

АВТОНОМНАЯ НЕКОММЕРЧЕСКАЯ ОРГАНИЗАЦИЯ ВЫСШЕГО ОБРАЗОВАНИЯ  
САМАРСКИЙ УНИВЕРСИТЕТ ГОСУДАРСТВЕННОГО УПРАВЛЕНИЯ  
«МЕЖДУНАРОДНЫЙ ИНСТИТУТ РЫНКА»

УТВЕРЖДАЮ  
Проректор по учебной работе и  
качеству образования

\_\_\_\_\_ И. А. Долгова

16 апреля 2025 г.

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДИСЦИПЛИНЫ

**ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ**

---

Направление подготовки:	09.03.03 Прикладная информатика
Профиль подготовки:	Корпоративные информационные системы
Квалификация:	бакалавр
Форма обучения:	очная, очно-заочная
Год начала подготовки:	2025

Самара  
2025

## 1. ОЦЕНОЧНЫЕ СРЕДСТВА, СООТНЕСЁННЫЕ С ПЛАНИРУЕМЫМИ РЕЗУЛЬТАТАМИ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ

Код и наименование компетенции	Код и наименование индикатора достижения компетенции	Результаты обучения по дисциплине	Вид аттестации и оценочных средств
ПК-5. Способен обеспечить качество функционирования информационной системы с учетом современных бизнес-решений и требований информационной безопасности	ПК-5.2. Выполняет требования информационной безопасности при функционировании информационной системы	ПК-5.2.1. Знает основные угрозы для информационной безопасности организации, а также методы их нейтрализации	Текущий контроль: устный опрос, лабораторная работа, промежуточный тест. Промежуточная аттестация: экзамен.
		ПК-5.2.1. Умеет применить комплекс мер по защите инфраструктуры предприятия от злоумышленников и вредоносных программ	Текущий контроль: устный опрос, лабораторная работа, промежуточный тест. Промежуточная аттестация: экзамен.

## 2. ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ТЕКУЩЕГО КОНТРОЛЯ

### 2.1. Вопросы для подготовки к семинарским/практическим занятиям

Раздел 1. Введение в изучение дисциплины «Информационная безопасность»

1. Какие категории информации используются в информационной безопасности?
2. Какие существуют методы обеспечения информационной безопасности и защиты информации.
3. Какие существуют разновидности угроз информации?
4. Какие существуют действия, приводящие к неправомерному овладению информацией.
5. Опишите направления обеспечения информационной безопасности и защиты информации.

Раздел 2. Правовые и организационные методы защиты информации

6. Назовите основные законодательные акты в области защиты информации.
7. Что такое персональные данные и какие есть особенности их обработки?
8. Что такое модель угроз информации предприятия?
9. Как строится модель угроз?
10. Какие существуют модели доступа к информации?

Раздел 3. Современная криптография и смежные дисциплины

11. Назовите и охарактеризуйте наиболее известные исторические шифры.
12. Опишите принцип работы симметричного шифрования.
13. Опишите принцип работы асимметричного шифрования.
14. Что такое криптографические хэши? Какие к ним предъявляются требования?
15. Для чего используется электронно-цифровая подпись?
16. Для чего создается и используется инфраструктура открытых ключей.
17. Что такое сертификат?
18. Что такое пост-квантовая криптография?
19. Как работает стеганография?

Раздел 4. Современные программные угрозы и злоумышленники

20. Какие существуют виды вредоносных программ
21. Какие существуют программные угрозы помимо вредоносных программ?
22. Какие существуют виды злоумышленников?
23. Какие угрозы создаются вредоносными программами и злоумышленниками в рамках информационной инфраструктуры предприятия.
24. Что такое социальная инженерия в контексте информационной безопасности?

Раздел 5. Программно-технические методы защиты данных

25. Какие существуют антивирусные пакеты и какой у них функционал?
26. Какие бывают и как работают межсетевые экраны.
27. Какие бывают и как работают средства резервного копирования.
28. Как работают системы обнаружения и предотвращения вторжений?
29. Как работают системы предотвращения утечек.

