ВСЕРОССИЙСКАЯ ОЛИМПИАДА ШКОЛЬНИКОВ
ТЕХНОЛОГИЯ. НАПРАВЛЕНИЕ «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»
2022–2023 уч. г. ШКОЛЬНЫЙ ЭТАП. 9–11 КЛАССЫ

ОТВЕТЫ И КРИТЕРИИ ОЦЕНИВАНИЯ

Максимальная оценка за работу – 60 баллов.

Название части и № задания	**Тип задания**	**Критерии**
Задание 1	Выбрать один ответ	1 балл
Задание 2	Выбрать один ответ	2 балла
Задание 3	Краткий ответ	3 балла
Задание 4, 5	Краткий ответ	2 балла
Задание 6	Выбрать один ответ	За каждый правильный ответ – 1 балл Максимальная оценка 5 баллов
Задание 7–13	Выбрать один ответ	За каждое задание –2 балла
Задание 14	Выбрать один ответ	3 балла
Задание 15	Выбрать несколько ответов	За каждый правильный ответ – 2 балла За каждый неправильный ответ – штраф 2 балла Если отмечено более четырёх ответов – 0 баллов Максимальная оценка 6 баллов
Задание 16	Открытый ответ	За полностью верный ответ – 13 баллов
Задание 17	Установить соответствие	За каждую верную пару – 1 балл За каждую неверную пару – штраф 0,5 балла Максимальная оценка 9 баллов

Задание 1
1 балл

Из предложенных рисунков выберите тот, на котором изображён 3D-принтер.

		
+ 		

Задание 2
2 балла

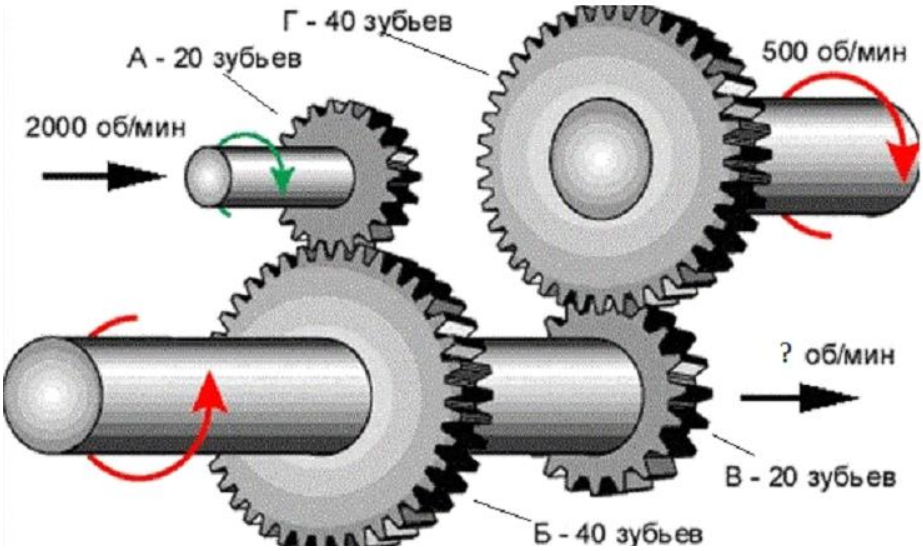
Манипуляционные знаки – это знаки на упаковке, которые указывают на способы обращения с упаковкой и упакованным в неё грузом.

Какой манипуляционный знак необходимо изобразить на упаковке товара, который необходимо беречь от влаги?

 +			

Задание 3
3 балла

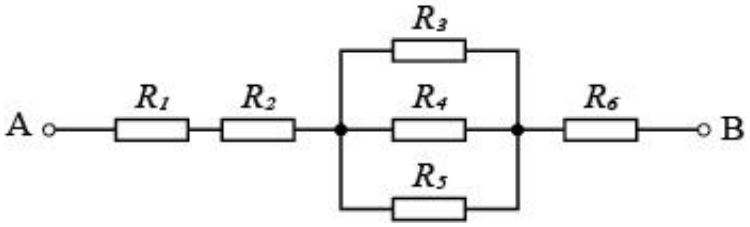
Определите, сколько оборотов за 3 минуты сделает шестерёнка В.



