Министерство науки и высшего образования Российской Федерации

ФГБОУ ВО «Дагестанский государственный технический университет»

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

по дисциплине «Защищенные информационные системы»
(индекс и наименование дисциплины)

Уровень образования — магистратура
(бакалавриат/магистратура/специалитет)

Направление подготовки — 10.04.01 Информационная безопасность
(код, наименование направления подготовки)

Направленность — Кибеpразведка и противодействие угрозам с применением технологий искусственного интеллекта
(наименование)

Разработчик _____ Мирземагомедова М.М. к.т.н.
подпись (ФИО уч. степень, уч. звание)

Фонд оценочных средств обсужден на заседании кафедры ИБиПИ
«05» февраля 2026 г., протокол № 6/1

Зав. выпускающей кафедрой _____ Качаева Г.И., к.э.н.
подпись (ФИО уч. степень, уч. звание)

г. Махачкала 2026

СОДЕРЖАНИЕ

1. ПАСПОРТ ФОНДА ОЦЕНОЧНЫХ СРЕДСТВ

Фонд оценочных средств (далее - ФОС) является неотъемлемой частью рабочей программы дисциплины «Защищенные информационные системы» и предназначен для контроля и оценки образовательных достижений обучающихся (в т.ч. самостоятельной работе обучающихся), освоивших программу данной дисциплины.

Целью разработки фонда оценочных средств является установление соответствия уровня подготовки обучающихся требованиям федерального государственного образовательного стандарта высшего образования (далее - ФГОС ВО) по направлению подготовки 10.04.01 Информационная безопасность.

Рабочей программой дисциплины «Защищенные информационные системы» предусмотрено формирование следующей компетенции:

УК-1. Способность осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий

ОПК-1 Способность обосновывать требования к системе обеспечения информационной безопасности и разрабатывать проект технического задания на ее создание;

Формой аттестации по дисциплине является экзамен.

2. РЕЗУЛЬТАТЫ ОСВОЕНИЯ ДИСЦИПЛИНЫ, ПОДЛЕЖАЩИЕ ПРОВЕРКЕ

В результате аттестации по дисциплине осуществляется комплексная проверка индикаторов достижения компетенций их формирования в процессе освоения ОПОП.

Таблица 1.

Результаты обучения: индикаторы достижения	**Формируемые компетенции**
УК-1.1 Анализирует проблемную ситуацию как систему, выявляя её составляющие и связи между ними; УК-1.2 Определяет пробелы в информации, необходимой для решения проблемной ситуации; критически оценивает надежность источников информации УК-1.3 Разрабатывает и содержательно аргументирует стратегию решения проблемной ситуации на основе системного и междисциплинарного подхода	УК-1
ОПК-1.1 Использует основы отечественных и зарубежных стандартов в области обеспечения информационной безопасности при формировании требований технического задания на создание автоматизированных систем в защищенном исполнении ОПК-1.2 Проектирует информационные системы с учетом технологий обеспечения информационной безопасности ОПК-1.3 Формирует актуальные модели угроз и нарушителей для автоматизированных информационных систем, учитывает их содержание при формировании требований технического задания, умеет разрабатывать и обосновывать критерии оценки эффективности проектируемой системы обеспечения информационной безопасности	ОПК-1

3. ОЦЕНКА ОСВОЕНИЯ ДИСЦИПЛИНЫ

3.1. Контроль и оценка освоения дисциплины по темам (разделам)

Предметом оценки служат индикаторы достижения компетенций, предусмотренные ОПОП, направленные на формирование универсальных и общепрофессиональных компетенций.

Таблица 2.

