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

Факультет среднего профессионального образования

УТВЕРЖДЕН
на заседании ПЦК
«15» 01 2024 г., протокол № 10

Председатель ПЦК
_____ И.М. Дубаев

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

ПМ.02 Защита информации в автоматизированных системах программными и программно-аппаратными средствами

Специальность

10.02.05 Обеспечение информационной безопасности автоматизированных систем

Квалификация

техник по защите информации

Составитель _____ А.У.Байдарова

Грозный – 2024 г

ПАСПОРТ

ФОНДА ОЦЕНОЧНЫХ СРЕДСТВ ПО ПРОФЕССИОНАЛЬНОМУ МОДУЛЮ

ПМ.02 Защита информации в автоматизированных системах программными и программно-аппаратными средствами

МДК 02 01 Программные и программно-аппаратные средства защиты информации

№ п/п	Контролируемые разделы (темы) дисциплины	Код контролируемой компетенции	Наименование оценочного средства	
Семестр 6				
1.	Предмет и задачи программноаппаратной защиты информации	ОК 02, ОК 09 ПК 2.1 ПК 2.2	Зачет	1-я рубежная аттестация
2.	Защищенная автоматизированная система			2-я рубежная аттестация
Семестр 7				
3.	Дестабилизирующее воздействие на объекты защиты	ОК 02, ОК 09 ПК 2.1 ПК 2.2	Экзамен	1-я рубежная аттестация
				2-я рубежная аттестация

ПРИМЕРНЫЙ ПЕРЕЧЕНЬ ОЦЕНОЧНЫХ СРЕДСТВ

№ п/п	Наименование оценочного средства	Краткая характеристика оценочного средства	Представление оценочного средствав фонде
1.	*Рубежная аттестация*	Средство контроля усвоения учебного материала виде тестирования обучающихся.	Комплект тестов по вариантам к аттестациям
2.	*Зачет/экзамен*	Итоговая форма оценки знаний	Комплект тестов по вариантам к зачету(экзамену)

Вопросы рубежного контроля МДК 02 01 Программные и программно-аппаратные средства защиты информации на 6 семестр.

Вопросы к 1-ой рубежной аттестации

1. Какие основные задачи решает программно-аппаратная защита информации?
2. Назовите основные понятия, характеризующие программно-аппаратную защиту информации.
3. Какие методы и средства программно-аппаратной защиты информации существуют, и как они классифицируются?
4. Какие профили защиты относятся к программным и программно-аппаратным средствам, таким как межсетевые экраны, средства контроля съемных машинных носителей информации, средства доверенной загрузки, средства антивирусной защиты?
5. Укажите нормативные правовые акты и методические документы, где содержатся требования и рекомендации по защите информации программными и программно-аппаратными средствами.
6. Какие стандарты в области защиты информации включают требования и рекомендации по применению программных и программно-аппаратных средств?
7. Какие политики безопасности могут быть реализованы в межсетевых экранах (firewall)? Укажите их достоинства и недостатки.
8. Что понимается под автоматизированной системой, и какие процессы она автоматизирует в обработке информации?
9. Какие особенности характеризуют автоматизированные системы в защищенном исполнении? Укажите основные виды таких систем.
10. Какие методы используются при создании безопасных систем и какие принципы лежат в их основе?
11. Какие методы защиты информации применяются при работе в сетях общего доступа?
12. Какие функции выполняют межсетевые экраны (firewall) при обеспечении безопасности сетей?
13. Какие недостатки и преимущества существуют при использовании средств контроля съемных машинных носителей информации?
14. Какие виды автоматизированных систем чаще всего используются в защищенном исполнении, и как они различаются между собой?
15. Какие стандарты по защите информации включают требования и рекомендации по использованию программных и программно-аппаратных средств?
16. В чем заключается суть автоматизации процесса обработки информации, и как это влияет на обеспечение безопасности?

17. Какие методы защиты информации применяются при работе в сетях общего доступа, и как они обеспечивают безопасность данных?
18. Какие преимущества и недостатки могут сопутствовать реализации политик безопасности в межсетевых экранах?
19. Какие основные требования предъявляются к автоматизированным системам в защищенном исполнении, и как они обеспечивают надежность защиты информации?
20. Какие стандарты по защите информации определяют требования к созданию безопасных систем, и как они соотносятся с программно-аппаратной защитой?

Образец билета к 1-ой рубежной аттестации

Федеральное государственное бюджетное образовательное учреждение высшего образования
Грозненский государственный нефтяной технический университет
им. акад. М.Д.Миллионщикова
Факультет среднего профессионального образования
Тестовое задание
по дисциплине МДК 02 01 «Программные и программно-аппаратные средства защиты информации»
I-аттестация
Вариант №___

ФИО_____групп_____Дата

№ вопроса	1	2	3	4	5	6	7	8	9	10
Ответ										
№ вопроса	11	12	13	14	15	16	17	18	19	20
Ответ										

Вариант №1

1. **Какие основные задачи решает программно-аппаратная защита информации?**

а) Защита от вредоносных программ.
б) Обеспечение конфиденциальности, целостности и доступности данных.
в) Ускорение работы компьютерных систем.
г) Расширение функционала программ.

2. **Назовите основные понятия, характеризующие программно-аппаратную защиту информации.**

а) Центр обработки данных (ЦОД).
б) Блокчейн.
в) Безопасная загрузка (Secure Boot).
г) Виртуализация.

3. **Какие методы и средства программно-аппаратной защиты информации существуют, и как они классифицируются?**

а) Фирменные программы.
б) Аппаратные бренды.
в) Антивирусные базы данных.
г) Средства шифрования, межсетевые экраны и системы контроля доступа.

4. **Какие профили защиты относятся к программным и программно-аппаратным средствам?**

а) Профиль мультиплеера.

б) Профиль аутентификации.
в) Профиль безопасности.
г) Профиль производительности.

5. **Укажите нормативные правовые акты и методические документы по защите информации программными и программно-аппаратными средствами.**

а) Конституция Российской Федерации.
б) ГОСТ Р.
в) Манифест защиты данных.
г) Правила дорожного движения.

6. **Какие стандарты в области защиты информации включают требования и рекомендации по применению программных и программно-аппаратных средств?**

а) ISO 9001.
б) HIPAA.
в) ГОСТ Р ИСО/МЭК 27001.
г) IEEE 802.11.

7. **Какие политики безопасности могут быть реализованы в межсетевых экранах (firewall)?**

а) Политика "Открытый доступ".
б) Политика "Разделяй и властвуй".
в) Политика "Защита от вредоносных программ".
г) Политика "Безлимитный доступ".

8. **Что понимается под автоматизированной системой, и какие процессы она автоматизирует в обработке информации?**

а) Система автоматического полива.
б) Система автоматической продажи билетов.
в) Система, выполняющая задачи без участия человека.
г) Система автоматического распределения приоритетов.

9. **Какие особенности характеризуют автоматизированные системы в защищенном исполнении?**

а) Высокая производительность.
б) Отсутствие необходимости в обновлениях.
в) Наличие средств доверенной загрузки.
г) Специализированные антивирусные функции.

10. **Какие методы используются при создании безопасных систем и какие принципы лежат в их основе?**

а) Принцип "Полный доступ".
б) Метод "Скрытие данных".
в) Принципы "Наименьших привилегий" и "Безопасности по умолчанию".
г) Метод "Исключение шифрования".

11. **Какие методы защиты информации применяются при работе в сетях общего доступа?**

а) Методы аутентификации.
б) Методы шифрования.
в) Методы резервирования.
г) Методы публичного доступа.

12. **Какие функции выполняют межсетевые экраны (firewall) при обеспечении безопасности сетей?**

а) Пропускание всего трафика.
б) Контроль и фильтрация сетевого трафика.
в) Исключительно шифрование данных.
г) Только усиление сигнала Wi-Fi.

13. **Какие недостатки и преимущества существуют при использовании средств контроля съемных машинных носителей информации?**

а) Преимущество - увеличение риска утраты данных.
б) Недостаток - ограничение возможности передачи данных на внешние носители.

в) Преимущество - улучшение производительности.
г) Недостаток - отсутствие контроля над передачей файлов.

14. **Какие виды автоматизированных систем чаще всего используются в защищенном исполнении, и как они различаются между собой?**

а) Автоматизированные системы управления производством и бизнес-процессами.
б) Автоматизированные системы учета персонала и оборудования.
в) Системы управления доступом и системы мониторинга.
г) Электронные таблицы и текстовые редакторы.

15. **Какие стандарты по защите информации включают требования и рекомендации по использованию программных и программно-аппаратных средств?**

а) ГОСТ Р ИСО 14001.
б) ГОСТ Р ИСО/МЭК 27002.
в) ГОСТ Р 53434.
г) ГОСТ Р 12345.

16. **В чем заключается суть автоматизации процесса обработки информации, и как это влияет на обеспечение безопасности?**

а) Суть в полной зависимости от человеческого вмешательства.
б) Автоматизация ускоряет процессы, но не влияет на безопасность.
в) Автоматизация уменьшает риск ошибок и улучшает безопасность обработки информации.
г) Суть в полном отсутствии контроля.

17. **Какие методы защиты информации применяются при работе в сетях общего доступа, и как они обеспечивают безопасность данных?**

а) Методы аутентификации и шифрования данных.
б) Методы замедления передачи данных.
в) Методы вирусных атак.
г) Методы публичного доступа.

18. **Какие преимущества и недостатки могут сопутствовать реализации политик безопасности в межсетевых экранах?**

а) Преимущество - улучшение производительности сети.
б) Недостаток - ограничение доступа к определенным ресурсам.
в) Преимущество - увеличение риска вирусных атак.
г) Недостаток - отсутствие контроля над трафиком.

19. **Какие основные требования предъявляются к автоматизированным системам в защищенном исполнении, и как они обеспечивают надежность защиты информации?**

а) Требование к наличию уязвимостей.
б) Требование к открытости исходного кода.
в) Требование к системам контроля доступа.
г) Требование к обязательному наличию вирусов.

20. **Какие стандарты по защите информации определяют требования к созданию безопасных систем, и как они соотносятся с программно-аппаратной защитой?**

а) ГОСТ Р ИСО/МЭК 27005.
б) ГОСТ Р ИСО/МЭК 27001.
в) ГОСТ Р ИСО 14001.
г) ГОСТ Р ИСО 9001.

Вариант №2

1. **Какие основные задачи решает программно-аппаратная защита информации?**

а) Повышение производительности компьютера.
б) Обеспечение доступности данных.
в) Разработка новых программных продуктов.
г) Уменьшение объема хранимой информации.

2. **Назовите основные понятия, характеризующие программно-аппаратную защиту информации.**

а) Технология виртуализации.
б) Аппаратные ключи шифрования.
в) Система контроля трафика.
г) Электронная таблица.

3. **Какие методы и средства программно-аппаратной защиты информации существуют, и как они классифицируются?**

а) Системы облачного хранения.
б) Методы обхода шифрования.
в) Средства обеспечения конфиденциальности.
г) Алгоритмы асимметричного шифрования.

4. **Какие профили защиты относятся к программным и программно-аппаратным средствам?**

а) Профиль энергосбережения.
б) Профиль бизнес-процессов.
в) Профиль антивирусной защиты.
г) Профиль медицинских приложений.

5. **Укажите нормативные правовые акты и методические документы по защите информации программными и программно-аппаратными средствами.**

а) Закон о налогах и сборах.
б) ГОСТ Р 54609.
в) Инструкция по эксплуатации компьютера.
г) Соглашение о технической поддержке.

6. **Какие стандарты в области защиты информации включают требования и рекомендации по применению программных и программно-аппаратных средств?**

а) ГОСТ Р ИСО 10006.
б) ГОСТ Р ИСО/МЭК 27003.
в) ГОСТ Р 12346.
г) ГОСТ Р ИСО 50001.

7. **Какие политики безопасности могут быть реализованы в межсетевых экранах (firewall)?**

а) Политика "Неограниченный доступ".
б) Политика "Прозрачность".
в) Политика "Защита от вредоносных программ".
г) Политика "Общественный доступ".

8. **Что понимается под автоматизированной системой, и какие процессы она автоматизирует в обработке информации?**

а) Система для создания автоматических ответов на электронные письма.
б) Система для автоматической генерации паролей.
в) Система, которая выполняет задачи без участия человека.
г) Система для автоматической установки программ.

9. **Какие особенности характеризуют автоматизированные системы в защищенном исполнении?**

а) Наличие открытого исходного кода.
б) Наличие системы распознавания лиц.
в) Применение стандартных паролей.
г) Наличие механизмов доверенной загрузки.

10. **Какие методы используются при создании безопасных систем и какие принципы лежат в их основе?**

а) Метод "Раскрытие данных".
б) Принцип "Максимальных привилегий".
в) Принципы "Безопасности по умолчанию" и "Наименьших привилегий".
г) Метод "Оперативной очистки диска".

11. **Какие методы защиты информации применяются при работе в сетях общего доступа?**

а) Методы отката системы к предыдущему состоянию.
б) Методы шифрования и аутентификации.
в) Методы сохранения данных на внешних носителях.
г) Методы исключительно внутреннего доступа.

12. **Какие функции выполняют межсетевые экраны (firewall) при обеспечении безопасности сетей?**

а) Формирование протоколов обмена данными.
б) Фильтрация и контроль сетевого трафика.
в) Преобразование форматов файлов.
г) Обеспечение скорости сетевого соединения.

13. **Какие недостатки и преимущества существуют при использовании средств контроля съемных машинных носителей информации?**

а) Преимущество - повышение риска утечки данных.

б) Недостаток - ограничение возможности переноса данных на внешние носители.
в) Преимущество - уменьшение общего объема данных.
г) Недостаток - увеличение вероятности вирусных атак.

14. **Какие виды автоматизированных систем чаще всего используются в защищенном исполнении, и как они различаются между собой?**

а) Системы управления рабочим временем и учета расходов.
б) Системы учета затрат и системы видеонаблюдения.
в) Системы управления доступом и системы мониторинга.
г) Текстовые редакторы и электронные таблицы.

15. **Какие стандарты по защите информации включают требования и рекомендации по использованию программных и программно-аппаратных средств?**

а) ГОСТ Р ИСО/МЭК 27004.
б) ГОСТ Р ИСО 14002.
в) ГОСТ Р 87654.
г) ГОСТ Р 56789.

16. **В чем заключается суть автоматизации процесса обработки информации, и как это влияет на обеспечение безопасности?**

а) Суть в полном отсутствии роботизации процесса обработки информации.
б) Автоматизация улучшает производительность, но не влияет на безопасность.
в) Автоматизация снижает риск ошибок и улучшает безопасность обработки информации.
г) Суть в полной изоляции человека от процесса обработки информации.

17. **Какие методы защиты информации применяются при работе в сетях общего доступа, и как они обеспечивают безопасность данных?**

а) Методы прокладывания отдельных сетевых кабелей.
б) Методы блокировки всех внешних устройств.
в) Методы аутентификации и шифрования данных.
г) Методы исключительно локального доступа.

18. **Какие преимущества и недостатки могут сопутствовать реализации политик безопасности в межсетевых экранах?**

а) Преимущество - увеличение риска вирусных атак.
б) Недостаток - ограничение доступа к определенным ресурсам.
в) Преимущество - обеспечение полного доступа ко всем данным.
г) Недостаток - отсутствие контроля над трафиком.

19. **Какие основные требования предъявляются к автоматизированным системам в защищенном исполнении, и как они обеспечивают надежность защиты информации?**

а) Требование к наличию вирусов.
б) Требование к резервному копированию данных.
в) Требование к системам контроля доступа.
г) Требование к открытости исходного кода.

20. **Какие стандарты по защите информации определяют требования к созданию безопасных систем, и как они соотносятся с программно-аппаратной защитой?**

а) ГОСТ Р ИСО/МЭК 27006.
б) ГОСТ Р ИСО 12347.
в) ГОСТ Р ИСО 77777.
г) ГОСТ Р ИСО 22222.

Вариант № 3

1. Какие основные задачи решает программно-аппаратная защита информации?

а) Поддержание стабильности электроснабжения.

б) Организация эффективного менеджмента проектов.

в) Обеспечение конфиденциальности, целостности и доступности данных.

г) Развитие искусственного интеллекта в компьютерных системах.

2. Назовите основные понятия, характеризующие программно-аппаратную защиту информации.

а) Блокчейн.

б) Функциональная зависимость.

в) Система обнаружения вторжений.

г) Электронная коммерция.

3. Какие методы и средства программно-аппаратной защиты информации существуют, и как они классифицируются?

а) Средства для оптимизации работы процессора.

б) Алгоритмы для сжатия файлов.

в) Средства шифрования, межсетевые экраны и системы контроля доступа.

г) Системы для управления телефонными звонками.

4. Какие профили защиты относятся к программным и программно-аппаратным средствам?

а) Профиль бухгалтерии.

б) Профиль антивирусной защиты.

в) Профиль управления персоналом.

г) Профиль географических информационных систем.

5. Укажите нормативные правовые акты и методические документы по защите информации программными и программно-аппаратными средствами.

а) Закон о космическом пространстве.

б) ГОСТ Р 56321.

в) Инструкция по эксплуатации автомобиля.

г) Соглашение о безопасности парашютов.

6. Какие стандарты в области защиты информации включают требования и рекомендации по применению программных и программно-аппаратных средств?

а) ГОСТ Р ИСО 17025.

б) ГОСТ Р ИСО/МЭК 27010.

в) ГОСТ Р 34567.

г) ГОСТ Р ИСО 9002.

7. Какие политики безопасности могут быть реализованы в межсетевых экранах (firewall)?

а) Политика "Ноль доступа".

б) Политика "Автоматического резервирования".

в) Политика "Защиты от компьютерных вирусов".

г) Политика "Открытого доступа".

8. Что понимается под автоматизированной системой, и какие процессы она автоматизирует в обработке информации?

а) Система для автоматической приготовки кофе.

б) Система для автоматического распознавания лиц.

в) Система, выполняющая задачи без участия человека.

г) Система для автоматической подачи теннисных мячей.

9. Какие особенности характеризуют автоматизированные системы в защищенном исполнении?

а) Применение устаревших технологий.

б) Наличие средств доверенной загрузки.

в) Обязательное подключение к глобальной сети.

г) Автоматизированные системы исключительно в развлекательных целях.

10. Какие методы используются при создании безопасных систем и какие принципы лежат в их основе?

а) Метод "Полного отказа от шифрования".

б) Принцип "Наименьших привилегий" и метод "Сокрытие информации".

в) Принцип "Безопасности по умолчанию" и метод "Публичного доступа".

г) Метод "Активного прослушивания".

11. Какие методы защиты информации применяются при работе в сетях общего доступа?

а) Методы "Изоляции от внешнего мира".

б) Методы шифрования и аутентификации.

в) Методы увеличения скорости передачи данных.

г) Методы введения дополнительных слоев физической защиты.

12. Какие функции выполняют межсетевые экраны (firewall) при обеспечении безопасности сетей?

а) Формирование исходного кода программ.

б) Фильтрация и контроль сетевого трафика.

в) Проведение метеорологических измерений.

г) Обеспечение долгосрочного хранения данных.

13. Какие недостатки и преимущества существуют при использовании средств контроля съемных машинных носителей информации?

а) Преимущество - увеличение вероятности вирусных атак.

б) Недостаток - отсутствие возможности управления доступом к данным.

в) Преимущество - уменьшение риска утечки конфиденциальной информации.

г) Недостаток - ограничение в использовании внешних устройств.

14. Какие виды автоматизированных систем чаще всего используются в защищенном исполнении, и как они различаются между собой?

а) Системы учета расходов и системы управления персоналом.

б) Системы для проектирования и системы видеонаблюдения.

в) Системы мониторинга и системы контроля доступа.

г) Текстовые редакторы и электронные таблицы.

15. Какие стандарты по защите информации включают требования и рекомендации по использованию программных и программно-аппаратных средств?

а) ГОСТ Р ИСО/МЭК 27007.

б) ГОСТ Р ИСО/МЭК 27008.

в) ГОСТ Р 12340.

г) ГОСТ Р 98765.

16. В чем заключается суть автоматизации процесса обработки информации, и как это влияет на обеспечение безопасности?

а) Суть в полном отсутствии автоматизации.

б) Автоматизация увеличивает риск ошибок и снижает безопасность.

в) Автоматизация уменьшает риск ошибок и улучшает безопасность обработки информации.

г) Суть в полной изоляции процесса от человека.

17. Какие методы защиты информации применяются при работе в сетях общего доступа, и как они обеспечивают безопасность данных?

а) Методы общественного доступа и борьбы с киберпреступностью.

б) Методы шифрования и аутентификации данных.

в) Методы увеличения скорости передачи данных.

г) Методы введения дополнительных слоев физической защиты.

18. Какие преимущества и недостатки могут сопутствовать реализации политик безопасности в межсетевых экранах?

а) Преимущество - уменьшение риска вирусных атак.

б) Недостаток - ограничение доступа к определенным ресурсам.

в) Преимущество - обеспечение полного доступа ко всем данным.

г) Недостаток - отсутствие контроля над трафиком.

19. Какие основные требования предъявляются к автоматизированным системам в защищенном исполнении, и как они обеспечивают надежность защиты информации?

а) Требование к наличию вирусов.

б) Требование к резервному копированию данных.

в) Требование к системам контроля доступа.

г) Требование к открытости исходного кода.

20. Какие стандарты по защите информации определяют требования к созданию безопасных систем, и как они соотносятся с программно-аппаратной защитой?

а) ГОСТ Р ИСО/МЭК 27009.

б) ГОСТ Р ИСО 22223.

в) ГОСТ Р ИСО 65432.

г) ГОСТ Р ИСО/МЭК 27011

Вариант № 4

1.Какие основные задачи решает программно-аппаратная защита информации?

а) Управление жизненным циклом продукта.

б) Соблюдение нормативных сроков бухгалтерской отчетности.

в) Обеспечение конфиденциальности, целостности и доступности информации.

г) Организация культурных мероприятий в компании.

2. **Назовите основные понятия, характеризующие программно-аппаратную защиту информации.**

а) Эффективность креативных процессов.

б) Методы обеспечения социальной справедливости.

в) Средства контроля доступа, системы обнаружения вторжений.

г) Принципы художественного оформления документов.

3.**Какие методы и средства программно-аппаратной защиты информации существуют, и как они классифицируются?**

а) Методы обучения сотрудников и средства мотивации.

б) Алгоритмы для кулинарного искусства.

в) Средства шифрования, межсетевые экраны и системы управления персоналом.

г) Технологии производства офисной мебели.

4.**Какие профили защиты относятся к программным и программно-аппаратным средствам, таким как межсетевые экраны, средства контроля съемных машинных носителей информации, средства доверенной загрузки, средства антивирусной защиты?**

а) Профиль управления креативными процессами.

б) Профиль бухгалтерской отчетности.

в) Профиль антивирусной защиты, профиль межсетевых экранов.

г) Профиль организации корпоративных мероприятий.

 Укажите нормативные правовые акты и методические документы, где содержатся требования и рекомендации по защите информации программными и программно-

аппаратными средствами.

а) Закон о защите прав потребителей.

б) ГОСТ Р 54321.

в) Инструкция по применению химических веществ.

г) Положение о бухгалтерии предприятия.

 Какие стандарты в области защиты информации включают требования и рекомендации по применению программных и программно-аппаратных средств?

а) ГОСТ Р ИСО 9001.

б) ГОСТ Р ИСО/МЭК 27002.

в) ГОСТ Р 87654.

г) ГОСТ Р ИСО 65432.

 Какие политики безопасности могут быть реализованы в межсетевых экранах (firewall)?

а) Политика "Защиты от насекомых".

б) Политика "Безопасности домашнего питомца".

в) Политика "Аутентификации и авторизации", "Защиты от внешних угроз".

г) Политика "Организации совместных праздников".

 Что понимается под автоматизированной системой, и какие процессы она автоматизирует в обработке информации?

а) Система для автоматического ухода за растениями.

б) Система для автоматической раздачи лекарств.

в) Система, выполняющая задачи без участия человека, автоматизирует процессы сбора, обработки и передачи информации.

г) Система для автоматического рисования портретов.

 Какие особенности характеризуют автоматизированные системы в защищенном исполнении?

а) Применение исключительно новейших технологий.

б) Наличие средств доверенной загрузки.

в) Обязательное подключение к глобальной сети.

г) Автоматизированные системы в основном используются для кулинарных экспериментов.

 Какие методы используются при создании безопасных систем и какие принципы лежат в их основе?

а) Метод "Сокрытия информации" и принцип "Безопасности по умолчанию".

б) Метод "Полного отказа от шифрования".

в) Принцип "Наименьших привилегий" и метод "Уменьшения скорости передачи данных".

г) Метод "Активного прослушивания" и принцип "Открытости исходного кода".

 Какие методы защиты информации применяются при работе в сетях общего доступа?

а) Методы "Блокировки всех сетевых портов".

б) Методы "Шифрования" и "Аутентификации".

в) Методы увеличения количества печатаемых страниц.

г) Методы "Сокрытия от внешнего мира".

 Какие функции выполняют межсетевые экраны (firewall) при обеспечении безопасности сетей?

а) Формирование графических изображений.

б) Фильтрация и контроль сетевого трафика.

в) Проведение химических анализов воздуха.

г) Обеспечение экологической безопасности.

 Какие недостатки и преимущества существуют при использовании средств контроля съемных машинных носителей информации?

а) Преимущество - увеличение риска вирусных атак.

б) Недостаток - ограничение в использовании внешних устройств.

в) Преимущество - уменьшение риска утечки конфиденциальной информации.

г) Недостаток - отсутствие контроля над доступом к данным.

 Какие виды автоматизированных систем чаще всего используются в защищенном исполнении, и как они различаются между собой?

а) Системы управления домашними хозяйствами и системы контроля доступа.

б) Системы для создания музыки и системы медицинского мониторинга.

в) Системы для управления транспортными потоками и системы для анализа данных.

г) Системы для проектирования и системы видеонаблюдения.

Какие стандарты по защите информации включают требования и рекомендации по использованию программных и программно-аппаратных средств?

а) ГОСТ Р ИСО/МЭК 27013.

б) ГОСТ Р ИСО/МЭК 27014.

в) ГОСТ Р 87698.

г) ГОСТ Р ИСО 99999.

В чем заключается суть автоматизации процесса обработки информации, и как это влияет на обеспечение безопасности?

а) Суть в полном отсутствии автоматизации.

б) Автоматизация увеличивает риск ошибок и снижает безопасность.

в) Автоматизация уменьшает риск ошибок и улучшает безопасность обработки информации.

г) Суть в полной изоляции процесса от человека.

 Какие методы защиты информации применяются при работе в сетях общего доступа, и как они обеспечивают безопасность данных?

а) Методы общественного доступа и борьбы с киберпреступностью.

б) Методы шифрования и аутентификации данных.

в) Методы увеличения скорости передачи данных.

г) Методы введения дополнительных слоев физической защиты.

 Какие преимущества и недостатки могут сопутствовать реализации политик безопасности в межсетевых экранах?

а) Преимущество - уменьшение риска вирусных атак.

б) Недостаток - ограничение доступа к определенным ресурсам.

в) Преимущество - обеспечение полного доступа ко всем данным.

г) Недостаток - отсутствие контроля над трафиком.

 Какие основные требования предъявляются к автоматизированным системам в защищенном исполнении, и как они обеспечивают надежность защиты информации?

а) Требование к наличию вирусов.

б) Требование к резервному копированию данных.

в) Требование к системам контроля доступа.

г) Требование к открытости исходного кода.

 Какие стандарты по защите информации определяют требования к созданию безопасных систем, и как они соотносятся с программно-аппаратной защитой?

а) ГОСТ Р ИСО/МЭК 27015.

б) ГОСТ Р ИСО 23232.

в) ГОСТ Р ИСО 76543.

г) ГОСТ Р ИСО/МЭК 27016.

Ключи к тесту

№ п/п	Вариант № 1	Вариант № 2	Вариант №3	Вариант №4
1	б	б	в	в
2	а, в, г	б, в	в	в
3	г	г	в	в
4	б, в	в	б	в
5	б	б	б	б
6	в	б	б	в
7	б, в	в	в	в
8	в	в	в	в
9	в	г	б	в
10	в	в	в	в
11	а, б	б	б	б
12	б	б	б	б
13	б	б	в	в
14	в	в	в	в
15	б	а	а	б
16	в	в	в	в
17	а	в	б	б
18	б	б	б	б
19	в	в	в	в
20	б	а	а	= в

Вопросы ко 2-ой рубежной аттестации

1. В чем заключается методология проектирования гарантированно защищенных компьютерных систем (КС)?
2. Какие основные принципы дискреционных моделей доступа? Приведите примеры сценариев их использования.
3. Какие основные принципы мандатных моделей доступа? Приведите примеры сценариев их использования.
4. Какие защитные механизмы включены в современное программное обеспечение, такое как MS Office?
5. Каким образом осуществляется учет, обработка, хранение и передача информации в автоматизированных информационных системах (АИС)?
6. Какие меры принимаются для ограничения доступа на вход в систему АИС?
7. Чем отличаются идентификация и аутентификация пользователей?
8. Как осуществляется разграничение доступа в информационных системах?
9. Зачем проводится регистрация событий (аудит) и какие цели она преследует?
10. Как обеспечивается контроль целостности данных в информационных системах?
11. Каким образом осуществляется уничтожение остаточной информации в

информационных системах?

12. Как управляется политика безопасности в информационных системах?
13. В чем заключаются шаблоны безопасности, и как они используются в проектировании информационных систем?
14. Какие методы криптографической защиты применяются для обеспечения безопасности информации?
15. Какие программы для шифрования данных вы знаете, и как они соотносятся с политикой безопасности?
16. Какие источники дестабилизирующего воздействия могут существовать на объекты защиты в информационных системах?
17. Какие способы воздействия на информацию можно выделить?
18. Какие могут быть причины и условия дестабилизирующего воздействия на информацию?
19. Каким образом можно предотвратить или смягчить воздействие дестабилизирующих факторов на объекты защиты?
20. Как важно понимание причин и условий дестабилизирующего воздействия для разработки эффективных стратегий безопасности?

Образец билета ко 2-ой рубежной аттестации

Федеральное государственное бюджетное образовательное учреждение высшего образования
Грозненский государственный нефтяной технический университет
им. акад. М.Д.Миллионщикова
Факультет среднего профессионального образования
Тестовое задание
по дисциплине МДК 02 01 «Управление процессом технического обслуживания и ремонта автомобилей»
II-аттестация
Вариант №___

ФИО_____групп_____Дата

№ вопроса	1	2	3	4	5	6	7	8	9	10
Ответ										
№ вопроса	11	12	13	14	15	16	17	18	19	20
Ответ										

Вариант № 1

1. **Методология проектирования гарантированно защищенных КС.**

а) Организационные принципы.
б) Методы создания маркетинговых кампаний.
в) Процессы финансового аудита.
г) Технические характеристики оборудования.

2. **Дискреционные модели. Мандатные модели.**

а) Модели взаимодействия с клиентами.

б) Модели управления доступом.
в) Модели регулирования цен.
г) Модели транспортной логистики.

3. Защитные механизмы в современном программном обеспечении на примере MS Office.

а) Механизмы контроля климата.
б) Механизмы защиты от несанкционированного доступа.
в) Механизмы сбора статистических данных.
г) Механизмы финансового аудита.

4. Учет, обработка, хранение и передача информации в АИС. Ограничение доступа на вход в систему.

а) Учет оборота товаров.
б) Обработка пищевых продуктов.
в) Хранение транспортных средств.
г) Ограничение доступа на основе идентификации.

5. Идентификация и аутентификация пользователей. Разграничение доступа.

а) Идентификация видов растений.
б) Аутентификация банковских транзакций.
в) Разграничение доступа к административным ресурсам.
г) Разграничение доступа к строительным материалам.

6. Регистрация событий (аудит). Контроль целостности данных.

а) Регистрация спортивных соревнований.
б) Контроль цветовых решений в дизайне.
в) Регистрация событий в жизни организации.
г) Контроль целостности научных данных.

7. Уничтожение остаточной информации. Управление политикой безопасности.

а) Уничтожение старых бумажных документов.
б) Управление графиками сбора урожая.
в) Уничтожение информации на основе политических решений.
г) Управление политикой использования солнечной энергии.

8. Шаблоны безопасности. Криптографическая защита.

а) Шаблоны для создания веб-сайтов.
б) Криптографическая защита банковских данных.
в) Шаблоны безопасности в строительстве.
г) Криптографическая защита маршрутов.

9. Обзор программ шифрования данных. Управление политикой безопасности. Шаблоны безопасности.

а) Обзор программ для учета расходов.
б) Управление политикой в области культуры.
в) Шаблоны безопасности для транспортных средств.
г) Программы для шифрования файлов.

10. Источники дестабилизирующего воздействия на объекты защиты. Способы воздействия на информацию. Причины и условия дестабилизирующего воздействия на информацию.

а) Источники изменения цвета красителей.
б) Способы воздействия на финансовые рынки.
в) Причины изменения климата.
г) Способы воздействия на транспортные средства.

11. Что представляет собой методология проектирования гарантированно защищенных КС?

а) Совокупность правил и принципов для создания маркетинговых стратегий.
б) Методы создания мобильных приложений.
в) Системный подход к проектированию информационных систем с высоким уровнем безопасности.
г) Процессы разработки рекламных кампаний.

12. Чем отличаются дискреционные модели от мандатных?

а) Дискреционные модели регулируют доступ на основе уровня конфиденциальности.
б) Мандатные модели определяются в процессе дизайна интерфейсов.
в) Дискреционные модели используются в маркетинговых исследованиях.
г) Мандатные модели ориентированы на управление финансами.

13. Какие механизмы защиты включаются в современное программное обеспечение, например, MS Office?

а) Механизмы управления производственным процессом.
б) Механизмы защиты от климатических изменений.
в) Механизмы обеспечения безопасности работы с офисными приложениями.
г) Механизмы контроля заражения воздуха в офисе.

