

КОМПЛЕКТ КРИТЕРИЕВ И МЕТОДИКИ ОЦЕНИВАНИЯ ДЛЯ 7-8 КЛАССОВ

школьного этапа всероссийской олимпиады школьников
по труду (технологии)
профиль «Информационная безопасность»
в 2024/2025 учебном году в Санкт-Петербурге

Санкт-Петербург

2024

КРИТЕРИИ И МЕТОДИКА ОЦЕНИВАНИЯ ДЛЯ 7-8 КЛАССОВ

По теоретическому туру максимальная оценка результатов участника 7 классов определяется арифметической суммой всех баллов, полученных за выполнение заданий и не должна превышать **60 баллов**.

Каждый ответ оценивается либо как правильный (полностью совпадает с ключом), либо как неправильный (отличается от ключа или отсутствует), кроме заданий 17 и 20, для которых введены особые критерии.

Задания 6, 11 и 14 требуют получения ответа в формате истина/ложь на утверждения.

Каждый правильный ответ может иметь вес: 1 балл, 2 балла, 3 балла, 4 балла.

Кейс-задание оценивается в совокупности 10 баллами.

Общая часть (10 баллов в сумме)

1. ОТВЕТ: **1,2,4** (2 балла)
2. ОТВЕТ: **длина 110, ширина 70, высота 85** (2 балла)
3. ОТВЕТ: **а. (логистика)** (2 балла)
4. ОТВЕТ: **б. (рециклинг-технологии)** (2 балла)
5. ОТВЕТ: **1- ритм** (2 балла)

Специальная часть (50 баллов в сумме)

6. ОТВЕТ: **1-да, 2-нет, 3-да, 4-да** (4 балла)
7. ОТВЕТ: **1** (2 балла)
8. ОТВЕТ: **4** (1 балл)
9. ОТВЕТ: **2** (1 балл)
10. ОТВЕТ: **3** (1 балла)
11. ОТВЕТ: **да** (1 балл)
12. ОТВЕТ: **(3 балла)**

1	2	3	4	5
В	Г	Д	А	Б

13. ОТВЕТ: **1** (1 балл)
14. ОТВЕТ: **нет** (1 балл)
15. ОТВЕТ: **3** (1 балл)
16. ОТВЕТ: **1** (1 балл)
17. ОТВЕТ: **(3 балла в сумме)**

Участник должен указать следующее:

Школьный этап всероссийской олимпиады школьников по труду (технологии)
профиль «Информационная безопасность»
в 2024/2025 учебном году в Санкт-Петербурге

КРИТЕРИИ И МЕТОДИКА ОЦЕНИВАНИЯ ДЛЯ 7-8 КЛАССОВ

Не переходить по ссылке в письме. Вместо этого зайти на официальный сайт благотворительной организации, введя его адрес вручную, и проверить наличие информации о текущих сборах средств.

или

Связаться напрямую с организацией через официальные контактные данные, указанные на их сайте, чтобы уточнить, была ли инициирована такая рассылка, и уточнить легитимные способы поддержки.

При указании одного из двух вариантов или близких к ним – 3 балла

Участник ни в коем случае не должен указывать:

- 1. Переход по ссылке в письме и выполнение пожертвования без проверки подлинности.*
- 2. Ответ на письмо с финансовыми данными или подтверждением готовности пожертвовать.*

(В случае указания одного из двух пунктов - 0 баллов за ответ, безотносительно начисленных ранее баллов)

18. ОТВЕТ: **octalsystem** (10 баллов)

19. ОТВЕТ: Значение сдвига: **17 налево**, сообщение: **crystal clear** (10 баллов)

20. ОТВЕТ: (10 баллов в сумме)

Ответ А: 2, 3 (2 балла)

Ответ Б: Да, является.

Участник должен привести в качестве обоснования пример механизма социальной инженерии из приведенного эпизода. Например:

Злоумышленники использовали фишинг, чтобы обманным путем заставить сотрудников ввести свои учетные данные на поддельном сайте.

Спуффинг был использован для подделки адреса электронной почты, чтобы письмо выглядело как отправленное внутренним отделом ИТ-поддержки

Правильный ответ без обоснования (0 баллов)

Правильный ответ с обоснованием (3 балла)

КРИТЕРИИ И МЕТОДИКА ОЦЕНИВАНИЯ ДЛЯ 7-8 КЛАССОВ

Ответ В: (3 балла)

Участник должен упомянуть как минимум одну профилактическую меру или превентивный механизм против методов социальной инженерии из эпизода, например:

1. *Никогда не вводить учетные данные на незнакомых или подозрительных сайтах, даже если они выглядят официальными.*
2. *Всегда проверять URL сайта перед вводом личных данных, чтобы убедиться в его подлинности.*
3. *Обратиться в ИТ-отдел через официальные каналы для проверки подлинности письма.*

Ответ Г: (2 балла)

Участник должен обоснованно указать на хотя бы 1 действие компании после инцидента, которое позволит предотвратить подобный инцидент или смягчить последствия текущего, например:

1. *Немедленно уведомить всех сотрудников о возможном компрометации учетных данных и потребовать смены паролей.*
2. *Провести внутреннее расследование для определения масштаба утечки и предпринять меры по защите скомпрометированных систем.*
2. *Внедрить многофакторную аутентификацию для предотвращения подобных атак в будущем.*