


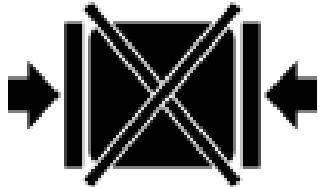
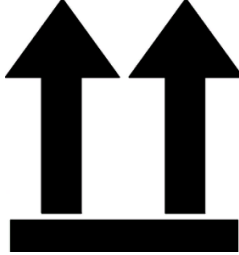
**Муниципальный этап всероссийской олимпиады школьников  
по технологии  
«Информационная безопасность»  
2023/2024 учебный год  
10-11 класс  
Максимальный балл – 100**

**Общая часть**

1. Определите какие функции выполняют представленные в таблице роботы.

		
1	2	3

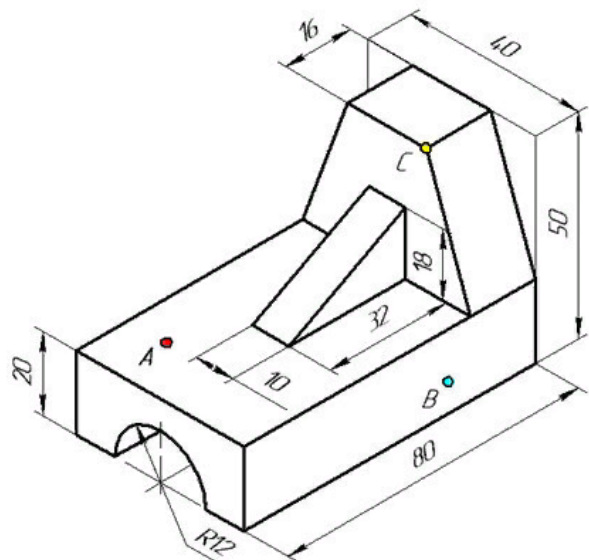
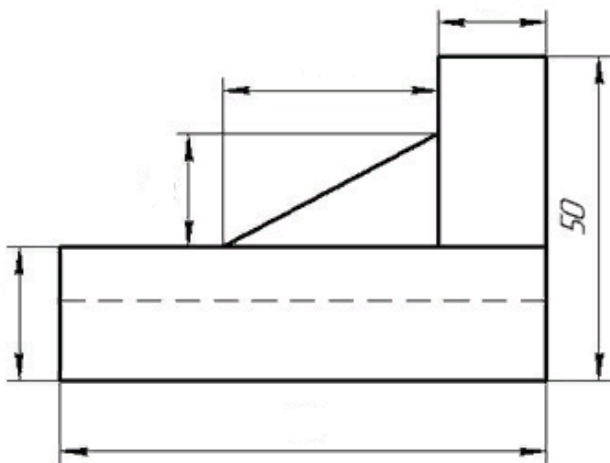
2. На упаковке товара помещают разные символы. Что обозначают символы, указанные в таблице

		
1	2	3

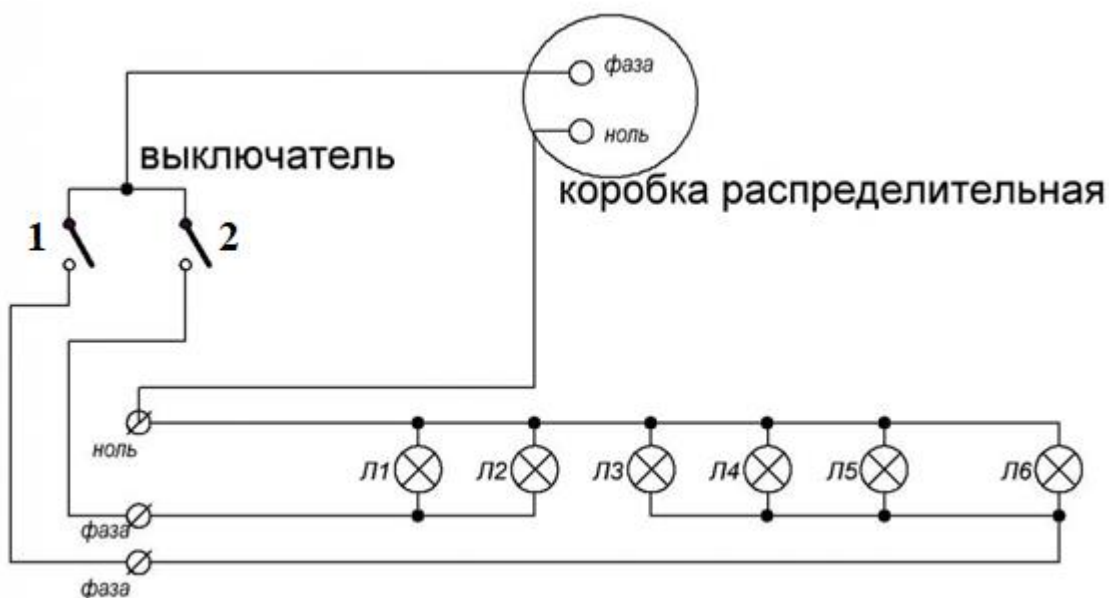
3. Продолжите предложение. Профессиональное испытание, моделирующее элементы конкретного вида профессиональной деятельности, называется

