

КОМПЛЕКТ КРИТЕРИЕВ И МЕТОДИКИ ОЦЕНИВАНИЯ ДЛЯ 10-11 КЛАССОВ

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

Санкт-Петербург

2024

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

КРИТЕРИИ И МЕТОДИКА ОЦЕНИВАНИЯ ДЛЯ 10-11 КЛАССОВ

По теоретическому туру максимальная оценка результатов участника 10-11 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 18, 20 и 21 для которых введены особые критерии.

Задания 6, 12 и 15 требуют получения ответа в формате истина/ложь на утверждения.

Каждый правильный ответ или часть ответа может иметь вес: 1 балл, 2 балла, 3 балла, 4 балла, 5 баллов.

Кейс-задание оценивается 10 баллами и является заданием со свободным ответом и требуют анализа ответа от методиста.

Общая часть
(10 баллов в сумме)

1. ОТВЕТ: **В** (2 балла)
2. ОТВЕТ: **4** (2 балла)
3. ОТВЕТ: **а, б, в, г, д** (последовательность выставлена в правильном порядке) (2 балла)
4. ОТВЕТ: **да (верно)** (2 балла)
5. ОТВЕТ: **3 - стиль** (2 балла)

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

КРИТЕРИИ И МЕТОДИКА ОЦЕНИВАНИЯ ДЛЯ 10-11 КЛАССОВ

Специальная часть
(50 баллов в сумме)

6. ОТВЕТ: **1-нет, 2-нет, 3-нет, 4-нет, 5-нет** (3 балла)
7. ОТВЕТ: **1, 3, 5** (2 балла)
8. ОТВЕТ: **3** (1 балла)
9. ОТВЕТ: **1** (1 балла)
10. ОТВЕТ: **2** (2 балла)
11. ОТВЕТ: **2** (1 балла)
12. ОТВЕТ: **нет** (1 балла)
13. ОТВЕТ: (5 баллов)

1	2	3	4	5	6
Б	Д	Е	Г	А	В

14. ОТВЕТ: **1** (1 балла)
15. ОТВЕТ: **нет** (1 балла)
16. ОТВЕТ: **3** (1 балла)
17. ОТВЕТ: **1** (1 балла)
18. ОТВЕТ: (5 баллов максимум)

Действия, которые должен выполнить участник:

1. Не выходить на контакт с отправителями письма (Не звонить, не отправлять ответное письмо) - 2 балла

- Участник должен указать, что нельзя взаимодействовать с отправителями письма (не переходить по ссылке, не отправлять данные в ответ на письмо).

2. Обратиться к официальной службе безопасности компании через проверенные каналы связи (телефон, внутренний мессенджер, официальный адрес электронной почты) - 2 балла

- Участник должен связаться с реальной службой безопасности компании, чтобы сообщить о подозрительном письме и удостовериться в том, что оно не является подлинным.

3. Сообщить официальной службе безопасности о подозрительном письме и возможной фишинговой атаке - 1 балл

КРИТЕРИИ И МЕТОДИКА ОЦЕНИВАНИЯ ДЛЯ 10-11 КЛАССОВ

- Участник должен уведомить службу безопасности о попытке фишинга, чтобы компания могла принять меры для защиты других сотрудников.

Действия, которые участник не должен выполнять:

1. Переход по ссылке в письме и/или введение своих учетных данных на предложенной странице - 0 баллов

- Если участник указывает на необходимость перехода по ссылке или ввода данных без проверки подлинности запроса, его ответ оценивается в 0 баллов.

2. Отправка ответного письма с данными - 0 баллов

- Если участник указывает на необходимость отправки данных в ответ на письмо, его ответ также оценивается в 0 баллов.

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

19. ОТВЕТ: **pushtothelimit** (7 баллов)

20. ОТВЕТ: **Карл у Клары украл кораллы, а Клара у Карла украла кларнет**
(8 баллов)

21. ОТВЕТ: (10 баллов в сумме)

Ответ А: **1, 3, 4, 7** (3 балла)

- **3 балла** за правильное указание всех четырех упомянутых видов атак и механизмов реализации уязвимостей.
- **2 балла** за правильное указание трех из четырех.
- **1 балл** за правильное указание двух из четырех.
- **0 баллов** за указание одного или менее правильного варианта.

Ответ Б: (3 балла)

Ожидается, что участник перечислит меры предосторожности, которые могли бы предотвратить инцидент:

1. *Использование систем обнаружения и предотвращения вторжений (IDS/IPS)*
2. *Сегментация сети и принцип минимальных привилегий*
3. *Мониторинг и анализ сетевого трафика*

КРИТЕРИИ И МЕТОДИКА ОЦЕНИВАНИЯ ДЛЯ 10-11 КЛАССОВ

4. *Использование технологий изоляции и виртуализации*
5. *Внедрение строгой парольной политики, включая уникальные пароли для критических систем.*
6. *Использование многофакторной аутентификации для доступа к важным системам и учетным записям.*

- **3 балла** за указание трех и более мер.
- **2 балла** за указание двух мер.
- **1 балл** за указание одной меры.
- **0 баллов** за отсутствие правильных указаний.

Ответ В: (2 балла)

Ожидается, что участник перечислит действия, которые нужно предпринять для минимизации последствий:

1. *Немедленно отключить скомпрометированные учетные записи и изменить все пароли, связанные с ними.*
2. *Уведомить всех пострадавших клиентов и сотрудников о произошедшем инциденте, чтобы предотвратить дальнейшее мошенничество.*

- **2 балла** за указание двух действий.
- **1 балл** за указание одного действия.
- **0 баллов** за отсутствие правильных указаний.

Ответ Г: (2 балла)

Участник должен предложить меры по улучшению политики управления учетными записями и паролями:

1. *Введение обязательного использования уникальных паролей*
2. *Регулярная ротация паролей*
3. *Требование использования сложных паролей*
4. *Внедрение многофакторной аутентификации*

- **2 балла** за указание двух и более мер.
- **1 балл** за указание одной меры.
- **0 баллов** за отсутствие правильных указаний.