Элемент дисциплины	Формы и методы контроля			
	Текущий контроль		Промежуточная аттестация	
	Форма контроля	Проверяемые компетенции/ индикаторы достижения	Форма контроля	Проверяемые компетенции/ индикаторы достижения
Тема 1. Теоретические вопросы защиты информации	Письменная работа №.1. Устный опрос Лабораторная работа №1 Самостоятельная работа Реферат	УК-1: УК-1.1, УК-1.2, УК-1.3; ОПК-1: ОПК-1.1, ОПК-1.2, ОПК-1.3.	экзаменационная работа	УК-1: УК-1.1, УК-1.2, УК-1.3; ОПК-1: ОПК-1.1, ОПК-1.2, ОПК-1.3.
Тема 2 Классификации систем защиты информации	Письменная работа №.1. Устный опрос Лабораторная работа №2 Самостоятельная работа Реферат	УК-1: УК-1.1, УК-1.2, УК-1.3; ОПК-1: ОПК-1.1, ОПК-1.2, ОПК-1.3.	экзаменационная работа	УК-1: УК-1.1, УК-1.2, УК-1.3; ОПК-1: ОПК-1.1, ОПК-1.2, ОПК-1.3.
Тема 3 Вопросы информационной безопасности	Письменная работа №.1. Устный опрос Лабораторная работа №3 Самостоятельная работа Реферат	УК-1: УК-1.1, УК-1.2, УК-1.3; ОПК-1: ОПК-1.1, ОПК-1.2, ОПК-1.3.	экзаменационная работа	УК-1: УК-1.1, УК-1.2, УК-1.3; ОПК-1: ОПК-1.1, ОПК-1.2, ОПК-1.3.
Тема 4 Аспекты построения защищенных систем	Письменная работа №.1. Устный опрос Лабораторная работа №4 Самостоятельная работа Реферат	УК-1: УК-1.1, УК-1.2, УК-1.3; ОПК-1: ОПК-1.1, ОПК-1.2, ОПК-1.3.	экзаменационная работа	УК-1: УК-1.1, УК-1.2, УК-1.3; ОПК-1: ОПК-1.1, ОПК-1.2, ОПК-1.3.
Тема 5 Требования к архитектуре ИС для обеспечения безопасности ее функционирования	Письменная работа №.1. Устный опрос Лабораторная работа №5 Самостоятельная работа Реферат	УК-1: УК-1.1, УК-1.2, УК-1.3; ОПК-1: ОПК-1.1, ОПК-1.2, ОПК-1.3.	экзаменационная работа	УК-1: УК-1.1, УК-1.2, УК-1.3; ОПК-1: ОПК-1.1, ОПК-1.2, ОПК-1.3.
Тема 6 Модели угроз информационной безопасности	Письменная работа №.2. Устный опрос Лабораторная работа №6 Самостоятельная работа Реферат	УК-1: УК-1.1, УК-1.2, УК-1.3; ОПК-1: ОПК-1.1, ОПК-1.2, ОПК-1.3.	экзаменационная работа	УК-1: УК-1.1, УК-1.2, УК-1.3; ОПК-1: ОПК-1.1, ОПК-1.2, ОПК-1.3.
Тема 7 Модели нарушителей информационной безопасности	Письменная работа №.2. Устный опрос Лабораторная работа №7 Самостоятельная работа Реферат	УК-1: УК-1.1, УК-1.2, УК-1.3; ОПК-1: ОПК-1.1, ОПК-1.2, ОПК-1.3.	экзаменационная работа	УК-1: УК-1.1, УК-1.2, УК-1.3; ОПК-1: ОПК-1.1, ОПК-1.2, ОПК-1.3.
Тема 8 Классификация каналов проникновения в систему	Письменная работа №.2. Устный опрос Лабораторная работа №8 Самостоятельная работа Реферат	УК-1: УК-1.1, УК-1.2, УК-1.3; ОПК-1: ОПК-1.1, ОПК-1.2, ОПК-1.3.	экзаменационная работа	УК-1: УК-1.1, УК-1.2, УК-1.3; ОПК-1: ОПК-1.1, ОПК-1.2, ОПК-1.3.