\_\_\_\_\_.

4. Проведите анализ геометрической формы детали. Соотнесите её форму и её главный вид. Внесите размеры детали на главном виде в бланке ответов.



5. Какие лампы будут гореть, если включить выключатель 2?



### Специальная часть

#### Определите один правильный ответ

6. Разработка и выполнение правил хранения и использования документов и носителей информации, определение правил доступа к информации — это меры защиты информации

- а. физические;
- б. организационные;
- в. программные;
- г. аппаратные.

7. К основным функциям системы безопасности можно отнести все перечисленное:

- а. Установление регламента, аудит системы, выявление рисков;
- б. Установка новых офисных приложений, смена хостинг-компании;

- в. Внедрение аутентификации, проверки контактных данных пользователей;
- г. Аудит системы, установка новых офисных приложений, выявление рисков.

8. При расследовании преступлений в сфере компьютерной информации подлежат выявлению следующие обстоятельства:

- а. способ совершения преступления;
- б. ввод в систему управления наличными фондами банка ложной информации о перечислении денежных средств;
- в. подключение к телекоммуникативному оборудованию компьютера вопреки воли его владельца;
- г. все ответы правильные.

9. Одним из методов защиты информации от утечки и несанкционированного использования является -

- а. криптографическое шифрование информации;
- б. постоянное использование антивирусных программ;
- в. стеганография информации;
- г. сжатие информации с помощью программ-архиваторов.

10. Что относится к классической стеганографии?

- а. невидимые чернила;
- б. микроточки;
- в. «жаргонные шифры», где слова имеют другое обусловленное значение;
- г. записи на боковой стороне колоды карт, расположенных в условленном порядке;
- д. трафареты, которые, если положить их на текст, оставляют видимыми только значащие буквы;
- е. узелки на нитках;
- ж. записи внутри варёного яйца.

11. Какие вопросы не могут быть разрешены программно-технической экспертизой:

- а. имеются ли в данном средстве компьютерной техники изменения вирусного характера;
- б. какая информация содержится на представленных физических носителях;
- в. какие текстовые документы (файлы) были уничтожены;
- г. исправно ли представленное на исследование средство компьютерной техники;
- д. кто из интересующих следствие лиц имеет доступ к конкретной информации.

12. Предметом преступного посягательства в сфере компьютерной информации является:

- а. компьютер;
- б. программное обеспечение компьютера;
- в. периферийное оборудование;
- г. информация, обрабатываемая в компьютерной системе;
- д. все ответы правильные.

13. Принцип Кирхгофа:
  - а. Секретность ключа определена секретностью открытого сообщения;
  - б. Секретность информации определена скоростью передачи данных;
  - в. Секретность информации определена секретностью сообщения;
  - г. Секретность закрытого сообщения определяется секретностью ключа.
  
14. Таргетированная атака — это:
  - а. атака на сетевое оборудование;
  - б. атака на компьютерную систему крупного предприятия;
  - в. атака на конкретный компьютер пользователя;
  - г. атака на компьютерный сайт пользователя.
  
