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

УТВЕРЖДАЮ
Директор
ГБПОУИО «ИАТ»
_____ Якубовский А.Н.
«30» мая 2025 г.

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ПО ДИСЦИПЛИНЕ

ОП.16 Безопасность информационных систем

специальности

09.02.07 Информационные системы и программирование

Иркутск, 2025

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

№	Разработчик ФИО
1	Бодоев Даниил Александрович

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
	1.4	нормативно-правовая база в области информационной безопасности
	1.5	технологии мониторинга и аудита безопасности
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, средства защиты информации и нормативные документы при проектировании и обеспечении безопасности информационных систем
	2.4	проводить аудит систем безопасности баз данных и серверов
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
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 (30 минут)

Тема занятия: 1.2.3.Вредоносное программное обеспечение
Метод и форма контроля: Письменный опрос (Опрос)
Вид контроля: Письменная работа
Дидактическая единица: 1.1 основные принципы и концепции безопасности информационных систем
Занятие(-я):
1.1.1.Основные понятия информационной безопасности.
1.1.2.Классификация объектов защиты
Задание №1 (15 минут)
Дать определение:
1. "Информационной безопасности",
2. "Защита информации",
3. "Доступность",
4. "Целостность информации",
5. "Конфиденциальность информации"

Оценка	*Показатели оценки*
5	Студент дал полное, точное определение, раскрыл ключевые характеристики понятия, не допустил ошибок.
4	Студент дал в целом верное определение, но допустил незначительную неточность или упустил 1–2 ключевых элемента.
3	Студент дал частично верное определение, допустил существенные пробелы.

Дидактическая единица: 2.1 анализировать угрозы и риски для информационных систем
Занятие(-я):
1.1.2.Классификация объектов защиты
Задание №1 (15 минут)
Выберите один верный вариант ответа. По 1 баллу за каждый вопрос.

1. Какой из видов вредоносного ПО предназначен для скрытого сбора информации?

    - а) Червь

- б) Троян
- в) Руткит
- г) Spyware

2. Как распространяется компьютерный червь?
   - а) Через загрузку зараженных файлов
   - б) Самостоятельно через сеть
   - в) Через фишинговые письма
   - г) Через USB-устройства
3. Что из перечисленного является целью вируса-вымогателя?
   - а) Удаление системных файлов
   - б) Блокировка системы с требованием выкупа
   - в) Шпионаж
   - г) Маскировка действий других программ
4. Какой вид атаки использует доверие к известному пользователю?
   - а) DDoS
   - б) SQL-инъекция
   - в) Социальная инженерия
   - г) Фишинг
5. Что из перечисленного не является вредоносным ПО?
   - а) Spyware
   - б) Adware

- в) Брандмауэр
- г) Троян

6. Что такое backdoor?
   - а) Защитный модуль
   - б) Программа удаленного администрирования
   - в) Скрытый доступ к системе
   - г) Вирус-шифровальщик
7. Какой тип вредоносного ПО может внедряться в загрузочный сектор жесткого диска?
   - а) Червь
   - б) Bootkit
   - в) Руткит
   - г) Троян
8. Что помогает обнаружить вирусы до их запуска?
   - а) Резервное копирование
   - б) Брандмауэр
   - в) Антивирус с эвристическим анализом
   - г) Шифрование данных
9. Почему руткиты сложно обнаружить?
   - а) Они не активируются
   - б) Используют цифровую подпись

- в) Встраиваются на уровне ядра ОС
- г) Не требуют интернета

10. Какой из методов наиболее эффективен для защиты от вредоносного ПО?
    - а) Частая переустановка ОС
    - б) Использование только лицензионного ПО и антивируса
    - в) Отключение всех сетевых соединений
    - г) Установка большого количества программ

Оценка	*Показатели оценки*
5	9–10 правильных ответов.
4	7–8 правильных ответов.
3	5–6 правильных ответов.

