозненский государственный нефтяной технический университет им.акад. М.Д. Миллионщикова
Кафедра «Информационные технологии»
Группа "" Семестр "8"
Дисциплина "Методы и средства защиты компьютерной информации"
Билет № 8

1. Подстановочные и перестановочные шифры. Шифры Цезаря, Виженера, Вернома. Исследования Шеннона в области криптографии. Нераскрываемость шифра Вернома.
2. Электронная подпись на основе алгоритма RSA.

Подпись преподавателя_____ Подпись заведующего кафедрой_____

Грозненский государственный нефтяной технический университет им.акад. М.Д. Миллионщикова
Кафедра «Информационные технологии»
Группа "" Семестр "8"
Дисциплина "Методы и средства защиты компьютерной информации"
Билет № 9

1. Электронная подпись на основе алгоритма RSA.
2. Основные задачи защиты информации.

Подпись преподавателя_____ Подпись заведующего кафедрой_____

Грозненский государственный нефтяной технический университет им.акад. М.Д. Миллионщикова
Кафедра «Информационные технологии»
Группа "" Семестр "8"
Дисциплина "Методы и средства защиты компьютерной информации"
Билет № 10

1. Основные задачи защиты информации.
2. Проблемы защиты информации в компьютерных системах.

Подпись преподавателя_____ Подпись заведующего кафедрой_____

Грозненский государственный нефтяной технический университет им.акад. М.Д. Миллионщикова
Кафедра «Информационные технологии»
Группа "" Семестр "8"
Дисциплина "Методы и средства защиты компьютерной информации"
Билет № 11

1. Шлюзы сетевого уровня.
2. Основные методы и алгоритмы встраивания и обнаружения водяных знаков.

Подпись преподавателя_____ Подпись заведующего кафедрой_____

Грозненский государственный нефтяной технический университет им.акад. М.Д. Миллионщикова
Кафедра «Информационные технологии»
Группа "" Семестр "8"
Дисциплина "Методы и средства защиты компьютерной информации"
Билет № 12

1. Стандарты в области ИОК. Стандарты PKIX. Стандарты, основанные на ИОК (S/MIME, SSL и TLS, SET, IPSEC).
2. Управление цифровыми сертификатами.

Подпись преподавателя_____ Подпись заведующего кафедрой_____

Грозненский государственный нефтяной технический университет им.акад. М.Д. Миллионщикова
Кафедра «Информационные технологии»
Группа "" Семестр "8"
Дисциплина "Методы и средства защиты компьютерной информации"
Билет № 13

1. Виды атак на информационные ресурсы, содержащие водяные знаки.
2. Понятие стеганографии.

Подпись преподавателя_____ Подпись заведующего кафедрой_____

Грозненский государственный нефтяной технический университет им.акад. М.Д. Миллионщикова
Кафедра «Информационные технологии»
Группа "" Семестр "8"
Дисциплина "Методы и средства защиты компьютерной информации"
Билет № 14

1. Использование ИОК в приложениях. Электронная почта и документооборот. Web-приложения.
2. Способы противодействия несанкционированному межсетевому доступу.

Подпись преподавателя_____ Подпись заведующего кафедрой_____

Грозненский государственный нефтяной технический университет им.акад. М.Д. Миллионщикова
Кафедра «Информационные технологии»
Группа "" Семестр "8"
Дисциплина "Методы и средства защиты компьютерной информации"
Билет № 15

1. Классификация способов несанкционированного доступа и жизненный цикл атак.
2. Безопасность в открытых сетях.

Подпись преподавателя_____ Подпись заведующего кафедрой_____

Грозненский государственный нефтяной технический университет им.акад. М.Д. Миллионщикова
Кафедра «Информационные технологии»
Группа "" Семестр "8"
Дисциплина "Методы и средства защиты компьютерной информации"
Билет № 16

1. Управление цифровыми сертификатами.
2. Задача встраивания скрытой служебной информации (цифровых водяных знаков) в аудио и видеосигналы.

Подпись преподавателя_____ Подпись заведующего кафедрой_____

Грозненский государственный нефтяной технический университет им.акад. М.Д. Миллионщикова
Кафедра «Информационные технологии»
Группа "" Семестр "8"
Дисциплина "Методы и средства защиты компьютерной информации"
Билет № 17

1. Задача встраивания скрытой служебной информации (цифровых водяных знаков) в аудио и видеосигналы.
2. Классификация способов несанкционированного доступа и жизненный цикл атак.

Подпись преподавателя_____ Подпись заведующего кафедрой_____

Грозненский государственный нефтяной технический университет им.акад. М.Д. Миллионщикова
Кафедра «Информационные технологии»
Группа "" Семестр "8"
Дисциплина "Методы и средства защиты компьютерной информации"
Билет № 18

1. Стандарты в области ИОК. Стандарты PKIX. Стандарты, основанные на ИОК (S/MIME, SSL и TLS, SET, IPSEC).
2. Понятие стеганографии.

Подпись преподавателя_____ Подпись заведующего кафедрой_____

Грозненский государственный нефтяной технический университет им.акад. М.Д. Миллионщикова
Кафедра «Информационные технологии»
Группа "" Семестр "8"
Дисциплина "Методы и средства защиты компьютерной информации"
Билет № 19

1. Управление цифровыми сертификатами.
2. Особенности межсетевого экранирования на различных уровнях модели OSI.

Подпись преподавателя_____ Подпись заведующего кафедрой_____

Грозненский государственный нефтяной технический университет им.акад. М.Д. Миллионщикова
Кафедра «Информационные технологии»
Группа "" Семестр "8"
Дисциплина "Методы и средства защиты компьютерной информации"
Билет № 20

1. Инфраструктура на основе криптографии с открытыми ключами (ИОК).
2. Режим функционирования межсетевых экранов и их основные компоненты.

Подпись преподавателя_____ Подпись заведующего кафедрой_____