#### Критерии оценки работы на практическом занятии

Критерии	Максимальное количество баллов за занятие
<b>Устный опрос, коллоквиум</b>	
Основные теоретические положения по вопросу раскрыты. Имеются элементы обоснования выводов.	5 баллов

Имеются элементы систематизации информации, факты применения профессиональной терминологии.  
Очевидно использование источников рекомендованной литературы.

## 2.2. Темы лабораторных работ

### Раздел 1. Введение в изучение дисциплины «Информационная безопасность»

Лабораторная работа №1. Введение в дисциплину

*Цель работы:* Ознакомиться с основными терминами, определениями и понятиями информационной безопасности и защиты информации

*Вопросы для самопроверки:*

1. Приведите пример разглашения информации
2. Приведите примеры утечек информации по техническим каналам
3. Приведите примеры несанкционированного доступа к информации
4. Охарактеризуйте направления защиты информации и приведите примеры по каждому направлению

### Раздел 2. Правовые и организационные методы защиты информации

Лабораторная работа №2. Изучение моделей доступа

*Цель работы:* Получить навыки работы с моделями разграничения доступа в современных системах

*Вопросы для самопроверки:*

1. Какие бывают модели доступа?
2. Какая модель доступа используется в файловых системах Windows
3. Как реализуется модель доступа в Linux
4. Приведите пример реализации моделей доступа в различных программных продуктах.

### Раздел 3. Современная криптография и смежные дисциплины

Лабораторная работа №3. Работа с VeraCrypt

*Цель работы:* Изучение работы системы шифрования информации на дисках VeraCrypt, получение практических навыков по работе с зашифрованными разделами и контейнерами.

*Вопросы для самопроверки:*

1. Какие типы зашифрованных носителей можно создать в VeraCrypt?
2. Какие алгоритмы шифрования поддерживаются в VeraCrypt?
3. Какие техники правдоподобного отрицания используются в VeraCrypt?
4. Что можно использовать в качестве ключа доступа к зашифрованным носителям?
5. Как организуются и как работают скрытые тома?

Лабораторная работа №4. Утилиты хэширования

*Цель работы:* Изучение работы утилит хэширования, освоение процедур проверки целостности файлов с помощью хэшей.

*Вопросы для самопроверки:*

1. Какие существуют популярные хэши, утвержденные на международном уровне?
2. Какие существуют отечественные алгоритмы хэширования?
3. Какие утилиты можно использовать для расчета хэшей файлов?

Лабораторная работа №5. Шифрование с открытым ключом

*Цель работы:* Освоить систему шифрования с открытым ключом GnuPG (в составе пакета Gpg4Win), понять принцип работы асимметричного шифрования (с открытым

ключом), научиться производить основные операции: операции с ключами, шифрование, подписывание

*Вопросы для самопроверки:*

1. Какие алгоритмы поддерживает утилита GnuPG?
2. Как создать пару ключей в утилите GnuPG?
3. Как подписать файл с помощью своего ключа?
4. Чем отличается режим открепленной подписи и режим прикрепленной подписи?
5. Каким ключом шифруется файл в шифровании с открытым ключом?
6. Как зашифровать файл с помощью утилиты GnuPG?

Лабораторная работа №6. Работа с сертификатами КриптоПро

*Цель работы:* Освоить систему пакет КриптоПро для шифрования и подписывания информации, научиться производить основные операции: операции с ключами, шифрование, подписывание

*Вопросы для самопроверки:*

1. Как создать ключевой носитель и сертификат подписи в КриптоПро?
3. Как подписать файл с помощью своего ключа?
4. Чем отличается режим открепленной подписи и режим прикрепленной подписи?
5. Каким сертификатом шифруется файл?

#### Раздел 4. Современные программные угрозы и злоумышленники

Лабораторная работа №7. Модель угроз

*Цель работы:* Изучить принципы построение модели угроз типового предприятия, получить практические навыки создания модели угроз.