2.2 Текущий контроль (ТК) № 2 (30 минут)

Тема занятия: 2.1.4.Ответственность за нарушения в сфере информационной безопасности
Метод и форма контроля: Практическая работа (Опрос)
Вид контроля: Письменная работа
Дидактическая единица: 1.4 нормативно-правовая база в области информационной безопасности
Занятие(-я):
2.1.1.152-ФЗ "О персональных данных", ГОСТ Р 57580
2.1.3.Ответственность за нарушения в сфере информационной безопасности
Задание №1 (15 минут)

Ответить на вопросы:

1. Раскройте основные положения Федерального закона №152-ФЗ «О персональных данных».
2. Что такое ГОСТ Р 57580? Назовите его ключевые принципы и область

применения.

3. Перечислите виды ответственности (уголовная, административная, дисциплинарная) за нарушения законодательства в области информационной безопасности.

4. Приведите примеры нарушений и соответствующих санкций, предусмотренных законодательством РФ.

5. Объясните, какие действия должен предпринять оператор персональных данных в случае утечки информации.

Оценка	***Показатели оценки***
5	Полно и правильно раскрыты все теоретические вопросы.
4	В основном раскрыты теоретические вопросы, допущены незначительные неточности.
3	Ответы на теоретические вопросы фрагментарные, с существенными упущениями или ошибками.

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

Занятие(-я):

1.2.1.Классификация угроз (физические, программные, сетевые)

1.2.2.Вредоносное программное обеспечение

1.3.1.Основные стратегии защиты данных

Задание №1 (15 минут)

1. Приведите примеры физических, программных и сетевых угроз информационной безопасности.

2.Кратко охарактеризуйте наиболее распространенные типы вредоносного ПО.

3. Назовите и опишите основные стратегии защиты данных в информационных системах.

4. Предложите план мероприятий по обеспечению ИБ для организации с учетом классификации угроз.

5. Составьте пример простой стратегии защиты персональных данных в локальной ИС образовательного учреждения.

Оценка	***Показатели оценки***

5	Полно и правильно раскрыты все теоретические вопросы.
4	В основном раскрыты теоретические вопросы, допущены незначительные неточности.
3	Ответы на теоретические вопросы фрагментарные, с существенными упущениями или ошибками.

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

Тема занятия: 3.3.1.Защита на уровне ОС, сетевые экраны, антивирусное ПО
Метод и форма контроля: Практическая работа (Опрос)
Вид контроля: Практическая работа с применением ИКТ
Дидактическая единица: 1.3 методы и средства защиты информации
Занятие(-я):
1.3.1.Основные стратегии защиты данных
3.1.1.Шифрование (AES, RSA)
3.1.2.Шифрование (цифровые подписи)
3.1.3.Генерация ключей, шифрование сообщений в OpenSSL
3.2.1.Настройка межсетевого экрана
3.2.2.Анализ логов антивирусного ПО

Задание №1 (15 минут)

Задание 1. Генерация ключей и шифрование в OpenSSL

- Сгенерируйте пару ключей RSA (2048 бит).
- Зашифруйте и расшифруйте произвольное текстовое сообщение.
- Сохраните команды, вывод и краткие пояснения в виде отчета.

Оценка	*Показатели оценки*
5	Все задания выполнены полностью и правильно.
4	Большинство заданий выполнено верно; имеются незначительные ошибки или недочеты в пояснениях или оформлении.
3	Задания выполнены частично или с ошибками.

Задание №2 (15 минут)

Задание 2. Настройка межсетевого экрана Windows

- Настройте правило, запрещающее входящие подключения для произвольной программы.
- Настройте правило, разрешающее исходящие подключения к порту 443 (HTTPS).
- Зафиксируйте действия и результаты в виде пошаговой инструкции с пояснениями.

Оценка	***Показатели оценки***
5	Все задания выполнены полностью и правильно.
4	Большинство заданий выполнено верно; имеются незначительные ошибки или недочеты в пояснениях или оформлении.
3	Задания выполнены частично или с ошибками.