15. Что такое CobIT и как он относится к разработке систем информационной безопасности и программ безопасности?
  - а. Список стандартов, процедур и политик для разработки программы безопасности;
  - б. Текущая версия ISO 17799;
  - в. Открытый стандарт, определяющий цели контроля;
  - г. Структура, которая была разработана для снижения внутреннего мошенничества в компаниях.
  
16. К основным типам средств воздействия на компьютерную сеть относится:
  - а. Компьютерный сбой;
  - б. Отсутствие пользователя в сети;
  - в. Логические закладки («мины»);
  - г. Аварийное отключение питания.
  
17. Какая из приведенных техник является самой важной при выборе конкретных защитных мер:
  - а. анализ рисков;
  - б. результаты ALE;
  - в. анализ затрат / выгоды;
  - г. анализ последствий.
  
18. Заключительным этапом построения системы защиты является:
  - а. Планирование;
  - б. Прогнозирование;
  - в. Анализ уязвимых мест;
  - г. Сопровождение.
  
19. Наиболее важным при реализации защитных мер политики безопасности является:
  - а. Аудит, анализ затрат на проведение защитных мер;
  - б. Аудит, анализ безопасности;
  - в. Аудит, анализ уязвимостей, риск-ситуаций;
  - г. Аудит, анализ количества обращений к сети.

20. Какое утверждение является правильным, если взглянуть на разницу в целях безопасности для коммерческой и военной организации?

- а. только военные имеют настоящую безопасность;
- б. коммерческая компания обычно больше заботится о целостности и доступности данных, а военные – о конфиденциальности;
- в. военным требуется больший уровень безопасности, т.к. их риски существенно выше;
- г. коммерческая компания обычно больше заботится о доступности и конфиденциальности данных, а военные – о целостности.

### Творческая часть

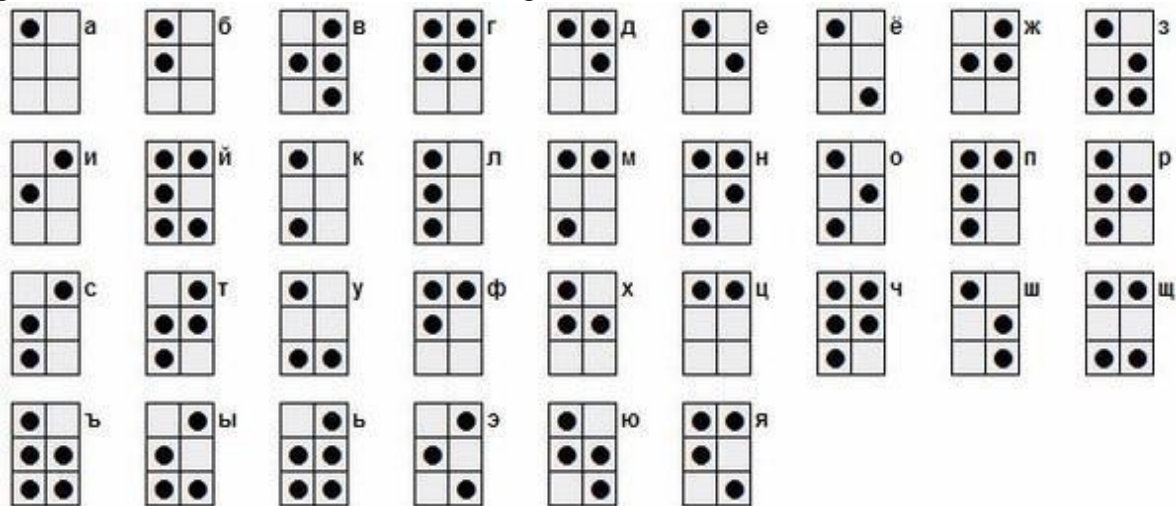
#### Задание 1

ШИФРОВКА 1						ШИФРОВКА 2					
Если вычеркнуть все повторяющиеся буквы, из оставшихся букв сложится название зодиакального созвездия.						Если вычеркнуть все повторяющиеся буквы, из оставшихся букв сложится название зодиакального созвездия.					
И	Д	Т	Е	Н	У	К	Г	О	Н	Ф	Б
Н	Х	Б	М	З	О	Д	П	Э	Ж	К	Э
К	Г	Р	Л	Х	П	У	И	М	У	Р	Л
У	П	С	А	К	Ы	Л	С	Ф	Б	А	Т
М	З	О	Т	Д	Б	Е	Т	Г	О	П	С
А	Р	И	Г	В	Л	Р	Ж	Н	В	М	И