Тема 9 Утечки информации	Письменная работа №.2. Устный опрос Лабораторная работа №9 Самостоятельная работа Реферат	УК-1: УК-1.1, УК-1.2, УК-1.3; ОПК-1: ОПК-1.1, ОПК-1.2, ОПК-1.3.	экзаменационная работа	УК-1: УК-1.1, УК-1.2, УК-1.3; ОПК-1: ОПК-1.1, ОПК-1.2, ОПК-1.3.
Тема 10 Обеспечение надежности и бесперебойного функционирования информационных систем среды	Письменная работа №.2. Устный опрос Лабораторная работа №10 Самостоятельная работа Реферат	УК-1: УК-1.1, УК-1.2, УК-1.3; ОПК-1: ОПК-1.1, ОПК-1.2, ОПК-1.3.	экзаменационная работа	УК-1: УК-1.1, УК-1.2, УК-1.3; ОПК-1: ОПК-1.1, ОПК-1.2, ОПК-1.3.
Тема 11 Виды угроз ресурсам Интернета	Письменная работа №.3. Устный опрос Лабораторная работа №11 Самостоятельная работа Реферат	УК-1: УК-1.1, УК-1.2, УК-1.3; ОПК-1: ОПК-1.1, ОПК-1.2, ОПК-1.3.	экзаменационная работа	УК-1: УК-1.1, УК-1.2, УК-1.3; ОПК-1: ОПК-1.1, ОПК-1.2, ОПК-1.3.
Тема 12 Средства защиты открытых информационных систем. Сервисы безопасности	Письменная работа №.3. Устный опрос Лабораторная работа №12 Самостоятельная работа Реферат	УК-1: УК-1.1, УК-1.2, УК-1.3; ОПК-1: ОПК-1.1, ОПК-1.2, ОПК-1.3.	экзаменационная работа	УК-1: УК-1.1, УК-1.2, УК-1.3; ОПК-1: ОПК-1.1, ОПК-1.2, ОПК-1.3.
Тема 13 Средства защиты открытых информационных систем. Аутентификация в сетях.	Письменная работа №.3. Устный опрос Лабораторная работа №13 Самостоятельная работа Реферат	УК-1: УК-1.1, УК-1.2, УК-1.3; ОПК-1: ОПК-1.1, ОПК-1.2, ОПК-1.3.	экзаменационная работа	УК-1: УК-1.1, УК-1.2, УК-1.3; ОПК-1: ОПК-1.1, ОПК-1.2, ОПК-1.3.
Тема 14 Мониторинг и аудит в информационных системах	Письменная работа №.3. Устный опрос Лабораторная работа №14 Самостоятельная работа Реферат Эссе	УК-1: УК-1.1, УК-1.2, УК-1.3; ОПК-1: ОПК-1.1, ОПК-1.2, ОПК-1.3.	экзаменационная работа	УК-1: УК-1.1, УК-1.2, УК-1.3; ОПК-1: ОПК-1.1, ОПК-1.2, ОПК-1.3.
Тема 15 Мониторинг и аудит в информационных системах	Письменная работа №.3. Устный опрос Лабораторная работа №15 Самостоятельная работа Реферат Эссе	УК-1: УК-1.1, УК-1.2, УК-1.3; ОПК-1: ОПК-1.1, ОПК-1.2, ОПК-1.3.	экзаменационная работа	УК-1: УК-1.1, УК-1.2, УК-1.3; ОПК-1: ОПК-1.1, ОПК-1.2, ОПК-1.3.
Тема 16 Криптографическая защита информации	Письменная работа №.3. Устный опрос Лабораторная работа №16 Самостоятельная работа Реферат	УК-1: УК-1.1, УК-1.2, УК-1.3; ОПК-1: ОПК-1.1, ОПК-1.2, ОПК-1.3.	экзаменационная работа	УК-1: УК-1.1, УК-1.2, УК-1.3; ОПК-1: ОПК-1.1, ОПК-1.2, ОПК-1.3.

3.2.Перечень заданий для текущего контроля

Фор*мируемые компетенции: УК-1*

Перечень заданий закрытого типа

Задание № 1. Триада КЦД — это:

а) Контроль, Целостность, Доступ
б) Конфиденциальность, Целостность, Доступность
в) Кодирование, Цифровизация, Доверие
г) Ключ, Цифровая подпись, Дешифрование

Задание № 2. Какой российский закон в первую очередь регулирует защиту персональных данных?