14. Что включает в себя процесс учета, обработки, хранения и передачи информации в АИС?

а) Учет рекламных бюджетов.
б) Обработка сельскохозяйственных продуктов.
в) Хранение транспортных средств в логистической системе.
г) Ограничение доступа с использованием системы идентификации.

15. Что включает в себя идентификация пользователей в контексте безопасности информации?

а) Идентификация видов растений на ферме.
б) Аутентификация кредитных транзакций.
в) Разграничение доступа к рабочим станциям.
г) Разграничение доступа к строительным материалам в складе.

16. Какие процессы обеспечивает регистрация событий (аудит) в информационных системах?

а) Регистрация событий научных конференций.
б) Контроль цветовых решений в графическом дизайне.
в) Регистрация событий в жизни организации.
г) Контроль целостности данных в финансовой отчетности.

17. Какие задачи решает уничтожение остаточной информации в системах безопасности?

а) Уничтожение старых бумажных документов.
б) Управление графиками сбора урожая.
в) Уничтожение остаточных данных на носителях.
г) Управление политикой в области энергосбережения.

18. Что представляют собой шаблоны безопасности в контексте информационной безопасности?

а) Шаблоны для создания рекламных баннеров.
б) Криптографическая защита банковских операций.
в) Шаблоны безопасности информационных систем.
г) Криптографическая защита логистических цепочек.

19. Какие программы обеспечивают шифрование данных в информационных системах?

а) Программы для создания музыкальных композиций.
б) Программы для управления логистикой.
в) Программы для шифрования файлов и сообщений.
г) Программы для анализа рыночных тенденций.

20. Что может являться источниками дестабилизирующего воздействия на объекты защиты информации?

а) Источники изменения цвета окружающей среды.
б) Способы воздействия на социальные структуры.
в) Причины изменения климата.
г) Способы воздействия на оборудование складских помещений.

Вариант № 2

1. **Какие основные задачи решает программно-аппаратная защита информации?**

а) Разработка рекламных кампаний.
б) Обеспечение безопасности информации.
в) Исследование климатических изменений.
г) Создание мультимедийных презентаций.

2. **Назовите основные понятия, характеризующие программно-аппаратную защиту информации.**

а) Компьютерные игры.
б) Антивирусные программы.
в) Финансовые отчеты.
г) Фауна и флора региона.

3. **Какие методы и средства программно-аппаратной защиты информации существуют, и как они классифицируются?**

а) Методы графического дизайна.
б) Способы управления бизнес-процессами.
в) Средства контроля климата.
г) Методы и средства обеспечения безопасности информации.

4. **Какие профили защиты относятся к программным и программно-аппаратным средствам, таким как межсетевые экраны, средства контроля съемных машинных носителей информации, средства доверенной загрузки, средства антивирусной защиты?**

а) Профили в области моды и стиля.
б) Профили в области бизнес-анализа.
в) Профили в области информационной безопасности.
г) Профили в области исследования климата.

5. **Укажите нормативные правовые акты и методические документы, где содержатся требования и рекомендации по защите информации программными и программно-аппаратными средствами.**

а) Технические характеристики автомобилей.
б) Кулинарные рецепты.
в) Правила дорожного движения.
г) Нормативные акты в области информационной безопасности.

6. **Какие стандарты в области защиты информации включают требования и рекомендации по применению программных и программно-аппаратных средств?**

а) Стандарты в области строительства.
б) Стандарты в области космических исследований.
в) Стандарты в области информационной безопасности.
г) Стандарты в области искусствоведения.

7. **Какие политики безопасности могут быть реализованы в межсетевых экранах (firewall)? Укажите их достоинства и недостатки.**

а) Политика безопасности в области геополитики.
б) Политика безопасности в области образования.
в) Политика безопасности в области информационных технологий.
г) Политика безопасности в области сельского хозяйства.

8. **Что понимается под автоматизированной системой, и какие процессы она автоматизирует в обработке информации?**

а) Автоматизация процессов врачебной диагностики.
б) Автоматизация процессов транспортировки грузов.
в) Автоматизация процессов обработки и передачи информации.
г) Автоматизация процессов кулинарного производства.

9. **Какие особенности характеризуют автоматизированные системы в защищенном исполнении? Укажите основные виды таких систем.**

а) Особенности автоматизированных систем в области искусства.
б) Особенности автоматизированных систем в области строительства.

в) Особенности автоматизированных систем в области информационной безопасности.
г) Особенности автоматизированных систем в области сельского хозяйства.

10. **Какие методы используются при создании безопасных систем и какие принципы лежат в их основе?**

а) Методы создания современных художественных произведений.
б) Методы создания инновационных технологий.
в) Методы создания систем с высоким уровнем безопасности.
г) Методы создания организационных структур.

11. **Какие методы защиты информации применяются при работе в сетях общего доступа?**

а) Методы управления сельскохозяйственными процессами.
б) Методы защиты финансовых транзакций.
в) Методы защиты информации в открытых сетях.
г) Методы управления климатическими условиями.

12. **Какие функции выполняют межсетевые экраны (firewall) при обеспечении безопасности сетей?**

а) Функции управления кулинарным производством.
б) Функции управления строительными процессами.
в) Функции контроля и фильтрации сетевого трафика.
г) Функции управления культурными событиями.

13. **Какие недостатки и преимущества существуют при использовании средств контроля съемных машинных носителей информации?**

а) Преимущества и недостатки в области геополитики.
б) Преимущества и недостатки в области сельского хозяйства.
в) Преимущества и недостатки в области информационной безопасности.
г) Преимущества и недостатки в области искусства.

14. **Какие виды автоматизированных систем чаще всего используются в защищенном исполнении, и как они различаются между собой?**

а) Виды систем в области космических исследований.
б) Виды систем в области строительства.
в) Виды систем в области информационной безопасности.
г) Виды систем в области искусства.

15. **Какие стандарты по защите информации включают требования и рекомендации по использованию программных и программно-аппаратных средств?**

а) Стандарты в области управления персоналом.
б) Стандарты в области оценки качества продукции.
в) Стандарты в области информационной безопасности.
г) Стандарты в области иностранных языков.

16. **В чем заключается суть автоматизации процесса обработки информации, и как это влияет на обеспечение безопасности?**

а) Суть автоматизации в области производства электроэнергии.
б) Суть автоматизации в области управления логистикой.
в) Суть автоматизации в обработке и передаче информации, что способствует повышению эффективности и безопасности процессов.
г) Суть автоматизации в области производства химических веществ.

17. **Какие методы защиты информации применяются при работе в сетях общего доступа, и как они обеспечивают безопасность данных?**

а) Методы управления производственными процессами.
б) Методы защиты данных в открытых сетях, включая шифрование и аутентификацию.
в) Методы управления транспортными потоками.
г) Методы управления общественными мероприятиями.

18. **Какие преимущества и недостатки могут сопутствовать реализации политик безопасности в межсетевых экранах?**

а) Преимущества и недостатки в области туризма.
б) Преимущества и недостатки в области строительства.

в) Преимущества и недостатки в области информационной безопасности.
г) Преимущества и недостатки в области образования.

19. **Какие основные требования предъявляются к автоматизированным системам в защищенном исполнении, и как они обеспечивают надежность защиты информации?**

а) Требования в области экологии.
б) Требования в области строительства.
в) Требования к системам с высоким уровнем безопасности и их способы обеспечения.
г) Требования в области здравоохранения.

20. **Какие стандарты по защите информации определяют требования к созданию безопасных систем, и как они соотносятся с программно-аппаратной защитой?**

а) Стандарты в области создания художественных произведений.
б) Стандарты в области обслуживания транспортных средств.
в) Стандарты в области информационной безопасности, определяющие требования к созданию безопасных систем.
г) Стандарты в области иностранных языков, влияющие на создание безопасных систем.

Вариант № 3

1. **Какие задачи решает программно-аппаратная защита информации?**

а) Управление транспортными потоками.
б) Обеспечение безопасности информации.
в) Разработка кулинарных рецептов.
г) Создание искусства.

2. **Основные понятия программно-аппаратной защиты информации:**

а) Понятия в области путешествий.
б) Антивирусные программы.
в) Понятия в области сельского хозяйства.
г) Понятия в области геологии.

3. **Методы и средства программно-аппаратной защиты:**

а) Методы управления финансами.
б) Средства управления климатом.
в) Методы и средства обеспечения безопасности информации.
г) Методы производства энергии.

4. **Профили защиты относятся к:**

а) Профилям в области моды.
б) Профилям в области информационной безопасности.
в) Профилям в области кулинарии.
г) Профилям в области иностранных языков.

5. **Нормативные акты по защите информации включают:**

а) Нормативные акты по геополитике.
б) Правила дорожного движения.
в) Правила готовки блюд.
г) Нормативные акты в области информационной безопасности.

6. **Стандарты в области защиты информации:**

а) Стандарты в области медицины.
б) Стандарты в области строительства.
в) Стандарты в области информационной безопасности.
г) Стандарты в области иностранных языков.

7. **Политики безопасности в межсетевых экранах:**

а) Политика в области науки.
б) Политика в области строительства.
в) Политика в области информационных технологий.
г) Политика в области географии.

8. **Автоматизированная система занимается:**

а) Автоматизацией процессов производства электроэнергии.
б) Автоматизацией процессов обработки информации.
в) Автоматизацией процессов строительства.
г) Автоматизацией процессов геологических исследований.

9. **Особенности автоматизированных систем в защищенном исполнении:**

а) Особенности в области искусства.
б) Особенности в области строительства.
в) Особенности в области информационной безопасности.
г) Особенности в области географии.

10. **Методы создания безопасных систем и их принципы:**

а) Методы создания современных художественных произведений.
б) Методы создания инновационных технологий.
в) Методы создания систем с высоким уровнем безопасности.
г) Методы создания организационных структур.

11. **Методы защиты информации в сетях общего доступа:**

а) Методы управления строительными процессами.
б) Методы защиты данных в открытых сетях.
в) Методы управления климатическими условиями.
г) Методы управления общественными мероприятиями.

12. **Функции межсетевых экранов (firewall) при обеспечении безопасности сетей:**

а) Функции управления культурными событиями.
б) Функции контроля и фильтрации сетевого трафика.
в) Функции управления производственными процессами.
г) Функции управления финансовыми транзакциями.

13. **Преимущества и недостатки средств контроля съемных машинных носителей информации:**

а) Преимущества и недостатки в области иностранных языков.
б) Преимущества и недостатки в области сельского хозяйства.
в) Преимущества и недостатки в области информационной безопасности.
г) Преимущества и недостатки в области искусства.

14. **Виды автоматизированных систем в защищенном исполнении:**

а) Виды систем в области космических исследований.
б) Виды систем в области строительства.
в) Виды систем в области географии.
г) Виды систем в области информационной безопасности.

15. **Стандарты по защите информации с требованиями к программно-аппаратным средствам:**

а) Стандарты в области управления персоналом.
б) Стандарты в области иностранных языков.
в) Стандарты в области информационной безопасности.
г) Стандарты в области электронной коммерции.

16. **Суть автоматизации процесса обработки информации и ее влияние на безопасность:**

а) Суть автоматизации в области производства энергии.
б) Суть автоматизации в области создания искусства.
в) Суть автоматизации в обработке информации и ее влияние на безопасность.
г) Суть автоматизации в области обслуживания транспортных средств.

17. **Методы защиты информации при работе в сетях общего доступа:**

а) Методы управления производственными процессами.
б) Методы защиты данных в открытых сетях, включая шифрование и аутентификацию.
в) Методы управления образовательными процессами.
г) Методы управления транспортными потоками.

18. **Преимущества и недостатки реализации политик безопасности в межсетевых экранах:**

а) Преимущества и недостатки в области образования.

б) Преимущества и недостатки в области производства электроэнергии.
в) Преимущества и недостатки в области информационной безопасности.
г) Преимущества и недостатки в области строительства.

19. **Требования к автоматизированным системам в защищенном исполнении и их роль в обеспечении безопасности:**

а) Требования в области экологии.
б) Требования в области медицины.
в) Требования к системам с высоким уровнем безопасности и их роль в обеспечении безопасности.
г) Требования в области иностранных языков.

20. **Стандарты по защите информации и их связь с программно-аппаратной защитой:**

а) Стандарты в области создания художественных произведений.
б) Стандарты в области информационной безопасности, определяющие требования к созданию безопасных систем.
в) Стандарты в области транспортного строительства.
г) Стандарты в области иностранных языков, влияющие на создание безопасных систем.

Вариант № 4

1. **Какие задачи решает программно-аппаратная защита информации?**

а) Регулирование оборота валюты.
б) Гарантирование безопасности информации.
в) Разработка дизайна интерьера.
г) Создание кулинарных рецептов.

2. **Основные понятия программно-аппаратной защиты информации:**

а) Основные понятия в области путешествий.
б) Программы для создания музыки.
в) Основные понятия в области сельского хозяйства.
г) Основные понятия в области архитектуры.

3. **Методы и средства программно-аппаратной защиты:**

а) Методы и средства управления транспортными потоками.
б) Средства управления метеорологическими условиями.
в) Методы и средства обеспечения безопасности информации.
г) Методы и средства создания художественных произведений.

4. **Профили защиты относятся к:**

а) Профилям в области дизайна интерьера.
б) Профилям в области информационной безопасности.
в) Профилям в области кулинарии.
г) Профилям в области литературы.

5. **Нормативные акты по защите информации включают:**

а) Нормативные акты по геополитике.
б) Правила дорожного движения.
в) Правила безопасности при плавании.
г) Нормативные акты в области информационной безопасности.

6. **Стандарты в области защиты информации:**

а) Стандарты в области медицины.
б) Стандарты в области строительства.
в) Стандарты в области информационной безопасности.
г) Стандарты в области иностранных языков.

7. **Политики безопасности в межсетевых экранах:**

а) Политика в области искусства.
б) Политика в области строительства.
в) Политика в области информационных технологий.
г) Политика в области экологии.

8. **Автоматизированная система занимается:**

а) Автоматизацией процессов производства электроэнергии.
б) Автоматизацией процессов обработки информации.
в) Автоматизацией процессов строительства.
г) Автоматизацией процессов визуального искусства.

9. **Особенности автоматизированных систем в защищенном исполнении:**

а) Особенности в области исследования океанов.
б) Особенности в области архитектуры.
в) Особенности в области информационной безопасности.
г) Особенности в области метеорологии.

10. **Методы создания безопасных систем и их принципы:**

а) Методы создания кулинарных систем.
б) Методы создания инновационных технологий.
в) Методы создания систем с высоким уровнем безопасности.
г) Методы создания образовательных структур.

11. **Методы защиты информации в сетях общего доступа:**

а) Методы управления производственными процессами.
б) Методы защиты данных в открытых сетях.
в) Методы управления климатическими условиями.
г) Методы управления образовательными мероприятиями.

12. **Функции межсетевых экранов (firewall) при обеспечении безопасности сетей:**

а) Функции управления социальными сетями.
б) Функции контроля и фильтрации сетевого трафика.
в) Функции управления производственными процессами.
г) Функции управления финансовыми транзакциями.

13. **Преимущества и недостатки средств контроля съемных машинных носителей информации:**

а) Преимущества и недостатки в области искусства.
б) Преимущества и недостатки в области метеорологии.
в) Преимущества и недостатки в области информационной безопасности.
г) Преимущества и недостатки в области гастрономии.

14. **Виды автоматизированных систем в защищенном исполнении:**

а) Виды систем в области образования.
б) Виды систем в области иностранных языков.
в) Виды систем с высоким уровнем безопасности.
г) Виды систем в области строительства.

15. **Стандарты по защите информации и их требования:**

а) Стандарты в области кулинарии.
б) Стандарты в области иностранных языков.
в) Стандарты в области информационной безопасности, определяющие требования к созданию безопасных систем.
г) Стандарты в области метеорологии.

16. **Суть автоматизации процесса обработки информации и ее влияние на безопасность:**

а) Суть автоматизации в области создания искусства.
б) Суть автоматизации в обработке информации и ее влияние на безопасность.
в) Суть автоматизации в области производства энергии.
г) Суть автоматизации в области обслуживания транспортных средств.

17. **Методы защиты информации при работе в сетях общего доступа:**

а) Методы управления производственными процессами.
б) Методы защиты данных в открытых сетях, включая шифрование и аутентификацию.
в) Методы управления образовательными процессами.
г) Методы управления транспортными потоками.

18. **Преимущества и недостатки реализации политик безопасности в межсетевых экранах:**

а) Преимущества и недостатки в области образования.
б) Преимущества и недостатки в области производства электроэнергии.

в) Преимущества и недостатки в области информационной безопасности.
г) Преимущества и недостатки в области строительства.

19. **Требования к автоматизированным системам в защищенном исполнении и их роль в обеспечении безопасности:**

а) Требования в области экологии.
б) Требования в области медицины.
в) Требования к системам с высоким уровнем безопасности и их роль в обеспечении безопасности.
г) Требования в области иностранных языков.

20. **Стандарты по защите информации и их связь с программно-аппаратной защитой:**

а) Стандарты в области создания художественных произведений.
б) Стандарты в области информационной безопасности, определяющие требования к созданию безопасных систем.
в) Стандарты в области транспортного строительства.
г) Стандарты в области иностранных языков, влияющие на создание безопасных систем.

Критерии оценивания рубежной аттестации:

Количество вопросов	**Оценка**	
16-20	**5**	**аттестован**
11-15	**4**	
6-10	**3**	
0-5	**2**	**не аттестован**

Аттестован - выставляется обучающемуся, ответившему правильно на 6-20 вопросов.

Не аттестован - выставляется обучающемуся, который ответил менее 5 вопроса.

Отлично - выставляется обучающемуся, ответившему на 16-20 вопросов.

Хорошо - выставляется обучающемуся, ответившему на 11-15 вопросов.

Удовлетворительно - выставляется обучающемуся, ответившему на 6-10 вопросов.

Ключи к тесту

№ п/п	**Вариант № 1**	**Вариант № 2**	**Вариант №3**	**Вариант №4**
1	**в**	**б**	**б**	**б**
2	**б**	**в**	**б**	**в**
3	**в**	**г**	**в**	**в**
4	**г**	**в**	**б**	**б**
5	**в**	**г**	**г**	**г**
6	**в**	**в**	**в**	**в**
7	**г**	**в**	**в**	**в**
8	**в**	**в**	**б**	**б**

9	**г**	**в**	**в**	**в**
10	**б**	**в**	**в**	**в**
11	**в**	**в**	**б**	**б**
12	**а**	**г**	**в**	**в**
13	**в**	**в**	**в**	**в**
14	**г**	**в**	**г**	**г**
15	**в**	**в**	**в**	**в**
16	**в**	**в**	**в**	**б**
17	**г**	**б**	**б**	**б**
18	**в**	**в**	**в**	**в**
19	**г**	**г**	**в**	**в**
20	**б**	**в**	**в**	**в**

Вопросы итогового контроля по дисциплине «МДК.02.01 Программные и программно-аппаратные средства защиты информации» на 6 семестр

1. Какие основные задачи решает программно-аппаратная защита информации?
2. Назовите основные понятия, характеризующие программно-аппаратную защиту информации.
3. Какие методы и средства программно-аппаратной защиты информации существуют, и как они классифицируются?
4. Какие профили защиты относятся к программным и программно-аппаратным средствам, таким как межсетевые экраны, средства контроля съемных машинных носителей информации, средства доверенной загрузки, средства антивирусной защиты?
5. Укажите нормативные правовые акты и методические документы, где содержатся требования и рекомендации по защите информации программными и программно-аппаратными средствами.
6. Какие стандарты в области защиты информации включают требования и рекомендации по применению программных и программно-аппаратных средств?
7. Какие политики безопасности могут быть реализованы в межсетевых экранах (firewall)? Укажите их достоинства и недостатки.
8. Что понимается под автоматизированной системой, и какие процессы она автоматизирует в обработке информации?
9. Какие особенности характеризуют автоматизированные системы в защищенном исполнении? Укажите основные виды таких систем.
10. Какие методы используются при создании безопасных систем и какие принципы лежат в их основе?
11. Какие методы защиты информации применяются при работе в сетях общего доступа?
12. Какие функции выполняют межсетевые экраны (firewall) при обеспечении безопасности сетей?
13. Какие недостатки и преимущества существуют при использовании средств контроля съемных машинных носителей информации?
14. Какие виды автоматизированных систем чаще всего используются в защищенном исполнении, и как они различаются между собой?
15. Какие стандарты по защите информации включают требования и рекомендации по использованию программных и программно-аппаратных средств?
16. В чем заключается суть автоматизации процесса обработки информации, и как это влияет на обеспечение безопасности?
17. Какие методы защиты информации применяются при работе в сетях общего доступа, и как они обеспечивают безопасность данных?
18. Какие преимущества и недостатки могут сопутствовать реализации политик безопасности в

межсетевых экранах?

19. Какие основные требования предъявляются к автоматизированным системам в защищенном исполнении, и как они обеспечивают надежность защиты информации?
20. Какие стандарты по защите информации определяют требования к созданию безопасных систем, и как они соотносятся с программно-аппаратной защитой?

Образец билета к зачету

Федеральное государственное бюджетное образовательное учреждение высшего образования
Грозненский государственный нефтяной технический университет
им. акад. М.Д.Миллионщикова
Факультет среднего профессионального образования
Тестовое задание
по дисциплине МДК 02 01 «Программные и программно-аппаратные средства защиты информации»
Зачет
Вариант №___

ФИО_____групп_____Дата

№ вопроса	1	2	3	4	5	6	7	8	9	10
Ответ										
№ вопроса	11	12	13	14	15	16	17	18	19	20
Ответ										
№ вопроса	21	22	23	24	25	26	27	28	29	30
Ответ										
№ вопроса	31	32	33	34	35	36	37	38	39	40
Ответ										

Вариант №1

1. Какие основные задачи решает программно-аппаратная защита информации?

а) Защита от вредоносных программ.
б) Обеспечение конфиденциальности, целостности и доступности данных.
в) Ускорение работы компьютерных систем.
г) Расширение функционала программ.

2. Назовите основные понятия, характеризующие программно-аппаратную защиту информации.

а) Центр обработки данных (ЦОД).
б) Блокчейн.
в) Безопасная загрузка (Secure Boot).
г) Виртуализация.

3. Какие методы и средства программно-аппаратной защиты информации существуют, и как они классифицируются?

а) Фирменные программы.
б) Аппаратные бренды.

в) Антивирусные базы данных.
г) Средства шифрования, межсетевые экраны и системы контроля доступа.
4. Какие профили защиты относятся к программным и программно-аппаратным средствам?
а) Профиль мультиплеера.
б) Профиль аутентификации.
в) Профиль безопасности.
г) Профиль производительности.
5. Укажите нормативные правовые акты и методические документы по защите информации программными и программно-аппаратными средствами.
а) Конституция Российской Федерации.
б) ГОСТ Р.
в) Манифест защиты данных.
г) Правила дорожного движения.
6. Какие стандарты в области защиты информации включают требования и рекомендации по применению программных и программно-аппаратных средств?
а) ISO 9001.
б) HIPAA.
в) ГОСТ Р ИСО/МЭК 27001.
г) IEEE 802.11.
7. Какие политики безопасности могут быть реализованы в межсетевых экранах (firewall)?
а) Политика "Открытый доступ".
б) Политика "Разделяй и властвуй".
в) Политика "Защита от вредоносных программ".
г) Политика "Безлимитный доступ".
8. Что понимается под автоматизированной системой, и какие процессы она автоматизирует в обработке информации?
а) Система автоматического полива.
б) Система автоматической продажи билетов.
в) Система, выполняющая задачи без участия человека.
г) Система автоматического распределения приоритетов.
9. Какие особенности характеризуют автоматизированные системы в защищенном исполнении?
а) Высокая производительность.
б) Отсутствие необходимости в обновлениях.
в) Наличие средств доверенной загрузки.
г) Специализированные антивирусные функции.
10. Какие методы используются при создании безопасных систем и какие принципы лежат в их основе?
а) Принцип "Полный доступ".
б) Метод "Скрытие данных".
в) Принципы "Наименьших привилегий" и "Безопасности по умолчанию".
г) Метод "Исключение шифрования".
11. Какие методы защиты информации применяются при работе в сетях общего доступа?
а) Методы аутентификации.
б) Методы шифрования.
в) Методы резервирования.
г) Методы публичного доступа.
12. Какие функции выполняют межсетевые экраны (firewall) при обеспечении безопасности сетей?
а) Пропускание всего трафика.
б) Контроль и фильтрация сетевого трафика.
в) Исключительно шифрование данных.
г) Только усиление сигнала Wi-Fi.
13. Какие недостатки и преимущества существуют при использовании средств контроля съемных машинных носителей информации?

а) Преимущество - увеличение риска утраты данных.
б) Недостаток - ограничение возможности передачи данных на внешние носители.
в) Преимущество - улучшение производительности.
г) Недостаток - отсутствие контроля над передачей файлов.

14. Какие виды автоматизированных систем чаще всего используются в защищенном исполнении, и как они различаются между собой?
а) Автоматизированные системы управления производством и бизнес-процессами.
б) Автоматизированные системы учета персонала и оборудования.
в) Системы управления доступом и системы мониторинга.
г) Электронные таблицы и текстовые редакторы.

15. Какие стандарты по защите информации включают требования и рекомендации по использованию программных и программно-аппаратных средств?
а) ГОСТ Р ИСО 14001.
б) ГОСТ Р ИСО/МЭК 27002.
в) ГОСТ Р 53434.
г) ГОСТ Р 12345.

16. В чем заключается суть автоматизации процесса обработки информации, и как это влияет на обеспечение безопасности?
а) Суть в полной зависимости от человеческого вмешательства.
б) Автоматизация ускоряет процессы, но не влияет на безопасность.
в) Автоматизация уменьшает риск ошибок и улучшает безопасность обработки информации.
г) Суть в полном отсутствии контроля.

17. Какие методы защиты информации применяются при работе в сетях общего доступа, и как они обеспечивают безопасность данных?
а) Методы аутентификации и шифрования данных.
б) Методы замедления передачи данных.
в) Методы вирусных атак.
г) Методы публичного доступа.

18. Какие преимущества и недостатки могут сопутствовать реализации политик безопасности в межсетевых экранах?
а) Преимущество - улучшение производительности сети.
б) Недостаток - ограничение доступа к определенным ресурсам.
в) Преимущество - увеличение риска вирусных атак.
г) Недостаток - отсутствие контроля над трафиком.

19. Какие основные требования предъявляются к автоматизированным системам в защищенном исполнении, и как они обеспечивают надежность защиты информации?
а) Требование к наличию уязвимостей.
б) Требование к открытости исходного кода.
в) Требование к системам контроля доступа.
г) Требование к обязательному наличию вирусов.

20. Какие стандарты по защите информации определяют требования к созданию безопасных систем, и как они соотносятся с программно-аппаратной защитой?
а) ГОСТ Р ИСО/МЭК 27005.
б) ГОСТ Р ИСО/МЭК 27001.
в) ГОСТ Р ИСО 14001.
г) ГОСТ Р ИСО 9001.

21.Какие задачи решает программно-аппаратная защита информации?
а) Регулирование оборота валюты.
б) Гарантирование безопасности информации.
в) Разработка дизайна интерьера.
г) Создание кулинарных рецептов.

22.Основные понятия программно-аппаратной защиты информации:
а) Основные понятия в области путешествий.

б) Программы для создания музыки.
в) Основные понятия в области сельского хозяйства.
г) Основные понятия в области архитектуры.

23Методы и средства программно-аппаратной защиты:

а) Методы и средства управления транспортными потоками.
б) Средства управления метеорологическими условиями.
в) Методы и средства обеспечения безопасности информации.
г) Методы и средства создания художественных произведений.

24Профили защиты относятся к:

а) Профилям в области дизайна интерьера.
б) Профилям в области информационной безопасности.
в) Профилям в области кулинарии.
г) Профилям в области литературы.

25Нормативные акты по защите информации включают:

а) Нормативные акты по геополитике.
б) Правила дорожного движения.
в) Правила безопасности при плавании.
г) Нормативные акты в области информационной безопасности.

26Стандарты в области защиты информации:

а) Стандарты в области медицины.
б) Стандарты в области строительства.
в) Стандарты в области информационной безопасности.
г) Стандарты в области иностранных языков.

27Политики безопасности в межсетевых экранах:

а) Политика в области искусства.
б) Политика в области строительства.
в) Политика в области информационных технологий.
г) Политика в области экологии.

28.Автоматизированная система занимается:

а) Автоматизацией процессов производства электроэнергии.
б) Автоматизацией процессов обработки информации.
в) Автоматизацией процессов строительства.
г) Автоматизацией процессов визуального искусства.

29.Особенности автоматизированных систем в защищенном исполнении:

а) Особенности в области исследования океанов.
б) Особенности в области архитектуры.
в) Особенности в области информационной безопасности.
г) Особенности в области метеорологии.

30.Методы создания безопасных систем и их принципы:

а) Методы создания кулинарных систем.
б) Методы создания инновационных технологий.
в) Методы создания систем с высоким уровнем безопасности.
г) Методы создания образовательных структур.

31.Методы защиты информации в сетях общего доступа:

а) Методы управления производственными процессами.
б) Методы защиты данных в открытых сетях.
в) Методы управления климатическими условиями.
г) Методы управления образовательными мероприятиями.

32.Функции межсетевых экранов (firewall) при обеспечении безопасности сетей:

а) Функции управления социальными сетями.
б) Функции контроля и фильтрации сетевого трафика.
в) Функции управления производственными процессами.
г) Функции управления финансовыми транзакциями.

33.Преимущества и недостатки средств контроля съемных машинных носителей информации:

а) Преимущества и недостатки в области искусства.
б) Преимущества и недостатки в области метеорологии.
в) Преимущества и недостатки в области информационной безопасности.
г) Преимущества и недостатки в области гастрономии.

34.Виды автоматизированных систем в защищенном исполнении:

а) Виды систем в области образования.
б) Виды систем в области иностранных языков.
в) Виды систем с высоким уровнем безопасности.
г) Виды систем в области строительства.

35.Стандарты по защите информации и их требования:

а) Стандарты в области кулинарии.
б) Стандарты в области иностранных языков.
в) Стандарты в области информационной безопасности, определяющие требования к созданию безопасных систем.
г) Стандарты в области метеорологии.

36.Суть автоматизации процесса обработки информации и ее влияние на безопасность:

а) Суть автоматизации в области создания искусства.
б) Суть автоматизации в обработке информации и ее влияние на безопасность.
в) Суть автоматизации в области производства энергии.
г) Суть автоматизации в области обслуживания транспортных средств.

37.Методы защиты информации при работе в сетях общего доступа:

а) Методы управления производственными процессами.
б) Методы защиты данных в открытых сетях, включая шифрование и аутентификацию.
в) Методы управления образовательными процессами.
г) Методы управления транспортными потоками.

38.Преимущества и недостатки реализации политик безопасности в межсетевых экранах:

а) Преимущества и недостатки в области образования.
б) Преимущества и недостатки в области производства электроэнергии.
в) Преимущества и недостатки в области информационной безопасности.
г) Преимущества и недостатки в области строительства.

39.Требования к автоматизированным системам в защищенном исполнении и их роль в обеспечении безопасности:

а) Требования в области экологии.
б) Требования в области медицины.
в) Требования к системам с высоким уровнем безопасности и их роль в обеспечении безопасности.
г) Требования в области иностранных языков.

40.Стандарты по защите информации и их связь с программно-аппаратной защитой:

а) Стандарты в области создания художественных произведений.
б) Стандарты в области информационной безопасности, определяющие требования к созданию безопасных систем.
в) Стандарты в области транспортного строительства.
г) Стандарты в области иностранных языков, влияющие на создание безопасных систем.

Вариант №2

1. Какие основные задачи решает программно-аппаратная защита информации?

а) Повышение производительности компьютера.
б) Обеспечение доступности данных.

в) Разработка новых программных продуктов.
г) Уменьшение объема хранимой информации.
2. Назовите основные понятия, характеризующие программно-аппаратную защиту информации.
а) Технология виртуализации.
б) Аппаратные ключи шифрования.
в) Система контроля трафика.
г) Электронная таблица.
3. Какие методы и средства программно-аппаратной защиты информации существуют, и как они классифицируются?
а) Системы облачного хранения.
б) Методы обхода шифрования.
в) Средства обеспечения конфиденциальности.
г) Алгоритмы асимметричного шифрования.
4. Какие профили защиты относятся к программным и программно-аппаратным средствам?
а) Профиль энергосбережения.
б) Профиль бизнес-процессов.
в) Профиль антивирусной защиты.
г) Профиль медицинских приложений.
5. Укажите нормативные правовые акты и методические документы по защите информации программными и программно-аппаратными средствами.
а) Закон о налогах и сборах.
б) ГОСТ Р 54609.
в) Инструкция по эксплуатации компьютера.
г) Соглашение о технической поддержке.
6. Какие стандарты в области защиты информации включают требования и рекомендации по применению программных и программно-аппаратных средств?
а) ГОСТ Р ИСО 10006.
б) ГОСТ Р ИСО/МЭК 27003.
в) ГОСТ Р 12346.
г) ГОСТ Р ИСО 50001.
7. Какие политики безопасности могут быть реализованы в межсетевых экранах (firewall)?
а) Политика "Неограниченный доступ".
б) Политика "Прозрачность".
в) Политика "Защита от вредоносных программ".
г) Политика "Общественный доступ".
8. Что понимается под автоматизированной системой, и какие процессы она автоматизирует в обработке информации?
а) Система для создания автоматических ответов на электронные письма.
б) Система для автоматической генерации паролей.
в) Система, которая выполняет задачи без участия человека.
г) Система для автоматической установки программ.
9. Какие особенности характеризуют автоматизированные системы в защищенном исполнении?
а) Наличие открытого исходного кода.
б) Наличие системы распознавания лиц.
в) Применение стандартных паролей.
г) Наличие механизмов доверенной загрузки.
10. Какие методы используются при создании безопасных систем и какие принципы лежат в их основе?
а) Метод "Раскрытие данных".
б) Принцип "Максимальных привилегий".
в) Принципы "Безопасности по умолчанию" и "Наименьших привилегий".
г) Метод "Оперативной очистки диска".
11. Какие методы защиты информации применяются при работе в сетях общего доступа?
а) Методы отката системы к предыдущему состоянию.

