

**Перечень теоретических и практических заданий к экзамену
по ОП.16 Безопасность информационных систем
(3 курс, 5 семестр 2026-2027 уч. г.)**

Форма контроля: Письменный опрос (Опрос)

Описательная часть: По выбору выполнить 1 теоретическое задание и 1 практическое задание

Перечень теоретических заданий:

Задание №1

Дать определение:

1. "Информационной безопасности",
2. "Защита информации",
3. "Доступность",
4. "Целостность информации",
5. "Конфиденциальность информации".

Оценка	Показатели оценки
5	Дано определение пяти понятиям.
4	Дано определение четырем понятиям.
3	Дано определение трем понятиям.

Задание №2

1. Дать определение "угроза", "окно опасности". Дать классификацию угроз.
2. Дать определение "вредоносное ПО", привести пример.
3. Дать определение "Основные угрозы целостности", привести пример.
4. Дать определение "Угроза конфиденциальности", привести пример.

Оценка	Показатели оценки
5	Задание выполнено полностью.
4	Выполнено три пункта задания.
3	Выполнено два пункта задания.

Задание №3

1. Дать определение - вирус. Описать классификация вирусов и способы заражения.
2. Дать определение - антивирус. Описать основные классы антивирусных программ.
3. Написать средства анализа защищенности сетевых протоколов и ОС. Перечислить требования к антивирусам.

Оценка	Показатели оценки
5	Выполнено три пункта задания.
4	Выполнено два пункта задания.
3	Выполнен один пункт задания.

Задание №4

Создайте таблицу (не менее 5 видов угроз) с описанием различных видов угроз для информационных систем (вирусы, фишинг, атаки DDoS и т.д.) и приведите примеры реальных инцидентов, связанных с каждой из этих угроз.

Оценка	Показатели оценки
5	В таблице описано более 5 видов угроз с примерами.
4	В таблице описано 4 вида угроз с примерами.
3	В таблице описано 2 вида угроз с примерами.

Задание №5

1. Описать проблемы безопасности IP-сетей.
2. Описать угрозы и уязвимости проводных корпоративных сетей. Описать угрозы и уязвимости беспроводных сетей.
3. Пояснить и описать технологии межсетевых экранов. Перечислить показатели защищенности межсетевых экранов.

Оценка	Показатели оценки
5	Выполнено три пункта задания.
4	Выполнено два пункта задания.
3	Выполнен один пункт задания.

Задание №6

Дать определение:

1. "Информационной безопасности",
2. "Защита информации",

3. "Доступность",

4. "Целостность информации",

5. "Конфиденциальность информации".

Оценка	Показатели оценки
5	Дано определение пяти понятиям.
4	Дано определение четырем понятиям.
3	Дано определение трем понятиям.

Задание №7

Расписать виды угроз и атак, характерные для сферы электронной коммерции. (не менее 4)

Оценка	Показатели оценки
5	Задание выполнено полностью. Приведено не менее 4 угроз.
4	Задание выполнено с описанием 3 угроз.
3	Задание выполнено с описанием 2 угроз.

Задание №8

1. Дать определение "угроза", "окно опасности". Дать классификацию угроз.
2. Дать определение "вредоносное ПО", привести пример.
3. Дать определение "Основные угрозы целостности", привести пример.
4. Дать определение "Угроза конфиденциальности", привести пример.

Оценка	Показатели оценки
5	Задание выполнено полностью.
4	Выполнено три пункта задания.
3	Выполнено два пункта задания.

Задание №9

1. Описать проблемы безопасности IP-сетей.
2. Описать угрозы и уязвимости проводных корпоративных сетей. Описать угрозы и уязвимости беспроводных сетей.
3. Пояснить и описать технологии межсетевых экранов. Перечислить показатели защищенности межсетевых экранов.

Оценка	Показатели оценки
5	Выполнено три пункта задания.

4	Выполнено два пункта задания.
3	Выполнен один пункт задания.

Задание №10

1. Дать определение - вирус. Описать классификация вирусов и способы заражения.
2. Дать определение - антивирус. Описать основные классы антивирусных программ.
3. Написать средства анализа защищенности сетевых протоколов и ОС. Перечислить требования к антивирусам.

