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

УТВЕРЖДАЮ
Директор
ГБПОУИО «ИАТ»
_____ Якубовский А.Н.
«29» мая 2026 г.

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ПО ДИСЦИПЛИНЕ

ОП.05 Основы информационной безопасности

специальности

09.02.11 Разработка и управление программным обеспечением

Иркутск, 2026

Рассмотрена
цикловой комиссией

№	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 09.02.11 Разработка и управление программным обеспечением

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	Понятия информационной безопасности: информационная безопасность, конфиденциальность информации, политика безопасности, риск, уязвимость
	1.2	Классификацию угроз информационной безопасности
	1.3	Нормативно-правовые акты информационной безопасности
	1.4	Организационные средства защиты информации
	1.5	Технические средства защиты информации
Уметь	2.1	Анализировать угрозы и риски информационной безопасности
	2.2	Выбирать и применять методы защиты информации

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
ПК.3.5 Осуществлять аудит безопасности веб-приложения в соответствии с регламентом по безопасности

2. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДИСЦИПЛИНЫ, ИСПОЛЬЗУЕМЫЙ ДЛЯ ТЕКУЩЕГО КОНТРОЛЯ

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

Тема занятия: 1.2.5.Выбор организационных мер защиты информации.
Метод и форма контроля: Тестирование (Опрос)
Вид контроля: Письменная работа
Дидактическая единица: 1.1 Понятия информационной безопасности: информационная безопасность, конфиденциальность информации, политика безопасности, риск, уязвимость
Занятие(-я):
1.1.1.Основные понятия информационной безопасности.

Задание №1 (10 минут)

Напишите определения понятиям:
1. Информационная безопасность;
2. Конфиденциальность информации;
3. Риск;
4. Уязвимость;
5. Политика безопасности.

Оценка	*Показатели оценки*
5	Все определения написаны полностью и без ошибок.
4	Все определения написаны, допущены незначительные ошибки.
3	Написаны только часть определений.

Дидактическая единица: 1.2 Классификацию угроз информационной безопасности
Занятие(-я):
1.2.1.Виды и классификация угроз информационной безопасности.

Задание №1 (10 минут)

Классифицируйте угрозы по заданным критериям.

Угрозы:
1. Вирусная атака.
2. Ошибка сотрудника.
3. DDoS-атака.
4. Кража оборудования.

Определить:
по источнику;
по характеру;

по способу реализации.

Оценка	*Показатели оценки*
5	Классификация угроз выполнена правильно по всем критериям.
4	В классификации угроз допущены отдельные неточности.
3	Допущены существенные ошибки в классификации угроз.

Дидактическая единица: 1.3 Нормативно-правовые акты информационной безопасности

Занятие(-я):

1.1.2.Нормативно-правовая база информационной безопасности.

Задание №1 (15 минут)

Ответьте на вопросы (в виде краткого письменного объяснения):

1. Что регулируют нормативно-правовые акты в области ИБ?
2. Какие последствия наступают при нарушении требований ИБ?
3. Что такое политика безопасности организации?

Оценка	*Показатели оценки*
5	Ответы полные и обоснованные.
4	Ответы частично неполные.
3	Ответы поверхностные или неполные.

Дидактическая единица: 1.4 Организационные средства защиты информации

Занятие(-я):

1.2.3.Организационные средства защиты информации.

1.2.4.Выбор организационных мер защиты информации.

Задание №1 (10 минут)

Проанализируйте ситуацию:

В организации отсутствует разграничение доступа, сотрудники используют одинаковые пароли, отсутствуют инструкции по работе с данными.

Необходимо:

1. выявить проблемы;
2. предложить не менее 3 организационных мер защиты;
3. обосновать их выбор.

Оценка	*Показатели оценки*
5	Организационные меры выбраны верно и аргументированы.
4	Организационные меры выбраны верно, но обоснование недостаточно аргументировано.
3	Организационные меры предложены частично или без обоснования.