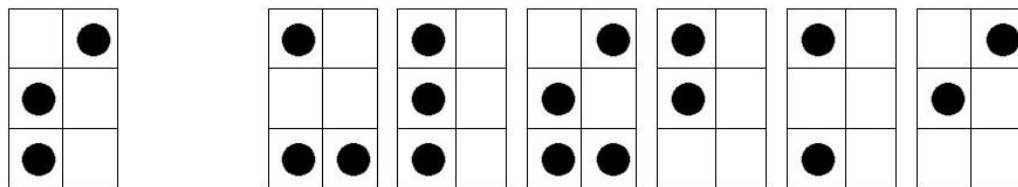
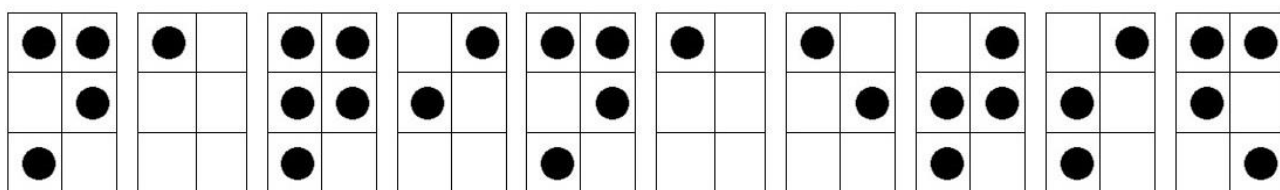
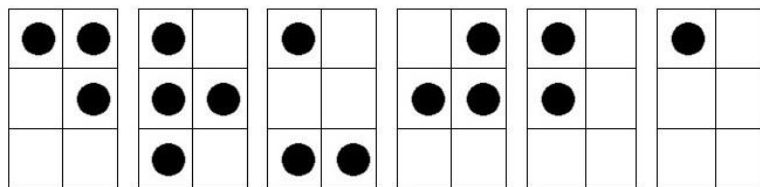
Ответ: \_\_\_\_\_

## Задание 2

Шрифт Брайля – рельефно-точечный тактильный шрифт, предназначенный для письма и чтения незрячими и плохо видящими людьми. Для изображения букв в шрифте Брайля используется шесть точек. Точки расположены в два столбца. При письме точки прокалываются, и поскольку читать можно только по выпуклым точкам, «писать» текст приходится с обратной стороны листа. Текст пишется справа налево, затем страница переворачивается, и текст читается слева направо.



Используя алфавит Брайля, расшифруйте данное сообщение.



Ответ: \_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

### Задание 3

Шифр Плейфера. Шифрование производится с помощью квадрата (или прямоугольника), в который занесены в произвольном порядке буквы и конфигурация таблицы составляют в совокупности секретный ключ. Для определённости возьмём прямоугольную таблицу размером 4\*8, в качестве букв алфавита - кириллицу, а буквы расположим в алфавитном порядке. Так как число русских букв 33, а число клеток - 32, исключим из таблицы букву Ё. Для того чтобы зашифровать сообщение необходимо разбить его на биграммы (группы из двух символов), например «криптография» становится «КР – ИП – ТО – ГР – АФ – ИЯ», и отыскать эти биграммы в таблице. Затем, руководствуясь следующими правилами, зашифровываем пары символов исходного текста:

1. Если буквы из пары букв шифруемого текста находятся в разных строках и столбцах, то в качестве заменяющих букв используются буквы, которые расположены в углах прямоугольника, охватывающего буквы открытого текста. Например, блок КР заменяется символами ИТ. (ТО заменяется на ЦК; ГР на АУ; АФ на ДР; ИЯ на ПШ)

2. Если пара букв открытого текста попадёт в одну строку, то шифрограмма получается путём циклического сдвига вправо на одну клетку. Например, блок ИП будет преобразован в ЙИ.

