ЗОЛОТОЕ СЕЧЕНИЕ
ФОНД ПОДДЕРЖКИ ТАЛАНТЛИВЫХ ДЕТЕЙ И МОЛОДЕЖИ

ВСОШ

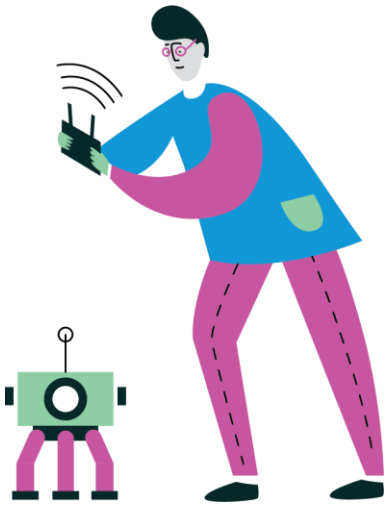
Разбор заданий школьного этапа всероссийской олимпиады школьников по технологии (информационная безопасность) 9 класс

2024/2025 учебного года в Свердловской области

Разработчик –
Алексеевский Петр Иванович,
ст. преп. кафедры ИИТиМОИ
УрГПУ

Виды заданий

- Общие теоретические вопросы:
  - с одним правильным вариантом ответа;
  - с несколькими вариантами ответа (обычно с двумя).
- Вычислительные задачи.
- Задания-головоломки на тему криптографии.



Классификация вредоносного ПО

Вид ПО	Определяющая характеристика
Вирус	Распространение путём встраивания собственного программного кода в исполняемые модули (как на устройствах хранения, так и непосредственно в ОЗУ).
Червь	Распространение с использованием уязвимостей в программном обеспечении (преимущественно сетевом - «сетевые черви»).
Троян	Распространение с использованием методов социальной инженерии (т. е. в конечном итоге виноват пользователь).
Malware	«Malfunctioning software», условно-вредоносное ПО, нарушающее работу информационной среды из-за допущенных при разработке ошибок.

Таким образом, ответы на вопрос 6 следующие:
Вариант I: В (внедрение кода)
Вариант II: Г (нарушение стабильности)

Основные компоненты информационной безопасности

- Конфиденциальность – свойство информации, предполагающее невозможность доступа к ней третьих лиц.
- Целостность – свойство информации, предполагающее неизменность её с момента создания или модификации доверенным субъектом.
- Доступность – свойство информации, предполагающее наличие возможности доступа к информации субъектами, имеющими на это право, в любой разрешённый момент времени.

Таким образом, ответы на вопросы 7-8 и 10-12:
Вариант I: 7 – Б, 8 – А, 10 – А,Б, 11 – Б, 12 – Д
Вариант II: 7 – Б, 8 – А, 10 – Б,Г, 11 – Б, 12 – Г

Правовые основы информационной безопасности

- Электронная подпись
  - Регулируется федеральным законом «Об электронной подписи» от 06.04.2011 N 63-ФЗ
  - Предусмотрено два вида:
    - Простая электронная подпись — используется в основном для проверки личности владельца.
    - Усиленная электронная подпись — используется для подписи документов.
      - Любое изменение подписанного документа приводит к ошибке проверки подписи.

Таким образом, ответы на 13 вопрос:
Вариант I: A
Вариант II: B

ЗОЛОТОЕ СЕЧЕНИЕ
ФОНД ПОДДЕРЖКИ ТАЛАНТЛИВЫХ ДЕТЕЙ И МОЛОДЕЖИ

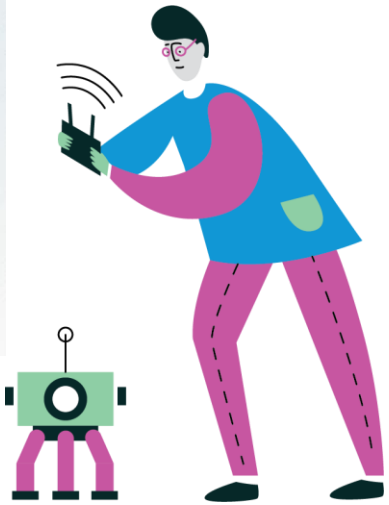
ВСОШ
ТЕХНОЛОГИЯ
ВСЕРОССИЙСКАЯ ОЛИМПИАДА ШКОЛЬНИКОВ

Программные средства защиты информации

- ОС Аврора является одной из немногих мобильных ОС, полностью соответствующих требованиям законодательства РФ к обеспечению конфиденциальности данных. (Вариант I, 15 — Г)
- Android Open Source Platform (AOSP) — минимальная платформа на базе ОС Android, содержащая только компоненты с открытым исходным кодом, выпускающиеся под свободными лицензиями. Ввиду отсутствия компонентов от сторонних разработчиков и наличия возможности аудита безопасности, такая платформа является предпочтительной в плане безопасности, при отсутствии более подходящих альтернатив. (Вариант II, 15- Б)
- SecureBoot — проприетарное решение, предотвращающее запуск неподписанного загрузчика операционной системы. Несмотря на возможность реализации с его помощью одного из компонентов доверенной вычислительной среды, в целом в этой роли решение бесполезно ввиду простоты отключения. (Вариант II, 24)