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

Тема занятия: 1.4.6.Построение и оценка эффективности системы защиты информации.
Метод и форма контроля: Письменный опрос (Опрос)
Вид контроля: Письменная работа
Дидактическая единица: 1.5 Технические средства защиты информации
Занятие(-я):
1.2.6.Технические средства защиты информации.
1.2.7.Комплексное применение средств защиты информации.
1.2.8.Выбор технических средств защиты информации.
1.4.3.Комплексный анализ безопасности информационной системы
1.4.4.Построение и оценка эффективности системы защиты информации.
Задание №1 (15 минут)
Проанализируйте информационную систему.

Описание:
В организации используется веб-приложение. Доступ сотрудников осуществляется по логину и паролю. Антивирус отсутствует, резервное копирование не настроено. Доступ к данным не разграничен.

Необходимо:
1. Определить не менее 3 угроз;
2. Классифицировать угрозы;
3. Оценить риски (вероятность / ущерб);
4. Предложить технические средства защиты;
5. Обосновать выбор средств защиты.

Оценка	*Показатели оценки*
5	Все задания выполнены полностью и без ошибок.
4	Задания выполнены, допущены незначительные ошибки.
3	Выполнена только часть заданий.

Дидактическая единица: 2.1 Анализировать угрозы и риски информационной безопасности

Занятие(-я):

1.2.2.Методы анализа угроз информационной безопасности.

1.3.1.Количественная и качественная оценка рисков информационной безопасности.

1.3.2.Разработка мер реагирования на риски (план обработки рисков).

1.4.3.Комплексный анализ безопасности информационной системы

Задание №1 (10 минут)

Проанализируйте соответствие угроз и средств защиты.

Для каждой угрозы:

- выберите ОДНО основное средство защиты;
- укажите ДОПОЛНИТЕЛЬНОЕ средство;
- объясните, почему одного средства недостаточно.

Угрозы:

1. Вредоносное ПО в системе.
2. Несанкционированный доступ к данным.
3. Сетевая атака (сканирование портов, попытки взлома).
4. Потеря данных из-за сбоя системы.

Ответ оформить в виде таблицы:

Угроза | Основное средство | Дополнительное средство | Обоснование

Оценка	***Показатели оценки***
5	Анализ соответствия угроз и средств защиты выполнен корректно.
4	Анализ соответствия угроз и средств защиты имеет неточности.
3	Анализ соответствия угроз и средств защиты выполнен с ошибками.

Дидактическая единица: 2.2 Выбирать и применять методы защиты информации

Занятие(-я):

1.2.7.Комплексное применение средств защиты информации.

1.4.1.Обоснование выбора методов защиты информации.

1.4.2.Обоснование выбора методов защиты информации.

1.4.4.Построение и оценка эффективности системы защиты информации.

1.4.5.Построение и оценка эффективности системы защиты информации.

Задание №1 (10 минут)

Постройте схему защиты информационной системы (описана в 1 задании).

Необходимо:

- выбрать не менее 3 средств защиты;
- указать их назначение;
- описать, как они взаимодействуют.

Оценка	***Показатели оценки***
5	Средства защиты подобраны правильно.
4	Средства защиты подобраны в целом верно.
3	Средства защиты подобраны частично или неверно.

Задание №2 (10 минут)

Оцените предложенную защиту из предыдущего задания.
Ответьте на вопросы:

- какие угрозы остаются;
- какие меры можно усилить;
- какие риски снижены.

Оценка	***Показатели оценки***
5	Решение комплексное и логичное.
4	Обоснование неполное.
3	Обоснование слабое или отсутствует.

3. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДИСЦИПЛИНЫ, ИСПОЛЬЗУЕМЫЙ ДЛЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

№ семестра	Вид промежуточной аттестации
4	Дифференцированный зачет

Дифференцированный зачет может быть выставлен автоматически по результатам текущих контролей
Текущий контроль №1
Текущий контроль №2

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 Понятия информационной безопасности: информационная безопасность, конфиденциальность информации, политика безопасности, риск, уязвимость
Задание №1 (из текущего контроля) (10 минут)
Напишите определения понятиям:
1. Информационная безопасность;
2. Конфиденциальность информации;
3. Риск;
4. Уязвимость;
5. Политика безопасности.

