Министерство науки и высшего образования Российской Федерации

ФГБОУ ВО «Дагестанский государственный технический университет»

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

ПРОИЗВОДСТВЕННОЙ (ТЕХНОЛОГИЧЕСКОЙ) ПРАКТИКИ

Уровень образования: магистратура
(бакалавриат/магистратура/специалитет)

Направление подготовки магистратуры: 10.04.01 Информационная безопасность
(код, наименование направления подготовки)

Направленность: Киберразведка и противодействие угрозам с применением технологий искусственного интеллекта
(наименование)

Разработчик _____ Качаева Г.И., к.э.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 3
2. Результаты освоения производственной (технологической) практики, подлежащие проверке 3
3. Оценка освоения производственной (технологической) практики 5
3.1. Контроль и оценка освоения производственной (технологической) практики по разделам (этапам) 5
4. Перечень заданий для оценки сформированности компетенций 6
5. Критерии оценки 17

1. ПАСПОРТ ФОНДА ОЦЕНОЧНЫХ СРЕДСТВ

Фонд оценочных средств (далее - ФОС) является неотъемлемой частью программы практической подготовки в форме производственной (технологической) практики и предназначен для контроля и оценки образовательных достижений обучающихся (в т.ч. самостоятельной работе обучающихся), освоивших программу данной практики.

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.

Программой практической подготовки в форме производственной (технологической) практики предусмотрено формирование следующих компетенций:

1) УК-2 Способен управлять проектом на всех этапах его жизненного цикла;
2) УК-3 Способен организовывать и руководить работой команды, вырабатывая командную стратегию для достижения поставленной цели;
3) ОПК-1 Способен обосновывать требования к системе обеспечения информационной безопасности и разрабатывать проект технического задания на ее создание;
4) ОПК-2 Способен разрабатывать технический проект системы (подсистемы либо компонента системы) обеспечения информационной безопасности;
5) ОПК-3. Способен разрабатывать проекты организационно-распорядительных документов по обеспечению информационной безопасности.

Формой аттестации по практике является зачет с оценкой.

2. РЕЗУЛЬТАТЫ ОСВОЕНИЯ ПРОИЗВОДСТВЕННОЙ (ТЕХНОЛОГИЧЕСКОЙ) ПРАКТИКИ, ПОДЛЕЖАЩИЕ ПРОВЕРКЕ

В результате аттестации по производственной (технологической) практики осуществляется комплексная проверка индикаторов достижения компетенций их формирования в процессе освоения ОПОП.

Таблица 1.

Результаты обучения: индикаторы достижения	Формируемые компетенции
УК-2.1 Формирует на основе поставленной проблемы проектную задачу и способ её решения через реализацию проектного управления	УК-2
УК-2.2 Разрабатывает концепцию проекта в рамках обозначенной проблемы и план реализации проекта с учётом возможных рисков реализации и возможностей их устранения	
УК-2.3 Осуществляет мониторинг хода реализации проекта, корректирует отклонения, вносит дополнительные изменения в план реализации проекта	
УК-3.1 Вырабатывает стратегию командной работы и на её основе организует отбор членов команд для достижения поставленной цели	УК-3
УК-3.2 Организует и корректирует работу команды, в том числе и на основе коллегиальных решений	
УК-3.3 Руководит работой команды, разрешает противоречия на основе учёта интереса всех сторон	
ОПК-1.1 Использует основы отечественных и зарубежных стандартов в области обеспечения информационной безопасности при формировании	ОПК-1

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-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	
ОПК-3.1 Применяет отечественные стандарты при сертификации средств защиты и аттестации объектов информатизации, в области управления информационной безопасностью с целью разработки организационно-распорядительных документов	ОПК-3
ОПК-3.2 Разрабатывает технические задания на создание подсистем обеспечения информационной безопасности	
ОПК-3.3 Исследует эффективность и проводит технико-экономическое обоснование проектных решений в области построения систем обеспечения информационной безопасности	

3. ОЦЕНКА ОСВОЕНИЯ ПРОИЗВОДСТВЕННОЙ (ТЕХНОЛОГИЧЕСКОЙ) ПРАКТИКИ

3.1. Контроль и оценка освоения производственной (технологической) практики по разделам (этапам)

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

Таблица 2.