Технические средства обеспечения информационной безопасности

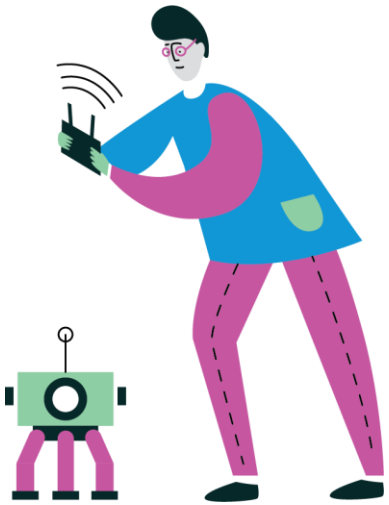
- Криптографические токены, смарт-карты и другие похожие устройства — представляют собой доверенное хранилище реквизитов (как криптографических ключей, так и алгоритмов, выполняющихся на самой смарт-карте). Токены (выглядят как USB Flash-накопители, хотя таковыми не являются) обычно представляют собой смарт-карту и устройство для работы с ней, объединённые в единую конструкцию.



Вариант I: 14 — В

Технические средства обеспечения информационной безопасности

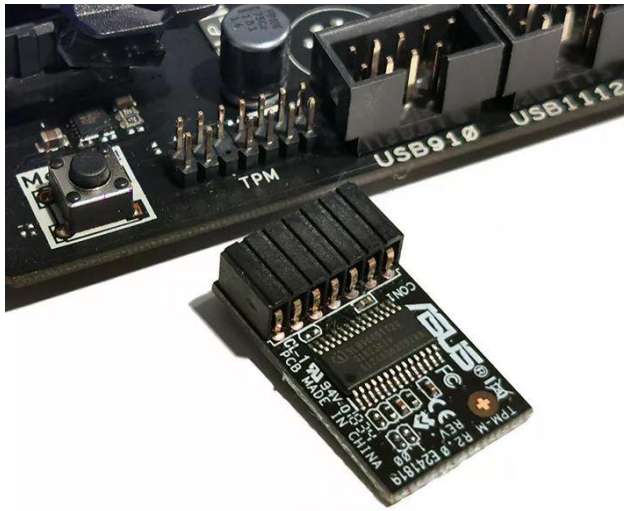
- OTP-генераторы — устройства для генерации одноразовых паролей с помощью специальных алгоритмов. За исключением кнопки включения и дисплея, обычно не имеют никаких средств взаимодействия с внешним миром. Для вычисления ключа используют встроенные часы, синхронизированные с сервером.

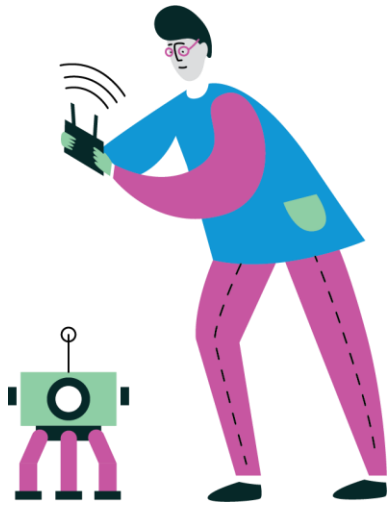


Вариант II: 14 - Г

Технические средства обеспечения информационной безопасности

- TPM-модуль — специализированное устройство, реализующее функции доверенного хранилища ключей, криптопроцессора и датчика случайных чисел.
- Если какое-либо криптографическое ПО использует этот модуль, то его извлечение приводит к невозможности работы этого ПО, в том числе, к невозможности загрузки ОС, если содержимое жёсткого диска зашифровано хранящимся в модуле ключом. (Вариант II, 24)