а) Федеральный закон № 187-ФЗ
б) Федеральный закон № 152-ФЗ
в) Федеральный закон № 149-ФЗ
г) Приказ ФСТЭК России № 17

Задание № 3. Установите соответствие между стандартом/законом и его основной областью регулирования:

Стандарт/закон	Основная область регулирования
1) ISO/IEC 27001	А) Требования к защите персональных данных.
2) Федеральный закон № 152-ФЗ	Б) Требования к безопасности критической информационной инфраструктуры (КИИ).
3) Федеральный закон № 187-ФЗ	В) Требования по защите информации, не содержащей сведений, составляющих государственную тайну (в госорганах, на значимых объектах).
4) Приказы ФСТЭК России (серия 17, 21, 31)	Г) Международный стандарт по построению системы менеджмента информационной безопасности (СМИБ).

Задание № 4. Установите соответствие между типом криптографического ключа и его описанием:

Тип криптографического ключа	Описание
1) Симметричный ключ	А) Используется для шифрования данных и проверки электронной подписи. Должен быть доступен всем.
2) Открытый ключ (публичный)	Б) Используется одним субъектом для шифрования и расшифрования. Должен храниться в секрете.
3) Закрытый ключ (приватный)	В) Используется для расшифрования данных и создания электронной подписи. Должен храниться в строгом секрете.

Задание № 5. При проектировании системы безопасности организации, в какой последовательности необходимо изучить теоретические основы?

1. Изучение общих вопросов информационной безопасности (принципы, задачи, политика).
2. Рассмотрение классификаций систем защиты информации (по объекту, методу, принципу действия).
3. Анализ теоретических вопросов защиты информации (конфиденциальность, целостность, доступность как триада CIA).
4. Определение требований к архитектуре ИС для обеспечения безопасности на этапе проектирования.

Перечень заданий открытого типа

Задание № 1. Какая технология позволяет создавать защищенный логический канал для передачи данных через публичные, недоверенные сети (например, интернет), обеспечивая конфиденциальность и целостность трафика?

Задание № 2. Как называется принцип безопасности, согласно которому пользователю или процессу должны предоставляться минимально необходимые права доступа, достаточные только для выполнения конкретных задач?

Задание № 3. Какая система предназначена для централизованного сбора, корреляции и анализа событий безопасности от различных источников (сетевых устройств, серверов, приложений) в реальном времени?

Задание № 4. Дополните определение, вставляя пропущенное слово:
В методе атаки_____ злоумышленник, находясь между двумя легитимными участниками обмена, перехватывает, а иногда и модифицирует их сообщения, оставаясь незамеченным?

Задание № 5. Дополните определение, вставляя пропущенное слово:
Международный стандарт _____задает требования к созданию, внедрению, поддержанию и непрерывному улучшению системы менеджмента информационной безопасности (СМИБ) в организации?

Фор*мируемые компетенции: ОПК – 1.*

Перечень заданий закрытого типа

Задание № 1. Что такое "риск" в информационной безопасности?

а) Вероятность возникновения угрозы
б) Наличие уязвимости в системе
в) Комбинация вероятности реализации угрозы и последствий от нее
г) Список всех возможных атак

Задание № 2. Какой метод резервного копирования копирует только данные, измененные с момента последнего полного бэкапа?

а) Полное копирование
б) Инкрементальное копирование
в) Дифференциальное копирование
г) Зеркальное копирование

Задание № 3. Установите соответствие между группами средств защиты и конкретными примерами или их главной функцией:

Группа средств / Сервис	**Пример или ключевая функция**
1. Сервисы безопасности (средства защиты открытых систем)	A. Kerberos, PKI (Инфраструктура открытых ключей) — обеспечивают управление доступом и шифрование.
2. Средства аутентификации в сетях	B. OTP-токены, биометрические сканеры, смарт-карты — подтверждают подлинность субъекта.
3. Средства криптографической защиты	C. Асимметричные алгоритмы (RSA), хэш-функции (SHA-256) — обеспечивают конфиденциальность и целостность.

Задание № 4. Установите соответствие между типами моделей и их ключевой характеристикой:

Модель / Классификация	Характеристика
1. Модель нарушителя	A. Формализованное описание возможных путей, методов и сценариев атак на активы системы.
2. Модель угроз	B. Описание возможных источников, причин и способов несанкционированного выхода информации за пределы контролируемой зоны.
3. Классификация каналов утечки информации	C. Формализация гипотетического злоумышленника по уровню квалификации, доступа, ресурсов и мотивов.

