Фонд оценочных средств
для промежуточной аттестации
по дисциплине (модулю)

ОП.05 Основы информационной безопасности

Специальность
09.02.11 Разработка и управление программным обеспечением

Направленность программы
Разработка мобильных приложений

Присваиваемая квалификация
Программист

Форма обучения
очная

Год набора 2026

Челябинск, 2026г.

09.02.11 Разработка и управление программным обеспечением, направленность программы: Разработка мобильных приложений,
фонд оценочных средств для промежуточной аттестации по дисциплине ОП.05 Основы информационной безопасности, 2026 год набора, очная форма обучения:

Утверждена:
Проректор по учебной работе _____ А.А. Саламатов
подпись И.О. Фамилия

Протокол заседания от « 23 » апреля 2026 г. № 5

Председатель Педагогического совета
Колледжа ЧелГУ _____ М.В. Найн
подпись И.О. Фамилия

Составитель _____ Д.С. Лебедев
подпись И.О. Фамилия

Структура фонда оценочных средств для промежуточной аттестации по дисциплине соответствует приказу ректора ФГБОУ ВО «ЧелГУ» от 09.07.2024г. № 327-1 «Об утверждении шаблонов документов».

Оглавление

1. ПАСПОРТ ФОНДА ОЦЕНОЧНЫХ СРЕДСТВ

Специальность09.02.11 Разработка и управление программным обеспечением
Дисциплина: ОП.05 Основы информационной безопасности
Очная форма обучения
Семестр (семестры) изучения: 3 семестр
Форма промежуточной аттестации: зачет с оценкой (3 семестр)

2. ПЕРЕЧЕНЬ ФОРМИРУЕМЫХ КОМПЕТЕНЦИЙ

2.1. Компетенции, закреплённые за дисциплиной

Изучение дисциплины «ОП.05 Основы информационной безопасности» направлено на формирование следующих компетенций:

Код компетенции согласно ФГОС (ОПОП СПО)	Содержание компетенций согласно ФГОС (ОПОП СПО)	Перечень планируемых результатов обучения по дисциплине
ОК 01	Выбирать способы решения задач профессиональной деятельности применительно к различным контекстам	**Умения:** распознавать задачу и/или проблему в профессиональном и/или социальном контексте, анализировать и выделять её составные части; определять этапы решения задачи, составлять план действия, реализовывать составленный план, определять необходимые ресурсы; выявлять и эффективно искать информацию, необходимую для решения задачи и/или проблемы; владеть актуальными методами работы в профессиональной и смежных сферах; оценивать результат и последствия своих действий (самостоятельно или с помощью наставника) **Знания:** актуальный профессиональный и социальный контекст, в котором приходится работать и жить; структура плана для решения задач, алгоритмы выполнения работ в профессиональной и смежных областях; основные источники информации и ресурсы для решения задач и/или проблем в профессиональном и/или социальном контексте; методы работы в профессиональной и смежных сферах; порядок оценки результатов решения задач профессиональной деятельности
ОК 02	Использовать современные средства поиска, анализа и интерпретации информации и информационные технологии для выполнения задач профессиональной деятельности	**Умения:** определять задачи для поиска информации, планировать процесс поиска, выбирать необходимые источники информации; выделять наиболее значимое в перечне информации, структурировать получаемую информацию, оформлять результаты поиска; оценивать практическую значимость результатов поиска; применять средства информационных технологий для решения профессиональных задач; использовать современное программное обеспечение в профессиональной деятельности; использовать различные цифровые средства для решения профессиональных задач **Знания:** номенклатура информационных источников, применяемых

		в профессиональной деятельности; приемы структурирования информации; формат оформления результатов поиска информации; современные средства и устройства информатизации, порядок их применения и программное обеспечение в профессиональной деятельности, в том числе цифровые средства
ОК 09	Пользоваться профессиональной документацией на государственном и иностранном языках	**Умения:** понимать общий смысл четко произнесенных высказываний на известные темы (профессиональные и бытовые), понимать тексты на базовые профессиональные темы; участвовать в диалогах на знакомые общие и профессиональные темы; строить простые высказывания о себе и о своей профессиональной деятельности кратко обосновывать и объяснять свои действия (текущие и планируемые); писать простые связные сообщения на знакомые или интересующие профессиональные темы **Знания:** правила построения простых и сложных предложений на профессиональные темы; основные общеупотребительные глаголы (бытовая и профессиональная лексика); лексический минимум, относящийся к описанию предметов, средств и процессов профессиональной деятельности; особенности произношения; правила чтения текстов профессиональной направленности
ПК 1.1.	Проектировать базы данных	**Навыки:** разработки концептуальной модели базы данных; разработки инфологической модели базы данных; разработки физической модели базы данных; разработки требований к базе данных; нормализация структуры базы данных; документирования схемы базы данных, включая диаграммы ER и описания таблиц; документирования прав доступа и безопасности базы данных, включая учетные записи пользователей и их роли **Умения:** анализировать предметную область и выделять основные сущности; определять требования к базе данных; разрабатывать концептуальную, логическую и физическую модели баз данных; проектировать схему базы данных; работать с современными case-средствами проектирования баз данных; определять связи между таблицами; определять типы данных для полей таблиц; оформление документации на спроектированную базу данных; разработки схемы базы данных, используя NoSQL модели данных, такие как документо-ориентированные, ключ-значение, колоночные и др. **Знания:** основные положения теории баз данных, хранилищ данных, баз знаний; основные принципы структуризации и нормализации базы данных; основные принципы построения концептуальной, логической и физической модели данных; методы описания схем баз данных в современных системах управления базами данных; структуру данных систем управления базами данных, основные понятия и принципы проектирования баз данных; структуру реляционной базы данных; язык SQL и особенности его реализации в различных системах

		управления базами данных; оптимизацию производительности баз данных; принципы безопасности хранения данных
ПК 1.4.	Администрировать базы данных	**Навыки:** установки и настройки СУБД; создания и удаления баз данных; восстановления баз данных; резервного копирования баз данных; создания пользователей и назначения прав доступа; оптимизации запросов к базе данных; мониторинга и обслуживания NoSQL баз данных, включая резервное копирование и восстановление данных. **Умения:** устанавливать и настраивать СУБД; создавать и удалять базы данных; создавать пользователей и назначать права доступа; оптимизировать запросы к базе данных; обеспечивать безопасность баз данных; создавать и настраивать базы данных в соответствии с требованиями бизнеса; управлять транзакциями и контролировать целостность данных; обеспечивать безопасность и управлять доступом к данным; создавать и восстанавливать резервные копии данных; работать с индексами и оптимизировать производительность запросов; нормализовать базы данных и проектировать эффективные структуры данных; мониторить и анализировать производительность баз данных; работать с нереляционными базами данных и выбирать наиболее подходящий тип базы данных для конкретной задачи **Знания:** архитектуру СУБД; основные принципы администрирования баз данных; методы мониторинга и оптимизации работы баз данных; принципы резервного копирования и восстановления баз данных; методы защиты баз данных от внешних угроз; особенности работы с различными СУБД; Язык SQL (Structured Query Language); управление транзакциями и контроль целостности данных; управление доступом и безопасностью баз данных; резервное копирование и восстановление данных; оптимизацию производительности баз данных; работу с индексами и оптимизация запросов; мониторинг и анализ производительности; принципы работы с реляционными базами данных; принципы работы с нереляционными базами данных
ПК 1.5.	Защищать информацию в базе данных с использованием технологии защиты информации.	**Навыки:** использования стандартных методов защиты объектов базы данных; разработки и внедрения систем защиты баз данных от несанкционированного доступа; разработки и внедрения систем резервного копирования и восстановления баз данных; аудита безопасности баз данных **Умения:** разрабатывать и внедрять системы защиты баз данных от несанкционированного доступа; разрабатывать и внедрять системы резервного копирования и восстановления баз данных; проводить аудит безопасности баз данных; устанавливать и настраивать механизмы аутентификации и авторизации пользователей; создавать и управлять ролями и правами доступа к данным; шифровать данные и обеспечивать их конфиденциальность; контролировать целостность данных и обнаруживать изменения; использовать меха-