Элемент производственной (технологической) практики	Формы и методы контроля			
	Текущий контроль		Промежуточная аттестация	
	Форма контроля	Проверяемые компетенции/ индикаторы достижения	Форма контроля	Проверяемые компетенции/ индикаторы достижения
Организационно-подготовительный этап. Инструктаж по ТБ. Знакомство с инфраструктурой и регламентами предприятия. Получение и анализ технического задания (ТЗ).	Устный опрос по правилам ТБ и внутренним регламентам. Проверка и утверждение руководителем плана-графика работ.	УК-2: УК-2.1, УК-2.2; УК-3: УК-3.1; ОПК-1: ОПК-1.1; ОПК-3: ОПК-3.1	Не предусмотрена	УК-2: УК-2.1, УК-2.2; УК-3: УК-3.1; ОПК-1: ОПК-1.1; ОПК-3: ОПК-3.1
Этап аналитики и проектирования. Исследование предметной области. Анализ данных и выбор технологий. Проектирование архитектуры решения.	Презентация и защита технического предложения (эскизного проекта) перед руководителями. Письменный отчет по анализу.	УК-2: УК-2.3; УК-3: УК-3.2; ОПК-1: ОПК-1.2; ОПК-2: ОПК-2.1, ОПК-2.2	Защита технического предложения	УК-2: УК-2.3; УК-3: УК-3.2; ОПК-1: ОПК-1.2; ОПК-2: ОПК-2.1, ОПК-2.2
Этап разработки и реализации. Программная реализация проекта. Настройка инструментов. Сбор и подготовка данных.	Проверка фрагментов кода и промежуточных результатов. Контроль ведения электронного журнала (лог-файла) разработки.	УК-3: УК-3.3; ОПК-1: ОПК-1.3; ОПК-2: ОПК-2.3; ОПК-3: ОПК-3.2	Не предусмотрена	УК-3: УК-3.3; ОПК-1: ОПК-1.3; ОПК-2: ОПК-2.3; ОПК-3: ОПК-3.2
Этап тестирования и валидации. Оценка качества и эффективности разработанного решения.	Предоставление отчета по тестированию с анализом метрик. Демонстрация работоспособности решения.	ОПК-3: ОПК-3.3	Не предусмотрена	ОПК-3: ОПК-3.3
Этап внедрения, документирования и отчетности. Подготовка решения к передаче. Оформление итоговой документации.	Защита итогового проекта (демонстрация + презентация). Проверка полного пакета документации и итогового отчета. Зачет с оценкой.	УК-2: УК-2.3; УК-3: УК-3.3; ОПК-3: ОПК-3.3	Зачетная работа	УК-2: УК-2.3; УК-3: УК-3.3; ОПК-3: ОПК-3.3

4. ПЕРЕЧЕНЬ ЗАДАНИЙ ДЛЯ ОЦЕНКИ СФОРМИРОВАННОСТИ КОМПЕТЕНЦИЙ

Формируемая компетенция: УК-2

Перечень заданий закрытого типа

Задание № 1. В рамках проектной задачи по разработке модуля обнаружения аномалий для SIEM-системы руководитель сформулировал цель: «Повысить безопасность». Какая формулировка лучше соответствует критериям конкретной и измеримой проектной задачи?

A) Изучить методы машинного обучения.

B) Разработать и интегрировать в тестовый контур SIEM Python-скрипт, который снизит долю ложных срабатываний на 15% при анализе сетевого трафика CICIDS-2017.

C) Сделать нашу систему лучше.

D) Нанять дополнительного аналитика безопасности.

E) Закупить более мощные серверы.

Задание № 2. Какой элемент плана реализации проекта по внедрению системы DLP является примером планирования действий по устранению возможного риска?

A) Описание общих преимуществ системы DLP для бизнеса.

B) Список сотрудников, которые будут проходить обучение.

C) Пункт: «При низкой производительности системы на пиковых нагрузках провести оптимизацию правил фильтрации и рассмотреть возможность аппаратного апгрейда».

D) Технические характеристики серверного оборудования.

E) Биография руководителя проекта.

Задание № 3. В ходе мониторинга проекта по разработке дашборда для кибербразведки выяснилось, что один из ключевых разработчиков выбывает на две недели по болезни. Какое действие руководителя проекта демонстрирует эффективную корректировку плана?

A) Объявить о сдвиге сроков сдачи всего проекта на две недели.

B) Немедленно уволить заболевшего разработчика за срыв сроков.