ЗОЛОТОЕ СЕЧЕНИЕ
ФОНД ПОДДЕРЖКИ ТАЛАНТЛИВЫХ ДЕТЕЙ И МОЛОДЕЖИ

ВСОШ
ТЕХНОЛОГИЯ ВСЕРОССИЙСКАЯ ОЛИМПИАДА ШКОЛЬНИКОВ

Технические средства обеспечения информационной безопасности

- RAID (Redundant Array of Independent Disks, избыточный массив самостоятельных дисков) — одна из технологий повышения надёжности (отказоустойчивости) и/или производительности подсистемы хранения данных.
- Модель RAID имеет несколько уровней, среди которых наиболее распространены представленные в соответствующем задании 0, 1, 5, 6, 1+0, 5+0.
- Уровень 0 предназначен для повышения производительности, обычно в ущерб надёжности
- Уровень 1 — полное дублирование данных на нескольких дисках, и этот вариант мог бы быть правильным ответом на вопрос, если бы присутствовал в списке как самостоятельный.
- Уровни 5 и 6 добавляют избыточность с использованием различных алгоритмов, и допускают выход из строя соответственно любого одного или двух дисков.
- «Гибридные» уровни 1+0 и 5+0 позволяют повысить производительность, в какой-то мере сохраняя надёжность (но не повышая её).
- Правильным ответом на задание 20 варианта II является B. RAID 6 — единственный уровень из предлагаемых, допускающий выход из строя одновременно двух любых дисков.

ЗОЛОТОЕ СЕЧЕНИЕ
ФОНД ПОДДЕРЖКИ ТАЛАНТЛИВЫХ ДЕТЕЙ И МОЛОДЕЖИ

ВСОШ
ТЕХНОЛОГИЯ
ВСЕРОССИЙСКАЯ ОЛИМПИАДА ШКОЛЬНИКОВ

Технические средства обеспечения информационной безопасности

- Резервное копирование — важный элемент обеспечения информационной безопасности. Оно может осуществляться на различные съёмные носители информации. При большом объёме информации, подлежащей резервному копированию, важным параметром становится стоимость хранения информации на таких носителях.
- Самый простой способ оценить стоимость хранения информации — разделить стоимость носителя на его объём. Впрочем, в реальности формула расчёта несколько сложнее, поскольку следует также учитывать срок службы носителей, а также затраты электроэнергии и [однократные] затраты на устройство для работы с этими носителями.
- Пример: жёсткий диск объёмом 4ТБ стоит 11800р, а диск объёмом 6ТБ — 14400р. Таким образом, стоимость хранения одного ТБ информации составляет 2950р и 2400р соответственно. Если требуемый объём хранилища — 24ТБ, то по данному показателю выгоднее использовать не 6 дешёвых дисков объёмом 4ТБ (70800р), а 4 более дорогих диска по 6ТБ (57600р).
- Стоимость ленточного картриджа LTO-8 объёмом 12ТБ (30ТБ со сжатием) на момент написания данного текста составляет около 9700р, таким образом, стоимость хранения 1ТБ будет составлять 808р (323р со сжатием).
- На данный момент при больших объёмах резервного копирования магнитная лента является (с очень большим разрывом) наиболее дешёвым носителем информации. (Вариант I: 20

Криптография

- Задачи на расшифрование слов, зашифрованных путём сдвига алфавита на некоторое смещение.

- Величина сдвига выбрана достаточно небольшой
- Важно заметить, что зашифровано было **слово**, а значит, в нём не может быть сочетаний букв, которые не встречаются в словах.
- Гарантированно неправильную величину сдвига алфавита можно определить по нескольким буквам, нет необходимости перебирать все варианты.
- Например, зашифрованное сообщение - «ИМОАГР». Попробуем сдвинуть первые две буквы по алфавиту на 1, 2 и 3 позиции в обе стороны:
  ЁЙ ← ЖК ← ЗЛ ← **ИМ** → ЙН → КО → ЛР (жирным шрифтом показан оригинал)
  Из полученных шести вариантов только два могли бы встретиться в начале слова. Добавим ещё одну букву:
  ЗЛН…, КОР… — видно, что первый вариант точно неправильный. Продолжая работать со вторым вариантом, получаем ответ на задание — слово «КОРВЕТ». Зашифровано было путём сдвига алфавита на две позиции назад. Таким образом,
- ЧУЗЁГХ → ФРЕГАТ (3 позиции вперёд), ЗИЁМВН → КЛИПЕР (3 позиции назад), (Вариант I и II, вопрос 16)

Криптография

- Задачи на расшифрование слов, зашифрованных путём замены алфавита

- Алфавит получен перемешиванием букв в случайном порядке. Этот новый алфавит и является ключом шифрования.
- Для расшифрования сообщения достаточно выполнить обратную замену.

Например, зашифрованное сообщение - «БШЮДБАЪЧЫ ЩЬЫР», таблица замен:

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

Заменяя каждую букву по таблице (находим букву во второй строке, заменяем на букву из первой строки той же колонки), т. е. Б→Т, Ш→Е, Ю→К и т. д., получаем ответ на задание - «ТЕКСТОВЫЙ ФАЙЛ».

Вариант I, 17 — «ОШИБКА ВВОДА»
Вариант II, 17 — «АППАРАТНЫЙ СБОЙ»

ЗОЛОТОЕ СЕЧЕНИЕ
ФОНД ПОДДЕРЖКИ ТАЛАНТЛИВЫХ ДЕТЕЙ И МОЛОДЕЖИ


Благодарю за внимание!