Задание № 5. Установите последовательность этапов анализа рисков и проектирования защищённой системы.

1. Построение модели нарушителя (цели, квалификация, ресурсы).
2. Разработка модели угроз для конкретной информационной системы (список возможных атак).
3. Классификация каналов проникновения и утечки информации.
4. Определение аспектов построения защищённых систем (выбор мер и средств защиты на основе анализа).

Перечень заданий открытого типа

Задание № 1. Как называется процесс преобразования открытого текста в шифрованный (нечитаемый вид) с использованием специального алгоритма и секретного ключа?

Задание № 2. Какая модель управления доступом, широко применяемая в бизнес-средах, предполагает назначение прав не конкретным пользователям, а их должностям или функциям в организации?

Задание № 3. Как называется комплекс мер и технологий, направленных на предотвращение несанкционированной передачи конфиденциальной информации за пределы контролируемого периметра организации?

Задание № 4. Дополните определение, вставляя пропущенное слово:
Базовый принцип информационной безопасности _____ — это, означает, что доступ к информации и связанным с ней активам имеют только авторизованные пользователи, процессы или системы.

Задание № 5. Дополните определение, вставляя пропущенное слово:
В модели нарушителя _____ нарушитель — это лицо, действующее внутри защищаемого периметра организации и имеющее определенный уровень легитимного доступа к ресурсам.

4. ПЕРЕЧЕНЬ ЗАДАНИЙ ДЛЯ ОЦЕНКИ СФОРМИРОВАННОСТИ КОМПЕТЕНЦИЙ

Формируемая компетенция: УК-1

Перечень заданий закрытого типа

Задание № 1. Что означает аббревиатура КЦД в информационной безопасности?

а) Код, Цифра, Данные
б) Контроль, Цель, Доступ
в) Конфиденциальность, Целостность, Доступность
г) Ключ, Цепочка, Доверие

Задание № 2. Какой закон РФ является базовым для защиты персональных данных?

а) ФЗ-149 "Об информации, информационных технологиях и о защите информации"
б) ФЗ-152 "О персональных данных"
в) ФЗ-187 "О безопасности критической информационной инфраструктуры"
г) ФЗ-98 "О коммерческой тайне"

Задание № 3. Что такое "угроза" в контексте информационной безопасности?

а) Аппаратный сбой сервера
б) Ошибка программиста в коде
в) Потенциальная возможность нарушения безопасности системы
г) Отсутствие антивируса на компьютере

Задание № 4. Какой класс средств защиты информации (СЗИ) включает в себя пропускной режим и инструктажи?

а) Технические средства
б) Программные средства
в) Организационные средства
г) Криптографические средства

Задание № 5. Что проверяет система IDS (Intrusion Detection System)?

а) Обнаруживает признаки атак и нарушений безопасности
б) Активно блокирует атаки в реальном времени
в) Шифрует сетевой трафик
г) Управляет доступом пользователей

Задание № 6. Какой фактор аутентификации относится к биометрии?

а) Пароль
б) Смарт-карта
в) Отпечаток пальца
г) Одноразовый код из SMS

Задание № 7. Установите соответствие между аспектом построения защищённой системы и конкретным требованием к архитектуре ИС:

Аспект построения	Требование к архитектуре ИС
1. Обеспечение надёжности и бесперебойности	A. Реализация отказоустойчивых конфигураций (кластеризация, резервирование каналов).
2. Организация мониторинга и аудита	B. Наличие централизованной системы сбора и анализа журналов событий (SIEM).
3. Защита от проникновения через сеть	C. Сегментация сети (DMZ), установка межсетевых экранов (NGFW).

Задание № 8. Установите соответствие между видом угрозы и ресурсом/принципом безопасности, на который она направлена в первую очередь:

Вид угрозы	Основной объект атаки / Нарушаемый принцип
1. DDoS-атака (Угроза ресурсам Интернета)	A. Доступность информационного сервиса или системы.
2. Фишинг (Угроза ресурсам Интернета)	B. Конфиденциальность учётных данных (логинов, паролей).
3. Внедрение SQL-кода (SQL-injection)	C. Целостность и конфиденциальность данных в БД.

