МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ «ГРОЗНЕНСКИЙ ГОСУДАРСТВЕННЫЙ НЕФТЯНОЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ ИМЕНИ АКАДЕМИКА М.Д.МИЛЛИОНЩИКОВА»

Сети связи и системы коммутации

УТВЕРЖДЕН
на заседании кафедры
«01» 09 2021 г., протокол №1
И. о. заведующего кафедрой
М.Я. Пашаев
(подпись)

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ПО УЧЕБНОЙ ДИСЦИПЛИНЕ

Методы и средства защиты информации в компьютерных сетях

Направление подготовки

11.03.02 Инфокоммуникационные технологии и системы связи

Направленность (профиль)

«Инфокоммуникационные сети и системы»

Квалификация (степень) выпускника

бакалавр

Составитель Х.А. Доудов

Грозный - 2021

ПАСПОРТ

ФОНДА ОЦЕНОЧНЫХ СРЕДСТВ ПО УЧЕБНОЙ ДИСЦИПЛИНЕ

«Методы и средства защиты информации в компьютерных сетях»

№ п/п	Контролируемые разделы (темы) дисциплины	Код контролируемой компетенции (или ее части)	Наименование оценочного средства
1.	Введение	ПК-3 ПК-3.1	Опрос
2.	Защита информации от ПЭМИН	ПК-9 ПК-9.1	Обсуждение сообщений
3.	Основы теории защиты информации в компьютерных системах. Критерии информационной безопасности	ПК-9 ПК-9.3	Опрос
4.	Основы криптографии	ПК-9 ПК-9.3	Опрос
5.	Применение симметричных криптосистем для защиты компьютерной информации	ПК-9 ПК-9.1	Обсуждение сообщений
6.	Инфраструктура открытых ключей	ПК-9 ПК-9.2	Обсуждение сообщений
7.	Методы идентификации и аутентификации пользователей компьютерных систем	ПК-3 ПК-3.1	Опрос

ПЕРЕЧЕНЬ ОЦЕНОЧНЫХ СРЕДСТВ

№ п/п	**Наименование оценочного средства**	**Краткая характеристика оценочного средства**	**Представление оценочного средства в фонде**
1	*Лабораторная работа*	Средство проверки умений применять полученные знания по заранее определенной методике для решения задач или заданий по модулю или дисциплине в целом	Комплект заданий для выполнения лабораторных работ
2	*Зачет*	Итоговая форма оценки знаний	Вопросы к зачету
3	*Экзамен*	Итоговая форма оценки знаний	Вопросы к экзамену

Второй семестр

Вопросы к первой рубежной аттестации

1. Цель, задачи, предмет и основное содержание дисциплины, ее роль в системе подготовки студентов, а также в последующей практической деятельности.
2. Безопасность информации. Цель обеспечения защиты информации.
3. Система защиты информации.
4. Обеспечение защиты информации с точки зрения риска.
5. Критерии оценки защищенной системы. Общее решение задачи проектирования оптимальной системы защиты.
6. Нормативно-правовая база функционирования систем защиты информации.
7. Понятие угрозы. Классификация угроз.
8. Утечка, разглашение и несанкционированный доступ к конфиденциальной информации.
9. Характеристики информации.
10. Угрозы безопасности информации. Классификация методов и средств защиты информации. Технические методы защиты.

Задачи, решаемые техническими методами защиты. Методы решения данных задач.

Вопросы ко второй рубежной аттестации

1. Средства обеспечения информационной безопасности в Internet.
2. История развития, структура и основные понятия криптологии.
3. Криптография как основа информационной безопасности.
4. Подстановочные и перестановочные криптоалгоритмы.
5. Потоковые и блочные криптоалгоритмы.
6. Симметричные и асимметричные криптоалгоритмы.
7. Симметричные криптосистемы. Общая схема симметричной криптосистемы.
8. Модель криптосистемы с открытым ключом. Сертификация открытых ключей.
9. Алгоритм с открытым ключом RSA.
10. Электронная цифровая подпись. Применение хэш-функции.
11. Стандарты шифрования DES и AES.
12. Российский стандарт шифрования ГОСТ 28147-89.

