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

Криптографические методы защиты и средства обеспечения информационной безопасности инфокоммуникаций

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

«Криптографические методы защиты и средства обеспечения информационной безопасности инфокоммуникаций»

№ п/п	Контролируемые разделы (темы) дисциплины	Код контролируемой компетенции (или ее части)	Наименование оценочного средства
1.	Введение	ПК-9 ПК-9.1	Опрос
2.	Пробой жидких, газообразных и твердых диэлектриков	ПК-9 ПК-9.3	Обсуждение сообщений
3.	Потери в диэлектриках. Сопротивление диэлектрика	ПК-9 ПК-9.2	Опрос
4.	Активные и пассивные диэлектрики. Основные компоненты активных диэлектриков, их свойства.	ПК-9 ПК-9.1	Опрос
5.	Конденсаторы. Конструкция конденсаторов.	ПК-9 ПК-9.3	Обсуждение сообщений
6.	Классификация полупроводниковых материалов по составу и свойствам.	ПК-9 ПК-9.3	Обсуждение сообщений
7.	Магнитные характеристики. Физическая природа магнитных эффектов	ПК-9 ПК-9.1	Опрос
8.	Исследование электропроводности диэлектриков	ПК-9 ПК-9.2	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

Шестой семестр

Вопросы к первой рубежной аттестации

1. Зависимость электропроводности диэлектриков от температуры.
2. Зависимость электропроводности диэлектриков от напряженности, влаги, времени эксплуатации.
3. Диэлектрические потери. Векторная диаграмма токов в диэлектрике; tg□, мощность потерь в диэлектрике.
4. Диэлектрические потери в нейтральных диэлектриках.
5. Диэлектрические потери в полярных диэлектриках.
6. Влияние напряжения и влаги на диэлектрические потери.
7. Пробой диэлектриков. Механизм пробоя.
8. Пробой газов в однородном поле.
9. Пробой газов в неоднородном поле.

Вопросы ко второй рубежной аттестации

1. Пробой жидких диэлектриков.
2. Пробой твердых диэлектриков.
3. Механические и тепловые характеристики электротехнических материалов.
4. Нагревостойкость, классы нагревостойкости ЭТМ.
5. Радиационная стойкость ЭТМ.
6. Газообразные диэлектрики.
7. Жидкие диэлектрики.
8. В.М.С. (высокомолекулярные соединения), классификация по природе, полимеризационные и поликонденсационные В.М.С.
9. Неполярные полимерные материалы.
10. Полярные полимерные материалы. Пластмассы.

Седьмой семестр

Вопросы к первой рубежной аттестации

1. Основные понятия, обозначения и задачи криптографии.

2. Исторические примеры криптосистем.
3. Основные принципы криптографической защиты информации. Общая схема системы защиты информации.
4. Функции шифрования. Односторонние функции. Простейшие шифры и их клас-сификация.
5. Основные требования к шифрам, к криптографическим системам.
6. Абсолютно стойкие (совершенные) шифры. Криптостойкость алгоритма шифро-вания. Особенности симметричных криптосистем.
7. Метод простой подстановки (замены). Метод перестановки. Метод блочных шифров.
8. Метод гаммирования. Метод шифрования на основе теоремы Эйлера-Ферма.
9. Композиция шифров.
10. Стандарт криптосистемы США DES.
11. Стандарт криптосистемы России – ГОСТ 28147-89. Системы защиты с открытым ключом.
12. Криптосистема RSA.
13. Теоретико-числовые алгоритмы и их сложность. Методы дискретного логариф-мирования.

Вопросы ко второй рубежной аттестации

1. Метод простой подстановки (замены). Метод перестановки. Метод блочных шифров.
2. Метод гаммирования. Метод шифрования на основе теоремы Эйлера-Ферма.
3. Композиция шифров.
4. Стандарт криптосистемы США DES.
5. Стандарт криптосистемы России – ГОСТ 28147-89. Системы защиты с открытым ключом.
6. Криптосистема RSA.
7. Теоретико-числовые алгоритмы и их сложность. Методы дискретного логариф-мирования.
8. Система защиты Диффи-Хеллмана. Система защиты информации на основе за-данного рюкзака.
9. Протоколы распределения секретных ключей. Основные цели протокола распре-деления ключей. Протокол Отвэй-Риса.
10. Протоколы распределения секретных ключей. Основные цели протокола распре-деления ключей. Цербер.
11. Арифметика остатков. Сравнение по модулю. Решение уравнения $ax = b \pmod N$.
12. Функция Эйлера. Мультипликативные обратные по модулю N. Теорема Лагранжа. Малая теорема Ферма. Применение в криптографии.