C) Перераспределить задачи его модуля между другими членами команды, скорректировав приоритеты и краткосрочные дедлайны.

D) Прекратить ежедневные собрания, чтобы дать команде сосредоточиться.

E) Дождаться возвращения разработчика, не меняя плана.

Задание № 4. При разработке концепции проекта по созданию системы мониторига угроз в соцсетях наиболее важно включить в раздел «Риски»:

A) Перечень всех известных социальных сетей.

B) Биографии членов команды.

C) Потенциальные юридические ограничения на сбор данных, риск изменения API соцсетей и угрозу получения недостоверной информации.

D) Рекламный проспект компании-заказчика.

E) Подробное техническое описание алгоритмов парсинга.

Задание № 5. Проблема: «Аналитики SOC перегружены рутинным анализом логов». Какая формулировка лучше всего преобразует эту проблему в проектную задачу?

A) «Заставить аналитиков работать быстрее».

B) «Автоматизировать процесс первичного анализа и классификации событий ИБ с помощью ML-модели, чтобы к концу квартала 70% низкоприоритетных инцидентов обрабатывались автоматически».

C) «Нанять еще двух аналитиков».

D) «Купить аналитикам более удобные кресла».

E) «Провести исследование о выгорании сотрудников».

Задание № 6. На статус-совещании по проекту обновления инфраструктуры PKI ответственный инженер сообщает, что поставка оборудования задерживается. Какой инструмент мониторинга проекта в первую очередь потребует корректировки?

A) Устав проекта.
B) Бюджет проекта.
C) Реестр рисков.
D) Диаграмма Ганта (календарный план).
E) Отчет о достижении целей.

Задание № 7. Установите соответствие между элементом проектной документации и его описанием.

Проектная документация	Описание проектной документации
1. Устав проекта	A) Декомпозиция всего объема работ проекта на управляемые пакеты работ.
2. Иерархическая структура работ	B) Документ, формально авторизующий начало проекта и наделяющий менеджера полномочиями.
3. Матрица ответственности	C) Таблица, распределяющая роли по задачам.
4. Дорожная карта	D) Визуализация ключевых этапов и результатов проекта на стратегическом уровне с привязкой к срокам.

Задание № 8. Установите соответствие между этапом жизненного цикла проекта и типичным действием в рамках проекта по разработке инструмента киберразведки с применением машинного обучения.

Этап жизненного цикла проекта	Действие в проекте
1. Инициация	A) Декомпозиция работ: парсинг источников угроз, разработка ML-модели для оценки критичности, создание дашборда.
2. Планирование	B) Разработка и тестирование MVP (минимально жизнеспособного продукта), ежедневные стендапы, отслеживание прогресса по спринтам.
3. Исполнение и мониторинг	C) Формальное закрытие репозитория кода, передача документации заказчику, проведение ретроспективы.
4. Завершение	D) Обоснование необходимости инструмента, определение стейкхолдеров, подготовка устава проекта.

Задание № 9. Установите правильную последовательность шагов при реагировании на выявленное в ходе мониторинга отклонение от плана проекта.

а) Разработка и выбор корректирующих действий.
б) Анализ влияния отклонения на сроки, бюджет и содержание проекта.
в) Внесение утвержденных изменений в план проекта и оповещение команды.
г) Идентификация и документирование факта отклонения.
д) Утверждение изменений у спонсора/стейкхолдеров проекта.

Задание № 10. Установите правильную логическую последовательность шагов в процессе управления изменениями плана проекта, если в ходе разработки прототипа системы обнаружения аномалий выяснилось, что выбранный алгоритм машинного обучения не обеспечивает требуемую точность.

а) Внесение утвержденных изменений в дорожную карту, план тестирования и документацию проекта.

б) Инициация запроса на изменение: формальное описание проблемы, анализ влияния на сроки, бюджет и качество.
в) Тестирование нового алгоритма на валидационной выборке для подтверждения улучшения метрик.
г) Предложение альтернативных решений и оценка их трудозатрат.
д) Согласование выбранного решения с техническим руководителем и спонсором проекта.

Перечень заданий открытого типа

Задание № 1. Как называется ключевой документ проекта, который формально его инициирует, определяет высокоуровневые цели, полномочия менеджера и основных стейкхолдеров?