Дидактическая единица: 2.3 применять методы, средства защиты информации и нормативные документы при проектировании и обеспечении безопасности информационных систем
Занятие(-я):
2.1.2.Основные положения, стратегия РФ в сфере информационной безопасности
2.1.4.Ответственность за нарушения в сфере информационной безопасности
3.1.1.Шифрование (AES, RSA)
3.1.2.Шифрование (цифровые подписи)
3.1.3.Генерация ключей, шифрование сообщений в OpenSSL
Задание №1 (15 минут)
Задание 3. Анализ логов антивирусного ПО

- Найдите и откройте журнал защиты (например, Защитника Windows).
- Проанализируйте последние 5 событий: какие угрозы найдены, какие действия предприняты.

- Сделайте вывод: какие типы угроз наиболее часто встречаются, насколько эффективна защита.

Оценка	*Показатели оценки*
5	Все задания выполнены полностью и правильно.
4	Большинство заданий выполнено верно; имеются незначительные ошибки или недочеты в пояснениях или оформлении.
3	Задания выполнены частично или с ошибками.

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

Тема занятия: 3.5.1.SIEM-системы и анализ логов
Метод и форма контроля: Практическая работа (Опрос)
Вид контроля: Практическая работа с применением ИКТ
Дидактическая единица: 1.2 различные виды угроз и атак на информационные системы
Занятие(-я):
1.2.1.Классификация угроз (физические, программные, сетевые)
1.2.2.Вредоносное программное обеспечение
1.3.2.Аппаратные и программные средства защиты
Задание №1 (15 минут)
Просканируйте IP виртуальной машины.
Выполните синтаксис: nmap -sS -sV -O <IP>.
Сохраните результат в файл и расшифруйте его.

Оценка	*Показатели оценки*
5	Полно и точно объясняет виды угроз и методы защиты ИС.
4	Студент обладает хорошими знаниями, но допускает отдельные неточности.
3	Студент показывает минимально достаточный уровень.

Дидактическая единица: 2.4 проводить аудит систем безопасности баз данных и серверов
Занятие(-я):
3.2.1.Настройка межсетевого экрана
3.3.2.Инструменты аудита (metasploit)

3.3.3.Инструменты аудита (Nmap)
3.3.4.Проведение тестирования безопасности системы (metasploit)
3.3.5.Проведение тестирования безопасности системы (Nmap)
3.4.1.Анализ сетевого трафика
3.4.2.Анализ журналов событий
3.4.3.Анализ логов в Splunk
3.4.4.Анализ логов Fluentd

Задание №1 (15 минут)

- Найдите аномалии (много запросов с одного IP, ошибки авторизации и т.д.).
- Представьте краткий отчет в виде диаграммы или таблицы (можно в Excel/Word).

Оценка	***Показатели оценки***
5	Полно и точно объясняет виды угроз и методы защиты ИС.
4	Студент обладает хорошими знаниями, но допускает отдельные неточности.
3	Студент показывает минимально достаточный уровень.

Задание №2 (15 минут)

- Заблокируйте доступ определенной программы к интернету.
- Разрешите доступ к порту 3389 (RDP) только по локальной сети.
- Сделайте скриншоты до/после и прокомментируйте изменения.

Оценка	***Показатели оценки***
5	Полно и точно объясняет виды угроз и методы защиты ИС.

4	Студент обладает хорошими знаниями, но допускает отдельные неточности.
3	Студент показывает минимально достаточный уровень.

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

Тема занятия: 3.7.1.Защита серверов и баз данных
Метод и форма контроля: Практическая работа (Опрос)
Вид контроля: Практическое задание
Дидактическая единица: 1.5 технологии мониторинга и аудита безопасности
Занятие(-я):
3.3.2.Инструменты аудита (metasploit)
3.3.3.Инструменты аудита (Nmap)
3.3.4.Проведение тестирования безопасности системы (metasploit)
3.3.5.Проведение тестирования безопасности системы (Nmap)
3.4.3.Анализ логов в Splunk
3.5.1.SIEM-системы и анализ логов
3.5.2.SQL-инъекции
3.5.3.Управления доступом к ресурсам (RBAC)
3.5.4.Выполнение SQL-инъекций
3.5.5.Управление доступом на основе ролей (RBAC)
3.6.1.Настройка Firewall, защита от DDos
3.6.2.Настройка Firewall
3.6.3.Настройка Защиты от DDos
Задание №1 (15 минут)

- Запустите Nmap для сканирования открытых портов и служб тестовой системы.
- Проанализируйте полученные результаты и определите потенциальные уязвимости.
- Опишите, какие порты и сервисы являются потенциальной угрозой для безопасности.
- Предложите методы устранения или минимизации риска этих угроз.

