Министерство образования Иркутской области
Государственное бюджетное профессиональное образовательное учреждение Иркутской области
«Иркутский авиационный техникум»

УТВЕРЖДАЮ
Директор
ГБПОУИО «ИАТ»
_____ Якубовский А.Н.
«30» мая 2024 г.

# ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ПО ДИСЦИПЛИНЕ

ОП.16 Безопасность информационных систем

специальности

09.02.07 Информационные системы и программирование

Иркутск, 2024

Рассмотрена
цикловой комиссией
ИСП-ИС протокол № 11 от
22.05.2024 г.

| № | Разработчик ФИО |
|---|---|
| 1 | Огородникова Наталья Романовна |

# 1. ОБЩИЕ ПОЛОЖЕНИЯ

## 1.1. Область применения фонда оценочных средств (ФОС)

ФОС по дисциплине является частью программы подготовки специалистов среднего звена по специальности 09.02.07 Информационные системы и программирование

## 1.2. Место дисциплины в структуре ППССЗ:

ОП.00 Общепрофессиональный цикл.

## 1.3. Цели и задачи дисциплины – требования к результатам освоения дисциплины

| Результаты освоения дисциплины | № результата | Формируемый результат |
|---|---|---|
| Знать | 1.1 | основные принципы и концепции безопасности информационных систем |
| | 1.2 | различные виды угроз и атак на информационные системы |
| | 1.3 | методы и средства защиты информации |
| Уметь | 2.1 | анализировать угрозы и риски для информационных систем |
| | 2.2 | разрабатывать стратегии и планы по обеспечению безопасности информационных систем |
| | 2.3 | применять методы и средства защиты информации в информационных системах |
| Личностные результаты реализации программы воспитания | 4.1 | Ориентированный на профессиональные достижения, деятельно выражающий познавательные интересы с учетом своих способностей, образовательного и профессионального маршрута, выбранной квалификации |
| | 4.2 | Демонстрирующий умение эффективно взаимодействовать в команде, вести диалог, в том числе с использованием средств коммуникации |
| | 4.3 | Демонстрирующий навыки анализа и интерпретации информации из различных источников с учетом нормативно-правовых норм |

| | | |
|---|---|---|
| | 4.4 | Демонстрирующий готовность и способность к образованию, в том числе самообразованию, на протяжении всей жизни; сознательное отношение к непрерывному образованию как условию успешной профессиональной и общественной деятельности |

**1.4. Формируемые компетенции:**

ОК.1 Выбирать способы решения задач профессиональной деятельности применительно к различным контекстам
ОК.2 Использовать современные средства поиска, анализа и интерпретации информации, и информационные технологии для выполнения задач профессиональной деятельности
ОК.3 Планировать и реализовывать собственное профессиональное и личностное развитие, предпринимательскую деятельность в профессиональной сфере, использовать знания по правовой и финансовой грамотности в различных жизненных ситуациях
ОК.4 Эффективно взаимодействовать и работать в коллективе и команде
ОК.5 Осуществлять устную и письменную коммуникацию на государственном языке Российской Федерации с учетом особенностей социального и культурного контекста
ОК.9 Пользоваться профессиональной документацией на государственном и иностранном языках
ПК.5.3 Разрабатывать подсистемы безопасности информационной системы в соответствии с техническим заданием
ПК.7.5 Проводить аудит систем безопасности баз данных и серверов с использованием регламентов по защите информации

## 2. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДИСЦИПЛИНЫ, ИСПОЛЬЗУЕМЫЙ ДЛЯ ТЕКУЩЕГО КОНТРОЛЯ

### 2.1 Текущий контроль (ТК) № 1 (45 минут)

**Тема занятия:** 1.2.5.Анализ Доктрины информационной безопасности Российской Федерации.

**Метод и форма контроля:** Письменный опрос (Опрос)

**Вид контроля:** Проверочная работа

**Дидактическая единица:** 1.1 основные принципы и концепции безопасности информационных систем

**Занятие(-я):**

1.1.1.Основные понятия информационной безопасности.

1.1.2.Анализ угроз информационной безопасности.

1.2.2.Сущность и понятие информационной безопасности. Принципы обеспечения информационной безопасности.

1.2.4.Доктрина информационной безопасности Российской Федерации.

**Задание №1 (19 минут)**

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. |

**Дидактическая единица:** 2.2 разрабатывать стратегии и планы по обеспечению безопасности информационных систем

**Занятие(-я):**

1.2.1.Информационная безопасность в системе национальной безопасности Российской Федерации.

1.2.2.Сущность и понятие информационной безопасности. Принципы обеспечения информационной безопасности.

1.2.3.Основные положения государственной информационной политики России.

1.2.4.Доктрина информационной безопасности Российской Федерации.

