Министерство науки и высшего образования Российской Федерации

ФГБОУ ВО «Дагестанский государственный технический университет»

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

по дисциплине «Технологии обеспечения информационной безопасности»
(указывается индекс и наименование дисциплины)

Уровень образования — магистратура
(бакалавриат/магистратура/специалитет)

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

Направленность — Киберразведка 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 «Технологии обеспечения информационной безопасности» 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 «Технологии обеспечения информационной безопасности» предусмотрено формирование следующих компетенций:

1) *ОПК-1. Способен обосновывать требования к системе обеспечения информационной безопасности и разрабатывать проект технического задания на ее создание.*

2) *ОПК-2 Способен разрабатывать технический проект системы (подсистемы либо компонента системы) обеспечения информационной безопасности.*

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**
ОПК-1.2 Проектирует информационные системы с учетом технологий обеспечения информационной безопасности	ОПК- 1
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-2.1 Применяет методы концептуального проектирования технологий обеспечения информационной безопасности	ОПК-2
ОПК-2.2 Выбирает и обосновывает преимущества методов решения задач для защиты информации компьютерных систем и сетей, а также систем обеспечения информационной безопасностью	
ОПК-2.3 Выполняет работы по защите информации при изготовлении, монтаже, наладке, испытаниях и сдаче в эксплуатацию систем и средств обеспечения информационной безопасности	

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 профессиональных 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
1. Основные понятия и угрозы информационной безопасности				
Тема 1.1 Основы информационной безопасности	Письменная работа №1 Устный опрос Лабораторная работа №1 Самостоятельная работа Реферат	ОПК-1: ОПК-1.2, ОПК-1.3; ОПК-2: ОПК-2,1, ОПК-2.2, ОПК-2.3	Экзаменационная работа	ОПК-1: ОПК-1.2, ОПК-1.3; ОПК-2: ОПК-2,1, ОПК-2.2, ОПК-2.3
Тема 1.2 Классификация методов и средств защиты информации	Письменная работа №2 Устный опрос Лабораторная работа №2 Самостоятельная работа Реферат	ОПК-1: ОПК-1.2, ОПК-1.3; ОПК-2: ОПК-2,1, ОПК-2.2, ОПК-2.3	Экзаменационная работа	ОПК-1: ОПК-1.2, ОПК-1.3; ОПК-2: ОПК-2,1, ОПК-2.2, ОПК-2.3
Тема 1.3 Задачи информационной безопасности	Письменная работа №3 Устный опрос Лабораторная работа №2 Самостоятельная работа Реферат	ОПК-1: ОПК-1.2, ОПК-1.3; ОПК-2: ОПК-2,1, ОПК-2.2, ОПК-2.3	Экзаменационная работа	ОПК-1: ОПК-1.2, ОПК-1.3; ОПК-2: ОПК-2,1, ОПК-2.2, ОПК-2.3
Тема 1.4 Угрозы информационной безопасности	Письменная работа №3 Устный опрос Лабораторная работа №3 Самостоятельная работа Реферат	ОПК-1: ОПК-1.2, ОПК-1.3; ОПК-2: ОПК-2,1, ОПК-2.2, ОПК-2.3	Экзаменационная работа	ОПК-1: ОПК-1.2, ОПК-1.3; ОПК-2: ОПК-2,1, ОПК-2.2, ОПК-2.3
Тема 1.5 Основы государственной политики и угрозы безопасности Российской Федерации в информационной сфере	Письменная работа №3 Устный опрос Лабораторная работа №5 Самостоятельная работа	ОПК-1: ОПК-1.2, ОПК-1.3; ОПК-2: ОПК-2,1, ОПК-2.2, ОПК-2.3	Экзаменационная работа	ОПК-1: ОПК-1.2, ОПК-1.3; ОПК-2: ОПК-2,1, ОПК-2.2, ОПК-2.3

