ВСЕРОССИЙСКАЯ ОЛИМПИАДА ШКОЛЬНИКОВ 2024/2025 гг.
ШКОЛЬНЫЙ ЭТАП
ТЕХНОЛОГИЯ
7-8 КЛАСС

МАТЕРИАЛЫ ДЛЯ ЧЛЕНОВ ЖЮРИ (КЛЮЧИ, КРИТЕРИИ)

МАКСИМАЛЬНОЕ КОЛИЧЕСТВО БАЛЛОВ - 60.

Общая часть (5 баллов)

1. **(1 балл)** Определите, к каким основным типам профессий относится профессия «графический дизайнер».

1) человек – знак
2) человек – природа
3) человек – техника
4) человек – человек
5) человек – художественный образ

2. **(1 балл)** Назовите составной элемент FFF (Fused Filament Fabrication) 3Dпринтера, предназначенный для нагрева и выдавливания термопластика через специальное сопло в зону печати.

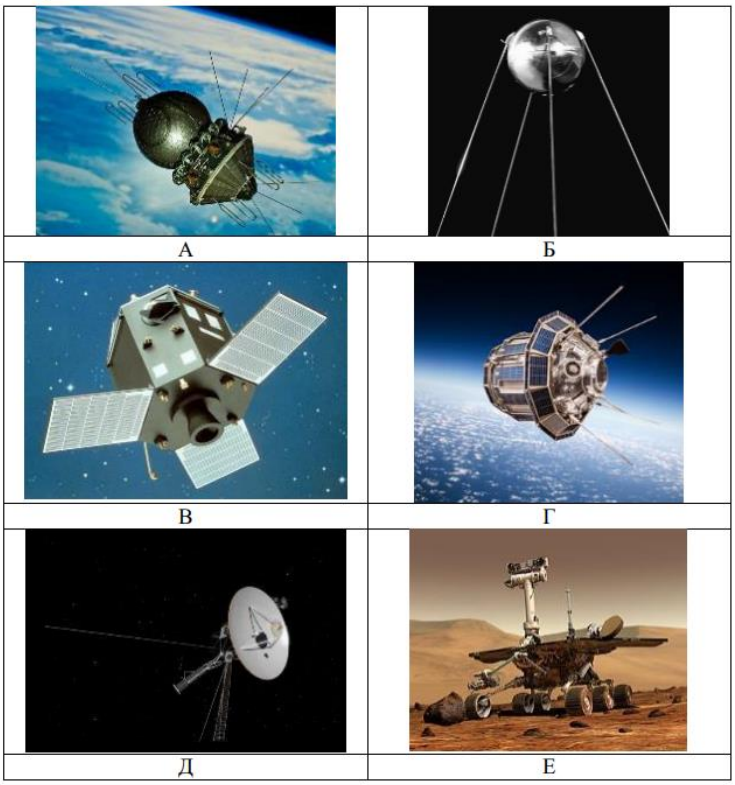
1) воронка
2) комбайн
3) цилиндр
4) филамент
5) экструдер
6) эксцентрик

3. **(1 балл)** Из предложенных изображений выберите два, на которых изображены инструменты, основанные на рычаге первого рода

Ответ: Б, З

4. (1 балл) 4 октября 1957 года на орбиту Земли был выведен первый искусственный спутник Земли, советский космический аппарат, который назывался «Спутник-1». Он получил кодовое обозначение — «ПС-1» («Простейший Спутник-1»).

Рассмотрите предложенные изображения. Среди них выберите то, на котором изображён ПС-1.



Ответ: Б

5. (1 балл) При благоустройстве парка было решено посыпать несколько тропинок песком. Длины тропинок равны 45 м 5 см, 12 м 6 дм 9 см, 707 дм и 314 см. Определите общую длину тропинок, которые решили посыпать песком. Ответ дайте в сантиметрах.

Ответ: 13158

Специальная часть (45 баллов)

1. (2 балла, по 1 баллу за каждую расшифрованную аудиторию)

Расшифруйте аббревиатуры:

АСОД Автоматизированная система обработки данных

КСЗИ Комплексная система защиты информации

2. (2 балла) Вставьте пропущенное слово/словосочетание в следующем утверждении:

Аутентификация – это процесс подтверждения ***ЛИЧНОСТИ ПОЛЬЗОВАТЕЛЯ,*** *часто используется в сочетании с паролями, биометрическими данными или одноразовыми кодами.*

3. (2 балла) Вставьте пропущенные слова/словосочетания в следующее утверждение

Под субъектами системы информационной безопасности понимают активные компоненты системы, которые могут стать причиной потока информации от объекта к субъекту или изменения системы. В качестве субъектов могут выступать ***ПОЛЬЗОВАТЕЛИ****, активные программы и процессы.*

4. (2 балла) Примером двухфакторной аутентификации является запрос пользователю:

1) ввести пароль и ответить на секретный вопрос;
2) приложить электронную карту к сканеру и ввести PIN-код;
3) пройти распознавание лица и затем отсканировать отпечаток пальца;
4) подключить электронный ключ (токен) и отсканировать штрихкод пропуска.

Ответ: 2

5. (2 балла) В мандатной модели разграничения доступа определение того, имеет липользователь право доступа к файлу, определяется на основе

1) наличия или отсутствия у данного пользователя прав доступа к данному файлу;
2) соотношения метки (уровня) секретности файла и уровня допуска пользователя;
3) установленного для файла режима доступа;
4) роли (уровня) пользователя в системе.