    Алгоритм Евклида. Китайская теорема об остатках. Расширенный алгоритм Ев-клида. Применение в криптографии

НАИМЕНОВАНИЕ ЛАБОРАТОРНЫХ РАБОТ (ТЕКУЩИЙ КОНТРОЛЬ)

1. Лабораторная работа №1. Изучение температурной зависимости удельногосопротивления материалов.
2. Лабораторная работа №2. Определение удельной проводимости материалов.Изготовление проволочных резисторов с требуемыми параметрами.
3. Лабораторная работа №3. Определение диэлектрической проницаемости различных диэлектрических материалов.
4. Лабораторная работа №4. Изучения механизмов пробоя и диэлектрических потерь в диэлектриках.

КОМПЛЕКТ ЗАДАНИЙ ДЛЯ ЛАБОРАТОРНЫХ РАБОТ

Вариант 1

Зашифровать слово с помощью шифра Цезаря Ход выполнения работы В приложении MS Excel создать книгу, содержащую пронумерованные символы русского алфавита:

1) в первом столбце ввести номера от 0 до 32;

2) во втором столбце – символы русского алфавита по порядку;

3) в третьем столбце – снова нумерацию от 0 до 32.

Зашифровать слово «ГЛАГОЛ» с помощью шифра Цезаря с выбранным ключом, для чего:

1) ввести шифруемое слово побуквенно в ячейки первой строки (можно использовать любые незаполненные ячейки листа);

2) строкой ниже получить числовой код символов шифруемого слова с помощью функции ВПР:

а) первым параметром (Искомое_значение) функции назначить ссылку на ячейку с текущим символом шифруемого слова;

б) вторым параметром (Таблица) функции назначить ссылку на таблицу с алфавитом, начиная со второго столбца (столбцы B и C), ссылку на таблицу сделать абсолютной, нажав кнопку F4;

в) значение третьего параметра (Номер_столбца) задать равным 2 (чтобы данные брались из второго столбца выделенного на предыдущем этапе диапазона с цифрами);

г) в качестве значения четвертого параметра (Интервальный_просмотр) ввести слово «ЛОЖЬ» (чтобы поиск был точным). Например: =ВПР(F1;$B$1:$C$33;2;ЛОЖЬ).

Вариант 2

Расшифровать криптограмму, полученную с помощью шифра Цезаря Для того, чтобы расшифровать криптограмму выбранным ключом, необходимо:

1) ввести побуквенно текст криптограммы в ячейки одной строки;

2) строкой ниже получить числовой код символов шифруемого слова с помощью функции ВПР;

3) строкой ниже получить код символов расшифрованного текста, вычтя по модулю 33 (по количеству букв в алфавите) значение ключа из полученного кода текущего символа криптограммы, используя функцию ОСТАТ;

4) строкой ниже с помощью функции ВПР перевести полученный код криптограммы в символьный вид.

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 зачету по дисциплине
«Криптографические методы защиты и средства обеспечения информационной безопасности инфокоммуникаций»

Вопросы к зачету

1. Алгоритм Эль Гамаль (асимметричная криптография).
2. Комбинирующий поточный шифр с элементом памяти.
3. Код аутентификации сообщения (MAC). Способы построения MAC. HMAC.
4. Динамический поточный шифр.
5. Определение блочного шифрования. Блок информации. Ключ алгоритма.
6. Абсолютно симметричный блочный шифр.
7. Аутентификация пользователя. Типы систем аутентификации (на симметричных и асимметричных криптосистемах, на сертификатах).
8. Обратимые операции в блочном шифровании.