**Задание №1 (26 минут)**

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. |

### 2.2 Текущий контроль (ТК) № 2 (45 минут)

**Тема занятия:** 3.1.4.Методы и системы защиты информации. Виды доступа. Уровни доступа. Контроль доступа.
**Метод и форма контроля:** Письменный опрос (Опрос)
**Вид контроля:** Проверочная работа
**Дидактическая единица:** 1.1 основные принципы и концепции безопасности информационных систем
**Занятие(-я):**

**Задание №1 (20 минут)**

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. |

**Дидактическая единица:** 2.3 применять методы и средства защиты информации в информационных системах
**Занятие(-я):**
1.2.3.Основные положения государственной информационной политики России.
1.2.4.Доктрина информационной безопасности Российской Федерации.
1.2.5.Анализ Доктрины информационной безопасности Российской Федерации.

1.3.2.Методы оценки уязвимости информации. Виды утечки информации.
2.1.3.Жизненные циклы конфиденциальной информации.
2.1.5.Защита информации, охраняемая авторским и патентным правом.
2.1.6.Анализ защищенности объекта защиты информации.
3.1.1.Интегральная безопасность. Угрозы безопасности автоматизированных систем обработки данных ( АСОД ).
3.1.2.Стандарты в области информационной безопасности АСОД.
3.1.3.Показатели защищенности СВТ. Защита информации в АСОД.

**Задание №1 (25 минут)**

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. |

### 2.3 Текущий контроль (ТК) № 3 (45 минут)

**Тема занятия:** 3.1.8.Средства и способы обеспечения информационной безопасности.
**Метод и форма контроля:** Письменный опрос (Опрос)
**Вид контроля:** Проверочная работа
**Дидактическая единица:** 1.3 методы и средства защиты информации
**Занятие(-я):**
1.2.3.Основные положения государственной информационной политики России.
1.2.4.Доктрина информационной безопасности Российской Федерации.
1.2.5.Анализ Доктрины информационной безопасности Российской Федерации.
1.3.1.Понятие угрозы безопасности информации. Системная классификация угроз безопасности информации.
1.3.2.Методы оценки уязвимости информации. Виды утечки информации.
2.1.1.Понятие конфиденциальной информации.
2.1.2.Классификация конфиденциальной информации по видам тайны и степени конфиденциальности.
3.1.5.Автоматизированная система, как объект информационной защиты.

**Задание №1 (19 минут)**

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. |

**Дидактическая единица:** 2.1 анализировать угрозы и риски для информационных систем

**Занятие(-я):**

1.1.1.Основные понятия информационной безопасности.
1.1.2.Анализ угроз информационной безопасности.
1.2.1.Информационная безопасность в системе национальной безопасности Российской Федерации.
1.2.3.Основные положения государственной информационной политики России.
1.2.4.Доктрина информационной безопасности Российской Федерации.
1.2.5.Анализ Доктрины информационной безопасности Российской Федерации.
1.3.1.Понятие угрозы безопасности информации. Системная классификация угроз безопасности информации.
1.3.2.Методы оценки уязвимости информации. Виды утечки информации.
2.1.1.Понятие конфиденциальной информации.
2.1.2.Классификация конфиденциальной информации по видам тайны и степени конфиденциальности.

**Задание №1 (26 минут)**

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. |

### 2.4 Текущий контроль (ТК) № 4 (45 минут)

**Тема занятия:** 3.3.3.Методы анализа сетевой информации.
**Метод и форма контроля:** Лабораторная работа (Опрос)
**Вид контроля:**
**Дидактическая единица:** 1.2 различные виды угроз и атак на информационные системы
**Занятие(-я):**
3.1.4.Методы и системы защиты информации. Виды доступа. Уровни доступа. Контроль доступа.
**Задание №1 (15 минут)**
Расписать виды угроз и атак, характерные для сферы электронной коммерции. Меры предотвращения угроз и атак, такие как
использование антивирусного ПО, шифрование данных, контроль доступа. Меры реагирования на инциденты
информационной безопасности, такие как обнаружение и блокировка атак, восстановление системы после атак.

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

**Дидактическая единица:** 2.2 разрабатывать стратегии и планы по обеспечению безопасности информационных систем
**Занятие(-я):**
1.2.5.Анализ Доктрины информационной безопасности Российской Федерации.
2.1.1.Понятие конфиденциальной информации.
2.1.2.Классификация конфиденциальной информации по видам тайны и степени конфиденциальности.
2.1.4.Защита информации составляющей государственную тайну.
**Задание №1 (30 минут)**
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. |

### 2.5 Текущий контроль (ТК) № 5 (45 минут)

**Тема занятия:** 3.3.10.Анализ защищенности объекта защиты информации.
**Метод и форма контроля:** Письменный опрос (Опрос)
**Вид контроля:** Проверочная работа
**Дидактическая единица:** 1.1 основные принципы и концепции безопасности