Оценка	Показатели оценки
5	Выполнено три пункта задания.
4	Выполнено два пункта задания.
3	Выполнен один пункт задания.

Задание №11

Составьте таблицу, в которой будут перечислены основные принципы безопасности информационных систем и даны краткие описания каждого из них.

Оценка	Показатели оценки
5	В таблице описаны 5 основных принципа, которым должна соответствовать информационная безопасность.
4	В таблице описаны 3 основных принципа, которым должна соответствовать информационная безопасность.
3	Втаблице описан один основной принцип или отсутствует характеристика основных принципов.

Задание №12

Перечислите пять видов угроз и атак на информационные системы, включая краткое описание каждой угрозы.

Оценка	Показатели оценки
5	Перечислены пять видов угроз и атак на информационные системы с кратким описание каждой угрозы.
4	Перечислены три вида угроз и атак на информационные системы с кратким описание каждой угрозы.
3	Представлен один из видов угроз и атак на информационные системы с кратким описание.

Задание №13

Необходимо рассказать о последствиях угроз для информационных систем и способах их предотвращения.

Оценка	Показатели оценки
5	Представлен анализ не менее 3 примеров угроз, их последствия с предложениями по их предотвращению.
4	Представлен анализ 2 примеров угроз, их последствия с предложениями по их предотвращению.
3	Представлен анализ 1 примера угроз, ее последствия с предложениями по их предотвращению.

Задание №14

Проанализируйте открытые источники информации и определите три наиболее актуальные угрозы для конкретной информационной системы (например, для системы электронной коммерции), включая краткое описание каждой угрозы.

Оценка	Показатели оценки
5	Проанализированы три актуальные угрозы с кратким описанием каждой угрозы.
4	Проанализированы две актуальные угрозы с кратким описанием каждой угрозы.
3	Проанализирована одна актуальная угроза с кратким описанием.

Задание №15

Перечислите пять основных принципов и концепций безопасности информационных систем, включая краткое описание каждого принципа.

Оценка	Показатели оценки
5	Перечислены пять принципов и концепций безопасности информационных систем с кратким описанием каждого принципа.
4	Перечислены три принципа и концепции безопасности информационных систем с кратким описанием каждого принципа.
3	Представлен один из принципов и концепций безопасности информационных систем с кратким описанием.

Задание №16

Перечислите пять видов угроз и атак на информационные системы, включая краткое описание каждой угрозы.

Оценка	Показатели оценки
--------	-------------------

5	Перечислены пять видов угроз и атак на информационные системы с кратким описанием каждой угрозы.
4	Перечислены три вида угроз и атак на информационные системы с кратким описанием каждой угрозы.
3	Представлен один из видов угроз и атак на информационные системы с кратким описанием.

Задание №17

1. Объясните концепцию доверенной третьей стороны и приведите пример ее применения в информационной безопасности.

Оценка	Показатели оценки
5	1. Концепция доверенной третьей стороны описана полностью и приведено 3 примера ее применения в информационной безопасности.
4	Концепция доверенной третьей стороны описана полностью и приведен пример ее применения в информационной безопасности.
3	Приведено описание концепции доверенной третьей стороны без примеров.

Задание №18

1. Дать определение авторское и патентное право.
2. Описать угрозы безопасности автоматизированных систем обработки данных (естественные угрозы, искусственные угрозы, непреднамеренные угрозы, преднамеренные угрозы)
3. Написать стандарты в области информационной безопасности автоматизированных систем обработки данных.

Оценка	Показатели оценки
5	Даны ответы на 3 вопроса.
4	Даны ответы на 2 вопроса.
3	Дан ответ на 1 вопрос.

Задание №19

1. Описать проблемы безопасности IP-сетей.
2. Описать угрозы и уязвимости проводных корпоративных сетей. Описать угрозы и уязвимости беспроводных сетей
3. Пояснить и описать технологии межсетевых экранов. Перечислить показатели защищенности межсетевых экранов.