9. Kerberos. Протокол распределения ключей.
10. Необратимые операции в блочном шифровании.
11. Распространение ключей. Протоколы, основанные на использовании симметричной
12. криптосистемы и случайных параметров.
13. Сети блочных шифров, ветви сети, раунд сети, образующая функция. SP-сеть,
14. KASLT-сеть.
15. Распространение ключей. 3-х этапный протокол Шамира (Shamir).
16. Классическая структура сети Фейстеля. Ветви сети, материал ключа, раунд сети, образующая функция.
17. Распространение ключей. Протокол Needham-Schroeder.
18. Абсолютно симметричная сеть Фейстеля. Модификация сети Фейстеля для
19. большего числа ветвей: тип 1 – размер блока, ветви сети, материал ключа, рунд сети, образующая функция.
20. Распространение ключей. Протоколы на основе асимметричных криптосистем.
21. Алгоритм RSA (асимметричная криптография).
22. Видовые демаскирующие признаки.
23. Сигнальные демаскирующие признаки.
24. Демаскирующие признаки веществ.
25. Состав и характеристики видовых, сигнальных признаков, признаков веществ.
26. Классификация демаскирующих признаков.

Критерии оценки знаний студента на зачете:

- 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.*

Билеты к зачету

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

БИЛЕТ № 1

Дисциплина Криптографические методы защиты и средства обеспечения информационной безопасности инфокоммуникаций
Институт ИПИТ *профиль подготовки* _____ *семестр* __-__

1. Алгоритм Эль Гамаль (асимметричная криптография).
2. Kerberos. Протокол распределения ключей.
3. Сети блочных шифров, ветви сети, раунд сети, образующая функция. SP-сеть, KASLT-сеть.

И. о. зав. кафедрой СС и СК _____

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

БИЛЕТ № 2

Дисциплина Криптографические методы защиты и средства обеспечения информационной безопасности инфокоммуникаций
Институт ИПИТ *профиль подготовки* _____ *семестр* __-__

1. Алгоритм RSA (асимметричная криптография).
2. Сигнальные демаскирующие признаки.
3. Состав и характеристики видовых, сигнальных признаков, признаков веществ.

И. о. зав. кафедрой СС и СК _____

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

БИЛЕТ № 3

Дисциплина Криптографические методы защиты и средства обеспечения информационной безопасности инфокоммуникаций
Институт ИПИТ *профиль подготовки* _____ *семестр* __-__

1. Аутентификация пользователя. Типы систем аутентификации (на симметричных и асимметричных криптосистемах, на сертификатах).
2. Криптосистемы и случайных параметров.
3. KASLT-сеть.

И. о. зав. кафедрой СС и СК _____

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

БИЛЕТ № 4

Дисциплина Криптографические методы защиты и средства обеспечения информационной безопасности инфокоммуникаций
Институт ИПИТ *профиль подготовки* _____ *семестр* __-__

1. Динамический поточный шифр.
2. Распространение ключей. Протоколы, основанные на использовании симметричной криптосистемы и случайных параметров.
3. Распространение ключей. Протокол Needham-Schroeder.

И. о. зав. кафедрой СС и СК _____

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

БИЛЕТ № 5

Дисциплина Криптографические методы защиты и средства обеспечения информационной безопасности инфокоммуникаций
Институт ИПИТ *профиль подготовки* _____ *семестр* __-__

1. Обратимые операции в блочном шифровании.
2. Демаскирующие признаки веществ.
3. Сети, образующая функция.

И. о. зав. кафедрой СС и СК _____

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

БИЛЕТ № 6

Дисциплина Криптографические методы защиты и средства обеспечения информационной безопасности инфокоммуникаций
Институт ИПИТ *профиль подготовки* _____ *семестр* __-__

1. Абсолютно симметричный блочный шифр.
2. Код аутентификации сообщения (MAC). Способы построения MAC. HMAC.
3. Динамический поточный шифр.

И. о. зав. кафедрой СС и СК _____

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

БИЛЕТ № 7

Дисциплина Криптографические методы защиты и средства обеспечения информационной безопасности инфокоммуникаций
Институт ИПИТ *профиль подготовки* _____ *семестр* __-__

1. Распространение ключей. 3-х этапный протокол Шамира (Shamir).
2. Видовые демаскирующие признаки.
3. Обратимые операции в блочном шифровании.

