

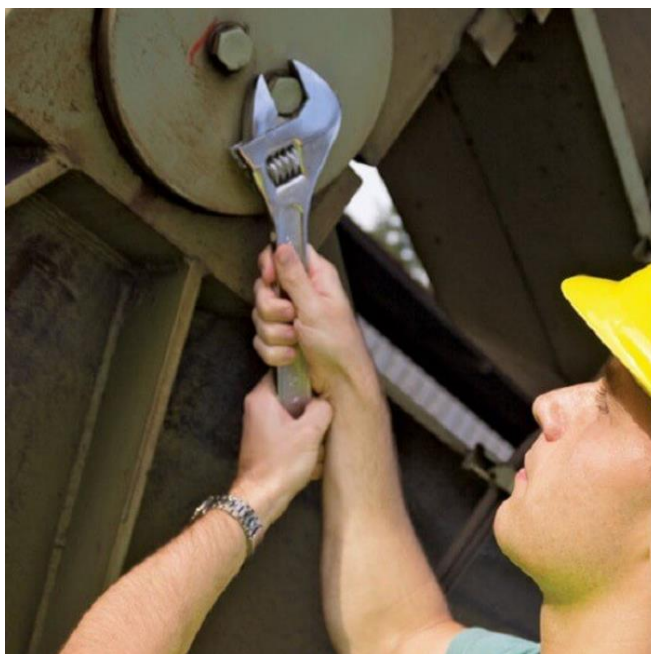
ВСЕРОССИЙСКАЯ ОЛИМПИАДА ШКОЛЬНИКОВ
ТЕХНОЛОГИЯ. ПРОФИЛЬ «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ».
МУНИЦИПАЛЬНЫЙ ЭТАП. 9 КЛАСС

ОТВЕТЫ И КРИТЕРИИ ОЦЕНИВАНИЯ

Максимальный балл за работу – 40.

Общая часть

Какой инструмент использует рабочий на фотографии?



- цепная пила
- шуруповёрт
- **разводной ключ**
- штангенциркуль
- отбойный молоток
- шлицевая отвёртка

За верный ответ – 1 балл.

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?

- дояр
- рыбак
- овцевод
- птицевод
- тракторист
- виноградарь

За верный ответ – 1 балл.

3. Какая сельскохозяйственная культура изображена на фотографии?

- лён
- кокос
- перец
- ананас
- апельсин
- баклажан
- хлопчатник



За верный ответ – 1 балл.

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.

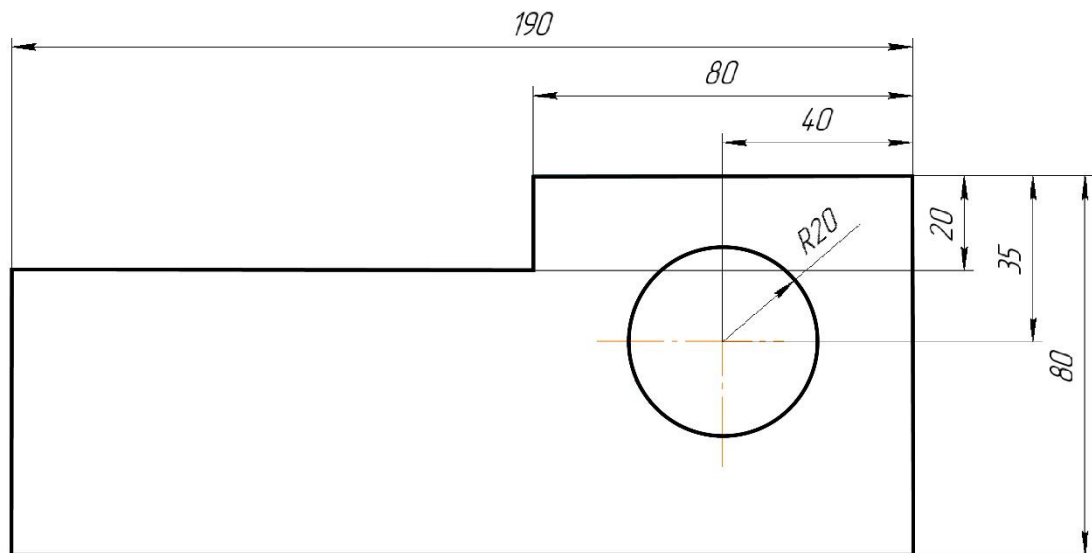
Ответ: 340.

Решение

(руб.)

За верный ответ – 1 балл.

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.

Ответ: 117.

Решение

Переведём миллиметры в сантиметры.

$$190 \text{ мм} = 19 \text{ см}$$

$$80 \text{ мм} = 8 \text{ см}$$

20 мм = 2 см. Площадь одной стороны детали будет равна:

$$(19 \cdot 8) - (19 - 8) \cdot 2 - 3,14 \cdot 2 \cdot 2 = 117,44 \approx 117 \text{ (см}^2\text{)}$$

За верный ответ – 1 балл.

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

- **конфиденциальность похищенных данных**
- доступность похищенных данных
- целостность и доступность похищенных данных
- конфиденциальность и доступность похищенных данных
- конфиденциальность и целостность похищенных данных
- конфиденциальность, целостность и доступность данных

За верный ответ – 1 балл.