Задание № 9. Выберите правильную последовательность действий при организации защиты открытых информационных систем (например, с доступом в Интернет).

1. Исследование видов угроз ресурсам Интернета (DDoS-атаки, фишинг, вредоносное ПО).
2. Внедрение базовых средств защиты открытых систем (брандмауэры, IPS/IDS).
3. Настройка сервисов безопасности для контроля доступа и управления ключами.
4. Организация надёжной аутентификации в сетях (двухфакторная, на основе сертификатов).

Задание № 10. В какой очерёдности внедряются процессы контроля и обеспечения непрерывности в действующей системе?

1. Организация мониторинга и аудита для выявления инцидентов и анализа журналов событий.
2. Планирование мер по обеспечению надёжности и бесперебойного функционирования (отказоустойчивость, резервирование).
3. Реализация систем криптографической защиты информации для данных на передачу и хранение.
4. Регулярный пересмотр моделей угроз и нарушителей на основе данных мониторинга.

Перечень заданий открытого типа

Задание № 1. Как называется базовый набор принципов, документ высшего уровня, который определяет цели, подходы и общие правила организации защиты информации в компании?

Задание № 2. Какая фундаментальная триада (три основных свойства) лежит в основе всех моделей и стандартов информационной безопасности?

Задание № 3. Какой процесс направлен на выявление, оценку и принятие решений по минимизации потенциального ущерба от реализации угроз с использованием уязвимостей системы?

Задание № 4. Какая модель управления доступом предполагает, что каждому объекту и субъекту системы присваивается метка (уровень) безопасности, а доступ разрешен только по определенным правилам (например, "не читать выше" или "не писать ниже")?

Задание № 5. Дополните определение, вставляя пропущенное слово:
_____ информации — это несанкционированный процесс передачи защищаемой информации за пределы защищаемой зоны или круга лиц, имеющих право доступа к ней.

Задание № 6. Дополните определение, вставляя пропущенное слово:
_____ — это свойство системы выполнять требуемые функции в заданных условиях в течение заданного периода времени, что является критическим аспектом обеспечения доступности.

Формируемая компетенция: ОПК -1

Перечень заданий закрытого типа

Задание № 1. Какой криптографический алгоритм является симметричным?

а) RSA
б) AES

в) ECC
г) SHA-256

Задание № 2. Основная цель DDoS-атаки — это:
а) Кража конфиденциальных данных
б) Установка вредоносного ПО
в) Нарушение доступности сервиса или ресурса
г) Получение несанкционированного доступа

Задание № 3. Что такое "социальная инженерия"?
а) Проектирование сетевой архитектуры
б) Метод манипулирования людьми для получения конфиденциальной информации
в) Разработка политик безопасности
г) Анализ программного кода на уязвимости

Задание № 4. Какой документ является основой для построения СМИБ в организации?
а) Политика информационной безопасности
б) Техническое задание на систему защиты
в) Должностная инструкция администратора
г) Акт классификации информации

Задание № 5. Что означает принцип "разделения обязанностей" (Separation of Duties)?
а) Разные сотрудники используют разные операционные системы
б) Критическая задача разделяется между несколькими сотрудниками для предотвращения мошенничества
в) Данные хранятся на разных физических носителях
г) Сети разделены на сегменты

Задание № 6. Для чего используется электронная цифровая подпись (ЭЦП)?
а) Для ускорения передачи файлов
б) Для подтверждения авторства и целостности электронного документа
в) Для автоматического шифрования сообщений
г) Для аутентификации в облачных сервисах

Задание № 7. Установите соответствие между типом криптографического ключа и его описанием:

Тип криптографического ключа	**Описание**
1. Симметричный ключ	А) Используется для шифрования данных и проверки электронной подписи. Должен быть доступен всем.
2. Открытый ключ (публичный)	Б) Используется одним субъектом для шифрования и расшифрования. Должен храниться в секрете.
3. Закрытый ключ (приватный)	В) Используется для расшифрования данных и создания электронной подписи. Должен храниться в строгом секрете.