*Вопросы для самопроверки:*

1. Какими нормативными актами регламентируется состав модели угроз?
2. По какому плану составляется общая и частная модель угроз?
3. Какова цель составления модели угроз?

#### Раздел 5. Программно-технические методы защиты данных

Лабораторная работа №8. Пользователи, группы и права доступа Windows

*Цель работы:* Изучить средства администрирования и управления пользователями и доступом в операционной системе Windows, получить навыки управления списками доступа к объектам файловых систем.

*Вопросы для самопроверки:*

1. Как создать пользователей и группы в Windows через графический интерфейс?
2. Как создать пользователей и группы в Windows через командную строку?
3. Как назначить пользователя в группу?
4. Как установить права доступа к файлу и каталогу?
5. Каким образом работает наследование в правах к объектам файловых систем?

Лабораторная работа №9. Пользователи, группы и права доступа Linux

*Цель работы:* Изучить средства администрирования и управления пользователями и доступом в операционной системе Linux, получить навыки управления списками доступа к объектам файловых систем.

*Вопросы для самопроверки:*

1. Как создать пользователей и группы в Linux через графический интерфейс?
2. Как создать пользователей и группы в Linux через командную строку?
3. Как назначить пользователя в группу?
4. Как установить права доступа к файлу и каталогу?
5. Каким образом работает наследование в правах к объектам файловых систем?

### **Цели лабораторных занятий:**

1. Углубление и закрепление знания теоретического курса путем практического изучения в лабораторных условиях изложенных в лекциях методов и технологий;
2. Приобретение навыков в научном экспериментировании, анализе полученных результатов;
3. Формирование первичных навыков организации, планирования и проведения научных исследований.

### **Порядок проведения лабораторного занятия:**

1. Вводная часть:
  - входной контроль подготовки обучаемого;
  - вводный инструктаж (знакомство обучающихся с содержанием предстоящей работы, краткий анализ теоретических положений и выводов, демонстрация подходов к выполнению отдельных операций, напоминание о технике безопасности, предупреждение о возможных ошибках).
2. Основная часть:
  - проведение обучаемым лабораторной работы;
  - текущее индивидуальное консультирование обучаемого;
3. Заключительная часть:
  - демонстрация результатов выполненного задания;
  - заключительный инструктаж (подведение итогов выполнения учебных задач, разбор допущенных ошибок и выявление их причин, сообщение результатов работы каждого обучаемого, объявление о том, что необходимо повторить к следующему занятию).

### **Особенности подготовки к проведению лабораторного занятия**

Подготовка лабораторного занятия начинается с изучения теоретических положений, определения (уточнения) целей и задач данного занятия, времени, выделяемого обучаемым для подготовки.

В ходе подготовки к лабораторной работе необходимо пояснить проблематику, объем и содержание лабораторного занятия, определить, какие понятия, определения, теории могут быть иллюстрированы данным экспериментом, какие умения и навыки должны приобрести обучаемые в ходе занятия, какие знания углубить и расширить.

При этом преподавателю необходимо решить, на каком этапе обучения следует поставить задачу о подготовке к лабораторной работе, каким образом достигнуть активизации познавательной деятельности обучающихся. Задача на подготовку к лабораторной работе может быть поставлена на лекции, с таким временным расчетом, чтобы обучаемые смогли качественно подготовиться к ее проведению. Одновременно им выдаются учебно-методические материалы, иллюстрирующие круг вопросов, затрагиваемых в ходе выполнения лабораторного задания. Это могут быть методические указания по соответствующему курсу, презентации, ссылки на Интернет-источники и др. Эти материалы могут отражать учебные вопросы, краткие сведения по теории, программу выполнения работы, содержание отчета, вопросы для подготовки и литературу, рекомендуемую к изучению и т.д. В них также ставятся задачи, которые обучаемые должны решить при подготовке к работе, в процессе эксперимента и при обработке полученных результатов.