Оценка	*Показатели оценки*
5	Работа выполнена полностью.
4	Основные понятия раскрыты, но есть незначительные упущения.
3	Выполнено минимум 50% практики.

Дидактическая единица: 2.4 проводить аудит систем безопасности баз данных и серверов

Занятие(-я):

3.5.1.SIEM-системы и анализ логов
3.5.2.SQL-инъекции
3.5.3.Управления доступом к ресурсам (RBAC)
3.5.4.Выполнение SQL-инъекций
3.5.5.Управление доступом на основе ролей (RBAC)
3.6.1.Настройка Firewall, защита от DDos
3.6.2.Настройка Firewall
3.6.3.Настройка Защиты от DDos

Задание №1 (15 минут)

- Откройте тестовый веб-сайт (с возможной SQL-инъекцией).
- Используя методы SQL-инъекций, получите несанкционированный доступ к базе данных.
- Задокументируйте полученные результаты: какие данные были извлечены или изменены.
- Объясните, как можно предотвратить SQL-инъекции на веб-сайте.

Оценка	*Показатели оценки*
5	Работа выполнена полностью.
4	Основные понятия раскрыты, но есть незначительные упущения.
3	Выполнено минимум 50% практики.

Задание №2 (15 минут)

- Установите и настройте систему RBAC на тестовом сервере.
- Создайте несколько ролей с разными уровнями доступа (например, администратор, менеджер, пользователь).
- Протестируйте, как разные роли могут управлять доступом к различным ресурсам на сервере.
- Зафиксируйте результаты тестирования и предложите улучшения безопасности.

Оценка	***Показатели оценки***
5	Работа выполнена полностью.
4	Основные понятия раскрыты, но есть незначительные упущения.
3	Выполнено минимум 50% практики.

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:
1.2 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)

Дать определение "угроза", "окно опасности". Дать классификацию угроз.
Дать определение - "вредоностное ПО", привести пример.
"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 №7 (15 минут)

1. Опишите цепочку кибератаки по модели Kill Chain.
2. Какие TTPs использует APT-группировка?
3. Как обнаружить признаки lateral movement?

Оценка	***Показатели оценки***
5	Выполнен подробный анализ с примерами.
4	Даны ответы на 2 вопроса.
3	Дано общее описание.

Дидактическая единица для контроля:
2.4 проводить аудит систем безопасности баз данных и серверов
Задание №1 (из текущего контроля) (15 минут)

- Откройте тестовый веб-сайт (с возможной SQL-инъекцией).
- Используя методы SQL-инъекций, получите несанкционированный доступ к базе данных.

- Задокументируйте полученные результаты: какие данные были извлечены или изменены.

- Объясните, как можно предотвратить SQL-инъекции на веб-сайте.

Оценка	***Показатели оценки***
5	Работа выполнена полностью.
4	Основные понятия раскрыты, но есть незначительные упущения.
3	Выполнено минимум 50% практики.

Задание №2 (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 №3 (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.

Задание №4 (30 минут)
На основе предоставленных логов:

1. Выявите 3 индикатора компрометации.

2. Определите тип атаки.

3. Составьте рекомендации по устранению уязвимостей.

Оценка	***Показатели оценки***
5	Полный анализ с конкретными рекомендациями.
4	Выявлены не все угрозы.
3	Поверхностный анализ.

Задание №5 (из текущего контроля) (15 минут)

- Заблокируйте доступ определенной программы к интернету.
- Разрешите доступ к порту 3389 (RDP) только по локальной сети.
- Сделайте скриншоты до/после и прокомментируйте изменения.