НАИМЕНОВАНИЕ ЛАБОРАТОРНЫХ РАБОТ (ТЕКУЩИЙ КОНТРОЛЬ)

1. Лабораторная работа №1 Классические криптосистемы. Методы генерации больших простых чисел
2. Лабораторная работа №2. Алгоритм Advance Encryption System (AES)
3. Лабораторная работа №3. Ассиметричные алгоритмы шифрования

КОМПЛЕКТ ЗАДАНИЙ ДЛЯ ЛАБОРАТОРНЫХ РАБОТ

Вариант 1

1. Разработать алгоритм и составить программу, позволяющую закодировать любой текст одним из вышеизложенных методов и выполнить обратное преобразование. Язык программирования выбирается произвольно.
2. Осуществить вывод на экран или принтер полученной криптограммы.
3. Провести дешифрование данной криптограммы, в результате должен быть получен исходный текст.
4. Результаты работы оформить в виде отчета.

Вариант 2

1. Выбрать параметры генератора ПСЧ: A, C, T0, b в соответствии с вариантом.
2. Разработать программу шифрования и дешифрования текста.
3. Произвести шифрование исходного текста, получить шифрограмму, осуществить ее дешифрование и сравнение с исходным текстом. Рекомендуется для представления символов исходного текста использовать стандартную кодировку символов.
4. Произвести изменение одного или несколько параметров генератора случайных чисел, осуществить получение шифрограммы и сравнение ее с предыдущим вариантом.
5. Результаты работы оформить в виде отчета.

Критерии оценки ответов на лабораторные работы:

- не зачтено выставляется студенту, если *дан неполный ответ*, представляющий собой разрозненные знания по теме вопроса с существенными ошибками в определениях. Присутствуют фрагментарность, нелогичность изложения. Студент не осознает связь данного понятия, теории, явления с другими объектами дисциплины. Отсутствуют выводы, конкретизация и доказательность изложения. Речь неграмотная. Дополнительные и уточняющие вопросы преподавателя не приводят к коррекции ответа студента не только на поставленный вопрос, но и на другие вопросы дисциплины.

- зачтено выставляется студенту, если *дан полный, развернутый ответ* на поставленный вопрос, показана совокупность осознанных знаний об объекте, доказательно раскрыты основные положения темы; в ответе прослеживается четкая структура, логическая последовательность, отражающая сущность раскрываемых понятий, теорий, явлений. *Знание об объекте демонстрируется на фоне понимания его в системе данной науки и междисциплинарных связей.* Ответ изложен литературным языком в терминах науки. *Могут быть допущены недочеты в определении понятий, исправленные студентом самостоятельно в процессе ответа.*

ГРОЗНЕНСКИЙ ГОСУДАРСТВЕННЫЙ НЕФТЯНОЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТИМЕНИ АКАДЕМИКА М.Д.МИЛЛИОНЩИКОВА

Институт прикладных информационных технологий

Кафедра СС и СК

Вопросы к экзамену по дисциплине
«Методы и средства защиты информации в компьютерных сетях»

Вопросы к экзамену

1. Цель, задачи, предмет и основное содержание дисциплины, ее роль в системе подготовки студентов, а также в последующей практической деятельности.
2. Защита информации на электронных носителях информации.
3. Архивация с шифрованием.
4. Аппаратные и программные средства защиты в реализации Microsoft.
5. Принципы построения парольной защиты.
6. Традиционные средства защиты компьютерной информации и их недостатки.
7. Комплексный подход к построению систем безопасности.
8. Классификация сетевых атак по цели.
9. Меры и средства обеспечения информационной безопасности компьютерных сетей.
10. Задачи защиты информации в компьютерных сетях и методы их решения.
11. Понятие межсетевых экранов. Типы межсетевых экранов.
12. Защитные механизмы, реализуемые межсетевыми экранами.
13. Интеграция межсетевых экранов с другими средствами защиты.
14. Перспективные направления исследований в компьютерной безопасности.
15. Назначение Proxy-сервера.
16. Туннелирование на канальном уровне. Протоколы PPTP и L2TP.
17. Туннелирование на сетевом уровне. Архитектура IPSec.
18. Защита соединения на сеансовом уровне. Протоколы SSL и TLS.
19. Методы внедрения программных закладок.
20. Алгоритм цифровой подписи DSA.