Оценка	*Показатели оценки*
5	Все определения написаны полностью и без ошибок.
4	Все определения написаны, допущены незначительные ошибки.
3	Написаны только часть определений.

Задание №2 (15 минут)
Дайте определения и приведите примеры:

- Угроза информационной безопасности.
- Внутренняя угроза.
- Внешняя угроза.

Оценка	*Показатели оценки*

5	Все определения даны корректно, примеры приведены.
4	Определения даны, примеры частично неточные.
3	Определения неполные или отсутствуют примеры.

Задание №3 (15 минут)
Объясните:
Что такое риск и как он определяется.

Оценка	***Показатели оценки***
5	Дано определение риска.
4	Определение дано, но без примера или неполное объяснение.
3	Определение некорректное или отсутствует логика.

Задание №4 (15 минут)
Объясните:
что такое активы информационной системы

Оценка	***Показатели оценки***
5	Дано определение активов.
4	Определение дано без примеров.
3	Определение неполное или неверное.

Дидактическая единица для контроля:
2.2 Выбирать и применять методы защиты информации
Задание №1 (25 минут)
Задание 2. Проанализируйте соответствие угроз и средств защиты.

Для каждой угрозы:

- выберите ОДНО основное средство защиты;
- укажите ДОПОЛНИТЕЛЬНОЕ средство;
- объясните, почему одного средства недостаточно.

Угрозы:
1. Вредоносное ПО в системе.
2. Несанкционированный доступ к данным.
3. Сетевая атака (сканирование портов, попытки взлома).

4. Потеря данных из-за сбоя системы.

Ответ оформить в виде таблицы:
Угроза | Основное средство | Дополнительное средство | Обоснование

Оценка	***Показатели оценки***
5	Средства защиты подобраны правильно.
4	Средства защиты подобраны в целом верно.
3	Средства защиты подобраны частично или неверно.

Задание №2 (25 минут)
Постройте схему защиты системы:

Описание:
В организации используется веб-приложение.
Доступ сотрудников осуществляется по логину и паролю.
Антивирус отсутствует, резервное копирование не настроено.
Доступ к данным не разграничен.

Необходимо:
выбрать не менее 3 средств защиты
указать их назначение
описать, как они взаимодействуют

Оценка	***Показатели оценки***
5	Средства защиты подобраны правильно.
4	Средства защиты подобраны в целом верно.
3	Средства защиты подобраны частично или неверно.

Задание №3 (30 минут)
Оцените предложенную защиту.

Описание:
В организации используется веб-приложение.
Доступ сотрудников осуществляется по логину и паролю.
Антивирус отсутствует, резервное копирование не настроено.
Доступ к данным не разграничен.

Ответьте:

какие угрозы остаются;
какие меры можно усилить;
какие риски снижены.

Оценка	*Показатели оценки*
5	Решение комплексное и логичное.
4	Обоснование неполное.
3	Обоснование слабое или отсутствует.

Задание №4 (25 минут)
Подберите защиту для:

- вирус;
- DDoS;
- утечка.

Оценка	*Показатели оценки*
5	Полнота выполнения задания.
4	В целом верное выполнение.
3	Частичное выполнение.

Задание №5 (30 минут)
Дана ситуация:
в системе есть антивирус, но нет firewall и резервного копирования.
Необходимо:

1. Определить, какие угрозы остаются.
2. Объяснить, почему антивируса недостаточно.
3. Предложить дополнительные средства защиты.
4. Обосновать выбор.

Оценка	*Показатели оценки*
5	выявлены угрозы, обоснована недостаточность, предложен комплекс;
4	предложения есть, но без обоснования;
3	поверхностный ответ.

Задание №6 (30 минут)
Задание:
Разработайте систему защиты для учебного компьютерного класса.
Условия:

- доступ к интернету;
- работа студентов;
- хранение данных.

