

## **Всероссийская олимпиада по труду**

### **Муниципальный этап**

**Уважаемый участник!**

**Перед выполнением задания  
внимательно прочтите инструкцию**

На выполнение задания отводится не более 1,5 часа (90 минут).

Задание состоит из 20 тестовых вопросов и творческого задания, в которых предложены тесты с одним или несколькими правильными ответами.

Также предложены теоретические вопросы, на которые следует дать исчерпывающий ответ. Задача участника внимательно ознакомиться с предложенными заданиями и выполнить их в строгом соответствии с формулировкой.

Максимальная оценка – 40 баллов (из них кейс-задание оценивается в 16 баллов).

**Задания теоретического тура**

**по номинации «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»**

**7 класс**

**Общая часть (5 баллов)**

- 1) (1 балл) Критерии: засчитывать указанные баллы за полностью верный ответ. При неверном ответе участник получает 0 баллов. (письменный ответ)

Какой инструмент использует рабочий на фотографии? Выберите из списка подходящее для него название и впишите в ответ: штангенциркуль, цепная пила, разводной ключ, шуруповёрт, отбойный молоток, шлицевая отвертка.



Ответ: \_\_\_\_\_

- 2) (1 балл) Критерии: засчитывать указанные баллы за полностью верный ответ. При неверном ответе участник получает 0 баллов. (запишите номера моделей машин)

1	2	3	4
			
Экскаватор	Трактор	Грузоподъемный кран	Автокар

Названия каких моделей автотехники нужно поменять местами?

Ответ: \_\_\_\_\_

3) (1 балл) Критерии: засчитывать указанные баллы за полностью верный ответ. При неверном ответе участник получает 0 баллов. (письменный ответ)

Какая сельскохозяйственная культура изображена на рисунке?

- 1) хлопчатник
- 2) авокадо
- 3) ананас
- 4) кокос
- 5) мандарин
- 6) груша
- 7) лён



Ответ: \_\_\_\_\_

4) (1 балл) Критерии: засчитывать указанные баллы за полностью верный ответ. При неверном ответе участник получает 0 баллов. (отметьте правильные ответы знаком +)

Как называется устройство, предназначенное для автоматического вычерчивания рисунков, схем, чертежей?

- 1) принтер
- 2) плоттер
- 3) сканер
- 4) системный блок

5) (1 балл) Критерии: засчитывать указанные баллы за полностью верный ответ. При неверном ответе участник получает 0 баллов. (письменный ответ)

Как называется народный промысел?



Ответ:

Специальная часть (14 баллов)

В компании «Конфиденциальность Inc.» провели усовершенствование систем защиты информации и теперь предоставляют полный цикл услуг по хранению и обеспечению безопасности пользовательских данных в облачном хранилище. К несчастью, недавно системы организации подверглись масштабной атаке, направленной на разные объекты и реализованной различными нарушителями.

6) (1 балл) Критерии: засчитывать указанные баллы за полностью верный ответ. При неверном ответе участник получает 0 баллов.

Для сбора сведений об информационной системе компании злоумышленники похитили внешний носитель администратора безопасности с паролями нескольких пользователей, при этом больше пароли нигде зафиксированы не были. Реализация этой угрозы нарушила

- 1      конфиденциальность похищенных данных
- 2      доступность похищенных данных
- 3      целостность и доступность похищенных данных
- 4      конфиденциальность и доступность похищенных данных
- 5      конфиденциальность и целостность похищенных данных
- 6      конфиденциальность, целостность и доступность данных

7) (1 балл) Критерии: засчитывать указанные баллы за полностью верный ответ. При неверном ответе участник получает 0 баллов.

Обнаружив пропажу, системный администратор немедленно заблокировал учётные записи пользователей, чьи пароли были на похищенном носителе, тем самым

- 1      повысил защищённость системы компании
- 2      нарушил доступность информации, к которой имели доступ пользователи
- 3      остановил утечку информации, к которой имели доступ пользователи

4    нарушил целостность информации в системе компании

5    предотвратил угрозу нарушения конфиденциальности информации на носителе

8) (1 балл) Критерии: засчитывать указанные баллы за полностью верный ответ. При неверном ответе участник получает 0 баллов.

Не используя пароли с внешнего носителя, нарушители подобрали пароль одного из пользователей, авторизовались в системе под его учётными данными, после чего скопировали его служебные данные и сменили пароль пользователя. Реализация этой угрозы нарушила

1    конфиденциальность данных

2    доступность данных

3    целостность и доступность данных

4    конфиденциальность и целостность данных

5    конфиденциальность и доступность данных

6    конфиденциальность, целостность и доступность данных

9.) (1 балл) Критерии: засчитывать указанные баллы за полностью верный ответ. При неверном ответе участник получает 0 баллов.