б) Методы шифрования и аутентификации.
в) Методы сохранения данных на внешних носителях.
г) Методы исключительно внутреннего доступа.
12. Какие функции выполняют межсетевые экраны (firewall) при обеспечении безопасности сетей?
а) Формирование протоколов обмена данными.
б) Фильтрация и контроль сетевого трафика.
в) Преобразование форматов файлов.
г) Обеспечение скорости сетевого соединения.
13. Какие недостатки и преимущества существуют при использовании средств контроля съемных машинных носителей информации?
а) Преимущество - повышение риска утечки данных.
б) Недостаток - ограничение возможности переноса данных на внешние носители.
в) Преимущество - уменьшение общего объема данных.
г) Недостаток - увеличение вероятности вирусных атак.
14. Какие виды автоматизированных систем чаще всего используются в защищенном исполнении, и как они различаются между собой?
а) Системы управления рабочим временем и учета расходов.
б) Системы учета затрат и системы видеонаблюдения.
в) Системы управления доступом и системы мониторинга.
г) Текстовые редакторы и электронные таблицы.
15. Какие стандарты по защите информации включают требования и рекомендации по использованию программных и программно-аппаратных средств?
а) ГОСТ Р ИСО/МЭК 27004.
б) ГОСТ Р ИСО 14002.
в) ГОСТ Р 87654.
г) ГОСТ Р 56789.
16. В чем заключается суть автоматизации процесса обработки информации, и как это влияет на обеспечение безопасности?
а) Суть в полном отсутствии роботизации процесса обработки информации.
б) Автоматизация улучшает производительность, но не влияет на безопасность.
в) Автоматизация снижает риск ошибок и улучшает безопасность обработки информации.
г) Суть в полной изоляции человека от процесса обработки информации.
17. Какие методы защиты информации применяются при работе в сетях общего доступа, и как они обеспечивают безопасность данных?
а) Методы прокладывания отдельных сетевых кабелей.
б) Методы блокировки всех внешних устройств.
в) Методы аутентификации и шифрования данных.
г) Методы исключительно локального доступа.
18. Какие преимущества и недостатки могут сопутствовать реализации политик безопасности в межсетевых экранах?
а) Преимущество - увеличение риска вирусных атак.
б) Недостаток - ограничение доступа к определенным ресурсам.
в) Преимущество - обеспечение полного доступа ко всем данным.
г) Недостаток - отсутствие контроля над трафиком.
19. Какие основные требования предъявляются к автоматизированным системам в защищенном исполнении, и как они обеспечивают надежность защиты информации?
а) Требование к наличию вирусов.
б) Требование к резервному копированию данных.
в) Требование к системам контроля доступа.
г) Требование к открытости исходного кода.
20. Какие стандарты по защите информации определяют требования к созданию безопасных систем, и как они соотносятся с программно-аппаратной защитой?
а) ГОСТ Р ИСО/МЭК 27006.

б) ГОСТ Р ИСО 12347.
в) ГОСТ Р ИСО 77777.
г) ГОСТ Р ИСО 22222.

1. Какие основные задачи решает программно-аппаратная защита информации?
а) Повышение производительности компьютера.
б) Обеспечение доступности данных.
в) Разработка новых программных продуктов.
г) Уменьшение объема хранимой информации.
2. Назовите основные понятия, характеризующие программно-аппаратную защиту информации.
а) Технология виртуализации.
б) Аппаратные ключи шифрования.
в) Система контроля трафика.
г) Электронная таблица.
3. Какие методы и средства программно-аппаратной защиты информации существуют, и как они классифицируются?
а) Системы облачного хранения.
б) Методы обхода шифрования.
в) Средства обеспечения конфиденциальности.
г) Алгоритмы асимметричного шифрования.
4. Какие профили защиты относятся к программным и программно-аппаратным средствам?
а) Профиль энергосбережения.
б) Профиль бизнес-процессов.
в) Профиль антивирусной защиты.
г) Профиль медицинских приложений.
5. Укажите нормативные правовые акты и методические документы по защите информации программными и программно-аппаратными средствами.
а) Закон о налогах и сборах.
б) ГОСТ Р 54609.
в) Инструкция по эксплуатации компьютера.
г) Соглашение о технической поддержке.
6. Какие стандарты в области защиты информации включают требования и рекомендации по применению программных и программно-аппаратных средств?
а) ГОСТ Р ИСО 10006.
б) ГОСТ Р ИСО/МЭК 27003.
в) ГОСТ Р 12346.
г) ГОСТ Р ИСО 50001.
7. Какие политики безопасности могут быть реализованы в межсетевых экранах (firewall)?
а) Политика "Неограниченный доступ".
б) Политика "Прозрачность".
в) Политика "Защита от вредоносных программ".
г) Политика "Общественный доступ".
8. Что понимается под автоматизированной системой, и какие процессы она автоматизирует в обработке информации?
а) Система для создания автоматических ответов на электронные письма.
б) Система для автоматической генерации паролей.
в) Система, которая выполняет задачи без участия человека.
г) Система для автоматической установки программ.
9. Какие особенности характеризуют автоматизированные системы в защищенном исполнении?
а) Наличие открытого исходного кода.
б) Наличие системы распознавания лиц.
в) Применение стандартных паролей.
г) Наличие механизмов доверенной загрузки.

10. Какие методы используются при создании безопасных систем и какие принципы лежат в их основе?
а) Метод "Раскрытие данных".
б) Принцип "Максимальных привилегий".
в) Принципы "Безопасности по умолчанию" и "Наименьших привилегий".
г) Метод "Оперативной очистки диска".
11. Какие методы защиты информации применяются при работе в сетях общего доступа?
а) Методы отката системы к предыдущему состоянию.
б) Методы шифрования и аутентификации.
в) Методы сохранения данных на внешних носителях.
г) Методы исключительно внутреннего доступа.
12. Какие функции выполняют межсетевые экраны (firewall) при обеспечении безопасности сетей?
а) Формирование протоколов обмена данными.
б) Фильтрация и контроль сетевого трафика.
в) Преобразование форматов файлов.
г) Обеспечение скорости сетевого соединения.
13. Какие недостатки и преимущества существуют при использовании средств контроля съемных машинных носителей информации?
а) Преимущество - повышение риска утечки данных.
б) Недостаток - ограничение возможности переноса данных на внешние носители.
в) Преимущество - уменьшение общего объема данных.
г) Недостаток - увеличение вероятности вирусных атак.
14. Какие виды автоматизированных систем чаще всего используются в защищенном исполнении, и как они различаются между собой?
а) Системы управления рабочим временем и учета расходов.
б) Системы учета затрат и системы видеонаблюдения.
в) Системы управления доступом и системы мониторинга.
г) Текстовые редакторы и электронные таблицы.
15. Какие стандарты по защите информации включают требования и рекомендации по использованию программных и программно-аппаратных средств?
а) ГОСТ Р ИСО/МЭК 27004.
б) ГОСТ Р ИСО 14002.
в) ГОСТ Р 87654.
г) ГОСТ Р 56789.
16. В чем заключается суть автоматизации процесса обработки информации, и как это влияет на обеспечение безопасности?
а) Суть в полном отсутствии роботизации процесса обработки информации.
б) Автоматизация улучшает производительность, но не влияет на безопасность.
в) Автоматизация снижает риск ошибок и улучшает безопасность обработки информации.
г) Суть в полной изоляции человека от процесса обработки информации.
17. Какие методы защиты информации применяются при работе в сетях общего доступа, и как они обеспечивают безопасность данных?
а) Методы прокладывания отдельных сетевых кабелей.
б) Методы блокировки всех внешних устройств.
в) Методы аутентификации и шифрования данных.
г) Методы исключительно локального доступа.
18. Какие преимущества и недостатки могут сопутствовать реализации политик безопасности в межсетевых экранах?
а) Преимущество - увеличение риска вирусных атак.
б) Недостаток - ограничение доступа к определенным ресурсам.
в) Преимущество - обеспечение полного доступа ко всем данным.
г) Недостаток - отсутствие контроля над трафиком.
19. Какие основные требования предъявляются к автоматизированным системам в защищенном

исполнении, и как они обеспечивают надежность защиты информации?
а) Требование к наличию вирусов.
б) Требование к резервному копированию данных.
в) Требование к системам контроля доступа.
г) Требование к открытости исходного кода.
20. Какие стандарты по защите информации определяют требования к созданию безопасных систем, и как они соотносятся с программно-аппаратной защитой?
а) ГОСТ Р ИСО/МЭК 27006.
б) ГОСТ Р ИСО 12347.
в) ГОСТ Р ИСО 77777.
г) ГОСТ Р ИСО 22222.

Вариант № 3

1. Какие основные задачи решает программно-аппаратная защита информации?
а) Поддержание стабильности электроснабжения.
б) Организация эффективного менеджмента проектов.
в) Обеспечение конфиденциальности, целостности и доступности данных.
г) Развитие искусственного интеллекта в компьютерных системах.
2. Назовите основные понятия, характеризующие программно-аппаратную защиту информации.
а) Блокчейн.
б) Функциональная зависимость.
в) Система обнаружения вторжений.
г) Электронная коммерция.
3. Какие методы и средства программно-аппаратной защиты информации существуют, и как они классифицируются?
а) Средства для оптимизации работы процессора.
б) Алгоритмы для сжатия файлов.
в) Средства шифрования, межсетевые экраны и системы контроля доступа.
г) Системы для управления телефонными звонками.
4. Какие профили защиты относятся к программным и программно-аппаратным средствам?
а) Профиль бухгалтерии.
б) Профиль антивирусной защиты.
в) Профиль управления персоналом.
г) Профиль географических информационных систем.
5. Укажите нормативные правовые акты и методические документы по защите информации программными и программно-аппаратными средствами.
а) Закон о космическом пространстве.
б) ГОСТ Р 56321.
в) Инструкция по эксплуатации автомобиля.
г) Соглашение о безопасности парашютов.
6. Какие стандарты в области защиты информации включают требования и рекомендации по применению программных и программно-аппаратных средств?
а) ГОСТ Р ИСО 17025.
б) ГОСТ Р ИСО/МЭК 27010.
в) ГОСТ Р 34567.
г) ГОСТ Р ИСО 9002.
7. Какие политики безопасности могут быть реализованы в межсетевых экранах (firewall)?
а) Политика "Ноль доступа".
б) Политика "Автоматического резервирования".
в) Политика "Защиты от компьютерных вирусов".
г) Политика "Открытого доступа".
8. Что понимается под автоматизированной системой, и какие процессы она автоматизирует в обработке информации?
а) Система для автоматической приготовки кофе.

б) Система для автоматического распознавания лиц.
в) Система, выполняющая задачи без участия человека.
г) Система для автоматической подачи теннисных мячей.
9. Какие особенности характеризуют автоматизированные системы в защищенном исполнении?
а) Применение устаревших технологий.
б) Наличие средств доверенной загрузки.
в) Обязательное подключение к глобальной сети.
г) Автоматизированные системы исключительно в развлекательных целях.
10. Какие методы используются при создании безопасных систем и какие принципы лежат в их основе?
а) Метод "Полного отказа от шифрования".
б) Принцип "Наименьших привилегий" и метод "Сокрытие информации".
в) Принцип "Безопасности по умолчанию" и метод "Публичного доступа".
г) Метод "Активного прослушивания".
11. Какие методы защиты информации применяются при работе в сетях общего доступа?
а) Методы "Изоляции от внешнего мира".
б) Методы шифрования и аутентификации.
в) Методы увеличения скорости передачи данных.
г) Методы введения дополнительных слоев физической защиты.
12. Какие функции выполняют межсетевые экраны (firewall) при обеспечении безопасности сетей?
а) Формирование исходного кода программ.
б) Фильтрация и контроль сетевого трафика.
в) Проведение метеорологических измерений.
г) Обеспечение долгосрочного хранения данных.
13. Какие недостатки и преимущества существуют при использовании средств контроля съемных машинных носителей информации?
а) Преимущество - увеличение вероятности вирусных атак.
б) Недостаток - отсутствие возможности управления доступом к данным.
в) Преимущество - уменьшение риска утечки конфиденциальной информации.
г) Недостаток - ограничение в использовании внешних устройств.
14. Какие виды автоматизированных систем чаще всего используются в защищенном исполнении, и как они различаются между собой?
а) Системы учета расходов и системы управления персоналом.
б) Системы для проектирования и системы видеонаблюдения.
в) Системы мониторинга и системы контроля доступа.
г) Текстовые редакторы и электронные таблицы.
15. Какие стандарты по защите информации включают требования и рекомендации по использованию программных и программно-аппаратных средств?
а) ГОСТ Р ИСО/МЭК 27007.
б) ГОСТ Р ИСО/МЭК 27008.
в) ГОСТ Р 12340.
г) ГОСТ Р 98765.
16. В чем заключается суть автоматизации процесса обработки информации, и как это влияет на обеспечение безопасности?
а) Суть в полном отсутствии автоматизации.
б) Автоматизация увеличивает риск ошибок и снижает безопасность.
в) Автоматизация уменьшает риск ошибок и улучшает безопасность обработки информации.
г) Суть в полной изоляции процесса от человека.
17. Какие методы защиты информации применяются при работе в сетях общего доступа, и как они обеспечивают безопасность данных?
а) Методы общественного доступа и борьбы с киберпреступностью.
б) Методы шифрования и аутентификации данных.
в) Методы увеличения скорости передачи данных.

г) Методы введения дополнительных слоев физической защиты.

18. Какие преимущества и недостатки могут сопутствовать реализации политик безопасности в межсетевых экранах?

а) Преимущество - уменьшение риска вирусных атак.

б) Недостаток - ограничение доступа к определенным ресурсам.

в) Преимущество - обеспечение полного доступа ко всем данным.

г) Недостаток - отсутствие контроля над трафиком.

19. Какие основные требования предъявляются к автоматизированным системам в защищенном исполнении, и как они обеспечивают надежность защиты информации?

а) Требование к наличию вирусов.

б) Требование к резервному копированию данных.

в) Требование к системам контроля доступа.

г) Требование к открытости исходного кода.

20. Какие стандарты по защите информации определяют требования к созданию безопасных систем, и как они соотносятся с программно-аппаратной защитой?

а) ГОСТ Р ИСО/МЭК 27009.

б) ГОСТ Р ИСО 22223.

в) ГОСТ Р ИСО 65432.

г) ГОСТ Р ИСО/МЭК 27011

1. **Какие основные задачи решает программно-аппаратная защита информации?**

а) Разработка рекламных кампаний.

б) Обеспечение безопасности информации.

в) Исследование климатических изменений.

г) Создание мультимедийных презентаций.

2. **Назовите основные понятия, характеризующие программно-аппаратную защиту информации.**

а) Компьютерные игры.

б) Антивирусные программы.

в) Финансовые отчеты.

г) Фауна и флора региона.

3. **Какие методы и средства программно-аппаратной защиты информации существуют, и как они классифицируются?**

а) Методы графического дизайна.

б) Способы управления бизнес-процессами.

в) Средства контроля климата.

г) Методы и средства обеспечения безопасности информации.

4. **Какие профили защиты относятся к программным и программно-аппаратным средствам, таким как межсетевые экраны, средства контроля съемных машинных носителей информации, средства доверенной загрузки, средства антивирусной защиты?**

а) Профили в области моды и стиля.

б) Профили в области бизнес-анализа.

в) Профили в области информационной безопасности.

г) Профили в области исследования климата.

5. **Укажите нормативные правовые акты и методические документы, где содержатся требования и рекомендации по защите информации программными и программно-аппаратными средствами.**

а) Технические характеристики автомобилей.

б) Кулинарные рецепты.

в) Правила дорожного движения.

г) Нормативные акты в области информационной безопасности.

6. **Какие стандарты в области защиты информации включают требования и рекомендации по применению программных и программно-аппаратных средств?**

а) Стандарты в области строительства.

б) Стандарты в области космических исследований.

в) Стандарты в области информационной безопасности.
г) Стандарты в области искусствоведения.

7. **Какие политики безопасности могут быть реализованы в межсетевых экранах (firewall)? Укажите их достоинства и недостатки.**

а) Политика безопасности в области геополитики.
б) Политика безопасности в области образования.
в) Политика безопасности в области информационных технологий.
г) Политика безопасности в области сельского хозяйства.

8. **Что понимается под автоматизированной системой, и какие процессы она автоматизирует в обработке информации?**

а) Автоматизация процессов врачебной диагностики.
б) Автоматизация процессов транспортировки грузов.
в) Автоматизация процессов обработки и передачи информации.
г) Автоматизация процессов кулинарного производства.

9. **Какие особенности характеризуют автоматизированные системы в защищенном исполнении? Укажите основные виды таких систем.**

а) Особенности автоматизированных систем в области искусства.
б) Особенности автоматизированных систем в области строительства.
в) Особенности автоматизированных систем в области информационной безопасности.
г) Особенности автоматизированных систем в области сельского хозяйства.

10. **Какие методы используются при создании безопасных систем и какие принципы лежат в их основе?**

а) Методы создания современных художественных произведений.
б) Методы создания инновационных технологий.
в) Методы создания систем с высоким уровнем безопасности.
г) Методы создания организационных структур.

11. **Какие методы защиты информации применяются при работе в сетях общего доступа?**

а) Методы управления сельскохозяйственными процессами.
б) Методы защиты финансовых транзакций.
в) Методы защиты информации в открытых сетях.
г) Методы управления климатическими условиями.

12. **Какие функции выполняют межсетевые экраны (firewall) при обеспечении безопасности сетей?**

а) Функции управления кулинарным производством.
б) Функции управления строительными процессами.
в) Функции контроля и фильтрации сетевого трафика.
г) Функции управления культурными событиями.

13. **Какие недостатки и преимущества существуют при использовании средств контроля съемных машинных носителей информации?**

а) Преимущества и недостатки в области геополитики.
б) Преимущества и недостатки в области сельского хозяйства.
в) Преимущества и недостатки в области информационной безопасности.
г) Преимущества и недостатки в области искусства.

14. **Какие виды автоматизированных систем чаще всего используются в защищенном исполнении, и как они различаются между собой?**

а) Виды систем в области космических исследований.
б) Виды систем в области строительства.
в) Виды систем в области информационной безопасности.
г) Виды систем в области искусства.

15. **Какие стандарты по защите информации включают требования и рекомендации по использованию программных и программно-аппаратных средств?**

а) Стандарты в области управления персоналом.
б) Стандарты в области оценки качества продукции.
в) Стандарты в области информационной безопасности.

г) Стандарты в области иностранных языков.

16. **В чем заключается суть автоматизации процесса обработки информации, и как это влияет на обеспечение безопасности?**

а) Суть автоматизации в области производства электроэнергии.
б) Суть автоматизации в области управления логистикой.
в) Суть автоматизации в обработке и передаче информации, что способствует повышению эффективности и безопасности процессов.
г) Суть автоматизации в области производства химических веществ.

17. **Какие методы защиты информации применяются при работе в сетях общего доступа, и как они обеспечивают безопасность данных?**

а) Методы управления производственными процессами.
б) Методы защиты данных в открытых сетях, включая шифрование и аутентификацию.
в) Методы управления транспортными потоками.
г) Методы управления общественными мероприятиями.

18. **Какие преимущества и недостатки могут сопутствовать реализации политик безопасности в межсетевых экранах?**

а) Преимущества и недостатки в области туризма.
б) Преимущества и недостатки в области строительства.
в) Преимущества и недостатки в области информационной безопасности.
г) Преимущества и недостатки в области образования.

19. **Какие основные требования предъявляются к автоматизированным системам в защищенном исполнении, и как они обеспечивают надежность защиты информации?**

а) Требования в области экологии.
б) Требования в области строительства.
в) Требования к системам с высоким уровнем безопасности и их способы обеспечения.
г) Требования в области здравоохранения.

20. **Какие стандарты по защите информации определяют требования к созданию безопасных систем, и как они соотносятся с программно-аппаратной защитой?**

а) Стандарты в области создания художественных произведений.
б) Стандарты в области обслуживания транспортных средств.
в) Стандарты в области информационной безопасности, определяющие требования к созданию безопасных систем.
г) Стандарты в области иностранных языков, влияющие на создание безопасных систем.

Вариант № 4

1.Какие основные задачи решает программно-аппаратная защита информации?

а) Управление жизненным циклом продукта.
б) Соблюдение нормативных сроков бухгалтерской отчетности.
в) Обеспечение конфиденциальности, целостности и доступности информации.
г) Организация культурных мероприятий в компании.

2. Назовите основные понятия, характеризующие программно-аппаратную защиту информации.

а) Эффективность креативных процессов.
б) Методы обеспечения социальной справедливости.
в) Средства контроля доступа, системы обнаружения вторжений.
г) Принципы художественного оформления документов.

3.Какие методы и средства программно-аппаратной защиты информации существуют, и как они классифицируются?

а) Методы обучения сотрудников и средства мотивации.
б) Алгоритмы для кулинарного искусства.
в) Средства шифрования, межсетевые экраны и системы управления персоналом.

г) Технологии производства офисной мебели.

4.Какие профили защиты относятся к программным и программно-аппаратным средствам, таким как межсетевые экраны, средства контроля съемных машинных носителей информации, средства доверенной загрузки, средства антивирусной защиты?

а) Профиль управления креативными процессами.

б) Профиль бухгалтерской отчетности.

в) Профиль антивирусной защиты, профиль межсетевых экранов.

г) Профиль организации корпоративных мероприятий.

5.Укажите нормативные правовые акты и методические документы, где содержатся требования и рекомендации по защите информации программными и программно-аппаратными средствами.

а) Закон о защите прав потребителей.

б) ГОСТ Р 54321.

в) Инструкция по применению химических веществ.

г) Положение о бухгалтерии предприятия.

6. Какие стандарты в области защиты информации включают требования и рекомендации по применению программных и программно-аппаратных средств?

а) ГОСТ Р ИСО 9001.

б) ГОСТ Р ИСО/МЭК 27002.

в) ГОСТ Р 87654.

г) ГОСТ Р ИСО 65432.

7. Какие политики безопасности могут быть реализованы в межсетевых экранах (firewall)?

а) Политика "Защиты от насекомых".

б) Политика "Безопасности домашнего питомца".

в) Политика "Аутентификации и авторизации", "Защиты от внешних угроз".

г) Политика "Организации совместных праздников".

8.Что понимается под автоматизированной системой, и какие процессы она автоматизирует в обработке информации?

а) Система для автоматического ухода за растениями.

б) Система для автоматической раздачи лекарств.

в) Система, выполняющая задачи без участия человека, автоматизирует процессы сбора, обработки и передачи информации.

г) Система для автоматического рисования портретов.

9.Какие особенности характеризуют автоматизированные системы в защищенном исполнении?

а) Применение исключительно новейших технологий.

б) Наличие средств доверенной загрузки.

в) Обязательное подключение к глобальной сети.

г) Автоматизированные системы в основном используются для кулинарных экспериментов.

10 Какие методы используются при создании безопасных систем и какие принципы лежат в их основе?

а) Метод "Сокрытия информации" и принцип "Безопасности по умолчанию".

б) Метод "Полного отказа от шифрования".

в) Принцип "Наименьших привилегий" и метод "Уменьшения скорости передачи данных".

г) Метод "Активного прослушивания" и принцип "Открытости исходного кода".

11 Какие методы защиты информации применяются при работе в сетях общего доступа?

а) Методы "Блокировки всех сетевых портов".

б) Методы "Шифрования" и "Аутентификации".

в) Методы увеличения количества печатаемых страниц.

г) Методы "Сокрытия от внешнего мира".

12Какие функции выполняют межсетевые экраны (firewall) при обеспечении безопасности сетей?

а) Формирование графических изображений.

б) Фильтрация и контроль сетевого трафика.

в) Проведение химических анализов воздуха.
г) Обеспечение экологической безопасности.

13.Какие недостатки и преимущества существуют при использовании средств контроля съемных машинных носителей информации?

а) Преимущество - увеличение риска вирусных атак.
б) Недостаток - ограничение в использовании внешних устройств.
в) Преимущество - уменьшение риска утечки конфиденциальной информации.
г) Недостаток - отсутствие контроля над доступом к данным.

14. Какие виды автоматизированных систем чаще всего используются в защищенном исполнении, и как они различаются между собой?

а) Системы управления домашними хозяйствами и системы контроля доступа.
б) Системы для создания музыки и системы медицинского мониторинга.
в) Системы для управления транспортными потоками и системы для анализа данных.
г) Системы для проектирования и системы видеонаблюдения.

15Какие стандарты по защите информации включают требования и рекомендации по использованию программных и программно-аппаратных средств?

а) ГОСТ Р ИСО/МЭК 27013.
б) ГОСТ Р ИСО/МЭК 27014.
в) ГОСТ Р 87698.
г) ГОСТ Р ИСО 99999.

16. В чем заключается суть автоматизации процесса обработки информации, и как это влияет на обеспечение безопасности?

а) Суть в полном отсутствии автоматизации.
б) Автоматизация увеличивает риск ошибок и снижает безопасность.
в) Автоматизация уменьшает риск ошибок и улучшает безопасность обработки информации.
г) Суть в полной изоляции процесса от человека.

17Какие методы защиты информации применяются при работе в сетях общего доступа, и как они обеспечивают безопасность данных?

а) Методы общественного доступа и борьбы с киберпреступностью.
б) Методы шифрования и аутентификации данных.
в) Методы увеличения скорости передачи данных.
г) Методы введения дополнительных слоев физической защиты.

18.Какие преимущества и недостатки могут сопутствовать реализации политик безопасности в межсетевых экранах?

а) Преимущество - уменьшение риска вирусных атак.
б) Недостаток - ограничение доступа к определенным ресурсам.
в) Преимущество - обеспечение полного доступа ко всем данным.
г) Недостаток - отсутствие контроля над трафиком.

19 Какие основные требования предъявляются к автоматизированным системам в защищенном исполнении, и как они обеспечивают надежность защиты информации?

а) Требование к наличию вирусов.
б) Требование к резервному копированию данных.
в) Требование к системам контроля доступа.
г) Требование к открытости исходного кода.

20 Какие стандарты по защите информации определяют требования к созданию безопасных систем, и как они соотносятся с программно-аппаратной защитой?

а) ГОСТ Р ИСО/МЭК 27015.
б) ГОСТ Р ИСО 23232.
в) ГОСТ Р ИСО 76543.
г) ГОСТ Р ИСО/МЭК 27016.

21Какие основные задачи решает программно-аппаратная защита информации?

а) Защита от вредоносных программ.
б) Обеспечение конфиденциальности, целостности и доступности данных.

в) Ускорение работы компьютерных систем.
г) Расширение функционала программ.

22Назовите основные понятия, характеризующие программно-аппаратную защиту информации.

а) Центр обработки данных (ЦОД).
б) Блокчейн.
в) Безопасная загрузка (Secure Boot).
г) Виртуализация.

Какие методы и средства программно-аппаратной защиты информации существуют, и как они классифицируются?

а) Фирменные программы.
б) Аппаратные бренды.
в) Антивирусные базы данных.
г) Средства шифрования, межсетевые экраны и системы контроля доступа.

Какие профили защиты относятся к программным и программно-аппаратным средствам?

а) Профиль мультиплеера.
б) Профиль аутентификации.
в) Профиль безопасности.
г) Профиль производительности.

Укажите нормативные правовые акты и методические документы по защите информации программными и программно-аппаратными средствами.

а) Конституция Российской Федерации.
б) ГОСТ Р.
в) Манифест защиты данных.
г) Правила дорожного движения.

Какие стандарты в области защиты информации включают требования и рекомендации по применению программных и программно-аппаратных средств?

а) ISO 9001.
б) HIPAA.
в) ГОСТ Р ИСО/МЭК 27001.
г) IEEE 802.11.

1. **Какие политики безопасности могут быть реализованы в межсетевых экранах (firewall)?**

а) Политика "Открытый доступ".
б) Политика "Разделяй и властвуй".
в) Политика "Защита от вредоносных программ".
г) Политика "Безлимитный доступ".

2. **Что понимается под автоматизированной системой, и какие процессы она автоматизирует в обработке информации?**

а) Система автоматического полива.
б) Система автоматической продажи билетов.
в) Система, выполняющая задачи без участия человека.
г) Система автоматического распределения приоритетов.

3. **Какие особенности характеризуют автоматизированные системы в защищенном исполнении?**

а) Высокая производительность.
б) Отсутствие необходимости в обновлениях.
в) Наличие средств доверенной загрузки.
г) Специализированные антивирусные функции.

4. **Какие методы используются при создании безопасных систем и какие принципы лежат в их основе?**

а) Принцип "Полный доступ".
б) Метод "Скрытие данных".
в) Принципы "Наименьших привилегий" и "Безопасности по умолчанию".

г) Метод "Исключение шифрования".

5. **Какие методы защиты информации применяются при работе в сетях общего доступа?**

а) Методы аутентификации.
б) Методы шифрования.
в) Методы резервирования.
г) Методы публичного доступа.

6. **Какие функции выполняют межсетевые экраны (firewall) при обеспечении безопасности сетей?**

а) Пропускание всего трафика.
б) Контроль и фильтрация сетевого трафика.
в) Исключительно шифрование данных.
г) Только усиление сигнала Wi-Fi.

7. **23Какие недостатки и преимущества существуют при использовании средств контроля съемных машинных носителей информации?**

а) Преимущество - увеличение риска утраты данных.
б) Недостаток - ограничение возможности передачи данных на внешние носители.
в) Преимущество - улучшение производительности.
г) Недостаток - отсутствие контроля над передачей файлов.

8. **24Какие виды автоматизированных систем чаще всего используются в защищенном исполнении, и как они различаются между собой?**

а) Автоматизированные системы управления производством и бизнес-процессами.
б) Автоматизированные системы учета персонала и оборудования.
в) Системы управления доступом и системы мониторинга.
г) Электронные таблицы и текстовые редакторы.

9. **25Какие стандарты по защите информации включают требования и рекомендации по использованию программных и программно-аппаратных средств?**

а) ГОСТ Р ИСО 14001.
б) ГОСТ Р ИСО/МЭК 27002.
в) ГОСТ Р 53434.
г) ГОСТ Р 12345.

10. **26В чем заключается суть автоматизации процесса обработки информации, и как это влияет на обеспечение безопасности?**

а) Суть в полной зависимости от человеческого вмешательства.
б) Автоматизация ускоряет процессы, но не влияет на безопасность.
в) Автоматизация уменьшает риск ошибок и улучшает безопасность обработки информации.
г) Суть в полном отсутствии контроля.

11. **27Какие методы защиты информации применяются при работе в сетях общего доступа, и как они обеспечивают безопасность данных?**

а) Методы аутентификации и шифрования данных.
б) Методы замедления передачи данных.
в) Методы вирусных атак.
г) Методы публичного доступа.

12. **28Какие преимущества и недостатки могут сопутствовать реализации политик безопасности в межсетевых экранах?**

а) Преимущество - улучшение производительности сети.
б) Недостаток - ограничение доступа к определенным ресурсам.
в) Преимущество - увеличение риска вирусных атак.
г) Недостаток - отсутствие контроля над трафиком.

13. **29Какие основные требования предъявляются к автоматизированным системам в защищенном исполнении, и как они обеспечивают надежность защиты информации?**

а) Требование к наличию уязвимостей.
б) Требование к открытости исходного кода.
в) Требование к системам контроля доступа.
г) Требование к обязательному наличию вирусов.

30Какие стандарты по защите информации определяют требования к созданию безопасных систем, и как они соотносятся с программно-аппаратной защитой?

а) ГОСТ Р ИСО/МЭК 27005.
б) ГОСТ Р ИСО/МЭК 27001.
в) ГОСТ Р ИСО 14001.
г) ГОСТ Р ИСО 9001.

Критерии оценивания зачета:

Количество вопросов	Оценка	
31-40	**5**	**зачтено**
21-30	**4**	
11-20	**3**	
0-10	**2**	**не зачтено**

Зачтено - выставляется обучающемуся, ответившему правильно на 11 вопросов.

Не зачтено - выставляется обучающемуся, который ответил 10 и менее вопроса.

