МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГРОЗНЕНСКИЙ ГОСУДАРСТВЕННЫЙ НЕФТЯНОЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ

имени академика М.Д. Миллионщикова

Кафедра «Информатика и вычислительная техника»

УТВЕРЖДЕН
на заседании кафедры
«08» 09 2025 г., протокол № 01
Заведующий кафедрой
___________________ Э.Д. Алисултанова

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ПО УЧЕБНОЙ ДИСЦИПЛИНЕ

«Методы и средства криптографической защиты информации»

Направление подготовки

10.03.01 Информационная безопасность

Направленность (профиль)

«Организация и технологии защиты информации (по отрасли или в сфере профессиональной деятельности)»

Квалификация

бакалавр

Составитель _______________ М.В. Магомадов

Грозный – 2025

ПАСПОРТ

ФОНДА ОЦЕНОЧНЫХ СРЕДСТВ ПО УЧЕБНОЙ ДИСЦИПЛИНЕ

«Методы и средства криптографической защиты информации»

№ п/п	Контролируемые разделы (темы) дисциплины	Код контролируемой компетенции (или ее части)	Наименование оценочного средства
1.	Математические основы	ОПК-8	Лабораторные работы Доклады с презентациями Письм. контрольная работа (аттестация) Зачет
2.	Потоковые средства шифрования	ОПК-8	Лабораторные работы Доклады с презентациями Письм. контрольная работа (аттестация) Зачет
3.	Симметричные криптосистемы	ОПК-8	Лабораторные работы Доклады с презентациями Письм. контрольная работа (аттестация) Зачет
4.	Асимметричные криптосистемы	ОПК-8	Лабораторные работы Доклады с презентациями Письм. контрольная работа (аттестация) Экзамен
5.	Средства хеширования	ОПК-8	Лабораторные работы Доклады с презентациями Письм. контрольная работа (аттестация) Экзамен
6.	ЭЦП	ОПК-8	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	Комплект заданий для выполнения лабораторных работ

		теоретических знаний и развития навыков самостоятельного проведения эксперимента	
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 / экзамен	Итоговая форма оценки знаний	Вопросы к зачету / экзамену

КОМПЛЕКТ ЗАДАНИЙ ДЛЯ ВЫПОЛНЕНИЯ ЛАБОРАТОРНЫХ РАБОТ

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

4 семестр

Лабораторная работа 1. Моноалфавитные и полиалфавитные шифры

Лабораторная работа 2. Шифры используемые в различные исторические периоды

Лабораторная работа 3. Генераторы псевдослучайной последовательности.

Лабораторная работа 4. Потоковые шифры.

Лабораторная работа 5. Шифрование данных в стандарте GSM

Лабораторная работа 6. Блочные шифры

Лабораторная работа7.Блочные шифры, используемые в гражданской и военных сферах деятельности

5 семестр

Лабораторная работа 1. Асимметричные средства шифрования

Лабораторная работа 2. Новые подходы к асимметричному шифрованию

Лабораторная работа 3. Алгоритмы хеш-функций

Лабораторная работа 4. ЭЦП

ТЕМЫ ДОКЛАДОВ С ПРЕЗЕНТАЦИЯМИ

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

4 семестр

Способ организации самостоятельной работы: подготовка презентации с устным докладом по заданной тематике.

Тематика докладов с презентациями:

1. Протоколы и их классификация.
2. Обмен ключами средствами симметричной криптографии.
3. Протоколы открытого распределения ключей.
4. Протоколы передачи секретного ключа по открытому каналу.
5. Аутентификация при входе в систему.
6. Вручение битов на хранение.
7. Бросание монеты по телефону.
8. Доказательство с нулевым разглашением.

9. Схемы аутентификации.
10. Методы разделения секрета.
11. Скрытый канал связи.
12. Мысленный покер.
13. Мысленный покер с тремя игроками.