3. Если обе буквы открытого текста попадают в один столбец, то для шифрования осуществляют циклический сдвиг на одну клетку вниз. Так, блок ЖЦ будет преобразован в символы ОЮ, а блок ТЪ – в символы ЪВ.

Таким образом, получаем: КРИПТОГРАФИЯ – ИТЙИЦКАУДРПШ

А	Б	В	Г	Д	Е	Ж	З
И	Й	К	Л	М	Н	О	П
Р	С	Т	У	Ф	Х	Ц	Ч
Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я

Зашифруйте шифром Плейфера слово «АЛГОРИТМ».

Ответ: \_\_\_\_\_

\_\_\_\_\_

#### Задание 4

(1)Сотруднику банка Антону поступил звонок с незнакомого номера. Звонивший представился сотрудником полиции из районного отделения по адресу проживания Антона и сообщил о том, что телефонный звонок записывается. По предложению звонившего Антон сверил названную информацию с данными об уполномоченном участковом сотруднике полиции на сайте мфд.рф. Названные фамилия, имя и отчество, а также номер телефона совпадали с указанными на официальном портале. «Вчера Вы совершали оплату покупки в продуктовом магазине», – сообщил звонивший. Это было правдой. «При этом Вы вводили PIN-код на терминале». Это также было верно. «Похоже, кто-то подсмотрел Ваш номер карты и PIN-код, потому что сегодня было зафиксировано несколько покупок через интернет-магазин с Вашей карты, а также было зафиксировано несколько попыток оплаты покупки с зарубежных интернетмагазинов. Для расследования этих действий и возврата Вам денежных средств нам необходим номер карты (чтобы убедиться, что она всё-таки принадлежит Вам), а также PIN-код и код безопасности с обратной стороны карты».

(2)Поняв, что его обманывают, Антон повесил трубку и открыл электронный почтовый ящик. Там обнаружилось письмо от магазина, в котором у Антона была скидочная карта. Магазин предлагал принять участие в акции, для чего требовалось зайти на сайт этого мероприятия, имевшего очень непростое название. Имя сайта было представлено в письме в виде картинки, поэтому его требовалось ввести вручную. На открывшемся сайте предлагалось ввести данные держателя скидочной карты, её номер и номер телефона, с которым связана карта. После этого потребовалось ввести код подтверждения, который должен был прийти на введённый номер телефона. Заметив, что ввёл в адресе пару букв неверно (поменяв местами), Антон исправил ошибку. На новой странице открылся сайт акции, проводимой указанным магазином, но вместо просьбы ввести сведения указывались лишь сроки и условия проведения. Поняв, что чуть не стал жертвой мошенников, Антон закрыл браузер.

(3)Открыв приложение социальной сети, он заметил сообщение от близкого друга. «Ну как вчера погулял? Днём хорошо провели время, да? (Антон в самом деле ходил с другом на спортивное мероприятие). Впрочем, похоже, у тебя такое не редкость!»

К письму были приложены несколько фото самого Антона в автосалоне, ювелирном магазине и дорогом ресторане. Задав пару вопросов, Антон понял, что имеет дело не со своим другом, а с кем-то представляющимся им, и подал жалобу модератору.

Соотнесите злоумышленников (звонивший по телефону – 1, приславший письмо – 2 и автор сообщения в социальной сети – 3), пытавшихся реализовать угрозы информационной безопасности в отношении Антона, с использованными ими техниками. Каждый из них мог использовать более одной техники, причём одной техникой могли воспользоваться несколько злоумышленников.



Кража личности
Сниффинг
Претекстинг
Луркинг
Киберсталкинг
Фишинг
Крэкинг
Кибербуллинг
Тайпсквоттинг
Спуфинг

1
2
3

### Задание 5

Посетив археологический музей, школьник увидел там дневник мореплавателя времён парусного флота. Увы, почти весь он был повреждён водой, однако удалось разобрать строку на первой странице:

*«Фрояюуг флпуьс ц нсяоашъс. Рс нмрцм ся афроь, ьрмрэдх эдхми э троь. Улзжъ сяжъх жйлсд ц поьынмяэцмг ньюь сцзъьр съэрчтриср».*

Дешифруйте запись. В ответ запишите последнее предложение.

Ответ: \_\_\_\_\_

---