Оценка	***Показатели оценки***
5	Полно и точно объясняет виды угроз и методы защиты ИС.
4	Студент обладает хорошими знаниями, но допускает отдельные неточности.
3	Студент показывает минимально достаточный уровень.

Задание №6 (30 минут)
На основе логов Windows Server:

1. Выявите подозрительные действия (например, множественные failed logins).

2. Определите, возможна ли атака Pass-the-Hash.

3. Предложите меры по усилению безопасности.

Оценка	*Показатели оценки*
5	Полный анализ с рекомендациями.
4	Выявлены не все угрозы.
3	Ответ содержит общие выводы.

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

Задание №1 (из текущего контроля) (15 минут)

1. Приведите примеры физических, программных и сетевых угроз информационной безопасности.
2.Кратко охарактеризуйте наиболее распространенные типы вредоносного ПО.
3. Назовите и опишите основные стратегии защиты данных в информационных системах.
4. Предложите план мероприятий по обеспечению ИБ для организации с учетом классификации угроз.
5. Составьте пример простой стратегии защиты персональных данных в локальной ИС образовательного учреждения.

Оценка	*Показатели оценки*
5	Полно и правильно раскрыты все теоретические вопросы.
4	В основном раскрыты теоретические вопросы, допущены незначительные неточности.
3	Ответы на теоретические вопросы фрагментарные, с существенными упущениями или ошибками.

Задание №2 (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 №3 (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 №4 (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 №5 (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 №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 (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 №8 (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 №9 (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.

Задание №10 (30 минут)
Для удаленных сотрудников компании:

1. Перечислите риски (например, утечка через домашний Wi-Fi).

2. Разработайте политику безопасности (VPN, 2FA, запрет личных устройств).

Оценка	*Показатели оценки*
5	Имеется политика с техническими и организационными мерами.
4	Предоставлены только технические меры.
3	Даны общие рекомендации.

Дидактическая единица для контроля:

1.1 основные принципы и концепции безопасности информационных систем

Задание №1 (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	В таблице описан один основной принцип или отсутствует характеристика основных принципов.

Задание №2 (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 №3 (20 минут)

Дать определение авторское и патентное право.

Описать угрозы безопасности автоматизированных систем обработки данных

(естественные угрозы, искусственные угрозы, непреднамеренные угрозы, преднамеренные угрозы).
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 №4 (20 минут)
Описать проблемы безопасности IP-сетей.
Описать угрозы и уязвимости проводных корпоративных сетей.
Описать угрозы и уязвимости беспроводных сетей.
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 №5 (15 минут)
Опишите основные принципы и концепции безопасности информационных систем. Включите в ответ следующие аспекты:

1. Конфиденциальность, целостность и доступность информации.
2. Принцип "наименьших привилегий".
3. Многоуровневая защита.
4. Управление доступом и аутентификация.
5. 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 №6 (15 минут)
Объясните на примерах:

1. Принцип минимальных привилегий.
2. "Глубину защиты" (Defense in Depth).
3. Как эти принципы применяются в облачных сервисах?

Оценка	***Показатели оценки***
5	Предоставлены примеры для всех пунктов.
4	Ответ без облачного контекста.
3	Ответ содержит только определения.

Дидактическая единица для контроля:
1.3 методы и средства защиты информации
Задание №1 (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 №2 (15 минут)
Объясните концепцию доверенной третьей стороны и приведите пример ее применения в информационной безопасности.

Оценка	***Показатели оценки***

5	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 №3 (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 №4 (15 минут)
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 №5 (15 минут)
Понятие конфиденциальной информации, классификация, степени конфиденциальности.
Описать жизненные циклы конфиденциальной информации.
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 №6 (15 минут)

Дать определение - "политика безопасности ","сетевая политика безопасности ".
Перечислить классификация систем обнаружения атак.
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.

Задание №7 (15 минут)

1. Сравните механизмы HSM и TPM.
2. Объясните принцип работы технологии "песочницы".
3. Когда применяется аппаратное шифрование?

Оценка	***Показатели оценки***
5	Даны технически грамотные ответы на 3 вопроса.
4	Даны ответы на 2 вопроса.
3	Даны общие формулировки.

