МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

«КАРАЧАЕВО-ЧЕРКЕССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИМЕНИ У.Д. АЛИЕВА»

Факультет экономики и управления

УТВЕРЖДАЮ
И. о. проректора по УР
М. Х. Чанкаев
«29» апреля 2026 г., протокол № 7

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

(наименование дисциплины (модуля)

Направление подготовки
09.03.03 – Прикладная информатика
(шифр, название направления)

Квалификация выпускника
Бакалавр

ТЕСТОВЫЕ ВОПРОСЫ «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»

Компетенции:

ОПК-3 Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности;

ОПК-4 Способен участвовать в разработке стандартов, норм и правил, а также технической документации, связанной с профессиональной деятельностью;

Номер задания	Правильный ответ	Содержание вопроса	Компетенция	Время выполнения (мин.)
1	2 Обоснование: Для обеспечения безопасности работы сотрудников необходимо внедрить многофакторную аутентификацию, которая значительно снижает риск несанкционированного доступа. Установка и регулярное обновление антивирусного программного обеспечения помогает защитить корпоративную сеть от различных видов вирусов и вредоносного ПО. Периодическое обновление ПО позволяет устранить уязвимости, используемые злоумышленниками.	**Прочитайте текст, выберите правильный ответ и запишите аргументы, обосновывающие выбор ответа** Какие меры следует предпринять для обеспечения безопасности работы сотрудников в корпоративной сети? Варианты ответов: 1. Отключить все антивирусные программы. 2. Обеспечить многофакторную аутентификацию, установить антивирусное ПО, проводить регулярные обновления. 3. Запретить доступ к корпоративной сети из внеофисных местоположений. 4. Установить пароли на каждый документ.	ОПК3	2 мин
2	3 Обоснование: Политика управления обновлениями	**Прочитайте текст, выберите правильный ответ и запишите аргументы, обосновывающие выбор ответа** Что из перечисленного является основным требованием к политике управления обновлениями программного	ОПК3	2 мин

	должна включать регулярные ежемесячные обновления всех программных средств для поддержания их в актуальном состоянии и устранения уязвимостей. Критические обновления, устраняющие серьезные уязвимости, должны быть установлены в течение 24 часов после их выпуска, чтобы минимизировать риск атак.	обеспечения? Варианты ответов: 1. Установка обновлений раз в год. 2. Обновление ПО исключительно в случае возникновения проблем. 3. Обязательное ежемесячное обновление ПО и установка критических обновлений в течение 24 часов после выпуска патча. 4. Удаление всех обновлений на старых системах.		
3	1 Обоснование: Управление рисками информационной безопасности - это процесс, включающий оценку потенциальных рисков, их минимизацию посредством внедрения мер защиты, а также периодический пересмотр и обновление политики безопасности. Это помогает обеспечить актуальность мер защиты и их адаптацию к новым угрозам.	**Прочитайте текст, выберите правильный ответ и запишите аргументы, обосновывающие выбор ответа** Каков основной принцип управления рисками информационной безопасности? Варианты ответов: 1. Оценить и минимизировать риски, внедрить соответствующие меры защиты и периодически пересматривать политику безопасности. 2. Игнорировать возможные риски. 3. Разработать политику на основе инцидентов, что произошли. 4. Полностью полагаться на самостоятельное обучение сотрудников.	ОПК3	1 мин
4	4 Обоснование: Для обеспечения безопасного	**Прочитайте текст, выберите правильный ответ и запишите аргументы, обосновывающие выбор ответа** Какие меры необходимо принять для обеспечения безопасного удаленного доступа сотрудников к	ОПК3	1 мин