В ходе подготовки к лабораторной работе необходимо обратить внимание обучающегося на результат ее выполнения. Результат лабораторной работы должен быть четко сформулирован, приведены критерии его достижения, перечень материалов, его (результат) иллюстрирующих – файлы, графики, скриншоты и т.д. Учащийся должен уметь формулировать основные выводы, опираясь на полученный на лабораторной работе результат.

В отдельных случаях, на лабораторном занятии может быть предусмотрена защита выполненной работы.

### **Шкала и критерии оценки лабораторной работы**

Критерии	Баллы
Степень соответствия выполненного задания поставленным требованиям	25
Структурирование и комментирование лабораторной работы	25
Уникальность выполненной работы (отличие от работ коллег)	25
Ответы на контрольные вопросы	25

Лабораторная работа оценивается по 100 балльной шкале, баллы переводятся в оценки успеваемости следующим образом:

90 – 100 баллов – «отлично»;

70 – 89 баллов – «хорошо»;

50 – 69 баллов – «удовлетворительно»;

менее 50 баллов – «неудовлетворительно».

### 3. ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

#### 3.1. Банк контрольных заданий (с указанием компетенции)

##### ПК-5.2

##### 1. Прочитайте текст и установите соответствие (ПК-5.2)

Установите соответствие между задачей по защите информации и типом защитного программного обеспечения

А)	Защита от вредоносных программ	1.	DLP
Б)	Защита от сетевых атак извне	2.	Антивирус
В)	Защита от утечек данных из организации	3.	ПО для шифрования
Г)	Защита конфиденциальности на сменных носителях	4.	Сертификаты
Д)	Обмен зашифрованной электронной почтой	5.	МСЭ

Запишите выбранные цифры под соответствующими буквами:

А	Б	В	Г	Д

##### 2. Прочитайте текст и установите последовательность (ПК-5.2)

Расположите шифры в порядке увеличения их оцениваемой теоретической криптостойкости от самого слабого до самого сильного.

1. Twofish
2. Blowfish
3. 3DES
4. AES256
5. DES
6. шифр замены
7. шифр Виженера

Запишите соответствующую последовательность букв слева направо

Ответ:

##### 3. Прочитайте текст, выберите правильные ответы и запишите аргументы, обосновывающие выбор ответов (ПК-5.2)

Выберите из приведенного три направления защиты информации

- А) инженерно-техническое
- Б) социальное
- Б) правовое
- В) экономическое
- Г) организационное
- Д) общественно-политическое



Ответ:

Обоснование:

**4. Прочитайте текст, выберите правильный ответ и запишите аргументы, обосновывающие выбор ответа (ПК-5.2)**

Кто должен создавать ключи в алгоритмах с открытым ключом?

- А) отправитель сообщений
- Б) получатель сообщений
- В) удостоверяющий центр

Ответ:

Обоснование:

**5. Прочитайте текст, выберите правильный ответ и запишите аргументы, обосновывающие выбор ответа (ПК-5.2)**

Как называется тип атаки, когда противник может вставлять, удалять или повторять сообщения, вклиниваясь между переговаривающимися партнерами?

- А) пассивная атака
- Б) нейтральная атака
- В) активная атака

Ответ:

Обоснование:

**6. Прочитайте текст и установите соответствие (ПК-5.2)**

Установите соответствие между категорией информации и ее определением

А)	Конфиденциальность	1.	Способность удостоверять имевшее место действие или событие так, чтобы эти события или действия не могли быть позже отвергнуты.
Б)	Аутентичность	2.	Свойство информации быть недоступной и закрытой для неавторизованного индивидуума, логического объекта или процесса.
В)	Неотказуемость	3.	Свойство объекта находиться в состоянии готовности и используемости по запросу авторизованного логического объекта.
Г)	Доступность	4.	Свойство, гарантирующее, что источником информации является именно то лицо, которое заявлено как ее автор

Запишите выбранные цифры под соответствующими буквами:

А	Б	В	Г

**7. Прочитайте текст и запишите развёрнутый обоснованный ответ (ПК-5.2)**

Нарисуйте схему работы шифрования с открытым ключом, указав этапы: создание ключей, процесс шифрования, процесс расшифровывания.