5 семестр

1. Схема Фейстеля.
2. Операции по модулю.
3. Нелинейное преобразование.
4. Преобразование ключа.
5. Обучение на основе компьютерной программы
6. Простые и расширенные поля Галуа.
7. Преобразование ключа..
8. SP-сети.
9. Реализация и исследование стандарта.
10. Понятие дискретного алгоритма.
11. Криптостойкость.
12. Обучение на основе компьютерной программы.
13. Протоколы передачи секретного ключа по открытому каналу.

ГРОЗНЕНСКИЙ ГОСУДАРСТВЕННЫЙ НЕФТЯНОЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ ИМЕНИ АКАДЕМИКА М.Д. МИЛЛИОНЩИКОВА

Институт прикладных информационных технологий

Кафедра Информатика и вычислительная техника

Вопросы к зачету (экзамену) по дисциплине «Методы и средства криптографической защиты 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 экзамен / зачет – 1 теоретический вопрос, 1 задача.

4 семестр

Вопросы к зачету

К 1-ой рубежной аттестации:

1. История криптографии.
2. Классические алгоритмы шифрования.
3. Стойкость классических шифров.
4. Симметричное и ассиметричное шифрование.
5. Модель угрозы Долева-Яо.
6. Протокол Нидхема-Шредера.
7. Возможные атаки.
8. Понятия аутентификации сущности и аутентификации сообщений.
9. Ассиметричная версия протокола Нидхема-Шредера.
10. Обобщенный алгоритм Евклида.

Ко 2-ой рубежной аттестации:

11. Понятие группы. Фактор-группа. Теорема Лагранжа. Порядок группы.
12. Циклические группы.
13. Мультипликативные группы.
14. Конечные поля.
15. Поле с простым числом элементов.
16. Поле неприводимых полиномов.
17. Поля, построенные с помощью полиномиального базиса.
18. Модулярная арифметика в фактор-группе Zn.
19. Алгоритм модулярного возведения в степень. Аддитивные цепочки.
20. Решение линейного уравнения в фактор-группе Zn.

5 семестр

Вопросы к экзамену

К 1-ой рубежной аттестации:

1. Китайская теорема об остатках.
2. Функция Эйлера. Теоремы Ферма и Эйлера.
3. Понятие квадратичных вычетов. Символы Лежандра-Якоби.
4. Вычисление квадратных корней по простому модулю.

5. Вычисление квадратных корней по составному модулю.
6. Симметричные алгоритмы шифрования. Сеть Файстеля.
7. Алгоритм DES. Тройной DES.
8. Дифференциальный криптоанализ. Понятие характеристик.
9. Алгоритм AES. Основные принципы.
10. Основные режимы шифрования (электронная кодовая книга, сцепление блоков, обратная связь по шифртексту, обратная связь по выходу).

Ко 2-ой рубежной аттестации:

11. Протокол обмена ключами Диффи-Хеллмана. Возможные атаки.
12. Криптосистема RSA. Стойкость системы RSA. Задача о разложении чисел на простые множители.
13. Алгоритмы генерации больших простых чисел (Соловэй-Штрассен, Миллер-Рабин, ГОСТ 34.10-94).
14. Криптосистема Эль-Гамаля. Описание. Возможные атаки.
15. Битовая стойкость алгоритма RSA. Понятие оракула.
16. Методы защиты целостности данных.
17. Хэш-функции.
18. Ассиметричные методы защиты целостности.
19. Электронная цифровая подпись. Подпись RSA.
20. Цифровая подпись Эль-Гамаля. Потенциальные уязвимости.

При оценке ответа студента на экзамене / зачете 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 / зачете 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 криптографической защиты информации»

Билеты к рубежной аттестации

4 СЕМЕСТР

Грозненский государственный нефтяной технический университет им.акад. М.Д. Миллионщикова
Институт прикладных информационных технологий
«Семестр 4»
1-я рубежная аттестация
Дисциплина " Методы и средства криптографической защиты информации "
Билет № 1

1. История криптографии.
2.Классические алгоритмы шифрования.