	удаленного доступа важно использовать VPN для шифрования передаваемых данных, внедрить двухфакторную аутентификацию для дополнительной защиты при входе и обеспечить шифрование данных на всех этапах. Это помогает предотвратить перехват данных и несанкционированный доступ.	корпоративным ресурсам? Варианты ответов: 1. Позволить удаленный доступ только через общедоступные Wi-Fi сети. 2. Разрешить сотрудникам использовать личные устройства без проверки безопасности. 3. Запретить удаленный доступ полностью. 4. Требовать использование VPN, внедрить двухфакторную аутентификацию и обеспечить шифрование передаваемых данных.		
5	2 Обоснование: Эффективный план реагирования на киберугрозы включает в себя обнаружение атаки и оценку ее серьезности, оповещение соответствующих подразделений и заинтересованных сторон, изоляцию атакованных систем для предотвращения дальнейшего распространения угрозы, восстановление данных из резервных копий, а также последующий анализ инцидента с целью улучшения мер защиты и предотвращения повторных атак.	**Прочитайте текст, выберите правильный ответ и запишите аргументы, обосновывающие выбор ответа** Какие действия включены в план реагирования на киберугрозы? Варианты ответов: 1. Немедленное отключение всех систем. 2. Обнаружение атаки, оценка ее серьезности, оповещение заинтересованных сторон, изоляция атакованных систем, восстановление данных и анализ инцидента. 3. Проведение пресс-конференции. 4. Введение карантина для всех сотрудников.	ОПК3	1 мин
6	1 Обоснование: Политика информационной	**Прочитайте текст, выберите правильный ответ и запишите аргументы, обосновывающие выбор ответа** Какими ключевыми аспектами должна обладать политика информационной безопасности?	ОПК4	2 мин

	безопасности должна учитывать основные аспекты защиты информации: конфиденциальность (защита от несанкционированного доступа), целостность (сохранение данных в неизменном виде), доступность (обеспечение доступа к данным authorized пользователям) и соответствие законодательным требованиям и стандартам. Эти аспекты позволяют создать надежную систему защиты информации, поддерживающую её безопасность и законность.	Варианты ответов: 1. Конфиденциальность, целостность, доступность и соответствие законодательным требованиям. 2. Отсутствие регламентов и открытое использование всех ресурсов. 3. Только конфиденциальностью документов сотрудников. 4. Упрощённое использование системы без паролей.		
7	4 Обоснование: Процесс разработки стандарта информационной безопасности предполагает несколько последовательных шагов: определение целей и задач стандарта, сбор и анализ требований, разработка черновой версии стандарта, ее тестирование, внесение необходимых корректировок на основе полученных данных и утверждение окончательной	**Прочитайте текст, выберите правильный ответ и запишите аргументы, обосновывающие выбор ответа** Какие шаги включаются в процесс разработки стандарта информационной безопасности? Варианты ответов: A) Определение цели, сбор требований, разработка неудобного интерфейса. B) Разработка стандартов без тестирования. C) Сбор требований и прекращение работы. D) Определение целей и задач стандарта, сбор требований, разработка черновой версии, тестирование, внесение изменений и утверждение.	ОПК4	2 мин

	версии стандарта. Это обеспечивает создание обоснованного и проверенного документа, соответствующего потребностям организации и требованиям безопасности.			
8	2 Обоснование: Анализ рисков является ключевым этапом в разработке норм и правил информационной безопасности, так как он позволяет выявить потенциальные угрозы и уязвимости информационных систем. Благодаря этому анализу можно определить, какие меры необходимо принять для минимизации рисков, и разработать соответствующие нормы и правила, обеспечивающие повышенный уровень защиты.	**Прочитайте текст, выберите правильный ответ и запишите аргументы, обосновывающие выбор ответа** Какую роль играет анализ рисков в разработке норм и правил информационной безопасности? Варианты ответов: 1. Анализ рисков не играет роли в разработке норм и правил. 2. Анализ рисков помогает выявить потенциальные угрозы и уязвимости, что позволяет разработать эффективные нормы и правила для их минимизации. 3. Анализ рисков нужен только для определения стоимости. 4. Анализ рисков проводится после разработки всех норм.	ОПК4	1 мин
9	3 Обоснование: Соответствие разработанных стандартов информационной безопасности международным и национальным стандартам является критически важным для обеспечения доверия со стороны	**Прочитайте текст, выберите правильный ответ и запишите аргументы, обосновывающие выбор ответа** Какое значение имеет соответствие разработанных стандартов информационной безопасности международным и национальным стандартам? Варианты ответов: 1. Соответствие стандартам не имеет значения. 2. Важно для создания сложных паролей. 3. Соответствие стандартам обеспечивает доверие со стороны клиентов и партнеров, а также помогает избежать юридических и финансовых санкций. 4. Соответствие стандартам важно, только чтобы	ОПК4	2 мин