Критерии оценки знаний студента на экзамене

Оценка «отлично» выставляется студенту, показавшему всесторонние, систематизированные,

глубокие знания учебной программы дисциплины и умение уверенно применять их на практике при решении конкретных задач, свободное и правильное обоснование принятых решений.

Оценка «хорошо» - выставляется студенту, если он твердо знает материал, грамотно и по существу излагает его, умеет применять полученные знания на практике, но допускает в ответе или в решении задач некоторые неточности, которые может устранить с помощью дополнительных вопросов преподавателя.

Оценка «удовлетворительно» - выставляется студенту, показавшему фрагментарный, разрозненный характер знаний, недостаточно правильные формулировки базовых понятий, нарушения логической последовательности в изложении программного материала, но при этом он владеет основными разделами учебной программы, необходимыми для дальнейшего обучения и может применять полученные знания по образцу в стандартной ситуации.

Оценка «неудовлетворительно» - выставляется студенту, который не знает большей части основного содержания учебной программы дисциплины, допускает грубые ошибки в формулировках основных понятий дисциплины и не умеет использовать полученные знания при решении типовых практических задач.

Экзаменационные билеты

ГРОЗНЕНСКИЙ ГОСУДАРСТВЕННЫЙ НЕФТЯНОЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ
имени академика М.Д. Миллионщикова

БИЛЕТ № 1

Дисциплина *Методы и средства защиты информации в компьютерных сетях*
Институт ИПИТ *профиль подготовки* _____ *семестр* __-__

1. Меры и средства обеспечения информационной безопасности компьютерных сетей.
2. Назначение Proxy-сервера.
3. Алгоритм цифровой подписи DSA.

И. о. зав. кафедрой СС и СК _____

ГРОЗНЕНСКИЙ ГОСУДАРСТВЕННЫЙ НЕФТЯНОЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ
имени академика М.Д. Миллионщикова

БИЛЕТ № 2

Дисциплина *Методы и средства защиты информации в компьютерных сетях*
Институт ИПИТ *профиль подготовки* _____ *семестр* __-__

1. Цель, задачи, предмет и основное содержание дисциплины, ее роль в системе подготовки студентов, а также в последующей практической деятельности.
2. Защитные механизмы, реализуемые межсетевыми экранами.
3. Комплексный подход к построению систем безопасности.

И. о. зав. кафедрой СС и СК _____

ГРОЗНЕНСКИЙ ГОСУДАРСТВЕННЫЙ НЕФТЯНОЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ
имени академика М.Д. Миллионщикова

БИЛЕТ № 3

Дисциплина *Методы и средства защиты информации в компьютерных сетях*
Институт ИПИТ *профиль подготовки* _____ *семестр* __-__

1. Перспективные направления исследований в компьютерной безопасности.
2. Понятие межсетевых экранов. Типы межсетевых экранов.
3. Традиционные средства защиты компьютерной информации и их недостатки.

И. о. зав. кафедрой СС и СК _____

ГРОЗНЕНСКИЙ ГОСУДАРСТВЕННЫЙ НЕФТЯНОЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ
имени академика М.Д. Миллионщикова

БИЛЕТ № 4

Дисциплина *Методы и средства защиты информации в компьютерных сетях*
Институт ИПИТ *профиль подготовки* _____ *семестр* __-__

1. Интеграция межсетевых экранов с другими средствами защиты.
2. Защита соединения на сеансовом уровне. Протоколы SSL и TLS.
3. Защита информации на электронных носителях информации.

И. о. зав. кафедрой СС и СК _____

ГРОЗНЕНСКИЙ ГОСУДАРСТВЕННЫЙ НЕФТЯНОЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ
имени академика М.Д. Миллионщикова

БИЛЕТ № 5

Дисциплина *Методы и средства защиты информации в компьютерных сетях*
Институт ИПИТ *профиль подготовки* _____ *семестр* __-__

1. Туннелирование на канальном уровне. Протоколы PPTP и L2TP.
2. Туннелирование на сетевом уровне. Архитектура IPSec
3. Понятие межсетевых экранов. Типы межсетевых экранов.

