**НОМИНАЦИЯ «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»**

## 8 - 9 классы

### Тестовые задания

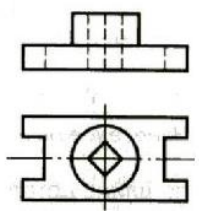
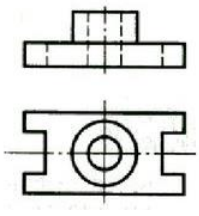
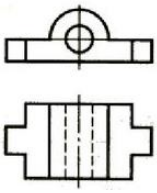
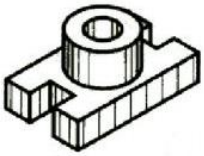
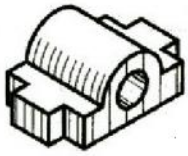
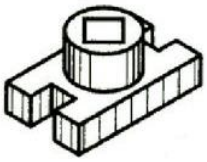
### *Общая часть*

*Впишите правильный ответ*

**1.** 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?

*Установите соответствие*

**2.** По видам деталей определите их наглядные изображения

| | | |
|---|---|---|
| а)  | б)  | в)  |
| 1.  | 2.  | 3.  |

*Выберите правильный ответ*

**3.** Укажите название технологии 3D-прототипирования, в которой для создания 3D-моделей используют жидкий фотополимер, который затвердевает под воздействием лазера, ультрафиолетового или инфракрасного излучения

а) стереолитография (SLA); б) прямое лазерное спекание (DMLS);
в) выборочная лазерная пайка (SLM); г) трёхмерное ламинирование (LOM);
д) выборочное лазерное спекание (SLS); е) электронно-лучевое плавление (EBM).

**4.** Какой инструмент использует рабочий на фотографии?

а) цепная пила; б) шуруповёрт; в) разводной ключ;
г) штангенциркуль д) отбойный молоток; г) шлицевая отвертка

*Впишите правильный ответ*

**5.** Показания счетчика холодной воды в начале месяца 243 куб.м., а в конце месяца 251 куб. м., счетчика горячей воды в начале месяца 186 куб.м., а в конце месяца 192 куб. м., счетчика электроэнергии в начале месяца 14 285 кВт*ч, а в конце месяца 14 327 кВт*ч.

1 куб.м холодной воды стоит 33 руб.
1 куб.м горячей воды стоит 163 руб.
1кВт*час электроэнергии стоит 5 руб.

Водоотвод холодной и горячей воды 23 руб в месяц.

Сколько надо заплатить в месяц за пользование холодной и горячей водой, электроэнергию и за водоотвод?

### *Специальная часть*

Вас пригласили в компанию «Конфиденциальность Inc.» в качестве специалиста по защите информации. Ваша задача – помочь компании усовершенствовать свои меры по защите конфиденциальных данных, а также обеспечить безопасность текущей системы всей компании.

Ваш первый шаг- разобраться с основными терминами.

**6.** Соотнесите термин и его определение.

| | |
|---|---|
| 1. Предоставление легальным пользователем дифференцированных прав доступа к ресурсам системы | а) Конфиденциальность |
| 2. Присвоение субъектам и объектам доступа уникального | б) Взлом |

| | |
|---|---|
| номера, шифра, кода и т.п. с целью получения доступа к информации | |
| 3. Проверка подлинности субъекта по предъявленному им идентификатору для принятия решения о предоставлении ему доступа к ресурсам системы | в) Авторизация |
| 4. Свойство, которое гарантирует, что информация не может быть доступна или раскрыта для неавторизованных личностей, объектов или процессов. | г) Аутентификация |
| 5. Удачная криптоатака | д) Идентификация |

**7.** Ваш следующий шаг – проведение аудита текущей системы безопасности компании. Выберите наиболее комплексный и корректный вариант действий.

а) Проверить, насколько сложно взломать пароли сотрудников, запуская переборщики паролей.