Подпись преподавателя_____

Грозненский государственный нефтяной технический университет им.акад. М.Д. Миллионщикова
Институт прикладных информационных технологий
«Семестр 4»
1-я рубежная аттестация
Дисциплина " Методы и средства криптографической защиты информации "
Билет № 2

1. Стойкость классических шифров.
2.Симметричное и ассиметричное шифрование.

Подпись преподавателя_____

Грозненский государственный нефтяной технический университет им.акад. М.Д. Миллионщикова
Институт прикладных информационных технологий
«Семестр 4»
1-я рубежная аттестация
Дисциплина " Методы и средства криптографической защиты информации "
Билет № 3

1.Модель угрозы Долева-Яо.
2.Протокол Нидхема-Шредера.

Подпись преподавателя_____

Грозненский государственный нефтяной технический университет им.акад. М.Д. Миллионщикова
Институт прикладных информационных технологий
«Семестр 4»
1-я рубежная аттестация
Дисциплина " Методы и средства криптографической защиты информации "
Билет № 4

1.Возможные атаки.
2.Понятия аутентификации сущности и аутентификации сообщений.

Подпись преподавателя_____

Грозненский государственный нефтяной технический университет им.акад. М.Д. Миллионщикова
Институт прикладных информационных технологий
«Семестр 4»

1-я рубежная аттестация
Дисциплина " Методы и средства криптографической защиты информации "
Билет № 5

1.Ассиметричная версия протокола Нидхема-Шредера.
2.Обобщенный алгоритм Евклида.

Подпись преподавателя_____

Грозненский государственный нефтяной технический университет им.акад. М.Д. Миллионщикова
Институт прикладных информационных технологий
«Семестр 4»
1-я рубежная аттестация
Дисциплина " Методы и средства криптографической защиты информации "
Билет № 6

1.Понятия аутентификации сущности и аутентификации сообщений.
2.Ассиметричная версия протокола Нидхема-Шредера.

Подпись преподавателя_____

Грозненский государственный нефтяной технический университет им.акад. М.Д. Миллионщикова
Институт прикладных информационных технологий
«Семестр 4»
1-я рубежная аттестация
Дисциплина " Методы и средства криптографической защиты информации "
Билет № 7

1.Классические алгоритмы шифрования.
2.Стойкость классических шифров.

Подпись преподавателя_____

Грозненский государственный нефтяной технический университет им.акад. М.Д. Миллионщикова
Институт прикладных информационных технологий
«Семестр 4»
1-я рубежная аттестация
Дисциплина " Методы и средства криптографической защиты информации "
Билет № 8

1.Протокол Нидхема-Шредера.
2.Возможные атаки.

Подпись преподавателя_____

Грозненский государственный нефтяной технический университет им.акад. М.Д. Миллионщикова
Институт прикладных информационных технологий
«Семестр 4»
1-я рубежная аттестация
Дисциплина " Методы и средства криптографической защиты информации "
Билет № 9

1.Возможные атаки.
2.Понятия аутентификации сущности и аутентификации сообщений.

Подпись преподавателя_____

Грозненский государственный нефтяной технический университет им.акад. М.Д. Миллионщикова
Институт прикладных информационных технологий
«Семестр 4»
1-я рубежная аттестация
Дисциплина " Методы и средства криптографической защиты информации "

Билет № 10

1.Понятия аутентификации сущности и аутентификации сообщений.

2.Ассиметричная версия протокола Нидхема-Шредера.

Подпись преподавателя_____

Грозненский государственный нефтяной технический университет им.акад. М.Д. Миллионщикова
Институт прикладных информационных технологий
«Семестр 4»
2-я рубежная аттестация
Дисциплина " Методы и средства криптографической защиты информации "
Билет № 1

1.Понятие группы. Фактор-группа. Теорема Лагранжа. Порядок группы.

2.Циклические группы.