Необходимо:

1. Определить угрозы.
2. Выбрать организационные меры.
3. Выбрать технические средства.
4. Обосновать выбор.

Оценка	***Показатели оценки***
5	комплексная система (орг + тех) + обоснование;
4	система есть, но не комплексная;
3	слабая проработка.

Задание №7 (30 минут)
Задание:
Разработайте политику паролей для организации.
Необходимо:

- требования к паролям;
- правила хранения;
- периодичность смены;
- ответственность.

Оценка	***Показатели оценки***
5	Задание содержит все элементы + логика.
4	Задание выполнено неполно.
3	Задание выполнено с ошибками.

Задание №8 (30 минут)
Задание:
Разработайте схему резервного копирования.
Необходимо:

- типы копий;
- периодичность;
- хранение;
- защита.

Оценка	***Показатели оценки***
5	Схема резервного копирования выполнена полностью.
4	Схема резервного копирования содержит ошибки.
3	Схема резервного копирования неточная.

Задание №9 (30 минут)
Задание:
Выявите уязвимости в сети Wi-Fi
Необходимо написать:

- угрозы;
- защита.

Оценка	***Показатели оценки***
5	Выявлены все уязвимости в сети Wi-Fi.
4	Выявлены основные уязвимости в сети Wi-Fi.
3	Выявлена часть уязвимостей в сети Wi-Fi.

Задание №10 (30 минут)
Проанализируйте систему организации:

- отсутствует политика безопасности;
- сотрудники работают под общими учетными записями;
- нет инструкций по работе с данными.

Необходимо:

1. Определить не менее 4 угроз, возникающих из-за отсутствия политики безопасности.
2. Определить уязвимости системы.
3. Оценить риски (вероятность и возможный ущерб).
4. Разработать основные положения политики безопасности (не менее 5 пунктов).
5. Обосновать, как предложенная политика снижает риски.

Оценка	***Показатели оценки***
5	выполнен полный анализ, предложена структурированная политика, есть логичное обоснование;
4	анализ выполнен, но политика раскрыта частично или без достаточного обоснования;
3	предложены отдельные меры без системности.

Задание №11 (30 минут)
Вам необходимо оценить существующую систему защиты:

- антивирус установлен;
- есть межсетевой экран;
- отсутствует резервное копирование;
- нет обучения персонала.

Необходимо:

1. Определить, какие элементы системы защиты реализованы.
2. Определить, какие элементы отсутствуют.
3. Выявить угрозы, которые остаются актуальными.
4. Предложить дополнения к системе защиты.
5. Обосновать необходимость каждого элемента.

Оценка	***Показатели оценки***
5	система проанализирована комплексно, предложены обоснованные дополнения;
4	предложения есть, но без полной аргументации;
3	анализ поверхностный.

Задание №12 (30 минут)
Разработайте комплексную систему защиты для информационной системы:

- используется локальная сеть;
- есть доступ в интернет;
- хранятся персональные данные.

Необходимо:

1. Определить угрозы.
2. Подобрать организационные меры защиты.
3. Подобрать технические средства защиты.
4. Описать, как эти меры работают совместно.
5. Показать, почему защита считается комплексной.

Оценка	***Показатели оценки***
5	предложена целостная система (орг + тех), показано взаимодействие;
4	меры предложены, но не раскрыта их взаимосвязь;
3	защита фрагментарная.

Задание №13 (30 минут)
Рассмотрите систему:

- есть антивирус;
- есть firewall;
- есть резервное копирование;
- отсутствует контроль доступа.

Необходимо:

1. Определить уровни защиты (что к какому уровню относится).
2. Выявить слабое место в системе.
3. Показать, где нарушен принцип многоуровневой защиты.
4. Предложить меры для устранения проблемы.
5. Обосновать, как система станет более устойчивой.

Оценка	*Показатели оценки*
5	корректно выделены уровни, выявлены слабости, предложено решение;
4	анализ есть, но без глубины;
3	допущены ошибки.