И. о. зав. кафедрой СС и СК _____

ГРОЗНЕНСКИЙ ГОСУДАРСТВЕННЫЙ НЕФТЯНОЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ
имени академика М.Д. Миллионщикова

БИЛЕТ № 6

Дисциплина *Методы и средства защиты информации в компьютерных сетях*
Институт ИПИТ *профиль подготовки* _____ *семестр* __-__

1. Классификация сетевых атак по цели.
2. Традиционные средства защиты компьютерной информации и их недостатки.
3. Интеграция межсетевых экранов с другими средствами защиты.

И. о. зав. кафедрой СС и СК _____

ГРОЗНЕНСКИЙ ГОСУДАРСТВЕННЫЙ НЕФТЯНОЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ
имени академика М.Д. Миллионщикова

БИЛЕТ № 7

Дисциплина *Методы и средства защиты информации в компьютерных сетях*
Институт ИПИТ *профиль подготовки* _____ *семестр* __-__

1. Принципы построения парольной защиты.
2. Методы внедрения программных закладок.
3. Аппаратные и программные средства защиты в реализации Microsoft.

И. о. зав. кафедрой СС и СК _____

ГРОЗНЕНСКИЙ ГОСУДАРСТВЕННЫЙ НЕФТЯНОЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ
имени академика М.Д. Миллионщикова

БИЛЕТ № 8

Дисциплина *Методы и средства защиты информации в компьютерных сетях*

Институт ИПИТ *профиль подготовки* _____ *семестр* __-__

1. Задачи защиты информации в компьютерных сетях и методы их решения.
2. Интеграция межсетевых экранов с другими средствами защиты..
3. Меры и средства обеспечения информационной безопасности компьютерных сетей.

И. о. зав. кафедрой СС и СК _____

ГРОЗНЕНСКИЙ ГОСУДАРСТВЕННЫЙ НЕФТЯНОЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ
имени академика М.Д. Миллионщикова

БИЛЕТ № 9

Дисциплина *Методы и средства защиты информации в компьютерных сетях*

Институт ИПИТ *профиль подготовки* _____ *семестр* __-__

1. Интеграция межсетевых экранов с другими средствами защиты.
2. Комплексный подход к построению систем безопасности.
3. Алгоритм цифровой подписи DSA.

И. о. зав. кафедрой СС и СК _____

ГРОЗНЕНСКИЙ ГОСУДАРСТВЕННЫЙ НЕФТЯНОЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ
имени академика М.Д. Миллионщикова

БИЛЕТ № 10

Дисциплина *Методы и средства защиты информации в компьютерных сетях*

Институт ИПИТ *профиль подготовки* _____ *семестр* __-__

1. Архивация с шифрованием.
2. Назначение Proxy-сервера.
3. Принципы построения парольной защиты.

И. о. зав. кафедрой СС и СК _____

ГРОЗНЕНСКИЙ ГОСУДАРСТВЕННЫЙ НЕФТЯНОЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ
имени академика М.Д. Миллионщикова

БИЛЕТ № 11

Дисциплина *Методы и средства защиты информации в компьютерных сетях*

Институт ИПИТ *профиль подготовки* _____ *семестр* __-__

1. Интеграция межсетевых экранов с другими средствами защиты.
2. Понятие межсетевых экранов. Типы межсетевых экранов.
3. Туннелирование на сетевом уровне. Архитектура IPSec.

И. о. зав. кафедрой СС и СК _____

ГРОЗНЕНСКИЙ ГОСУДАРСТВЕННЫЙ НЕФТЯНОЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ
имени академика М.Д. Миллионщикова

БИЛЕТ № 12

Дисциплина *Методы и средства защиты информации в компьютерных сетях*

Институт ИПИТ *профиль подготовки* _____ *семестр* __-__

1. Традиционные средства защиты компьютерной информации и их недостатки.
2. Понятие межсетевых экранов. Типы межсетевых экранов.
3. Принципы построения парольной защиты.

И. о. зав. кафедрой СС и СК _____

ГРОЗНЕНСКИЙ ГОСУДАРСТВЕННЫЙ НЕФТЯНОЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ
имени академика М.Д. Миллионщикова

БИЛЕТ № 13

Дисциплина *Методы и средства защиты информации в компьютерных сетях*

Институт ИПИТ *профиль подготовки* _____ *семестр* __-__

1. Меры и средства обеспечения информационной безопасности компьютерных сетей.
2. Защита соединения на сеансовом уровне. Протоколы SSL и TLS.
3. Интеграция межсетевых экранов с другими средствами защиты.

