

КОМПЛЕКТ КРИТЕРИЕВ И МЕТОДИКИ ОЦЕНИВАНИЯ ДЛЯ 9 КЛАССОВ

школьного этапа всероссийской олимпиады школьников
по труд (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 9 КЛАССОВ

По теоретическому туру максимальная оценка результатов участника 8-9 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.

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

Каждый правильный ответ имеет свой вес: 1 балл, 2 балла, 4 балла, 5 баллов.

Задания на кодирование/декодирование оцениваются в 8 баллов, кейс заданий оценивается 10 баллами в совокупности.

Общая часть
(10 баллов в сумме)

1. ОТВЕТ: **А** (2 балла)
2. ОТВЕТ: **1-В, 2-А, 3-Б** (2 балла)
3. ОТВЕТ: **в. (бюджет профицитный)** (2 балла)
4. ОТВЕТ: **а. МРОТ (минимальный размер оплаты труда)** (2 балла)
5. ОТВЕТ: **1- композиция** (2 балла)

Специальная часть
(50 баллов в сумме)

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

1	2	3	4	5
В	Б	Д	А	Г

14. ОТВЕТ: **5** (1 балла)
15. ОТВЕТ: **нет** (1 балла)
16. ОТВЕТ: **1** (1 балла)
17. ОТВЕТ: **2** (1 балла)

КРИТЕРИИ И МЕТОДИКА ОЦЕНИВАНИЯ ДЛЯ 9 КЛАССОВ

18. ОТВЕТ: (4 баллов максимум)

Допустимые действия:

1. **Не звонить по номеру, указанному в письме, и не предоставлять никакие данные (2 балла):**
 - **2 балла:** Если участник указывает, что нельзя звонить по указанному в письме номеру и/или предоставлять данные, такие как логин, пароль и код из SMS, поскольку это может быть попытка мошенничества.
 - **0 баллов:** Если участник указывает, что можно или нужно позвонить по указанному номеру, либо предоставляет какие-либо данные.
2. **Связаться с отделом ИТ-поддержки напрямую через корпоративные каналы связи для проверки подлинности запроса (2 балла):**
 - **2 балла:** Если участник указывает, что следует связаться с ИТ-поддержкой через проверенные каналы связи, такие как внутренний мессенджер, официальный номер телефона, указанный в корпоративном справочнике, или личное обращение, чтобы проверить подлинность запроса.
 - **1 балл:** Если участник указывает, что следует проверить подлинность запроса, но не уточняет, каким образом или упоминает частично правильные методы.
 - **0 баллов:** Если участник не указывает, что нужно проверить подлинность запроса, или предлагает предоставить данные без проверки.

Запрещенные действия:

1. **Звонок по указанному в письме номеру и предоставление логина, пароля или кода из SMS:**
 - Если участник указывает, что можно позвонить по указанному номеру или предоставляет какие-либо данные, такие как логин, пароль или код из SMS, это может привести к компрометации учетных данных. В этом случае оценка ответа будет 0 баллов, независимо от других правильно выполненных пунктов.

КРИТЕРИИ И МЕТОДИКА ОЦЕНИВАНИЯ ДЛЯ 9 КЛАССОВ

2. Ответ на письмо с предоставлением какой-либо информации:

- Если участник указывает, что можно или нужно ответить на письмо, предоставив какие-либо данные, это может привести к компрометации учетных данных. В этом случае оценка ответа будет 0 баллов, независимо от других правильно выполненных пунктов.

19. ОТВЕТ: **decodingisajoy** (8 баллов)

20. ОТВЕТ: **ученье свет, а неученье тьма** (8 баллов)

21. ОТВЕТ: (10 баллов в сумме)

Ответ А: 3,7,8 (2 балла)

+1 балл за каждое правильное указание.

- 1 балл за каждое неправильное указание.

Ответ Б: Нет, системы защиты периметра не гарантируют полной защиты. (3 балла)

Участник должен объяснить, что системы защиты периметра (например, фаерволлы и системы предотвращения вторжений) играют важную роль, но они не защищают от атак, которые используют методы социальной инженерии, внутренние угрозы, или от атак, которые происходят уже внутри сети после компрометации учетных данных.

Возможные обоснования:

1. Социальная инженерия позволяет злоумышленникам обойти периметровую защиту, получив доступ к внутренним учетным записям.

2. Вредоносное ПО может быть внедрено через действия самих пользователей или через устройства, которые не отслеживаются системами периметровой защиты.

*3. Защита периметра не обнаружит и не предотвратит атаки, которые уже происходят внутри сети, такие как **атака с повышением привилегий**.*

- **3 балла** за правильный ответ с полным и аргументированным объяснением.
- **2 балла** за правильный ответ с частичным или не совсем

КРИТЕРИИ И МЕТОДИКА ОЦЕНИВАНИЯ ДЛЯ 9 КЛАССОВ

точным объяснением.

- **1 балл** за правильный ответ, но без достаточного объяснения.
- **0 баллов** за отсутствие объяснения или неверный ответ.

Ответ В: (3 балла)

Участник должен упомянуть меры, которые, исходя из описания атаки, помогут предотвратить повторение подобных инцидентов.

Возможные меры:

- 1. Внедрение регулярного обучения сотрудников по вопросам кибербезопасности, особенно по распознаванию фишинга и других методов социальной инженерии.*
- 2. Усиление мониторинга и анализа сетевого трафика для обнаружения аномальной активности, в том числе внутри сети.*
- 3. Обновление и усиление политики управления доступом, включая более строгие требования к паролям и их ротацию.*
- 4. Регулярное проведение аудита безопасности и тестирования на проникновение (пентестов) для выявления слабых мест в системе*

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

Ответ Г: (2 балла)

Участник должен описать действия, которые нужно предпринять при обнаружении вредоносного ПО, которое контролирует системы компании. Возможные шаги:

- 1. Немедленно изолировать зараженные системы от сети, чтобы предотвратить дальнейшую передачу данных и ограничить доступ злоумышленников.*
- 2. Провести полное сканирование и анализ системы для определения масштабов компрометации, включая поиск других уязвимых систем.*
- 3. Уведомить соответствующие группы (например, команда безопасности, руководство) и начать процедуру восстановления, используя резервные копии.*
- 4. Удалить вредоносное ПО и восстановить систему из резервных копий, которые были сделаны до компрометации, с последующим*

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

КРИТЕРИИ И МЕТОДИКА ОЦЕНИВАНИЯ ДЛЯ 9 КЛАССОВ

усилением защиты.

- **2 балла** за правильное указание двух шагов.
- **1 балл** за указание одного правильного шага.
- **0 баллов** за отсутствие правильных шагов или неверные действия.