		низмы аудита для отслеживания доступа к данным; использовать механизмы мониторинга для обнаружения угроз безопасности; создавать и управлять защищенными соединениями с базой данных; использовать механизмы защиты от SQL-инъекций и других видов атак; создавать и управлять бэкапами и резервными копиями данных; обеспечивать безопасность базы данных при использовании облачных сервисов **Знания:** методы защиты баз данных от несанкционированного доступа; методы создания и восстановления резервных копий баз данных; особенности работы с различными типами СУБД; методы проведения аудита безопасности баз данных; принципы криптографии и методов шифрования данных; стандарты и протоколы безопасности, таких как SSL/TLS, SSH, Kerberos и др.; методы аутентификации и авторизации пользователей, включая использование паролей, сертификатов и биометрических данных; методы контроля доступа, включая создание ролей и групп пользователей, управление правами доступа и аудит доступа к данным; методы обнаружения и предотвращения атак, включая защиту от SQL-инъекций, DoS/DDoS-атак и других угроз безопасности; методы мониторинга и анализа журналов событий для обнаружения угроз безопасности и анализа производительности базы данных; методы создания и управления защищенными соединениями с базой данных, включая VPN-туннели и SSL-шифрование; методы создания и управления бэкапами и резервными копиями данных, включая использование инкрементальных и дифференциальных бэкапов; методы обеспечения безопасности базы данных при использовании облачных сервисов, включая защиту от утечки данных и управление доступом к облачным ресурсам; законодательство и стандарты безопасности, такие как GDPR, HIPAA, PCI DSS и др.
ПК 3.1	Разрабатывать модули программного обеспечения для мобильных платформ.	**Навыки:** разработки модулей программного обеспечения для мобильных платформ; разработки многопоточных приложений; оптимизации производительности приложений; работы с интеграцией сторонних библиотек **Умения:** разрабатывать программный код; отлаживать приложения на различных устройствах; работать с системами контроля версий; использовать паттерны проектирования; осуществлять тестирование кода; производить рефакторинг; интегрировать приложения с облачными сервисами **Знания:** основы языков программирования; принципы ООП и функционального программирования; архитектуры мобильных приложений (MVC, MVVM, VIPER); принципы работы основных мобильных ОС (iOS, Android); жизненный цикл мобильного приложения; методы оптимизации производительности; основы работы с графическим интерфейсом и анимацией; основы безопасности в мобильной разработке; основы работы с сетью и API; принципы работы с базами

		данных на мобильных платформах; платформы по кросс-сплатформенной разработке, таких как Flutter, React Native или MAUI.
ПК 3.2	Проектировать и разрабатывать пользовательский интерфейс и пользовательский опыт.	**Навыки:** создания пользовательских интерфейсов с использованием инструментов и библиотек, таких как UIKit (iOS) и Android XML (Android); разработки адаптивных и мультирезолюционных интерфейсов; тестирования пользовательского опыта; проведения юзабилити-тестов; проектирование пользовательского интерфейса (UI) и пользовательского опыта (UX) для различных веб-приложений и сайтов; разработки прототипов и макетов пользовательского интерфейса с использованием инструментов, таких как Sketch, Adobe XD или Figma; проведения пользовательских исследований, включая сбор обратной связи от пользователей и анализ конкурентного рынка; создания дизайн-системы и стайл-гайдов для обеспечения единообразия визуального стиля и пользовательского опыта; тестирования и итеративное улучшения пользовательского интерфейса на основе обратной связи пользователей. **Умения:** создавать интуитивно понятные и легко навигируемые интерфейсы; использовать анимацию и переходы для улучшения пользовательского опыта; оптимизировать интерфейс для работы на разных экранах и устройствах; интегрировать элементы пользовательского интерфейса с серверной частью или базой данных приложения; анализировать пользовательские данные и обратную связь для улучшения UX; разрабатывать макеты и прототипы приложений; владеть инструментами дизайна интерфейса; глубоко понимать принципы дизайна пользовательского интерфейса и пользовательского опыта; проводить пользовательские исследования, включая создание опросов, интервью с пользователями и анализ данных; работать с прототипированием и созданием макетов пользовательского интерфейса; работать в команде и эффективно взаимодействовать с разработчиками и менеджерами проектов. **Знания:** принципы дизайна пользовательского интерфейса (UI) и пользовательского опыта (UX); основы графического дизайна и типографики; гайдлайны и стандарты для создания интерфейсов на платформах iOS и Android; принципы адаптивного дизайна; основы работы с векторной и растровой графикой; процесс проектирования интерфейса от идеи до реализации; основные принципы дизайна пользовательского интерфейса, таких как иерархия информации, цветовая гамма, типографика и композиция; психологию пользователей и их потребности при взаимодействии с веб-приложениями; современные тенденции в дизайне пользовательского интерфейса и пользовательского опыта; основные принципы разработки адаптивного и доступного пользовательского интерфейса; основные технологии веб-разработки, такие как HTML, CSS и JavaScript.

ПК 3.3	Проектировать и разрабатывать базы данных для мобильных платформ.	**Навыки:** работы с SQLite и другими СУБД для мобильных платформ; разработки эффективных схем баз данных; работы с NoSQL и графовыми базами данных; работы с ORM (Object-Relational Mapping) инструментами; работы с асинхронным доступом к данным; разработки функций и возможностей для работы с базами данных в программном обеспечении для мобильных платформ; создания интерфейсов для работы с базами данных, включая CRUD операции (создание, чтение, обновление, удаление данных); интеграции баз данных в пользовательский интерфейс приложений для удобного доступа и управления данными;оптимизации работы с базами данных для обеспечения высокой производительности и эффективного использования ресурсов устройства. **Умения:** проектировать и оптимизировать базы данных; выполнять CRUD (Create, Read, Update, Delete) операции; обеспечивать синхронизацию данных между устройствами; работать с кэшированием данных; обрабатывать конфликты данных в распределенных системах; работать с многозадачностью и потоками данных; владеть языком SQL для работы с базами данных; глубоко понимать принципы работы с базами данных в программном обеспечении для мобильных платформ; создавать и оптимизировать структуру баз данных для хранения и обработки данных в мобильных приложениях; работать с ORM (Object-Relational Mapping) инструментами для более удобного взаимодействия с базами данных; обеспечивать безопасность и защиту данных при работе с базами данных в мобильных приложениях. **Знания:** основы реляционных баз данных; основы NoSQL и графовых баз данных; принципы работы с транзакциями; основы безопасности и шифрования данных; принципы работы с миграциями баз данных; основы работы с асинхронными операциями; основные принципы работы с базами данных в программном обеспечении для мобильных платформ; различные типы баз данных, таких как реляционные, NoSQL и графовые базы данных; современные тенденции в разработке мобильных приложений с использованием баз данных; основные принципы проектирования баз данных для эффективного хранения и обработки данных в мобильных приложениях; основные технологии разработки мобильных приложений, таких как Java, Kotlin, Swift или React Native, для работы с базами данных.
ПК 3.5	Выполнять тестирование и отладку программного обеспечения	**Навыки:** создания тестовых сценариев и единиц тестирования для мобильных платформ; отладки и анализа проблем в работе мобильных приложений; использования инструментов и оборудования для тестирования программных компонентов мобильных платформ; работы с эмуляторами и симуляторами для программного обеспечения мобильных платформ

		Умения: разрабатывать и запускать тестовые сценарии для проверки функциональности программного обеспечения для мобильных платформ; выявлять и исправлять ошибки и несоответствия в работе ПО; проводить аппаратное и программное тестирование программного обеспечения для мобильных платформ; использовать инструменты анализа и отладки для поиска и устранения проблем; работать с инструментами для обнаружения и исправления ошибок; работать с отчетами о тестировании; анализировать и устранять утечки памяти **Знания:** основы тестирования программного обеспечения; виды тестирования (функциональное, нагрузочное, UI-тестирование и др.); принципы работы с отладчиками; основы continuous integration и continuous delivery (CI/CD); основы создания тестовых сценариев; принципы и методы тестирования программного обеспечения для мобильных платформ; особенности отладки программного обеспечения для мобильных платформ; принципы работы эмуляторов и симуляторов; методы аппаратного и программного тестирования
ПК 3.7	Осуществлять защиту данных в мобильных приложениях.	**Навыки:** разработки безопасных методов аутентификации и авторизации пользователей; обработки и хранения конфиденциальных данных; отслеживания и обработки уязвимостей безопасности; использования шифрования для защиты данных в покое и в движении; использования шифрования данных для защиты конфиденциальной информации, такой как пароли, персональные данные пользователей и другие чувствительные данные; реализации механизмов аутентификации и авторизации для обеспечения доступа только авторизованным пользователям; применения механизмов хеширования для защиты паролей пользователей от несанкционированного доступа; обеспечения безопасности передачи данных между клиентскими устройствами и серверами с использованием протоколов шифрования, таких как SSL/TLS; разработки механизмов контроля доступа к данным, чтобы предотвратить несанкционированное чтение, изменение или удаление данных; проектирования и реализации систем резервного копирования и восстановления данных для обеспечения их сохранности в случае сбоев или потери устройства; тестирования приложений на уязвимости безопасности, такие как SQL-инъекции, межсайтовые сценарии и другие уязвимости, и принятие мер по их устранению; соблюдение законодательства и регуляций в области защиты данных **Умения:** разрабатывать и реализовывать меры безопасности; реализовывать хэширование паролей, сессионные токены и двухфакторную аутентификацию; осуществлять валидацию данных, поступающих от пользователей; разрабатывать политику доступа и права пользователей к данным и функциональности приложения; реализовывать меры контроля доступа и аудита для отслеживания

		действий пользователей и обнаружения несанкционированных действий. **Знания:** основные угрозы безопасности мобильных приложений; принципы криптографии и шифрования данных; стандарты и протоколы безопасности, такие как HTTPS, OAuth и OpenID Connect; законодательные и регуляторные требования к защите данных, включая GDPR и HIPAA; основные принципы безопасности информации и методов ее защиты; стандартные криптографические алгоритмы для шифрования данных; методы аутентификации и авторизации пользователей, таких как OAuth или JWT; многоуровневые механизмы контроля доступа к данным; методы тестирования на уязвимости безопасности и опыт применения инструментов для их обнаружения; принципы обеспечения безопасности передачи данных по сети; законодательство и регуляции в области защиты данных и умение применять их в практической разработке мобильных приложений.