И. о. зав. кафедрой СС и СК _____

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

БИЛЕТ № 8

Дисциплина Криптографические методы защиты и средства обеспечения информационной безопасности инфокоммуникаций
Институт ИПИТ *профиль подготовки* _____ *семестр* __-__

1. Абсолютно симметричный блочный шифр.
2. Алгоритм Эль Гамаль (асимметричная криптография)..
3. Абсолютно симметричная сеть Фейстеля. Модификация сети Фейстеля для большего числа ветвей: тип 1 – размер блока, ветви сети, материал ключа, рунд сети, образующая функция.

И. о. зав. кафедрой СС и СК _____

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

БИЛЕТ № 9

Дисциплина Криптографические методы защиты и средства обеспечения информационной безопасности инфокоммуникаций
Институт ИПИТ *профиль подготовки* _____ *семестр* __-__

1. Распространение ключей. Протоколы, основанные на использовании симметричной
2. Аутентификация пользователя. Типы систем аутентификации (на симметричных и асимметричных криптосистемах, на сертификатах).
3. Динамический поточный шифр.

И. о. зав. кафедрой СС и СК _____

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

БИЛЕТ № 10

Дисциплина Криптографические методы защиты и средства обеспечения информационной безопасности инфокоммуникаций
Институт ИПИТ *профиль подготовки* _____ *семестр* __-__

1. Комбинирующий поточный шифр с элементом памяти.
2. Код аутентификации сообщения (MAC). Способы построения MAC. HMAC.
3. Алгоритм RSA (асимметричная криптография).

И. о. зав. кафедрой СС и СК _____

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

БИЛЕТ № 11

Дисциплина Криптографические методы защиты и средства обеспечения информационной безопасности инфокоммуникаций
Институт ИПИТ *профиль подготовки* _____ *семестр* __-__

1. Демаскирующие признаки веществ.
2. Состав и характеристики видовых, сигнальных признаков, признаков веществ.
3. Классификация демаскирующих признаков.

И. о. зав. кафедрой СС и СК _____

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

БИЛЕТ № 12

Дисциплина Криптографические методы защиты и средства обеспечения информационной безопасности инфокоммуникаций
Институт ИПИТ *профиль подготовки* _____ *семестр* __-__

1. Динамический поточный шифр.
2. Распространение ключей. Протокол Needham-Schroeder.
3. Видовые демаскирующие признаки.

И. о. зав. кафедрой СС и СК _____

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

БИЛЕТ № 13

Дисциплина Криптографические методы защиты и средства обеспечения информационной безопасности инфокоммуникаций
Институт ИПИТ *профиль подготовки* _____ *семестр* __-__

1. Необратимые операции в блочном шифровании.
2. Аутентификация пользователя. Типы систем аутентификации (на симметричных и асимметричных криптосистемах, на сертификатах).
3. Динамический поточный шифр.

И. о. зав. кафедрой СС и СК _____

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

БИЛЕТ № 14

Дисциплина Криптографические методы защиты и средства обеспечения информационной безопасности инфокоммуникаций
Институт ИПИТ *профиль подготовки* _____ *семестр* __-__

1. Сети блочных шифров, ветви сети, раунд сети, образующая функция. SP-сеть,
2. KASLT-сеть.
3. Видовые демаскирующие признаки.
4. Распространение ключей. Протоколы на основе асимметричных криптосистем.

И. о. зав. кафедрой СС и СК _____

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

БИЛЕТ № 15

Дисциплина Криптографические методы защиты и средства обеспечения информационной безопасности инфокоммуникаций
Институт ИПИТ *профиль подготовки* _____ *семестр* __-__

1. Распространение ключей. Протокол Needham-Schroeder.
2. Абсолютно симметричная сеть Фейстеля. Модификация сети Фейстеля для большего числа ветвей: тип 1 – размер блока, ветви сети, материал ключа, рунд сети, образующая функция.
3. Распространение ключей. 3-х этапный протокол Шамира (Shamir).