Задание № 2. Как называется основной процесс проектного управления, в ходе которого отслеживается выполнение плана, идентифицируются отклонения и управляются изменения?

Задание № 3. Как называется графический инструмент планирования, который представляет расписание проекта в виде столбчатой диаграммы?

Задание № 4. Как называется метод декомпозиции общей цели проекта на более мелкие и управляемые пакеты работ?

Задание № 5. Дополните определение, вставляя пропущенное слово: Потенциальное неопределенное событие или условие, которое в случае наступления окажет положительное или отрицательное влияние на цели проекта, называется _____.

Задание № 6. Дополните определение, вставляя пропущенное слово: Документ, который содержит утвержденный перечень работ, необходимых для завершения проекта, называется _____ проекта.

Формируемая компетенция: УК-3

Перечень заданий закрытого типа

Задание № 1. При формировании команды для срочного проекта по анализу инцидента кибербезопасности руководитель выбирает специалистов по анализу сетевого трафика, аналитиков вредоносного ПО и эксперта по цифровой криминалистике. Какой принцип отбора членов команды он применяет?

A) Принцип дружеских связей.
B) Принцип комплементарности компетенций.
C) Принцип минимальной стоимости.
D) Принцип территориальной близости.

Задание № 2. В команде разработчиков системы обнаружения вторжений возник спор между data scientist, предлагающим сложную модель, и инженером, выступающим за простоту и скорость. Какой подход руководителя НАИБОЛЕЕ эффективен для разрешения этого противоречия?

A) Авторитарно принять решение в пользу более опытного сотрудника.
B) Игнорировать спор, надеясь, что сотрудники договорятся сами.
C) Организовать фасилитированное обсуждение для поиска сбалансированного решения, учитывающего технические требования проекта.
D) Передать решение на рассмотрение высшему руководству.

Задание № 3. Какая стратегия командной работы наиболее эффективна для достижения сложной цели, такой как разработка нового алгоритма киберразведки?

A) Каждый член команды работает независимо над своей частью, а результаты собираются в конце.

B) Работа строится по гибкой методологии с короткими итерациями, ежедневной синхронизацией и общей ответственностью за результат.

C) Руководитель детально расписывает задачи на весь срок, а команда строго их исполняет.

D) Команда проводит ежемесячные длительные совещания для обсуждения прогресса.

Задание № 4. Для быстрого сбора и анализа данных об уязвимостях из открытых источников руководителю необходимо сформировать мобильную рабочую группу. Какой размер команды будет НАИБОЛЕЕ оптимальным?

A) 1 человек.

B) 15 человек.

C) 3-5 человек.

D) 10-12 человек.

Задание № 5. В ходе проекта один из членов команды систематически не успевает выполнять свои задачи, ссылаясь на высокую нагрузку. Что должен сделать руководитель в первую очередь, чтобы скорректировать работу команды?

A) Немедленно применить дисциплинарное взыскание.

B) Провести личную беседу, чтобы выяснить причины, перераспределить нагрузку или оказать поддержку.

C) Публично указать на недопустимость срывов сроков на общем собрании.

D) Взять задачи сотрудника на себя.

Задание № 6. Какой инструмент наиболее подходит для визуализации текущего статуса задач всех членов команды в рамках одного спринта в методологии Agile?

A) Отчет о прибылях и убытках.

B) Диаграмма сгорания задач.

C) Организационная структура компании.

D) Техническое задание на проект.

Задание № 7. Установите соответствие между стилем руководства командой и его описанием.

Стиль руководства командой	Описание стиля
1. Авторитарный	A) Руководитель принимает решения единолично, сотрудники четко выполняют инструкции.
2. Демократический	B) Руководитель распределяет задачи, дает широкие полномочия и контролирует только ключевые точки.
3. Делегирующий	C) Руководитель вовлекает команду в обсуждение проблем, решения принимаются коллегиально.

Задание № 8. Установите соответствие между этапом развития команды (по Такману) и типичным поведением участников.

Тип документа	Назначение
1. Формирование	A) Возникновение разногласий по методам работы и распределению ролей.
2. Конфликт	B) Установление негласных правил взаимодействия, рост сплоченности.
3. Нормирование	C) Настороженность, формальное общение, уточнение целей и задач.
4. Результативность	D) Слаженная и эффективная работа на общий результат.

Задание № 9. Установите правильную последовательность шагов руководителя при организации работы новой команды над проектом.