Ключи к тесту

№ п/п	Вариант № 1	Вариант № 2	Вариант №3	Вариант №4
1	**б**	**б**	**в**	**в**
2	**а, в, г**	**б, в**	**в**	**в**
3	**г**	**г**	**в**	**в**
4	**б, в**	**в**	**б**	**в**
5	**б**	**б**	**б**	**б**
6	**в**	**б**	**б**	**в**
7	**б, в**	**в**	**в**	**в**
8	**в**	**в**	**в**	**в**
9	**в**	**г**	**б**	**в**
10	**в**	**в**	**в**	**в**
11	**а, б**	**б**	**б**	**б**
12	**б**	**б**	**б**	**б**

13	**б**	**б**	**в**	**в**
14	**в**	**в**	**в**	**в**
15	**б**	**а**	**а**	**б**
16	**в**	**в**	**в**	**в**
17	**а**	**в**	**б**	**б**
18	**б**	**б**	**б**	**б**
19	**в**	**в**	**в**	**в**
20	**б**	**а**	**а**	**= в**
21	**в**	**в**	**б**	**в**
22	**в**	**в**	**а, в,**	**в**
23	**в**	**в**	**г**	**в**
24	**в**	**б**	**б, в**	**в**
25	**б**	**б**	**б**	**б**
26	**в**	**б**	**в**	**в**
27	**в**	**в**	**б, в**	**в**
28	**в**	**в**	**в**	**в**
29	**в**	**б**	**в**	**в**
30	**в**	**в**	**в**	**в**
31	**б**	**б**	**а, б**	**б**
32	**б**	**б**	**б**	**б**
33	**в**	**в**	**б**	**в**
34	**в**	**в**	**в**	**в**
35	**б**	**а**	**б**	**б**
36	**в**	**в**	**в**	**в**
37	**а**	**в**	**б**	**б**
38	**б**	**б**	**б**	**б**
39	**в**	**в**	**в**	**в**
40	**б**	**а**	**а**	**= в**

ПАСПОРТ

ФОНДА ОЦЕНОЧНЫХ СРЕДСТВ ПО ПРОФЕССИОНАЛЬНОМУ МОДУЛЮ

ПМ 02 Защита информации в автоматизированных системах программными и программно-аппаратными средствами

МДК.02.02 Криптографические средства защиты информации

№ п/п	Контролируемые разделы (темы) дисциплины	Код контролируемой компетенции	Наименование оценочного средства	
Семестр 7				
1.	Математические основы защиты информации	ОК 1, ОК 09 ПК 2.3, ПК 2.4 ПК 2.5, ПК 2.6	Зачет	1-я рубежная аттестация
2.	Методы криптографического защиты информации			2-я рубежная аттестация
3.	Криптоанализ			
Семестр 8				
4.	Поточные шифры и генераторы псевдослучайных чисел	ОК 1, ОК 09 ПК 2.3, ПК 2.4 ПК 2.5, ПК 2.6	Экзамен	1-я рубежная аттестация
5.	Кодирование информации. Компьютеризация шифрования.			
6.	Симметричные системы шифрования			
7.	Асимметричные системы шифрования			2-я рубежная аттестация
8.	Аутентификация данных. Электронная подпись			
9.	Криптозащита информации в сетях передачи данных			

ПРИМЕРНЫЙ ПЕРЕЧЕНЬ ОЦЕНОЧНЫХ СРЕДСТВ

№ п/п	Наименование оценочного средства	Краткая характеристика оценочного средства	Представление оценочного средствав фонде
1.	*Рубежная аттестация*	Средство контроля усвоения учебного материала виде тестирования обучающихся.	Комплект тестов по вариантам к аттестациям

2.	Экзамен	Итоговая форма оценки знаний	Комплект тестов по вариантам к зачету

Вопросы рубежного контроля по дисциплине
«Криптографические средства защиты информации» на 7 семестр.

Вопросы к 1-ой рубежной аттестации

1. Что такое множество в теории множеств?
2. Какие операции определены для множеств?
3. Что такое группа в алгебре?
4. Что такое кольцо?
5. Что такое поле?
6. Что такое делимость чисел?
7. Какой признак делимости позволяет проверить делимость числа на 2?
8. Что такое простое число?
9. Что такое составное число?
10. Что утверждает основная теорема арифметики?
11. Что такое наибольший общий делитель (НОД) двух чисел?
12. Что такое взаимно простые числа?
13. Какой алгоритм используется для нахождения НОД двух чисел?
14. Что такое модулярная арифметика?
15. Что такое класс в модулярной арифметике?
16. Что такое полная система вычетов по модулю?
17. Что такое функция Эйлера?
18. Что утверждает теорема Ферма-Эйлера?
19. Какой алгоритм используется для быстрого возведения в степень по модулю?
20. Что такое сравнение первой степени?
21. Что такое линейное диофантово уравнение?
22. Какой алгоритм используется для решения линейных диофантовых уравнений?
23. Что такое криптография?
24. Что такое симметричное шифрование?
25. Что такое асимметричное шифрование?

Образец билета к 1-ой рубежной аттестации

Федеральное государственное бюджетное образовательное учреждение высшегообразования
Грозненский государственный нефтяной технический университет
им. акад. М.Д.Миллионщикова
Факультет среднего профессионального образования
Тестовое задание
по модулю МДК.02.02 «Криптографические средства защиты информации»
I-аттестация
Вариант №___

ФИО_____групп_____Дата

№ вопроса	1	2	3	4	5	6	7	8	9	10
Ответ										
№ вопроса	11	12	13	14	15	16	17	18	19	20
Ответ										

Вариант №1

1. **Что такое множество в теории множеств?**

а) Совокупность элементов, не имеющая порядка
б) Упорядоченная совокупность элементов
в) Взаимосвязанные элементы
г) Нет правильного ответа

2. **Какой признак делимости позволяет проверить делимость числа на 2?**

а) Признак делимости на 3
б) Признак делимости на 4
в) Признак делимости на 5
г) Признак делимости на 2

3. **Что такое группа в алгебре?**

а) Множество с определенной ассоциативной операцией
б) Множество с операцией сложения
в) Множество с операцией умножения
г) Нет правильного ответа

4. **Что такое сравнение первой степени?**

а) Сравнение двух чисел по модулю
б) Решение уравнения вида $ax \equiv b \pmod n$
в) Сравнение двух чисел по степени
г) Нет правильного ответа

5. **Что такое наибольший общий делитель (НОД) двух чисел?**

а) Наибольшее число, на которое делятся оба числа
б) Наименьшее число, на которое делятся оба числа
в) Среднее арифметическое двух чисел
г) Нет правильного ответа

6. **Что такое простое число?**

а) Число, имеющее только два делителя: 1 и само число
б) Число, имеющее три делителя
в) Число, имеющее четыре делителя
г) Нет правильного ответа

7. Что такое симметричное шифрование?
а) Тип шифрования, при котором используется один и тот же ключ для шифрования и расшифрования
б) Тип шифрования, при котором используются разные ключи для шифрования и расшифрования
в) Тип шифрования, при котором не используются ключи
г) Нет правильного ответа

8. Что такое криптография?
а) Наука, изучающая методы защиты информации
б) Наука, изучающая методы сжатия информации
в) Наука, изучающая методы передачи информации
г) Нет правильного ответа

9. Что такое асимметричное шифрование?
а) Тип шифрования, при котором используется один и тот же ключ для шифрования и расшифрования
б) Тип шифрования, при котором используются разные ключи для шифрования и расшифрования
в) Тип шифрования, при котором не используются ключи
г) Нет правильного ответа

10. Что такое модулярная арифметика?
а) Арифметика, основанная на операциях с остатками от деления
б) Арифметика, основанная на операциях с десятичными числами
в) Арифметика, основанная на операциях с отрицательными числами
г) Нет правильного ответа

11. Что такое поле?
а) Множество, обладающее свойствами группы и кольца
б) Множество с операциями сложения, вычитания, умножения и деления
в) Множество с операциями возведения в степень и корень
г) Нет правильного ответа

12. Что такое функция Эйлера?
а) Функция, определяющая количество взаимно простых чисел с заданным числом
б) Функция, определяющая количество простых чисел до заданного числа
в) Функция, определяющая количество делителей заданного числа
г) Нет правильного ответа

13. Что такое полная система вычетов по модулю?
а) Множество классов, содержащих все возможные числа
б) Множество классов, содержащих только нечетные числа
в) Множество классов, содержащих только простые числа
г) Нет правильного ответа

14. Что такое делимость чисел?
а) Возможность без остатка разделить одно число на другое
б) Свойство числа быть четным
в) Свойство числа быть нечетным
г) Нет правильного ответа

15. Что такое линейное диофантово уравнение?
а) Уравнение вида ax + by = c, где a, b, c - целые числа
б) Уравнение вида ax ≡ b (mod n), где a, b, n - целые числа
в) Уравнение вида ax^2 + bx + c = 0, где a, b, c - целые числа
г) Нет правильного ответа

16. Что такое составное число?
а) Число, имеющее только два делителя: 1 и само число
б) Число, имеющее три делителя
в) Число, имеющее четыре делителя
г) Нет правильного ответа

17. Что такое кольцо?
а) Множество с операцией сложения и умножения
б) Множество с операцией вычитания и деления
в) Множество с операцией возведения в степень
г) Нет правильного ответа

18. Что такое взаимно простые числа?
а) Множество с операцией сложения и умножения
б) Множество с операцией вычитания и деления
в) Множество с операцией возведения в степень
г) Нет правильного ответа

19. Какой алгоритм используется для нахождения НОД двух чисел?
а) Алгоритм Евклида
б) Алгоритм Ферма
в) Алгоритм Шорра
г) Алгоритм Полларда

20. Какой алгоритм используется для решения линейных диофантовых уравнений?
а) Алгоритм Евклида
б) Алгоритм Ферма
в) Расширенный алгоритм Евклида
г) Алгоритм Шорра

Вариант №2

1. Что такое составное число?
а) Число, имеющее только два делителя: 1 и само число
б) Число, имеющее три делителя
в) Число, имеющее четыре делителя
г) Нет правильного ответа

2. Что такое простое число?
а) Число, имеющее только два делителя: 1 и само число
б) Число, имеющее три делителя
в) Число, имеющее четыре делителя
г) Нет правильного ответа

3. Что такое криптография?

а) Наука, изучающая методы защиты информации
б) Наука, изучающая методы сжатия информации
в) Наука, изучающая методы передачи информации
г) Нет правильного ответа

4. Что такое группа в алгебре?
а) Множество с определенной ассоциативной операцией
б) Множество с операцией сложения
в) Множество с операцией умножения
г) Нет правильного ответа

5. Что такое сравнение первой степени?
а) Сравнение двух чисел по модулю
б) Решение уравнения вида $ax \equiv b \pmod{n}$
в) Сравнение двух чисел по степени
г) Нет правильного ответа

6. Что такое наибольший общий делитель (НОД) двух чисел?
а) Наибольшее число, на которое делятся оба числа
б) Наименьшее число, на которое делятся оба числа
в) Среднее арифметическое двух чисел
г) Нет правильного ответа

7. Что такое модулярная арифметика?
а) Арифметика, основанная на операциях с остатками от деления
б) Арифметика, основанная на операциях с десятичными числами
в) Арифметика, основанная на операциях с отрицательными числами
г) Нет правильного ответа

8. Что такое поле?
а) Множество, обладающее свойствами группы и кольца
б) Множество с операциями сложения, вычитания, умножения и деления
в) Множество с операциями возведения в степень и корень
г) Нет правильного ответа

9. Что такое делимость чисел?
а) Возможность без остатка разделить одно число на другое
б) Свойство числа быть четным
в) Свойство числа быть нечетным
г) Нет правильного ответа

10. Что такое симметричное шифрование?
а) Тип шифрования, при котором используется один и тот же ключ для шифрования и расшифрования
б) Тип шифрования, при котором используются разные ключи для шифрования и расшифрования
в) Тип шифрования, при котором не используются ключи
г) Нет правильного ответа

11. Что такое асимметричное шифрование?
а) Тип шифрования, при котором используется один и тот же ключ для шифрования и расшифрования
б) Тип шифрования, при котором используются разные ключи для шифрования и расшифрования
в) Тип шифрования, при котором не используются ключи
г) Нет правильного ответа

12. Что такое кольцо?
а) Множество с операцией сложения и умножения
б) Множество с операцией вычитания и деления
в) Множество с операцией возведения в степень
г) Нет правильного ответа

13. Что такое полная система вычетов по модулю?
а) Множество классов, содержащих все возможные числа
б) Множество классов, содержащих только нечетные числа
в) Множество классов, содержащих только простые числа
г) Нет правильного ответа

14. Что такое функция Эйлера?
а) Функция, определяющая количество взаимно простых чисел с заданным числом
б) Функция, определяющая количество простых чисел до заданного числа
в) Функция, определяющая количество делителей заданного числа
г) Нет правильного ответа

15. Что такое линейное диофантово уравнение?
а) Уравнение вида ax + by = c, где a, b, c - целые числа
б) Уравнение вида ax ≡ b (mod n), где a, b, n - целые числа
в) Уравнение вида ax^2 + bx + c = 0, где a, b, c - целые числа
г) Нет правильного ответа

16. Какой признак делимости позволяет проверить делимость числа на 2?
а) Признак делимости на 3
б) Признак делимости на 4
в) Признак делимости на 5
г) Признак делимости на 2

17. Какой алгоритм используется для нахождения НОД двух чисел?
а) Алгоритм Евклида
б) Алгоритм Ферма
в) Алгоритм Шорра
г) Алгоритм Полларда

18. Что такое взаимно простые числа?
а) Числа, у которых НОД равен 1
б) Числа, у которых НОД равен 2
а) Числа, у которых НОД равен 2
в) Числа, у которых НОД равен 0
г) Нет правильного ответа

19. Какой алгоритм используется для решения линейных диофантовых уравнений?
а) Алгоритм Евклида
б) Алгоритм Ферма
в) Расширенный алгоритм Евклида
г) Алгоритм Шорра

20. Что утверждает основная теорема арифметики?
а) Всякое натуральное число можно представить в виде произведения простых чисел
б) Всякое натуральное число можно представить в виде суммы простых чисел

в) Всякое натуральное число можно представить в виде разности простых чисел
г) Всякое натуральное число можно представить в виде деления на простое число

Вариант №3

1. Что такое модулярная арифметика?
а) Арифметика, основанная на операциях с остатками от деления
б) Арифметика, основанная на операциях с десятичными числами
в) Арифметика, основанная на операциях с отрицательными числами
г) Нет правильного ответа

2. Что такое сравнение первой степени?
а) Сравнение двух чисел по модулю
б) Решение уравнения вида $ax \equiv b \pmod{n}$
в) Сравнение двух чисел по степени
г) Нет правильного ответа

3. Что такое кольцо?
а) Множество с операцией сложения и умножения
б) Множество с операцией вычитания и деления
в) Множество с операцией возведения в степень
г) Нет правильного ответа

4. Что такое группа в алгебре?
а) Множество с определенной ассоциативной операцией
б) Множество с операцией сложения
в) Множество с операцией умножения
г) Нет правильного ответа

5. Что такое функция Эйлера?
а) Функция, определяющая количество взаимно простых чисел с заданным числом
б) Функция, определяющая количество простых чисел до заданного числа
в) Функция, определяющая количество делителей заданного числа
г) Нет правильного ответа

6. Что такое наибольший общий делитель (НОД) двух чисел?
а) Наибольшее число, на которое делятся оба числа
б) Наименьшее число, на которое делятся оба числа
в) Среднее арифметическое двух чисел
г) Нет правильного ответа

7. Что такое простое число?
а) Число, имеющее только два делителя: 1 и само число
б) Число, имеющее три делителя
в) Число, имеющее четыре делителя
г) Нет правильного ответа

8. Что такое делимость чисел?
а) Возможность без остатка разделить одно число на другое
б) Свойство числа быть четным
в) Свойство числа быть нечетным
г) Нет правильного ответа

9. Что такое полная система вычетов по модулю?

а) Множество классов, содержащих все возможные числа
б) Множество классов, содержащих только нечетные числа
в) Множество классов, содержащих только простые числа
г) Нет правильного ответа

10. Что такое линейное диофантово уравнение?

а) Уравнение вида ax + by = c, где a, b, c - целые числа
б) Уравнение вида ax ≡ b (mod n), где a, b, n - целые числа
в) Уравнение вида ax^2 + bx + c = 0, где a, b, c - целые числа
г) Нет правильного ответа

11. Что такое составное число?

а) Число, имеющее только два делителя: 1 и само число
б) Число, имеющее три делителя
в) Число, имеющее четыре делителя
г) Нет правильного ответа

12. Что такое криптография?

а) Наука, изучающая методы защиты информации
б) Наука, изучающая методы сжатия информации
в) Наука, изучающая методы передачи информации
г) Нет правильного ответа

13. Что такое поле?

а) Множество, обладающее свойствами группы и кольца
б) Множество с операциями сложения, вычитания, умножения и деления
в) Множество с операциями возведения в степень и корень
г) Нет правильного ответа

14. Что такое взаимно простые числа?

а) Числа, у которых НОД равен 1
б) Числа, у которых НОД равен 2
а) Числа, у которых НОД равен 2
в) Числа, у которых НОД равен 0
г) Нет правильного ответа

15. Что такое симметричное шифрование?

а) Тип шифрования, при котором используется один и тот же ключ для шифрования и расшифрования
б) Тип шифрования, при котором используются разные ключи для шифрования и расшифрования
в) Тип шифрования, при котором не используются ключи
г) Нет правильного ответа

16. Что такое асимметричное шифрование?

а) Тип шифрования, при котором используется один и тот же ключ для шифрования и расшифрования
б) Тип шифрования, при котором используются разные ключи для шифрования и расшифрования
в) Тип шифрования, при котором не используются ключи
г) Нет правильного ответа

17. Какой признак делимости позволяет проверить делимость числа на 2?

а) Признак делимости на 3
б) Признак делимости на 4
в) Признак делимости на 5
г) Признак делимости на 2

18. Какой алгоритм используется для нахождения НОД двух чисел?
а) Алгоритм Евклида
б) Алгоритм Ферма
в) Алгоритм Шорра
г) Алгоритм Полларда

19. Какой алгоритм используется для решения линейных диофантовых уравнений?
а) Алгоритм Евклида
б) Алгоритм Ферма
в) Расширенный алгоритм Евклида
г) Алгоритм Шорра

20. Что утверждает основная теорема арифметики?
а) Всякое натуральное число можно представить в виде произведения простых чисел
б) Всякое натуральное число можно представить в виде суммы простых чисел
в) Всякое натуральное число можно представить в виде разности простых чисел
г) Всякое натуральное число можно представить в виде деления на простое число

Вариант №4

1. Что такое симметричное шифрование?
а) Тип шифрования, при котором используется один и тот же ключ для шифрования и расшифрования
б) Тип шифрования, при котором используются разные ключи для шифрования и расшифрования
в) Тип шифрования, при котором не используются ключи
г) Нет правильного ответа

2. Что такое асимметричное шифрование?
а) Тип шифрования, при котором используется один и тот же ключ для шифрования и расшифрования
б) Тип шифрования, при котором используются разные ключи для шифрования и расшифрования
в) Тип шифрования, при котором не используются ключи
г) Нет правильного ответа

3. Что такое криптография?
а) Наука, изучающая методы защиты информации
б) Наука, изучающая методы сжатия информации
в) Наука, изучающая методы передачи информации
г) Нет правильного ответа

4. Что такое модулярная арифметика?
а) Арифметика, основанная на операциях с остатками от деления
б) Арифметика, основанная на операциях с десятичными числами
в) Арифметика, основанная на операциях с отрицательными числами
г) Нет правильного ответа

5. Что такое функция Эйлера?

а) Функция, определяющая количество взаимно простых чисел с заданным числом
б) Функция, определяющая количество простых чисел до заданного числа
в) Функция, определяющая количество делителей заданного числа
г) Нет правильного ответа

6. Что такое простое число?
а) Число, имеющее только два делителя: 1 и само число
б) Число, имеющее три делителя
в) Число, имеющее четыре делителя
г) Нет правильного ответа

7. Что такое наибольший общий делитель (НОД) двух чисел?
а) Наибольшее число, на которое делятся оба числа
б) Наименьшее число, на которое делятся оба числа
в) Среднее арифметическое двух чисел
г) Нет правильного ответа

8. Что такое делимость чисел?
а) Возможность без остатка разделить одно число на другое
б) Свойство числа быть четным
в) Свойство числа быть нечетным
г) Нет правильного ответа

9. Что такое полная система вычетов по модулю?
а) Множество классов, содержащих все возможные числа
б) Множество классов, содержащих только нечетные числа
в) Множество классов, содержащих только простые числа
г) Нет правильного ответа

10. Что такое линейное диофантово уравнение?
а) Уравнение вида ax + by = c, где a, b, c - целые числа
б) Уравнение вида ax ≡ b (mod n), где a, b, n - целые числа
в) Уравнение вида ax^2 + bx + c = 0, где a, b, c - целые числа
г) Нет правильного ответа

11. Что такое составное число?
а) Число, имеющее только два делителя: 1 и само число
б) Число, имеющее три делителя
в) Число, имеющее четыре делителя
г) Нет правильного ответа

12. Что такое группа в алгебре?
а) Множество с определенной ассоциативной операцией
б) Множество с операцией сложения
в) Множество с операцией умножения
г) Нет правильного ответа

13. Что такое кольцо?
а) Множество с операцией сложения и умножения
б) Множество с операцией вычитания и деления
в) Множество с операцией возведения в степень
г) Нет правильного ответа

14. Что такое поле?

а) Множество, обладающее свойствами группы и кольца
б) Множество с операциями сложения, вычитания, умножения и деления
в) Множество с операциями возведения в степень и корень
г) Нет правильного ответа

15. Что такое взаимно простые числа?
а) Числа, у которых НОД равен 1
б) Числа, у которых НОД равен 2
а) Числа, у которых НОД равен 2
в) Числа, у которых НОД равен 0
г) Нет правильного ответа

16. Какой признак делимости позволяет проверить делимость числа на 2?
а) Признак делимости на 3
б) Признак делимости на 4
в) Признак делимости на 5
г) Признак делимости на 2

17. Какой алгоритм используется для нахождения НОД двух чисел?
а) Алгоритм Евклида
б) Алгоритм Ферма
в) Алгоритм Шорра
г) Алгоритм Полларда

18. Какой алгоритм используется для решения линейных диофантовых уравнений?
а) Алгоритм Евклида
б) Алгоритм Ферма
в) Расширенный алгоритм Евклида
г) Алгоритм Шорра

19. Что утверждает основная теорема арифметики?
а) Всякое натуральное число можно представить в виде произведения простых чисел
б) Всякое натуральное число можно представить в виде суммы простых чисел
в) Всякое натуральное число можно представить в виде разности простых чисел
г) Всякое натуральное число можно представить в виде деления на простое число

20. Что такое сравнение первой степени?
а) Сравнение двух чисел по модулю
б) Решение уравнения вида $ax \equiv b \pmod{n}$
в) Сравнение двух чисел по степени
г) Нет правильного ответа

Критерии оценивания рубежной аттестации:

Количество вопросов	Оценка	
16-20	**5**	**аттестован**
11-15	**4**	
6-10	**3**	
0-5	**2**	**не аттестован**

Аттестован - выставляется обучающемуся, ответившему правильно на 6-20 вопросов.
Не аттестован - выставляется обучающемуся, который ответил на 5 и менее вопроса.
Отлично - выставляется обучающемуся, ответившему на 16-20 вопросов.
Хорошо - выставляется обучающемуся, ответившему на 11-15 вопросов.
Удовлетворительно - выставляется обучающемуся, ответившему на 6-10 вопросов.

Ключи к тесту

№ п/п	Вариант № 1	Вариант № 2	Вариант №3	Вариант №4
1	а	г	а	а
2	г	а	б	б
3	а	а	а	а
4	б	а	а	а
5	а	б	а	а
6	а	а	а	а
7	а	а	а	а
8	а	б	а	а
9	б	а	а	а
10	а	а	а	а
11	б	б	г	г
12	а	а	а	а
13	а	а	б	а
14	а	а	а	б
15	а	а	а	а
16	г	г	б	г
17	а	а	г	а
18	а	а	а	в
19	а	в	в	а
20	в	а	а	б

Вопросы ко 2-ой рубежной аттестации

1. Какие методы криптографической защиты можно классифицировать как симметричные шифры?
2. Какой из следующих методов криптографической защиты является простой заменой?
3. Какой метод разрешения основан на замене каждого символа в открытый текст другим символом?
4. Какой метод шифрования основан на перестановке символов в открытый текст?
5. Какой метод шифрования использует случайные символы для формирования зашифрованного текста?
6. Какой метод шифрования использует фиксированную таблицу для замены символов в открытом тексте?
7. Какой метод шифрования использует последовательности ключей для генерации зашифрованного текста?
8. Какую из следующих атак можно использовать для замены расшифровки шифра?
9. Какую из следующих атак можно использовать для расшифровки метода перестановки?
10. Что означает криптографическая стойкость?
11. Каковы принципы Киркхоффса с криптографической стойкостью?
12. Какие криптосистемы можно назвать абсолютно стойкими?
13. Какая из последующих криптографических атак использует большое количество зашифрованных сообщений с известными открытыми текстами?
14. Что из следующего нападает на анализ признаков шифрованного текста?
15. Какое условие должно выполняться для абсолютно стойкой криптосистемы?
16. Какой метод криптоанализа основан на анализе небольших изменений входных данных и их обработке в выходные данные?
17. Какую из следующих атак можно использовать для расшифровки шифра замены известными открытыми и зашифрованными текстами?
18. Какую из следующих атак можно использовать для расшифровки метод перестановки с известными открытыми и зашифрованными текстами?
19. Какой метод шифрования является наиболее распространенным и использует один ключ для шифрования и расшифрования?
20. Какой принцип Киркхоффса утверждает, что безопасность криптосистемы не должна защищать от секретности алгоритма шифрования?
21. Какая атака основана на анализе времени, затрачиваемом на шифрование или расшифрование данных?
22. Какие атаки основаны на анализе линейных зависимостей между входными и выходными данными криптосистемы?
23. Какой метод криптоанализа основан на использовании большого количества зашифрованных и расшифрованных сообщений?
24. Какой метод криптоанализа основан на изучении изменений входных данных и их обработки в выходные дни в криптосистемах данных?
25. Что такое атака «человек посередине» в десятках криптографических систем и сетевой безопасности?

Образец билета ко 2-ой рубежной аттестации

Федеральное государственное бюджетное образовательное учреждение высшегообразования
Грозненский государственный нефтяной технический университет
им. акад. М.Д.Миллионщикова
Факультет среднего профессионального образования
Тестовое задание
по модулю МДК.02.02 «Криптографические средства защиты информации»
II-аттестация
Вариант №___

ФИО_____групп_____Дата

№ вопроса	1	2	3	4	5	6	7	8	9	10
Ответ										
№ вопроса	11	12	13	14	15	16	17	18	19	20
Ответ										

Вариант №1

1. Какие методы криптографической защиты можно классифицировать как симметричные шифры?
а) Шифры замены
б) Методы перестановки
в) Гаммирование
г) Все вышеперечисленные

2. Какой метод разрешения основан на замене каждого символа в открытый текст другим символом?
а) Многоалфавитная подстановка
б) Пропорциональный шифр
в) Гаммирование
г) Табличная перестановка

3. Какой метод шифрования основан на перестановке символов в открытый текст?
а) Табличная перестановка
б) Многоалфавитная подстановка
в) Пропорциональный шифр
г) Гаммирование

4. Какой метод шифрования использует случайные символы для формирования зашифрованного текста?
а) Гаммирование с конечной гаммой
б) Гаммирование с бесконечной гаммой
в) Многоалфавитная подстановка
г) Пропорциональный шифр

5. Какой метод шифрования использует фиксированную таблицу для замены символов в открытом тексте?
а) Многоалфавитная подстановка

б) Табличная перестановка
в) Пропорциональный шифр
г) Гаммирование

6. Какой метод шифрования использует последовательности ключей для генерации зашифрованного текста?
а) Гаммирование с конечной гаммой
б) Гаммирование с бесконечной гаммой
в) Многоалфавитная подстановка
г) Табличная перестановка

7. Какую из следующих атак можно использовать для расшифровки метода перестановки?
а) Атака по частотному анализу
б) Дифференциальный криптоанализ
в) Линейный криптоанализ
г) Атака по времени

8. Какую из следующих атак можно использовать для расшифровки шифра замены известными открытыми и зашифрованными текстами?
а) Частотный анализ
б) Дифференциальный криптоанализ
в) Линейный криптоанализ
г) Атака по времени

9. Что означает криптографическая стойкость?
а) Способность криптосистемы защищать от атак
б) Сложность криптосистемы в США
в) Скорость шифрования и расшифрования
г) Размер ключа шифрования

10. Какие криптосистемы можно назвать абсолютно стойкими?
а) КГБ-шифр
б) РСА
в) Шифр Вернама
г) АЕС

11. Какой метод криптоанализа основан на анализе небольших изменений входных данных и их обработке в выходные данные?
а) Дифференциальный криптоанализ
б) Линейный криптоанализ
в) Атака по времени
г) Криптоанализ с выбранным открытым текстом

12. Какой метод шифрования является наиболее распространенным и использует один ключ для шифрования и расшифрования?
а) Многоалфавитная подстановка
б) Гаммирование
в) Табличная перестановка
г) Симметричное шифрование

13. Что такое атака "человек посередине" в десятках криптографических систем и сетевой безопасности?
а) Это атака, в ходе которой злоумышленник перехватывает и изменяет служебные данные между

двумя участниками коммуникации, не вызывая у них подозрений.
б) Это атака, в результате которой злоумышленник проникает в систему и получает несанкционированный доступ к конфиденциальным данным.
в) Это нападение, при котором злоумышленник отправляет измененные данные с целью нарушения работоспособности системы.
г) Это нападение, при котором злоумышленник угрожает использовать секретную информацию для шантажа или вымогательства.

14. Какой принцип Киркхоффса утверждает, что безопасность криптосистемы не должна защищать от секретности алгоритма шифрования?
а) Принцип открытости
б) Принцип секретности
в) Принцип стойкости
г) Принцип эффективности

15. Какая атака основана на анализе времени, затрачиваемом на шифрование или расшифрование данных?
а) Атака по частотному анализу
б) Дифференциальный криптоанализ
в) Атака по времени
г) Линейный криптоанализ

16. Какие атаки основаны на анализе линейных зависимостей между входными и выходными данными криптосистемы?
а) Атака по частотному анализу
б) Дифференциальный криптоанализ
в) Атака по времени
г) Линейный криптоанализ

17. Какой метод криптоанализа основан на использовании большого количества зашифрованных и расшифрованных сообщений?
а) Криптоанализ с выбранным открытым текстом
б) Криптоанализ с выбранным зашифрованным текстом
в) Дифференциальный криптоанализ
г) Линейный криптоанализ

18. Какой метод криптоанализа основан на изучении изменений входных данных и их обработки в выходные дни в криптосистемах данных?
а) Дифференциальный криптоанализ
б) Линейный криптоанализ
в) Криптоанализ с выбранным открытым текстом
г) Криптоанализ с выбранным зашифрованным текстом

19. Какую из следующих атак можно использовать для расшифровки метод перестановки с известными открытыми и зашифрованными текстами?
а) Частотный анализ
б) Дифференциальный криптоанализ
в) Линейный криптоанализ
г) Атака по времени

20. Какое условие должно выполняться для абсолютно стойкой криптосистемы?
а) Сложность алгоритма шифрования
б) Долговечность алгоритма шифрования

в) Ключ должен быть случайным и использоваться только один раз
г) Известность алгоритма шифрования

Вариант №2

1. Какие методы криптографической защиты можно классифицировать как симметричные шифры?
а) Шифры замены
б) Методы перестановки
в) Гаммирование
г) Все вышеперечисленные

2. Какой из следующих методов криптографической защиты является простой заменой?
а) Многоалфавитная подстановка
б) Табличная перестановка
в) Пропорциональный шифр
г) Маршрутная перестановка

3. Какой метод разрешения основан на замене каждого символа в открытый текст другим символом?
а) Многоалфавитная подстановка
б) Пропорциональный шифр
в) Гаммирование
г) Табличная перестановка

4. Какой метод шифрования основан на перестановке символов в открытый текст?
а) Табличная перестановка
б) Многоалфавитная подстановка
в) Пропорциональный шифр
г) Гаммирование

5. Какой метод шифрования использует случайные символы для формирования зашифрованного текста?
а) Гаммирование с конечной гаммой
б) Гаммирование с бесконечной гаммой
в) Многоалфавитная подстановка
г) Пропорциональный шифр

6. Какой метод шифрования использует фиксированную таблицу для замены символов в открытом тексте?
а) Многоалфавитная подстановка
б) Табличная перестановка
в) Пропорциональный шифр
г) Гаммирование

7. Какой метод шифрования использует последовательности ключей для генерации зашифрованного текста?
а) Гаммирование с конечной гаммой
б) Гаммирование с бесконечной гаммой
в) Многоалфавитная подстановка

г) Табличная перестановка

8. Какую из следующих атак можно использовать для замены расшифровки шифра?
а) Атака по частотному анализу
б) Дифференциальный криптоанализ
в) Линейный криптоанализ
г) Атака по времени

9. Какую из следующих атак можно использовать для расшифровки метода перестановки?
а) Атака по частотному анализу
б) Дифференциальный криптоанализ
в) Линейный криптоанализ
г) Атака по времени

10. Что означает криптографическая стойкость?
а) Способность криптосистемы защищать от атак
б) Сложность криптосистемы в США
в) Скорость шифрования и расшифрования
г) Размер ключа шифрования

11. Каковы принципы Киркхоффса с криптографической стойкостью?
а) Безопасность должна основываться на секретности ключа
б) Криптосистема должна быть простой в использовании
в) Криптосистема должна быть стойкой даже при известном алгоритме
г) Все вышеперечисленные

12. Какие криптосистемы можно назвать абсолютно стойкими?
а) КГБ-шифр
б) РСА
в) Шифр Вернама
г) АЕС

13. Какая из последующих криптографических атак использует большое количество зашифрованных сообщений с известными открытыми текстами?
а) Атака по частотному анализу
б) Дифференциальный криптоанализ
в) Криптоанализ с выбранным открытым текстом
г) Криптоанализ с выбранным зашифрованным текстом

14. Что из следующего нападает на анализ признаков шифрованного текста?
а) Атака по частотному анализу
б) Дифференциальный криптоанализ
в) Атака по времени
г) Линейный криптоанализ

15. Какое условие должно выполняться для абсолютно стойкой криптосистемы?
а) Сложность алгоритма шифрования
б) Долговечность алгоритма шифрования
в) Ключ должен быть случайным и использоваться только один раз
г) Известность алгоритма шифрования

16. Какой метод криптоанализа основан на анализе небольших изменений входных данных и их обработке в выходные данные?