Задание №14 (30 минут)
В системе установлен только межсетевой экран (firewall).
Необходимо:

1. Определить, какие угрозы он предотвращает.
2. Определить, какие угрозы остаются.
3. Привести не менее 3 примеров атак, которые firewall не остановит.
4. Предложить дополнительные средства защиты.
5. Обосновать необходимость комбинирования средств защиты.

Оценка	*Показатели оценки*
5	полный анализ возможностей и ограничений + обоснованные решения;
4	анализ частичный;
3	перечисление без объяснений.

Дидактическая единица для контроля:
1.2 Классификацию угроз информационной безопасности
Задание №1 (из текущего контроля) (10 минут)
Классифицируйте угрозы по заданным критериям.

Угрозы:
1. Вирусная атака.
2. Ошибка сотрудника.
3. DDoS-атака.
4. Кража оборудования.

Определить:
по источнику;
по характеру;
по способу реализации.

Оценка	*Показатели оценки*
5	Классификация угроз выполнена правильно по всем критериям.
4	В классификации угроз допущены отдельные неточности.
3	Допущены существенные ошибки в классификации угроз.

Задание №2 (15 минут)
Опишите связь «угроза — уязвимость — риск».

Оценка	*Показатели оценки*
5	Показана связь угроза–уязвимость–риск.
4	Связь указана, но объяснение неполное.
3	Связь не раскрыта или дана с ошибками.

Задание №3 (15 минут)
Перечислите основные этапы анализа угроз.

Оценка	*Показатели оценки*
5	Перечислены этапы анализа угроз.
4	Этапы перечислены без пояснений.
3	Перечислены не все этапы.

Дидактическая единица для контроля:
1.3 Нормативно-правовые акты информационной безопасности
Задание №1 (из текущего контроля) (15 минут)
Ответьте на вопросы (в виде краткого письменного объяснения):

1. Что регулируют нормативно-правовые акты в области ИБ?
2. Какие последствия наступают при нарушении требований ИБ?
3. Что такое политика безопасности организации?

Оценка	*Показатели оценки*
5	Ответы полные и обоснованные.
4	Ответы частично неполные.
3	Ответы поверхностные или неполные.

Задание №2 (15 минут)
Опишите основные виды ущерба в ИБ.

Оценка	*Показатели оценки*
5	Перечислены виды ущерба с пояснениями.
4	Виды ущерба перечислены без пояснений.
3	Перечислены не все виды ущерба.

Дидактическая единица для контроля:

2.1 Анализировать угрозы и риски информационной безопасности

Задание №1 (30 минут)

Определите угрозы для системы:

- нет антивируса;
- общий пароль у сотрудников;
- нет резервного копирования.

Нужно: ≥3 угрозы + тип

Оценка	*Показатели оценки*
5	≥3 угрозы + классификация;
4	≥3 угрозы без классификации;
3	<3 угроз.

Задание №2 (25 минут)

Оцените риск (вероятность/ущерб) для:

- вирус;
- утечка данных;
- сбой системы.

Оценка	*Показатели оценки*
5	Полнота выполнения задания.
4	В целом верное выполнение.
3	Частичное выполнение.

Задание №3 (25 минут)

Разграничьте доступ:

- администратор;
- пользователь;
- гость.

Оценка	*Показатели оценки*
5	Полнота выполнения задания.
4	В целом верное выполнение.
3	Частичное выполнение.

Задание №4 (30 минут)
Найдите уязвимости, если в системе:

- слабые пароли;
- нет обновлений;
- открытые порты.

Оценка	*Показатели оценки*
5	Полнота выполнения задания.
4	В целом верное выполнение.
3	Частичное выполнение.

Задание №5 (30 минут)
Задание:
Проведите анализ угроз для веб-приложения.
Условия:

- авторизация по логину/паролю;
- доступ через интернет;
- нет ограничения попыток входа.

Необходимо:

1. Выявить угрозы.
2. Определить уязвимости.
3. Оценить риски.
4. Предложить защиту.

Оценка	*Показатели оценки*
5	полный анализ + адекватная защита;
4	неполный анализ;
3	ошибки.