а) Определение и согласование с командой конкретных целей, ролей и зон ответственности.

б) Проведение установочного совещания для представления членов команды и общего видения проекта.

в) Выбор и внедрение инструментов для коммуникации, совместной работы и контроля задач.

г) Анализ требований проекта и подбор специалистов с необходимыми компетенциями.

Задание № 10. Установите правильную логическую последовательность действий руководителя для разрешения конструктивного конфликта в команде.

а) Выслушивание аргументов и позиций всех сторон конфликта.

б) Совместный поиск и оценка альтернативных решений, удовлетворяющих интересы команды и цели проекта.

в) Четкое определение и формулировка сути возникшего противоречия.

г) Фасилитация дискуссии, направление обсуждения в продуктивное русло.

д) Фиксация достигнутого соглашения и плана действий по его реализации.

Перечень заданий открытого типа

Задание № 1. Как называется гибкая методология управления проектами, основанная на коротких циклах разработки и ежедневных командных собраниях?

Задание № 2. Как называется принцип формирования команды, предполагающий, что её размер должен позволять накормить участников двумя пиццами?

Задание № 3. Как называется процесс управления, направленный на помощь группе в выполнении задачи, облегчение коммуникации и поддержание конструктивной атмосферы?

Задание № 4. Как называется документ, который фиксирует основные правила взаимодействия, коммуникации и принятия решений внутри команды?

Задание № 5. Дополните определение: Процесс выявления, обсуждения и разрешения противоречий между членами команды для достижения консенсуса называется управление _____.

Задание № 6. Дополните определение: Краткое ежедневное совещание команды для синхронизации деятельности и выявления препятствий называется _____ митинг.

Формируемая компетенция: ОПК-1

Перечень заданий закрытого типа

Задание 1. При формировании требований к системе защиты персональных данных в государственной информационной системе РФ необходимо в первую очередь руководствоваться требованиями:

A) ISO/IEC 27001

B) GDPR

C) Федерального закона №152-ФЗ и приказов ФСТЭК России

D) Рекомендациями PCI DSS

Задание № 2. Какой принцип проектирования защищенной информационной системы предполагает, что доступ к ресурсам предоставляется только при явной необходимости для выполнения задач?

A) Принцип открытого дизайна

B) Принцип минимальных привилегий

C) Принцип полномочий

D) Принцип разнообразия защитных мер

Задание № 3. Ключевым отличием «нарушителя» от «угрозы» в модели угроз является то, что нарушитель - это:

A) Конкретный источник опасности, обладающий мотивацией и потенциалом
B) Уязвимость в программном обеспечении
C) Потенциальное событие, которое может нанести ущерб
D) Техническая характеристика системы

Задание № 4. Какой стандарт серии ГОСТ Р ИСО/МЭК наиболее применим для разработки общих требований к системе менеджмента информационной безопасности в организации?
A) ГОСТ Р ИСО/МЭК 19790
B) ГОСТ Р ИСО/МЭК 15408
C) ГОСТ Р ИСО/МЭК 27001
D) ГОСТ Р ИСО/МЭК 12207

Задание № 5. Проектирование сегментации корпоративной сети на уровни доверия (DMZ, внутренняя сеть) в первую очередь направлено на реализацию мер:
A) Криптографической защиты
B) Антивирусной защиты
C) Сетевого экранирования и контроля доступа
D) Резервного копирования

Задание № 6. Какой из перечисленных элементов НЕ является обязательным для включения в модель нарушителя по методическим документам ФСТЭК России?
A) Уровень технической оснащенности
B) Категория персональных данных, к которым стремится получить доступ
C) Мотивация и цели
D) Исходный уровень подготовки

Задание № 7. Установите соответствие между типом автоматизированной системы и основным отечественным нормативным документом, регламентирующим требования к ее защите.

Тип АС	Основной нормативный документ
1. Система персональных данных (ПДн)	A) Приказы ФСТЭК России, устанавливающие требования к защите информации в КИИ
2. Государственная информационная система (ГИС)	B) Федеральный закон №152-ФЗ «О персональных данных» и сопутствующие акты
3. Критическая информационная инфраструктура (КИИ)	C) Требования к защите информации, не содержащей сведений, составляющих государственную тайну, для ГИС

Задание № 8. Установите соответствие между этапом проектирования защищенной системы и примером проектного решения.

