

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 конкурса
по номинации «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»

8 - 9 классы

Общая часть (5 баллов)

1) (1 балл) Критерии: засчитывать указанные баллы за полностью верный ответ. При неверном ответе участник получает 0 баллов. (Ответ дайте в рублях. В ответе запишите целое число).

Какую сумму денежных средств необходимо заложить в раздел «Энергозатраты на выполнение всех операций при производстве одной серийной единицы изделия» при выполнении сложного технологического проекта. Вам нужно посчитать энергозатраты при его серийном производстве. Условия следующие

- 1 кВт/ч электроэнергии стоит 5,54 руб.
- Лазерно-гравировальный станок имеет энергопотребление 400 Вт в час и выжигает лицевую панель 30 минут.
- 3D принтер работает 3 часа, печатая основной корпус, потребляя 200 Вт за один час.
- Паяльная станция имеет энергопотребление 100 Вт за один час и работает ровно один час при пайке схемы.
- Компьютер используется 10 минут при прошивке микроконтроллера и имеет энергопотребление 600 Вт в час.

Ответ: _____

2) (1 балл) Критерии: засчитывать указанные баллы за полностью верный ответ. При неверном ответе участник получает 0 баллов. (отметьте правильные ответы знаком +)

Из предложенных вариантов ответов выберите метод проектирования (от греч. *bion* – элемент, ячейка жизни), который изучает особенности строения жизнедеятельности организмов для создания новых систем (приборов, механизмов) и совершенствования существующих.

- а. Кинетизм
- б. Бионика
- в. Ассоциация

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

Опасность попадания нефти в воду заключается в ухудшении ее качества, а также в создании на поверхности воды плотной пленки, через которую не проникают
1 и 2, необходимые подводным жителям.

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

Выберите из списка профессий те, которые появились во второй половине XX века.

- 1) кондитер
- 2) портной
- 3) веб-дизайнер
- 4) повар
- 5) стюардесса
- 6) каменщик
- 7) промоутер

5) (1 балл) Критерии: засчитывать указанные баллы за полностью верный ответ. При неверном ответе участник получает 0 баллов. (впишите номера игрушек в таблицу)

Установите соответствие между изображением игрушки и названием народного промысла, к которому она относится.

1	2	3
		
4	5	6

		
Название игрушки	№	
Филимоновская игрушка		
Абашевская игрушка		
Дымковская игрушка		
Каргопольская игрушка		
Городецкая игрушка		
Богородская игрушка		

Специальная часть

В компании «Крипто Секрет Ltd.» учли прежние инциденты и усовершенствовали систему информационной безопасности. К несчастью, недавно информационная система компании стала целью атаки со стороны злоумышленников.

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

Сначала нарушители решили скомпрометировать системы шифрования
компании, для чего осуществили перехват ключа шифрования в момент
передачи с аппаратного носителя в систему шифрования. Реализация такой
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.

После успешной компрометации ключа шифрования нарушители перехватили несколько передаваемых по сети зашифрованных сообщений и, заблокировав их доставку получателю, прочли их и подменили на собственные, которые затем были отправлены по назначению. Реализация такой 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

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

В другом случае нарушители просто исказили хранимую на сервере в зашифрованном виде информацию таким образом, чтобы при попытке её расшифровать пользователь получал лишь бессмысленный набор символов. Реализация такой угрозы нарушила

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

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

Помимо системы шифрования целью атаки стала и система электронной подписи, разработанная компанией. Однако ещё до действий нарушителей отправитель (один из сотрудников компании) ошибся в выборе ключа генерации подписи, в результате чего отправленное сообщение не могло пройти проверку подлинности подписи на стороне получателя. Такие действия отправителя

- 1 нарушили доступность передаваемой информации
- 2 нарушили доступность и целостность передаваемой информации
- 3 не нарушили безопасность передаваемой информации
- 4 нарушили целостность передаваемой информации
- 5 нарушили достоверность передаваемой информации

Одним из направлений деятельности компании «Крипто Секрет Ltd.» является разработка решений для обеспечения целостности данных.

10) (1 балл) Критерии: засчитывать указанные баллы. При неверном ответе участник получает 0 баллов.

Одна из наиболее распространённых задач – обеспечение контроля целостности информации, передаваемой по открытым каналам связи. Выберите меру защиты информации, которая подойдёт для решения указанной задачи.

- 1 система хэширования
- 2 электронная подпись
- 3 вычисление контрольной суммы
- 4 надёжные цифровые водяные знаки

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

Одной из категорий продуктов, выпускаемых компанией «КриптоСекрет Ltd.», являются программные средства выработки функций хэширования.

Выберите задачу, для решения которой может применяться одно из таких средств.

1 обеспечение целостности информации, передаваемой по открытым каналам связи

2 обеспечение контроля достоверности поступающих сообщений

3 обеспечение целостности хранимых на сервере файлов

4 контроль неизменности отправляемых сообщений

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

Для функций хэширования коллизией называется :

1 ситуация, когда невозможно корректно вычислить значение функции хэширования.