Задание №6 (30 минут)
Задание:
Составьте таблицу соответствия:
угроза — уязвимость — последствие — защита
Необходимо заполнить минимум 4 строки.

Оценка	*Показатели оценки*
5	все элементы связаны логично.
4	есть разрывы логики.
3	задание выполнено частично.

Задание №7 (30 минут)
Задание:
Оцените безопасность системы:

- есть firewall;
- нет обновлений ПО;
- слабые пароли.

Необходимо:

1. Определить проблемы.
2. Оценить риски.
3. Предложить меры.

Оценка	*Показатели оценки*
5	выявлены все проблемы + решения;
4	Задание выполнено частично;
3	Задание выполнено с ошибками.

Задание №8 (30 минут)

Задание:
Проведите оценку рисков для:

- утечки данных;
- вирусной атаки;
- отказа системы.

Необходимо:
вероятность + ущерб + уровень риска

Оценка	***Показатели оценки***
5	Корректная оценка + логика;
4	Задание без обоснования;
3	Задание выполнено с ошибками.

Задание №9 (30 минут)
Задание:
Оцените систему защиты:

- антивирус;
- firewall;
- IDS.

Необходимо:

1. Определить, что защищено.
2. Что не защищено.
3. Что добавить.

Оценка	***Показатели оценки***
5	Оценка системы защиты выполнена верно.
4	Оценка системы защиты имеет не значительные ошибки.
3	Оценка системы защиты поверхностная.

Задание №10 (30 минут)
Проанализируйте систему защиты:

- установлен антивирус;
- пользователи скачивают файлы из интернета;
- нет фильтрации трафика;
- нет обучения пользователей.

Необходимо:

1. Определить, какие угрозы антивирус не предотвращает.
2. Объяснить ограничения антивируса.
3. Определить дополнительные угрозы.
4. Предложить дополнительные средства защиты.
5. Обосновать необходимость комплексной защиты.

Оценка	***Показатели оценки***
5	показаны ограничения антивируса + предложена комплексная защита;
4	ограничения названы, но без глубокого анализа;
3	ответ частичный.

Задание №11 (30 минут)
Проанализируйте информационную систему организации:

- используется веб-приложение;
- доступ осуществляется по логину и паролю;
- отсутствует двухфакторная аутентификация;
- резервное копирование выполняется нерегулярно;
- сотрудники используют слабые пароли;
- отсутствует контроль действий пользователей.

Необходимо:

1. Определить не менее 5 угроз для данной системы.
2. Выявить уязвимости системы.
3. Оценить риски (вероятность и возможный ущерб).
4. Предложить:
    - организационные меры защиты;
    - технические средства защиты.

5. Построить краткую схему защиты системы (описательно).
6. Обосновать, как предложенные меры снижают риски.

Оценка	*Показатели оценки*
5	проведен полный и системный анализ;
4	меры защиты предложены, но обоснование неполное;
3	меры защиты предложены без обоснования.

Дидактическая единица для контроля:
1.4 Организационные средства защиты информации
Задание №1 (из текущего контроля) (10 минут)
Проанализируйте ситуацию:
В организации отсутствует разграничение доступа, сотрудники используют одинаковые пароли, отсутствуют инструкции по работе с данными.

Необходимо:

1. выявить проблемы;
2. предложить не менее 3 организационных мер защиты;
3. обосновать их выбор.

Оценка	*Показатели оценки*
5	Организационные меры выбраны верно и аргументированы.
4	Организационные меры выбраны верно, но обоснование недостаточно аргументировано.
3	Организационные меры предложены частично или без обоснования.

Задание №2 (15 минут)
Перечислите и кратко опишите организационные средства защиты информации.

Оценка	*Показатели оценки*
5	Перечислены и корректно описаны основные меры.
4	Перечислены основные меры, описание неполное.
3	Перечислены не все меры, описание отсутствует.

Задание №3 (15 минут)

Опишите процесс разграничения доступа.