3. СОДЕРЖАНИЕ ОЦЕНОЧНЫХ СРЕДСТВ ПО ДИСЦИПЛИНЕ

3.1 Виды оценочных средств

Код, наименование компетенции согласно ФГОС	Перечень планируемых результатов обучения по дисциплине	Контролируемые темы/разделы (номер и название раздела из РПД п.2.2)	Семестр	Номер задания	Наименование оценочного средства
ОК 01 Выбирать способы решения задач профессиональной деятельности применительно к различным контекстам	**Знания:** актуальный профессиональный и социальный контекст, в котором приходится работать и жить; структура плана для решения задач, алгоритмы выполнения работ в профессиональной и смежных областях; основные источники информации и ресурсы для решения задач и/или проблем в профессиональном и/или социальном контексте; методы работы в профессиональной и смежных сферах; порядок оценки результатов решения задач профессиональной деятельности	Раздел 1. Основы информационной безопасности;	5	1,2,26	
	Умения: распознавать задачу и/или	Раздел 1. Основы информационной	5	41	

	проблему в профессиональном и/или социальном контексте, анализировать и выделять её составные части; определять этапы решения задачи, составлять план действия, реализовывать составленный план, определять необходимые ресурсы; выявлять и эффективно искать информацию, необходимую для решения задачи и/или проблемы; владеть актуальными методами работы в профессиональной и смежных сферах; оценивать результат и последствия своих действий (самостоятельно или с помощью наставника)	безопасности;			
ОК 02 Использовать современные средства поиска, анализа и интерпретации информации и информационные технологии для выполнения задач профессиональной деятельности	**Знания:** номенклатура информационных источников, применяемых в профессиональной деятельности приемы структурирования информации формат оформления результатов поиска информации, современные средства и устройства информатизации порядок их применения и программное обеспечение в профессиональной деятельности в том числе с использованием цифровых средств	Раздел 1. Основы информационной безопасности;	5	3,4,33	Тестовые задания закрытого типа
	Умения: определять задачи для поиска информации определять необходимые источники информации планировать процесс поиска; структурировать получаемую информацию выделять наиболее значимое в перечне информации оценивать практическую значимость результатов	Раздел 1. Основы информационной безопасности;	5	42	Задания с развернутым ответом

	поиска оформлять результаты поиска, применять средства информационных технологий для решения профессиональных задач использовать современное программное обеспечение использовать различные цифровые средства для решения профессиональных задач				
ОК 09 Пользоваться профессиональной документацией на государственном и иностранном языках	**Знания:** правила построения простых и сложных предложений на профессиональные темы; основные общеупотребительные глаголы (бытовая и профессиональная лексика); лексический минимум, относящийся к описанию предметов, средств и процессов профессиональной деятельности; особенности произношения; правила чтения текстов профессиональной направленности	Раздел 1. Основы информационной безопасности;	5	5,6,27	Тестовые задания закрытого типа
	Умения: понимать общий смысл четко произнесенных высказываний на известные темы (профессиональные и бытовые), понимать тексты на базовые профессиональные темы; участвовать в диалогах на знакомые общие и профессиональные темы; строить простые высказывания о себе и о своей профессиональной деятельности кратко обосновывать и объяснять свои действия (текущие и планируемые);писать простые связные сообщения на знакомые или интересующие профессиональные темы	Раздел 1. Основы информационной безопасности;	5	43	Задания с развернутым ответом

ПК 1.1 Проектировать базы данных.	**Знания:** основные положения теории баз данных, хранилищ данных, баз знаний; основные принципы структуризации и нормализации базы данных; основные принципы построения концептуальной, логической и физической модели данных; методы описания схем баз данных в современных системах управления базами данных; структуру данных систем управления базами данных, основные понятия и принципы проектирования баз данных; структуру реляционной базы данных; язык SQL и особенности его реализации в различных системах управления базами данных; оптимизацию производительности баз данных; принципы безопасности хранения данных	Раздел 1. Основы информационной безопасности;	5	7,8,34	Тестовые задания закрытого типа
	Умения: анализировать предметную область и выделять основные сущности; определять требования к базе данных; разрабатывать концептуальную, логическую и физическую модели баз данных; проектировать схему базы данных; работать с современными case-средствами проектирования баз данных; определять связи между таблицами; определять типы данных для полей таблиц; оформление документации на спроектированную базу данных; разработки схемы базы данных, используя NoSQL модели данных,	Раздел 1. Основы информационной безопасности;	5	44	Задания с развернутым ответом

	такие как документо-ориентированные, ключ-значение, колоночные и др.				
	Навыки: разработки концептуальной модели базы данных; разработки инфологической модели базы данных; разработки физической модели базы данных; разработки требований к базе данных; нормализация структуры базы данных; документирования схемы базы данных, включая диаграммы ER и описания таблиц; документирования прав доступа и безопасности базы данных, включая учетные записи пользователей и их роли	Раздел 1. Основы информационной безопасности;	5	52	Задания с развернутым ответом
ПК 1.4. Администрировать базы данных	**Знания:** архитектуру СУБД; основные принципы администрирования баз данных; методы мониторинга и оптимизации работы баз данных; принципы резервного копирования и восстановления баз данных; методы защиты баз данных от внешних угроз; особенности работы с различными СУБД; Язык SQL (Structured Query Language); управление транзакциями и контроль целостности данных; управление доступом и безопасностью баз данных; резервное копирование и восстановление данных; оптимизацию производительности баз данных; работу с индексами и оптимизация запросов; мониторинг и анализ производительности; принципы работы с реляционными базами	Раздел 1. Основы информационной безопасности;	5	9,10,11, 28	Тестовые задания закрытого типа

	данных; принципы работы с нереляционными базами данных				
	Умения: устанавливать и настраивать СУБД; создавать и удалять базы данных; создавать пользователей и назначать права доступа; оптимизировать запросы к базе данных; обеспечивать безопасность баз данных; создавать и настраивать базы данных в соответствии с требованиями бизнеса; управлять транзакциями и контролировать целостность данных; обеспечивать безопасность и управлять доступом к данным; создавать и восстанавливать резервные копии данных; работать с индексами и оптимизировать производительность запросов; нормализовать базы данных и проектировать эффективные структуры данных; мониторить и анализировать производительность баз данных; работать с нереляционными базами данных и выбирать наиболее подходящий тип базы данных для конкретной задачи	Раздел 1. Основы информационной безопасности;	5	45	Задания с развернутым ответом
	Навыки: установки и настройки СУБД; создания и удаления баз данных; восстановления баз данных; резервного копирования баз данных; создания пользователей и назначения прав доступа; оптимизации запросов к базе данных; мониторинга и обслуживания NoSQL баз данных, включая резервное копирование и	Раздел 1. Основы информационной безопасности;	5	53	Задания с развернутым ответом

	восстановление данных.				
ПК 1.5. Защищать информацию в базе данных с использованием технологии защиты информации	**Знания:** методы защиты баз данных от несанкционированного доступа; методы создания и восстановления резервных копий баз данных; особенности работы с различными типами СУБД; методы проведения аудита безопасности баз данных; принципы криптографии и методов шифрования данных; стандарты и протоколы безопасности, таких как SSL/TLS, SSH, Kerberos и др.; методы аутентификации и авторизации пользователей, включая использование паролей, сертификатов и биометрических данных; методы контроля доступа, включая создание ролей и групп пользователей, управление правами доступа и аудит доступа к данным; методы обнаружения и предотвращения атак, включая защиту от SQL-инъекций, DoS/DDoS-атак и других угроз безопасности; методы мониторинга и анализа журналов событий для обнаружения угроз безопасности и анализа производительности базы данных; методы создания и управления защищенными соединениями с базой данных, включая VPN-туннели и SSL-шифрование; методы создания и управления бэкапами и резервными копиями данных, включая использование инкрементальных и дифференциальных бэкапов; методы обеспечения безопасности	Раздел 1. Основы информационной безопасности;	5	12, 13, 14,35	Тестовые задания закрытого типа