а) Дифференциальный криптоанализ
б) Линейный криптоанализ
в) Атака по времени
г) Криптоанализ с выбранным открытым текстом

17. Какую из следующих атак можно использовать для расшифровки шифра замены известными открытыми и зашифрованными текстами?
а) Частотный анализ
б) Дифференциальный криптоанализ
в) Линейный криптоанализ
г) Атака по времени

18. Какую из следующих атак можно использовать для расшифровки метода перестановки?
а) Атака по частотному анализу
б Дифференциальный криптоанализ
в) Линейный криптоанализ
г) Атака по времени

19. Какой метод шифрования является наиболее распространенным и использует один ключ для шифрования и расшифрования?
а) Многоалфавитная подстановка
б) Гаммирование
в) Табличная перестановка
г) Симметричное шифрование

20. Какой принцип Киркхоффса утверждает, что безопасность криптосистемы не должна защищать от секретности алгоритма шифрования?
а) Принцип открытости
б) Принцип секретности
в) Принцип стойкости
г) Принцип эффективности

Вариант №3

1. Какой метод шифрования использует фиксированную таблицу для замены символов в открытом тексте?
а) Многоалфавитная подстановка
б) Табличная перестановка
в) Пропорциональный шифр
г) Гаммирование

2. Какую из следующих атак можно использовать для расшифровки шифра замены известными открытыми и зашифрованными текстами?
а) Частотный анализ
б) Дифференциальный криптоанализ
в) Линейный криптоанализ
г) Атака по времени

3. Какой метод шифрования использует случайные символы для формирования зашифрованного текста?
а) Гаммирование с конечной гаммой

б) Гаммирование с бесконечной гаммой
в) Многоалфавитная подстановка
г) Пропорциональный шифр

4. Какой метод разрешения основан на замене каждого символа в открытый текст другим символом?
а) Многоалфавитная подстановка
б) Пропорциональный шифр
в) Гаммирование
г) Табличная перестановка

5. Какой принцип Киркхоффса утверждает, что безопасность криптосистемы не должна защищать от секретности алгоритма шифрования?
а) Принцип открытости
б) Принцип секретности
в) Принцип стойкости
г) Принцип эффективности

6. Какой метод криптоанализа основан на использовании большого количества зашифрованных и расшифрованных сообщений?
а) Криптоанализ с выбранным открытым текстом
б) Криптоанализ с выбранным зашифрованным текстом
в) Дифференциальный криптоанализ
г) Линейный криптоанализ

7. Что из следующего нападает на анализ признаков шифрованного текста?
а) Атака по частотному анализу
б) Дифференциальный криптоанализ
в) Атака по времени
г) Линейный криптоанализ

8. Какой метод криптоанализа основан на анализе небольших изменений входных данных и их обработке в выходные данные?
а) Дифференциальный криптоанализ
б) Линейный криптоанализ
в) Атака по времени
г) Криптоанализ с выбранным открытым текстом

9. Какие методы криптографической защиты можно классифицировать как симметричные шифры?
а) Шифры замены
б) Методы перестановки
в) Гаммирование
г) Все вышеперечисленные

10. Какую из следующих атак можно использовать для расшифровки метода перестановки?
а) Атака по частотному анализу
б) Дифференциальный криптоанализ
в) Линейный криптоанализ
г) Атака по времени

11. Какой метод шифрования основан на перестановке символов в открытый текст?
а) Табличная перестановка

б) Многоалфавитная подстановка
в) Пропорциональный шифр
г) Гаммирование

12. Какая атака основана на анализе времени, затрачиваемом на шифрование или расшифрование данных?
а) Атака по частотному анализу
б) Дифференциальный криптоанализ
в) Атака по времени
г) Линейный криптоанализ

13. Какой метод криптоанализа основан на изучении изменений входных данных и их обработки в выходные дни в криптосистемах данных?
а) Дифференциальный криптоанализ
б) Линейный криптоанализ
в) Криптоанализ с выбранным открытым текстом
г) Криптоанализ с выбранным зашифрованным текстом

14. Какую из следующих атак можно использовать для замены расшифровки шифра?
а) Атака по частотному анализу
б) Дифференциальный криптоанализ
в) Линейный криптоанализ
г) Атака по времени

15. Какая атака основана на анализе времени, затрачиваемом на шифрование или расшифрование данных?
а) Атака по частотному анализу
б) Дифференциальный криптоанализ
в) Атака по времени
г) Линейный криптоанализ

16. Какой метод шифрования использует последовательности ключей для генерации зашифрованного текста?
а) Гаммирование с конечной гаммой
б) Гаммирование с бесконечной гаммой
в) Многоалфавитная подстановка
г) Табличная перестановка

17. Какой метод криптографической защиты является простой заменой?
а) Многоалфавитная подстановка
б) Табличная перестановка
в) Пропорциональный шифр
г) Маршрутная перестановка

18. Какое условие должно выполняться для абсолютно стойкой криптосистемы?
а) Сложность алгоритма шифрования
б) Долговечность алгоритма шифрования
в) Ключ должен быть случайным и использоваться только один раз
г) Известность алгоритма шифрования

19. Какие атаки основаны на анализе линейных зависимостей между входными и выходными данными криптосистемы?
а) Атака по частотному анализу

б) Дифференциальный криптоанализ
в) Атака по времени
г) Линейный криптоанализ

20. Какие криптосистемы можно назвать абсолютно стойкими?
а) КГБ-шифр
б) РСА
в) Шифр Вернама
г) АЕС

Вариант №4

1. Какой метод шифрования использует случайные символы для формирования зашифрованного текста?
а) Гаммирование с конечной гаммой
б) Гаммирование с бесконечной гаммой
в) Многоалфавитная подстановка
г) Пропорциональный шифр

2. Какую из следующих атак можно использовать для расшифровки метода перестановки?
а) Атака по частотному анализу
б) Дифференциальный криптоанализ
в) Линейный криптоанализ
г) Атака по времени

3. Какое условие должно выполняться для абсолютно стойкой криптосистемы?
а) Сложность алгоритма шифрования
б) Долговечность алгоритма шифрования
в) Ключ должен быть случайным и использоваться только один раз
г) Известность алгоритма шифрования

4. Какой метод разрешения основан на замене каждого символа в открытый текст другим символом?
а) Многоалфавитная подстановка
б) Пропорциональный шифр
в) Гаммирование
г) Табличная перестановка

5. Какие криптосистемы можно назвать абсолютно стойкими?
а) КГБ-шифр
б) РСА
в) Шифр Вернама
г) АЕС

6. Какую из следующих атак можно использовать для расшифровки шифра замены известными открытыми и зашифрованными текстами?
а) Частотный анализ
б) Дифференциальный криптоанализ
в) Линейный криптоанализ
г) Атака по времени

7. Какой метод шифрования использует фиксированную таблицу для замены символов в открытом тексте?

а) Многоалфавитная подстановка
б) Табличная перестановка
в) Пропорциональный шифр
г) Гаммирование

8. Какой метод криптоанализа основан на изучении изменений входных данных и их обработки в выходные дни в криптосистемах данных?

а) Дифференциальный криптоанализ
б) Линейный криптоанализ
в) Криптоанализ с выбранным открытым текстом
г) Криптоанализ с выбранным зашифрованным текстом

9. Каковы принципы Киркхоффса с криптографической стойкостью?

а) Безопасность должна основываться на секретности ключа
б) Криптосистема должна быть простой в использовании
в) Криптосистема должна быть стойкой даже при известном алгоритме
г) Все вышеперечисленные

10. Какая атака основана на анализе времени, затрачиваемом на шифрование или расшифрование данных?

а) Атака по частотному анализу
б) Дифференциальный криптоанализ
в) Атака по времени
г) Линейный криптоанализ

11. Что означает криптографическая стойкость?

а) Способность криптосистемы защищать от атак
б) Сложность криптосистемы в США
в) Скорость шифрования и расшифрования
г) Размер ключа шифрования

12. Какие методы криптографической защиты можно классифицировать как симметричные шифры?

а) Шифры замены
б) Методы перестановки
в) Гаммирование
г) Все вышеперечисленные

13. Какой метод шифрования основан на перестановке символов в открытый текст?

а) Табличная перестановка
б) Многоалфавитная подстановка
в) Пропорциональный шифр
г) Гаммирование

14. Какую из следующих атак можно использовать для замены расшифровки шифра?

а) Атака по частотному анализу
б) Дифференциальный криптоанализ
в) Линейный криптоанализ
г) Атака по времени

15. Какую из следующих атак можно использовать для расшифровки метод перестановки с известными открытыми и зашифрованными текстами?
а) Частотный анализ
б) Дифференциальный криптоанализ
в) Линейный криптоанализ
г) Атака по времени

16. Какой метод криптоанализа основан на анализе небольших изменений входных данных и их обработке в выходные данные?
а) Дифференциальный криптоанализ
б) Линейный криптоанализ
в) Атака по времени
г) Криптоанализ с выбранным открытым текстом

17. Какой метод шифрования использует последовательности ключей для генерации зашифрованного текста?
а) Гаммирование с конечной гаммой
б) Гаммирование с бесконечной гаммой
в) Многоалфавитная подстановка
г) Табличная перестановка

18. Какая из последующих криптографических атак использует большое количество зашифрованных сообщений с известными открытыми текстами?
а) Атака по частотному анализу
б) Дифференциальный криптоанализ
в) Криптоанализ с выбранным открытым текстом
г) Криптоанализ с выбранным зашифрованным текстом

19. Какой принцип Киркхоффса утверждает, что безопасность криптосистемы не должна защищать от секретности алгоритма шифрования?
а) Принцип открытости
б) Принцип секретности
в) Принцип стойкости
г) Принцип эффективности

20. Какой метод шифрования является наиболее распространенным и использует один ключ для шифрования и расшифрования?
а) Многоалфавитная подстановка
б) Гаммирование
в) Табличная перестановка
г) Симметричное шифрование

Критерии оценивания рубежной аттестации:

Количество вопросов	Оценка	
16-20	**5**	**аттестован**
11-15	**4**	
6-10	**3**	
0-5	**2**	**не аттестован**

Аттестован - выставляется обучающемуся, ответившему правильно на 6-20 вопросов.
Не аттестован - выставляется обучающемуся, который ответил на 5 и менее вопроса.
Отлично - выставляется обучающемуся, ответившему на 16-20 вопросов.
Хорошо - выставляется обучающемуся, ответившему на 11-15 вопросов.
Удовлетворительно - выставляется обучающемуся, ответившему на 6-10 вопросов.

Ключи к тесту

№ п/п	Вариант № 1	Вариант № 2	Вариант №3	Вариант №4
1	г	г	б	а
2	а	в	а	г
3	а	а	а	в
4	а	а	а	а
5	б	а	а	в
6	а	б	а	а
7	г	а	а	б
8	а	а	а	а
9	а	г	г	а, в
10	а	а	г	в
11	а	а, в	а	а
12	г	в	в	г
13	а	в	а	а
14	а	а	а	а
15	в	в	в	г
16	г	а	а	а
17	а	а	в	а
18	а	г	в	в
19	г	г	г	а
20	в	а	в	г

Образец билета к зачету

Федеральное государственное бюджетное образовательное учреждение высшегообразования
Грозненский государственный нефтяной технический университет
им. акад. М.Д.Миллионщикова
Факультет среднего профессионального образования
Тестовое задание
по модулю МДК.02.02 «Криптографические средства защиты информации»
Зачет
Вариант №___

ФИО_____групп_____Дата

№ вопроса	1	2	3	4	5	6	7	8	9	10
Ответ										
№ вопроса	11	12	13	14	15	16	17	18	19	20
Ответ										
№ вопроса	21	22	23	24	25	26	27	28	29	30
Ответ										
№ вопроса	31	32	33	34	35	36	37	38	39	40
Ответ										

Вариант №1

1. Что такое составное число?
а) Число, имеющее только два делителя: 1 и само число
б) Число, имеющее три делителя
в) Число, имеющее четыре делителя
г) Нет правильного ответа

2. Что такое простое число?
а) Число, имеющее только два делителя: 1 и само число
б) Число, имеющее три делителя
в) Число, имеющее четыре делителя
г) Нет правильного ответа

3. Что такое криптография?
а) Наука, изучающая методы защиты информации
б) Наука, изучающая методы сжатия информации
в) Наука, изучающая методы передачи информации
г) Нет правильного ответа

4. Что такое группа в алгебре?
а) Множество с определенной ассоциативной операцией
б) Множество с операцией сложения
в) Множество с операцией умножения
г) Нет правильного ответа

5. Что такое сравнение первой степени?

а) Сравнение двух чисел по модулю
б) Решение уравнения вида $ax \equiv b \pmod{n}$
в) Сравнение двух чисел по степени
г) Нет правильного ответа

6. Что такое наибольший общий делитель (НОД) двух чисел?

а) Наибольшее число, на которое делятся оба числа
б) Наименьшее число, на которое делятся оба числа
в) Среднее арифметическое двух чисел
г) Нет правильного ответа

7. Что такое модулярная арифметика?

а) Арифметика, основанная на операциях с остатками от деления
б) Арифметика, основанная на операциях с десятичными числами
в) Арифметика, основанная на операциях с отрицательными числами
г) Нет правильного ответа

8. Что такое поле?

а) Множество, обладающее свойствами группы и кольца
б) Множество с операциями сложения, вычитания, умножения и деления
в) Множество с операциями возведения в степень и корень
г) Нет правильного ответа

9. Что такое делимость чисел?

а) Возможность без остатка разделить одно число на другое
б) Свойство числа быть четным
в) Свойство числа быть нечетным
г) Нет правильного ответа

10. Что такое симметричное шифрование?

а) Тип шифрования, при котором используется один и тот же ключ для шифрования и расшифрования
б) Тип шифрования, при котором используются разные ключи для шифрования и расшифрования
в) Тип шифрования, при котором не используются ключи
г) Нет правильного ответа

11. Что такое асимметричное шифрование?

а) Тип шифрования, при котором используется один и тот же ключ для шифрования и расшифрования
б) Тип шифрования, при котором используются разные ключи для шифрования и расшифрования
в) Тип шифрования, при котором не используются ключи
г) Нет правильного ответа

12. Что такое кольцо?

а) Множество с операцией сложения и умножения
б) Множество с операцией вычитания и деления
в) Множество с операцией возведения в степень
г) Нет правильного ответа

13. Что такое полная система вычетов по модулю?

а) Множество классов, содержащих все возможные числа

б) Множество классов, содержащих только нечетные числа
в) Множество классов, содержащих только простые числа
г) Нет правильного ответа

14. Что такое функция Эйлера?
а) Функция, определяющая количество взаимно простых чисел с заданным числом
б) Функция, определяющая количество простых чисел до заданного числа
в) Функция, определяющая количество делителей заданного числа
г) Нет правильного ответа

15. Что такое линейное диофантово уравнение?
а) Уравнение вида ax + by = c, где a, b, c - целые числа
б) Уравнение вида ax ≡ b (mod n), где a, b, n - целые числа
в) Уравнение вида ax^2 + bx + c = 0, где a, b, c - целые числа
г) Нет правильного ответа

16. Какой признак делимости позволяет проверить делимость числа на 2?
а) Признак делимости на 3
б) Признак делимости на 4
в) Признак делимости на 5
г) Признак делимости на 2

17. Какой алгоритм используется для нахождения НОД двух чисел?
а) Алгоритм Евклида
б) Алгоритм Ферма
в) Алгоритм Шорра
г) Алгоритм Полларда

18. Что такое взаимно простые числа?
а) Числа, у которых НОД равен 1
б) Числа, у которых НОД равен 2
а) Числа, у которых НОД равен 2
в) Числа, у которых НОД равен 0
г) Нет правильного ответа

19. Какой алгоритм используется для решения линейных диофантовых уравнений?
а) Алгоритм Евклида
б) Алгоритм Ферма
в) Расширенный алгоритм Евклида
г) Алгоритм Шорра

20. Что утверждает основная теорема арифметики?
а) Всякое натуральное число можно представить в виде произведения простых чисел
б) Всякое натуральное число можно представить в виде суммы простых чисел
в) Всякое натуральное число можно представить в виде разности простых чисел
г) Всякое натуральное число можно представить в виде деления на простое число

21. Какой метод шифрования использует фиксированную таблицу для замены символов в открытом тексте?
а) Многоалфавитная подстановка
б) Табличная перестановка
в) Пропорциональный шифр
г) Гаммирование

22. Какую из следующих атак можно использовать для расшифровки шифра замены известными открытыми и зашифрованными текстами?
а) Частотный анализ
б) Дифференциальный криптоанализ
в) Линейный криптоанализ
г) Атака по времени

23. Какой метод шифрования использует случайные символы для формирования зашифрованного текста?
а) Гаммирование с конечной гаммой
б) Гаммирование с бесконечной гаммой
в) Многоалфавитная подстановка
г) Пропорциональный шифр

24. Какой метод разрешения основан на замене каждого символа в открытый текст другим символом?
а) Многоалфавитная подстановка
б) Пропорциональный шифр
в) Гаммирование
г) Табличная перестановка

25. Какой принцип Киркхоффса утверждает, что безопасность криптосистемы не должна защищать от секретности алгоритма шифрования?
а) Принцип открытости
б) Принцип секретности
в) Принцип стойкости
г) Принцип эффективности

26. Какой метод криптоанализа основан на использовании большого количества зашифрованных и расшифрованных сообщений?
а) Криптоанализ с выбранным открытым текстом
б) Криптоанализ с выбранным зашифрованным текстом
в) Дифференциальный криптоанализ
г) Линейный криптоанализ

27. Что из следующего нападает на анализ признаков шифрованного текста?
а) Атака по частотному анализу
б) Дифференциальный криптоанализ
в) Атака по времени
г) Линейный криптоанализ

28. Какой метод криптоанализа основан на анализе небольших изменений входных данных и их обработке в выходные данные?
а) Дифференциальный криптоанализ
б) Линейный криптоанализ
в) Атака по времени
г) Криптоанализ с выбранным открытым текстом

29. Какие методы криптографической защиты можно классифицировать как симметричные шифры?
а) Шифры замены
б) Методы перестановки

в) Гаммирование
г) Все вышеперечисленные

30. Какую из следующих атак можно использовать для расшифровки метода перестановки?
а) Атака по частотному анализу
б) Дифференциальный криптоанализ
в) Линейный криптоанализ
г) Атака по времени

31. Какой метод шифрования основан на перестановке символов в открытый текст?
а) Табличная перестановка
б) Многоалфавитная подстановка
в) Пропорциональный шифр
г) Гаммирование

32. Какая атака основана на анализе времени, затрачиваемом на шифрование или расшифрование данных?
а) Атака по частотному анализу
б) Дифференциальный криптоанализ
в) Атака по времени
г) Линейный криптоанализ

33. Какой метод криптоанализа основан на изучении изменений входных данных и их обработки в выходные дни в криптосистемах данных?
а) Дифференциальный криптоанализ
б) Линейный криптоанализ
в) Криптоанализ с выбранным открытым текстом
г) Криптоанализ с выбранным зашифрованным текстом

34. Какую из следующих атак можно использовать для замены расшифровки шифра?
а) Атака по частотному анализу
б) Дифференциальный криптоанализ
в) Линейный криптоанализ
г) Атака по времени

35. Какая атака основана на анализе времени, затрачиваемом на шифрование или расшифрование данных?
а) Атака по частотному анализу
б) Дифференциальный криптоанализ
в) Атака по времени
г) Линейный криптоанализ

36. Какой метод шифрования использует последовательности ключей для генерации зашифрованного текста?
а) Гаммирование с конечной гаммой
б) Гаммирование с бесконечной гаммой
в) Многоалфавитная подстановка
г) Табличная перестановка

37. Какой метод криптографической защиты является простой заменой?
а) Многоалфавитная подстановка
б) Табличная перестановка
в) Пропорциональный шифр

г) Маршрутная перестановка

38. Какое условие должно выполняться для абсолютно стойкой криптосистемы?
а) Сложность алгоритма шифрования
б) Долговечность алгоритма шифрования
в) Ключ должен быть случайным и использоваться только один раз
г) Известность алгоритма шифрования

39. Какие атаки основаны на анализе линейных зависимостей между входными и выходными данными криптосистемы?
а) Атака по частотному анализу
б) Дифференциальный криптоанализ
в) Атака по времени
г) Линейный криптоанализ

40. Какие криптосистемы можно назвать абсолютно стойкими?
а) КГБ-шифр
б) РСА
в) Шифр Вернама

Вариант №2

1. Что такое множество в теории множеств?
а) Совокупность элементов, не имеющая порядка
б) Упорядоченная совокупность элементов
в) Взаимосвязанные элементы
г) Нет правильного ответа

2. Какой признак делимости позволяет проверить делимость числа на 2?
а) Признак делимости на 3
б) Признак делимости на 4
в) Признак делимости на 5
г) Признак делимости на 2

3. Что такое группа в алгебре?
а) Множество с определенной ассоциативной операцией
б) Множество с операцией сложения
в) Множество с операцией умножения
г) Нет правильного ответа

4. Что такое сравнение первой степени?
а) Сравнение двух чисел по модулю
б) Решение уравнения вида $ax \equiv b \pmod n$
в) Сравнение двух чисел по степени
г) Нет правильного ответа

5. Что такое наибольший общий делитель (НОД) двух чисел?
а) Наибольшее число, на которое делятся оба числа
б) Наименьшее число, на которое делятся оба числа
в) Среднее арифметическое двух чисел

г) Нет правильного ответа

6. Что такое простое число?

а) Число, имеющее только два делителя: 1 и само число
б) Число, имеющее три делителя
в) Число, имеющее четыре делителя
г) Нет правильного ответа

7. Что такое симметричное шифрование?

а) Тип шифрования, при котором используется один и тот же ключ для шифрования и расшифрования
б) Тип шифрования, при котором используются разные ключи для шифрования и расшифрования
в) Тип шифрования, при котором не используются ключи
г) Нет правильного ответа

8. Что такое криптография?

а) Наука, изучающая методы защиты информации
б) Наука, изучающая методы сжатия информации
в) Наука, изучающая методы передачи информации
г) Нет правильного ответа

9. Что такое асимметричное шифрование?

а) Тип шифрования, при котором используется один и тот же ключ для шифрования и расшифрования
б) Тип шифрования, при котором используются разные ключи для шифрования и расшифрования
в) Тип шифрования, при котором не используются ключи
г) Нет правильного ответа

10. Что такое модулярная арифметика?

а) Арифметика, основанная на операциях с остатками от деления
б) Арифметика, основанная на операциях с десятичными числами
в) Арифметика, основанная на операциях с отрицательными числами
г) Нет правильного ответа

11. Что такое поле?

а) Множество, обладающее свойствами группы и кольца
б) Множество с операциями сложения, вычитания, умножения и деления
в) Множество с операциями возведения в степень и корень
г) Нет правильного ответа

12. Что такое функция Эйлера?

а) Функция, определяющая количество взаимно простых чисел с заданным числом
б) Функция, определяющая количество простых чисел до заданного числа
в) Функция, определяющая количество делителей заданного числа
г) Нет правильного ответа

13. Что такое полная система вычетов по модулю?

а) Множество классов, содержащих все возможные числа
б) Множество классов, содержащих только нечетные числа
в) Множество классов, содержащих только простые числа
г) Нет правильного ответа

14. Что такое делимость чисел?

а) Возможность без остатка разделить одно число на другое
б) Свойство числа быть четным
в) Свойство числа быть нечетным
г) Нет правильного ответа

15. Что такое линейное диофантово уравнение?
а) Уравнение вида ax + by = c, где a, b, c - целые числа
б) Уравнение вида ax ≡ b (mod n), где a, b, n - целые числа
в) Уравнение вида ax^2 + bx + c = 0, где a, b, c - целые числа
г) Нет правильного ответа

16. Что такое составное число?
а) Число, имеющее только два делителя: 1 и само число
б) Число, имеющее три делителя
в) Число, имеющее четыре делителя
г) Нет правильного ответа

17. Что такое кольцо?
а) Множество с операцией сложения и умножения
б) Множество с операцией вычитания и деления
в) Множество с операцией возведения в степень
г) Нет правильного ответа

18. Что такое взаимно простые числа?
а) Множество с операцией сложения и умножения
б) Множество с операцией вычитания и деления
в) Множество с операцией возведения в степень
г) Нет правильного ответа

19. Какой алгоритм используется для нахождения НОД двух чисел?
а) Алгоритм Евклида
б) Алгоритм Ферма
в) Алгоритм Шорра
г) Алгоритм Полларда

20. Какой алгоритм используется для решения линейных диофантовых уравнений?
а) Алгоритм Евклида
б) Алгоритм Ферма
в) Расширенный алгоритм Евклида
г) Алгоритм Шорра

21. Какой метод шифрования использует случайные символы для формирования зашифрованного текста?
а) Гаммирование с конечной гаммой
б) Гаммирование с бесконечной гаммой
в) Многоалфавитная подстановка
г) Пропорциональный шифр

22. Какую из следующих атак можно использовать для расшифровки метода перестановки?
а) Атака по частотному анализу
б) Дифференциальный криптоанализ
в) Линейный криптоанализ
г) Атака по времени

23. Какое условие должно выполняться для абсолютно стойкой криптосистемы?
а) Сложность алгоритма шифрования
б) Долговечность алгоритма шифрования
в) Ключ должен быть случайным и использоваться только один раз
г) Известность алгоритма шифрования

24. Какой метод разрешения основан на замене каждого символа в открытый текст другим символом?
а) Многоалфавитная подстановка
б) Пропорциональный шифр
в) Гаммирование
г) Табличная перестановка

25. Какие криптосистемы можно назвать абсолютно стойкими?
а) КГБ-шифр
б) РСА
в) Шифр Вернама
г) АЕС

26. Какую из следующих атак можно использовать для расшифровки шифра замены известными открытыми и зашифрованными текстами?
а) Частотный анализ
б) Дифференциальный криптоанализ
в) Линейный криптоанализ
г) Атака по времени

27. Какой метод шифрования использует фиксированную таблицу для замены символов в открытом тексте?
а) Многоалфавитная подстановка
б) Табличная перестановка
в) Пропорциональный шифр
г) Гаммирование

28. Какой метод криптоанализа основан на изучении изменений входных данных и их обработки в выходные дни в криптосистемах данных?
а) Дифференциальный криптоанализ
б) Линейный криптоанализ
в) Криптоанализ с выбранным открытым текстом
г) Криптоанализ с выбранным зашифрованным текстом

29. Каковы принципы Киркхоффса с криптографической стойкостью?
а) Безопасность должна основываться на секретности ключа
б) Криптосистема должна быть простой в использовании
в) Криптосистема должна быть стойкой даже при известном алгоритме
г) Все вышеперечисленные

30. Какая атака основана на анализе времени, затрачиваемом на шифрование или расшифрование данных?
а) Атака по частотному анализу
б) Дифференциальный криптоанализ
в) Атака по времени
г) Линейный криптоанализ

31. Что означает криптографическая стойкость?
а) Способность криптосистемы защищать от атак
б) Сложность криптосистемы в США
в) Скорость шифрования и расшифрования
г) Размер ключа шифрования

32. Какие методы криптографической защиты можно классифицировать как симметричные шифры?
а) Шифры замены
б) Методы перестановки
в) Гаммирование
г) Все вышеперечисленные

33. Какой метод шифрования основан на перестановке символов в открытый текст?
а) Табличная перестановка
б) Многоалфавитная подстановка
в) Пропорциональный шифр
г) Гаммирование

34. Какую из следующих атак можно использовать для замены расшифровки шифра?
а) Атака по частотному анализу
б) Дифференциальный криптоанализ
в) Линейный криптоанализ
г) Атака по времени

35. Какую из следующих атак можно использовать для расшифровки метод перестановки с известными открытыми и зашифрованными текстами?
а) Частотный анализ
б) Дифференциальный криптоанализ
в) Линейный криптоанализ
г) Атака по времени

36. Какой метод криптоанализа основан на анализе небольших изменений входных данных и их обработке в выходные данные?
а) Дифференциальный криптоанализ
б) Линейный криптоанализ
в) Атака по времени
г) Криптоанализ с выбранным открытым текстом

37. Какой метод шифрования использует последовательности ключей для генерации зашифрованного текста?
а) Гаммирование с конечной гаммой
б) Гаммирование с бесконечной гаммой
в) Многоалфавитная подстановка
г) Табличная перестановка

38. Какая из последующих криптографических атак использует большое количество зашифрованных сообщений с известными открытыми текстами?
а) Атака по частотному анализу
б) Дифференциальный криптоанализ
в) Криптоанализ с выбранным открытым текстом
г) Криптоанализ с выбранным зашифрованным текстом

39. Какой принцип Киркхоффса утверждает, что безопасность криптосистемы не должна защищать от секретности алгоритма шифрования?
а) Принцип открытости
б) Принцип секретности
в) Принцип стойкости
г) Принцип эффективности

40. Какой метод шифрования является наиболее распространенным и использует один ключ для шифрования и расшифрования?
а) Многоалфавитная подстановка
б) Гаммирование
в) Табличная перестановка
г) Симметричное шифрование

Вариант №3

1. Что такое модулярная арифметика?
а) Арифметика, основанная на операциях с остатками от деления
б) Арифметика, основанная на операциях с десятичными числами
в) Арифметика, основанная на операциях с отрицательными числами
г) Нет правильного ответа

2. Что такое сравнение первой степени?
а) Сравнение двух чисел по модулю
б) Решение уравнения вида $ax \equiv b \pmod{n}$
в) Сравнение двух чисел по степени
г) Нет правильного ответа

3. Что такое кольцо?
а) Множество с операцией сложения и умножения
б) Множество с операцией вычитания и деления
в) Множество с операцией возведения в степень
г) Нет правильного ответа

4. Что такое группа в алгебре?
а) Множество с определенной ассоциативной операцией
б) Множество с операцией сложения
в) Множество с операцией умножения
г) Нет правильного ответа

5. Что такое функция Эйлера?
а) Функция, определяющая количество взаимно простых чисел с заданным числом
б) Функция, определяющая количество простых чисел до заданного числа
в) Функция, определяющая количество делителей заданного числа
г) Нет правильного ответа

6. Что такое наибольший общий делитель (НОД) двух чисел?
а) Наибольшее число, на которое делятся оба числа
б) Наименьшее число, на которое делятся оба числа

в) Среднее арифметическое двух чисел
г) Нет правильного ответа

7. Что такое простое число?
а) Число, имеющее только два делителя: 1 и само число
б) Число, имеющее три делителя
в) Число, имеющее четыре делителя
г) Нет правильного ответа

8. Что такое делимость чисел?
а) Возможность без остатка разделить одно число на другое
б) Свойство числа быть четным
в) Свойство числа быть нечетным
г) Нет правильного ответа

9. Что такое полная система вычетов по модулю?
а) Множество классов, содержащих все возможные числа
б) Множество классов, содержащих только нечетные числа
в) Множество классов, содержащих только простые числа
г) Нет правильного ответа

10. Что такое линейное диофантово уравнение?
а) Уравнение вида ax + by = c, где a, b, c - целые числа
б) Уравнение вида ax ≡ b (mod n), где a, b, n - целые числа
в) Уравнение вида ax^2 + bx + c = 0, где a, b, c - целые числа
г) Нет правильного ответа

11. Что такое составное число?
а) Число, имеющее только два делителя: 1 и само число
б) Число, имеющее три делителя
в) Число, имеющее четыре делителя
г) Нет правильного ответа

12. Что такое криптография?
а) Наука, изучающая методы защиты информации
б) Наука, изучающая методы сжатия информации
в) Наука, изучающая методы передачи информации
г) Нет правильного ответа

13. Что такое поле?
а) Множество, обладающее свойствами группы и кольца
б) Множество с операциями сложения, вычитания, умножения и деления
в) Множество с операциями возведения в степень и корень
г) Нет правильного ответа

14. Что такое взаимно простые числа?
а) Числа, у которых НОД равен 1
б) Числа, у которых НОД равен 2
а) Числа, у которых НОД равен 2
в) Числа, у которых НОД равен 0
г) Нет правильного ответа

15. Что такое симметричное шифрование?

а) Тип шифрования, при котором используется один и тот же ключ для шифрования и расшифрования
б) Тип шифрования, при котором используются разные ключи для шифрования и расшифрования
в) Тип шифрования, при котором не используются ключи
г) Нет правильного ответа

16. Что такое асимметричное шифрование?
а) Тип шифрования, при котором используется один и тот же ключ для шифрования и расшифрования
б) Тип шифрования, при котором используются разные ключи для шифрования и расшифрования
в) Тип шифрования, при котором не используются ключи
г) Нет правильного ответа

17. Какой признак делимости позволяет проверить делимость числа на 2?
а) Признак делимости на 3
б) Признак делимости на 4
в) Признак делимости на 5
г) Признак делимости на 2

18. Какой алгоритм используется для нахождения НОД двух чисел?
а) Алгоритм Евклида
б) Алгоритм Ферма
в) Алгоритм Шорра
г) Алгоритм Полларда

19. Какой алгоритм используется для решения линейных диофантовых уравнений?
а) Алгоритм Евклида
б) Алгоритм Ферма
в) Расширенный алгоритм Евклида
г) Алгоритм Шорра

20. Что утверждает основная теорема арифметики?
а) Всякое натуральное число можно представить в виде произведения простых чисел
б) Всякое натуральное число можно представить в виде суммы простых чисел
в) Всякое натуральное число можно представить в виде разности простых чисел
г) Всякое натуральное число можно представить в виде деления на простое число

21. Какие методы криптографической защиты можно классифицировать как симметричные шифры?
а) Шифры замены
б) Методы перестановки
в) Гаммирование
г) Все вышеперечисленные

22. Какой метод разрешения основан на замене каждого символа в открытый текст другим символом?
а) Многоалфавитная подстановка
б) Пропорциональный шифр
в) Гаммирование
г) Табличная перестановка

23. Какой метод шифрования основан на перестановке символов в открытый текст?
а) Табличная перестановка

б) Многоалфавитная подстановка
в) Пропорциональный шифр
г) Гаммирование

24. Какой метод шифрования использует случайные символы для формирования зашифрованного текста?
а) Гаммирование с конечной гаммой
б) Гаммирование с бесконечной гаммой
в) Многоалфавитная подстановка
г) Пропорциональный шифр

25. Какой метод шифрования использует фиксированную таблицу для замены символов в открытом тексте?
а) Многоалфавитная подстановка
б) Табличная перестановка
в) Пропорциональный шифр
г) Гаммирование

26. Какой метод шифрования использует последовательности ключей для генерации зашифрованного текста?
а) Гаммирование с конечной гаммой
б) Гаммирование с бесконечной гаммой
в) Многоалфавитная подстановка
г) Табличная перестановка

27. Какую из следующих атак можно использовать для расшифровки метода перестановки?
а) Атака по частотному анализу
б) Дифференциальный криптоанализ
в) Линейный криптоанализ
г) Атака по времени

28. Какую из следующих атак можно использовать для расшифровки шифра замены известными открытыми и зашифрованными текстами?
а) Частотный анализ
б) Дифференциальный криптоанализ
в) Линейный криптоанализ
г) Атака по времени

29. Что означает криптографическая стойкость?
а) Способность криптосистемы защищать от атак
б) Сложность криптосистемы в США
в) Скорость шифрования и расшифрования
г) Размер ключа шифрования

30. Какие криптосистемы можно назвать абсолютно стойкими?
а) КГБ-шифр
б) РСА
в) Шифр Вернама
г) АЕС

31. Какой метод криптоанализа основан на анализе небольших изменений входных данных и их обработке в выходные данные?
а) Дифференциальный криптоанализ

б) Линейный криптоанализ
в) Атака по времени
г) Криптоанализ с выбранным открытым текстом

32. Какой метод шифрования является наиболее распространенным и использует один ключ для шифрования и расшифрования?
а) Многоалфавитная подстановка
б) Гаммирование
в) Табличная перестановка
г) Симметричное шифрование

33. Что такое атака "человек посередине" в десятках криптографических систем и сетевой безопасности?
а) Это атака, в ходе которой злоумышленник перехватывает и изменяет служебные данные между двумя участниками коммуникации, не вызывая у них подозрений.
б) Это атака, в результате которой злоумышленник проникает в систему и получает несанкционированный доступ к конфиденциальным данным.
в) Это нападение, при котором злоумышленник отправляет измененные данные с целью нарушения работоспособности системы.
г) Это нападение, при котором злоумышленник угрожает использовать секретную информацию для шантажа или вымогательства.