Этап проектирования защищенной системы	Пример проектного решения
1. Архитектурное проектирование	A) Разработка регламента разграничения доступа по ролям (RBAC)
2. Проектирование политик безопасности	B) Решение о применении двухфакторной аутентификации на границе сети
3. Выбор средств защиты	C) Схема разделения сети на VLAN и зоны доверия

Задание № 9. Установите правильную логическую последовательность разработки раздела «Требования к системе защиты» в техническом задании.
а) Формулировка требований по противодействию идентифицированным угрозам
б) Разработка и утверждение модели угроз и модели нарушителя
в) Определение классов защищенности/уровней доверия обрабатываемой информации
г) Выбор и спецификация конкретных мер и средств защиты информации

Задание № 10. Установите правильную логическую последовательность действий при внедрении подсистемы контроля доступа.

а) Аудит и анализ существующих процессов доступа к информационным ресурсам

б) Интеграция и настройка выбранного технического решения (HW/SW)

в) Разработка и внедрение организационно-распорядительной документации (положений, инструкций)

г) Тестирование функционирования подсистемы в тестовой среде

Перечень заданий открытого типа

Задание № 1. Как называется уполномоченный государственный орган России, разрабатывающий требования по защите информации для государственных информационных систем?

Задание № 2. Как называется базовый принцип информационной безопасности, требующий, чтобы при проектировании системы безопасность была встроена в архитектуру, а не добавлена позже?

Задание № 3. Как называется документ, который формально описывает возможные источники, цели, методы и объекты атак на информационную систему?

Задание № 4. Какой международный стандарт определяет критерии оценки безопасности информационных технологий?

Задание № 5. Дополните определение: Лицо, преднамеренно осуществляющее попытку нарушения безопасности информации, в модели угроз называется _____.

Задание № 6. Дополните определение: Проектирование системы, при котором безопасность обеспечивается на нескольких независимых уровнях, называется защитой в _____.

Формируемая компетенция: ОПК-2

Перечень заданий закрытого типа

Задание № 1. Какой документ, разрабатываемый на этапе концептуального проектирования, содержит принципиальные решения, общую структуру и основные характеристики будущей системы защиты?

A) Техническое задание

B) Эскизный проект

C) Рабочая документация

D) Паспорт системы

Задание № 2. Для защиты корпоративной сети от утечек данных через внешние USB-накопители наиболее обоснованным методологическим решением является:

A) Установка антивируса на все рабочие станции

B) Развертывание системы DLP с контролем внешних устройств

C) Повышение мощности межсетевого экрана

D) Регулярное обучение пользователей

Задание № 3. Какая работа выполняется напрямую перед сдачей системы защиты информации в опытную эксплуатацию?

A) Формирование концепции системы

B) Комплексные испытания

C) Разработка технического задания

D) Маркетинговый анализ

Задание № 4. Выбор архитектуры «защита периметра» при концептуальном проектировании подразумевает фокусировку на:

A) Шифровании всех данных на серверах
B) Контроле точек входа/выхода в сеть организации
C) Установке систем обнаружения вторжений на каждую рабочую станцию
D) Биометрической аутентификации всех пользователей

Задание № 5. Какое преимущество является ключевым при выборе аппаратного межсетевого экрана перед программным для защиты магистрального канала связи?

A) Более низкая стоимость
B) Простота обновления правил
C) Высокая производительность и отказоустойчивость
D) Возможность тонкой настройки под конкретное приложение

Задание № 6. Документ, фиксирующий состав, содержание и результаты работ по наладке средств защиты, — это:

A) Протокол испытаний
B) Акт выполненных работ
C) Журнал наладки
D) Руководство по эксплуатации

Задание № 7. Установите соответствие между принципом концептуального проектирования безопасных систем и его описанием.

Принцип концептуального проектирования	**Описание принципав**
1. Принцип минимальных привилегий	A) Для выполнения критической операции требуется участие нескольких лиц
2. Принцип разделения обязанностей	B) Пользователь получает доступ ровно к тем ресурсам, которые необходимы для работы
3. Принцип эшелонированной обороны	C) Защита организуется на нескольких независимых уровнях

Задание **№** 8. Установите соответствие между типом защищаемых данных и рекомендуемым криптографическим методом для обеспечения конфиденциальности.