	Реферат			
Тема 1.6 Понятие и виды защищаемой информации	Письменная работа №8 Устный опрос Лабораторная работа №4 Самостоятельная работа Реферат	ОПК-1: ОПК-1.2, ОПК-1.3; ОПК-2: ОПК-2,1, ОПК-2.2, ОПК-2.3	Экзаменационная работа	ОПК-1: ОПК-1.2, ОПК-1.3; ОПК-2: ОПК-2,1, ОПК-2.2, ОПК-2.3
Тема 1.7 Защита информации. Общая характеристика способов и средств защиты информации	Письменная работа №8 Устный опрос Лабораторная работа №4 Самостоятельная работа Реферат	ОПК-1: ОПК-1.2, ОПК-1.3; ОПК-2: ОПК-2,1, ОПК-2.2, ОПК-2.3	Экзаменационная работа	ОПК-1: ОПК-1.2, ОПК-1.3; ОПК-2: ОПК-2,1, ОПК-2.2, ОПК-2.3
2. Методы и средства защиты информации				
Тема 2.1 Криптографические методы защиты информации	Письменная работа №8 Устный опрос Лабораторная работа №5 Самостоятельная работа Реферат	ОПК-1: ОПК-1.2, ОПК-1.3; ОПК-2: ОПК-2,1, ОПК-2.2, ОПК-2.3	Экзаменационная работа	ОПК-1: ОПК-1.2, ОПК-1.3; ОПК-2: ОПК-2,1, ОПК-2.2, ОПК-2.3
Тема 2.2 Криптографические методы защиты информации. Одностороннее шифрование	Письменная работа №9 Устный опрос Лабораторная работа №5 Самостоятельная работа Реферат	ОПК-1: ОПК-1.2, ОПК-1.3; ОПК-2: ОПК-2,1, ОПК-2.2, ОПК-2.3	Экзаменационная работа	ОПК-1: ОПК-1.2, ОПК-1.3; ОПК-2: ОПК-2,1, ОПК-2.2, ОПК-2.3
Тема 2.3 Криптографические методы защиты информации. Симметричной шифрование	Письменная работа №10 Устный опрос Лабораторная работа №6 Самостоятельная работа Реферат	ОПК-1: ОПК-1.2, ОПК-1.3; ОПК-2: ОПК-2,1, ОПК-2.2, ОПК-2.3	Экзаменационная работа	ОПК-1: ОПК-1.2, ОПК-1.3; ОПК-2: ОПК-2,1, ОПК-2.2, ОПК-2.3
Тема 2.4 Криптографические методы защиты информации. Асимметричной шифрование	Письменная работа №11 Устный опрос Лабораторная работа №6 Самостоятельная работа Реферат	ОПК-1: ОПК-1.2, ОПК-1.3; ОПК-2: ОПК-2,1, ОПК-2.2, ОПК-2.3	Экзаменационная работа	ОПК-1: ОПК-1.2, ОПК-1.3; ОПК-2: ОПК-2,1, ОПК-2.2, ОПК-2.3
Тема 2.5 Электронная	Письменная работа №12	ОПК-1: ОПК-1.2, ОПК-1.3;	Экзаменационная работа	ОПК-1: ОПК-1.2, ОПК-1.3;

цифровая подпись и цифровые сертификаты	Устный опрос Лабораторная работа №7 Самостоятельная работа Реферат	ОПК-2: ОПК-2,1, ОПК-2.2, ОПК-2.3		ОПК-2: ОПК-2,1, ОПК-2.2, ОПК-2.3
Тема 2.6 Обеспечение высокой доступности, туннелированные и управление	Письменная работа №13 Устный опрос Лабораторная работа №7 Самостоятельная работа Реферат	ОПК-1: ОПК-1.2, ОПК-1.3; ОПК-2: ОПК-2,1, ОПК-2.2, ОПК-2.3	Экзаменационная работа	ОПК-1: ОПК-1.2, ОПК-1.3; ОПК-2: ОПК-2,1, ОПК-2.2, ОПК-2.3
Тема 2.7 Практические аспекты криптографии	Письменная работа №14 Устный опрос Лабораторная работа №8 Самостоятельная работа Реферат	ОПК-1: ОПК-1.2, ОПК-1.3; ОПК-2: ОПК-2,1, ОПК-2.2, ОПК-2.3	Экзаменационная работа	ОПК-1: ОПК-1.2, ОПК-1.3; ОПК-2: ОПК-2,1, ОПК-2.2, ОПК-2.3
Тема 2.8 Методы организации безопасного доступа	Письменная работа №15 Устный опрос Лабораторная работа №8 Самостоятельная работа Реферат	ОПК-1: ОПК-1.2, ОПК-1.3; ОПК-2: ОПК-2,1, ОПК-2.2, ОПК-2.3	Экзаменационная работа	ОПК-1: ОПК-1.2, ОПК-1.3; ОПК-2: ОПК-2,1, ОПК-2.2, ОПК-2.3
Тема 2.9 Программно-аппаратные средства защиты информации	Письменная работа №16 Устный опрос Лабораторная работа №9 Самостоятельная работа Реферат	ОПК-1: ОПК-1.2, ОПК-1.3; ОПК-2: ОПК-2,1, ОПК-2.2, ОПК-2.3	Экзаменационная работа	ОПК-1: ОПК-1.2, ОПК-1.3; ОПК-2: ОПК-2,1, ОПК-2.2, ОПК-2.3
Тема 2.10 Классификация вирусов. Применение антивирусных программ	Письменная работа №16 Устный опрос Лабораторная работа №9 Самостоятельная работа Реферат	ОПК-1: ОПК-1.2, ОПК-1.3; ОПК-2: ОПК-2,1, ОПК-2.2, ОПК-2.3	Экзаменационная работа	ОПК-1: ОПК-1.2, ОПК-1.3; ОПК-2: ОПК-2,1, ОПК-2.2, ОПК-2.3