	базы данных при использовании облачных сервисов, включая защиту от утечки данных и управление доступом к облачным ресурсам;				
	Умения: разрабатывать и внедрять системы защиты баз данных от несанкционированного доступа; разрабатывать и внедрять системы резервного копирования и восстановления баз данных; проводить аудит безопасности баз данных; устанавливать и настраивать механизмы аутентификации и авторизации пользователей; создавать и управлять ролями и правами доступа к данным; шифровать данные и обеспечивать их конфиденциальность; контролировать целостность данных и обнаруживать изменения; использовать механизмы аудита для отслеживания доступа к данным; использовать механизмы мониторинга для обнаружения угроз безопасности; создавать и управлять защищенными соединениями с базой данных; использовать механизмы защиты от SQL-инъекций и других видов атак; создавать и управлять бэкапами и резервными копиями данных; обеспечивать безопасность базы данных при использовании облачных сервисов	Раздел 1. Основы информационной безопасности;	5	46	Задания с развернутым ответом
	Навыки: использования стандартных методов защиты объектов базы данных; разработки и внедрения систем защиты баз данных от	Раздел 1. Основы информационной безопасности;	5	54	Задания с развернутым ответом

	несанкционированного доступа; разработки и внедрения систем резервного копирования и восстановления баз данных; аудита безопасности баз данных				
ПК 3.1. Разрабатывать модули программного обеспечения для мобильных платформ.	**Знания:** основы языков программирования; принципы ООП и функционального программирования; архитектуры мобильных приложений (MVC, MVVM, VIPER); принципы работы основных мобильных ОС (iOS, Android); жизненный цикл мобильного приложения; методы оптимизации производительности; основы работы с графическим интерфейсом и анимацией; основы безопасности в мобильной разработке; основы работы с сетью и API; принципы работы с базами данных на мобильных платформах; платформы по кроссплатформенной разработке, таких как Flutter, React Native или MAUI.	Раздел 1. Основы информационной безопасности;	5	15,16,17, 29	Тестовые задания закрытого типа
	Умения: разрабатывать программный код; отлаживать приложения на различных устройствах; работать с системами контроля версий; использовать паттерны проектирования; осуществлять тестирование кода; производить рефакторинг; интегрировать приложения с облачными сервисами	Раздел 1. Основы информационной безопасности;	5	47	Задания с развернутым ответом
	Навыки: разработки модулей программного обеспечения для мобильных платформ;	Раздел 1. Основы информационной безопасности;	5	55	Задания с развернутым ответом

	разработки многопоточных приложений; оптимизации производительности приложений; работы с интеграцией сторонних библиотек				
ПК 3.2 Проектировать и разрабатывать пользовательский интерфейс и пользовательский опыт.	**Знания:** принципы дизайна пользовательского интерфейса (UI) и пользовательского опыта (UX); основы графического дизайна и типографики; гайдлайны и стандарты для создания интерфейсов на платформах iOS и Android; принципы адаптивного дизайна; основы работы с векторной и растровой графикой; процесс проектирования интерфейса от идеи до реализации; основные принципы дизайна пользовательского интерфейса, таких как иерархия информации, цветовая гамма, типографика и композиция; психологию пользователей и их потребности при взаимодействии с веб-приложениями; современные тенденции в дизайне пользовательского интерфейса и пользовательского опыта; основные принципы разработки адаптивного и доступного пользовательского интерфейса; основные технологии веб-разработки, такие как HTML, CSS и JavaScript	Раздел 1. Основы информационной безопасности;	5	18,19,30, 36	Тестовые задания закрытого типа
	Умения: создавать интуитивно понятные и легко навигируемые интерфейсы; использовать анимацию и переходы для улучшения пользовательского опыта;	Раздел 1. Основы информационной безопасности;	5	48	Задания с развернутым ответом

	оптимизировать интерфейс для работы на разных экранах и устройствах; интегрировать элементы пользовательского интерфейса с серверной частью или базой данных приложения; анализировать пользовательские данные и обратную связь для улучшения UX; разрабатывать макеты и прототипы приложений; владеть инструментами дизайна интерфейса; глубоко понимать принципы дизайна пользовательского интерфейса и пользовательского опыта; проводить пользовательские исследования, включая создание опросов, интервью с пользователями и анализ данных; работать с прототипированием и созданием макетов пользовательского интерфейса; работать в команде и эффективно взаимодействовать с разработчиками и менеджерами проектов.				
	Навыки: создания пользовательских интерфейсов с использованием инструментов и библиотек, таких как UIKit (iOS) и Android XML (Android); разработки адаптивных и мультирезолюционных интерфейсов; тестирования пользовательского опыта; проведения юзабилити-тестов; проектирование пользовательского интерфейса (UI) и пользовательского опыта	Раздел 1. Основы информационной безопасности;	5	56	Задания с развернутым ответом

	(UX) для различных веб-приложений и сайтов; разработки прототипов и макетов пользовательского интерфейса с использованием инструментов, таких как Sketch, Adobe XD или Figma; проведения пользовательских исследований, включая сбор обратной связи от пользователей и анализ конкурентного рынка; создания дизайн-системы и стайл-гайдов для обеспечения единообразия визуального стиля и пользовательского опыта; тестирования и итеративное улучшения пользовательского интерфейса на основе обратной связи пользователей.				
ПК 3.3. Проектировать и разрабатывать базы данных для мобильных платформ	**Знания:** основы реляционных баз данных; основы NoSQL и графовых баз данных; принципы работы с транзакциями; основы безопасности и шифрования данных; принципы работы с миграциями баз данных; основы работы с асинхронными операциями; основные принципы работы с базами данных в программном обеспечении для мобильных платформ; различные типы баз данных, таких как реляционные, NoSQL и графовые базы данных; современные тенденции в разработке мобильных приложений с использованием баз данных; основные принципы проектирования баз данных для эффективного хранения и обработки данных в мобильных приложениях;	Раздел 1. Основы информационной безопасности;	5	20,21,31, 37	Тестовые задания закрытого типа

	основные технологии разработки мобильных приложений, таких как Java, Kotlin, Swift или React Native, для работы с базами данных.				
	Умения: проектировать и оптимизировать базы данных; выполнять CRUD (Create, Read, Update, Delete) операции; обеспечивать синхронизацию данных между устройствами; работать с кэшированием данных; обрабатывать конфликты данных в распределенных системах; работать с многозадачностью и потоками данных; владеть языком SQL для работы с базами данных; глубоко понимать принципы работы с базами данных в программном обеспечении для мобильных платформ; создавать и оптимизировать структуру баз данных для хранения и обработки данных в мобильных приложениях; работать с ORM (Object-Relational Mapping) инструментами для более удобного взаимодействия с базами данных; обеспечивать безопасность и защиту данных при работе с базами данных в мобильных **приложениях.**	Раздел 1. Основы информационной безопасности;	5	49	Задания с развернутым ответом
	Навыки: работы с SQLite и другими СУБД для мобильных платформ; разработки эффективных схем баз данных; работы с NoSQL и графовыми базами данных; работы с ORM (Object-Relational Mapping) инструментами; работы с асинхронным доступом к данным; разработки функций и возможностей для работы	Раздел 1. Основы информационной безопасности;	5	57	Задания с развернутым ответом

	с базами данных в программном обеспечении для мобильных платформ; создания интерфейсов для работы с базами данных, включая CRUD операции (создание, чтение, обновление, удаление данных); интеграции баз данных в пользовательский интерфейс приложений для удобного доступа и управления данными;оптимизации работы с базами данных для обеспечения высокой производительности и эффективного использования ресурсов устройства.				
ПК 3.5. Выполнять тестирование и отладку программного обеспечения.	**Знания:** основы тестирования программного обеспечения; виды тестирования (функциональное, нагрузочное, UI-тестирование и др.); принципы работы с отладчиками; основы continuous integration и continuous delivery (CI/CD); основы создания тестовых сценариев; принципы и методы тестирования программного обеспечения для мобильных платформ; особенности отладки программного обеспечения для мобильных платформ; принципы работы эмуляторов и симуляторов; методы аппаратного и программного тестирования	Раздел 1. Основы информационной безопасности;	5	22,23,32, 38	Тестовые задания закрытого типа
	Умения: разрабатывать и запускать тестовые сценарии для проверки функциональности программного обеспечения для	Раздел 1. Основы информационной безопасности;	5	50	Задания с развернутым ответом