б) Выяснить у руководства сведения об информационной системе и на их основе составить план аудита всех аспектов безопасности.

в) Провести тестирование на проникновение сетевой инфраструктуры компании.

г) Провести попытку применения приёмов социальной инженерии к сотрудникам.

д) Попытаться проникнуть в различные помещения компании

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

а) электронная подпись

б) хрупкие цифровые водяные знаки

в) функции хэширования

г) надёжные цифровые водяные знаки

д) полухрупкие цифровые водяные знаки

е) система контроля версий программного обеспечения

**9.** Для запуска компьютера на рабочем месте сотрудника вы решили установить 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.

а) однофакторная аутентификация

б) двухфакторная аутентификация

в) трёхфакторная аутентификация

г) аутентификация на основе факторов знания и биометрии

д) аутентификация на основе факторов владения и биометрии

**10.** Что из перечисленного отличает сетевые черви от других видов вредоносного ПО?

а) Способность маскироваться под полезные программы

б) Способность распространяться по компьютерной сети через уязвимости в сетевом ПО

в) Способность выполнять деструктивные действия без ведома пользователя

г) Способность заражать исполняемые файлы, внедряя в них свой программный код

**11.** Выберите из перечисленных действий и расположите в правильной последовательности три этапа получения доступа к информации.

а) Автоматизация

б) Авторизация

в) Идентификация

г) Инициализация

д) Аутентификация

**12.** Укажите, что из перечисленного лежит в основе мандатного управления доступом?

а) Предотвращение исполнения программного кода из области данных

б) Разграничение привилегий на основе меток уровня доступа

в) Ограничение возможности вызова функций операционной системы

г) Разграничение привилегий на основе именованных субъектов и объектов

**13.** Подбери верный ответ к каждому сообщению

| | |
|---|---|
| 1) риск подвергнуться оскорблениям, нападкам, преследованиям со стороны участников интернет-общения | а) Веб-серфинг |
| | б) Техническая угроза |
| 2) навязчивое желание войти в социальные сети, интернет-магазины | в) Коммуникационная угроза |
| | г) Интернет-зависимость |
| 3) приобретение товаров ненадлежащего качества | д) Потребительская угроза |

**14.** Для обеспечения контроля пропуска сотрудников была нанята охрана и установлены пропускные турникеты, к которым сотрудники должны прикладывать смарт-карты. Какие типы аутентификации реализованы?

а) биометрическая аутентификация

б) однофакторная аутентификация

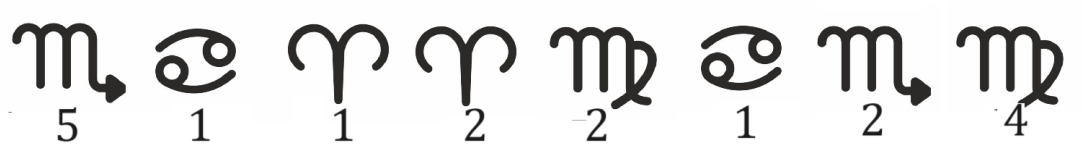
в) аутентификация по ЭЦП

г) аутентификация на основе фактора владения

д) двухфакторная аутентификация

е) многофакторная аутентификация

**15.** Интересный криптографический ребус. Расшифруй странное сообщение




**16.** Какие приёмы может использовать злоумышленник, взаимодействуя с потенциальной жертвой через электронную почту:

а) фишинг

б) скимминг

в) претекстинг

г) кардинг

д) спуфинг

**17.** 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

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

**18.** Установите шифробозначение (замену) буквы «В»

**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»?

а) ОЗЕЛЕНЕНИЕ

б) ОСТОЛБЕНЕНИЕ

в) ОСВОБОЖДЕНИЕ

г) ОПРЕДЕЛЕНИЕ

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

***Кейс-задание. (25 баллов)***

**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.