ВСЕРОССИЙСКАЯ ОЛИМПИАДА ШКОЛЬНИКОВ
ТЕХНОЛОГИЯ. ПРОФИЛЬ «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ».
МУНИЦИПАЛЬНЫЙ ЭТАП. 7–8 КЛАССЫ

Максимальный балл за работу – 40.

Общая часть

1. Какой инструмент использует рабочий на фотографии?

- цепная пила
- шуруповёрт
- разводной ключ
- штангенциркуль
- отбойный молоток
- 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?

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

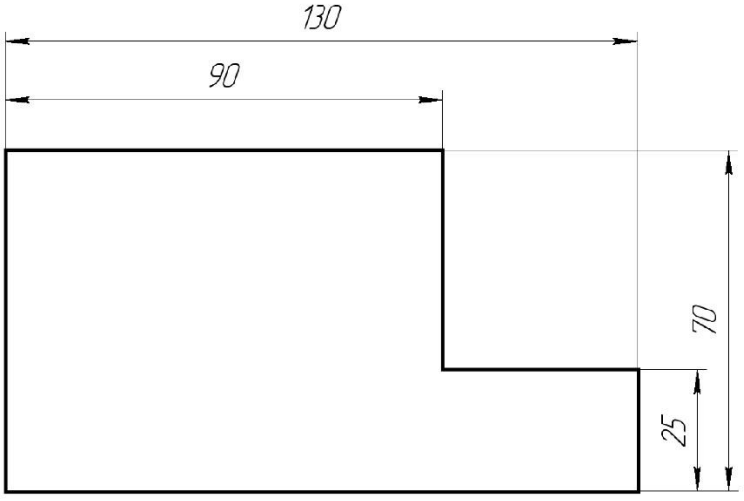
3. Какая сельскохозяйственная культура изображена на фотографии?

- лён
- кокос
- перец
- ананас
- апельсин
- баклажан
- 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?

Ответ: _____.

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



Чертёж

Определите площадь (в квадратных сантиметрах) одной стороны детали.

Ответ: _____.

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

- 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

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

- повысил защищённость системы компании
- нарушил доступность информации, к которой имели доступ пользователи
- остановил утечку информации, к которой имели доступ пользователи
- нарушил целостность информации в системе компании
- 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

- конфиденциальность данных
- доступность данных
- целостность и доступность данных
- конфиденциальность и целостность данных
- конфиденциальность и доступность данных
- конфиденциальность, целостность и доступность данных

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

- конфиденциальность данных
- доступность данных
- целостность и доступность данных
- конфиденциальность и целостность данных
- конфиденциальность и доступность данных
- 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.

- хрупкие цифровые водяные знаки
- электронная подпись
- функции хэширования
- асимметричные системы шифрования

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

- хрупкие цифровые водяные знаки
- электронная подпись
- функции хэширования
- 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

- хрупкие цифровые водяные знаки
- электронную подпись
- функции хэширования
- надёжные цифровые водяные знаки

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

- электронная подпись
- хрупкие цифровые водяные знаки
- функции хэширования
- надёжные цифровые водяные знаки
- полухрупкие цифровые водяные знаки
- 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?

- биометрическая аутентификация
- многофакторная аутентификация
- однофакторная аутентификация
- двухфакторная аутентификация
- 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?

- биометрическая аутентификация
- аутентификация с помощью электронной подписи
- двухфакторная аутентификация
- мультифакторная аутентификация
- аутентификация по уникальному параметру
- 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?

- биометрическая аутентификация
- многофакторная аутентификация
- двухфакторная аутентификация
- парольная аутентификация

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.

Ответ: _____.

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

Ответ: _____.

19. Определите, какое слово зашифровано шифртекстом

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

- АВТОСИГНАЛИЗАЦИЯ
- АВТОМАТИЗАЦИЯ
- АВТОМОБИЛИЗАЦИЯ
- АВТОНОМИЗАЦИЯ

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

Ответ: _____.

21. 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.

Максимальный балл за работу – 40.