Ответ: 3000.

Задание 4
2 балла

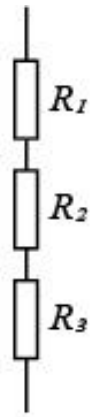
Никита соединил несколько резисторов следующим образом:



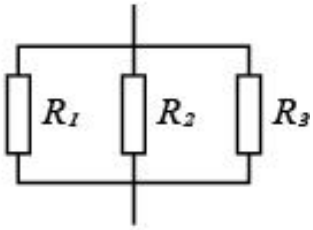
Определите величину общего сопротивления участка AB (R). $R_1 = 2$ Ом, $R_2 = 2$ Ом, $R_3 = R_4 = R_5 = 1$ Ом, $R_6 = 3$ Ом. Ответ выразите в омах, округлив результат до десятых.

Справочная информация

При последовательном соединении резисторов и параллельном соединении резисторов общее сопротивление рассчитывается следующим образом, как показано ниже:



$$R = R_1 + R_2 + R_3$$

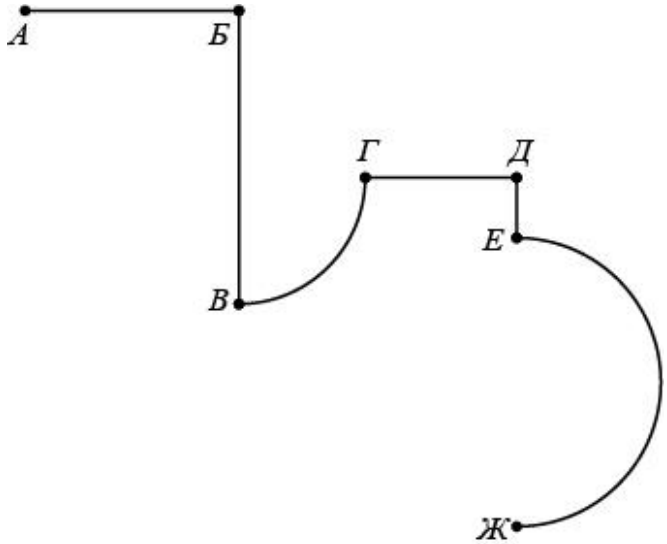


$$R = \frac{1}{\frac{1}{R_1} + \frac{1}{R_2} + \frac{1}{R_3}}$$

Ответ: 7,3.

Задание 5
2 балла

Определите длину траектории АЖ, которая изображена на рисунке. Диаметр большой окружности равен 50, а радиус маленькой равен 20. Участок *АБ* = 30, *БВ* = 50, *ГД* = 20, *ДЕ* = 10.



Справочная информация

Длина окружности $L = 2 \cdot \pi \cdot R$, где число $\pi \approx 3{,}14$, а R–радиус окружности.

Ответ: 219,9.

Задание 6
5 баллов

Верны ли следующие утверждения?

Киберпреступность – это противозаконная деятельность, совершаемая с использованием сети Интернет.	Верно	**Неверно**
Часть угроз информационной безопасности может создаваться случайно.	**Верно**	Неверно
Для преодоления мер защиты хакеры всегда полагаются на ошибки программного или аппаратного обеспечения.	Верно	**Неверно**
Уязвимость – недостаток атакуемой системы, возникающий в результате успешной кибератаки.	Верно	**Неверно**
Полученные из любых источников файлы документов (текстовые, изображения, таблицы) можно открывать, не опасаясь нанести вред компьютеру.	Верно	**Неверно**

Задание 7
2 балла

Кража личности подразумевает использование чужих

- **персональных данных**
- документов
- учётных записей в социальных сетях
- списков контактов

Задание 8
2 балла

Система аутентификации, требующая от пользователя ввода определённой комбинации символов, называется

- **парольной**
- биометрической
- лингвистической
- мнемонической

Задание 9
2 балла

Перегружая сервер запросами, нарушители реализуют

- **атаку отказа в обслуживании**
- атаку прямого доступа
- несанкционированный доступ
- крэкерскую атаку