Оценка	Показатели оценки
5	Даны ответы на 3 вопроса.
4	Даны ответы на 2 вопроса.
3	Дан ответ на 1 вопрос.

Задание №20

Используя "Доктрину информационной безопасности РФ" описать уровни информационной безопасности РФ, от национального до персонального.

Оценка	Показатели оценки
5	Описаны 4 уровня информационной безопасности.
4	Описаны 3 уровня информационной безопасности.
3	Описано 2 уровня информационной безопасности.

Задание №21

Объясните, как работает технология двухфакторной аутентификации, и приведите пример ее использования.

Оценка	Показатели оценки
5	Дано объяснение и приведено 3 примера.
4	Дано объяснение и приведено 2 примера.
3	Дано объяснение, без примеров.

Задание №22

Опишите основные принципы и концепции безопасности информационных систем. Включите в ответ следующие аспекты:

- Конфиденциальность, целостность и доступность информации.
- Принцип "наименьших привилегий".
- Многоуровневая защита.
- Управление доступом и аутентификация.

- Резервное копирование и восстановление данных.

Оценка	Показатели оценки
5	Подробно описаны 5 основных принципов и концепций безопасности информационных систем.
4	Описаны 3-4 основных принципа и концепции.
3	писаны 1-2 основных принципа и концепции.

Задание №23

1. Понятие конфиденциальной информации, классификация, степени конфиденциальности.
2. Описать жизненные циклы конфиденциальной информации.
3. Понятие "государственная тайна". Описать способы защиты государственной информации

Оценка	Показатели оценки
5	Даны ответы на 3 вопроса.
4	Даны ответы на 2 вопроса.
3	Дан ответ на 1 вопрос.

Задание №24

1. Дать определение "угроза", "окно опасности". Дать классификацию угроз.
2. Дать определение - "вредоносное ПО", привести пример.
3. "Основные угрозы целостности" - дать определение, привести пример. "Угроза конфиденциальности" - дать определение.

Оценка	Показатели оценки
5	Даны ответы на 3 вопроса.
4	Даны ответы на 2 вопроса.
3	Дан ответ на 1 вопрос.

Задание №25

1. Дать определение - "политика безопасности", "сетевая политика безопасности"
2. Перечислить классификация систем обнаружения атак
3. Описать компоненты и архитектура системы обнаружения атак.

Оценка	Показатели оценки
5	Даны ответы на 3 вопроса.
4	Даны ответы на 2 вопроса.
3	Дан ответ на 1 вопрос.

Перечень практических заданий:

Задание №1

1. Описать методы оценки уязвимости информации. Виды утечки информации.
2. Используя "Доктрину информационной безопасности РФ" описать уровни информационной безопасности РФ.
3. Дать определение : лицензия, лицензирующие органы (привести примеры), электронная цифровая подпись (открытая и закрытая).

Оценка	Показатели оценки
5	Задание выполнено полностью.
4	Выполнено 2 пункта задания.
3	Выполнен один пункт задания.

Задание №2

1. Понятие конфиденциальной информации, классификация, степени конфиденциальности.
2. Описать жизненные циклы конфиденциальной информации.
3. Понятие "государственная тайна". Описать способы защиты государственной информации.

Оценка	Показатели оценки
5	Выполнено три пункта задания.
4	Выполнено два пункта задания.
3	Выполнен один пункт задания.

Задание №3

1. Описать методы и системы защиты информации.
2. Написать виды доступа, уровни доступа. Дать определение - контроль доступа.
3. Описать основные методы и приемы защиты от несанкционированного доступа.

Оценка	Показатели оценки
3	Выполнен один пункт задания.
4	Выполнено два пункта задания.
5	Выполнено три пункта задания.

Задание №4

Разработайте систему контроля доступа для гипотетической компании, занимающейся разработкой программного обеспечения. Система должна включать в себя различные уровни доступа для сотрудников, клиентов и внешних подрядчиков, а также механизмы аутентификации и авторизации. Для каждого уровня доступа определите набор прав и возможностей, доступных

пользователю. Например, сотрудники отдела разработки могут иметь право на чтение и изменение исходного кода проектов, а клиенты — только на просмотр демонстраций продуктов.