Тип защищаемых данных	**Метод защиты**
1. Данные, хранящиеся на сервере	A) Симметричное шифрование (AES)
2. Данные, передаваемые по открытой сети	B) Асимметричное шифрование (RSA) или TLS
3. Аутентификационные данные пользователя	C) Хеширование с солью

Задание № 9. Установите правильную последовательность работ при внедрении и сдаче в эксплуатацию нового межсетевого экрана.

а) Проведение приемосдаточных испытаний и подписание акта ввода в эксплуатацию
б) Монтаж оборудования в стойку, физическое подключение
в) Настройка политик безопасности и правил фильтрации в тестовом режиме
г) Разработка и согласование регламента эксплуатации и политик безопасности

Задание № 10. Установите правильную последовательность этапов разработки технического проекта.

а) Детализация и описание всех подсистем, интерфейсов, алгоритмов
б) Согласование и утверждение документации заказчиком
в) Анализ требований технического задания
г) Выбор и обоснование принципиальных технических решений и архитектуры

Перечень заданий открытого типа

Задание № 1. Как называется основной документ, содержащий полное описание проектных решений, достаточное для изготовления, монтажа и настройки системы?

Задание № 2. Как называется метод защиты информации, при котором данные преобразуются с использованием секретного ключа для обеспечения конфиденциальности?

Задание № 3. Как называется процесс проверки работоспособности и соответствия средств защиты требованиям проектной документации?

Задание № 4. Как называется раздел технического проекта, описывающий взаимодействие компонентов системы и внешних систем?

Задание № 5. Дополните определение: Совокупность организационных и технических мер, реализуемых при вводе системы в действие, называется _____ в эксплуатацию.

Задание № 6. Дополните определение: Принцип защиты, при котором компрометация одного компонента системы не ведет к компрометации всей системы, называется _____ изоляцией.

Формируемая компетенция: ОПК-3

Перечень заданий закрытого типа

Задание № 1. Для проведения обязательной сертификации средства защиты информации, используемого в государственной информационной системе, разработчик должен обратиться в:

A) Роскомнадзор
B) ФСБ России
C) ФСТЭК России
D) Минцифры России

Задание № 2. Раздел «Назначение разработки» в техническом задании на подсистему защиты должен содержать:

A) Подробные схемы алгоритмов работы
B) Перечень нормативных документов
C) Формулировку решаемой проблемы и цели создания подсистемы
D) Смету расходов на оборудование

Задание № 3. При технико-экономическом обосновании внедрения системы DLP ключевым экономическим показателем эффективности (ROI) является:

A) Количество обнаруженных инцидентов
B) Соотношение предотвращенного ущерба к затратам на систему
C) Скорость обработки трафика
D) Количество пользователей

Задание № 4. «Инструкция пользователя по обеспечению безопасности при работе в корпоративной сети» является примером документа уровня:

A) Политики
B) Стандарта
C) Процедуры
D) Руководства

Задание № 5. Какой раздел ТЗ на систему обнаружения вторжений определяет, при каком проценте ложных срабатываний система считается работоспособной?

A) Требования к надежности
B) Требования к функциональным характеристикам
C) Условия эксплуатации

D) Требования к составу и параметрам технических средств

Задание № 6. Какой показатель НАИБОЛЕЕ точно характеризует операционную эффективность системы антивирусной защиты?

A) Стоимость лицензии на одно рабочее место
B) Процент обнаружения вредоносного ПО в независимых тестах
C) Количество сотрудников отдела ИБ
D) Размер занимаемой дискового пространства

Задание № 7. Установите соответствие между видом организационно-распорядительного документа по ИБ и его основным содержанием.

Вид организационно-распорядительного документа	Основное содержание документа
1. Политика информационной безопасности	A) Детальное пошаговое описание выполнения конкретной операции
2. Регламент резервного копирования	B) Документ, закрепляющий перечень сведений, составляющих секрет предприятия
3. Положение о коммерческой тайне	C) Верховный документ, определяющий цели, принципы и подходы организации к ИБ

Задание № 8. Установите соответствие между методом оценки эффективности системы защиты и оцениваемой характеристикой.

Метод оценки эффективности системы защиты	Оцениваемая характеристика
1. Аудит соответствия	A) Соответствие настроек и политик требованиям нормативных документов
2. Тестирование на проникновение	B) Стоимость потенциальных инцидентов и обоснованность затрат на защиту
3. Анализ рисков	C) Способность системы противостоять реальным атакам

Задание № 9. Установите правильную логическую последовательность разделов при разработке проекта технического задания.