Ответ: 2

6. (2 балла) Стеганография – это категория мер защиты информации:

1) основанных на сохранении в секрете факта передачи и хранения информации;
2) предназначенных для усиления криптографии;
3) предназначенных для передачи секретной информации из системы;
4) основанных на криптографии, но не требующих от пользователей использовать секретные ключи;

Ответ: 1

7. (2 балла) Среди вредоносных программ различных классов создавать собственныекопии могут:

1) троянские программы;
2) сетевые черви;
3) руткиты;
4) шифровальщики;

Ответ: 2

8. (2 балла) Укажите, что из перечисленного может составлять коммерческую тайну:

1) Сведения о загрязнении окружающей среды, состоянии противопожарной безопасности, санитарно-эпидемиологической и радиационной обстановке.

2) Сведения об устройстве или компонентном составе некоторого изделия.

3) Сведения, содержащиеся в учредительных документах юридического лица.

4) Сведения об использовании государственным или муниципальным предприятием средств соответствующих бюджетов.

5) Сведения о задолженности организации по заработной плате.

Ответ: 3

9. (5 баллов) 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. Далее система осуществляет пилотирование по указаниям наземных служб, передавая управление пилоту в случае необходимости принятия решений, возникновении внештатных ситуаций и в иных предусмотренных случаях.

Оцените, какие из утверждений являются верными, а какие нет.

1) Для обеспечения корректного исполнения поступающих от наземных служб указаний требуется обеспечить, в первую очередь, их конфиденциальность.

2) Для того, чтобы наземные службы могли постоянно следить за координатами самолёта, требуется обеспечить доступность этих данных.

3) Для корректного принятия решений системой пилотирования с учётом параметров самолёта необходимо обеспечить целостность этих данных в памяти программы.

4) Пилоты в момент пилотирования могут рассматриваться в качестве потенциальных нарушителей безопасности информации в системе.

5) Во время полёта пассажирам может быть запрещено использовать коммуникационные устройства из-за возможности нарушения доступности сигналов от наземных служб при случайном совпадении частот сигналов и внесения искажений.

Ответ: Верные утверждения: 2,3,4 Неверные утверждения: 1,5

10. (4 балла) Сопоставьте категории вредоносного программного обеспечения с их характерными особенностями.

11.

Категория вредоносного программного обеспечения	**Характерные особенности**
1) вирус	А) может создавать собственные копии
2) руткит	Б) маскируется под легальную программу
3) троянская программа	В) блокирует доступ к пользовательским данным
4) шифровальщик	Г) позволяет нарушителю скрывать активность в системе

Ответ: 1- А, 2-Г, 3-Б, 4-В

Задания 10-11

С помощью шифра Цезаря осуществляется шифрование сдвигом. Каждая из букв алфавита заменяется на букву, находящуюся от неё на определённом расстоянии слева или справа.

Если в качестве ключа взять пару «Ё – Я», то часть таблицы замены будет выглядеть следующим образом:

Исходный текст	**А**	**Б**	**В**	**Г**	**Д**	**Е**	**Ё**	**Ж**	**З**	**И**	**Й**	**К**	**Л**	**М**	**Н**	**О**	**П**
Зашифрованный текст						Ю	Я	А	Б	В	Г	Д					

Исходный текст	**Р**	**С**	**Т**	**У**	**Ф**	**Х**	**Ц**	**Ч**	**Ш**	**Щ**	**Ъ**	**Ы**	**Ь**	**Э**	**Ю**	**Я**
Зашифрованный текст																

12. (4 балла) С помощью данного шифра зашифруйте слово ПАРАЛЛЕЛОГРАММ.

В ответ запишите последовательность букв без кавычек и пробелов.

Ответ: ИЩЙЩЕЕЮОЕЗЬЙЩЁЁ

13. (4 балла) С помощью данного шифра расшифруйте слово ДЗЭВНВДЩЛЗЙ.

В ответ запишите последовательность букв без кавычек и пробелов.

Ответ: КОДИФИКАТОР

12. (12 баллов, по 1,5 балла за каждое слово и знак препинания) 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 и запятой):

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

Напишите слова из зашифрованного сообщения.

Ответ: ЧЕМ СЛОЖНЕЕ МЕТОД, ТЕМ МЕНЬШЕ СВОБОДЫ.

Кейс-задание (10 баллов)

Сформулируйте 10 основных правил безопасности в Интернете (Участник может дать близкие по смыслу формулировки). **По 1 баллу за каждое правило**

1) Используйте надежный пароль.

2) Заходите в интернет с компьютера, на котором установлен антивирус.

3) Заведите один основной почтовый адрес и придумайте к нему сложный пароль.

4) Если Вы хотите скачать какой-то материал из интернета, на сайте где не нужна регистрация, но от Вас требуют ввести адрес своей электронной почты, то, скорее всего, на Ваш адрес будут высылать рекламу или спам. В таких случаях пользуйтесь одноразовыми почтовыми ящиками.

5) Скачивайте программы либо с официальных сайтов разработчиков. Не скачивайте программы с подозрительных сайтов или с файлообменников.

6) Не нажимайте на красивые баннеры или рекламные блоки на сайтах, какими бы привлекательными и заманчивыми они не были.

7) Если Вы работаете за компьютером, к которому имеют доступ другие люди

(на роботе или в интернет кафе), не сохраняйте пароли в браузере.

8) Не открывайте письма от неизвестных Вам пользователей (адресов) или письма с оповещением о выигрыше в лотереи, в которой Вы просто не участвовали.

9) Не нажимайте на вплывающие окна, в которых написано, что Ваша учетная запись в социальной сети заблокирована.

10) Периодическим меняйте пароли на самых важных сайтах.