Подпись преподавателя_____

Грозненский государственный нефтяной технический университет им.акад. М.Д. Миллионщикова
Институт прикладных информационных технологий
«Семестр 4»
2-я рубежная аттестация
Дисциплина " Методы и средства криптографической защиты информации "
Билет № 2

1.Мультипликативные группы.

2.Конечные поля.

Подпись преподавателя_____

Грозненский государственный нефтяной технический университет им.акад. М.Д. Миллионщикова
Институт прикладных информационных технологий
«Семестр 4»
2-я рубежная аттестация
Дисциплина " Методы и средства криптографической защиты информации "
Билет № 3

1.Поле с простым числом элементов.

2.Поле неприводимых полиномов.

Подпись преподавателя_____

Грозненский государственный нефтяной технический университет им.акад. М.Д. Миллионщикова
Институт прикладных информационных технологий
«Семестр 4»
2-я рубежная аттестация
Дисциплина " Методы и средства криптографической защиты информации "
Билет № 4

1.Поля, построенные с помощью полиномиального базиса.

2.Модулярная арифметика в фактор-группе Zn.

Подпись преподавателя_____

Грозненский государственный нефтяной технический университет им.акад. М.Д. Миллионщикова
Институт прикладных информационных технологий
«Семестр 4»
2-я рубежная аттестация

Дисциплина " Методы и средства криптографической защиты информации "
Билет № 5

1.Алгоритм модулярного возведения в степень. Аддитивные цепочки.
2.Решение линейного уравнения в фактор-группе Zn.

Подпись преподавателя_____

Грозненский государственный нефтяной технический университет им.акад. М.Д. Миллионщикова
Институт прикладных информационных технологий
«Семестр 4»
2-я рубежная аттестация
Дисциплина " Методы и средства криптографической защиты информации "
Билет № 6

1.Циклические группы.
2.Мультипликативные группы.

Подпись преподавателя_____

Грозненский государственный нефтяной технический университет им.акад. М.Д. Миллионщикова
Институт прикладных информационных технологий
«Семестр 4»
2-я рубежная аттестация
Дисциплина " Методы и средства криптографической защиты информации "
Билет № 7

1.Конечные поля.
2.Поле с простым числом элементов.

Подпись преподавателя_____

Грозненский государственный нефтяной технический университет им.акад. М.Д. Миллионщикова
Институт прикладных информационных технологий
«Семестр 4»
2-я рубежная аттестация
Дисциплина " Методы и средства криптографической защиты информации "
Билет № 8

1.Поле неприводимых полиномов.
2.Поля, построенные с помощью полиномиального базиса.

Подпись преподавателя_____

Грозненский государственный нефтяной технический университет им.акад. М.Д. Миллионщикова
Институт прикладных информационных технологий
«Семестр 4»
2-я рубежная аттестация
Дисциплина " Методы и средства криптографической защиты информации "
Билет № 9

1.Модулярная арифметика в фактор-группе Zn.
2.Алгоритм модулярного возведения в степень. Аддитивные цепочки.

Подпись преподавателя_____

Грозненский государственный нефтяной технический университет им.акад. М.Д. Миллионщикова
Институт прикладных информационных технологий
«Семестр 4»
2-я рубежная аттестация
Дисциплина " Методы и средства криптографической защиты информации "
Билет № 10

1.Алгоритм модулярного возведения в степень. Аддитивные цепочки.
2.Решение линейного уравнения в фактор-группе Zn.

Подпись преподавателя_____

ЗАЧЕТНО-ЭКЗАМЕНАЦИОННЫЕ МАТЕРИАЛЫ

4 СЕМЕСТР, ЗАЧЕТ

Грозненский государственный нефтяной технический университет им.акад. М.Д. Миллионщикова
Институт прикладных информационных технологий
«Семестр 4»
Дисциплина " Методы и средства криптографической защиты информации "
Билет № 1

1. История криптографии.
2.Классические алгоритмы шифрования.