Оценка	*Показатели оценки*
5	Процесс описан по этапам.
4	Процесс описан по этапам с замечаниями.
3	Процесс описан с ошибками.

Задание №4 (15 минут)
Объясните роль пользователя в обеспечении ИБ.

Оценка	*Показатели оценки*
5	Роль пользователя раскрыта полностью.
4	Роль пользователя раскрыта, но не полностью.
3	Ответ поверхностный.

Задание №5 (15 минут)
Перечислите основные ошибки сотрудников, приводящие к угрозам.

Оценка	*Показатели оценки*
5	Перечислены основные ошибки сотрудников с пояснениями.
4	Перечислены основные ошибки без пояснений.
3	Перечислены не все ошибки или есть ошибки в ответе.

Задание №6 (15 минут)
Опишите принцип многоуровневой защиты.

Оценка	*Показатели оценки*
5	Раскрыт принцип многоуровневой защиты.
4	Принцип описан частично.
3	Ответ поверхностный.

Задание №7 (15 минут)
Объясните:
Почему нельзя использовать только одно средство защиты?

Оценка	*Показатели оценки*

5	Ответ полный, логичный, приведены примеры.
4	Ответ правильный, но неполный.
3	Ответ поверхностный.

Дидактическая единица для контроля:
1.5 Технические средства защиты информации

Задание №1 (из текущего контроля) (15 минут)
Проанализируйте информационную систему.

Описание:
В организации используется веб-приложение. Доступ сотрудников осуществляется по логину и паролю. Антивирус отсутствует, резервное копирование не настроено. Доступ к данным не разграничен.

Необходимо:
1. Определить не менее 3 угроз;
2. Классифицировать угрозы;
3. Оценить риски (вероятность / ущерб);
4. Предложить технические средства защиты;
5. Обосновать выбор средств защиты.

Оценка	***Показатели оценки***
5	Все задания выполнены полностью и без ошибок.
4	Задания выполнены, допущены незначительные ошибки.
3	Выполнена только часть заданий.

Задание №2 (15 минут)
Перечислите и кратко опишите технические средства защиты информации.

Оценка	***Показатели оценки***
5	Перечислены и корректно описаны основные меры.
4	Перечислены основные меры, описание неполное.
3	Перечислены не все меры, описание отсутствует.

Задание №3 (15 минут)
Объясните различия: антивирус / межсетевой экран / IDS

Оценка	***Показатели оценки***

5	Корректно раскрыты различия между средствами.
4	Показаны их функции и назначение.
3	Указаны области применения.

Задание №4 (15 минут)
Объясните:
Что такое резервное копирование и зачем оно нужно?

Оценка	***Показатели оценки***
5	Ответ полный и правильный.
4	Допущены незначительные неточности.
3	Допущены ошибки в понятиях.

Задание №5 (15 минут)
Объясните:
Зачем нужна политика безопасности?

Оценка	***Показатели оценки***
5	Раскрыто назначение политики безопасности.
4	Назначение указано, но без раскрытия роли.
3	Ответ поверхностный или неполный.

Задание №6 (15 минут)
Перечислите основные элементы системы защиты информации.

Оценка	***Показатели оценки***
5	Перечислены элементы системы защиты.
4	Перечислены элементы без структуры.
3	Перечислены не все элементы.

Задание №7 (15 минут)
Объясните:
Что такое комплексная защита информации?

Оценка	***Показатели оценки***

5	Дано определение комплексной защиты с примерами и пояснениями.
4	Определение дано без пояснения.
3	Ответ неполный.

Задание №8 (15 минут)
Объясните:
Роль антивируса и его ограничения.

Оценка	***Показатели оценки***
5	Раскрыта роль антивируса.
4	Роль описана, ограничения не раскрыты.
3	Ответ неполный.

Задание №9 (15 минут)
Объясните:
Роль межсетевого экрана.

Оценка	***Показатели оценки***
5	Раскрыта роль межсетевого экрана с пояснениями.
4	Роль описана без объяснения принципа.
3	Ответ поверхностный.