	клиентов и партнеров, а также для соблюдения законодательных требований. Это помогает предотвратить юридические и финансовые санкции и способствует созданию надежной системы за щиты данных, признанной на международном уровне.	следовать моде.		
10	1 Обоснование: При разработке технической документации по информационной безопасности необходимо подготовить комплект документов, включающий следующие компоненты: политика информационной безопасности, стандарты, регламентирующие действия и процедуры сотрудников при работе с информацией, нормы и правила использования информационных систем, инструкции по выполнению конкретных задач, и планы реагирования на инциденты. Эта документация обеспечивает комплексный подход к защите	**Прочитайте текст, выберите правильный ответ и запишите аргументы, обосновывающие выбор ответа** Какие документы необходимо подготовить при разработке технической документации по информационной безопасности? Варианты ответов: 1. Полный комплект документации, включающий политику информационной безопасности, стандарты, нормы, процедуры, инструкции и план реагирования на инциденты. 2. Только один документ с общим описанием всех процессов. 3. Комиксы для сотрудников. 4. Документы только для высшего руководства.	. ОПК4	2-3 мин

	информации и помогает поддерживать высокий уровень безопасности организации.			
11	24 Обоснование: При решении стандартных задач профессиональной деятельности с использованием информационно-коммуникационных технологий важно учитывать конфиденциальность данных, чтобы предотвратить утечку информации, а также надежность и целостность передаваемых данных, чтобы обеспечить их неизменность и достоверность. :	**Прочитайте текст, выберите правильные ответы и запишите аргументы, обосновывающие выбор ответов** Какие факторы важно учитывать при решении стандартных задач профессиональной деятельности с применением информационно-коммуникационных технологий? Варианты ответов: 1. Удобство пользователей. 2. Конфиденциальность данных. 3. Изоляция от внешних сетей. 4. Надежность и целостность передаваемых данных. 5. Экономия на информационных системах.	ОПК3	3-5 мин
12	134 Обоснование: Элементы информационно-библиографической культуры, такие как умение создавать и систематизировать библиографические записи, навыки работы с правовыми базами данных и знание методов криптографической защиты, являются ключевыми для	**Прочитайте текст, выберите правильные ответы и запишите аргументы, обосновывающие выбор ответов** Какие аспекты информационно-библиографической культуры способствуют решению задач профессиональной деятельности в области информационной безопасности? Варианты ответов: 1. Умение создавать и систематизировать библиографические записи. 2. Навыки работы с правовыми базами данных. 3. Игнорирование новых технических стандартов. 4. Знание методов криптографической защиты. 5. Пользование только устаревшими источниками информации.	ОПК3	3-5 мин

	решения задач информационной безопасности. Они обеспечивают доступ к актуальной информации, способствуют правовой грамотности и помогают защитить данные.			
13	145 Обоснование: При применении информационно-коммуникационных технологий необходимо обеспечить доступность информации только для авторизованных пользователей, установить и регулярно обновлять антивирусное ПО, а также проектировать сети так, чтобы минимизировать риски вторжений. Это основные требования информационной безопасности, которые помогают защитить данные и системы от различных угроз.	**Прочитайте текст, выберите правильные ответы и запишите аргументы, обосновывающие выбор ответов** Какие требования информационной безопасности важно учитывать при применении информационно-коммуникационных технологий? Варианты ответов: 1. Обеспечение доступности информации только для авторизованных пользователей. 2. Пользование публичными незащищенными Wi-Fi сетями для передачи конфиденциальной информации. 3. Игнорирование обновлений программного обеспечения. 4. Установка антивирусного ПО и его регулярное обновление. 5. Проектирование сетей с учетом минимизации рисков вторжений.	ОПК3	3-5 мин
14	23 Обоснование: Эффективный поиск и использование информационных ресурсов для решения профессиональных	**Прочитайте текст, выберите правильные ответы и запишите аргументы, обосновывающие выбор ответов** Какие методы позволяют эффективно найти и использовать информационные ресурсы для решения профессиональных задач? Варианты ответов: 1. Использование только печатных источников.	ОПК3	3-5 мин

	задач в области информационной безопасности обеспечивается за счет применения специализированных баз данных и электронных библиотек, а также систематического мониторинга научных публикаций и технических отчетов. Это позволяет получить доступ к актуальной и на дежной информации, необходимой для принятия обоснованных решений.	2. Применение специализированных баз данных и электронных библиотек. 3. Систематический мониторинг научных публикаций и технических отчетов. 4. Неучет релевантности и надежности источников. 5. Игнорирование современных методов поиска информации.		
15	15 Обоснование: Для обеспечения информационной безопасности при выполнении профессиональных задач важно применять безопасные протоколы передачи данных, такие как HTTPS, SSL/TLS, а также использовать многофакторную аутентификацию. Эти технологические решения помогают защитить данные от перехвата и несанкционированного доступа, снижая вероятность взломов и утечек информации.	**Прочитайте текст, выберите правильные ответы и запишите аргументы, обосновывающие выбор ответов** Какие технологические решения способствуют обеспечению информационной безопасности при выполнении профессиональных задач? Варианты ответов: 1. Безопасные протоколы передачи данных (например, HTTPS, SSL/TLS). 2. Отключение всех обновлений безопасности. 3. Киберфизические системы. 4. Использование слабых паролей. 5. Многофакторная аутентификация.	ОПК3	3-5 мин
16	234	**Прочитайте текст, выберите правильные ответы и**	ОПК4	3-5 мин

