ВСЕРОССИЙСКАЯ ОЛИМПИАДА ШКОЛЬНИКОВ
ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ. 2025 г.
ПРИГЛАСИТЕЛЬНЫЙ ЭТАП. 6–7 КЛАССЫ

Максимальный балл за работу – 30.

1. Выберите **три** характерные особенности для ролевой модели разграничения доступа.

- добавление нового объекта сводится к присвоению единственного атрибута
- добавление нового объекта требует заполнения столбца матрицы
- добавление субъектов с аналогичным набором прав осуществляется заполнением одной строки матрицы доступа
- определение наличия права доступа производится на основе сопоставления двух значений
- права доступа предоставляются к неразделимым группам объектов
- допускает настройку произвольных прав доступа для субъекта

2. Саша хочет придумать пароль в соответствии с маской: **H_*?@#_!9dZ** со следующими условиями:

– Звёздочка (*) обозначает латинскую букву или цифру.
– Вопросительный знак (?) обозначает цифру.
– Символ @ обозначает одну из следующих специальных букв: A, B, C.
– Символ # обозначает одну из следующих цифр: 3, 5, 7.
– Остальные символы должны оставаться неизменными.

Какие **три** из нижеперечисленных паролей соответствуют предложенной маске?

- H_a5A3_!9dZ
- H_1C7_!9dZ
- H_x?@3_!9dZ
- H_B8#_!9dZ
- H_d5B5_!9dZ
- H_5B5_!9bZ
- H_00A7_!9dZ

3. Имеется следующее сообщение:

8192 65536 16 1024 32768

Какое слово скрыто в данном сообщении?

4. Составьте сообщение из числовых данных таким же образом, как в предыдущем задании, в котором будет скрыто слово ВИЗА. В ответ запишите последовательность чисел, не разделяя пробелами.

5. Пароль от сейфа содержит три цифры.

Известно, что:

- среди цифр не должно быть 0, 2, 7 и 9
- число, которое составлено из трёх цифр кодовой комбинации должно делиться на 3
- каждую цифру можно использовать не более 1 раза

Сколько существует комбинаций, которые удовлетворяют всем трём условиям?

6. Дан квадрат, называющийся магическим. В каждой его строке, в каждом его столбце и в каждой его диагонали сумма цифр одинакова. Известно, что ключом к шифрованию был представленный на картинке квадрат. Расшифруйте послание **СХВТРКАОЕ**. В ответ запишите получившееся слово.

2	**7**	**6**
9	**5**	**1**
4	**3**	**8**

7. Шифр Цезаря является одним из самых простых и древних методов шифрования. Схема шифрования очень проста: используется сдвиг буквы алфавита на фиксированное число позиций. Какой основной недостаток этого метода, который делает его небезопасным для использования в современных условиях?

- Ограниченная возможность использования при шифровании длинных сообщений.
- Большое количество ключей, которые возможно использовать для записи и расшифровки сообщения.
- Возможна расшифровка сообщения без использования ключа, например перебором.
- Нет возможности автоматизировать шифровку сообщений.

8. 15-летняя Аня хочет получить от родителей на 8 Марта подарок, но родители не знают, что ей подарить. Поэтому Аня решила помочь им с выбором подарка и дать родителям записку с загадочной последовательностью цифр и зашифрованным посланием о трёх её самых любимых увлечениях. Аня также оставила подсказку родителям: «Дорогие родители, обратите внимание на длину всего зашифрованного послания, на делители найденной длины и на последовательность цифр в записке».

Последовательностью цифр: 35124**.**

Зашифрованное сообщение: РБАКОИААТКМАГИНИАСТКЛФГОЬ.

Какие увлечения зашифровала Аня в послании? Ответ запишите без пробелов.

9. Установите соответствия между методами защиты информации и угрозами информационной безопасности.

Угрозы информационной безопасности: внедрение вредоносного ПО, неавторизованный доступ, утрата данных, сниффинг-атака.

Использование брандмауэра (файервола)
Обновление антивирусного ПО
Аутентификация и контроль доступа
Резервное копирование данных

Внедрение вредоносного ПО
Неавторизованный доступ
Утрата данных
Сниффинг-атака

10. Для каждого описанного ниже примера определите вид кибермошенничества.

Виды кибермошенничества: кардинг, скимминг, фишинг.

- Мошенники при помощи определённых технических инструментов копируют магнитную полосу платёжной карты и считывают её пин-код. На основе полученных данных злоумышленники изготавливают поддельную пластиковую карту, при использовании которой деньги списываются с оригинала.

- Мошенники создают сайт, который будет пользоваться доверием у пользователей, так как похож на сайт банка. Злоумышленники, представляясь сотрудниками банка, присылают пользователям ссылку на этот сайт, через который и происходит похищение реквизитов карт.

- Мошенники берут реквизиты платёжных карт со взломанных серверов интернет-магазинов, платёжных и расчётных систем, а также с персональных компьютеров держателей платёжных карт.

Максимальный балл за работу – 30.