Разработайте механизмы контроля доступа, которые будут проверять соответствие прав пользователя его текущему

уровню доступа. Опишите, как система будет реагировать на попытки несанкционированного доступа.

Представьте свою систему в виде диаграммы или схемы, отражающей уровни доступа, механизмы аутентификации и авторизации, а также принципы контроля доступа.

Оценка	Показатели оценки
5	Определены пять уровней доступа для сотрудников, клиентов и внешних подрядчиков, включая административный уровень и уровень аудита. Механизмы аутентификации и авторизации разработаны для каждого уровня доступа с учетом специфики выполняемых задач. Права и возможности для каждого уровня доступа четко определены, обоснованы и соответствуют должностным обязанностям. Принципы контроля доступа описаны подробно и включают меры реагирования на попытки несанкционированного доступа, а также механизмы аудита действий пользователей.
4	Определены четыре уровня доступа для сотрудников, клиентов и внешних подрядчиков, включая административный уровень. Для каждого уровня доступа разработаны подробные механизмы аутентификации и авторизации. Права и возможности для каждого уровня доступа четко определены и обоснованы. Принципы контроля доступа описаны подробно и включают меры реагирования на попытки несанкционированного доступа.
3	Определены три уровня доступа для сотрудников, клиентов и внешних подрядчиков. Описаны механизмы аутентификации и авторизации для каждого уровня доступа. Указаны права и возможности для каждого уровня доступа. Описаны принципы контроля доступа.

Задание №5

1. Дать определение - "политика безопасности", "сетевая политика безопасности".
2. Перечислить классификация систем обнаружения атак.
3. Описать компоненты и архитектура системы обнаружения атак.

Оценка	Показатели оценки
3	Выполнен один пункт задания.
4	Выполнено два пункта задания.
5	Выполнено три пункта задания.

Задание №6

1. Описать методы и системы защиты информации.
2. Написать виды доступа, уровни доступа. Дать определение - контроль доступа.
3. Описать основные методы и приемы защиты от несанкционированного доступа.

Оценка	Показатели оценки
3	Выполнен один пункт задания.
4	Выполнено два пункта задания.
5	Выполнено три пункта задания.

Задание №7

Разработайте систему контроля доступа для гипотетической компании, занимающейся разработкой программного обеспечения. Система должна включать в себя различные уровни доступа для сотрудников, клиентов и внешних подрядчиков, а также механизмы аутентификации и авторизации. Для каждого уровня доступа определите набор прав и возможностей, доступных пользователю. Например, сотрудники отдела разработки могут иметь право на чтение и изменение исходного кода проектов, а клиенты — только на просмотр демонстраций продуктов.

Разработайте механизмы контроля доступа, которые будут проверять соответствие прав пользователя его текущему

уровню доступа. Опишите, как система будет реагировать на попытки несанкционированного доступа.

Представьте свою систему в виде диаграммы или схемы, отражающей уровни доступа, механизмы аутентификации и авторизации, а также принципы контроля доступа.

Оценка	Показатели оценки
5	Определены пять уровней доступа для сотрудников, клиентов и внешних подрядчиков, включая административный уровень и уровень аудита. Механизмы аутентификации и авторизации разработаны для каждого уровня доступа с учетом специфики выполняемых задач. Права и возможности для каждого уровня доступа четко определены, обоснованы и соответствуют должностным обязанностям. Принципы контроля доступа описаны подробно и включают меры реагирования на попытки несанкционированного доступа, а также механизмы аудита действий пользователей.
4	Определены четыре уровня доступа для сотрудников, клиентов и внешних подрядчиков, включая административный уровень. Для каждого уровня доступа разработаны подробные механизмы аутентификации и авторизации. Права и возможности для каждого уровня доступа четко определены и обоснованы. Принципы контроля доступа описаны подробно и включают меры реагирования на попытки несанкционированного доступа.
3	Определены три уровня доступа для сотрудников, клиентов и внешних подрядчиков. Описаны механизмы аутентификации и авторизации для каждого уровня доступа. Указаны права и возможности для каждого уровня доступа. Описаны принципы контроля доступа.