Задание № 8. Установите соответствие между классификационной категорией нарушителя (модель нарушителя) и её описанием:

Категория нарушителя	**Описание**
1. Внешний нарушитель	А. Лицо, имеющее санкционированный доступ в систему, но совершающее действия за пределами своих полномочий.
2. Внутренний нарушитель	В. Злоумышленник, не имеющий легального доступа к системе, атакующий извне через сеть.
3. «Митник» (высококвалифицированный хакер)	С. Нарушитель с глубокими экспертными знаниями в области ИТ и безопасности, целью которого является преодоление защиты как интеллектуальный вызов или для извлечения прибыли.

Задание № 9. Установите последовательность расследования предполагаемой утечки информации.

1. Анализ логов мониторинга и аудита на предмет аномальной активности.
2. Определение возможного канала проникновения в систему или утечки информации.
3. Сопоставление обнаруженных событий с актуальными моделями угроз и нарушителей.
4. Применение криптографических средств для блокировки компрометированных данных или каналов.

Задание № 10. Выберите правильный порядок действий при модернизации системы безопасности для соответствия новым требованиям.

1. Пересмотр требований к архитектуре ИС с учётом новых бизнес-процессов.
2. Актуализация моделей угроз и классификации каналов проникновения.
3. Оценка существующих средств защиты (аутентификации, сервисов безопасности) на соответствие новым моделям угроз.
4. Усиление подсистем криптографической защиты и мониторинга на основе выявленных пробелов.

Перечень заданий открытого типа

Задание № 1. Какой российский федеральный закон является основным регулятором в области обработки и защиты сведений, относящихся к физическим лицам?

Задание № 2. Как называется процесс проверки соответствия средств защиты информации и объекта информатизации установленным требованиям регуляторов (например, ФСТЭК России) с последующей выдачей официального заключения?

Задание № 3. Какая технология позволяет создавать защищенный логический канал для передачи данных через публичные, недоверенные сети (например, интернет), обеспечивая конфиденциальность и целостность трафика?

Задание № 4. Как называется принцип безопасности, согласно которому пользователю или процессу должны предоставляться минимально необходимые права доступа, достаточные только для выполнения конкретных задач?

Задание № 5. Дополните определение, вставляя пропущенное слово:
_____ — это непрерывный процесс наблюдения за событиями, происходящими в информационной системе, для выявления подозрительной активности или отклонений от нормального режима работы.

Задание № 6. Дополните определение, вставляя пропущенное слово:
_____ — это криптографический сервис безопасности, который обеспечивает подтверждение подлинности субъекта (пользователя, системы или процесса) перед предоставлением доступа.

5. КРИТЕРИИ ОЦЕНКИ

5.1. Критерии оценки текущего контроля и промежуточной аттестации

В ФГБОУ ВО «ДГТУ» внедрена модульно-рейтинговая система оценки учебной деятельности обучающихся. В соответствии с этой системой применяются пятибальная, двадцатибальная и стобальная шкалы знаний, умений, навыков.

Таблица 3.

Шкалы оценивания			**Критерии оценивания**
пятибальная	двадцатибальная	стобальная	
«Отлично» - 5 баллов	«Отлично» - 18-20 баллов	«Отлично» - 85 – 100 баллов	Показывает высокий уровень сформированности компетенций, т.е.: – продемонстрирует глубокое и прочное усвоение материала; – исчерпывающе, четко, последовательно, грамотно и логически стройно излагает теоретический материал; – правильно формирует определения; – демонстрирует умения самостоятельной работы с нормативно-правовой литературой; – умеет делать выводы по излагаемому материалу.
«Хорошо» - 4 баллов	«Хорошо» - 15 - 17 баллов	«Хорошо» - 70 - 84 баллов	Показывает достаточный уровень сформированности компетенций, т.е.: – демонстрирует достаточно полное знание материала, основных теоретических положений; – достаточно последовательно, грамотно логически стройно излагает материал; – демонстрирует умения ориентироваться в нормальной литературе; – умеет делать достаточно обоснованные выводы по излагаемому материалу.
«Удовлетворительно» - 3 баллов	«Удовлетворительно» - 12 - 14 баллов	«Удовлетворительно» - 56 – 69 баллов	Показывает пороговый уровень сформированности компетенций, т.е.: – демонстрирует общее знание изучаемого материала; – испытывает серьезные затруднения при ответах на дополнительные вопросы; – знает основную рекомендуемую литературу; – умеет строить ответ в соответствии со структурой излагаемого материала.
«Неудовлетворительно» - 2 баллов	«Неудовлетворительно» - 1-11 баллов	«Неудовлетворительно» - 1-55 баллов	Ставится в случае: – незнания значительной части программного материала; – не владения понятийным аппаратом дисциплины; – допущения существенных ошибок при изложении учебного материала; – неумение строить ответ в соответствии со структурой излагаемого вопроса; – неумение делать выводы по излагаемому материалу.