Подпись преподавателя_____ Подпись заведующего кафедрой_____

Грозненский государственный нефтяной технический университет им.акад. М.Д. Миллионщикова
Институт прикладных информационных технологий
«Семестр 4»
Дисциплина " Методы и средства криптографической защиты информации "
Билет № 2

1. Стойкость классических шифров.
2.Симметричное и ассиметричное шифрование.

Подпись преподавателя_____ Подпись заведующего кафедрой_____ _

Грозненский государственный нефтяной технический университет им.акад. М.Д. Миллионщикова
Институт прикладных информационных технологий
«Семестр 4»
Дисциплина " Методы и средства криптографической защиты информации "
Билет № 3

1.Модель угрозы Долева-Яо.
2.Протокол Нидхема-Шредера.

Подпись преподавателя_____ Подпись заведующего кафедрой_____ _

Грозненский государственный нефтяной технический университет им.акад. М.Д. Миллионщикова
Институт прикладных информационных технологий
«Семестр 4»
Дисциплина " Методы и средства криптографической защиты информации "
Билет № 4

1.Возможные атаки.
2.Понятия аутентификации сущности и аутентификации сообщений.

Подпись преподавателя_____ Подпись заведующего кафедрой_____

Грозненский государственный нефтяной технический университет им.акад. М.Д. Миллионщикова
Институт прикладных информационных технологий
«Семестр 4»
Дисциплина " Методы и средства криптографической защиты информации "
Билет № 5

1.Ассиметричная версия протокола Нидхема-Шредера.
2.Обобщенный алгоритм Евклида.

Подпись преподавателя_____ Подпись заведующего кафедрой_____

Грозненский государственный нефтяной технический университет им.акад. М.Д. Миллионщикова
Институт прикладных информационных технологий
«Семестр 4»
Дисциплина " Методы и средства криптографической защиты информации "
Билет № 5

1.Алгоритм модулярного возведения в степень. Аддитивные цепочки.
2.Решение линейного уравнения в фактор-группе Zn.

Подпись преподавателя_____ Подпись заведующего кафедрой_____

Грозненский государственный нефтяной технический университет им.акад. М.Д. Миллионщикова
Институт прикладных информационных технологий
«Семестр 4»
Дисциплина " Методы и средства криптографической защиты информации "
Билет № 6

1.Циклические группы.
2.Мультипликативные группы.

Подпись преподавателя_____ Подпись заведующего кафедрой_____

Грозненский государственный нефтяной технический университет им.акад. М.Д. Миллионщикова
Институт прикладных информационных технологий
«Семестр 4»
Дисциплина " Методы и средства криптографической защиты информации "
Билет № 7

1.Конечные поля.
2.Поле с простым числом элементов.

Подпись преподавателя_____ Подпись заведующего кафедрой_____

Грозненский государственный нефтяной технический университет им.акад. М.Д. Миллионщикова
Институт прикладных информационных технологий
«Семестр 4»
Дисциплина " Методы и средства криптографической защиты информации "
Билет № 8

1.Поле неприводимых полиномов.
2.Поля, построенные с помощью полиномиального базиса.

Подпись преподавателя_____ Подпись заведующего кафедрой_____

Грозненский государственный нефтяной технический университет им.акад. М.Д. Миллионщикова
Институт прикладных информационных технологий
«Семестр 4»
Дисциплина " Методы и средства криптографической защиты информации "
Билет № 9

1.Модулярная арифметика в фактор-группе Zn.
2.Алгоритм модулярного возведения в степень. Аддитивные цепочки.

Подпись преподавателя_____ Подпись заведующего кафедрой_____

Грозненский государственный нефтяной технический университет им.акад. М.Д. Миллионщикова
Институт прикладных информационных технологий

«Семестр 4»
Дисциплина " Методы и средства криптографической защиты информации "
Билет № 10

1.Алгоритм модулярного возведения в степень. Аддитивные цепочки.
2.Решение линейного уравнения в фактор-группе Zn.