И. о. зав. кафедрой СС и СК _____

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

БИЛЕТ № 16

Дисциплина Криптографические методы защиты и средства обеспечения информационной безопасности инфокоммуникаций
Институт ИПИТ *профиль подготовки* _____ *семестр* __-__

1. Распространение ключей. Протоколы на основе асимметричных криптосистем.
2. Алгоритм RSA (асимметричная криптография).
3. Распространение ключей. Протокол Needham-Schroeder.

И. о. зав. кафедрой СС и СК _____

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

БИЛЕТ № 17

Дисциплина Криптографические методы защиты и средства обеспечения информационной безопасности инфокоммуникаций
Институт ИПИТ *профиль подготовки* _____ *семестр* __-__

1. Классификация демаскирующих признаков.
2. Динамический поточный шифр.
3. Комбинирующий поточный шифр с элементом памяти.

И. о. зав. кафедрой СС и СК _____

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

БИЛЕТ № 18

Дисциплина Криптографические методы защиты и средства обеспечения информационной безопасности инфокоммуникаций
Институт ИПИТ *профиль подготовки* _____ *семестр* __-__

1. Необратимые операции в блочном шифровании.
2. Сигнальные демаскирующие признаки.
3. Алгоритм Эль Гамаль (асимметричная криптография).

И. о. зав. кафедрой СС и СК _____

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

БИЛЕТ № 19

Дисциплина Криптографические методы защиты и средства обеспечения информационной безопасности инфокоммуникаций
Институт ИПИТ *профиль подготовки* _____ *семестр* __-__

1. Определение блочного шифрования. Блок информации. Ключ алгоритма.
2. Абсолютно симметричный блочный шифр.
3. Аутентификация пользователя. Типы систем аутентификации (на симметричных и асимметричных криптосистемах, на сертификатах).

И. о. зав. кафедрой СС и СК _____

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

БИЛЕТ № 20

Дисциплина Криптографические методы защиты и средства обеспечения информационной безопасности инфокоммуникаций
Институт ИПИТ *профиль подготовки* _____ *семестр* __-__

1. Распространение ключей. 3-х этапный протокол Шамира (Shamir).
2. Классическая структура сети Фейстеля. Ветви сети, материал ключа, раунд сети, образующая функция.
3. Распространение ключей. Протокол Needham-Schroeder.

И. о. зав. кафедрой СС и СК _____

ГРОЗНЕНСКИЙ ГОСУДАРСТВЕННЫЙ НЕФТЯНОЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТИМЕНИ АКАДЕМИКА М.Д.МИЛЛИОНЩИКОВА

Институт прикладных информационных технологий

Кафедра Сети связи и системы коммутации

Вопросы к экзамену по дисциплине
««Криптографические методы защиты и средства обеспечения информационной безопасности»

Вопросы к экзамену

13. Основные понятия, обозначения и задачи криптографии.
14. Исторические примеры криптосистем.

15. Основные принципы криптографической защиты информации. Общая схема системы защиты информации.
16. Функции шифрования. Односторонние функции. Простейшие шифры и их классификация.
17. Основные требования к шифрам, к криптографическим системам.
18. Абсолютно стойкие (совершенные) шифры. Криптостойкость алгоритма шифрования. Особенности симметричных криптосистем.
19. Метод простой подстановки (замены). Метод перестановки. Метод блочных шифров.
20. Метод гаммирования. Метод шифрования на основе теоремы Эйлера-Ферма.
21. Композиция шифров.
22. Стандарт криптосистемы США DES.
23. Стандарт криптосистемы России – ГОСТ 28147-89. Системы защиты с открытым ключом.
24. Криптосистема RSA.
25. Теоретико-числовые алгоритмы и их сложность. Методы дискретного логарифмирования.
26. Система защиты Диффи-Хеллмана. Система защиты информации на основе заданного рюкзака.
27. Протоколы распределения секретных ключей. Основные цели протокола распределения ключей. Протокол Отвэй-Риса.
28. Протоколы распределения секретных ключей. Основные цели протокола распределения ключей. Цербер.
29. Арифметика остатков. Сравнение по модулю. Решение уравнения $ax = b \pmod N$.
30. Функция Эйлера. Мультипликативные обратные по модулю N. Теорема Лагранжа. Малая теорема Ферма. Применение в криптографии.
31. Алгоритм Евклида. Китайская теорема об остатках. Расширенный алгоритм Евклида. Применение в криптографии.
32. Криптосистема с открытым ключом. Криптографическая односторонняя функция. Важнейшие криптографические односторонние функции.
33. Оценка сложности задач. Сложность алгоритма: Полиноминальная, экспоненциальная, субэкспоненциальная Оракул. Сравнительный анализ сложности криптографических алгоритмов (без доказательства).
34. Алгоритм RSA. Шифрование в RSA. Дешифрование в RSA. Доказательство алгоритма.