Задание 10
2 балла

Под спуфингом обычно понимают приёмы, связанные с

- **подменой информации**
- искажением информации
- похищением информации
- утечкой информации

Задание 11
2 балла

Каналы утечки информации, не предполагающие влияния на работающую систему или взаимодействия с системой, называются

- пассивными
- **побочными**
- непроявляющимися
- естественными

Задание 12
2 балла

Побуждение перейти по ссылке, ведущей на клон сайта банка, на котором требуется ввести личные данные, называется

- **фишингом**
- кардингом
- скиммингом
- тайпсквоттингом

Задание 13
2 балла

Для защиты от утечки информации, передаваемой по беспроводному (wi-fi) каналу связи, может применяться

- межсетевой экран
- **шифрование информации**
- зашумление канала
- антивирус

Задание 14
3 балла

Вася обнаружил, что в его аккаунт в соцсети был совершён вход с неизвестного устройства. Вспоминая свои действия за день, он пришёл к выводу, что причиной утечки пароля могло(-а) стать

- подключение к проектору в школе для демонстрации презентации
- отправка электронного письма через почтовый клиент
- **авторизация в соцсети при подключении к wi-fi в кафе**
- подключение беспроводной мыши из класса информатики

Задание 15
6 баллов

Выберите все приёмы, которые может применить злоумышленник, взаимодействуя с потенциальной жертвой через электронную почту.

- **фишинг**
- **спуфинг**
- **претекстинг**
- кардинг
- скимминг

Задание 16
13 баллов

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 флпуъс ц нсяоашъс. Рс нмрцм ся афроъ, ьрмрэдх эдхмц э троъ. Улзжъ сяжъх жйлсд ц поъынмяэцмг нъюъ сцзъьр съэрчтршср».

Дешифруйте запись. В ответ запишите последнее предложение.

Ответ: Лучше нашей шхуны и представить себе ничего невозможно.

Задание 17
9 баллов

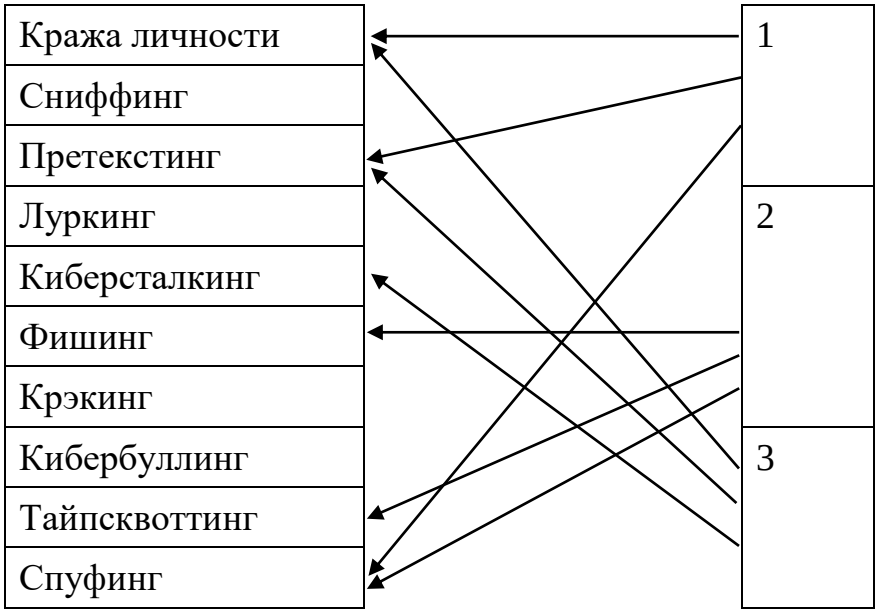
(1)Сотруднику банка Антону поступил звонок с незнакомого номера. Звонивший представился сотрудником полиции из районного отделения по адресу проживания Антона и сообщил о том, что телефонный звонок записывается. По предложению звонившего Антон сверил названную информацию с данными об уполномоченном участковом 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 интернет-магазинов. 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.



Максимальная оценка за работу – 60.