	Обоснование: При разработке стандарта информационной безопасности необходимо учитывать несколько ключевых аспектов: конфиденциальность (защита данных от несанкционированного доступа), целостность (обеспечение неизменности данных), доступность информации для авторизованных пользователей, а также соответствие законодательным и отраслевым требованиям. Это позволяет создать стандарт, обеспечивающий надежную защиту информации и соответствие нормативным актам.	**запишите аргументы, обосновывающие выбор ответов** Какие составляющие следует учитывать при разработке стандарта информационной безопасности? Варианты ответов: 1. Полная свобода действий для пользователей. 2. Конфиденциальность и целостность данных. 3. Доступность информации для авторизованных пользователей. 4. Соответствие законодательным и отраслевым требованиям. 5. Снижение затрат без учета безопасности.		
17	134 Обоснование: Процесс разработки норм и правил информационной безопасности включает следующие этапы: определение целей и задач, сбор и анализ требований, разработка черновой версии, её	**Прочитайте текст, выберите правильные ответы и запишите аргументы, обосновывающие выбор ответов** Какие шаги включаются в процесс разработки норм и правил информационной безопасности? Варианты ответов: 1. Определение целей и задач. 2. Игнорирование требований пользователей. 3. Сбор и анализ требований. 4. Разработка черновой версии и её тестирование. 5. Внедрение без проверки.	ОПК4	3-5 мин

	тестирование, внесение необходимых изменений на основе полученных результатов и утверждение окончательной версии. Эти шаги помогают сформировать нормы и правила, которые эффективны и соответствуют потребностям организации.			
18	234 Обоснование: Анализ рисков играет несколько ключевых ролей в разработке стандартов информационной безопасности: он позволяет выявить потенциальные угрозы и уязвимости, установить приоритеты для защищаемых ресурсов и определить необходимость в различных механизмах защиты. Без анализа рисков невозможно адекватно оценить угрозы и выбрать соответствующие меры защиты.	**Прочитайте текст, выберите правильные ответы и запишите аргументы, обосновывающие выбор ответов** Какие роли выполняет анализ рисков в разработке стандартов информационной безопасности? Варианты ответов: 1. Игнорирование возможных угроз. 2. Выявление потенциальных угроз и уязвимостей. 3. Установление приоритетов для защищаемых ресурсов. 4. Определение необходимости в механизмах защиты. 5. Снижение потребностей пользователей.	ОПК4	3-5 мин

19	135 Обоснование: Соответствие разработанных стандартов международным и национальным нормативам важно по нескольким причинам: оно повышает доверие со стороны клиентов и партнеров, снижает юридические и финансовые риски и увеличивает возможность экспорта продукции. Это обеспечивает конкурентоспособность и соблюдение всех необходимых правовых аспектов, что важно для любой организации.	**Прочитайте текст, выберите правильные ответы и запишите аргументы, обосновывающие выбор ответов** В чем заключается значимость соответствия разработанных стандартов международным и национальным? Варианты ответов: 1. Повышение доверия со стороны клиентов и партнеров. 2. Исключение необходимости учитывать правовые аспекты. 3. Снижение юридических и финансовых рисков. 4. Обеспечение свободы действий для работников. 5. Увеличение возможности экспорта продукции.	ОПК4	3-5 мин
20	1345 Обоснование: Техническая документация по информационной безопасности включает в себя несколько важных документов: политика информационной безопасности, стандарты и нормы, процедуры и инструкции, а также планы реагирования на инциденты. Эти документы обеспечивают комплексный подход к защите информации и соблюдение стандартов безопасности в	**Прочитайте текст, выберите правильные ответы и запишите аргументы, обосновывающие выбор ответов** Какие документы включаются в техническую документацию по информационной безопасности? Варианты ответов: 1. Политика информационной безопасности. 2. Одиночный документ с общим описанием. 3. Стандарты и нормы. 4. Процедуры и инструкции. 5. Планы реагирования на инциденты.	ОПК4	3-5 мин