35. Алгоритм RSA. Задача криптоаналитика. Криптостойкость RSA
36. Криптосистема Эль-Гамаль. Параметры домена. Шифрование. Дешифрование.
37. Криптосистема Рабина. Алгоритм. Шифрование. Дешифрование.
38. Простые числа. Важность проблемы тестирования простых чисел. Пробное деление.
39. Распределение ключей Диффи ? Хеллмана. Алгоритм. Стойкость. Атака человек посередине. Необходимость использования цифровой подписи.
40. Алгоритмом цифровой подписи RSA.
41. Криптографическая Хэш-функция. Свойства криптографической хэш-функции. Свойство односторонности Защищенность от повторений, защищенностью от вторых прообразов.
42. Алгоритмом цифровой подписи DSA.
43. Отечественный стандарт цифровой подписи ГОСТ Р 34.10-94.
44. Квантовая криптография.

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 Криптографические методы защиты и средства обеспечения информационной безопасности инфокоммуникаций
Институт ИПИТ *профиль подготовки* _____ *семестр* __-__

1. Основные понятия, обозначения и задачи криптографии.
2. Исторические примеры криптосистем.
3. Основные принципы криптографической защиты информации. Общая схема системы защиты информации.

И. о. зав. кафедрой СС и СК _____

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

БИЛЕТ № 2

Дисциплина Криптографические методы защиты и средства обеспечения информационной безопасности инфокоммуникаций
Институт ИПИТ *профиль подготовки* _____ *семестр* __-__

1. Абсолютно стойкие (совершенные) шифры. Криптостойкость алгоритма шифрования. Особенности симметричных криптосистем.
2. Метод простой подстановки (замены). Метод перестановки. Метод блочных шифров.
3. Метод гаммирования. Метод шифрования на основе теоремы Эйлера-Ферма.

И. о. зав. кафедрой СС и СК _____

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

БИЛЕТ № 3

Дисциплина Криптографические методы защиты и средства обеспечения информационной безопасности инфокоммуникаций
Институт ИПИТ *профиль подготовки* _____ *семестр* __-__

1. Алгоритм RSA. Шифрование в RSA. Дешифрование в RSA. Доказательство алго-ритма.
2. Алгоритм RSA. Задача криптоаналитика. Криптостойкость RSA
3. Криптосистема Эль-Гамаль. Параметры домена. Шифрование. Дешифрование.

И. о. зав. кафедрой СС и СК _____

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

БИЛЕТ № 4

Дисциплина Криптографические методы защиты и средства обеспечения информационной безопасности инфокоммуникаций
Институт ИПИТ *профиль подготовки* _____ *семестр* __-__

1. Распределение ключей Диффи ? Хеллмана. Алгоритм. Стойкость. Атака человек посередине. Необходимость использования цифровой подписи.
2. Алгоритмом цифровой подписи RSA.
3. Криптографическая Хэш-функция. Свойства криптографической хэш-функции. Свойство односторонности Защищенность от повторений, защищенностью от вторых прообразов.

И. о. зав. кафедрой СС и СК _____

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

БИЛЕТ № 5

Дисциплина Криптографические методы защиты и средства обеспечения информационной безопасности инфокоммуникаций
Институт ИПИТ *профиль подготовки* _____ *семестр* __-__

1. Алгоритмом цифровой подписи DSA.
2. Отечественный стандарт цифровой подписи ГОСТ Р 34.10-94.
3. Квантовая криптография.