	мобильных платформ; выявлять и исправлять ошибки и несоответствия в работе ПО; проводить аппаратное и программное тестирование программного обеспечения для мобильных платформ; использовать инструменты анализа и отладки для поиска и устранения проблем; работать с инструментами для обнаружения и исправления ошибок; работать с отчетами о тестировании; анализировать и устранять утечки памяти				
	Навыки: создания тестовых сценариев и единиц тестирования для мобильных платформ; отладки и анализа проблем в работе мобильных приложений; использования инструментов и оборудования для тестирования программных компонентов мобильных платформ; работы с эмуляторами и симуляторами для программного обеспечения мобильных платформ	Раздел 1. Основы информационной безопасности;	5	58	Задания с развернутым ответом
ПК 3.7. Осуществлять защиту данных в мобильных приложениях.	**Знания:** основные угрозы безопасности мобильных приложений; принципы криптографии и шифрования данных; стандарты и протоколы безопасности, такие как HTTPS, OAuth и OpenID Connect; законодательные и регуляторные требования к защите данных, включая GDPR и HIPAA; основные принципы безопасности информации и методов ее защиты; стандартные	Раздел 1. Основы информационной безопасности;	5	24,25,39, 40	Тестовые задания закрытого типа

	криптографические алгоритмы для шифрования данных; методы аутентификации и авторизации пользователей, таких как OAuth или JWT; многоуровневые механизмы контроля доступа к данным; методы тестирования на уязвимости безопасности и опыт применения инструментов для их обнаружения; принципы обеспечения безопасности передачи данных по сети; законодательство и регуляции в области защиты данных и умение применять их в практической разработке мобильных приложений.				
	Умения: разрабатывать и реализовывать меры безопасности; реализовывать хэширование паролей, сессионные токены и двухфакторную аутентификацию; осуществлять валидацию данных, поступающих от пользователей; разрабатывать политику доступа и права пользователей к данным и функциональности приложения; реализовывать меры контроля доступа и аудита для отслеживания действий пользователей и обнаружения несанкционированных действий.	Раздел 1. Основы информационной безопасности;	5	51	Задания с развернутым ответом
	Навыки: разработки безопасных методов аутентификации и авторизации пользователей; обработки и хранения конфиденциальных данных; отслеживания и обработки уязвимостей	Раздел 1. Основы информационной безопасности;	5	59	Задания с развернутым ответом

	безопасности; использования шифрования для защиты данных в покое и в движении; использования шифрования данных для защиты конфиденциальной информации, такой как пароли, персональные данные пользователей и другие чувствительные данные; реализации механизмов аутентификации и авторизации для обеспечения доступа только авторизованным пользователям; применения механизмов хеширования для защиты паролей пользователей от несанкционированного доступа; обеспечения безопасности передачи данных между клиентскими устройствами и серверами с использованием протоколов шифрования, таких как SSL/TLS; разработки механизмов контроля доступа к данным, чтобы предотвратить несанкционированное чтение, изменение или удаление данных; проектирования и реализации систем резервного копирования и восстановления данных для обеспечения их сохранности в случае сбоев или потери устройства; тестирования приложений на уязвимости безопасности, такие как SQL-инъекции, межсайтовые сценарии и другие уязвимости, и принятие мер по их устранению; соблюдение законодательства и регуляций в области защиты данных				

3.2 Содержание оценочных средств.

*Часть 1. База тестовых вопросов **закрытого типа***

1. *Прочитайте задние, среди предложенных вариантов выберите правильные ответы. Как называется свойство информации, гарантирующее, что доступ к ней могут получить только авторизованные пользователи?*

1. Целостность
2. Конфиденциальность
3. Доступность
4. Достоверность

2. Прочитайте задние, среди предложенных вариантов выберите правильные ответы. К какому типу угроз относится преднамеренное уничтожение резервных копий данных системным администратором?

1. Внутренняя преднамеренная
2. Внутренняя непреднамеренная
3. Внешняя преднамеренная
4. Внешняя непреднамеренная

3. Прочитайте задние, среди предложенных вариантов выберите правильные ответы. Какой нормативно-правовой акт РФ является основным в сфере защиты персональных данных?

1. ФЗ-149 «Об информации, информационных технологиях и о защите информации»
2. ФЗ-152 «О персональных данных»
3. ФЗ-187 «О безопасности критической информационной инфраструктуры РФ»
4. Уголовный кодекс РФ (глава 28)

4. Прочитайте задние, среди предложенных вариантов выберите правильные ответы. Что из перечисленного относится к программно-техническим мерам защиты информации?

1. Разработка регламента смены паролей
2. Установка межсетевого экрана
3. Проведение инструктажа для сотрудников
4. Заключение договора о неразглашении

5. Прочитайте задние, среди предложенных вариантов выберите правильные ответы. Как называется вредоносная программа, которая маскируется под легитимное программное обеспечение, но выполняет скрытые деструктивные функции?

1. Компьютерный вирус
2. Сетевой червь
3. Троянская программа
4. Программа-вымогатель

6. Прочитайте задние, среди предложенных вариантов выберите правильные ответы. Какая атака направлена на переполнение буфера памяти или сетевого канала легитимного сервиса с целью вызвать его отказ в обслуживании?

1. Phishing
2. Man-in-the-Middle (MitM)
3. DoS / DDoS
4. Brute Force

7. Прочитайте задние, среди предложенных вариантов выберите правильные ответы. Какое шифрование использует один и тот же секретный ключ как для кодирования, так и для декодирования информации?

1. Асимметричное
2. Симметричное
3. Хеширование
4. Стеганография

8. Прочитайте задние, среди предложенных вариантов выберите правильные ответы. Что проверяет процесс аутентификации пользователя?

1. Права доступа к конкретному файлу
2. Подлинность предъявленного идентификатора (пароля, биометрии)
3. Уникальное имя (логин) в системе
4. Регистрацию пользователя в журнале событий

9. Прочитайте задние, среди предложенных вариантов выберите правильные ответы. Какой протокол обеспечивает защищенное (зашифрованное) удаленное управление операционной системой через консоль?

1. Telnet
2. SSH
3. HTTP
4. FTP

10. Прочитайте задние, среди предложенных вариантов выберите правильные ответы. Как называется метод социальной инженерии, основанный на массовой рассылке поддельных электронных писем с целью кражи учетных данных?

1. Фишинг
2. Смишинг
3. Вишинг
4. Скимминг

11. Прочитайте задние, среди предложенных вариантов выберите правильные ответы. Для чего используется функция криптографического хеширования?

1. Для обратимого шифрования больших файлов
2. Для проверки целостности данных и хранения паролей в скрытом виде
3. Для генерации открытых ключей
4. Для распределения прав доступа

12. Прочитайте задние, среди предложенных вариантов выберите правильные ответы. Какое аппаратное устройство или программный модуль контролирует и фильтрует входящий и исходящий сетевой трафик на основе заданных правил?

1. Маршрутизатор
2. Прокси-сервер
3. Межсетевой экран (Брандмауэр)
4. Концентратор

13. *Прочитайте задние, среди предложенных вариантов выберите правильные ответы.* Что гарантирует применение электронной цифровой подписи (ЭЦП)?

1. Конфиденциальность содержимого документа
2. Авторство и неизменность (целостность) документа после подписания
3. Скорость передачи документа по сети
4. Автоматическое резервное копирование

14. *Прочитайте задние, среди предложенных вариантов выберите правильные ответы.* Какая технология позволяет объединить несколько физических жестких дисков в один логический элемент для повышения надежности и/или производительности?

1. DMZ
2. RAID
3. VLAN
4. VPN

15. *Прочитайте задние, среди предложенных вариантов выберите правильные ответы.* Какой класс средств защиты информации предназначен для обнаружения и блокирования несанкционированных действий внутри корпоративной сети в реальном времени?

1. DLP-системы
2. IDS / IPS-системы
3. SIEM-системы
4. Антивирусы общего назначения

16. *Прочитайте задние, среди предложенных вариантов выберите правильные ответы.* Какой тип резервного копирования сохраняет только те файлы, которые изменились со времени последнего полного резервного копирования?

1. Дифференциальный (разностный)
2. Инкрементный (приращаемый)
3. Зеркальный
4. Выборочный

17. *Прочитайте задние, среди предложенных вариантов выберите правильные ответы.* Какая модель управления доступом основана на присвоении уровней конфиденциальности информации (например, «секретно») и уровней допуска пользователям?

1. Дискреционная (избирательная)
2. Мандатная (принудительная)
3. Ролевая
4. Контекстная

18. *Прочитайте задние, среди предложенных вариантов выберите правильные ответы.* Как называется защищенный виртуальный туннель, создаваемый поверх незащищенной сети (Интернет) для безопасного подключения удаленных сотрудников?

1. VLAN
2. DMZ
3. VPN
4. NAT

19. *Прочитайте задние, среди предложенных вариантов выберите правильные ответы.* Что из перечисленного является примером двухфакторной аутентификации?

1. Ввод сложного пароля, состоящего из букв и цифр
2. Ввод пароля и последующий ввод одноразового кода из SMS
3. Сканирование отпечатка пальца два раза подряд
4. Ввод логина и кодового слова

20. *Прочитайте задние, среди предложенных вариантов выберите правильные ответы.* Какая атака основана на перехвате и подмене данных в канале связи между двумя легитимными участниками сети без их ведома?