3.2. Перечень заданий для текущего контроля

Формируемая компетенция: ОПК- 1

Перечень заданий закрытого типа

Задание № 1. При проектировании архитектуры информационной системы с высокими требованиями к конфиденциальности передаваемых данных, в первую очередь необходимо предусмотреть:

A) Установку антивирусного ПО на клиентские станции.

B) Использование криптографических протоколов (например, TLS) для защиты каналов связи.

C) Регулярное резервное копирование данных.

D) Настройку сложных паролей для пользователей.

Задания № 2. Какой ключевой документ является результатом этапа моделирования угроз и содержит систематизированное описание потенциальных атак на активы информационной системы?

A) План маркетинговых коммуникаций.

B) Модель угроз.

C) Штатное расписание отдела ИТ.

D) Годовой финансовый отчет.

Задания № 3. Установите соответствие между этапом проектирования системы защиты информации и его ключевым результатом:

Этап проектирования	Ключевой результат
1. Анализ рисков и моделирование угроз	A) Техническое задание, содержащее детальные требования к функционалу, безопасности и интерфейсам.
2. Разработка технического задания (ТЗ)	B) Архитектурная схема системы, спецификации интерфейсов и протоколов взаимодействия компонентов.
3. Концептуальное проектирование архитектуры	C) Документ, описывающий потенциальные уязвимости, сценарии атак и уровень остаточного риска.
4. Выбор и обоснование средств защиты	D) Сравнительный анализ решений, обоснование выбора конкретных технологий и продуктов.

Задания № 4. Установите соответствие между классом угрозы информационной безопасности и типом контрмеры (средства защиты), который предназначен для ее нейтрализации:

Класс угрозы	Тип контрмеры (средства защиты)
1. Сетевые атаки (сканирование, DDoS)	A) Системы антивирусной защиты и песочницы (sandbox).
2. Вредоносное программное обеспечение	B) Межсетевые экраны (файрволы), системы обнаружения и предотвращения вторжений (IDS/IPS).
3. Несанкционированный доступ к данным	C) Средства криптографической защиты информации (шифрование, ЭЦП).
4. Нарушение целостности или авторства документа	D) Системы разграничения доступа (СРД), системы управления идентификацией и доступом (IAM).

Задания № 5. Установите правильную логическую последовательность этапов формирования модели угроз для автоматизированной системы:

а) Идентификация и оценка активов системы (данные, сервисы, оборудование).

б) Разработка рекомендаций по выбору и внедрению средств защиты для снижения выявленных рисков.
в) Идентификация потенциальных уязвимостей в архитектуре и компонентах системы.
г) Определение возможных нарушителей, их мотивации и возможностей.
д) Анализ и ранжирование рисков на основе комбинации "актив-уязвимость-угроза-нарушитель".

Перечень заданий открытого типа

Задание № 1. Как называется фундаментальный принцип безопасности, требующий предоставления пользователям минимально необходимых полномочий для выполнения их задач?

Задания № 2. Какой отечественный стандарт определяет требования к алгоритмам шифрования, хэширования и электронной цифровой подписи?

Задания № 3. Как называется документ, который является основой для проведения любой проверки эффективности СЗИ и описывает, что именно и как должно быть защищено?