Критерии оценки тестовых заданий

Таблица 4.

Процент выполненных тестовых заданий	Оценка
до 50%	неудовлетворительно
50-69%	удовлетворительно
70-84%	хорошо
85-100%	отлично

Критерии оценки тестовых заданий, заданий на дополнение, с развернутым ответом и на установление правильной последовательности

Верный ответ - 2 балла.
Неверный ответ или его отсутствие - 0 баллов.

Критерии оценки заданий на сопоставление

Верный ответ - 2 балла
1 ошибка - 1 балл
более 1-й ошибки или ответ отсутствует - 0 баллов

КЛЮЧИ К ЗАДАНИЯМ ДЛЯ ТЕКУЩЕГО КОНТРОЛЯ

Таблица 5.

Формируемые компетенции	№ задания	Ответ
УК-1	**Задания закрытого типа**	
	№ 1	б
	№ 2	б
	№ 3	1-Г, 2-А, 3-Б, 4-В
	№ 4	1-Б, 2-А, 3-В
	№ 5	3 1 2 4
	Задания открытого типа	
	№ 1	VPN (Виртуальная частная сеть).
	№ 2	Принцип наименьших привилегий.
	№ 3	SIEM-система (Security Information and Event Management).
	№ 4	Конфиденциальность
	№ 5	ISO/IEC 27001.
ОПК-1	**Задания закрытого типа**	
	№ 1	в
	№ 2	б
	№ 3	1-А, 2-В, 3-С
	№ 4	1-С, 2-А, 3-В
	№ 5	1 2 3 4
	Задания открытого типа	
	№ 1	Шифрование
	№ 2	Ролевое управление доступом (RBAC).
	№ 3	DLP-система (Data Loss/Leak Prevention).
	№4	Конфиденциальность
	№ 5	внутренний

КЛЮЧИ К ЗАДАНИЯМ ДЛЯ ОЦЕНКИ СФОРМИРОВАННОСТИ КОМПЕТЕНЦИЙ

Таблица 6.

Формируемые компетенции	№ задания	Ответ
УК-1	**Задания закрытого типа**	
	№ 1	в
	№ 2	б
	№ 3	в
	№ 4	в
	№ 5	а
	№ 6	в
	№ 7	1-А, 2-В, 3-С
	№ 8	1-А, 2-В, 3-С
	№ 9	1 2 3 4
	№ 10	2 3 1 4
	Задания открытого типа	
	№ 1	Политика ИБ.
	№ 2	КЦД (Конфиденциальность, целостность и доступность).
	№ 3	Управление рисками (или Оценка рисков).
	№ 4	Мандатное управление доступом (МУД или МАС).
	№ 5	Утечка
	№ 6	Надежность (или Отказоустойчивость).
ОПК-1	**Задания закрытого типа**	
	№ 1	б
	№ 2	в
	№ 3	б
	№ 4	б
	№ 5	а
	№ 6	б
	№ 7	1-Б, 2-А, 3-В
	№ 8	1-В, 2-А, 3-С
	№ 9	1 3 2 4
	№ 10	1 2 3 4
	Задания открытого типа	
	№ 1	152-ФЗ "О персональных данных".
	№ 2	Аттестация (или Сертификация).
	№ 3	VPN (Виртуальная частная сеть).
	№ 4	Принцип наименьших привилегий.
	№ 5	Мониторинг
	№ 6	Аутентификация