1. SQL-инъекция

2. Атака «человек посередине» (Man-in-the-Middle)
3. Cross-Site Scripting (XSS)
4. Переполнение буфера

21. *Прочитайте задние, среди предложенных вариантов выберите правильные ответы.* В каком документе организации прописываются общие цели, принципы, правила и требования в области обеспечения безопасности данных?

1. Должностная инструкция системного администратора
2. Политика информационной безопасности
3. Техническое задание на закупку серверов
4. Сетевая топология компании

22. *Прочитайте задние, среди предложенных вариантов выберите правильные ответы.* Какая служба отвечает за централизованное управление учетными записями, компьютерами и правами доступа в инфраструктуре Windows Server?

1. DHCP
2. DNS
3. Active Directory (AD)
4. IIS

23. *Прочитайте задние, среди предложенных вариантов выберите правильные ответы.* Как называется изолированный сегмент сети, где располагаются общедоступные серверы (например, веб-сайт компании), защищающий внутреннюю корпоративную сеть от внешних угрозы?

1. VPN
2. NAT
3. Демилитаризованная зона (DMZ)
4. Прокси-зона

24. *Прочитайте задние, среди предложенных вариантов выберите правильные ответы.* Какое программное обеспечение используется для предотвращения утечек конфиденциальной информации за пределы корпоративной сети организации?

1. SIEM
2. DLP
3. ИБП (UPS)
4. Антивирус

25. *Прочитайте задние, среди предложенных вариантов выберите правильные ответы.* Как называется специализированное устройство (или программное обеспечение), которое анализирует сетевые пакеты и системные логи для обнаружения подозрительной активности и автоматического предотвращения сетевых атак?

1. Прокси-сервер
2. IPS (Система предотвращения вторжений)
3. Концентратор (Хаб)
4. DLP-система

26. *Прочитайте текст и установите последовательность*.
Установите правильную последовательность этапов классического процесса аутентификации и предоставления доступа пользователю в операционную систему:
а) Авторизация (предоставление прав на основе полномочий)
б) Идентификация (ввод логина / предъявление имени)
в) Аутентификация (проверка пароля или токена)

27. *Прочитайте текст и установите последовательность*.
Установите правильный алгоритм действий системного администратора при обнаружении активного вирусного заражения одного из компьютеров в локальной сети:
а) Изоляция зараженного компьютера от локальной сети (отключение сетевого кабеля/Wi-Fi)
б) Проведение полного антивирусного сканирования и лечение/удаление вредоносного ПО
в) Фиксация инцидента в журнале и анализ причин заражения
г) Проверка обновлений антивирусных баз на сервере администрирования
28. *Прочитайте текст и установите последовательность*.
Расположите этапы жизненного цикла инцидента информационной безопасности в логическом порядке согласно международным стандартам:
а) Сдерживание и локализация угрозы
б) Обнаружение и регистрация инцидента
в) Искоренение источника и восстановление систем
г) Анализ извлеченных уроков и подготовка отчетов
29. *Прочитайте текст и установите последовательность*.
Расположите уровни эталонной модели OSI в порядке возрастания (от физического уровня к прикладному):
а) Сетевой
б) Физический
в) Прикладной
г) Транспортный
30. *Прочитайте текст и установите последовательность*.
Расположите типы паролей в порядке увеличения их стойкости к атакам методом перебора (Brute Force) при условии одинаковой длины:
а) Пароль, состоящий только из строчных букв
б) Пароль, состоящий из букв разного регистра, цифр и специальных символов
в) Пароль, состоящий только из цифр
31. *Прочитайте текст и установите последовательность*.
Установите правильную последовательность действий при создании инфраструктуры открытых ключей (PKI) для шифрования переписки между двумя пользователями (Абонент А и Абонент Б):
а) Абонент А шифрует сообщение открытым ключом Абонента Б
б) Абонент Б генерирует пару ключей (открытый и закрытый)
в) Абонент Б передает свой открытый ключ Абоненту А по открытым каналам связи
г) Абонент Б расшифровывает полученное сообщение своим закрытым ключом
32. *Прочитайте текст и установите последовательность*.
Установите хронологическую последовательность действий злоумышленника при реализации целевой кибератаки (Cyber Kill Chain) на инфраструктуру организации:
а) Разведка и сбор информации о целях/сотрудниках
б) Закрепление в системе и повышение привилегий
в) Доставка вредоносного ПО (например, через фишинговое письмо)
г) Эксплуатация уязвимости инфраструктуры
33. *Прочитайте текст и установите соответствие.* Установите соответствие между вредоносными программами и их основными особенностями:

Программы:	Особенности:

1. Компьютерный вирус	А) Самостоятельно распространяется по сетевым каналам и уязвимостям без участия пользователя
2. Сетевой червь	Б) Шифрует файлы на диске и требует выкуп за ключ дешифрования
3. Программа-вымогатель	В) Внедряет свой код в другие исполняемые файлы и требует для запуска действий пользователя

1	2	3

34. *Прочитайте текст и установите соответствие.* Установите соответствие между базовыми понятиями информационной безопасности и их определениями:

Понятия:	Определения:
1. Угроза	А) Мера вероятности реализации угрозы и масштаба ее возможных негативных последствий
2. Уязвимость	Б) Потенциальная возможность нарушения безопасности информационной системы
3. Риск	В) Недостаток или слабое место в программном обеспечении или архитектуре сети

1	2	3

35. *Прочитайте текст и установите соответствие.*

Атаки:	Методы защиты:
1. DDoS-атака	А) Использование сильного шифрования WPA3 и VPN-туннелей
2. Brute Force (перебор паролей)	Б) Фильтрация трафика на уровне провайдера (ограничение частоты запросов, гео-блок)
3. Перехват трафика в сети Wi-Fi	В) Блокировка IP-адреса после нескольких неудачных попыток ввода, использование капчи

1	2	3

36. *Прочитайте текст и установите соответствие.* Установите соответствие между аббревиатурами технологий защиты и их назначением:

Технологии:	Назначение:
1. VPN	А) Логическое сегментирование локальной сети на уровне коммутатора для изоляции трафика
2. DMZ	Б) Построение защищенного шифрованного виртуального канала поверх публичных сетей
3. VLAN	В) Выделенная подсеть для размещения внешних веб-серверов компании

1	2	3

37. *Прочитайте текст и установите соответствие.* Установите соответствие между типами аутентификации и используемыми факторами:

Типы факторов:	Примеры факторов:
1. То, что пользователь знает	А) Аппаратный USB-токен или смарт-карта
2. То, что пользователь имеет	Б) Отпечаток пальца или сетчатка глаза
3. То, кем пользователь является	В) Пароль, PIN-код или графический ключ

1	2	3

38. *Прочитайте текст и установите соответствие.* Установите соответствие между сетевыми протоколами и их номерами стандартных портов:

Протоколы:	Порты:
1. SSH	А) 443
2. HTTPS	Б) 3389
3. RDP	В) 22

1	2	3

39. *Прочитайте текст и установите соответствие.* Установите соответствие между видами резервного копирования и объемом сохраняемых данных:

Виды бэкапа:	Объем данных:
1. Полный (Full)	А) Копируются все данные, изменившиеся только с момента последнего инкрементного (или полного) бэкапа
2. Инкрементный (Incremental)	Б) Копируются абсолютно все выбранные файлы и папки системы
3. Дифференциальный (Differential)	В) Копируются все данные, изменившиеся с момента самого первого полного бэкапа

1	2	3

40. *Прочитайте текст и установите соответствие.* Установите соответствие между законодательными терминами и их сущностями:

Термины:	Сущности:
1. Субъект персональных данных	А) Физическое лицо, к которому относятся эти данные (например, студент или сотрудник)
2. Оператор персональных данных	Б) Любая информация, относящаяся к прямо или косвенно определенному физлицу
3. Персональные данные	В) Государственный орган или юрлицо, организующее и осуществляющее обработку данных

1	2	3

Часть 2. Задания с развернутым ответом

41. *Прочитайте текст и запишите развернутый обоснованный ответ.*
Опишите, из каких основных программно-технических элементов должна состоять защита сетевого периметра коммерческой организации. Объясните назначение каждого элемента.
42. *Прочитайте текст и запишите развернутый обоснованный ответ.*
Проведите сравнительный анализ симметричного и асимметричного шифрования. Укажите главное преимущество и главный недостаток каждого метода.
43. *Прочитайте текст и запишите развернутый обоснованный ответ.*
Сформулируйте «принцип наименьших привилегий» (Least Privilege).
44. *Прочитайте текст и запишите развернутый обоснованный ответ.*
Объяснить механизм реализации сетевой атаки «Человек посередине» (MitM) на примере незащищенного Wi-Fi соединения в общественном месте.
45. *Прочитайте текст и запишите развернутый обоснованный ответ.*
Опишите, что такое фишинг и почему технические средства защиты (антивирусы, межсетевые экраны) не всегда способны защитить организацию от этого типа угроз.
46. *Прочитайте текст и запишите развернутый обоснованный ответ.*
Разработайте оптимальные требования к корпоративной парольной политике для домена Active Directory организации среднего масштаба.
47. *Прочитайте текст и запишите развернутый обоснованный ответ.*
Объясните роль централизованного сбора логов (например, с использованием SIEM-систем) в обеспечении информационной безопасности.
48. *Прочитайте текст и запишите развернутый обоснованный ответ.*
Дайте определение инсайдерским угрозам. Объясните, какие задачи решает DLP-система (Data Loss Prevention) в организации.
49. *Прочитайте текст и запишите развернутый обоснованный ответ.*
Обоснуйте, почему обеспечение информационной безопасности серверного помещения невозможно без мер физической защиты.
50. *Прочитайте текст и запишите развернутый обоснованный ответ.*
В корпоративной сети организации до сих пор используются протоколы передачи данных HTTP, FTP и Telnet. Объясните, какую критическую угрозу безопасности это несет.
51. *Прочитайте текст и запишите развернутый обоснованный ответ.*
Дайте определение понятию «горизонтальное перемещение злоумышленника» (Lateral Movement) внутри сети. Какую роль в предотвращении этой угрозы играет технология VLAN (виртуальные локальные сети).