Задания № 4. Дополните определение, вставляя пропущенное слово.
Процесс подтверждения подлинности субъекта (пользователя, системы) по предъявленным им идентификаторам называется _____.

Задание № 5. Дополните определение, вставляя пропущенное слово.
Качественная или количественная характеристика, позволяющая измерить, насколько система защиты соответствует поставленным целям, называется _____ эффективности.

Формируемая компетенция: ОПК-2

Перечень заданий закрытого типа

Задание № 1. Какой ключевой документ, разрабатываемый согласно ГОСТ 34.601-90, следует сразу за техническим заданием и служит для детального проектирования архитектуры и выбора средств защиты информации?
A) Пояснительная записка.
B) Технический проект.
C) Эскизный проект.
D) Рабочая документация.

Задания № 2. При проектировании подсистемы защиты информации для объекта критической информационной инфраструктуры (КИИ), разработчик в первую очередь должен руководствоваться требованиями:
A) Международных стандартов серии ISO/IEC 27000.
B) Внутренних корпоративных политик.
C) Федерального закона № 187-ФЗ и нормативных актов ФСТЭК России.
D) Рекомендаций производителей оборудования.

Задания № 3. Установите соответствие между этапом создания системы защиты информации согласно ГОСТ и его ключевым результатом или содержанием работ:

Этап создания СЗИ	Ключевой результат / Содержание работ
1. Техническое задание (ТЗ)	A) Детальное описание архитектуры, спецификации средств защиты, схемы взаимодействия компонентов.
2. Технический проект (ТП)	B) Поставка оборудования, пусконаладка, проведение приемо-сдаточных испытаний.

3. Рабочая документация (РД)	C) Формализация целей, задач, требований к системе и условий ее функционирования.
4. Ввод в действие	D) Комплект инструкций, регламентов, монтажных и наладочных чертежей для непосредственного монтажа и настройки.

Задания № 4. Установите соответствие между типом защищаемой информационной системы и ключевым нормативным документом, устанавливающим требования к ее защите в РФ:

Тип информационной системы	**Ключевой нормативный документ**
1. Государственная информационная система (ГИС)	A) Приказ ФСТЭК России № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных...»
2. Информационная система персональных данных (ИСПДн)	B) Приказ ФСТЭК России № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»
3. Объект критической информационной инфраструктуры (ОКИИ)	C) Приказ ФСТЭК России № 31 «Об утверждении требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами...»
4. Автоматизированная система управления технологическим процессом (АСУ ТП) на опасном объекте	D) Федеральный закон № 187-ФЗ «О безопасности критической информационной инфраструктуры РФ» и приказы ФСТЭК России № 235, 239

Задание № 5. Установите правильную логическую последовательность основных стадий создания системы защиты информации согласно ГОСТ Р 59793-2021.

а) Техническое задание.
б) Технический проект.
в) Формирование требований.
г) Рабочая документация.
д) Эскизный проект.

Перечень заданий открытого типа

Задание № 1. Какой государственный стандарт серии 34 определяет виды, комплектность и обозначение документов на стадии технического проекта?

Задание № 2. Какой принцип информационной безопасности реализует подсистема, обеспечивающая невозможность отказа от авторства действия (например, отправки документа)?

Задание № 3. Как называется документ, определяющий общую стратегию, цели и базовые принципы построения системы защиты информации в организации, который обычно предшествует техническому проектированию?

Задание № 4. Дополните определение, вставляя пропущенное слово.
Совокупность организационных мер и программно-технических средств, предназначенная для парирования определенного класса угроз и интегрированная в общую архитектуру, называется _____ информационной безопасности.

Задание № 5. Дополните определение, вставляя пропущенное слово.
Комплекс работ, включающий проверку функциональности, корректности взаимодействия компонентов и соответствия системы требованиям технического задания перед ее принятием заказчиком, называется _____ испытаниями.

4. ПЕРЕЧЕНЬ ЗАДАНИЙ ДЛЯ ОЦЕНКИ СФОРМИРОВАННОСТИ КОМПЕТЕНЦИЙ

Формируемая компетенция: ОПК- 1

Перечень заданий закрытого типа

Задание № 1. При проектировании архитектуры информационной системы с высокими требованиями к конфиденциальности передаваемых данных, в первую очередь необходимо предусмотреть:

A) Установку антивирусного ПО на клиентские станции.

B) Использование криптографических протоколов (например, TLS) для защиты каналов связи.

