Номер задания	Ответ	Критерии оценивания
1	14120	10 баллов
2	5987977305	12 баллов
3	А	2 балла
4	БАС	3 балла
5	АГ	4 балла
6	В	2 балла
7	В	2 балла
8	Б	3 балла
9	273	10 баллов
10	5	8 баллов
11	Б	2 балла
12	зехетчнд	10 баллов
13	В	1 балл
14	АД	5 баллов
15	А	1 балл
Кейс-задание	Творческое задание. Это примерные выдержки для оценивания. Риски фишинга для бизнеса 1. **Утечка конфиденциальной информации**: Успешные атаки могут привести к потере данных клиентов, партнеров и сотрудников, что может вызвать серьезные последствия. 2. **Финансовые потери**: Злоумышленники могут получить доступ к финансовым ресурсам компании, что приведет к прямым убыткам. 3. **Репутационные потери**: Утечка данных и нарушение безопасности могут негативно сказаться на репутации компании, что может привести к потере клиентов и снижению доверия со стороны партнеров. 4. **Юридические последствия**: Компании могут столкнуться с юридическими последствиями из-за несоблюдения законодательства о защите данных. 5. **Влияние на операционную деятельность**: Фишинг-атаки могут привести к сбоям в работе системы, что может повлиять на производительность и эффективность бизнеса. ### Способы защиты от фишинга на уровне компании 1. **Обучение сотрудников**: Регулярные тренинги по безопасности, где сотрудники учатся распознавать фишинговые сообщения и другие угрозы. 2. **Фильтрация электронной почты**: Использование специальных фильтров и антиспам-технологий для блокировки подозрительных писем. 3. **Двухфакторная аутентификация (2FA)**: Внедрение дополнительных уровней защиты при входе в учетные записи, что затрудняет доступ злоумышленников даже при наличии пароля. 4. **Регулярное обновление ПО**: Установка обновлений для операционных систем и программного обеспечения, чтобы устранить уязвимости. 5. **Создание политики безопасности**: Разработка и внедрение четкой политики безопасности, охватывающей использование электронной почты и интернет-ресурсов. 6. **Мониторинг и анализ**: Регулярный аудит систем безопасности и мониторинг подозрительной активности. 7. **Создание фейковых фишинг-атак**: Проведение тестовых фишинг-атак для оценки готовности сотрудников и выявления слабых мест. 8. **Использование VPN**: Защита данных при использовании общедоступных сетей Wi-Fi.	Если названо 1-3 риска – 7 баллов Если названо более 3х рисков – 10 баллов Если названо 1-3 Способа защиты – 10 баллов Если названо более 3 способы защиты – 15 баллов
		100 баллов