Подпись преподавателя_____ Подпись заведующего кафедрой_____

---

5 СЕМЕСТР, ЭКЗАМЕН

Грозненский государственный нефтяной технический университет им.акад. М.Д. Миллионщикова
Институт прикладных информационных технологий
«Семестр 5»
Дисциплина " Методы и средства криптографической защиты информации "
Билет № 1

1.Схема Фейстеля.
2.Операции по модулю..

Подпись преподавателя_____ Подпись заведующего кафедрой_____

Грозненский государственный нефтяной технический университет им.акад. М.Д. Миллионщикова
Институт прикладных информационных технологий
«Семестр 5»
Дисциплина " Методы и средства криптографической защиты информации "
Билет № 2

1.Нелинейное преобразование.
2.Преобразование ключа.

Подпись преподавателя_____ Подпись заведующего кафедрой_____

Грозненский государственный нефтяной технический университет им.акад. М.Д. Миллионщикова
Институт прикладных информационных технологий
«Семестр 5»
Дисциплина " Методы и средства криптографической защиты информации "
Билет № 3

1.Обучение на основе компьютерной программы
2.Простые и расширенные поля Галуа.

Подпись преподавателя_____ Подпись заведующего кафедрой_____

Грозненский государственный нефтяной технический университет им.акад. М.Д. Миллионщикова
Институт прикладных информационных технологий
«Семестр 5»
Дисциплина " Методы и средства криптографической защиты информации "
Билет № 4

1.Преобразование ключа..
2.SP-сети.

Подпись преподавателя_____ Подпись заведующего кафедрой_____

Грозненский государственный нефтяной технический университет им.акад. М.Д. Миллионщикова
Институт прикладных информационных технологий
«Семестр 5»
Дисциплина " Методы и средства криптографической защиты информации "
Билет № 5

1.Реализация и исследование стандарта.
2.Понятие дискретного алгоритма.
Подпись преподавателя_____ Подпись заведующего кафедрой_____

Грозненский государственный нефтяной технический университет им.акад. М.Д. Миллионщикова
Институт прикладных информационных технологий
«Семестр 5»
Дисциплина " Методы и средства криптографической защиты информации "
Билет № 6

1.Криптостойкость.
2.Обучение на основе компьютерной программы.
Подпись преподавателя_____ Подпись заведующего кафедрой_____

Грозненский государственный нефтяной технический университет им.акад. М.Д. Миллионщикова
Институт прикладных информационных технологий
«Семестр 5»
Дисциплина " Методы и средства криптографической защиты информации "
Билет № 7

1.Обучение на основе компьютерной программы.
2.Протоколы передачи секретного ключа по открытому каналу.
Подпись преподавателя_____ Подпись заведующего кафедрой_____

Грозненский государственный нефтяной технический университет им.акад. М.Д. Миллионщикова
Институт прикладных информационных технологий
«Семестр 5»
Дисциплина " Методы и средства криптографической защиты информации "
Билет № 8

1.SP-сети.
2.Реализация и исследование стандарта.
Подпись преподавателя_____ Подпись заведующего кафедрой_____

Грозненский государственный нефтяной технический университет им.акад. М.Д. Миллионщикова
Институт прикладных информационных технологий
«Семестр 5»
Дисциплина " Методы и средства криптографической защиты информации "
Билет № 9

1.Обучение на основе компьютерной программы
2.Простые и расширенные поля Галуа.
Подпись преподавателя_____ Подпись заведующего кафедрой_____

Грозненский государственный нефтяной технический университет им.акад. М.Д. Миллионщикова
Институт прикладных информационных технологий
«Семестр 5»
Дисциплина " Методы и средства криптографической защиты информации "
Билет № 10

1.Операции по модулю.
2.Нелинейное преобразование.
Подпись преподавателя_____ Подпись заведующего кафедрой_____