C) Регулярное резервное копирование данных.

D) Настройку сложных паролей для пользователей.

Задания № 2. Какой ключевой документ является результатом этапа моделирования угроз и содержит систематизированное описание потенциальных атак на активы информационной системы?

A) План маркетинговых коммуникаций.

B) Модель угроз.

C) Штатное расписание отдела ИТ.

D) Годовой финансовый отчет.

Задания № 3. При выборе криптографического алгоритма для защиты данных в создаваемой системе, проектировщик должен руководствоваться в первую очередь:

A) Личными предпочтениями.

B) Модными тенденциями в IT-индустрии.

C) Требованиями национальных стандартов (например, ГОСТ) и оценкой криптостойкости.

D) Стоимостью лицензии на алгоритм.

Задания № 4. Какой из перечисленных компонентов является обязательной частью модели нарушителя информационной безопасности?

A) Любимый цвет нарушителя.

B) Уровень мотивации, квалификации и потенциальный доступ к системе.

C) Его годовой доход.

D) Географическое местоположение.

Задания № 5. Для обоснования требований к системе обнаружения вторжений (IDS) в техническом задании, необходимо определить:

A) Бренд и модель устанавливаемых сетевых коммутаторов.

B) Целевые показатели полноты обнаружения атак и уровня ложных срабатываний.

C) Количество мониторов на рабочем месте администратора.

D) Дизайн интерфейса панели управления.

Задания № 6. При разработке критериев оценки эффективности внедренной системы разграничения доступа (СРД), корректно измерять:

A) Удовлетворенность пользователей цветом интерфейса СРД.

B) Количество успешно предотвращенных попыток несанкционированного доступа к защищаемым ресурсам.

C) Среднюю температуру в серверной комнате.

D) Стоимость электроэнергии, потребляемой серверами СРД.

Задания № 7. Установите соответствие между этапом проектирования системы защиты информации и его ключевым результатом:

Этап проектирования	Ключевой результат
1. Анализ рисков и моделирование угроз	A) Техническое задание, содержащее детальные требования к функционалу,

	безопасности и интерфейсам.
2. Разработка технического задания (ТЗ)	B) Архитектурная схема системы, спецификации интерфейсов и протоколов взаимодействия компонентов.
3. Концептуальное проектирование архитектуры	C) Документ, описывающий потенциальные уязвимости, сценарии атак и уровень остаточного риска.
4. Выбор и обоснование средств защиты	D) Сравнительный анализ решений, обоснование выбора конкретных технологий и продуктов.

Задания № 8. Установите соответствие между классом угрозы информационной безопасности и типом контрмеры (средства защиты), который предназначен для ее нейтрализации:

Класс угрозы	**Тип контрмеры (средства защиты)**
1. Сетевые атаки (сканирование, DDoS)	A) Системы антивирусной защиты и песочницы (sandbox).
2. Вредоносное программное обеспечение	B) Межсетевые экраны (файрволы), системы обнаружения и предотвращения вторжений (IDS/IPS).
3. Несанкционированный доступ к данным	C) Средства криптографической защиты информации (шифрование, ЭЦП).
4. Нарушение целостности или авторства документа	D) Системы разграничения доступа (СРД), системы управления идентификацией и доступом (IAM).

Задания № 9. Установите правильную логическую последовательность этапов формирования модели угроз для автоматизированной системы:

а) Идентификация и оценка активов системы (данные, сервисы, оборудование).

б) Разработка рекомендаций по выбору и внедрению средств защиты для снижения выявленных рисков.

в) Идентификация потенциальных уязвимостей в архитектуре и компонентах системы.

г) Определение возможных нарушителей, их мотивации и возможностей.

д) Анализ и ранжирование рисков на основе комбинации "актив-уязвимость-угроза-нарушитель".

Задания № 10. Установите правильную последовательность разработки раздела требований информационной безопасности в рамках технического задания на систему:

а) Формулировка функциональных требований к средствам защиты (аутентификация, аудит, шифрование).

б) Анализ нормативно-правовой базы и отраслевых стандартов безопасности.

в) Определение перечня защищаемых информационных активов.

г) Формулировка нефункциональных требований (производительность, надежность средств защиты).

д) Формализация требований на основе утвержденной модели угроз и модели нарушителя.