34. Какой принцип Киркхоффса утверждает, что безопасность криптосистемы не должна защищать от секретности алгоритма шифрования?
а) Принцип открытости
б) Принцип секретности
в) Принцип стойкости
г) Принцип эффективности

35. Какая атака основана на анализе времени, затрачиваемом на шифрование или расшифрование данных?
а) Атака по частотному анализу
б) Дифференциальный криптоанализ
в) Атака по времени
г) Линейный криптоанализ

36. Какие атаки основаны на анализе линейных зависимостей между входными и выходными данными криптосистемы?
а) Атака по частотному анализу
б) Дифференциальный криптоанализ
в) Атака по времени
г) Линейный криптоанализ

37. Какой метод криптоанализа основан на использовании большого количества зашифрованных и расшифрованных сообщений?
а) Криптоанализ с выбранным открытым текстом
б) Криптоанализ с выбранным зашифрованным текстом
в) Дифференциальный криптоанализ
г) Линейный криптоанализ

38. Какой метод криптоанализа основан на изучении изменений входных данных и их обработки в выходные дни в криптосистемах данных?
а) Дифференциальный криптоанализ

б) Линейный криптоанализ
в) Криптоанализ с выбранным открытым текстом
г) Криптоанализ с выбранным зашифрованным текстом

39. Какую из следующих атак можно использовать для расшифровки метод перестановки с известными открытыми и зашифрованными текстами?
а) Частотный анализ
б) Дифференциальный криптоанализ
в) Линейный криптоанализ
г) Атака по времени

40. Какое условие должно выполняться для абсолютно стойкой криптосистемы?
а) Сложность алгоритма шифрования
б) Долговечность алгоритма шифрования
в) Ключ должен быть случайным и использоваться только один раз
г) Известность алгоритма шифрования

Вариант №4

1. Что такое симметричное шифрование?
а) Тип шифрования, при котором используется один и тот же ключ для шифрования и расшифрования
б) Тип шифрования, при котором используются разные ключи для шифрования и расшифрования
в) Тип шифрования, при котором не используются ключи
г) Нет правильного ответа

2. Что такое асимметричное шифрование?
а) Тип шифрования, при котором используется один и тот же ключ для шифрования и расшифрования
б) Тип шифрования, при котором используются разные ключи для шифрования и расшифрования
в) Тип шифрования, при котором не используются ключи
г) Нет правильного ответа

3. Что такое криптография?
а) Наука, изучающая методы защиты информации
б) Наука, изучающая методы сжатия информации
в) Наука, изучающая методы передачи информации
г) Нет правильного ответа

4. Что такое модулярная арифметика?
а) Арифметика, основанная на операциях с остатками от деления
б) Арифметика, основанная на операциях с десятичными числами
в) Арифметика, основанная на операциях с отрицательными числами
г) Нет правильного ответа

5. Что такое функция Эйлера?
а) Функция, определяющая количество взаимно простых чисел с заданным числом
б) Функция, определяющая количество простых чисел до заданного числа
в) Функция, определяющая количество делителей заданного числа
г) Нет правильного ответа

6. Что такое простое число?
а) Число, имеющее только два делителя: 1 и само число
б) Число, имеющее три делителя
в) Число, имеющее четыре делителя
г) Нет правильного ответа

7. Что такое наибольший общий делитель (НОД) двух чисел?
а) Наибольшее число, на которое делятся оба числа
б) Наименьшее число, на которое делятся оба числа
в) Среднее арифметическое двух чисел
г) Нет правильного ответа

8. Что такое делимость чисел?
а) Возможность без остатка разделить одно число на другое
б) Свойство числа быть четным
в) Свойство числа быть нечетным
г) Нет правильного ответа

9. Что такое полная система вычетов по модулю?
а) Множество классов, содержащих все возможные числа
б) Множество классов, содержащих только нечетные числа
в) Множество классов, содержащих только простые числа
г) Нет правильного ответа

10. Что такое линейное диофантово уравнение?
а) Уравнение вида $ax + by = c$, где a, b, c - целые числа
б) Уравнение вида $ax \equiv b \pmod n$, где a, b, n - целые числа
в) Уравнение вида $ax^2 + bx + c = 0$, где a, b, c - целые числа
г) Нет правильного ответа

11. Что такое составное число?
а) Число, имеющее только два делителя: 1 и само число
б) Число, имеющее три делителя
в) Число, имеющее четыре делителя
г) Нет правильного ответа

12. Что такое группа в алгебре?
а) Множество с определенной ассоциативной операцией
б) Множество с операцией сложения
в) Множество с операцией умножения
г) Нет правильного ответа

13. Что такое кольцо?
а) Множество с операцией сложения и умножения
б) Множество с операцией вычитания и деления
в) Множество с операцией возведения в степень
г) Нет правильного ответа

14. Что такое поле?
а) Множество, обладающее свойствами группы и кольца
б) Множество с операциями сложения, вычитания, умножения и деления
в) Множество с операциями возведения в степень и корень
г) Нет правильного ответа

15. Что такое взаимно простые числа?
а) Числа, у которых НОД равен 1
б) Числа, у которых НОД равен 2
а) Числа, у которых НОД равен 2
в) Числа, у которых НОД равен 0
г) Нет правильного ответа

16. Какой признак делимости позволяет проверить делимость числа на 2?
а) Признак делимости на 3
б) Признак делимости на 4
в) Признак делимости на 5
г) Признак делимости на 2

17. Какой алгоритм используется для нахождения НОД двух чисел?
а) Алгоритм Евклида
б) Алгоритм Ферма
в) Алгоритм Шорра
г) Алгоритм Полларда

18. Какой алгоритм используется для решения линейных диофантовых уравнений?
а) Алгоритм Евклида
б) Алгоритм Ферма
в) Расширенный алгоритм Евклида
г) Алгоритм Шорра

19. Что утверждает основная теорема арифметики?
а) Всякое натуральное число можно представить в виде произведения простых чисел
б) Всякое натуральное число можно представить в виде суммы простых чисел
в) Всякое натуральное число можно представить в виде разности простых чисел
г) Всякое натуральное число можно представить в виде деления на простое число

20. Что такое сравнение первой степени?
а) Сравнение двух чисел по модулю
б) Решение уравнения вида $ax \equiv b \pmod{n}$
в) Сравнение двух чисел по степени
г) Нет правильного ответа

21. Какие методы криптографической защиты можно классифицировать как симметричные шифры?
а) Шифры замены
б) Методы перестановки
в) Гаммирование
г) Все вышеперечисленные

22. Какой из следующих методов криптографической защиты является простой заменой?
а) Многоалфавитная подстановка
б) Табличная перестановка
в) Пропорциональный шифр
г) Маршрутная перестановка

23. Какой метод разрешения основан на замене каждого символа в открытый текст другим символом?

а) Многоалфавитная подстановка
б) Пропорциональный шифр
в) Гаммирование
г) Табличная перестановка

24. Какой метод шифрования основан на перестановке символов в открытый текст?
а) Табличная перестановка
б) Многоалфавитная подстановка
в) Пропорциональный шифр
г) Гаммирование

25. Какой метод шифрования использует случайные символы для формирования зашифрованного текста?
а) Гаммирование с конечной гаммой
б) Гаммирование с бесконечной гаммой
в) Многоалфавитная подстановка
г) Пропорциональный шифр

26. Какой метод шифрования использует фиксированную таблицу для замены символов в открытом тексте?
а) Многоалфавитная подстановка
б) Табличная перестановка
в) Пропорциональный шифр
г) Гаммирование

27. Какой метод шифрования использует последовательности ключей для генерации зашифрованного текста?
а) Гаммирование с конечной гаммой
б) Гаммирование с бесконечной гаммой
в) Многоалфавитная подстановка
г) Табличная перестановка

28. Какую из следующих атак можно использовать для замены расшифровки шифра?
а) Атака по частотному анализу
б) Дифференциальный криптоанализ
в) Линейный криптоанализ
г) Атака по времени

29. Какую из следующих атак можно использовать для расшифровки метода перестановки?
а) Атака по частотному анализу
б) Дифференциальный криптоанализ
в) Линейный криптоанализ
г) Атака по времени

30. Что означает криптографическая стойкость?
а) Способность криптосистемы защищать от атак
б) Сложность криптосистемы в США
в) Скорость шифрования и расшифрования
г) Размер ключа шифрования

31. Каковы принципы Киркхоффса с криптографической стойкостью?
а) Безопасность должна основываться на секретности ключа
б) Криптосистема должна быть простой в использовании

в) Криптосистема должна быть стойкой даже при известном алгоритме
г) Все вышеперечисленные

32. Какие криптосистемы можно назвать абсолютно стойкими?
а) КГБ-шифр
б) РСА
в) Шифр Вернама
г) АЕС

33. Какая из последующих криптографических атак использует большое количество зашифрованных сообщений с известными открытыми текстами?
а) Атака по частотному анализу
б) Дифференциальный криптоанализ
в) Криптоанализ с выбранным открытым текстом
г) Криптоанализ с выбранным зашифрованным текстом

34. Что из следующего нападает на анализ признаков шифрованного текста?
а) Атака по частотному анализу
б) Дифференциальный криптоанализ
в) Атака по времени
г) Линейный криптоанализ

35. Какое условие должно выполняться для абсолютно стойкой криптосистемы?
а) Сложность алгоритма шифрования
б) Долговечность алгоритма шифрования
в) Ключ должен быть случайным и использоваться только один раз
г) Известность алгоритма шифрования

36. Какой метод криптоанализа основан на анализе небольших изменений входных данных и их обработке в выходные данные?
а) Дифференциальный криптоанализ
б) Линейный криптоанализ
в) Атака по времени
г) Криптоанализ с выбранным открытым текстом

37. Какую из следующих атак можно использовать для расшифровки шифра замены известными открытыми и зашифрованными текстами?
а) Частотный анализ
б) Дифференциальный криптоанализ
в) Линейный криптоанализ
г) Атака по времени

38. Какую из следующих атак можно использовать для расшифровки метода перестановки?
а) Атака по частотному анализу
б Дифференциальный криптоанализ
в) Линейный криптоанализ
г) Атака по времени

39. Какой метод шифрования является наиболее распространенным и использует один ключ для шифрования и расшифрования?
а) Многоалфавитная подстановка
б) Гаммирование
в) Табличная перестановка

г) Симметричное шифрование

40. Какой принцип Киркхоффса утверждает, что безопасность криптосистемы не должна защищать от секретности алгоритма шифрования?
а) Принцип открытости
б) Принцип секретности
в) Принцип стойкости
г) Принцип эффективности

Критерии оценивания экзамена (зачета):

Количество вопросов	Оценка	
31-40	**5**	**зачтено**
21-30	**4**	
11-20	**3**	
0-10	**2**	**не зачтено**

Зачтено - выставляется обучающемуся, ответившему правильно на 11-40 вопросов.
Не зачтено - выставляется обучающемуся, который ответил на 10 и менее вопросов.
Отлично - выставляется обучающемуся, ответившему на 31-40 вопросов.
Хорошо - выставляется обучающемуся, ответившему на 21-30 вопросов.
Удовлетворительно - выставляется обучающемуся, ответившему на 11-20 вопросов.

Ключи к тесту

№ п/п	Вариант № 1	Вариант № 2	Вариант №3	Вариант №4
1	г	а	а	а
2	а	г	б	б
3	а	а	а	а
4	а	б	а	а
5	б	а	а	а
6	а	а	а	а
7	а	а	а	а
8	б	а	а	а
9	а	б	а	а
10	а	а	а	а
11	б	б	г	г
12	а	а	а	а
13	а	а	б	а
14	а	а	а	б
15	а	а	а	а
16	г	г	б	г
17	а	а	г	а
18	а	а	а	в

19	в	а	в	а
20	а	в	а	б
21	б	а	г	г
22	а	г	а	в
23	а	в	а	а
24	а	а	а	а
25	а	в	б	а
26	а	а	а	б
27	а	б	г	а
28	а	а	а	а
29	г	а, в	а	г
30	г	в	а	а
31	а	а	а	а, в
32	в	г	г	в
33	а	а	а	в
34	а	а	а	а
35	в	г	в	в
36	а	а	г	а
37	в	а	а	а
38	в	в	а	г
39	г	а	г	г
40	в	г	в	а

Вопросы рубежного контроля по модулю
«Криптографические средства защиты информации» на 8 семестр.

Вопросы к 1-ой рубежной аттестации

1. Что такое поточное шифрование?
2. Какие принципы лежат в основе поточного шифрования?
3. Что такое генераторы ПСЧ?
4. Какие методы используются для получения псевдослучайных последовательностей?
5. Какие методы кодирования информации вы знаете?
6. Что представляет собой таблица ASCII?
7. Что такое механизация шифрования?
8. Что такое компьютеризация шифрования?
9. Что такое аппаратное шифрование?
10. Что такое программное шифрование?
11. Что такое стандартизация программно-аппаратных криптографических систем и средств?
12. Что такое симметричные криптографические системы?
13. Что такое отечественные алгоритмы Магма и Кузнечик?
14. Какие стандарты соответствуют алгоритмам Магма и Кузнечик?
15. Какие алгоритмы относятся к симметричным алгоритмам?
16. Что такое DES?
17. Что такое AES?
18. Какие ключевые размеры поддерживает AES?
19. Что такое асимметричные криптографические системы?
20. Какой алгоритм шифрования наиболее широко используется в асимметричной криптографии?
21. Что такое алгоритм RSA?
22. Что такое цифровая подпись?
23. Что такое хэш-функция?
24. Какие основные свойства должны обладать хорошая хэш-функция?
25. Что такое атака на основе словаря (dictionary attack)?

Образец билета к 1-ой рубежной аттестации

Федеральное государственное бюджетное образовательное учреждение высшегообразования
Грозненский государственный нефтяной технический университет
им. акад. М.Д.Миллионщикова
Факультет среднего профессионального образования
Тестовое задание
по модулю МДК.02.02 «Криптографические средства защиты информации»
I-аттестация
Вариант №___

ФИО_____групп_____Дата

№ вопроса	1	2	3	4	5	6	7	8	9	10
Ответ										
№ вопроса	11	12	13	14	15	16	17	18	19	20
Ответ										

Вариант №1

1. **Что такое поточное шифрование?**

а) Многоалфавитная подстановка
б) Гаммирование
в) Табличная перестановка
г) Симметричное шифрование

2. **Какие принципы лежат в основе поточного шифрования?**

а) XOR и сдвиг
б) RSA и диффи-хеллман
в) Хеш-функции и эллиптические кривые
г) Линейные операции и перестановки

3. **Что такое генераторы ПСЧ?**

а) Устройства для генерации случайных чисел
б) Устройства для генерации псевдослучайных чисел
в) Устройства для генерации паролей
г) Устройства для генерации хэш-кодов

4. **Какие методы используются для получения псевдослучайных последовательностей?**

а) Линейный конгруэнтный генератор, метод Фибоначчи, метод Блума
б) Линейно-сдвиговый регистр, метод RSA, метод Монте-Карло
в) Линейный конгруэнтный генератор, метод Фибоначчи, метод BBS
г) Метод DES, метод AES, метод ГОСТ 28147-89

5. **Какие методы кодирования информации вы знаете?**

а) Символьное кодирование, смысловое кодирование, бинарное кодирование
б) Хаффмановское кодирование, кодирование Хемминга, кодирование CRC
в) Бинарное кодирование, кодирование Грея, кодирование Рида-Соломона
г) Бинарное кодирование, кодирование Грея, кодирование Фибоначчи

6. **Что представляет собой таблица ASCII?**

а) Таблица символов и их двоичных представлений
б) Таблица символов и их шестнадцатеричных представлений
в) Таблица символов и их десятичных представлений
г) Таблица символов и их восьмеричных представлений

7. Что такое механизация шифрования?
а) Процесс автоматизации шифрования
б) Процесс механического шифрования
в) Процесс программного шифрования
г) Процесс смешанного шифрования

8. Что такое компьютеризация шифрования?
а) Процесс применения компьютеров для шифрования данных
б) Процесс разработки компьютерных программ для шифрования
в) Процесс разработки компьютерных алгоритмов шифрования
г) Процесс применения компьютерных средств для анализа шифров

9. Что такое аппаратное шифрование?
а) Шифрование, выполняемое программными средствами
б) Шифрование, выполняемое специализированными устройствами
в) Шифрование, выполняемое с помощью аппаратных ключей
г) Шифрование, выполняемое на аппаратных уровнях компьютера

10. Что такое программное шифрование?
а) Шифрование, выполняемое с использованием программных средств
б) Шифрование, выполняемое на уровне операционной системы
в) Шифрование, выполняемое на уровне ядра компьютера
г) Шифрование, выполняемое на уровне аппаратных устройств

11. Что такое стандартизация программно-аппаратных криптографических систем и средств?
а) Процесс разработки и утверждения стандартов для криптографических систем и средств
б) Процесс тестирования и сертификации криптографических систем и средств
в) Процесс патентования и лицензирования криптографических систем и средств
г) Процесс разработки и маркировки криптографических систем и средств

12. Что такое симметричные криптографические системы?
а) Системы, использующие один и тот же ключ для шифрования и расшифрования данных
б) Системы, использующие разные ключи для шифрования и расшифрования данных
в) Системы, использующие открытый ключ для шифрования и закрытый ключ для расшифрования данных
г) Системы, использующие хэш-функции для шифрования данных

13. Что такое отечественные алгоритмы Магма и Кузнечик?
а) Симметричные алгоритмы шифрования, разработанные в России
б) Асимметричные алгоритмы шифрования, разработанные в России
в) Хэш-функции, разработанные в России
г) Алгоритмы цифровой подписи, разработанные в России

14. Какие стандарты соответствуют алгоритмам Магма и Кузнечик?
а) ГОСТ Р 34.12-2015 и ГОСТ Р 34.13-2015
б) ГОСТ Р 28147-89 и ГОСТ Р 34.11-2012
в) ГОСТ Р 34.10-2012 и ГОСТ Р 34.12-2015

г) ГОСТ Р 34.13-2015 и ГОСТ Р 34.11-2012

15. Какие алгоритмы относятся к симметричным алгоритмам?
а) RSA, DSA, ECDSA, ElGamal
б) DES, AES, ГОСТ 28147-89, RC4
в) SHA-1, SHA-256, MD5, HMAC
г) Diffie-Hellman, RSA, ElGamal, DSA

16. Что такое DES?
а) Симметричный алгоритм шифрования с блочным размером 64 бита
б) Асимметричный алгоритм шифрования с блочным размером 64 бита
в) Хэш-функция с блочным размером 64 бита
г) Алгоритм цифровой подписи с блочным размером 64 бита

17. Что такое AES?
а) Симметричный алгоритм шифрования с блочным размером 128 бит
б) Асимметричный алгоритм шифрования с блочным размером 128 бит
в) Хэш-функция с блочным размером 128 бит
г) Алгоритм цифровой подписи с блочным размером 128 бит

18. Какие ключевые размеры поддерживает AES?
а) 64 бит, 256 бит, 512 бит
б) 64 бит, 128 бит, 256 бит
в) 128 бит, 256 бит, 512 бит
г) 128 бит, 192 бит, 256 бит

19. Что такое асимметричные криптографические системы?
а) Системы, использующие один и тот же ключ для шифрования и расшифрования данных
б) Системы, использующие разные ключи для шифрования и расшифрования данных
в) Системы, использующие открытый ключ для шифрования и закрытый ключ для расшифрования данных
г) Системы, использующие хэш-функции для шифрования данных

20. Какой алгоритм шифрования наиболее широко используется в асимметричной криптографии?
а) DES
б) AES
в) RSA
г) HMAC

Вариант №2

1. Что такое поточное шифрование?
а) Шифрование, использующее потоки данных
б) Шифрование, использующее блоки данных
в) Шифрование, использующее хэш-функции
г) Шифрование, использующее симметричные ключи

2. Что такое асимметричные криптографические системы?
а) Системы, использующие один и тот же ключ для шифрования и расшифрования данных
б) Системы, использующие разные ключи для шифрования и расшифрования данных

в) Системы, использующие открытый ключ для шифрования и закрытый ключ для расшифрования данных
г) Системы, использующие хэш-функции для шифрования данных

3. Что такое генераторы ПСЧ?
а) Устройства для генерации случайных чисел
б) Устройства для генерации псевдослучайных чисел
в) Устройства для генерации паролей
г) Устройства для генерации хэш-кодов

4. Что такое алгоритм RSA?
а) Асимметричный алгоритм шифрования и подписи
б) Симметричный алгоритм шифрования
в) Хэш-функция
г) Алгоритм генерации случайных чисел

5. Какие методы используются для получения псевдослучайных последовательностей?
а) Линейный конгруэнтный генератор, метод Фибоначчи, метод Блума
б) Линейно-сдвиговый регистр, метод RSA, метод Монте-Карло
в) Линейный конгруэнтный генератор, метод Фибоначчи, метод BBS
г) Метод DES, метод AES, метод ГОСТ 28147-89

6. Что такое хэш-функция?
а) Математическая функция, преобразующая входные данные в случайную последовательность битов
б) Математическая функция, преобразующая входные данные в строку переменной длины
в) Математическая функция, преобразующая входные данные в фиксированную строку фиксированной длины
г) Математическая функция, используемая для шифрования данных

7. Какие основные свойства должны обладать хорошая хэш-функция?
а) Односторонняя функция, стойкость к коллизиям, равномерное распределение значений
б) Обратимость, стойкость к коллизиям, высокая скорость вычислений
в) Стойкость к коллизиям, равномерное распределение значений, высокая скорость вычислений
г) Обратимость, стойкость к коллизиям, равномерное распределение значений

8. Что такое цифровая подпись?
а) Процесс расшифрования данных с использованием закрытого ключа
б) Процесс шифрования данных с использованием открытого ключа
в) Алгоритм, используемый для генерации псевдослучайных чисел
г) Математическая конструкция, позволяющая установить авторство и целостность сообщения

9. Что такое механизация шифрования?
а) Процесс автоматизации шифрования
б) Процесс механического шифрования
в) Процесс программного шифрования
г) Процесс смешанного шифрования

10. Какие методы кодирования информации вы знаете?
а) Символьное кодирование, смысловое кодирование, бинарное кодирование
б) Хаффмановское кодирование, кодирование Хемминга, кодирование CRC
в) Бинарное кодирование, кодирование Грея, кодирование Рида-Соломона
г) Бинарное кодирование, кодирование Грея, кодирование Фибоначчи

11. Что такое компьютеризация шифрования?
а) Процесс применения компьютеров для шифрования данных
б) Процесс разработки компьютерных программ для шифрования
в) Процесс разработки компьютерных алгоритмов шифрования
г) Процесс применения компьютерных средств для анализа шифров

12. Что представляет собой таблица ASCII?
а) Таблица символов и их двоичных представлений
б) Таблица символов и их шестнадцатеричных представлений
в) Таблица символов и их десятичных представлений
г) Таблица символов и их восьмеричных представлений

13. Что такое атака на основе словаря (dictionary attack)?
а) Атака, при которой злоумышленник пытается получить доступ к системе, подбирая разные словарные слова
б) Атака, при которой злоумышленник перебирает все возможные комбинации паролей из заданного словаря
в) Атака, при которой злоумышленник обменивается словарями с другими злодеями
г) Атака, при которой не используются общеупотребительные слова или фразы из словарей для компрометации учетных данных пользователя

14. Что такое аппаратное шифрование?
а) Шифрование, выполняемое программными средствами
б) Шифрование, выполняемое специализированными устройствами
в) Шифрование, выполняемое с помощью аппаратных ключей
г) Шифрование, выполняемое на аппаратных уровнях компьютера

15. Что такое программное шифрование?
а) Шифрование, выполняемое с использованием программных средств
б) Шифрование, выполняемое на уровне операционной системы
в) Шифрование, выполняемое на уровне ядра компьютера
г) Шифрование, выполняемое на уровне аппаратных устройств

16. Что такое стандартизация программно-аппаратных криптографических систем и средств?
а) Процесс разработки и утверждения стандартов для криптографических систем и средств
б) Процесс тестирования и сертификации криптографических систем и средств
в) Процесс патентования и лицензирования криптографических систем и средств
г) Процесс разработки и маркировки криптографических систем и средств

17. Что такое симметричные криптографические системы?
а) Системы, использующие один и тот же ключ для шифрования и расшифрования данных
б) Системы, использующие разные ключи для шифрования и расшифрования данных
в) Системы, использующие открытый ключ для шифрования и закрытый ключ для расшифрования данных
г) Системы, использующие хэш-функции для шифрования данных

18. Что такое отечественные алгоритмы Магма и Кузнечик?
а) Симметричные алгоритмы шифрования, разработанные в России
б) Асимметричные алгоритмы шифрования, разработанные в России
в) Хэш-функции, разработанные в России
г) Алгоритмы цифровой подписи, разработанные в России

19. Какие стандарты соответствуют алгоритмам Магма и Кузнечик?
а) ГОСТ Р 34.12-2015 и ГОСТ Р 34.13-2015
б) ГОСТ Р 28147-89 и ГОСТ Р 34.11-2012
в) ГОСТ Р 34.10-2012 и ГОСТ Р 34.12-2015
г) ГОСТ Р 34.13-2015 и ГОСТ Р 34.11-2012

20. Какой алгоритм шифрования наиболее широко используется в асимметричной криптографии?
а) DES
б) AES
в) RSA
г) HMAC

Вариант №3

1. Что такое генераторы ПСЧ?
а) Устройства для генерации случайных чисел
б) Устройства для генерации псевдослучайных чисел
в) Устройства для генерации паролей
г) Устройства для генерации хэш-кодов

2. Что такое алгоритм RSA?
а) Асимметричный алгоритм шифрования и подписи
б) Симметричный алгоритм шифрования
в) Хэш-функция
г) Алгоритм генерации случайных чисел

3. Что такое поточное шифрование?
а) Шифрование, использующее потоки данных
б) Шифрование, использующее блоки данных
в) Шифрование, использующее хэш-функции
г) Шифрование, использующее симметричные ключи

4. Что такое атака на основе словаря (dictionary attack)?
а) Атака, при которой злоумышленник пытается получить доступ к системе, подбирая разные словарные слова
б) Атака, при которой злоумышленник перебирает все возможные комбинации паролей из заданного словаря
в) Атака, при которой злоумышленник обменивается словарями с другими злодеями
г) Атака, при которой не используются общеупотребительные слова или фразы из словарей для компрометации учетных данных пользователя

5. Какие методы кодирования информации вы знаете?
а) Символьное кодирование, смысловое кодирование, бинарное кодирование
б) Хаффмановское кодирование, кодирование Хемминга, кодирование CRC
в) Бинарное кодирование, кодирование Грея, кодирование Рида-Соломона
г) Бинарное кодирование, кодирование Грея, кодирование Фибоначчи

6. Что такое асимметричные криптографические системы?
а) Системы, использующие один и тот же ключ для шифрования и расшифрования данных

б) Системы, использующие разные ключи для шифрования и расшифрования данных
в) Системы, использующие открытый ключ для шифрования и закрытый ключ для расшифрования данных
г) Системы, использующие хэш-функции для шифрования данных

7. Что такое программное шифрование?
а) Шифрование, выполняемое с использованием программных средств
б) Шифрование, выполняемое на уровне операционной системы
в) Шифрование, выполняемое на уровне ядра компьютера
г) Шифрование, выполняемое на уровне аппаратных устройств

8. Что такое хэш-функция?
а) Математическая функция, преобразующая входные данные в случайную последовательность битов
б) Математическая функция, преобразующая входные данные в строку переменной длины
в) Математическая функция, преобразующая входные данные в фиксированную строку фиксированной длины
г) Математическая функция, используемая для шифрования данных

9. Что такое механизация шифрования?
а) Процесс автоматизации шифрования
б) Процесс механического шифрования
в) Процесс программного шифрования
г) Процесс смешанного шифрования

10. Что такое отечественные алгоритмы Магма и Кузнечик?
а) Симметричные алгоритмы шифрования, разработанные в России
б) Асимметричные алгоритмы шифрования, разработанные в России
в) Хэш-функции, разработанные в России
г) Алгоритмы цифровой подписи, разработанные в России

11. Что такое компьютеризация шифрования?
а) Процесс применения компьютеров для шифрования данных
б) Процесс разработки компьютерных программ для шифрования
в) Процесс разработки компьютерных алгоритмов шифрования
г) Процесс применения компьютерных средств для анализа шифров

12. Что такое цифровая подпись?
а) Процесс расшифрования данных с использованием закрытого ключа
б) Процесс шифрования данных с использованием открытого ключа
в) Алгоритм, используемый для генерации псевдослучайных чисел
г) Математическая конструкция, позволяющая установить авторство и целостность сообщения

13. Какие основные свойства должны обладать хорошая хэш-функция?
а) Односторонняя функция, стойкость к коллизиям, равномерное распределение значений
б) Обратимость, стойкость к коллизиям, высокая скорость вычислений
в) Стойкость к коллизиям, равномерное распределение значений, высокая скорость вычислений
г) Обратимость, стойкость к коллизиям, равномерное распределение значений

14. Что такое симметричные криптографические системы?
а) Системы, использующие один и тот же ключ для шифрования и расшифрования данных
б) Системы, использующие разные ключи для шифрования и расшифрования данных
в) Системы, использующие открытый ключ для шифрования и закрытый ключ для расшифрования

данных
г) Системы, использующие хэш-функции для шифрования данных

15. Какие методы используются для получения псевдослучайных последовательностей?
а) Линейный конгруэнтный генератор, метод Фибоначчи, метод Блума
б) Линейно-сдвиговый регистр, метод RSA, метод Монте-Карло
в) Линейный конгруэнтный генератор, метод Фибоначчи, метод BBS
г) Метод DES, метод AES, метод ГОСТ 28147-89

16. Что такое аппаратное шифрование?
а) Шифрование, выполняемое программными средствами
б) Шифрование, выполняемое специализированными устройствами
в) Шифрование, выполняемое с помощью аппаратных ключей
г) Шифрование, выполняемое на аппаратных уровнях компьютера

17. Что такое стандартизация программно-аппаратных криптографических систем и средств?
а) Процесс разработки и утверждения стандартов для криптографических систем и средств
б) Процесс тестирования и сертификации криптографических систем и средств
в) Процесс патентования и лицензирования криптографических систем и средств
г) Процесс разработки и маркировки криптографических систем и средств

18. Что такое DES?
а) Симметричный алгоритм шифрования с блочным размером 64 бита
б) Асимметричный алгоритм шифрования с блочным размером 64 бита
в) Хэш-функция с блочным размером 64 бита
г) Алгоритм цифровой подписи с блочным размером 64 бита

19. Что представляет собой таблица ASCII?
а) Таблица символов и их двоичных представлений
б) Таблица символов и их шестнадцатеричных представлений
в) Таблица символов и их десятичных представлений
г) Таблица символов и их восьмеричных представлений

20. Какие ключевые размеры поддерживает AES?
а) 64 бит, 256 бит, 512 бит
б) 64 бит, 128 бит, 256 бит
в) 128 бит, 256 бит, 512 бит
г) 128 бит, 192 бит, 256 бит

Вариант №4

1. Что такое хэш-функция?
а) Математическая функция, преобразующая входные данные в случайную последовательность битов
б) Математическая функция, преобразующая входные данные в строку переменной длины
в) Математическая функция, преобразующая входные данные в фиксированную строку фиксированной длины
г) Математическая функция, используемая для шифрования данных

2. Что такое атака на основе словаря (dictionary attack)?