информационных систем
**Занятие(-я):**

**Задание №1 (20 минут)**

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. |

**Дидактическая единица:** 2.3 применять методы и средства защиты информации в информационных системах
**Занятие(-я):**
3.1.4.Методы и системы защиты информации. Виды доступа. Уровни доступа. Контроль доступа.
3.1.5.Автоматизированная система, как объект информационной защиты.
3.1.6.Основные методы и приемы защиты от несанкционированного доступа.
3.1.7.Методы и средства защиты информации.
3.2.1.Проблема вирусного заражения программ. Классификация вирусов. Способы заражения программ.
3.2.2.Структура современных вирусных программ. Перспективные методы антивирусной защиты. Основные классы антивирусных программ.
3.3.1.Адаптивное управление безопасностью.
3.3.2.Средства анализа защищенности сетевых протоколов. Средства анализа защищенности операционной системы. Общие требования к выбираемым средствам анализа защищенности.
3.3.3.Методы анализа сетевой информации.
3.3.4.Проблемы безопасности IP-сетей. Угрозы и уязвимости проводных корпоративных сетей. Угрозы и уязвимости беспроводных сетей.
3.3.5.Основы сетевого и межсетевого взаимодействия.
3.3.6.Технологии межсетевых экранов. Требования и показатели защищенности межсетевых экранов. Схемы сетевой защиты на базе межсетевых экранов.
3.3.8.Классификация систем обнаружения атак. Компоненты и архитектура

системы обнаружения атак. Особенности обнаружения атак на сетевом и операционном уровне. Реагирование на атаку.

3.3.9.Обзор современных средств обнаружения атак.

**Задание №1 (25 минут)**

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. |

## 3. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДИСЦИПЛИНЫ, ИСПОЛЬЗУЕМЫЙ ДЛЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

| № семестра | Вид промежуточной аттестации |
|---|---|
| 5 | Экзамен |

| Экзамен может быть выставлен автоматически по результатам текущих контролей |
|---|
| Текущий контроль №1 |
| Текущий контроль №2 |
| Текущий контроль №3 |
| Текущий контроль №4 |
| Текущий контроль №5 |

**Метод и форма контроля:** Письменный опрос (Опрос)
**Вид контроля:** По выбору выполнить 1 теоретическое задание и 1 практическое задание
**Дидактическая единица для контроля:**
1.1 основные принципы и концепции безопасности информационных систем
**Задание №1 (из текущего контроля) (19 минут)**
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 (из текущего контроля) (20 минут)**

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 (из текущего контроля) (20 минут)**

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 №4 (16 минут)**
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 №5 (20 минут)**
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 №6 (20 минут)**

1. Дать определение авторское и потентное 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 №7 (20 минут)**

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 №8 (15 минут)**
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. |

**Дидактическая единица для контроля:**
2.2 разрабатывать стратегии и планы по обеспечению безопасности информационных систем
**Задание №1 (из текущего контроля) (26 минут)**

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 (из текущего контроля) (30 минут)**
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 №3 (29 минут)**
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 №4 (30 минут)**
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 №5 (30 минут)**
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 №6 (25 минут)**
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 №7 (25 минут)**
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 №8 (30 минут)**
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 №9 (30 минут)**
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 №10 (30 минут)**
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. |

**Дидактическая единица для контроля:**
2.3 применять методы и средства защиты информации в информационных системах
**Задание №1 (из текущего контроля) (25 минут)**

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 №2 (из текущего контроля) (25 минут)**

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 №3 (25 минут)**
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 №4 (30 минут)**
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. |

**Дидактическая единица для контроля:**
1.3 методы и средства защиты информации
**Задание №1 (из текущего контроля) (19 минут)**

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 №2 (15 минут)**
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 №3 (15 минут)**

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 №4 (15 минут)**
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 №5 (15 минут)**
Объясните, как работает технология двухфакторной аутентификации, и приведите пример ее использования.

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

**Задание №6 (15 минут)**

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 №7 (15 минут)**

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. |

**Дидактическая единица для контроля:**

2.1 анализировать угрозы и риски для информационных систем

**Задание №1 (из текущего контроля) (26 минут)**

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 №2 (25 минут)**

1. Дать определение - вирус. Описать классификация вирусов и способы заражения.
2. Дать определение - анитивирус. 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 №3 (25 минут)**

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 №4 (30 минут)**
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 №5 (30 минут)**
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 №6 (30 минут)**
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. |

**Дидактическая единица для контроля:**
1.2 различные виды угроз и атак на информационные системы
**Задание №1 (15 минут)**
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 №2 (15 минут)**
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 №3 (15 минут)**
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 №4 (20 минут)**
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 №5 (15 минут)**
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 №6 (15 минут)**

1. Дать определение "угроза", "окно опасности". Дать классификацию угроз.
2. Дать определение - "вредоностное 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. |