И. о. зав. кафедрой СС и СК _____

ГРОЗНЕНСКИЙ ГОСУДАРСТВЕННЫЙ НЕФТЯНОЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ
имени академика М.Д. Миллионщикова

БИЛЕТ № 14

Дисциплина *Методы и средства защиты информации в компьютерных сетях*

Институт ИПИТ *профиль подготовки* _____ *семестр* __-__

1. Архивация с шифрованием.
2. Перспективные направления исследований в компьютерной безопасности.
3. Цель, задачи, предмет и основное содержание дисциплины, ее роль в системе подготовки студентов, а также в последующей практической деятельности.

И. о. зав. кафедрой СС и СК _____

ГРОЗНЕНСКИЙ ГОСУДАРСТВЕННЫЙ НЕФТЯНОЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ
имени академика М.Д. Миллионщикова

БИЛЕТ № 15

Дисциплина *Методы и средства защиты информации в компьютерных сетях*

Институт ИПИТ *профиль подготовки* _____ *семестр* __-__

1. Меры и средства обеспечения информационной безопасности компьютерных сетей.
2. Классификация сетевых атак по цели.
3. Перспективные направления исследований в компьютерной безопасности.

И. о. зав. кафедрой СС и СК _____

ГРОЗНЕНСКИЙ ГОСУДАРСТВЕННЫЙ НЕФТЯНОЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ
имени академика М.Д. Миллионщикова

БИЛЕТ № 16

Дисциплина *Методы и средства защиты информации в компьютерных сетях*

Институт ИПИТ *профиль подготовки* _____ *семестр* __-__

1. Меры и средства обеспечения информационной безопасности компьютерных сетей.
2. Защита информации на электронных носителях информации.
3. Назначение Proxy-сервера.

И. о. зав. кафедрой СС и СК _____

ГРОЗНЕНСКИЙ ГОСУДАРСТВЕННЫЙ НЕФТЯНОЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ
имени академика М.Д. Миллионщикова

БИЛЕТ № 17

Дисциплина *Методы и средства защиты информации в компьютерных сетях*

Институт ИПИТ *профиль подготовки* _____ *семестр* __-__

1. Защитные механизмы, реализуемые межсетевыми экранами.
2. Туннелирование на канальном уровне. Протоколы PPTP и L2TP.
3. Комплексный подход к построению систем безопасности.

И. о. зав. кафедрой СС и СК _____

ГРОЗНЕНСКИЙ ГОСУДАРСТВЕННЫЙ НЕФТЯНОЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ
имени академика М.Д. Миллионщикова

БИЛЕТ № 18

Дисциплина *Методы и средства защиты информации в компьютерных сетях*

Институт ИПИТ *профиль подготовки* _____ *семестр* __-__

1. Назначение Proxy-сервера.
2. Классификация сетевых атак по цели.
3. Принципы построения парольной защиты.

И. о. зав. кафедрой СС и СК _____

ГРОЗНЕНСКИЙ ГОСУДАРСТВЕННЫЙ НЕФТЯНОЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ
имени академика М.Д. Миллионщикова

БИЛЕТ № 19

Дисциплина *Методы и средства защиты информации в компьютерных сетях*

Институт ИПИТ *профиль подготовки* _____ *семестр* __-__

1. Интеграция межсетевых экранов с другими средствами защиты.
2. Классификация сетевых атак по цели.
3. Цель, задачи, предмет и основное содержание дисциплины, ее роль в системе подготовки студентов, а также в последующей практической деятельности.

И. о. зав. кафедрой СС и СК _____

ГРОЗНЕНСКИЙ ГОСУДАРСТВЕННЫЙ НЕФТЯНОЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ
имени академика М.Д. Миллионщикова

БИЛЕТ № 20

Дисциплина *Методы и средства защиты информации в компьютерных сетях*

Институт ИПИТ *профиль подготовки* _____ *семестр* __-__

1. Алгоритм цифровой подписи DSA.
2. Защитные механизмы, реализуемые межсетевыми экранами.
3. Классификация сетевых атак по цели.

И. о. зав. кафедрой СС и СК _____