а) Атака, при которой злоумышленник пытается получить доступ к системе, подбирая разные словарные слова
б) Атака, при которой злоумышленник перебирает все возможные комбинации паролей из заданного словаря
в) Атака, при которой злоумышленник обменивается словарями с другими злодеями
г) Атака, при которой не используются общеупотребительные слова или фразы из словарей для компрометации учетных данных пользователя

3. Что такое асимметричные криптографические системы?
а) Системы, использующие один и тот же ключ для шифрования и расшифрования данных
б) Системы, использующие разные ключи для шифрования и расшифрования данных
в) Системы, использующие открытый ключ для шифрования и закрытый ключ для расшифрования данных
г) Системы, использующие хэш-функции для шифрования данных

4. Какие методы кодирования информации вы знаете?
а) Символьное кодирование, смысловое кодирование, бинарное кодирование
б) Хаффмановское кодирование, кодирование Хемминга, кодирование CRC
в) Бинарное кодирование, кодирование Грея, кодирование Рида-Соломона
г) Бинарное кодирование, кодирование Грея, кодирование Фибоначчи

5. Что такое генераторы ПСЧ?
а) Устройства для генерации случайных чисел
б) Устройства для генерации псевдослучайных чисел
в) Устройства для генерации паролей
г) Устройства для генерации хэш-кодов

6. Что такое алгоритм RSA?
а) Асимметричный алгоритм шифрования и подписи
б) Симметричный алгоритм шифрования
в) Хэш-функция
г) Алгоритм генерации случайных чисел

7. Что такое поточное шифрование?
а) Шифрование, использующее потоки данных
б) Шифрование, использующее блоки данных
в) Шифрование, использующее хэш-функции
г) Шифрование, использующее симметричные ключи

8. Что такое программное шифрование?
а) Шифрование, выполняемое с использованием программных средств
б) Шифрование, выполняемое на уровне операционной системы
в) Шифрование, выполняемое на уровне ядра компьютера
г) Шифрование, выполняемое на уровне аппаратных устройств

9. Что такое механизация шифрования?
а) Процесс автоматизации шифрования
б) Процесс механического шифрования
в) Процесс программного шифрования
г) Процесс смешанного шифрования

10. Что представляет собой таблица ASCII?
а) Таблица символов и их двоичных представлений

б) Таблица символов и их шестнадцатеричных представлений
в) Таблица символов и их десятичных представлений
г) Таблица символов и их восьмеричных представлений

11. Что такое компьютеризация шифрования?
а) Процесс применения компьютеров для шифрования данных
б) Процесс разработки компьютерных программ для шифрования
в) Процесс разработки компьютерных алгоритмов шифрования
г) Процесс применения компьютерных средств для анализа шифров

12. Что такое цифровая подпись?
а) Процесс расшифрования данных с использованием закрытого ключа
б) Процесс шифрования данных с использованием открытого ключа
в) Алгоритм, используемый для генерации псевдослучайных чисел
г) Математическая конструкция, позволяющая установить авторство и целостность сообщения

13. Что такое симметричные криптографические системы?
а) Системы, использующие один и тот же ключ для шифрования и расшифрования данных
б) Системы, использующие разные ключи для шифрования и расшифрования данных
в) Системы, использующие открытый ключ для шифрования и закрытый ключ для расшифрования данных
г) Системы, использующие хэш-функции для шифрования данных

14. Какие методы используются для получения псевдослучайных последовательностей?
а) Линейный конгруэнтный генератор, метод Фибоначчи, метод Блума
б) Линейно-сдвиговый регистр, метод RSA, метод Монте-Карло
в) Линейный конгруэнтный генератор, метод Фибоначчи, метод BBS
г) Метод DES, метод AES, метод ГОСТ 28147-89

15. Что такое отечественные алгоритмы Магма и Кузнечик?
а) Симметричные алгоритмы шифрования, разработанные в России
б) Асимметричные алгоритмы шифрования, разработанные в России
в) Хэш-функции, разработанные в России
г) Алгоритмы цифровой подписи, разработанные в России

16. Что такое DES?
а) Симметричный алгоритм шифрования с блочным размером 64 бита
б) Асимметричный алгоритм шифрования с блочным размером 64 бита
в) Хэш-функция с блочным размером 64 бита
г) Алгоритм цифровой подписи с блочным размером 64 бита

17. Что такое AES?
а) Симметричный алгоритм шифрования с блочным размером 128 бит
б) Асимметричный алгоритм шифрования с блочным размером 128 бит
в) Хэш-функция с блочным размером 128 бит
г) Алгоритм цифровой подписи с блочным размером 128 бит

18. Какие ключевые размеры поддерживает AES?
а) 64 бит, 256 бит, 512 бит
б) 64 бит, 128 бит, 256 бит
в) 128 бит, 256 бит, 512 бит
г) 128 бит, 192 бит, 256 бит

19. Что такое аппаратное шифрование?

а) Шифрование, выполняемое программными средствами
б) Шифрование, выполняемое специализированными устройствами
в) Шифрование, выполняемое с помощью аппаратных ключей
г) Шифрование, выполняемое на аппаратных уровнях компьютера

20. Что такое стандартизация программно-аппаратных криптографических систем и средств?

а) Процесс разработки и утверждения стандартов для криптографических систем и средств
б) Процесс тестирования и сертификации криптографических систем и средств
в) Процесс патентования и лицензирования криптографических систем и средств
г) Процесс разработки и маркировки криптографических систем и средств

Критерии оценивания рубежной аттестации:

Количество вопросов	**Оценка**	
16-20	**5**	**аттестован**
11-15	**4**	
6-10	**3**	
0-5	**2**	**не аттестован**

Аттестован - выставляется обучающемуся, ответившему правильно на 6-20 вопросов.
Не аттестован - выставляется обучающемуся, который ответил на 5 и менее вопроса.
Отлично - выставляется обучающемуся, ответившему на 16-20 вопросов.
Хорошо - выставляется обучающемуся, ответившему на 11-15 вопросов.
Удовлетворительно - выставляется обучающемуся, ответившему на 6-10 вопросов.

Ключи к тесту

№ п/п	**Вариант № 1**	**Вариант № 2**	**Вариант №3**	**Вариант №4**
1	г	а	б	в
2	а	в	а	б
3	а	б	а	в
4	в	а	б	б
5	б	в	б	б
6	а	в	в	а
7	б	а	а	а
8	а	г	в	а
9	б	б	б	б
10	а	б	а	а
11	а	а	а	а
12	а	а	г	г
13	а	б	а	а
14	а	б	а	в
15	б	а	в	а
16	а	а	б	а
17	а	а	а	а
18	г	а	а	г
19	в	а	а	б
20	в	в	г	а

Вопросы ко 2-ой рубежной аттестации

1. Какие криптосистемы используются с открытым ключом?
2. Что такое необратимость систем в криптографии?
3. Что такое структурная схема шифрования с открытым ключом?
4. Какие элементы теории чисел используются в криптографии с открытым ключом?
5. Что такое аутентификация данных в криптографии?
6. Какие понятия связаны с аутентификацией данных?
7. Что такое однонаправленные хеш-функции?
8. Какие алгоритмы используются для цифровой подписи?
9. Что такое абонентское шифрование?
10. Что такое пакетное шифрование?
11. Что нужно защищать в центре генерации ключей при абонентском шифровании?
12. Что такое криптомаршрутизатор?
13. Что такое пакетный фильтр?
14. Какая криптографическая защита используется в беспроводных сетях стандарта 802.11?
15. Что означает сокращение WPA?
16. Что означает сокращение WEP?
17. Какие протоколы используются для криптографической защиты беспроводных соединений?
18. Какая основная проблема с протоколом WEP?
19. Какой алгоритм используется для шифрования в протоколе WPA2?
20. Какая основная проблема с протоколом WPA?
21. Какой алгоритм используется для шифрования в протоколе WPA3?
22. Какие преимущества имеет протокол WPA3 по сравнению с WPA2?
23. Какие уязвимости имеет протокол WEP?
24. Какой протокол обеспечивает криптографическую защиту беспроводных соединений в сетях стандарта 802.11?
25. Какие методы шифрования используются для обеспечения защиты данных в сетевых коммуникациях?

Образец билета ко 2-ой рубежной аттестации

Федеральное государственное бюджетное образовательное учреждение высшегообразования
Грозненский государственный нефтяной технический университет
им. акад. М.Д.Миллионщикова
Факультет среднего профессионального образования
Тестовое задание
по модулю МДК.02.02 «Криптографические средства защиты информации»
II-аттестация
Вариант №___

ФИО_____групп_____Дата

№ вопроса	1	2	3	4	5	6	7	8	9	10
Ответ										
№ вопроса	11	12	13	14	15	16	17	18	19	20
Ответ										

Вариант №1

1. Какие понятия связаны с аутентификацией данных?
а) ЭП (электронная подпись)
б) MAC (код аутентификации сообщений)
в) Однонаправленные хеш-функции
г) Все варианты ответов верны

2. Что такое необратимость систем в криптографии?
а) Возможность восстановления исходных данных из зашифрованных
б) Невозможность восстановления исходных данных из зашифрованных
в) Возможность восстановления ключа шифрования из шифротекста
г) Невозможность восстановления ключа шифрования из шифротекста

3. Какая криптографическая защита используется в беспроводных сетях стандарта 802.11?
а) WPA
б) WEP
в) SSL
г) IPSec

4. Что такое криптомаршрутизатор?
а) Устройство, обеспечивающее шифрование данных при маршрутизации
б) Устройство, обеспечивающее аутентификацию данных при маршрутизации
в) Устройство, обеспечивающее обнаружение вторжений при маршрутизации
г) Устройство, обеспечивающее анонимность при маршрутизации

5. Какие протоколы используются для криптографической защиты беспроводных соединений?
а) WPA2
б) WEP
в) WPA3
г) Все варианты ответов верны

6. Что такое структурная схема шифрования с открытым ключом?

а) Процесс шифрования и расшифрования данных с использованием одного ключа
б) Процесс шифрования и расшифрования данных с использованием двух разных ключей
в) Процесс шифрования и расшифрования данных без использования ключей
г) Процесс шифрования и расшифрования данных с использованием общего секретного ключа

7. Какие алгоритмы используются для цифровой подписи?

а) RSA
б) AES
в) DES
г) SHA-256

8. Что такое пакетный фильтр?

а) Устройство, контролирующее передачу пакетов данных
б) Устройство, шифрующее пакеты данных перед передачей
в) Устройство, выполняющее аутентификацию пакетов данных
г) Устройство, отслеживающее пакеты данных в сети

9. Какие преимущества имеет протокол WPA3 по сравнению с WPA2?

а) Более высокая производительность
б) Улучшенная защита от взлома
в) Расширенная поддержка устройств
г) Все варианты ответов верны

10. Какие методы шифрования используются для обеспечения защиты данных в сетевых коммуникациях?

а) Абонентское шифрование и пакетное шифрование
б) Симметричное шифрование и асимметричное шифрование
в) все варианты верны
г) все варианты неверны

11. Что такое однонаправленные хеш-функции?

а) Функции, которые могут быть использованы только для шифрования данных
б) Функции, которые могут быть использованы только для расшифрования данных
в) Функции, которые могут быть использованы только для аутентификации данных
г) Функции, которые могут быть использованы только для генерации случайных чисел

12. Что такое аутентификация данных в криптографии?

а) Процесс передачи данных по зашифрованному каналу связи
б) Процесс проверки подлинности и целостности данных
в) Процесс шифрования данных перед передачей
г) Процесс дешифрования данных после передачи

13. Какие уязвимости имеет протокол WEP?

а) Легко поддаётся взлому с помощью атак перебора ключа
б) Ограниченная поддержка устройств
в) Низкая производительность
г) Высокая стоимость реализации

14. Что такое абонентское шифрование?

а) Шифрование данных перед передачей их по сети

б) Шифрование данных, используя открытый ключ получателя
в) Шифрование данных, используя общий секретный ключ
г) Шифрование данных, используя публичный ключ отправителя

15. Что такое пакетное шифрование?
а) Шифрование данных в пакете, перед отправкой по сети
б) Шифрование данных в режиме потока передачи
в) Шифрование данных в режиме блочной передачи
г) Шифрование данных в пакете, после отправки по сети

16. Какие криптосистемы используются с открытым ключом?
а) DES
б) RSA
в) AES
г) Blowfish

17. Какие элементы теории чисел используются в криптографии с открытым ключом?
а) Простые числа
б) Рациональные числа
в) Комплексные числа
г) Натуральные числа

18. Что нужно защищать в центре генерации ключей при абонентском шифровании?
а) Отправленные данные
б) Приватные ключи
в) Публичные ключи
г) Аутентификационные данные

19. Какая основная проблема с протоколом WEP?
а) Низкая производительность
б) Легко подвержен взлому
в) Ограниченная поддержка устройств
г) Высокая стоимость реализации

20. Какой протокол обеспечивает криптографическую защиту беспроводных соединений в сетях стандарта 802.11?
а) WPA
б) WEP
в) SSL
г) IPSec

Вариант №2

1. Что такое аутентификация данных в криптографии?
а) Процесс передачи данных по зашифрованному каналу связи
б) Процесс проверки подлинности и целостности данных
в) Процесс шифрования данных перед передачей
г) Процесс дешифрования данных после передачи

2. Какие понятия связаны с аутентификацией данных?
а) ЭП (электронная подпись)

б) MAC (код аутентификации сообщений)
в) Однонаправленные хеш-функции
г) Все варианты ответов верны

3. Какая криптографическая защита используется в беспроводных сетях стандарта 802.11?
а) WPA
б) WEP
в) SSL
г) IPSec

4. Какие протоколы используются для криптографической защиты беспроводных соединений?
а) WPA2
б) WEP
в) WPA3
г) Все варианты ответов верны

5. Что такое структурная схема шифрования с открытым ключом?
а) Процесс шифрования и расшифрования данных с использованием одного ключа
б) Процесс шифрования и расшифрования данных с использованием двух разных ключей
в) Процесс шифрования и расшифрования данных без использования ключей
г) Процесс шифрования и расшифрования данных с использованием общего секретного ключа

6. Какие алгоритмы используются для цифровой подписи?
а) RSA
б) AES
в) DES
г) SHA-256

7. Что такое пакетный фильтр?
а) Устройство, контролирующее передачу пакетов данных
б) Устройство, шифрующее пакеты данных перед передачей
в) Устройство, выполняющее аутентификацию пакетов данных
г) Устройство, отслеживающее пакеты данных в сети

8. Какие преимущества имеет протокол WPA3 по сравнению с WPA2?
а) Более высокая производительность
б) Улучшенная защита от взлома
в) Расширенная поддержка устройств
г) Все варианты ответов верны

9. Какие методы шифрования используются для обеспечения защиты данных в сетевых коммуникациях?
а) Абонентское шифрование и пакетное шифрование
б) Симметричное шифрование и асимметричное шифрование
в) все варианты верны
г) все варианты неверны

10. Что такое необратимость систем в криптографии?
а) Возможность восстановления исходных данных из зашифрованных
б) Невозможность восстановления исходных данных из зашифрованных
в) Возможность восстановления ключа шифрования из шифротекста
г) Невозможность восстановления ключа шифрования из шифротекста

11. Что такое однонаправленные хеш-функции?
а) Функции, которые могут быть использованы только для шифрования данных
б) Функции, которые могут быть использованы только для расшифрования данных
в) Функции, которые могут быть использованы только для аутентификации данных
г) Функции, которые могут быть использованы только для генерации случайных чисел

12. Какие уязвимости имеет протокол WEP?
а) Легко поддаётся взлому с помощью атак перебора ключа
б) Ограниченная поддержка устройств
в) Низкая производительность
г) Высокая стоимость реализации

13. Что такое абонентское шифрование?
а) Шифрование данных перед передачей их по сети
б) Шифрование данных, используя открытый ключ получателя
в) Шифрование данных, используя общий секретный ключ
г) Шифрование данных, используя публичный ключ отправителя

14. Что такое пакетное шифрование?
а) Шифрование данных в пакете, перед отправкой по сети
б) Шифрование данных в режиме потока передачи
в) Шифрование данных в режиме блочной передачи
г) Шифрование данных в пакете, после отправки по сети

15. Какие криптосистемы используются с открытым ключом?
а) DES
б) RSA
в) AES
г) Blowfish

16. Какие элементы теории чисел используются в криптографии с открытым ключом?
а) Простые числа
б) Рациональные числа
в) Комплексные числа
г) Натуральные числа

17. Что нужно защищать в центре генерации ключей при абонентском шифровании?
а) Отправленные данные
б) Приватные ключи
в) Публичные ключи
г) Аутентификационные данные

18. Какая основная проблема с протоколом WEP?
а) Низкая производительность
б) Легко подвержен взлому
в) Ограниченная поддержка устройств
г) Высокая стоимость реализации

19. Какой протокол обеспечивает криптографическую защиту беспроводных соединений в сетях стандарта 802.11?
а) WPA
б) WEP

в) SSL
г) IPSec

20. Какой алгоритм используется для шифрования в протоколе WPA2?
а) AES
б) DES
в) RSA
г) Blowfish

Вариант №3

1. Что такое аутентификация данных в криптографии?
а) Процесс передачи данных по зашифрованному каналу связи
б) Процесс проверки подлинности и целостности данных
в) Процесс шифрования данных перед передачей
г) Процесс дешифрования данных после передачи

2. Какие понятия связаны с аутентификацией данных?
а) ЭП (электронная подпись)
б) MAC (код аутентификации сообщений)
в) Однонаправленные хеш-функции
г) Все варианты ответов верны

3. Что такое пакетное шифрование?
а) Шифрование данных в пакете, перед отправкой по сети
б) Шифрование данных в режиме потока передачи
в) Шифрование данных в режиме блочной передачи
г) Шифрование данных в пакете, после отправки по сети

4. Что такое криптомаршрутизатор?
а) Устройство, обеспечивающее шифрование данных при маршрутизации
б) Устройство, обеспечивающее аутентификацию данных при маршрутизации
в) Устройство, обеспечивающее обнаружение вторжений при маршрутизации
г) Устройство, обеспечивающее анонимность при маршрутизации

5. Какие протоколы используются для криптографической защиты беспроводных соединений?
а) WPA2
б) WEP
в) WPA3
г) Все варианты ответов верны

6. Что такое структурная схема шифрования с открытым ключом?
а) Процесс шифрования и расшифрования данных с использованием одного ключа
б) Процесс шифрования и расшифрования данных с использованием двух разных ключей
в) Процесс шифрования и расшифрования данных без использования ключей
г) Процесс шифрования и расшифрования данных с использованием общего секретного ключа

7. Какие алгоритмы используются для цифровой подписи?
а) RSA
б) AES

в) DES
г) SHA-256

8. Что такое пакетный фильтр?
а) Устройство, контролирующее передачу пакетов данных
б) Устройство, шифрующее пакеты данных перед передачей
в) Устройство, выполняющее аутентификацию пакетов данных
г) Устройство, отслеживающее пакеты данных в сети

9. Какие преимущества имеет протокол WPA3 по сравнению с WPA2?
а) Более высокая производительность
б) Улучшенная защита от взлома
в) Расширенная поддержка устройств
г) Все варианты ответов верны

10. Какие методы шифрования используются для обеспечения защиты данных в сетевых коммуникациях?
а) Абонентское шифрование и пакетное шифрование
б) Симметричное шифрование и асимметричное шифрование
в) все варианты верны
г) все варианты неверны

11. Что такое необратимость систем в криптографии?
а) Возможность восстановления исходных данных из зашифрованных
б) Невозможность восстановления исходных данных из зашифрованных
в) Возможность восстановления ключа шифрования из шифротекста
г) Невозможность восстановления ключа шифрования из шифротекста

12. Что такое однонаправленные хеш-функции?
а) Функции, которые могут быть использованы только для шифрования данных
б) Функции, которые могут быть использованы только для расшифрования данных
в) Функции, которые могут быть использованы только для аутентификации данных
г) Функции, которые могут быть использованы только для генерации случайных чисел

13. Какие уязвимости имеет протокол WEP?
а) Легко поддаётся взлому с помощью атак перебора ключа
б) Ограниченная поддержка устройств
в) Низкая производительность
г) Высокая стоимость реализации

14. Что такое абонентское шифрование?
а) Шифрование данных перед передачей их по сети
б) Шифрование данных, используя открытый ключ получателя
в) Шифрование данных, используя общий секретный ключ
г) Шифрование данных, используя публичный ключ отправителя

15. Какие криптосистемы используются с открытым ключом?
а) DES
б) RSA
в) AES
г) Blowfish

16. Какие элементы теории чисел используются в криптографии с открытым ключом?

а) Простые числа
б) Рациональные числа
в) Комплексные числа
г) Натуральные числа

17. Что нужно защищать в центре генерации ключей при абонентском шифровании?
а) Отправленные данные
б) Приватные ключи
в) Публичные ключи
г) Аутентификационные данные

18. Какая основная проблема с протоколом WEP?
а) Низкая производительность
б) Легко подвержен взлому
в) Ограниченная поддержка устройств
г) Высокая стоимость реализации

19. Какой протокол обеспечивает криптографическую защиту беспроводных соединений в сетях стандарта 802.11?
а) WPA
б) WEP
в) SSL
г) IPSec

20. Какие методы шифрования используются для обеспечения конфиденциальности данных в беспроводных сетях?
а) Абонентское шифрование и пакетное шифрование
б) Симметричное шифрование и асимметричное шифрование
в) все варианты верны
г) все варианты неверны

Вариант №4

1. Какие криптосистемы используются с открытым ключом?
а) DES
б) RSA
в) AES
г) Blowfish

2. Что такое аутентификация данных в криптографии?
а) Процесс передачи данных по зашифрованному каналу связи
б) Процесс проверки подлинности и целостности данных
в) Процесс шифрования данных перед передачей
г) Процесс дешифрования данных после передачи

3. Какие понятия связаны с аутентификацией данных?
а) ЭП (электронная подпись)
б) MAC (код аутентификации сообщений)
в) Однонаправленные хеш-функции
г) Все варианты ответов верны

4. Что такое структурная схема шифрования с открытым ключом?
а) Процесс шифрования и расшифрования данных с использованием одного ключа
б) Процесс шифрования и расшифрования данных с использованием двух разных ключей
в) Процесс шифрования и расшифрования данных без использования ключей
г) Процесс шифрования и расшифрования данных с использованием общего секретного ключа

5. Какие элементы теории чисел используются в криптографии с открытым ключом?
а) Простые числа
б) Рациональные числа
в) Комплексные числа
г) Натуральные числа

6. Что такое необратимость систем в криптографии?
а) Возможность восстановления исходных данных из зашифрованных
б) Невозможность восстановления исходных данных из зашифрованных
в) Возможность восстановления ключа шифрования из шифротекста
г) Невозможность восстановления ключа шифрования из шифротекста

7. Что такое однонаправленные хеш-функции?
а) Функции, которые могут быть использованы только для шифрования данных
б) Функции, которые могут быть использованы только для расшифрования данных
в) Функции, которые могут быть использованы только для аутентификации данных
г) Функции, которые могут быть использованы только для генерации случайных чисел

8. Какие алгоритмы используются для цифровой подписи?
а) RSA
б) AES
в) DES
г) SHA-256

9. Что такое абонентское шифрование?
а) Шифрование данных перед передачей их по сети
б) Шифрование данных, используя открытый ключ получателя
в) Шифрование данных, используя общий секретный ключ
г) Шифрование данных, используя публичный ключ отправителя

10. Что такое пакетное шифрование?
а) Шифрование данных в пакете, перед отправкой по сети
б) Шифрование данных в режиме потока передачи
в) Шифрование данных в режиме блочной передачи
г) Шифрование данных в пакете, после отправки по сети

11. Что нужно защищать в центре генерации ключей при абонентском шифровании?
а) Отправленные данные
б) Приватные ключи
в) Публичные ключи
г) Аутентификационные данные

12. Что такое криптомаршрутизатор?
а) Устройство, обеспечивающее шифрование данных при маршрутизации
б) Устройство, обеспечивающее аутентификацию данных при маршрутизации
в) Устройство, обеспечивающее обнаружение вторжений при маршрутизации
г) Устройство, обеспечивающее анонимность при маршрутизации

13. Что такое пакетный фильтр?
а) Устройство, контролирующее передачу пакетов данных
б) Устройство, шифрующее пакеты данных перед передачей
в) Устройство, выполняющее аутентификацию пакетов данных
г) Устройство, отслеживающее пакеты данных в сети

14. Какая криптографическая защита используется в беспроводных сетях стандарта 802.11?
а) WPA
б) WEP
в) SSL
г) IPSec

15. Что означает сокращение WPA?
а) Wireless Privacy Access
б) Wi-Fi Protected Access
в) Wireless Protected Access
г) Wi-Fi Privacy Access

16. Что означает сокращение WEP?
а) Wireless Encryption Protocol
б) Wi-Fi Encryption Protocol
в) Wireless Enhanced Protection
г) Wi-Fi Enhanced Privacy

17. Какие протоколы используются для криптографической защиты беспроводных соединений?
а) WPA2
б) WEP
в) WPA3
г) Все варианты ответов верны

18. Какая основная проблема с протоколом WEP?
а) Низкая производительность
б) Легко подвержен взлому
в) Ограниченная поддержка устройств
г) Высокая стоимость реализации

19. Какой алгоритм используется для шифрования в протоколе WPA2?
а) AES
б) DES
в) RSA
г) Blowfish

20. Какие методы шифрования используются для обеспечения защиты данных в сетевых коммуникациях?
а) Абонентское шифрование и пакетное шифрование
б) Симметричное шифрование и асимметричное шифрование
в) все варианты верны
г) все варианты неверны

Критерии оценивания рубежной аттестации:

Количество вопросов	Оценка	
16-20	**5**	**аттестован**
11-15	**4**	
6-10	**3**	
0-5	**2**	**не аттестован**

Аттестован - выставляется обучающемуся, ответившему правильно на 6-20 вопросов.
Не аттестован - выставляется обучающемуся, который ответил на 5 и менее вопроса.
Отлично - выставляется обучающемуся, ответившему на 16-20 вопросов.
Хорошо - выставляется обучающемуся, ответившему на 11-15 вопросов.
Удовлетворительно - выставляется обучающемуся, ответившему на 6-10 вопросов.

Ключи к тесту

№ п/п	Вариант № 1	Вариант № 2	Вариант №3	Вариант №4
1	г	б	б	б
2	б	г	г	б
3	а	а	а	г
4	а	г	а	б
5	г	б	г	а
6	б	а	б	б
7	а	а	а	в
8	а	г	а	а
9	г	в	г	б
10	в	б	в	а
11	в	в	б	б
12	б	а	в	а
13	а	б	а	а
14	б	а	б	а
15	а	б	б	б
16	б	а	а	а
17	а	б	б	г
18	б	б	б	б
19	б	а	а	а
20	а	а	в	в

Образец билета к экзамену

Федеральное государственное бюджетное образовательное учреждение высшегообразования
Грозненский государственный нефтяной технический университет
им. акад. М.Д.Миллионщикова
Факультет среднего профессионального образования
Тестовое задание
по модулю МДК.02.02 «Криптографические средства защиты информации»
Экзамен
Вариант №___

ФИО_____групп_____Дата

№ вопроса	1	2	3	4	5	6	7	8	9	10
Ответ										
№ вопроса	11	12	13	14	15	16	17	18	19	20
Ответ										
№ вопроса	21	22	23	24	25	26	27	28	29	30
Ответ										
№ вопроса	31	32	33	34	35	36	37	38	39	40
Ответ										

Вариант №1

1. Что такое генераторы ПСЧ?
а) Устройства для генерации случайных чисел
б) Устройства для генерации псевдослучайных чисел
в) Устройства для генерации паролей
г) Устройства для генерации хэш-кодов

2. Что такое алгоритм RSA?
а) Асимметричный алгоритм шифрования и подписи
б) Симметричный алгоритм шифрования
в) Хэш-функция
г) Алгоритм генерации случайных чисел

3. Что такое поточное шифрование?
а) Шифрование, использующее потоки данных
б) Шифрование, использующее блоки данных
в) Шифрование, использующее хэш-функции
г) Шифрование, использующее симметричные ключи

4. Что такое атака на основе словаря (dictionary attack)?
а) Атака, при которой злоумышленник пытается получить доступ к системе, подбирая разные словарные слова
б) Атака, при которой злоумышленник перебирает все возможные комбинации паролей из заданного словаря

в) Атака, при которой злоумышленник обменивается словарями с другими злодеями
г) Атака, при которой не используются общеупотребительные слова или фразы из словарей для компрометации учетных данных пользователя

5. Какие методы кодирования информации вы знаете?
а) Символьное кодирование, смысловое кодирование, бинарное кодирование
б) Хаффмановское кодирование, кодирование Хемминга, кодирование CRC
в) Бинарное кодирование, кодирование Грея, кодирование Рида-Соломона
г) Бинарное кодирование, кодирование Грея, кодирование Фибоначчи

6. Что такое асимметричные криптографические системы?
а) Системы, использующие один и тот же ключ для шифрования и расшифрования данных
б) Системы, использующие разные ключи для шифрования и расшифрования данных
в) Системы, использующие открытый ключ для шифрования и закрытый ключ для расшифрования данных
г) Системы, использующие хэш-функции для шифрования данных

7. Что такое программное шифрование?
а) Шифрование, выполняемое с использованием программных средств
б) Шифрование, выполняемое на уровне операционной системы
в) Шифрование, выполняемое на уровне ядра компьютера
г) Шифрование, выполняемое на уровне аппаратных устройств

8. Что такое хэш-функция?
а) Математическая функция, преобразующая входные данные в случайную последовательность битов
б) Математическая функция, преобразующая входные данные в строку переменной длины
в) Математическая функция, преобразующая входные данные в фиксированную строку фиксированной длины
г) Математическая функция, используемая для шифрования данных

9. Что такое механизация шифрования?
а) Процесс автоматизации шифрования
б) Процесс механического шифрования
в) Процесс программного шифрования
г) Процесс смешанного шифрования

10. Что такое отечественные алгоритмы Магма и Кузнечик?
а) Симметричные алгоритмы шифрования, разработанные в России
б) Асимметричные алгоритмы шифрования, разработанные в России
в) Хэш-функции, разработанные в России
г) Алгоритмы цифровой подписи, разработанные в России

11. Что такое компьютеризация шифрования?
а) Процесс применения компьютеров для шифрования данных
б) Процесс разработки компьютерных программ для шифрования
в) Процесс разработки компьютерных алгоритмов шифрования
г) Процесс применения компьютерных средств для анализа шифров

12. Что такое цифровая подпись?
а) Процесс расшифрования данных с использованием закрытого ключа
б) Процесс шифрования данных с использованием открытого ключа
в) Алгоритм, используемый для генерации псевдослучайных чисел

г) Математическая конструкция, позволяющая установить авторство и целостность сообщения

13. Какие основные свойства должны обладать хорошая хэш-функция?
а) Односторонняя функция, стойкость к коллизиям, равномерное распределение значений
б) Обратимость, стойкость к коллизиям, высокая скорость вычислений
в) Стойкость к коллизиям, равномерное распределение значений, высокая скорость вычислений
г) Обратимость, стойкость к коллизиям, равномерное распределение значений

14. Что такое симметричные криптографические системы?
а) Системы, использующие один и тот же ключ для шифрования и расшифрования данных
б) Системы, использующие разные ключи для шифрования и расшифрования данных
в) Системы, использующие открытый ключ для шифрования и закрытый ключ для расшифрования данных
г) Системы, использующие хэш-функции для шифрования данных

15. Какие методы используются для получения псевдослучайных последовательностей?
а) Линейный конгруэнтный генератор, метод Фибоначчи, метод Блума
б) Линейно-сдвиговый регистр, метод RSA, метод Монте-Карло
в) Линейный конгруэнтный генератор, метод Фибоначчи, метод BBS
г) Метод DES, метод AES, метод ГОСТ 28147-89

16. Что такое аппаратное шифрование?
а) Шифрование, выполняемое программными средствами
б) Шифрование, выполняемое специализированными устройствами
в) Шифрование, выполняемое с помощью аппаратных ключей
г) Шифрование, выполняемое на аппаратных уровнях компьютера

17. Что такое стандартизация программно-аппаратных криптографических систем и средств?
а) Процесс разработки и утверждения стандартов для криптографических систем и средств
б) Процесс тестирования и сертификации криптографических систем и средств
в) Процесс патентования и лицензирования криптографических систем и средств
г) Процесс разработки и маркировки криптографических систем и средств

18. Что такое DES?
а) Симметричный алгоритм шифрования с блочным размером 64 бита
б) Асимметричный алгоритм шифрования с блочным размером 64 бита
в) Хэш-функция с блочным размером 64 бита
г) Алгоритм цифровой подписи с блочным размером 64 бита

19. Что представляет собой таблица ASCII?
а) Таблица символов и их двоичных представлений
б) Таблица символов и их шестнадцатеричных представлений
в) Таблица символов и их десятичных представлений
г) Таблица символов и их восьмеричных представлений

20. Какие ключевые размеры поддерживает AES?
а) 64 бит, 256 бит, 512 бит
б) 64 бит, 128 бит, 256 бит
в) 128 бит, 256 бит, 512 бит
г) 128 бит, 192 бит, 256 бит

21. Что такое аутентификация данных в криптографии?