Для нанесения финального удара нарушители одновременно провели DDoS-атаку на облачное хранилище компании, а также проникли в него и изменили права доступа одного из клиентов к его базе данных таким образом, чтобы он больше не мог запрашивать из неё сведения. Реализация этой угрозы нарушила

1    конфиденциальность данных

2    доступность данных

3    целостность и доступность данных

4    конфиденциальность и целостность данных

5    конфиденциальность и доступность данных

- 10) (1 балл) Критерии: засчитывать указанные баллы за полностью верный ответ. При неверном ответе участник получает 0 баллов.

Помимо конфиденциальности в компании «Конфиденциальность Inc.» требуется уделять внимание обеспечению целостности обрабатываемой информации.

Укажите, какую из предложенных ниже мер предпочтительно использовать самой компании для контроля целостности пользовательских данных, хранимых в облачном хранилище. Эти данные могут передаваться и храниться клиентами в зашифрованном виде.

- 1 хрупкие цифровые водяные знаки
- 2 электронная подпись
- 3 функции хэширования

- 11) (1 балл) Критерии: засчитывать указанные баллы за полностью верный ответ. При неверном ответе участник получает 0 баллов.

Укажите меру из перечисленных ниже, которая наиболее предпочтительна для клиентов облачного хранилища с целью контроля целостности хранимых в нём данных.

- 1 хрупкие цифровые водяные знаки
- 2 электронная подпись
- 3 функции хэширования
- 4 система протоколирования действий сотрудников компании «Конфиденциальность Inc.»

- 12) (1 балл) Критерии: засчитывать указанные баллы за полностью верный ответ. При неверном ответе участник получает 0 баллов.

1 Передавая партнёрам программные продукты, дальнейшее распространение которых не допускается лицензионным соглашением, компании следует использовать для отслеживания несанкционированного распространения

- 2 хрупкие цифровые водяные знаки
- 3 электронную подпись
- 4 функции хэширования
- 5 надёжные цифровые водяные знаки

13) (1 балл) Критерии: засчитывать указанные баллы за полностью верный ответ. При неверном ответе участник получает 0 баллов.

Укажите две меры, которые компания может использовать для подтверждения внесения клиентами изменений в библиотеки распространённого по лицензии программного обеспечения.

- 1      электронная подпись
- 2      хрупкие цифровые водяные знаки
- 3      функции хэширования
- 4      надёжные цифровые водяные знаки
- 5      полухрупкие цифровые водяные знаки
- 6      система контроля версий программного обеспечения

Служба безопасности одного из органов власти стремится повысить уровень информационной безопасности своих сотрудников и посетителей. Для этого было решено провести обновление и усовершенствование систем авторизации посетителей и пользователей информационной системы.

14) (1 балл) Критерии: засчитывать указанные баллы за полностью верный ответ. При неверном ответе участник получает 0 баллов.

Для обеспечения контроля пропуска сотрудников была нанята охрана и установлены пропускные турникеты, при этом руководитель отдела информационной безопасности решил заменить пропуска на универсальный ключ доступа. Какой тип аутентификации тут предусмотрен?

- 1      биометрическая аутентификация
- 2      многофакторная аутентификация
- 3      однофакторная аутентификация
- 4      двухфакторная аутентификация

5 аутентификация через географическое местоположение

15) (1 балл) Критерии: засчитывать указанные баллы за полностью верный ответ. При неверном ответе участник получает 0 баллов.

Для удостоверения авторства документов каждому сотруднику, работающему не менее 3 месяцев, требуется подписывать документ с помощью специального устройства, в котором исполненная вручную подпись будет проверяться на соответствие хранящемуся цифровому эталону. Какой тип аутентификации используется?

- 1 биометрическая аутентификация
- 2 аутентификация с помощью электронной подписи
- 3 двухфакторная аутентификация
- 4 мультифакторная аутентификация
- 5 аутентификация по уникальному параметру
- 6 аутентификация с помощью аналоговой подписи

16) (1 балл) Критерии: засчитывать указанные баллы за полностью верный ответ. При неверном ответе участник получает 0 баллов.

Для доступа в рабочие кабинеты установлена усиленная система контроля. Теперь каждый сотрудник должен произнести специально разработанную для этой системы фразу, после чего программное средство принимает решение о пропуске по звуковому диапазону голоса. Какой тип аутентификации используется?