И. о. зав. кафедрой СС и СК _____

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

БИЛЕТ № 6

Дисциплина Криптографические методы защиты и средства обеспечения информационной безопасности инфокоммуникаций
Институт ИПИТ *профиль подготовки* _____ *семестр* __-__

1. Система защиты Диффи-Хеллмана. Система защиты информации на основе заданного рюкзака.
2. Протоколы распределения секретных ключей. Основные цели протокола распределения ключей. Протокол Отвэй-Риса.
3. Протоколы распределения секретных ключей. Основные цели протокола распределения ключей. Цербер.

И. о. зав. кафедрой СС и СК _____

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

БИЛЕТ № 7

Дисциплина Криптографические методы защиты и средства обеспечения информационной безопасности инфокоммуникаций
Институт ИПИТ *профиль подготовки* _____ *семестр* __-__

1. Метод гаммирования. Метод шифрования на основе теоремы Эйлера-Ферма.
2. Композиция шифров.
3. Стандарт криптосистемы США DES.

И. о. зав. кафедрой СС и СК _____

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

БИЛЕТ № 8

Дисциплина Криптографические методы защиты и средства обеспечения информационной безопасности инфокоммуникаций
Институт ИПИТ *профиль подготовки* _____ *семестр* __-__

1. Протоколы распределения секретных ключей. Основные цели протокола распре-деления ключей. Протокол Отвэй-Риса.
2. Протоколы распределения секретных ключей. Основные цели протокола распре-деления ключей. Цербер.
3. Арифметика остатков. Сравнение по модулю. Решение уравнения $ax = b \pmod N$.

И. о. зав. кафедрой СС и СК _____

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

БИЛЕТ № 9

Дисциплина Криптографические методы защиты и средства обеспечения информационной безопасности инфокоммуникаций

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

1. Алгоритмом цифровой подписи DSA.
2. Отечественный стандарт цифровой подписи ГОСТ Р 34.10-94.
3. Квантовая криптография.

И. о. зав. кафедрой СС и СК _____

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

БИЛЕТ № 10

Дисциплина Криптографические методы защиты и средства обеспечения информационной безопасности инфокоммуникаций
Институт ИПИТ *профиль подготовки* _____ *семестр* __-__

1. Функции шифрования. Односторонние функции. Простейшие шифры и их клас-сификация.
2. Основные требования к шифрам, к криптографическим системам.
3. Абсолютно стойкие (совершенные) шифры. Криптостойкость алгоритма шифро-вания. Особенности симметричных криптосистем.

И. о. зав. кафедрой СС и СК _____

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

БИЛЕТ № 11

Дисциплина Криптографические методы защиты и средства обеспечения информационной безопасности инфокоммуникаций
Институт ИПИТ *профиль подготовки* _____ *семестр* __-__

1. Стандарт криптосистемы США DES.
2. Стандарт криптосистемы России – ГОСТ 28147-89. Системы защиты с открытым ключом.
3. Криптосистема RSA.

И. о. зав. кафедрой СС и СК _____

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

БИЛЕТ № 12

Дисциплина Криптографические методы защиты и средства обеспечения информационной безопасности инфокоммуникаций
Институт ИПИТ *профиль подготовки* _____ *семестр* __-__

1. Криптосистема с открытым ключом. Криптографическая односторонняя функция. Важнейшие криптографические односторонние функции.
2. Оценка сложности задач. Сложность алгоритма: Полиноминальная, экспоненци-альная, субэкспоненциальная Оракул. Сравнительный анализ сложности крипто-графических алгоритмов (без доказательства).
3. Алгоритм RSA. Шифрование в RSA. Дешифрование в RSA. Доказательство алго-ритма.

И. о. зав. кафедрой СС и СК _____

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

БИЛЕТ № 13

Дисциплина Криптографические методы защиты и средства обеспечения информационной безопасности инфокоммуникаций
Институт ИПИТ *профиль подготовки* _____ *семестр* __-__

1. Распределение ключей Диффи ? Хеллмана. Алгоритм. Стойкость. Атака человек посередине. Необходимость использования цифровой подписи.
2. Алгоритмом цифровой подписи RSA.
3. Криптографическая Хэш-функция. Свойства криптографической хэш-функции. Свойство односторонности Защищенность от повторений, защищенностью от вторых прообразов.