Задание №8

1. Дать определение - "политика безопасности ", "сетевая политика безопасности ".
2. Перечислить классификация систем обнаружения атак.
3. Описать компоненты и архитектура системы обнаружения атак.

Оценка	Показатели оценки
3	Выполнен один пункт задания.
4	Выполнено два пункта задания.
5	Выполнено три пункта задания.

Задание №9

1. Понятие конфиденциальной информации, классификация, степени конфиденциальности.
2. Описать жизненные циклы конфиденциальной информации.
3. Понятие "государственная тайна". Описать способы защиты государственной информации.

Оценка	Показатели оценки
5	Выполнено три пункта задания.
4	Выполнено два пункта задания.
3	Выполнен один пункт задания.

Задание №10

1. Описать методы оценки уязвимости информации. Виды утечки информации.
2. Используя "Доктрину информационной безопасности РФ" описать уровни информационной безопасности РФ.
3. Дать определение : лицензия, лицензирующие органы (привести примеры), электронная цифровая подпись (открытая и закрытая).

Оценка	Показатели оценки
5	Задание выполнено полностью.
4	Выполнено 2 пункта задания.
3	Выполнен один пункт задания.

Задание №11

Подготовьте презентацию, в которой объясните взаимосвязь между принципами безопасности и их применением в реальных информационных системах.

Оценка	Показатели оценки

5	Представлена презентация с 5 примерами из реальной жизни, демонстрирующую взаимосвязь и практическое применение принципов безопасности.
4	Представлена презентация с 3 примерами из реальной жизни, демонстрирующую взаимосвязь и практическое применение принципов безопасности.
3	Представлена презентация с 2 примерами из реальной жизни, демонстрирующую взаимосвязь и практическое применение принципов безопасности.

Задание №12

Разработайте схему, которая наглядно показывает, как различные принципы безопасности взаимодействуют в контексте защиты корпоративных информационных систем.

Оценка	Показатели оценки
5	Представлена графическая схема, интегрирующая принципы безопасности в комплексную систему защиты, с подробными пояснениями.
4	Представлена графическая схема с незначительными ошибками, интегрирующая принципы безопасности в комплексную систему защиты, с подробными пояснениями.
3	Представлена графическая схема с грубыми ошибками, интегрирующая принципы безопасности в комплексную систему защиты, с подробными пояснениями.

Задание №13

Разработайте инфографику, которая наглядно покажет цепочку событий, начиная с возникновения угрозы и заканчивая ее воздействием на информационную систему.

Оценка	Показатели оценки
5	Предоставлена инфографика, визуализирующая цепочку событий, связанных с угрозами, и описаны комплексные меры защиты.
4	Предоставлена инфографика, визуализирующая цепочку событий, связанных с угрозами, и описаны комплексные меры защиты с незначительными ошибками.
3	Предоставлена инфографика, визуализирующая цепочку событий, связанных с угрозами, и описаны комплексные меры защиты с грубыми ошибками.

Задание №14

Разработайте стратегию безопасности для небольшой компании, включая основные цели, задачи и мероприятия по обеспечению безопасности.

Оценка	Показатели оценки
5	Разработана стратегия безопасности с основными целями, задачами и мероприятиями.

4	Разработана стратегия безопасности с основными целями и задачами, но без детальных мероприятий.
3	Сформулированы основные цели и задачи стратегии безопасности.

Задание №15

Выберите один из методов защиты информации (например, шифрование данных) и разработайте пошаговую инструкцию по его внедрению в информационной системе.

Оценка	Показатели оценки
5	Разработана пошаговая инструкция по внедрению метода защиты с детальными этапами.
4	Разработана пошаговая инструкция по внедрению метода защиты с основными этапами.
3	Представлены общие идеи по внедрению метода защиты.

Задание №16

Разработайте стратегию безопасности для небольшой компании, включая основные цели, задачи и мероприятия по обеспечению безопасности.