<table>
<tr><td></td><td>организации.</td><td></td><td></td><td></td></tr>
<tr><td>21</td><td>21543</td><td>Прочитайте текст и установите соответствие между методами защиты информации с соответствующими типами угроз:
<table><tr><td>а) Файрвол (межсетевой экран)
б) Антивирусное ПО
в) Шифрование данных
г) Бэкап (резервное копирование)
д) Многофакторная аутентификация</td><td>1) Вирусы и вредоносное ПО
2) Несанкционированный доступ
3) Взлом паролей
4) Потеря данных
5) Перехват данных в сети</td></tr></table>
Запишите выбранные цифры под соответствующими буквами:<table><tr><td>а</td><td>б</td><td>в</td><td>г</td><td>д</td></tr><tr><td></td><td></td><td></td><td></td><td></td></tr></table></td><td>ОПК3
ОПК4</td><td>2 мин</td></tr>
<tr><td>22</td><td>53142</td><td>Прочитайте текст и установите соответствие стандартов информационной безопасности с их целями
<table><tr><td>а) Защита персональных данных граждан ЕС
б) Управление информационной безопасностью
в) Защита данных держателей платежных карт
г) Защита информации в здравоохранении
д) Меры по управлению безопасностью информации в организациях</td><td>1) PCI-DSS
2) NIST SP 800-53
3) ISO/IEC 27001
4) HIPAA
5) GDPR</td></tr></table>
Запишите выбранные цифры под соответствующими буквами:<table><tr><td>а</td><td>б</td><td>в</td><td>г</td><td>д</td></tr><tr><td></td><td></td><td></td><td></td><td></td></tr></table></td><td>ОПК3
ОПК4</td><td>2 мин</td></tr>
<tr><td>23</td><td>41235</td><td>Прочитайте текст и установите соответствие технологий и типов атак:</td><td>ОПК3
ОПК4</td><td>2 мин</td></tr>
</table>

		а) Система предотвращения вторжений (IPS) б) Антифишинговое ПО в) Система обнаружения вторжений (IDS) г) Шифрование электронной почты д) Контроль доступа к сети (NAC) 1) Фишинг 2) Анализ несанкционированных действий 3) Сниффинг (прослушка сетевого трафика) 4) Обнаружение и блокировка атак в реальном времени 5) Управление доступом по правилам безопасности Запишите выбранные цифры под соответствующими буквами: а: б: в: г: д:		
24	13245	**Прочитайте текст и установите соответствие** процессов управления информационной безопасностью и их функций: а) Управление рисками б) Управление инцидентами в) Контроль доступа г) Обучение пользователей д) Управление активами 1) Определение и минимизация рисков для информационных систем 2) Регулирование прав доступа к информационным ресурсам 3) Реакция и восстановление после инцидентов безопасности 4) Обучение сотрудников принципам и методам информационной безопасности 5) Инвентаризация и защита информационных активов Запишите выбранные цифры под соответствующими буквами: а: б: в: г: д:	ОПК3 ОПК4	2 мин
25	45123	**Прочитайте текст и установите соответствие** видов аудита информационной безопасности и их целей: а) Технический аудит 1) Проверка соответствия международным и		2 мин

		б) Процессный аудит в) Аудит соответствия г) Операционный аудит д) Аудит уязвимостей	национальным стандартам 2) Анализ и улучшение операционных процессов и процедур 3) Обнаружение и устранение уязвимостей в системах 4) Оценка безопасности технических средств и систем 5) Оценка и совершенствование процессов управления безопасностью		
		Запишите выбранные цифры под соответствующими буквами: а б в г д _ _ _ _ _			
26	142536	**Прочитайте текст и установите последовательность.** Установите правильную последовательность шагов для установки и настройки системы антивирусной защиты: 1) Анализ потребностей и выбор антивирусного ПО. 2) Установка антивирусного ПО на серверы и рабочие станции. 3) Проведение первого полного сканирования всех систем. 4) Закупка и лицензирование антивирусного ПО. 5) Настройка параметров сканирования и обновлений. 6) Обучение сотрудников использованию антивирусного ПО. Запишите соответствующую последовательность цифр слева направо: _ _ _ _ _		ОПК3 ОПК4	3 мин
27	465231	**Прочитайте текст и установите последовательность.** Установите правильную последовательность действий по внедрению политики управления паролями.: 1) Обучение сотрудников новым правилам управления паролями 2) Обсуждение и утверждение политики с руководством. 3) Настройка систем для обеспечения соответствия политике. 4) Анализ текущего состояния управления паролями. 5) Создание документа с политикой управления паролями. 6) Разработка требований и правил для паролей		ОПК3 ОПК4	2 мин