Перечень заданий открытого типа

Задание № 1. Как называется фундаментальный принцип безопасности, требующий предоставления пользователям минимально необходимых полномочий для выполнения их задач?

Задания № 2. Какой отечественный стандарт определяет требования к алгоритмам шифрования, хэширования и электронной цифровой подписи?

Задания № 3. Как называется документ, который является основой для проведения любой проверки эффективности СЗИ и описывает, что именно и как должно быть защищено?

Задания № 4. Какой универсальный метод оценки рисков ИБ представляет собой произведение вероятности реализации угрозы на размер потенциального ущерба?

Задание № 5. Дополните определение, вставляя пропущенное слово.
Процесс подтверждения подлинности субъекта (пользователя, системы) по предъявленным им идентификаторам называется _____.

Задание № 6. Дополните определение, вставляя пропущенное слово.
Качественная или количественная характеристика, позволяющая измерить, насколько система защиты соответствует поставленным целям, называется _____ эффективности.

Формируемая компетенция: ОПК-2

Перечень заданий закрытого типа

Задание № 1. Какой ключевой документ, разрабатываемый согласно ГОСТ 34.601-90, следует сразу за техническим заданием и служит для детального проектирования архитектуры и выбора средств защиты информации?

A) Пояснительная записка.
B) Технический проект.
C) Эскизный проект.
D) Рабочая документация.

Задания № 2. При проектировании подсистемы защиты информации для объекта критической информационной инфраструктуры (КИИ), разработчик в первую очередь должен руководствоваться требованиями:

A) Международных стандартов серии ISO/IEC 27000.
B) Внутренних корпоративных политик.
C) Федерального закона № 187-ФЗ и нормативных актов ФСТЭК России.
D) Рекомендаций производителей оборудования.

Задания № 3. Какой стадией жизненного цикла системы информационной безопасности, согласно стандартному подходу, является разработка комплекта рабочей и эксплуатационной документации, а также программ и методик проведения тестирования?

A) Формирование требований.
B) Техническое проектирование.
C) Реализация (внедрение).
D) Эксплуатация.

Задания № 4. При выборе между несколькими принципиально разными архитектурными решениями для системы защиты информации, на какой предварительной стадии осуществляется их анализ и обоснование наиболее подходящего варианта?

A) Техническое задание.
B) Эскизный проект.
C) Технический проект.
D) Рабочий проект.

Задания № 5. Какой из перечисленных компонентов обычно НЕ входит в архитектуру комплексной системы защиты информации как специализированное программно-аппаратное средство?

A) Подсистема резервного копирования и восстановления данных.

B) Межсетевой экран (файрвол).
C) Сервер баз данных.
D) Система обнаружения и предотвращения вторжений (IPS).

Задания № 6. Основной целью привлечения стороннего интегратора к разработке проекта системы информационной безопасности является:
A) Полное устранение необходимости участия внутренних специалистов заказчика.
B) Получение готового проекта без учета специфики бизнес-процессов компании.
C) Использование профессиональных знаний и опыта для учета инфраструктурных особенностей и правильного выбора средств защиты.
D) Снижение бюджета проекта за счет использования типовых решений.

Задания № 7. Установите соответствие между этапом создания системы защиты информации согласно ГОСТ и его ключевым результатом или содержанием работ:

Этап создания СЗИ	**Ключевой результат / Содержание работ**
1. Техническое задание (ТЗ)	A) Детальное описание архитектуры, спецификации средств защиты, схемы взаимодействия компонентов.
2. Технический проект (ТП)	B) Поставка оборудования, пусконаладка, проведение приемо-сдаточных испытаний.
3. Рабочая документация (РД)	C) Формализация целей, задач, требований к системе и условий ее функционирования.
4. Ввод в действие	D) Комплект инструкций, регламентов, монтажных и наладочных чертежей для непосредственного монтажа и настройки.

Задания № 8. Установите соответствие между типом защищаемой информационной системы и ключевым нормативным документом, устанавливающим требования к ее защите в РФ:

Тип информационной системы	**Ключевой нормативный документ**
1. Государственная информационная система (ГИС)	A) Приказ ФСТЭК России № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных...»
2. Информационная система персональных данных (ИСПДн)	B) Приказ ФСТЭК России № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»
3. Объект критической информационной инфраструктуры (ОКИИ)	C) Приказ ФСТЭК России № 31 «Об утверждении требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами...»
4. Автоматизированная система управления технологическим процессом (АСУ ТП) на опасном объекте	D) Федеральный закон № 187-ФЗ «О безопасности критической информационной инфраструктуры РФ» и приказы ФСТЭК России № 235, 239

Задание № 9. Установите правильную логическую последовательность основных стадий создания системы защиты информации согласно ГОСТ Р 59793-2021.
а) Техническое задание.
б) Технический проект.
в) Формирование требований.
г) Рабочая документация.
д) Эскизный проект.

