

Цель тестового задания: Проверка навыков, качеств и умений кандидатов в следующих областях:

- **Определение конфликта интересов:** умение выявлять потенциальные конфликты интересов.
- **Этические качества:** демонстрация приверженности принципам объективности и независимости при работе с информацией и клиентами.
- **Внимательность к деталям:** умение вникать в детали и замечать незначительные несоответствия.

Инструкция:

Часть 1. Внимательно прочитайте каждый вопрос и выберите один или несколько из предложенных вариантов ответа. Вы можете выбирать любое количество ответов.

Часть 2. Внимательно прочитайте предложенную ситуацию и впишите свой ответ в текстовое поле. Не ограничивайте объём своего ответа видимыми границами текстового поля, оно может вместить неограниченное количество символов.

Не существует «правильных» или «неправильных» ответов. Важно, чтобы ваш выбор был обоснован и отражал ваши знания, навыки и качества. При необходимости делайте пометки в отдельном файле или на черновике для более подробных ответов, которые вы можете представить на собеседовании.

Часть 1: тест.

Вопрос 1: после начала ИТ-аудита вы обнаружили, что руководитель службы информационной безопасности аудируемой компании является вашим близким другом, с которым вы знакомы с детства. Как вы поступите в данной ситуации?

Варианты ответа:

- 1. Сообщить о возможном конфликте интересов своему руководству по ИТ-аудиту.
- 2. Продолжить аудит без учёта данного фактора.
- 3. Запросить перевод на другой аудит.
- 4. Ничего не предпринимать.
- 5. Все варианты верные
- 6. Все варианты неверные

Вопрос 2: в ходе аудита ИТ-системы вы заметили, что один из сотрудников ИТ-подразделения является бывшим сотрудником поставщика ИТ-оборудования для аудируемой компании. Как вы будете действовать?

Варианты ответа:

- 1. Зафиксировать данную информацию в своём рабочем журнале и доложить руководству.
- 2. Попросить сотрудника ИТ-подразделения доказать свою независимость.
- 3. Провести дополнительную проверку ИТ-системы на предмет возможных уязвимостей.
- 4. Ничего не предпринимать, так как это не входит в ваши обязанности.
- 5. Все варианты верные
- 6. Все варианты неверные

Вопрос 3: во время ИТ-аудита вы получили от одного из сотрудников ИТ-подразделения конфиденциальную информацию, не связанную с предметом аудита. Как вы поступите с этой информацией?

Варианты ответа:

- 1. Сообщить о получении конфиденциальной информации руководству компании и не использовать ее в своих целях.
- 2. Использовать полученную информацию для выявления нарушений в работе ИТ-подразделения.
- 3. Передать полученную информацию своему руководителю.
- 4. Ничего не предпринимать.
- 5. Все варианты верные
- 6. Все варианты неверные

Вопрос 4: в процессе аудита вы обнаружили, что один из сотрудников ИТ-подразделения допустил ошибку, которая могла привести к серьёзным последствиям. Как вы будете действовать?

Варианты ответа:

- 1. Зафиксировать ошибку в своём рабочем журнале и доложить руководству компании.
- 2. Предложить сотруднику ИТ-подразделения самостоятельно исправить ошибку.
- 3. Сообщить о допущенной ошибке руководству ИТ-подразделения.
- 4. Ничего не предпринимать, так как это не входит в ваши обязанности.

- 5. Все варианты верные
- 6. Все варианты неверные

Вопрос 5: при анализе журналов регистрации ИТ-системы вы заметили, что в определенное время суток наблюдается резкий рост трафика. Как вы интерпретируете эту информацию?

Варианты ответа:

- 1. Возможна попытка несанкционированного доступа к ИТ-системе.
- 2. Вероятно, в это время происходит резервное копирование данных.
- 3. Это может быть связано с пиковой нагрузкой на ИТ-систему.
- 4. Необходимо провести дополнительную проверку для выяснения причин роста трафика.
- 5. Все варианты верные
- 6. Все варианты неверные


Вопрос 6: в ходе проверки ИТ-документации вы обнаружили несоответствие между заявленной версией программного обеспечения и версией, установленной на сервере. Как вы поступите в данной ситуации?

Варианты ответа:

- 1. Зафиксировать несоответствие в своём рабочем журнале и доложить своему руководству.
- 2. Попросить сотрудников ИТ-подразделения предоставить документы, подтверждающие установку корректной версии ПО.
- 3. Провести тестирование программного обеспечения на предмет его работоспособности.
- 4. Ничего не предпринимать, так как это не является критическим нарушением.
- 5. Все варианты верные
- 6. Все варианты неверные

Часть 2: ситуационные задачи

Ситуация 1: вы проводите аудит политики паролей в компании. В документе утверждается, что пароли должны быть не менее 8 символов длиной, включать заглавные и строчные буквы, цифры и специальные символы. Однако при проверке случайной выборки учётных записей вы обнаруживаете, что многие пароли состоят только из строчных букв и цифр. Опишите, какие действия вы предпримете.

Ситуация 2: вам предоставлен журнал доступа к критически важной системе для аудита (к тесту приложен файл `xlsx`, кликните по иконке справа). Проанализировав эти данные, какие выводы вы можете сделать? 

Ситуация 3: вы изучаете документацию процедур реагирования на инциденты информационной безопасности в организации. Документ предписывает немедленно уведомлять руководство о всех инцидентах безопасности. При анализе отчетов о последних инцидентах вы обнаруживаете, что некоторые из них были рассмотрены только через несколько дней после обнаружения. Как вы оцените эту ситуацию и что предложите для улучшения процесса?

Спасибо. Сохраните этот файл с названием «Ваше имя и фамилия» и отправьте электронной почтой на адрес: vtkachev@bakertilly.kg