Часть 3. Задачи

52. Пользователь сообщает, что у него пропал доступ к корпоративному веб-серверу (IP: 192.168.1.50). Напишите последовательность из 3-х базовых консольных команд (утилит) в ОС Windows, с помощью которых системный администратор должен последовательно проверить:
1. Наличие локального IP-адреса на машине пользователя.
2.Сетевую доступность (связность) до веб-сервера на сетевом уровне.
3.Маршрут прохождения пакетов до сервера для поиска точки отказа.

53. В операционной системе Linux системный администратор выполнил команду ls -l для файла shadow_copy.txt и получил следующий вывод:
-rwxr-----[...] root security_group shadow_copy.txt
Определите, какие права (чтение, запись, исполнение) имеют на этот файл:
1.Владелец файла (root).
2.Пользователи, входящие в группу security_group.
3.Все остальные пользователи в системе (остальные/others).
54. Напишите логическое правило для межсетевого экрана (Firewall), которое заблокирует возможность удаленного управления сервером (10.0.0.5) по небезопасному протоколу Telnet для всех узлов внешней сети (0.0.0.0/0), но при этом оставит сервер доступным для обычного веб-трафика (HTTP). В ответе укажите: действие (Action), протокол (Protocol), IP-назначения (Destination IP) и порт назначения (Destination Port).
55. Системному администратору на согласование прислали пароль Admin2026! для технологической учетной записи службы резервного копирования. Соответствует ли этот пароль критериям безопасности? Укажите главный недостаток этого пароля и предложите способ его исправления, если он имеется.
56. Организация делает полный бэкап данных каждую субботу. Объем исходных данных на сервере составляет 500 ГБ и не меняется. Какое минимальное количество терабайт (ТБ) на диске сетевого хранилища (NAS) должен заложить системный администратор, чтобы гарантированно хранить копии за последние 4 недели? (Сжатие и дедупликация данных не используются).
57. Сотрудник офиса обратился к системному администратору со словами: «Я случайно перешел по ссылке из подозрительного письма, у меня на секунду открылось какое-то окно консоли, а теперь компьютер сильно тормозит». Опишите первое и самое незамедлительное действие администратора, которое предотвратит распространение потенциальной угрозы на другие компьютеры сети.
58. Администратор настраивает доступ к новому внутреннему веб-порталу. При переходе в браузере по адресу https://portal.local появляется предупреждение: «Ваше подключение не защищено. Срок действия сертификата истек или он является самоподписанным».
1. Означает ли это, что трафик между пользователем и сервером перестал шифроваться?
2. Какое действие должен предпринять администратор на веб-сервере для устранения этой ошибки?
59. В логах сетевого экрана зафиксирована запись:SRC=192.168.1.15 DST=192.168.1.100 PROTO=TCP SPT=49215 DPT=443 ACTION=ALLOW
Проанализируйте запись и ответьте на вопросы:
1. Какой узел (IP-адрес) инициировал соединение?
2. К какому сетевому сервису (протоколу прикладного уровня) пытались подключиться?

3.3 Ключи и критерии к оцениванию задания

№ задания	Верный ответ	Критерии
1	2	Верный ответ – 3 балла; Неверный ответ или его отсутствие - 0 баллов
2	1	Верный ответ – 3 балла; Неверный ответ или его отсутствие -

		0 баллов
3	2	Верный ответ – 3 балла; Неверный ответ или его отсутствие - 0 баллов
4	2	Верный ответ – 3 балла; Неверный ответ или его отсутствие - 0 баллов
5	3	Верный ответ – 3 балла; Неверный ответ или его отсутствие - 0 баллов
6	3	Верный ответ – 3 балла; Неверный ответ или его отсутствие - 0 баллов
7	2	Верный ответ – 3 балла; Неверный ответ или его отсутствие - 0 баллов
8	2	Верный ответ – 3 балла; Неверный ответ или его отсутствие - 0 баллов
9	2	Верный ответ – 3 балла; Неверный ответ или его отсутствие - 0 баллов
10	1	Верный ответ – 3 балла; Неверный ответ или его отсутствие - 0 баллов
11	2	Верный ответ – 3 балла; Неверный ответ или его отсутствие - 0 баллов
12	3	Верный ответ – 3 балла; Неверный ответ или его отсутствие - 0 баллов
13	2	Верный ответ – 3 балла; Неверный ответ или его отсутствие - 0 баллов
14	2	Верный ответ – 3 балла; Неверный ответ или его отсутствие - 0 баллов
15	2	Верный ответ – 3 балла; Неверный ответ или его отсутствие - 0 баллов
16	1	Верный ответ – 3 балла; Неверный ответ или его отсутствие - 0 баллов
17	2	Верный ответ – 3 балла; Неверный ответ или его отсутствие - 0 баллов
18	3	Верный ответ – 3 балла; Неверный ответ или его отсутствие - 0 баллов
19	2	Верный ответ – 3 балла; Неверный ответ или его отсутствие - 0 баллов
20	2	Верный ответ – 3 балла; Неверный ответ или его отсутствие - 0 баллов

21	2	Верный ответ – 3 балла; Неверный ответ или его отсутствие - 0 баллов
22	3	Верный ответ – 3 балла; Неверный ответ или его отсутствие - 0 баллов
23	3	Верный ответ – 3 балла; Неверный ответ или его отсутствие - 0 баллов
24	2	Верный ответ – 3 балла; Неверный ответ или его отсутствие - 0 баллов
25	2	Верный ответ – 3 балла; Неверный ответ или его отсутствие - 0 баллов
26	бва	Верный ответ – 3 балла; Неверный ответ или его отсутствие - 0 баллов
27	агбв	Верный ответ – 3 балла; Неверный ответ или его отсутствие - 0 баллов
28	бавг	Верный ответ – 3 балла; Неверный ответ или его отсутствие - 0 баллов
29	багв	Верный ответ – 3 балла; Неверный ответ или его отсутствие - 0 баллов
30	ваб	Верный ответ – 3 балла; Неверный ответ или его отсутствие - 0 баллов
31	бваг	Верный ответ – 3 балла; Неверный ответ или его отсутствие - 0 баллов
32	авгб	Верный ответ – 3 балла; Неверный ответ или его отсутствие - 0 баллов
33	1-В, 2-А, 3-Б	Верный ответ – 3 балла; Неверный ответ или его отсутствие - 0 баллов
34	1-Б, 2-В, 3-А	Верный ответ – 3 балла; Неверный ответ или его отсутствие - 0 баллов
35	1-Б, 2-В, 3-А	Верный ответ – 3 балла; Неверный ответ или его отсутствие - 0 баллов
36	1-Б, 2-В, 3-А	Верный ответ – 3 балла; Неверный ответ или его отсутствие - 0 баллов
37	1-В, 2-А, 3-Б	Верный ответ – 3 балла; Неверный ответ или его отсутствие - 0 баллов
38	1-В, 2-А, 3-Б	Верный ответ – 3 балла; Неверный ответ или его отсутствие - 0 баллов
39	1-Б, 2-А, 3-В	Верный ответ – 3 балла;