Ответ:

**8. Прочитайте текст и запишите развёрнутый обоснованный ответ (ПК-5.2)**

Нарисуйте схему подписывания с использованием открытого и закрытого ключа

Ответ:

**9. Прочитайте текст, выберите правильные ответы и запишите аргументы, обосновывающие выбор ответов (ПК-5.2)**

Какие из приведенных алгоритмов являются алгоритмами шифрования с открытым ключом?

- А) RC5
- Б) RSA
- В) DES
- Г) ElGamal
- Д) AES

Ответ:

Обоснование:

**10. Прочитайте текст и запишите развёрнутый обоснованный ответ (ПК-5.2)**

Опишите, какими тремя свойствами должны обладать криптографические хэш функции

Ответ:

**11. Прочитайте текст, выберите правильные ответы и запишите аргументы, обосновывающие выбор ответов (ПК-5.2)**

Какие параметры из приведенных обязательно присутствуют в любом сертификате X.509?

- А) имя сайта
- Б) открытый ключ субъекта
- В) срок действия сертификата
- Г) адрес электронной почты
- Д) название организации, заказавшей сертификат
- Е) серийный номер сертификата

Ответ:

Обоснование:

**12. Прочитайте текст, выберите правильный ответ и запишите аргументы, обосновывающие выбор ответа (ПК-5.2)**

Какое утверждение верно по отношению к компьютерным вирусам?

- А) заражают любые файлы, содержащие исполняемые инструкции
- Б) заражают только исполняемые файлы
- В) заражают только файлы документов с макросами
- Г) заражают только почтовые вложения

Ответ:

Обоснование:

**13. Прочитайте текст, выберите правильные ответы и запишите аргументы, обосновывающие выбор ответов (ПК-5.2)**

Какие из приведенных элементов, входят в концептуальную модель безопасности?

- А) угрозы
- Б) выпускаемая продукция
- В) услуги других организаций
- Г) источники информации
- Д) способы защиты информации

Ответ:

Обоснование:

**14. Прочитайте текст, выберите правильные ответы и запишите аргументы, обосновывающие выбор ответов (ПК-5.2)**

Какие два типа доступа существуют с точки зрения модели безопасности?

- А) чтение
- Б) создание
- В) запись
- Г) удаление

Ответ:

