

**Теоретические задания муниципального этапа  
всероссийской олимпиады школьников по технологии 2023-24 учебного года  
профиль «Информационная безопасность»  
7-8 класс  
(время выполнения не более 90 минут)  
Общая часть**

1. Лицо, самостоятельно создавшее информацию либо получившее на основании закона или договора право разрешать или ограничивать доступ к информации:
  - 1) Источник информации
  - 2) Потребитель информации
  - 3) Уничтожитель информации
  - 4) Носитель информации
  - 5) Владелец информации
  
2. Обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее владельца это:
  - 1) Электронное сообщение
  - 2) Распространение информации
  - 3) Предоставление информации
  - 4) Конфиденциальность информации
  - 5) Доступ к информации
  
3. Возможность получения информации и ее использования это:
  - 1) Сохранение информации
  - 2) Распространение информации
  - 3) Предоставление информации
  - 4) Конфиденциальность информации
  - 5) Доступ к информации
  
4. Отношения, связанные с обработкой персональных данных, регулируются законом...
  - 1) «Об информации, информационных технологиях»
  - 2) «О защите информации»
  - 3) Федеральным законом «О персональных данных»
  - 4) Федеральным законом «О конфиденциальной информации»
  - 5) «Об утверждении перечня сведений конфиденциального характера»
  
5. Последствиями сетевой атаки для Вашего компьютера могут быть (несколько вариантов):
  - 1) неработоспособность программ
  - 2) поломка компьютера
  - 3) кража или уничтожение информации
  - 4) заражение компьютера вредоносными программами

**Специальная часть**

1. Какая категория является наиболее рискованной для компании с точки зрения вероятного мошенничества и нарушения безопасности?
  - а) Сотрудники
  - б) Хакеры
  - в) Атакующие
  - г) Контрагенты (лица, работающие по договору)

2. Выберите наиболее точное определение понятия «Информационная безопасность»

- 1) Набор программ, которые обеспечивают всестороннюю защиту конфиденциальной корпоративной информации от неправильного использования, несанкционированного доступа, искажения или уничтожения.
- 2) Набор руководящих документов, которые обеспечивают всестороннюю защиту конфиденциальной корпоративной информации от неправильного использования, несанкционированного доступа, искажения или уничтожения.
- 3) Набор процедур и инструментов, которые обеспечивают всестороннюю защиту конфиденциальной корпоративной информации от неправильного использования, несанкционированного доступа, искажения или уничтожения.

3. Какая основная цель компьютерного вируса, отличающая его от остальных вредоносных программ?

- 1) Нанесение вреда программам и данным
- 2) Распространение своих копий
- 3) Повреждение компьютера
- 4) Блокирование работы компьютерной сети

4. Блокчейн – это

- 1) Выстроенная по определённым правилам непрерывная последовательная цепочка блоков (связный список), содержащих информацию.
- 2) Метод потоковой обработки данных
- 3) Это альтернативное название криптовалюты Биткоин
- 4) Выстроенная по определённым правилам непрерывная последовательная цепочка блоков (связный список), содержащих информацию и хеш-суммы.

5. Хеш-сумма это

- 1) Результат расчета специальной хэш-функцией. Основная особенность такой функции – невозможность обратного преобразования
- 2) Сумма четных бит информации для контроля четности
- 3) Сумма нечетных бит информации для контроля четности
- 4) Процесс проверки данных

6. Майнинг в криптосистемах – это

- 1) Деятельность по добычи полезных ископаемых в онлайн-играх
- 2) Процесс обработки транзакций при функционировании криптовалютных систем
- 3) Деятельность по созданию новых блоков в блокчейн для обеспечения функционирования криптовалютных платформ.

7. Макровирус. Обычно под этим понятием подразумевают

- 1) Вирусы, имеющие очень большой охват компьютеров по всему миру
- 2) Представляют собой макросы, встраиваемые в табличные или текстовые документы
- 3) Вирусы, имеющие в своем программном коде специальные макросы для исполняемых файлов программ

8. Ботнет это

- 1) Сеть из зараженных информационных систем, которая действует в интересах злоумышленников
- 2) Сеть из людей, которые управляют ботами в Интернет
- 3) Вирус в системе, распространяющийся по компьютерной сети

9. Выберите пункт, описывающий основные объекты информационной безопасности:
- 1) Компьютерные сети, базы данных
  - 2) Информационные системы, психологическое состояние пользователей
  - 3) Бизнес-ориентированные, коммерческие системы
10. Основными рисками информационной безопасности являются:
- 1) Искажение, уменьшение объема, перекодировка информации
  - 2) Техническое вмешательство, выведение из строя оборудования сети
  - 3) Потеря, искажение, утечка информации
11. Когда получен спам по e-mail с приложенным файлом, следует
- 1) Прочитать приложение, если оно не содержит ничего ценного – удалить
  - 2) Сохранить приложение в парке «Спам», выяснить затем IP-адрес генератора спама
  - 3) Удалить письмо с приложением, не раскрывая (не читая) его
12. ЭЦП – это:
- 1) Электронно-цифровой преобразователь
  - 2) Электронно-цифровая подпись
  - 3) Электронно-цифровой процессор
13. Утечкой информации в системе называется ситуация, характеризуемая:
- 1) Потерей данных в системе
  - 2) Изменением формы информации
  - 3) Изменением содержания информации
14. Окончательно, ответственность за защищенность данных в компьютерной сети несет:
- 1) Администратор сети
  - 2) Владелец сети
  - 3) Пользователь сети
15. Отличие страниц, адрес которых начинается с https от страниц http состоит в
- 1) это запись адреса страницы по протоколу гипертекстовой разметки
  - 2) альтернативная форма записи электронного адреса, используемая в современных информационных системах
  - 3) используется шифрование передаваемых данных по протоколу ssl

### **Кейс-задание**

В ходе радиоразведки вы перехватили следующее сообщение  
Ёфирг зинхцётёдца цтыст.

По некоторым предположениям, оно зашифровано шифром Цезаря со сдвигом от 1 до 5. Вам необходимо расшифровать сообщение и определить значение коэффициента сдвига  $k$ .