- 1 биометрическая аутентификация
- 2 многофакторная аутентификация
- 3 двухфакторная аутентификация
- 4 парольная аутентификация



Шифр, известный как «квадрат Полибия», устроен следующим образом. В квадратную или прямоугольную таблицу вписываются буквы алфавита (для кодирования - в алфавитном порядке, для шифрования - в произвольном, при этом расположение букв в таблице является ключом), строки и столбцы таблицы обозначаются цифрами. При зашифровании буквы открытого текста заменяются на пары цифр, которыми отмечены, соответственно, строка и столбец, в которых стоит данная буква. Например, на иллюстрации ниже буква «О» зашифрована сочетанием цифр «34», а слово «ОКО» - «34 26 34».

	1	2	3	4	5	6
1	А	Б	В	Г	Д	Е
2	Ё	Ж	З	И	Й	К
3	Л	М	Н	О	П	Р
4	С	Т	У	Ф	Х	Ц
5	Ч	Ш	Щ	Ъ	Ы	Ь
6	Э	Ю	Я	.	,	?

Таким шифром зашифрован некоторый текст (без пробелов, но с сохранением знаков препинания - точки, запятой и вопросительного знака):

51 16 32 41 31 34 22 33 16 16 32 16 42 34 15 65 42 16 32 32 16 33 56 52 16 41 13 34

17) (2 балла) Критерии: засчитывать указанные баллы за полностью верный ответ. При неверном ответе участник получает 0 баллов. (дайте письменный ответ)

Установите, сколько запятых зашифровано в сообщении.

Ответ: \_\_\_\_\_ .

18) (2 балла) Критерии: засчитывать указанные баллы за полностью верный ответ. При неверном ответе участник получает 0 баллов. (дайте письменный ответ)

Зашифруйте слово «ПАРОЛЬ» по приведённому квадрату Полибия. Ответ запишите как одно число без разделителей.

Ответ: \_\_\_\_\_ .

19) (2 балла) Критерии: засчитывать указанные баллы за полностью верный ответ. При неверном ответе участник получает 0 баллов.

Определите, какое слово зашифровано шифртекстом

11 13 42 34 32 11 42 24 23 11 46 24 63.

1     АВТОСИГНАЛИЗАЦИЯ

2     АВТОМАТИЗАЦИЯ

3     АВТОМОБИЛИЗАЦИЯ

4     АВТОНОМИЗАЦИЯ

20) (2 балла) Критерии: засчитывать указанные баллы за полностью верный ответ. При неверном ответе участник получает 0 баллов.

Напишите шестое слово открытого текста без изменения его написания.

Ответ: \_\_\_\_\_.

21) Выполните творческое задание (ответы - 16 баллов):

На вокзале города N установлены терминалы самообслуживания. Пассажиру для приобретения билета требуется самостоятельно ввести дату отправления и номер поезда, на который требуется билет, ввести при помощи экранной клавиатуры и встроенного сканера паспортные данные, выбрать место, отсканировать документы, дающие право на приобретение льготного билета, после чего осуществить оплату банковской картой, вставив её в соответствующий разъём терминала и введя PIN-код.

Спустя некоторое время были обнаружены утечки персональных данных пассажиров (паспортных данных и данных других личных документов, сведений о приобретённых билетах) и сведений их банковских карт (номеров карт, сведений о

владельцах карт, PIN-кодов и CVV-кодов).

1. Оцените, по каким из физических каналов утечки информации - оптическому, акустическому, радиоэлектронному - нарушители могут перехватить информацию из документов или карты пассажира.
2. Оцените, в какой момент, то есть при совершении пассажиром каких действий, это может произойти.
3. Для каждой определённой Вами возможности перехвата информации
  - паспортные данные
  - данные прочих документов, дающих право на льготные билеты
  - открытую информацию о банковской карте
  - CVV-код
  - PIN-код

по какому-то конкретному каналу приведите пример того, как (возможно, с помощью каких средств) это может быть совершено. Подтвердите свои оценки и выводы аргументами.

Достаточным является лаконичный ответ, содержащий ответы на пункты 1-3 в сочетании «информация (конкретные данные из приведённых в условии) - канал утечки - момент времени (действия пассажира) - способ реализации угрозы (средство)», например: «Паспортные данные посетителя банка могут быть похищены по оптическому каналу в момент предъявления паспорта охране при помощи скрытой камеры, установленной рядом с постом охраны; телефонный номер может быть похищен по акустическому каналу в момент сообщения его оператору банка при помощи подслушивающего устройства («жучка»), размещённого рядом с рабочим местом оператора».

Рассмотрите все возможные сочетания похищаемой информации и каналов утечки.

Всероссийская олимпиада школьников по труду.  
Номинация «Информационная Безопасность» 2024-2025 уч. г.  
Муниципальный этап. 7 класс