		Неверный ответ или его отсутствие - 0 баллов
40	1-А, 2-В, 3-Б	Верный ответ – 3 балла; Неверный ответ или его отсутствие - 0 баллов
41	Межсетевой экран: фильтрация входящего/исходящего трафика на основе правил для блокировки несанкционированного доступа. Система предотвращения вторжений: глубокий анализ пакетов в реальном времени, поиск сигнатур атак и их автоматическая блокировка. Демилитаризованная зона: изолированный сегмент сети для публичных серверов, защищающий внутреннюю сеть от компрометации в случае их взлома. VPN-шлюз: создание защищенного зашифрованного туннеля для безопасного подключения удаленных сотрудников через Интернет.	Верный ответ – 10 балла; Неверный ответ или его отсутствие - 0 баллов
42	Симметричное шифрование (один ключ для шифрования и дешифрования): Преимущество: Высокая скорость работы, низкая нагрузка на процессор. Недостаток: Проблема безопасной передачи секретного ключа участникам. Асимметричное шифрование (пара из открытого и закрытого ключей): Преимущество: Нет необходимости передавать секретный (закрытый) ключ по сети. Недостаток: Низкая скорость работы из-за сложных математических вычислений.	Верный ответ – 10 балла; Неверный ответ или его отсутствие - 0 баллов
43	Суть принципа: Предоставление пользователю или процессу только того минимального уровня прав доступа, который необходим для выполнения текущих рабочих обязанностей. Минимизирует ущерб от ошибок сотрудников или умышленного саботажа, а также локализует заражение вредоносным ПО, не позволяя вирусам получить административный доступ к ОС.	Верный ответ – 10 балла; Неверный ответ или его отсутствие - 0 баллов
44	1. Злоумышленник создает поддельную беспроводную сеть с легитимным именем. 2. Жертва добровольно подключается к ней, после чего весь её сетевой трафик физически проходит через устройство хакера. 3. С помощью анализаторов пакетов злоумышленник перехватывает передаваемые в открытом виде логины, пароли и файлы сессий.	Верный ответ – 10 балла; Неверный ответ или его отсутствие - 0 баллов
45	Фишинг — метод социальной инженерии, направленный на обман пользователя с целью кражи паролей/данных или запуска вируса под видом легитимного вложения. Атака направлена на «человеческий фактор». Если пользователь сам вводит пароль на поддельной странице, технические средства защиты расценивают это как легитимное действие авторизованного владельца.	Верный ответ – 10 балла; Неверный ответ или его отсутствие - 0 баллов
46	Длина: от 12 символов для пользователей, от 14–16 — для администраторов.	Верный ответ – 10 балла; Неверный ответ или его отсутствие - 0 баллов

	Сложность: обязательное сочетание заглавных, строчных букв, цифр и спецсимволов. Блокировка: закрытие учетной записи на 15–30 минут после 3–5 неверных попыток ввода. История: запрет на повторение последних 10–12 использованных паролей.	
47	При взломе хакер удаляет локальные логи на сервере. При централизованном сборе логи мгновенно улетают на защищенный сервер SIEM, где остаются целыми. SIEM сопоставляет разрозненные мелкие события с разных устройств в единую цепочку атаки в реальном времени.	Верный ответ – 10 балла; Неверный ответ или его отсутствие - 0 баллов
48	Инсайдерские угрозы — угрозы ИБ, исходящие от сотрудников организации, имеющих легитимный доступ к системам, но использующих его во вред. Задачи DLP: Предотвращение утечек данных наружу. Решается путем мониторинга и блокировки каналов: веб-почты.	Верный ответ – 10 балла; Неверный ответ или его отсутствие - 0 баллов
49	Без физической защиты программная безопасность теряет смысл. Имея доступ к оборудованию, злоумышленник может: 1. Извлечь жесткие диски или загрузить сервер с флешки для обхода паролей ОС. 2. Установить аппаратные закладки. 3. Физически уничтожить инфраструктуру.	Верный ответ – 10 балла; Неверный ответ или его отсутствие - 0 баллов
50	Критическая угроза: Данные протоколы передают всю информацию через сеть в открытом, незашифрованном виде. Последствие: Трафик легко перехватывается простейшими анализаторами пакетов, что ведет к полной компрометации сети.	Верный ответ – 10 балла; Неверный ответ или его отсутствие - 0 баллов
51	Горизонтальное перемещение — продвижение хакера внутри сети от одного скомпрометированного ПК к соседним машинам и серверам с целью поиска критических данных. Роль VLAN: Логически разделяет сеть на изолированные сегменты. Компьютеры из разных VLAN не видят друг друга напрямую, а их трафик фильтруется на межсетевом экране, что блокирует хакеру возможность распространять атаку по сети.	Верный ответ – 10 балла; Неверный ответ или его отсутствие - 0 баллов
52	1. ipconfig — для проверки локальных настроек и наличия IP-адреса на машине. 2. ping 192.168.1.50 — для проверки доступности сервера на сетевом уровне. 3. tracert 192.168.1.50 — для трассировки маршрута и поиска узла, на котором обрывается пакет.	Верный ответ – 30 баллов; 1 фактическая ошибка – 20 баллов 2 фактические ошибки – 10 баллов более 2 фактических ошибок или ответ отсутствует - 0 баллов
53	1. Владелец (root): полные права — чтение, запись, исполнение (rwx) 2. Группа (security_group): только право на чтение (r--). 3. Остальные (others): нет никаких прав доступа (---).	Верный ответ – 30 баллов; 1 фактическая ошибка – 20 баллов 2 фактические ошибки – 10 баллов более 2 фактических ошибок или ответ отсутствует - 0 баллов
54	Действие: Запретить / Блокировать Протокол: TCP.	Верный ответ – 30 баллов; 1 фактическая ошибка – 20 баллов

	IP-назначения: 10.0.0.5. Порт назначения: 23	2 фактические ошибки – 10 баллов более 2 фактических ошибок или ответ отсутствует - 0 баллов
55	Не соответствует. Содержит словарное слово (Admin), текущий год (2026) и предсказуемый спецсимвол, что делает его уязвимым. Способ исправления: Сгенерировать случайную последовательность символов разного регистра без явной логики.	Верный ответ – 30 баллов; 1 фактическая ошибка – 20 баллов 2 фактические ошибки – 10 баллов более 2 фактических ошибок или ответ отсутствует - 0 баллов
56	Расчет: 4 копии * 500 ГБ = 2000 ГБ. Минимальное количество ТБ: 2 ТБ (при коммерческом расчете 1 ТБ = 1000 ГБ) или 1.95 ТБ (при системном расчете 2000 ГБ / 1024). Для закупки закладывается диск емкостью 2 ТБ.	Верный ответ – 30 баллов; 1 фактическая ошибка – 20 баллов 2 фактические ошибки – 10 баллов более 2 фактических ошибок или ответ отсутствует - 0 баллов
57	Физически изолировать ПК от сети — выдернуть сетевой кабель и/или отключить Wi-Fi. Это заблокирует потенциальному вирусу возможность атаковать другие узлы и серверы в локальной сети.	Верный ответ – 30 баллов; 1 фактическая ошибка – 20 баллов 2 фактические ошибки – 10 баллов более 2 фактических ошибок или ответ отсутствует - 0 баллов
58	Нет, не означает. Трафик по-прежнему шифруется. Ошибка говорит о том, что браузер не может доверять подлинности издателя сертификата. Необходимо обновить истекший сертификат либо выпустить новый валидный сертификат, подписанный доверенным в организации Центром сертификации, и установить его на веб-сервер.	Верный ответ – 30 баллов; 1 фактическая ошибка – 20 баллов 2 фактические ошибки – 10 баллов более 2 фактических ошибок или ответ отсутствует - 0 баллов
59	Узел-инициатор: 192.168.1.15 (SRC — Source IP).Сетевой сервис: HTTPS, так как порт назначения равен 443.	Верный ответ – 30 баллов; 1 фактическая ошибка – 20 баллов 2 фактические ошибки – 10 баллов более 2 фактических ошибок или ответ отсутствует - 0 баллов

4. ПОРЯДОК ПРОВЕДЕНИЯ И КРИТЕРИИ ОЦЕНИВАНИЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

Промежуточная аттестация обучающихся осуществляется по пятибалльной системе оценивания

Экзамен, зачет, зачет с оценкой и пр. состоит из двух частей:

1 часть – студент решает 10 тестовых вопросов закрытого типа, выбранных случайным образом. Продолжительность – *15 минут.*

Максимальное количество баллов за выполнение задания – 30 баллов

2 часть – студент решает задание с развернутым ответом, выбранное случайным образом. Всего 4 тестовых вопроса, выбранных случайным образом. Продолжительность – *50 минут.* Максимальное количество баллов за выполнение задания – 40 баллов

3 часть – студент решает задачу, выбранную случайным образом. Продолжительность – 25 минут. Максимальное количество баллов за выполнение задания – 30 баллов

Всего заданий – 15.

Максимальный балл – *100 баллов:*

0-49 баллов - неудовлетворительно (оценка 2) (не зачтено);

50-69 баллов - удовлетворительно (оценка 3) (зачтено);

70-90 баллов - хорошо (оценка 4) (зачтено);

91-100 баллов - отлично (оценка 5) (зачтено).

Общее время выполнения работы – 2 ак.ч.

Особенности проведении процедуры оценивания результатов обучения инвалидов и лиц с ограниченными возможностями здоровья обозначены в рабочей программе дисциплины (модуля).