Задание № 10. Установите правильную последовательность действий в рамках стадии «Реализация» (внедрения) системы защиты информации.

а) Проведение пусконаладочных работ и настройка всех компонентов системы.

б) Разработка и утверждение программы и методики приемо-сдаточных испытаний.

в) Поставка программных и технических средств защиты на объект.

г) Проведение приемо-сдаточных испытаний и подписание акта ввода в эксплуатацию.

д) Монтаж оборудования и установка программного обеспечения.

Перечень заданий открытого типа

Задание № 1. Какой государственный стандарт серии 34 определяет виды, комплектность и обозначение документов на стадии технического проекта?

Задание № 2. Какой принцип информационной безопасности реализует подсистема, обеспечивающая невозможность отказа от авторства действия (например, отправки документа)?

Задание № 3. Как называется документ, определяющий общую стратегию, цели и базовые принципы построения системы защиты информации в организации, который обычно предшествует техническому проектированию?

Задание № 4. Какой этап жизненного цикла, следующий за внедрением, включает техническую поддержку, обновления и мониторинг эффективности системы защиты?

Задание № 5. Дополните определение, вставляя пропущенное слово.
Совокупность организационных мер и программно-технических средств, предназначенная для парирования определенного класса угроз и интегрированная в общую архитектуру, называется _____ информационной безопасности.

Задание № 6. Дополните определение, вставляя пропущенное слово.
Комплекс работ, включающий проверку функциональности, корректности взаимодействия компонентов и соответствия системы требованиям технического задания перед ее принятием заказчиком, называется _____ испытаниями.

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
ОПК-1	**Задания закрытого типа**	
	№ 1	B
	№ 2	B
	№ 3	1-C, 2-A, 3-B, 4-D
	№ 4	1-B, 2-A, 3-D, 4-C
	№ 5	а г в д б
	Задания открытого типа	
	№ 1	Принцип
	№ 2	ГОСТ
	№ 3	Политика
	№ 4	Аутентификация
	№ 5	Мерой
ОПК-2	**Задания закрытого типа**	
	№ 1	B
	№ 2	C
	№ 3	1-C, 2-A, 3-D, 4-B
	№ 4	1-B, 2-A, 3-D, 4-C
	№ 5	в а д б г
	Задания открытого типа	
	№ 1	ГОСТ 34.201-89
	№ 2	Неотказуемость
	№ 3	Концепция
	№ 4	Подсистемой
	№ 5	Приемо-сдаточными

КЛЮЧИ К ЗАДАНИЯМ ДЛЯ ОЦЕНКИ СФОРМИРОВАННОСТИ КОМПЕТЕНЦИЙ

Таблица 6.

Формируемые компетенции	№ задания	Ответ
ОПК-1	**Задания закрытого типа**	
	№ 1	B
	№ 2	B
	№ 3	C
	№ 4	B
	№ 5	B
	№ 6	B
	№ 7	1-C, 2-A, 3-B, 4-D
	№ 8	1-B, 2-A, 3-D, 4-C
	№ 9	а г в д б
	№ 10	б в д а г
	Задания открытого типа	
	№ 1	Принцип
	№ 2	ГОСТ
	№ 3	Политика
	№ 4	Формула
	№ 5	Аутентификация
	№ 6	Мерой
ОПК-2	**Задания закрытого типа**	
	№ 1	B
	№ 2	C
	№ 3	B
	№ 4	B
	№ 5	C
	№ 6	C
	№ 7	1-C, 2-A, 3-D, 4-B
	№ 8	1-B, 2-A, 3-D, 4-C
	№ 9	в а д б г
	№ 10	в д а б г
	Задания открытого типа	
	№ 1	ГОСТ 34.201-89
	№ 2	Неотказуемость
	№ 3	Концепция
	№ 4	Эксплуатация
	№ 5	Подсистемой
	№ 6	Приемо-сдаточными