		Запишите соответствующую последовательность цифр слева направо: | | | | | |		
28	312654	**Прочитайте текст и установите последовательность.** Расположите действия в правильной последовательности при разработке и внедрении политики конфиденциальности: 1) Разработка ключевых положений политики конфиденциальности. 2) Согласование политики с юридической службой и руководством. 3) Проведение анализа данных, подлежащих защите. 4) Постоянный мониторинг соблюдения политики и обновление при необходимости. 5) Информирование и обучение сотрудников по новым требованиям. 6) Оформление и выпуск официального документа о политике конфиденциальности. Запишите соответствующую последовательность цифр слева направо: | | | | | |	ОПК3 ОПК4	2 мин
29	643251	**Прочитайте текст и установите последовательность.** Установите правильную последовательность действий для внедрения системы управления инцидентами: 1) Тестирование и оценка эффективности системы управления инцидентами. 2) Разработка и утверждение процедур реагирования на инциденты. 3) Настройка и интеграция системы с существующей ИТ-инфраструктурой. 4) Выбор и приобретение программного обеспечения для управления инцидентами. 5) Обучение команды реагирования на инциденты и сотрудников. 6) Определение условий и требований для системы управления инцидентами. Запишите соответствующую последовательность цифр слева направо: | | | | | |	ОПК3 ОПК4	2 мин
30	415362	**Прочитайте текст и установите последовательность.** Расположите действия в правильной последовательности	ОПК3 ОПК4	3 мин

		для проведения аудита информационной безопасности: 1) Составление плана аудита. 2) Предоставление отчета руководству и разработка рекомендаций. 3) Проведение интервью с сотрудниками. 4) Формирование аудиторской группы. 5) Сбор и анализ данных. 6) Документирование результатов аудита. Запишите соответствующую последовательность цифр слева направо: | | | | | |		
31	Основные риски включают несанкционированный доступ, утечку данных и вредоносное ПО. Для минимизации рисков внедряется многофакторная аутентификация, шифрование данных и регулярные обновления антивирусного ПО. Дополнительные меры включают обучение сотрудников и использование систем обнаружения вторжений.	**Прочитайте текст и запишите развернутый обоснованный ответ** Оцените основные риски для информационной системы муниципальной администрации и предложите меры их минимизации.		3 мин
32	План включает этапы обнаружения атаки, оценку ее серьезности, оповещение всех заинтересованных сторон и подразделений. Определяются меры нейтрализации атаки, такие как изоляция атакованных систем, восстановление данных из резервных копий и проведение обновлений ПО. Завершается план анализом инцидента	**Прочитайте текст и запишите развернутый обоснованный ответ** Разработайте план реагирования на киберугрозы для организаций в случае выявления атак на информационные системы.		3 мин

	и формулировкой выводов для улучшения защитных мер			
33	Политика включает обязательное использование VPN для подключения к корпоративным ресурсам, двухфакторную аутентификацию для входа в систему и шифрование всех передаваемых данных. Также предусматриваются регулярные обновления удаленных клиентов и проведение проверки устройств на соответствие требованиям безопасности перед предоставлением доступа. Сотрудники проходят обучение по безопасности удаленной работы и подписывают соглашение о принятии ответственности за соблюдение установленных норм.	**Прочитайте текст и запишите развернутый обоснованный ответ** Разработайте политику обеспечения безопасного удаленного доступа для сотрудников компании.		3 мин
34	Стандарт включает использование VPN для защищенного доступа, обязательное шифрование всех данных и регулярные обновления мобильного ПО. Запрещено использование публичных Wi-Fi сетей без VPN. Устройства должны	**Прочитайте текст и запишите развернутый обоснованный ответ** Напишите стандарт использования мобильных устройств для доступа к корпоративным ресурсам компании.		3 мин

	быть защищены паролями и средствами удаленного управления в случае кражи или утери.			
35	Программа включает введение в информационную безопасность, методы защиты от фишинга и социальных атак. Сотрудники учатся создавать надежные пароли, защищать конфиденциальную информацию и распознавать вредоносные атаки. Завершающий модуль посвящен процедурам реагирования на инциденты безопасности.	**Прочитайте текст и запишите развернутый обоснованный ответ** Разработайте краткую программу обучения сотрудников по вопросам безопасности данных.		3 мин