

Код участника: _____

Инструкция для участников олимпиады

Уважаемый участник олимпиады!

Использовать справочные материалы, средства сотовой связи, фото- и видео аппаратуру запрещено!

Вам предстоит выполнить письменные задания.

Время выполнения заданий соревновательного тура – 90 минут.

Выполнение письменных заданий целесообразно организовать следующим образом:

- не спеша, внимательно прочитайте задание;
- обдумайте и сформулируйте конкретный ответ только на поставленный вопрос;
- если Вы отвечаете на задание, связанное с заполнением таблицы или схемы, не старайтесь детализировать информацию, вписывайте только те сведения или данные, которые указаны в вопросе;

- особое внимание обратите на задания, в выполнении которых требуется выразить Ваше мнение с учетом анализа поставленной проблемы. Внимательно и вдумчиво определите смысл вопроса и логику ответа (последовательность и точность изложения). Отвечая на вопрос, предлагайте свой вариант решения проблемы, при этом ответ должен быть кратким, но содержать необходимую информацию.

Задание соревновательного тура считается выполненным, если Вы вовремя сдаете его членам жюри.

Теоретические задания обеспечивают возможность объективной оценки Ваших знаний и умений в баллах по единым критериям.

Теоретические задания первого тура состоят из 20 задания.

Задача участника - внимательно ознакомиться с предложенными заданиями и выполнить их в строгом соответствии с формулировкой.

Тестовое задание считается выполненным, если в нем отмечены или записаны все правильные ответы и не отмечено ни одного не правильного ответа.

Всего за теоретический тур максимальное количество баллов, которое может набрать участник, составляет **40 баллов**.

Приступайте к выполнению задания.

Желаем удачи!

Код участника: _____

Общая часть

1. Какой инструмент использует рабочий на фотографии?



1. цепная пила
2. шуруповёрт
3. разводной ключ
4. штангенциркуль
5. отбойный молоток
6. шлицевая отвёртка

2. На станции «Добрынинская» Московского метрополитена установлены 12 резных миниатюр на прямоугольных пластинах белого мрамора. Их автор – скульптор Елена Александровна Янсон-Манизер. На барельефах изображены представители разных профессий.

Представитель какой профессии изображён на фотографии?



1. дояр
2. рыбак
3. овцевод
4. птицевод
5. тракторист
6. виноградарь

3. Какая сельскохозяйственная культура изображена на фотографии?

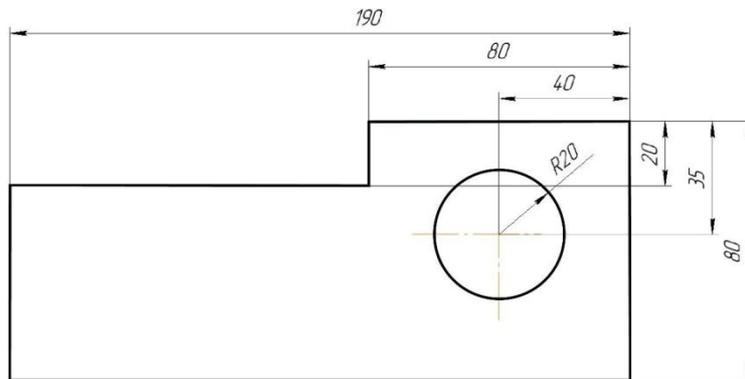
1. лён
2. кокос
3. перец
4. ананас
5. апельсин
6. баклажан
7. хлопчатник



4. Маша решила купить авокадо. Она знает, что цена за 1 штуку равна 80 рублям. Придя в магазин, Маша узнала, что сегодня на авокадо действует скидка 15 %. Определите, какую сумму в рублях заплатит Маша за 5 авокадо.

Код участника: _____

5. Саша выполнил чертёж плоской детали и нанёс на него размеры в миллиметрах (см. чертёж). Деталь содержит круглое отверстие.



Чертёж

Определите площадь (в квадратных сантиметрах) одной стороны детали. При расчётах примите $\pi \approx 3,14$. Ответ округлите до целого. Для получения более точного результата округление стоит производить только при получении финального ответа.

Специальная часть

Задания 6–9

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

6. 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. 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

Код участника: _____

8. 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. 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

Задания 10–13

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

10. 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. 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

12. Для функций хэширования коллизией называется

1. ситуация, когда невозможно корректно вычислить значение функции хэширования.

Код участника: _____

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.
5. контроль неизменности отправляемых сообщений

13. 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

Задания 14–16

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. Для обеспечения контроля пропуска сотрудников была нанята охрана и установлены пропускные турникеты, к которым сотрудники должны прикладывать смарт-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. 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. 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.

Код участника: _____

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

Задания 17–20

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

18. Установите шифробозначение (замену) буквы «Ь».

19. 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»?

- ОЗЕЛЕНЕНИЕ
- ОСТОЛБЕНЕНИЕ
- ОСВОБОЖДЕНИЕ
- ОПРЕДЕЛЕНИЕ

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

Код участника: _____

21. 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.