а) Процесс передачи данных по зашифрованному каналу связи
б) Процесс проверки подлинности и целостности данных
в) Процесс шифрования данных перед передачей
г) Процесс дешифрования данных после передачи

22. Какие понятия связаны с аутентификацией данных?
а) ЭП (электронная подпись)
б) MAC (код аутентификации сообщений)
в) Однонаправленные хеш-функции
г) Все варианты ответов верны

23. Какая криптографическая защита используется в беспроводных сетях стандарта 802.11?
а) WPA
б) WEP
в) SSL
г) IPSec

24. Какие протоколы используются для криптографической защиты беспроводных соединений?
а) WPA2
б) WEP
в) WPA3
г) Все варианты ответов верны

25. Что такое структурная схема шифрования с открытым ключом?
а) Процесс шифрования и расшифрования данных с использованием одного ключа
б) Процесс шифрования и расшифрования данных с использованием двух разных ключей
в) Процесс шифрования и расшифрования данных без использования ключей
г) Процесс шифрования и расшифрования данных с использованием общего секретного ключа

26. Какие алгоритмы используются для цифровой подписи?
а) RSA
б) AES
в) DES
г) SHA-256

27. Что такое пакетный фильтр?
а) Устройство, контролирующее передачу пакетов данных
б) Устройство, шифрующее пакеты данных перед передачей
в) Устройство, выполняющее аутентификацию пакетов данных
г) Устройство, отслеживающее пакеты данных в сети

28. Какие преимущества имеет протокол WPA3 по сравнению с WPA2?
а) Более высокая производительность
б) Улучшенная защита от взлома
в) Расширенная поддержка устройств
г) Все варианты ответов верны

29. Какие методы шифрования используются для обеспечения защиты данных в сетевых коммуникациях?
а) Абонентское шифрование и пакетное шифрование
б) Симметричное шифрование и асимметричное шифрование
в) все варианты верны

г) все варианты неверны

30. Что такое необратимость систем в криптографии?
а) Возможность восстановления исходных данных из зашифрованных
б) Невозможность восстановления исходных данных из зашифрованных
в) Возможность восстановления ключа шифрования из шифротекста
г) Невозможность восстановления ключа шифрования из шифротекста

31. Что такое однонаправленные хеш-функции?
а) Функции, которые могут быть использованы только для шифрования данных
б) Функции, которые могут быть использованы только для расшифрования данных
в) Функции, которые могут быть использованы только для аутентификации данных
г) Функции, которые могут быть использованы только для генерации случайных чисел

32. Какие уязвимости имеет протокол WEP?
а) Легко поддаётся взлому с помощью атак перебора ключа
б) Ограниченная поддержка устройств
в) Низкая производительность
г) Высокая стоимость реализации

33. Что такое абонентское шифрование?
а) Шифрование данных перед передачей их по сети
б) Шифрование данных, используя открытый ключ получателя
в) Шифрование данных, используя общий секретный ключ
г) Шифрование данных, используя публичный ключ отправителя

34. Что такое пакетное шифрование?
а) Шифрование данных в пакете, перед отправкой по сети
б) Шифрование данных в режиме потока передачи
в) Шифрование данных в режиме блочной передачи
г) Шифрование данных в пакете, после отправки по сети

35. Какие криптосистемы используются с открытым ключом?
а) DES
б) RSA
в) AES
г) Blowfish

36. Какие элементы теории чисел используются в криптографии с открытым ключом?
а) Простые числа
б) Рациональные числа
в) Комплексные числа
г) Натуральные числа

37. Что нужно защищать в центре генерации ключей при абонентском шифровании?
а) Отправленные данные
б) Приватные ключи
в) Публичные ключи
г) Аутентификационные данные

38. Какая основная проблема с протоколом WEP?
а) Низкая производительность
б) Легко подвержен взлому

в) Ограниченная поддержка устройств
г) Высокая стоимость реализации

39. Какой протокол обеспечивает криптографическую защиту беспроводных соединений в сетях стандарта 802.11?
а) WPA
б) WEP
в) SSL
г) IPSec

40. Какой алгоритм используется для шифрования в протоколе WPA2?
а) AES
б) DES
в) RSA
г) Blowfish

Вариант №2

1. Что такое хэш-функция?
а) Математическая функция, преобразующая входные данные в случайную последовательность битов
б) Математическая функция, преобразующая входные данные в строку переменной длины
в) Математическая функция, преобразующая входные данные в фиксированную строку фиксированной длины
г) Математическая функция, используемая для шифрования данных

2. Что такое атака на основе словаря (dictionary attack)?
а) Атака, при которой злоумышленник пытается получить доступ к системе, подбирая разные словарные слова
б) Атака, при которой злоумышленник перебирает все возможные комбинации паролей из заданного словаря
в) Атака, при которой злоумышленник обменивается словарями с другими злодеями
г) Атака, при которой не используются общеупотребительные слова или фразы из словарей для компрометации учетных данных пользователя

3. Что такое асимметричные криптографические системы?
а) Системы, использующие один и тот же ключ для шифрования и расшифрования данных
б) Системы, использующие разные ключи для шифрования и расшифрования данных
в) Системы, использующие открытый ключ для шифрования и закрытый ключ для расшифрования данных
г) Системы, использующие хэш-функции для шифрования данных

4. Какие методы кодирования информации вы знаете?
а) Символьное кодирование, смысловое кодирование, бинарное кодирование
б) Хаффмановское кодирование, кодирование Хемминга, кодирование CRC
в) Бинарное кодирование, кодирование Грея, кодирование Рида-Соломона
г) Бинарное кодирование, кодирование Грея, кодирование Фибоначчи

5. Что такое генераторы ПСЧ?
а) Устройства для генерации случайных чисел
б) Устройства для генерации псевдослучайных чисел

в) Устройства для генерации паролей
г) Устройства для генерации хэш-кодов

6. Что такое алгоритм RSA?
а) Асимметричный алгоритм шифрования и подписи
б) Симметричный алгоритм шифрования
в) Хэш-функция
г) Алгоритм генерации случайных чисел

7. Что такое поточное шифрование?
а) Шифрование, использующее потоки данных
б) Шифрование, использующее блоки данных
в) Шифрование, использующее хэш-функции
г) Шифрование, использующее симметричные ключи

8. Что такое программное шифрование?
а) Шифрование, выполняемое с использованием программных средств
б) Шифрование, выполняемое на уровне операционной системы
в) Шифрование, выполняемое на уровне ядра компьютера
г) Шифрование, выполняемое на уровне аппаратных устройств

9. Что такое механизация шифрования?
а) Процесс автоматизации шифрования
б) Процесс механического шифрования
в) Процесс программного шифрования
г) Процесс смешанного шифрования

10. Что представляет собой таблица ASCII?
а) Таблица символов и их двоичных представлений
б) Таблица символов и их шестнадцатеричных представлений
в) Таблица символов и их десятичных представлений
г) Таблица символов и их восьмеричных представлений

11. Что такое компьютеризация шифрования?
а) Процесс применения компьютеров для шифрования данных
б) Процесс разработки компьютерных программ для шифрования
в) Процесс разработки компьютерных алгоритмов шифрования
г) Процесс применения компьютерных средств для анализа шифров

12. Что такое цифровая подпись?
а) Процесс расшифрования данных с использованием закрытого ключа
б) Процесс шифрования данных с использованием открытого ключа
в) Алгоритм, используемый для генерации псевдослучайных чисел
г) Математическая конструкция, позволяющая установить авторство и целостность сообщения

13. Что такое симметричные криптографические системы?
а) Системы, использующие один и тот же ключ для шифрования и расшифрования данных
б) Системы, использующие разные ключи для шифрования и расшифрования данных
в) Системы, использующие открытый ключ для шифрования и закрытый ключ для расшифрования данных
г) Системы, использующие хэш-функции для шифрования данных

14. Какие методы используются для получения псевдослучайных последовательностей?

а) Линейный конгруэнтный генератор, метод Фибоначчи, метод Блума
б) Линейно-сдвиговый регистр, метод RSA, метод Монте-Карло
в) Линейный конгруэнтный генератор, метод Фибоначчи, метод BBS
г) Метод DES, метод AES, метод ГОСТ 28147-89

15. Что такое отечественные алгоритмы Магма и Кузнечик?
а) Симметричные алгоритмы шифрования, разработанные в России
б) Асимметричные алгоритмы шифрования, разработанные в России
в) Хэш-функции, разработанные в России
г) Алгоритмы цифровой подписи, разработанные в России

16. Что такое DES?
а) Симметричный алгоритм шифрования с блочным размером 64 бита
б) Асимметричный алгоритм шифрования с блочным размером 64 бита
в) Хэш-функция с блочным размером 64 бита
г) Алгоритм цифровой подписи с блочным размером 64 бита

17. Что такое AES?
а) Симметричный алгоритм шифрования с блочным размером 128 бит
б) Асимметричный алгоритм шифрования с блочным размером 128 бит
в) Хэш-функция с блочным размером 128 бит
г) Алгоритм цифровой подписи с блочным размером 128 бит

18. Какие ключевые размеры поддерживает AES?
а) 64 бит, 256 бит, 512 бит
б) 64 бит, 128 бит, 256 бит
в) 128 бит, 256 бит, 512 бит
г) 128 бит, 192 бит, 256 бит

19. Что такое аппаратное шифрование?
а) Шифрование, выполняемое программными средствами
б) Шифрование, выполняемое специализированными устройствами
в) Шифрование, выполняемое с помощью аппаратных ключей
г) Шифрование, выполняемое на аппаратных уровнях компьютера

20. Что такое стандартизация программно-аппаратных криптографических систем и средств?
а) Процесс разработки и утверждения стандартов для криптографических систем и средств
б) Процесс тестирования и сертификации криптографических систем и средств
в) Процесс патентования и лицензирования криптографических систем и средств
г) Процесс разработки и маркировки криптографических систем и средств

21. Какие понятия связаны с аутентификацией данных?
а) ЭП (электронная подпись)
б) MAC (код аутентификации сообщений)
в) Однонаправленные хеш-функции
г) Все варианты ответов верны

22. Что такое необратимость систем в криптографии?
а) Возможность восстановления исходных данных из зашифрованных
б) Невозможность восстановления исходных данных из зашифрованных
в) Возможность восстановления ключа шифрования из шифротекста
г) Невозможность восстановления ключа шифрования из шифротекста

23. Какая криптографическая защита используется в беспроводных сетях стандарта 802.11?
а) WPA
б) WEP
в) SSL
г) IPSec

24. Что такое криптомаршрутизатор?
а) Устройство, обеспечивающее шифрование данных при маршрутизации
б) Устройство, обеспечивающее аутентификацию данных при маршрутизации
в) Устройство, обеспечивающее обнаружение вторжений при маршрутизации
г) Устройство, обеспечивающее анонимность при маршрутизации

25. Какие протоколы используются для криптографической защиты беспроводных соединений?
а) WPA2
б) WEP
в) WPA3
г) Все варианты ответов верны

26. Что такое структурная схема шифрования с открытым ключом?
а) Процесс шифрования и расшифрования данных с использованием одного ключа
б) Процесс шифрования и расшифрования данных с использованием двух разных ключей
в) Процесс шифрования и расшифрования данных без использования ключей
г) Процесс шифрования и расшифрования данных с использованием общего секретного ключа

27. Какие алгоритмы используются для цифровой подписи?
а) RSA
б) AES
в) DES
г) SHA-256

28. Что такое пакетный фильтр?
а) Устройство, контролирующее передачу пакетов данных
б) Устройство, шифрующее пакеты данных перед передачей
в) Устройство, выполняющее аутентификацию пакетов данных
г) Устройство, отслеживающее пакеты данных в сети

29. Какие преимущества имеет протокол WPA3 по сравнению с WPA2?
а) Более высокая производительность
б) Улучшенная защита от взлома
в) Расширенная поддержка устройств
г) Все варианты ответов верны

30. Какие методы шифрования используются для обеспечения защиты данных в сетевых коммуникациях?
а) Абонентское шифрование и пакетное шифрование
б) Симметричное шифрование и асимметричное шифрование
в) все варианты верны
г) все варианты неверны

31. Что такое однонаправленные хеш-функции?
а) Функции, которые могут быть использованы только для шифрования данных

б) Функции, которые могут быть использованы только для расшифрования данных
в) Функции, которые могут быть использованы только для аутентификации данных
г) Функции, которые могут быть использованы только для генерации случайных чисел

32. Что такое аутентификация данных в криптографии?
а) Процесс передачи данных по зашифрованному каналу связи
б) Процесс проверки подлинности и целостности данных
в) Процесс шифрования данных перед передачей
г) Процесс дешифрования данных после передачи

33. Какие уязвимости имеет протокол WEP?
а) Легко поддаётся взлому с помощью атак перебора ключа
б) Ограниченная поддержка устройств
в) Низкая производительность
г) Высокая стоимость реализации

34. Что такое абонентское шифрование?

а) Шифрование данных перед передачей их по сети
б) Шифрование данных, используя открытый ключ получателя
в) Шифрование данных, используя общий секретный ключ
г) Шифрование данных, используя публичный ключ отправителя

35. Что такое пакетное шифрование?
а) Шифрование данных в пакете, перед отправкой по сети
б) Шифрование данных в режиме потока передачи
в) Шифрование данных в режиме блочной передачи
г) Шифрование данных в пакете, после отправки по сети

36. Какие криптосистемы используются с открытым ключом?
а) DES
б) RSA
в) AES
г) Blowfish

37. Какие элементы теории чисел используются в криптографии с открытым ключом?
а) Простые числа
б) Рациональные числа
в) Комплексные числа
г) Натуральные числа

38. Что нужно защищать в центре генерации ключей при абонентском шифровании?
а) Отправленные данные
б) Приватные ключи
в) Публичные ключи
г) Аутентификационные данные

39. Какая основная проблема с протоколом WEP?
а) Низкая производительность
б) Легко подвержен взлому
в) Ограниченная поддержка устройств
г) Высокая стоимость реализации

40. Какой протокол обеспечивает криптографическую защиту беспроводных соединений в сетях стандарта 802.11?
а) WPA
б) WEP
в) SSL
г) IPSec

Вариант №3

1. Что такое поточное шифрование?
а) Многоалфавитная подстановка
б) Гаммирование
в) Табличная перестановка
г) Симметричное шифрование

2. Какие принципы лежат в основе поточного шифрования?
а) XOR и сдвиг
б) RSA и диффи-хеллман
в) Хеш-функции и эллиптические кривые
г) Линейные операции и перестановки

3. Что такое генераторы ПСЧ?
а) Устройства для генерации случайных чисел
б) Устройства для генерации псевдослучайных чисел
в) Устройства для генерации паролей
г) Устройства для генерации хэш-кодов

4. Какие методы используются для получения псевдослучайных последовательностей?
а) Линейный конгруэнтный генератор, метод Фибоначчи, метод Блума
б) Линейно-сдвиговый регистр, метод RSA, метод Монте-Карло
в) Линейный конгруэнтный генератор, метод Фибоначчи, метод BBS
г) Метод DES, метод AES, метод ГОСТ 28147-89

5. Какие методы кодирования информации вы знаете?
а) Символьное кодирование, смысловое кодирование, бинарное кодирование
б) Хаффмановское кодирование, кодирование Хемминга, кодирование CRC
в) Бинарное кодирование, кодирование Грея, кодирование Рида-Соломона
г) Бинарное кодирование, кодирование Грея, кодирование Фибоначчи

6. Что представляет собой таблица ASCII?
а) Таблица символов и их двоичных представлений
б) Таблица символов и их шестнадцатеричных представлений
в) Таблица символов и их десятичных представлений
г) Таблица символов и их восьмеричных представлений

7. Что такое механизация шифрования?
а) Процесс автоматизации шифрования
б) Процесс механического шифрования
в) Процесс программного шифрования
г) Процесс смешанного шифрования

8. Что такое компьютеризация шифрования?
а) Процесс применения компьютеров для шифрования данных
б) Процесс разработки компьютерных программ для шифрования
в) Процесс разработки компьютерных алгоритмов шифрования
г) Процесс применения компьютерных средств для анализа шифров

9. Что такое аппаратное шифрование?
а) Шифрование, выполняемое программными средствами
б) Шифрование, выполняемое специализированными устройствами
в) Шифрование, выполняемое с помощью аппаратных ключей
г) Шифрование, выполняемое на аппаратных уровнях компьютера

10. Что такое программное шифрование?
а) Шифрование, выполняемое с использованием программных средств
б) Шифрование, выполняемое на уровне операционной системы
в) Шифрование, выполняемое на уровне ядра компьютера
г) Шифрование, выполняемое на уровне аппаратных устройств

11. Что такое стандартизация программно-аппаратных криптографических систем и средств?
а) Процесс разработки и утверждения стандартов для криптографических систем и средств
б) Процесс тестирования и сертификации криптографических систем и средств
в) Процесс патентования и лицензирования криптографических систем и средств
г) Процесс разработки и маркировки криптографических систем и средств

12. Что такое симметричные криптографические системы?
а) Системы, использующие один и тот же ключ для шифрования и расшифрования данных
б) Системы, использующие разные ключи для шифрования и расшифрования данных
в) Системы, использующие открытый ключ для шифрования и закрытый ключ для расшифрования данных
г) Системы, использующие хэш-функции для шифрования данных

13. Что такое отечественные алгоритмы Магма и Кузнечик?
а) Симметричные алгоритмы шифрования, разработанные в России
б) Асимметричные алгоритмы шифрования, разработанные в России
в) Хэш-функции, разработанные в России
г) Алгоритмы цифровой подписи, разработанные в России

14. Какие стандарты соответствуют алгоритмам Магма и Кузнечик?
а) ГОСТ Р 34.12-2015 и ГОСТ Р 34.13-2015
б) ГОСТ Р 28147-89 и ГОСТ Р 34.11-2012
в) ГОСТ Р 34.10-2012 и ГОСТ Р 34.12-2015
г) ГОСТ Р 34.13-2015 и ГОСТ Р 34.11-2012

15. Какие алгоритмы относятся к симметричным алгоритмам?
а) RSA, DSA, ECDSA, ElGamal
б) DES, AES, ГОСТ 28147-89, RC4
в) SHA-1, SHA-256, MD5, HMAC
г) Diffie-Hellman, RSA, ElGamal, DSA

16. Что такое DES?
а) Симметричный алгоритм шифрования с блочным размером 64 бита
б) Асимметричный алгоритм шифрования с блочным размером 64 бита

в) Хэш-функция с блочным размером 64 бита
г) Алгоритм цифровой подписи с блочным размером 64 бита

17. Что такое AES?
а) Симметричный алгоритм шифрования с блочным размером 128 бит
б) Асимметричный алгоритм шифрования с блочным размером 128 бит
в) Хэш-функция с блочным размером 128 бит
г) Алгоритм цифровой подписи с блочным размером 128 бит

18. Какие ключевые размеры поддерживает AES?
а) 64 бит, 256 бит, 512 бит
б) 64 бит, 128 бит, 256 бит
в) 128 бит, 256 бит, 512 бит
г) 128 бит, 192 бит, 256 бит

19. Что такое асимметричные криптографические системы?
а) Системы, использующие один и тот же ключ для шифрования и расшифрования данных
б) Системы, использующие разные ключи для шифрования и расшифрования данных
в) Системы, использующие открытый ключ для шифрования и закрытый ключ для расшифрования данных
г) Системы, использующие хэш-функции для шифрования данных

20. Какой алгоритм шифрования наиболее широко используется в асимметричной криптографии?
а) DES
б) AES
в) RSA
г) HMAC

21. Что такое аутентификация данных в криптографии?
а) Процесс передачи данных по зашифрованному каналу связи
б) Процесс проверки подлинности и целостности данных
в) Процесс шифрования данных перед передачей
г) Процесс дешифрования данных после передачи

22. Какие понятия связаны с аутентификацией данных?
а) ЭП (электронная подпись)
б) MAC (код аутентификации сообщений)
в) Однонаправленные хеш-функции
г) Все варианты ответов верны

23. Что такое пакетное шифрование?
а) Шифрование данных в пакете, перед отправкой по сети
б) Шифрование данных в режиме потока передачи
в) Шифрование данных в режиме блочной передачи
г) Шифрование данных в пакете, после отправки по сети

24. Что такое криптомаршрутизатор?
а) Устройство, обеспечивающее шифрование данных при маршрутизации
б) Устройство, обеспечивающее аутентификацию данных при маршрутизации
в) Устройство, обеспечивающее обнаружение вторжений при маршрутизации
г) Устройство, обеспечивающее анонимность при маршрутизации

25. Какие протоколы используются для криптографической защиты беспроводных соединений?
а) WPA2
б) WEP
в) WPA3
г) Все варианты ответов верны

26. Что такое структурная схема шифрования с открытым ключом?
а) Процесс шифрования и расшифрования данных с использованием одного ключа
б) Процесс шифрования и расшифрования данных с использованием двух разных ключей
в) Процесс шифрования и расшифрования данных без использования ключей
г) Процесс шифрования и расшифрования данных с использованием общего секретного ключа

27. Какие алгоритмы используются для цифровой подписи?
а) RSA
б) AES
в) DES
г) SHA-256

28. Что такое пакетный фильтр?
а) Устройство, контролирующее передачу пакетов данных
б) Устройство, шифрующее пакеты данных перед передачей
в) Устройство, выполняющее аутентификацию пакетов данных
г) Устройство, отслеживающее пакеты данных в сети

29. Какие преимущества имеет протокол WPA3 по сравнению с WPA2?
а) Более высокая производительность
б) Улучшенная защита от взлома
в) Расширенная поддержка устройств
г) Все варианты ответов верны

30. Какие методы шифрования используются для обеспечения защиты данных в сетевых коммуникациях?
а) Абонентское шифрование и пакетное шифрование
б) Симметричное шифрование и асимметричное шифрование
в) все варианты верны
г) все варианты неверны

31. Что такое необратимость систем в криптографии?
а) Возможность восстановления исходных данных из зашифрованных
б) Невозможность восстановления исходных данных из зашифрованных
в) Возможность восстановления ключа шифрования из шифротекста
г) Невозможность восстановления ключа шифрования из шифротекста

32. Что такое однонаправленные хеш-функции?
а) Функции, которые могут быть использованы только для шифрования данных
б) Функции, которые могут быть использованы только для расшифрования данных
в) Функции, которые могут быть использованы только для аутентификации данных
г) Функции, которые могут быть использованы только для генерации случайных чисел

33. Какие уязвимости имеет протокол WEP?
а) Легко поддаётся взлому с помощью атак перебора ключа
б) Ограниченная поддержка устройств

в) Низкая производительность
г) Высокая стоимость реализации

34. Что такое абонентское шифрование?
а) Шифрование данных перед передачей их по сети
б) Шифрование данных, используя открытый ключ получателя
в) Шифрование данных, используя общий секретный ключ
г) Шифрование данных, используя публичный ключ отправителя

35. Какие криптосистемы используются с открытым ключом?
а) DES
б) RSA
в) AES
г) Blowfish

36. Какие элементы теории чисел используются в криптографии с открытым ключом?
а) Простые числа
б) Рациональные числа
в) Комплексные числа
г) Натуральные числа

37. Что нужно защищать в центре генерации ключей при абонентском шифровании?
а) Отправленные данные
б) Приватные ключи
в) Публичные ключи
г) Аутентификационные данные

38. Какая основная проблема с протоколом WEP?
а) Низкая производительность
б) Легко подвержен взлому
в) Ограниченная поддержка устройств
г) Высокая стоимость реализации

39. Какой протокол обеспечивает криптографическую защиту беспроводных соединений в сетях стандарта 802.11?
а) WPA
б) WEP
в) SSL
г) IPSec

40. Какие методы шифрования используются для обеспечения конфиденциальности данных в беспроводных сетях?
а) Абонентское шифрование и пакетное шифрование
б) Симметричное шифрование и асимметричное шифрование
в) все варианты верны
г) все варианты неверны

Вариант №4

1. Что такое поточное шифрование?
а) Шифрование, использующее потоки данных

б) Шифрование, использующее блоки данных
в) Шифрование, использующее хэш-функции
г) Шифрование, использующее симметричные ключи

2. Что такое асимметричные криптографические системы?
а) Системы, использующие один и тот же ключ для шифрования и расшифрования данных
б) Системы, использующие разные ключи для шифрования и расшифрования данных
в) Системы, использующие открытый ключ для шифрования и закрытый ключ для расшифрования данных
г) Системы, использующие хэш-функции для шифрования данных

3. Что такое генераторы ПСЧ?
а) Устройства для генерации случайных чисел
б) Устройства для генерации псевдослучайных чисел
в) Устройства для генерации паролей
г) Устройства для генерации хэш-кодов

4. Что такое алгоритм RSA?
а) Асимметричный алгоритм шифрования и подписи
б) Симметричный алгоритм шифрования
в) Хэш-функция
г) Алгоритм генерации случайных чисел

5. Какие методы используются для получения псевдослучайных последовательностей?
а) Линейный конгруэнтный генератор, метод Фибоначчи, метод Блума
б) Линейно-сдвиговый регистр, метод RSA, метод Монте-Карло
в) Линейный конгруэнтный генератор, метод Фибоначчи, метод BBS
г) Метод DES, метод AES, метод ГОСТ 28147-89

6. Что такое хэш-функция?
а) Математическая функция, преобразующая входные данные в случайную последовательность битов
б) Математическая функция, преобразующая входные данные в строку переменной длины
в) Математическая функция, преобразующая входные данные в фиксированную строку фиксированной длины
г) Математическая функция, используемая для шифрования данных

7. Какие основные свойства должны обладать хорошая хэш-функция?
а) Односторонняя функция, стойкость к коллизиям, равномерное распределение значений
б) Обратимость, стойкость к коллизиям, высокая скорость вычислений
в) Стойкость к коллизиям, равномерное распределение значений, высокая скорость вычислений
г) Обратимость, стойкость к коллизиям, равномерное распределение значений

8. Что такое цифровая подпись?
а) Процесс расшифрования данных с использованием закрытого ключа
б) Процесс шифрования данных с использованием открытого ключа
в) Алгоритм, используемый для генерации псевдослучайных чисел
г) Математическая конструкция, позволяющая установить авторство и целостность сообщения

9. Что такое механизация шифрования?
а) Процесс автоматизации шифрования
б) Процесс механического шифрования
в) Процесс программного шифрования

г) Процесс смешанного шифрования

10. Какие методы кодирования информации вы знаете?
а) Символьное кодирование, смысловое кодирование, бинарное кодирование
б) Хаффмановское кодирование, кодирование Хемминга, кодирование CRC
в) Бинарное кодирование, кодирование Грея, кодирование Рида-Соломона
г) Бинарное кодирование, кодирование Грея, кодирование Фибоначчи

11. Что такое компьютеризация шифрования?
а) Процесс применения компьютеров для шифрования данных
б) Процесс разработки компьютерных программ для шифрования
в) Процесс разработки компьютерных алгоритмов шифрования
г) Процесс применения компьютерных средств для анализа шифров

12. Что представляет собой таблица ASCII?
а) Таблица символов и их двоичных представлений
б) Таблица символов и их шестнадцатеричных представлений
в) Таблица символов и их десятичных представлений
г) Таблица символов и их восьмеричных представлений

13. Что такое атака на основе словаря (dictionary attack)?
а) Атака, при которой злоумышленник пытается получить доступ к системе, подбирая разные словарные слова
б) Атака, при которой злоумышленник перебирает все возможные комбинации паролей из заданного словаря
в) Атака, при которой злоумышленник обменивается словарями с другими злодеями
г) Атака, при которой не используются общеупотребительные слова или фразы из словарей для компрометации учетных данных пользователя

14. Что такое аппаратное шифрование?
а) Шифрование, выполняемое программными средствами
б) Шифрование, выполняемое специализированными устройствами
в) Шифрование, выполняемое с помощью аппаратных ключей
г) Шифрование, выполняемое на аппаратных уровнях компьютера

15. Что такое программное шифрование?
а) Шифрование, выполняемое с использованием программных средств
б) Шифрование, выполняемое на уровне операционной системы
в) Шифрование, выполняемое на уровне ядра компьютера
г) Шифрование, выполняемое на уровне аппаратных устройств

16. Что такое стандартизация программно-аппаратных криптографических систем и средств?
а) Процесс разработки и утверждения стандартов для криптографических систем и средств
б) Процесс тестирования и сертификации криптографических систем и средств
в) Процесс патентования и лицензирования криптографических систем и средств
г) Процесс разработки и маркировки криптографических систем и средств

17. Что такое симметричные криптографические системы?
а) Системы, использующие один и тот же ключ для шифрования и расшифрования данных
б) Системы, использующие разные ключи для шифрования и расшифрования данных
в) Системы, использующие открытый ключ для шифрования и закрытый ключ для расшифрования данных

г) Системы, использующие хэш-функции для шифрования данных

18. Что такое отечественные алгоритмы Магма и Кузнечик?
а) Симметричные алгоритмы шифрования, разработанные в России
б) Асимметричные алгоритмы шифрования, разработанные в России
в) Хэш-функции, разработанные в России
г) Алгоритмы цифровой подписи, разработанные в России

19. Какие стандарты соответствуют алгоритмам Магма и Кузнечик?
а) ГОСТ Р 34.12-2015 и ГОСТ Р 34.13-2015
б) ГОСТ Р 28147-89 и ГОСТ Р 34.11-2012
в) ГОСТ Р 34.10-2012 и ГОСТ Р 34.12-2015
г) ГОСТ Р 34.13-2015 и ГОСТ Р 34.11-2012

20. Какой алгоритм шифрования наиболее широко используется в асимметричной криптографии?
а) DES
б) AES
в) RSA
г) HMAC

21. Какие криптосистемы используются с открытым ключом?
а) DES
б) RSA
в) AES
г) Blowfish

22. Что такое аутентификация данных в криптографии?
а) Процесс передачи данных по зашифрованному каналу связи
б) Процесс проверки подлинности и целостности данных
в) Процесс шифрования данных перед передачей
г) Процесс дешифрования данных после передачи

23. Какие понятия связаны с аутентификацией данных?
а) ЭП (электронная подпись)
б) MAC (код аутентификации сообщений)
в) Однонаправленные хеш-функции
г) Все варианты ответов верны

24. Что такое структурная схема шифрования с открытым ключом?
а) Процесс шифрования и расшифрования данных с использованием одного ключа
б) Процесс шифрования и расшифрования данных с использованием двух разных ключей
в) Процесс шифрования и расшифрования данных без использования ключей
г) Процесс шифрования и расшифрования данных с использованием общего секретного ключа

25. Какие элементы теории чисел используются в криптографии с открытым ключом?
а) Простые числа
б) Рациональные числа
в) Комплексные числа
г) Натуральные числа

26. Что такое необратимость систем в криптографии?
а) Возможность восстановления исходных данных из зашифрованных

б) Невозможность восстановления исходных данных из зашифрованных
в) Возможность восстановления ключа шифрования из шифротекста
г) Невозможность восстановления ключа шифрования из шифротекста

27. Что такое однонаправленные хеш-функции?
а) Функции, которые могут быть использованы только для шифрования данных
б) Функции, которые могут быть использованы только для расшифрования данных
в) Функции, которые могут быть использованы только для аутентификации данных
г) Функции, которые могут быть использованы только для генерации случайных чисел

28. Какие алгоритмы используются для цифровой подписи?
а) RSA
б) AES
в) DES
г) SHA-256

29. Что такое абонентское шифрование?
а) Шифрование данных перед передачей их по сети
б) Шифрование данных, используя открытый ключ получателя
в) Шифрование данных, используя общий секретный ключ
г) Шифрование данных, используя публичный ключ отправителя

30. Что такое пакетное шифрование?
а) Шифрование данных в пакете, перед отправкой по сети
б) Шифрование данных в режиме потока передачи
в) Шифрование данных в режиме блочной передачи
г) Шифрование данных в пакете, после отправки по сети

31. Что нужно защищать в центре генерации ключей при абонентском шифровании?
а) Отправленные данные
б) Приватные ключи
в) Публичные ключи
г) Аутентификационные данные

32. Что такое криптомаршрутизатор?
а) Устройство, обеспечивающее шифрование данных при маршрутизации
б) Устройство, обеспечивающее аутентификацию данных при маршрутизации
в) Устройство, обеспечивающее обнаружение вторжений при маршрутизации
г) Устройство, обеспечивающее анонимность при маршрутизации

33. Что такое пакетный фильтр?
а) Устройство, контролирующее передачу пакетов данных
б) Устройство, шифрующее пакеты данных перед передачей
в) Устройство, выполняющее аутентификацию пакетов данных
г) Устройство, отслеживающее пакеты данных в сети

34. Какая криптографическая защита используется в беспроводных сетях стандарта 802.11?
а) WPA
б) WEP
в) SSL
г) IPSec

35. Что означает сокращение WPA?

а) Wireless Privacy Access
б) Wi-Fi Protected Access
в) Wireless Protected Access
г) Wi-Fi Privacy Access

36. Что означает сокращение WEP?
а) Wireless Encryption Protocol
б) Wi-Fi Encryption Protocol
в) Wireless Enhanced Protection
г) Wi-Fi Enhanced Privacy

37. Какие протоколы используются для криптографической защиты беспроводных соединений?
а) WPA2
б) WEP
в) WPA3
г) Все варианты ответов верны

38. Какая основная проблема с протоколом WEP?
а) Низкая производительность
б) Легко подвержен взлому
в) Ограниченная поддержка устройств
г) Высокая стоимость реализации

39. Какой алгоритм используется для шифрования в протоколе WPA2?
а) AES
б) DES
в) RSA
г) Blowfish

40. Какие методы шифрования используются для обеспечения защиты данных в сетевых коммуникациях?
а) Абонентское шифрование и пакетное шифрование
б) Симметричное шифрование и асимметричное шифрование
в) все варианты верны
г) все варианты неверны

Критерии оценивания экзамена (зачета):

Количество вопросов	Оценка	
31-40	**5**	**отлично**
21-30	**4**	**хорошо**
11-20	**3**	**удовлетворительно**
0-10	**2**	**не зачтено**

Зачтено - выставляется обучающемуся, ответившему правильно на 11-40 вопросов.
Не зачтено - выставляется обучающемуся, который ответил на 10 и менее вопросов.
Отлично - выставляется обучающемуся, ответившему на 31-40 вопросов.
Хорошо - выставляется обучающемуся, ответившему на 21-30 вопросов.
Удовлетворительно - выставляется обучающемуся, ответившему на 11-20 вопросов.

Ключи к тесту

№ п/п	Вариант № 1	Вариант № 2	Вариант №3	Вариант №4
1	б	а	г	а
2	а	в	а	в
3	а	б	а	б
4	б	а	в	а
5	б	в	б	в
6	в	в	а	в
7	а	а	б	а
8	в	г	а	г
9	б	б	б	б
10	а	б	а	б
11	а	а	а	а
12	г	а	а	а
13	а	б	а	б
14	а	б	а	б
15	в	а	б	а
16	б	а	а	а
17	а	а	а	а
18	а	а	г	а
19	а	а	в	а
20	г	в	в	в
21	б	г	б	б
22	г	б	г	б
23	а	а	а	г
24	г	а	а	б
25	б	г	г	а
26	а	б	б	б

27	а	а	а	в
28	г	а	а	а
29	в	г	г	б
30	б	в	в	а
31	в	в	б	б
32	а	б	в	а
33	б	а	а	а
34	а	б	б	а
35	б	а	б	б
36	а	б	а	а
37	б	а	б	г
38	б	б	б	б
39	а	б	а	а
40	а	а	в	в