Задание №8 (15 минут)
Сравните:

1. HSM vs TPM (назначение, применение).

2. Аппаратное vs программное шифрование.

3. Когда используется квантовая криптография?

Оценка	*Показатели оценки*
5	Сравнение с примерами использования.
4	Решение без примеров.
3	Ответ содержит только определения.

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

Задание №1 (25 минут)

Дать определение - вирус. Описать классификация вирусов и способы заражения. Дать определение - антивирус. Описать основные классы антивирусных программ. 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 №2 (25 минут)

Описать методы оценки уязвимости информации. Виды утечки информации. 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 №3 (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 №4 (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 №5 (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.

Задание №6 (30 минут)
Для фишинговой атаки:

1. Постройте диаграмму атаки.

2. Предложите контрмеры.

3. Рассчитайте риск по методике FAIR.

Оценка	*Показатели оценки*
5	Выполнен полный анализ с расчетами.
4	Выполнена неполная оценка рисков.
3	Отсутствие количественных показателей.

Задание №7 (30 минут)
Проанализируйте риски IoT-устройств в умном доме:

1. Уязвимости протоколов (Zigbee, Wi-Fi).

2. Возможные атаки (например, перехват данных с камер).

3. Рекомендации по защите.

Оценка	*Показатели оценки*
5	Выполнен анализ с конкретными векторами атак.
4	Ответ без примеров атак.
3	Содержит только общие риски.

Дидактическая единица для контроля:
1.5 технологии мониторинга и аудита безопасности
Задание №1 (15 минут)

Объясните архитектуру SIEM-системы.
Какие события должны мониториться в первую очередь?
Приведите пример правил корреляции для выявления атак.

Оценка	*Показатели оценки*
5	Даны ответы на 3 вопроса с техническими деталями.
4	Даны ответы на 2 вопроса.
3	Дано общее описание без примеров.

Задание №2 (15 минут)

1. Объясните, как работает SIEM-система.
2. Какие типы событий должны мониториться в банковской сфере?
3. Приведите пример правила корреляции для обнаружения DDoS.

Оценка	*Показатели оценки*
5	Предоставлены ответы с техническими деталями и примером.
4	Ответ без примера.
3	Содержит только определение SIEM.

Дидактическая единица для контроля:
2.3 применять методы, средства защиты информации и нормативные документы при проектировании и обеспечении безопасности информационных систем

Задание №1 (30 минут)

Разработайте схему защиты сервера БД с использованием:

1. Дискового шифрования.
2. Мандатного контроля доступа.
3. Межсетевого экранирования.

Оценка	*Показатели оценки*
5	Предоставлена комплексная схема с пояснениями.
4	Предоставлена схема с недочетами.
3	Предоставлены отдельные элементы без системности.

Задание №2 (30 минут)

1. Какие стандарты (ГОСТ, ФСТЭК) должны быть учтены?

2. Составьте чек-лист для проверки соответствия.

Оценка	*Показатели оценки*
5	Имеется список стандартов + детальный чек-лист.
4	Предоставлен только список.
3	Изложены общие требования без привязки к стандартам.

Дидактическая единица для контроля:
1.4 нормативно-правовая база в области информационной безопасности
Задание №1 (15 минут)

1. Какие статьи УК РФ касаются киберпреступлений?

2. Требования ФСТЭК к СЗИ.

3. Особенности 187-ФЗ "О безопасности КИИ".

Оценка	*Показатели оценки*
5	Даны полные ответы с ссылками на законы.

4	Даны ответы на 2 вопроса.
3	Имеются общие знания законодательства.

Задание №2 (15 минут)

1. Перечислите 3 федеральных закона РФ, регулирующих информационную безопасность.

2. Дайте краткое описание 187-ФЗ "О безопасности КИИ".

3. Какие организации отвечают за контроль соблюдения этих законов?

Оценка	***Показатели оценки***
5	Полные ответы с примерами регулирующих органов.
4	Указаны законы без деталей.
3	Назван 1 закон.