2 входное значение, для которого не определено выходное значение функции.

3 пара входных значений, для которых значения функции совпадают.

4 значение функции, для которого не определено ни одного входного значения.

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

В отдельных случаях для контроля целостности могут применяться цифровые водяные знаки. Для решения какой задачи они используются?

1 контроль неизменности данных, хранимых на сервере

2 контроль целостности записей в базе данных

3 контроль неизменности продуктов, распространяемых по лицензии

4 обеспечение подтверждения авторства отправителя сообщений

Руководство банка решило усовершенствовать системы информационной безопасности и для этого внедрить новые способы аутентификации. На основе анализа угроз было принято решение защищать как информационные ресурсы организации, так и служебные помещения от несанкционированного доступа.

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

Для обеспечения контроля пропуска сотрудников была нанята охрана и установлены пропускные турникеты, к которым сотрудники должны прикладывать март-карты. Какие типы аутентификации реализованы? Выберите 2 варианта.

1 биометрическая аутентификация

2 аутентификация по ЭЦП

3 однофакторная аутентификация

4 двухфакторная аутентификация

5 многофакторная аутентификация

6 аутентификация на основе фактора владения

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

Перед входом в каждый служебный кабинет стоит робот, который получает уведомление о посетителе и просит его пройти аутентификацию, чтобы войти внутрь. Для этого требуется встать на отмеченную позицию перед роботом и замереть на несколько секунд, пока робот проводит «осмотр» и сопоставляет отсканированную картинку с внутренней базой данных сотрудников. Какой тип аутентификации используется?

1 аутентификация по ЭЦП

2 биометрическая аутентификация

3 двухфакторная аутентификация

4 аутентификация на основе фактора знания

5 аутентификация по GPS

16) (1 балл) Критерии: засчитывать указанные баллы за 3 верных варианта ответа. При неверном ответе участник получает 0 баллов.

Для запуска компьютера на рабочем месте сотрудника руководство установило следующую систему: сначала она требует ввести PIN-код, после его успешного ввода пользователю требуется поднести электронный ключ к считывателю, а если ключ распознан как корректный, то пользователю предлагается приложить палец к сканеру. Укажите, какая система аутентификации реализована.

1 однофакторная аутентификация

2 двухфакторная аутентификация

3 трёхфакторная аутентификация

4 аутентификация на основе факторов знания и биометрии

5 аутентификация на основе факторов владения и биометрии

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 с некоторым (неизвестным) ключом зашифрован некоторый текст (без пробелов, но с сохранением знаков препинания – точки, запятой и вопросительного знака):

31 32 23 35 43 32 35 23 44 23 24 65 61 25 25 24 63 26 23 24 64 23 61 22 22 44 23
24 65 61 25 44 63 26 24 66 32 65 63 23 42 66 61 63 32 45 61 43 24 25 44 31 43 21
52 11 41 25 25 24 64 24 32 23 63 32 13 63 64 24 54

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

Известно, что в сообщении открытого текста содержится слово ТРЕТЬЕГО. Запишите расшифрованное четвёртое слово открытого текста.

Ответ: _____.

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

Установите шифробозначение (замену) буквы «Ь».

Ответ: _____.

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

Какое слово зашифровано тем же ключом, который был использован для приведённого выше сообщения «24 31 32 24 21 62 63 25 63 25 44 63»?

1 ОЗЕЛЕНЕНИЕ

2 ОСТОЛБЕНЕНИЕ

3 ОСВОБОЖДЕНИЕ

4 ОПРЕДЕЛЕНИЕ

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

Зашифруйте слово «ВЕКТОР» тем же ключом, который был использован для приведённого выше сообщения. Ответ запишите как одно число без разделителей.

Ответ: _____.

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

Авиакомпания N для облегчения пилотирования самолётов устанавливает на них системы автоматического управления (автопилот). Для запуска работы такой системы пилот должен ввести координаты пунктов отправления и назначения, параметры самолёта, а также авторизационные данные для связи с наземными диспетчерскими службами по пути следования.

Недавно были обнаружены случаи перехвата вводимой пилотами информации (пункты отправления и назначения не являются секретными, но точный маршрут и промежуточные точки следования, а также служебные сведения

компания желает сохранить конфиденциальными для обеспечения безопасности перелёта).

1. Оцените, какие сведения о перелёте могут быть перехвачены злоумышленниками из системы автоматического управления по побочным физическим каналам.
2. Оцените, приведя аргументы, какие каналы могли быть задействованы для совершения перехвата такой информации.
3. Приведите примеры устройств для каждой пары «канал – сведения», которые могли быть использованы для реализации таких угроз безопасности информации. Уточните, в какой момент (при каких действиях пилота или в какие моменты работы автопилота) эти угрозы могут быть реализованы. Аргументируйте свою оценку.

Достаточным является лаконичный ответ, содержащий ответы на пункты 1–3 в сочетании «информация (конкретные данные из приведённых в условии) – канал утечки – момент времени (действия пилотов или этапы полёта) – 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.