Оценка	Показатели оценки
5	Разработана стратегия безопасности с основными целями, задачами и мероприятиями.
4	Разработана стратегия безопасности с основными целями и задачами, но без детальных мероприятий.
3	Сформулированы основные цели и задачи стратегии безопасности.

Задание №17

Разработайте стратегию безопасности для компании, включая основные цели, задачи и мероприятия по обеспечению безопасности.

Оценка	Показатели оценки
5	Разработана стратегия безопасности с основными целями, задачами и мероприятиями.
4	Разработана стратегия безопасности с основными целями и задачами, но без детальных мероприятий.
3	Сформулированы основные цели и задачи стратегии безопасности.

Задание №18

1. Дать определение - вирус. Описать классификация вирусов и способы заражения.
2. Дать определение - антивирус. Описать основные классы антивирусных программ.
3. Написать средства анализа защищенности сетевых протоколов и ОС. Перечислить требования к антивирусам.

Оценка	Показатели оценки
5	Даны ответы на 3 вопроса.
4	Даны ответы на 2 вопроса.
3	Дан ответ на 1 вопрос.

Задание №19

1. Описать методы оценки уязвимости информации. Виды утечки информации.
2. Дать определение : лицензия, лицензирующие органы (привести примеры), электронная цифровая подпись(открытая и закрытая).

Оценка	Показатели оценки
5	Даны подробные ответы на 2 вопроса.
4	Ответы на вопросы даны с незначительными ошибками.
3	Ответ дан на 1 вопрос.

Задание №20

Проанализировать угрозы для системы электронной коммерции, такие как кража персональных данных клиентов, взлом платежных систем и мошенничество с использованием поддельных сайтов.

Оценка	Показатели оценки
5	Проанализированы 3 угрозы.
4	Проанализированы 2 угрозы.
3	Проанализирована 1 угроза.

Задание №21

Объяснить, как происходит атака «человек посередине» и какие меры можно предпринять для ее предотвращения.

Оценка	Показатели оценки

5	Приведено не менее 5 мер предотвращения атаки.
4	Приведено 3 меры предотвращения атаки.
3	Приведена 1 мера предотвращения атаки.

Задание №22

Проанализируйте угрозы и риски для информационной системы Вашей организации. Разработайте стратегию и план по обеспечению безопасности этой информационной системы.

Оценка	Показатели оценки
5	Выполнен всесторонний анализ угроз и рисков, разработана подробная стратегия и план по обеспечению безопасности информационной системы.
4	Выполнен анализ основных угроз и рисков, разработана общая стратегия и план по обеспечению безопасности информационной системы.
3	Выполнен поверхностный анализ угроз и рисков, разработаны общие рекомендации по обеспечению безопасности информационной системы.

Задание №23

Выберите реальную организацию и проведите SWOT-анализ (анализ сильных и слабых сторон, возможностей и угроз) ее информационной безопасности. Определите основные риски и предложите методы их минимизации.

Оценка	Показатели оценки
5	Задание выполнено полностью.
4	Задание выполнено с незначительными ошибками.
3	Задание выполнено с грубыми ошибками.

Задание №24

Разработайте стратегию безопасности для гипотетической компании, описывающую политику безопасности, процедуры реагирования на инциденты и план обучения сотрудников. Включите в стратегию как технические, так и организационные меры.

Оценка	Показатели оценки
5	Задание выполнено полностью.
4	Задание выполнено с незначительными ошибками.
3	Задание выполнено с грубыми ошибками.

Задание №25

Рассказать о принципах конфиденциальности, целостности и доступности (CIA) в контексте информационной безопасности. Приведите примеры, как каждое из этих понятий применяется на практике в современных информационных системах.

Оценка	Показатели оценки
5	Дано подробное описание о принципах конфиденциальности, целостности и доступности (CIA) в контексте информационной безопасности с примерами.
4	Дано подробное описание о принципах конфиденциальности, целостности и доступности (CIA) в контексте информационной безопасности.
3	Дано краткое описание о принципах конфиденциальности, целостности и доступности (CIA) в контексте информационной безопасности.