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

- конфиденциальность похищенных данных
- доступность похищенных данных
- целостность и доступность похищенных данных
- конфиденциальность и доступность похищенных данных
- **конфиденциальность и целостность похищенных данных**
- конфиденциальность, целостность и доступность данных

За верный ответ – 1 балл.

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

- конфиденциальность хранимых данных
- доступность хранимых данных
- **целостность и доступность хранимых данных**
- конфиденциальность и доступность хранимых данных
- конфиденциальность и целостность хранимых данных
- конфиденциальность, целостность и доступность хранимых данных

За верный ответ – 1 балл.

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

- нарушили доступность передаваемой информации
- нарушили доступность и целостность передаваемой информации
- **не нарушили безопасность передаваемой информации**
- нарушили целостность передаваемой информации
- нарушили достоверность передаваемой информации

За верный ответ – 1 балл.

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.

- система хэширования
- **электронная подпись**
- вычисление контрольной суммы
- надёжные цифровые водяные знаки

За верный ответ – 1 балл.

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.

- обеспечение целостности информации, передаваемой по открытым каналам связи
- обеспечение контроля достоверности поступающих сообщений
- **обеспечение целостности хранимых на сервере файлов**
- контроль неизменности отправляемых сообщений

За верный ответ – 1 балл.

12. Для функций хэширования коллизией называется

- ситуация, когда невозможно корректно вычислить значение функции хэширования.
- входное значение, для которого не определено выходное значение функции.
- **пара входных значений, для которых значения функции совпадают.**
- значение функции, для которого не определено ни одного входного значения.

За верный ответ – 1 балл.

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

- контроль неизменности данных, хранимых на сервере
- контроль целостности записей в базе данных
- **контроль неизменности продуктов, распространяемых по лицензии**
- обеспечение подтверждения авторства отправителя сообщений

За верный ответ – 1 балл.

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.

- биометрическая аутентификация
- аутентификация по ЭЦП
- **однофакторная аутентификация**
- двухфакторная аутентификация
- многофакторная аутентификация
- **аутентификация на основе фактора владения**

За верный ответ – 1 балл.

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?

- аутентификация по ЭЦП
- **биометрическая аутентификация**
- двухфакторная аутентификация
- аутентификация на основе фактора знания
- аутентификация по GPS

За верный ответ – 1 балл.

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. Укажите, какая система аутентификации реализована.

- однофакторная аутентификация
- двухфакторная аутентификация
- **трёхфакторная аутентификация**
- аутентификация на основе факторов знания и биометрии
- аутентификация на основе факторов владения и биометрии

За верный ответ – 1 балл.

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.

Ответ: ЗАКОН

За верный ответ – 2 балла.

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

Ответ: 13

За верный ответ – 2 балла.

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

За верный ответ – 2 балла.

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

Ответ: 656343322423

За верный ответ – 2 балла.

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.

Критерии оценивания

В ответе должны присутствовать следующие предусмотренные сочетания:

1) маршрут перелёта – оптический канал – ввод пунктов следования пилотом/отображение маршрута на экране в процессе полёта – скрытая камера, установленная рядом с пультом управления пилота (допустимо любое иное устройство, позволяющее подсмотреть информацию при вводе или с экрана места пилота) **К1**;

2) маршрут перелёта – акустический канал – ввод пунктов следования пилотом – подслушивающее устройство, установленное рядом с пультом управления пилота (допустимо любое иное устройство, позволяющее подслушать нажатия клавиш) **К2**;

3) маршрут перелёта – радиоэлектронный канал – ввод пунктов следования пилотом/работа автопилота с маршрутом перелёта – устройство перехвата ПЭМИН (побочных электромагнитных излучений и наводок) (допустимо любое устройство, действующее по такому принципу) **К3**;

4) параметры (технические данные) самолёта – ввод пилотом в начале полёта – скрытая камера, установленная рядом с пультом управления пилота (допустимо любое иное устройство, позволяющее подсмотреть информацию при вводе или с экрана места пилота) **К4**;

5) параметры (технические данные) самолёта – ввод пилотом в начале полёта/ работа автопилота – устройство перехвата ПЭМИН (побочных электромагнитных излучений и наводок) (допустимо любое устройство, действующее по такому принципу) **К5**;

6) авторизационные данные для связи с наземными службами – ввод пилотом в начале полёта – скрытая камера, установленная рядом с пультом управления пилота (допустимо любое иное устройство, позволяющее подсмотреть информацию при вводе) **К6**;

7) авторизационные данные для связи с наземными службами – ввод пилотом в начале полёта – подслушивающее устройство, установленное рядом с пультом управления пилота (допустимо любое иное устройство, позволяющее подслушать нажатия клавиш) **К7**;

8) авторизационные данные для связи с наземными службами – ввод пилотом в начале полёта/связь на протяжении перелёта – устройство перехвата ПЭМИН (побочных электромагнитных излучений и наводок) (допустимо любое устройство, действующее по такому принципу) **К8**.

Каждое корректно описанное сочетание – **2 балла** (частичных баллов не предусмотрено).

Если сумма баллов за приведённые сочетания менее 16 баллов, то могут быть начислены бонусные баллы в пределах 16 баллов за всё задание (**К9**):

- каждое корректное сочетание вне списка предусмотренных – **2 балла**;
- приведено более одного устройства для уже засчитанного сочетания – **1 балл**.

Максимальный балл за задание – 16.

Максимальный балл за работу – 40.