а) Требования к функциональным характеристикам
б) Цель и назначение разработки
в) Порядок контроля и приемки
г) Основания для разработки и наименование проекта

Задание № 10. Установите правильную логическую последовательность действий при подготовке объекта информатизации к аттестации.

а) Проведение специальной оценки и оформление результатов
б) Разработка полного комплекта организационно-распорядительной документации
в) Выбор класса защищенности и разработка модели угроз
г) Установка и настройка сертифицированных средств защиты

Перечень заданий открытого типа

Задание № 1. Как называется комплекс мероприятий по проверке соответствия объекта информатизации требованиям по защите информации?

Задание № 2. Как называется основной документ, определяющий технические требования к создаваемой системе или подсистеме?

Задание № 3. Как называется показатель, вычисляемый как отношение вероятных годовых потерь до и после внедрения системы защиты?

Задание № 4. Как называется документ, устанавливающий правила обработки персональных данных в организации?

Задание № 5. Дополните определение: Экономия средств за счет предотвращения инцидентов за вычетом затрат на систему защиты составляет чистый _____ эффект.

Задание № 6. Дополните определение: Раздел ТЗ, описывающий, что должна делать система, называется требованиями к _____ характеристикам.

5. КРИТЕРИИ ОЦЕНКИ

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 ОЦЕНКИ СФОРМИРОВАННОСТИ КОМПЕТЕНЦИЙ

Таблица 5.

Формируемые компетенции	№ задания	Ответ
УК-2	**Задания закрытого типа**	
	№ 1	B
	№ 2	C
	№ 3	C
	№ 4	C
	№ 5	B
	№ 6	D
	№ 7	1-B, 2-A, 3-C, 4-D
	№ 8	1-D, 2-A, 3-B, 4-C
	№ 9	г б а д в
	№ 10	б г д в а
	Задания открытого типа	
	№ 1	Устав
	№ 2	Мониторинг
	№ 3	Диаграмма ганта
	№ 4	Иерархическая структура
	№ 5	Риском
	№ 6	Объемом работ
УК-3	**Задания закрытого типа**	
	№ 1	B
	№ 2	C
	№ 3	B
	№ 4	C
	№ 5	B
	№ 6	B
	№ 7	1-A, 2-C, 3-B
	№ 8	1-C, 2-A, 3-B, 4-D
	№ 9	г б а в
	№ 10	в а г б д
	Задания открытого типа	
	№ 1	Scrum,
	№ 2	Двухпиццечный
	№ 3	Фасилитация
	№ 4	Регламент
	№ 5	Конфликтами
	№ 6	Стендап
ОПК-1	**Задания закрытого типа**	
	№ 1	C
	№ 2	B
	№ 3	A
	№ 4	C
	№ 5	C
	№ 6	B
	№ 7	1-B, 2-C, 3-A
	№ 8	1-C, 2-A, 3-B
	№ 9	в б а г

	№ 10	а в б г
	Задания открытого типа	
	№ 1	ФСТЭК
	№ 2	Security by Design
	№ 3	Модель угроз
	№ 4	Common Criteria
	№ 5	Нарушитель
	№ 6	Глубину
ОПК-2	**Задания закрытого типа**	
	№ 1	B
	№ 2	B
	№ 3	B
	№ 4	B
	№ 5	C
	№ 6	C
	№ 7	1-B, 2-A, 3-C
	№ 8	1-A, 2-B, 3-C
	№ 9	г б в а
	№ 10	в г а б
	Задания открытого типа	
	№ 1	Технический_проект
	№ 2	Шифрование
	№ 3	Испытания
	№ 4	Интерфейсы
	№ 5	Сдача
	№ 6	Функциональной
ОПК-3	**Задания закрытого типа**	
	№ 1	C
	№ 2	C
	№ 3	B
	№ 4	D
	№ 5	A
	№ 6	B
	№ 7	1-C, 2-A, 3-B
	№ 8	1-A, 2-C, 3-B
	№ 9	г б а в
	№ 10	в б г а
	Задания открытого типа	
	№ 1	Аттестация
	№ 2	Техническое задание
	№ 3	Эффективность
	№ 4	Политика
	№ 5	Дисконтированный
	№ 6	Функциональным