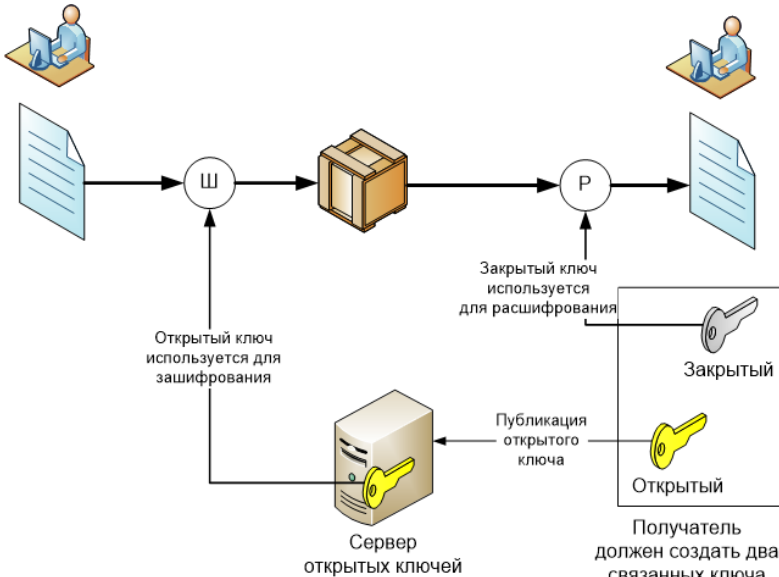
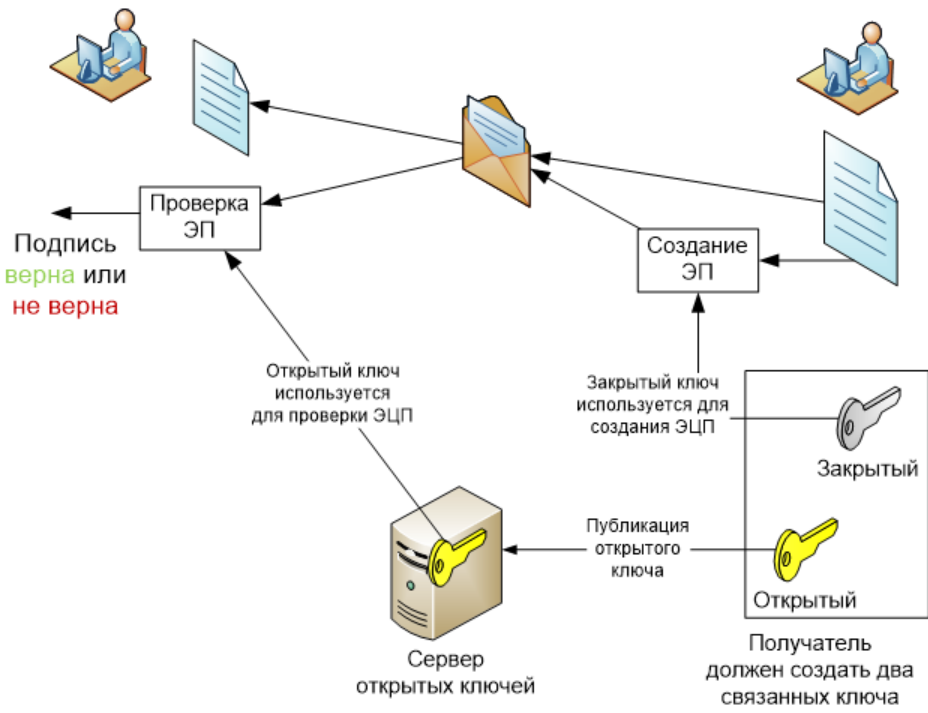
Обоснование:

**15. Прочитайте текст и запишите развёрнутый обоснованный ответ (ПК-5.2)**

Нарисуйте схему подписывания и проверки подписи в современных системах, где подписывается не все сообщение а его дайджест

Ответ:

### 3.2. Ключи к контрольным заданиям

№ задания	Верный ответ
1	A2 B5 B1 Г3 Д4
2	6 7 5 3 2 1 4
3	АБГ Существует только три направления защиты информации. Остальные указанные пункты не относятся к направлениям защиты.
4	Б В шифровании с открытым ключом тот, кто хочет получать зашифрованные сообщения, должен создать пару ключей – открытый и закрытый. Закрытый ключ хранится у него, а открытый выкладывается в публичный доступ.
5	В В случае пассивной атаки атакующий только прослушивает коммуникации, но не может на них влиять. Понятия "нейтральная" атака не существует.
6	A2 B4 B1 Д3
7	
8	
9	БГ

	RC5 – патентованный алгоритм симметричного шифрования, DES – устаревший алгоритм симметричного шифрования, AES – современный наиболее распространенный алгоритм симметричного шифрования.
10	1) Защищенностью от восстановления прообразов: должно быть невозможно в вычислительном отношении найти сообщение с данным значением хэш-функции; 2) Защищенностью от повторов: вычислительно невозможно найти два сообщения с одним и тем же значением хэш-функции; 3) Защищенностью от вторых прообразов: по данному сообщению нереально найти другое сообщение с тем же значением хэш-функции.
11	БВЕ Из приведенного списка в любом сертификате будет присутствовать открытый ключ субъекта, срок действия сертификата с определенной даты по определенную дату, серийный номер сертификата. Адрес электронной почты могут быть в персональных сертификатах для электронной почты. Адрес сайта указывается только в сертификатах сайтов. Название организации используется только в небольшом числе узкоспециализированных сертификатов.
12	А Заражаться могут любые файлы, которые содержат инструкции для исполнения либо программного кода, либо инструкции для интерпретации некоторого кода, например, макросы или скрипты в документах.
13	АГД Выпускаемая продукция не является ни объектом, ни субъектом обработки информации. Услуги других организаций не входят в модель, а только могут влиять на состав угроз и источников информации.
14	АВ Создание и удаление являются частным случаем доступа на запись.
15	<p>Создание подписи</p> <p>Проверка подписи</p>