И. о. зав. кафедрой СС и СК _____

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

БИЛЕТ № 14

Дисциплина Криптографические методы защиты и средства обеспечения информационной безопасности инфокоммуникаций
Институт ИПИТ *профиль подготовки* _____ *семестр* __-__

1. Криптосистема Эль-Гамаль. Параметры домена. Шифрование. Дешифрование.
2. Криптосистема Рабина. Алгоритм. Шифрование. Дешифрование.
3. Простые числа. Важность проблемы тестирования простых чисел. Пробное деле-ние.

И. о. зав. кафедрой СС и СК _____

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

БИЛЕТ № 15

Дисциплина Криптографические методы защиты и средства обеспечения информационной безопасности инфокоммуникаций
Институт ИПИТ *профиль подготовки* _____ *семестр* __-__

1. Протоколы распределения секретных ключей. Основные цели протокола распре-деления ключей. Протокол Отвэй-Риса.
2. Протоколы распределения секретных ключей. Основные цели протокола распре-деления ключей. Цербер.
3. Арифметика остатков. Сравнение по модулю. Решение уравнения $ax = b \pmod N$.

И. о. зав. кафедрой СС и СК _____

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

БИЛЕТ № 16

Дисциплина Криптографические методы защиты и средства обеспечения информационной безопасности инфокоммуникаций
Институт ИПИТ *профиль подготовки* _____ *семестр* __-__

1. Основные требования к шифрам, к криптографическим системам.
2. Абсолютно стойкие (совершенные) шифры. Криптостойкость алгоритма шифро-вания. Особенности симметричных криптосистем.
3. Метод простой подстановки (замены). Метод перестановки. Метод блочных шифров.

И. о. зав. кафедрой СС и СК _____

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

БИЛЕТ № 17

Дисциплина Криптографические методы защиты и средства обеспечения информационной безопасности инфокоммуникаций
Институт ИПИТ *профиль подготовки* _____ *семестр* __-__

1. Теоретико-числовые алгоритмы и их сложность. Методы дискретного логариф-мирования.
2. Система защиты Диффи-Хеллмана. Система защиты информации на основе за-данного рюкзака.
3. Протоколы распределения секретных ключей. Основные цели протокола распре-деления ключей. Протокол Отвэй-Риса.

И. о. зав. кафедрой СС и СК _____

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

БИЛЕТ № 18

Дисциплина Криптографические методы защиты и средства обеспечения информационной безопасности инфокоммуникаций

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

1. Функция Эйлера. Мультипликативные обратные по модулю N. Теорема Лагранжа. Малая теорема Ферма. Применение в криптографии.
2. Алгоритм Евклида. Китайская теорема об остатках. Расширенный алгоритм Ев-клида. Применение в криптографии.
3. Криптосистема с открытым ключом. Криптографическая односторонняя функция. Важнейшие криптографические односторонние функции.

И. о. зав. кафедрой СС и СК _____

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

БИЛЕТ № 19

Дисциплина Криптографические методы защиты и средства обеспечения информационной безопасности инфокоммуникаций
Институт ИПИТ *профиль подготовки* _____ *семестр* __-__

1. Система защиты Диффи-Хеллмана. Система защиты информации на основе за-данного рюкзака.
2. Протоколы распределения секретных ключей. Основные цели протокола распре-деления ключей. Протокол Отвэй-Риса.
3. Протоколы распределения секретных ключей. Основные цели протокола распре-деления ключей. Цербер.

И. о. зав. кафедрой СС и СК _____

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

БИЛЕТ № 20

Дисциплина Криптографические методы защиты и средства обеспечения информационной безопасности инфокоммуникаций
Институт ИПИТ *профиль подготовки* _____ *семестр* __-__

1. Криптосистема Эль-Гамаль. Параметры домена. Шифрование. Дешифрование.
2. Криптосистема Рабина. Алгоритм. Шифрование. Дешифрование.
3. Простые числа. Важность проблемы тестирования простых чисел. Пробное деле-ние.

И. о. зав. кафедрой СС и СК _____