

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 21 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?

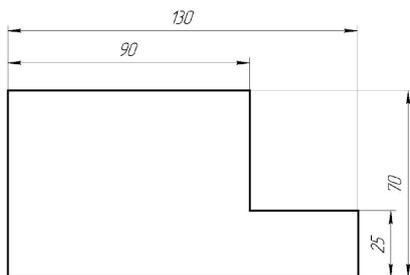
1. лён
2. кокос
3. перец
4. ананас
5. апельсин
6. баклажан
7. хлопчатник



4. Маша решила купить персики. Цена за 1 кг персиков равна 160 рублям. Выбрав несколько штук, Маша положила их на весы и узнала, что их масса равна 1 кг 200 г. Сколько рублей должна заплатить Маша за эти персики?

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

Код участника: _____



Чертёж

Определите площадь (в квадратных сантиметрах) одной стороны детали.

Специальная часть Задания 6–9

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. 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. 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. 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

Код участника: _____

9. 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
6. конфиденциальность, целостность и доступность данных

Задания 10–13

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

10. 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
4. асимметричные системы шифрования

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

1. хрупкие цифровые водяные знаки
2. электронную подпись
3. функции хэширования
4. надёжные цифровые водяные знаки

□

13. 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

Код участника: _____

4. надёжные цифровые водяные знаки
5. полухрупкие цифровые водяные знаки
6. система контроля версий программного обеспечения

Задания 14–16

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. 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. 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. 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

Код участника: _____

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 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
12 34 15 55 64 64

17. Установите, сколько запятых зашифровано в сообщении.

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

19. 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. Напишите шестое слово открытого текста без изменения его написания.

Код участника: _____

21. На вокзале города N установлены терминалы самообслуживания. Пассажиру для приобретения билета требуется самостоятельно ввести дату отправления 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 разъем 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

1. паспортные данные
2. данные прочих документов, дающих право на льготные билеты
3. открытую информацию о банковской карте
4. CVV-код
5. 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.