### Шкала и критерии оценки текущего тестирования

Число правильных ответов	Оценка
90-100% правильных ответов	Оценка «отлично»
70-89% правильных ответов	Оценка «хорошо»

50-69% правильных ответов	Оценка «удовлетворительно»
Менее 50% правильных ответов	Оценка «неудовлетворительно»

### 3.3. Перечень тем для проверки образовательных результатов на знания (вопросы к экзамену)

1. Дайте определения понятиям: конфиденциальность, целостность, доступность, аутентичность, апеллируемость.
2. Опишите угрозы информации, их классификацию и дайте краткую характеристику.
3. Опишите действия, приводящие к неправомерному овладению информацией.
4. Назовите направления обеспечения защиты информации и дайте краткую характеристику.
5. Охарактеризуйте правовое направление защиты информации и приведите примеры.
6. Охарактеризуйте организационное направление защиты информации и приведите примеры.
7. Охарактеризуйте инженерно-техническое направление защиты информации и приведите примеры.
8. Назовите текущие законодательные и подзаконные акты, касающиеся защиты информации.
9. Назовите и дайте краткую характеристику законодательным и подзаконным актам, которые регламентируют применение средств криптографической защиты информации в РФ.
10. Опишите основные идеи и принципы в законе о персональных данных.
11. Дайте характеристику статей УК, касающихся защиты информации, и приведите примеры действий, попадающих под описанные статьи.
12. Назовите основные определения из закона об электронной подписи.
13. Назовите основные определения из закона об информации и информационных технологиях.
14. Какие законодательные инициативы в области защиты информации были реализованы в последние три года?
15. Дайте определение конфиденциальности, аутентичности с точки зрения криптографии и опишите требования к криптосистемам.
16. Назовите известные исторические шифры и дайте им характеристику.
17. Дайте определение и опишите работу симметричных шифров, дайте определение принципу Керкхоффа.
18. Опишите существующие на текущий момент сертифицированные в РФ алгоритмы шифрования.
19. Дайте характеристику популярным блочным шифрам.
20. Опишите историю шифров DES и 3DES и дайте им характеристику.
21. Опишите историю появления шифра AES и дайте ему характеристику.
22. Опишите режимы работы блочных шифров.
23. Опишите принцип работы криптографии с открытым ключом.
24. Опишите работу алгоритмов хэширования.
25. Охарактеризуйте математические проблемы на которых строится криптография с открытым ключом.
26. Опишите недостатки криптографии с открытым ключом.
27. Опишите принципы работы центров сертификации.
28. Опишите принципы работы пост-квантовой криптографии.
29. Дайте определение и характеристику стеганографии.
30. Опишите принципы работы вирусов и сетевых червей.
31. Опишите принципы работы троянских и шпионских программ.
32. Дайте характеристику riskware, adware.
33. Дайте характеристику rootkit.
34. Дайте характеристику хакеру и опишите появление термина.
35. Дайте характеристику фишеру и скрипт-кидди.
36. Дайте характеристику фрикеру и кардеру и опишите, чем они занимаются.
37. Дайте определение фишингу и приведите примеры.
38. Дайте определение понятию "ботнет" и опишите сценарий возникновения.
39. Дайте характеристику и опишите принципы работы антивирусных средств защиты.
40. Опишите работу сигнатурного анализа в антивирусах.
41. Опишите работу эвристического анализа в антивирусах.
42. Дайте характеристику и опишите принципы работы систем обнаружения вторжений.

43. Дайте характеристику и опишите принципы работы межсетевых экранов.
44. Дайте характеристику и опишите принципы работы систем предотвращения утечек.
45. Опишите современные средства защиты информации корпоративного уровня.