ЗОЛОТОЕ СЕЧЕНИЕ
ФОНД ПОДДЕРЖКИ ТАЛАНТЛИВЫХ ДЕТЕЙ И МОЛОДЕЖИ

ВСОШ

Разбор заданий школьного этапа всероссийской олимпиады школьников по технологии (информационная безопасность) 7-8 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 вопросы 6-7 следующие:
Вариант I: 6 — Д (внедрение кода), 7 — Б (социальная инженерия)
Вариант II: 6 — Б (нарушение стабильности), 7 — Д (распространение по сети)

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 8-9 и 13-15:
Вариант I: 8 — В, 9 — А, 13 — А,В, 14 — Г, 15 — А
Вариант II: 8 — Б, 9 — В, 13 — Б,В, 14 — Д, 15 — Г

Правовые основы информационной безопасности

- Законодательство РФ предусматривает более 80 видов тайн.
- Существует информация, которая не может составлять никакую тайну, и обязана находиться в свободном доступе.
- С каждым видом тайны связан по крайней мере один федеральный закон (обычно больше).

Правовые основы информационной безопасности

- Пример 1:
  - В Федеральном законе «О банках и банковской деятельности» перечислено, какие сведения кредитная организация обязана держать в тайне. Что из перечисленного не может составлять банковскую тайну?
    - Информация о составе личного имущества клиента — эта информация не входит в перечень видов информации, относящихся к банковской тайне. Тем не менее, доступ к этой информации регулируется другими законами. (Вариант I, 16 - А)

- Пример 2:
  - Персональные данные — это сведения, позволяющие однозначно определить личность субъекта или отнести его к определённой группе. Какие из перечисленных сведений не относятся к персональным данным?
    - Госномер транспортного средства — это идентификатор транспортного средства, а не его владельца. (Вариант II, 16 - Д)

Правовые основы информационной безопасности

- Информацию о государственных ведомствах и их деятельности можно узнать на сайтах этих ведомств (см. раздел «документы» или аналогичный):
  - Федеральная служба по техническому и экспортному контролю
    - https://fstec.ru/
  - Министерство обороны
    - https://mil.ru/
  - Министерство промышленности и торговли
    - https://minpromtorg.gov.ru/
  - Министерство цифрового развития
    - https://digital.gov.ru/ru/
  - Федеральная служба безопасности
    - http://www.fsb.ru/

Правовые основы информационной безопасности

- Банк данных угроз безопасности — https://bdu.fstec.ru/, располагается на сайте ФСТЭК.
- Реестр радиоэлектронной продукции находится в Государственной информационной системе промышленности — https://gisp.gov.ru/, являющейся частью ресурсов Минпромторга.
- Реестр отечественного ПО находится на сайте Минцифры — https://reestr.digital.gov.ru/.
- Вариант I: 10 — В, 11 — А, 12 — Г.
- Вариант II: 10 — В, 11 — Б, 12 — Г.

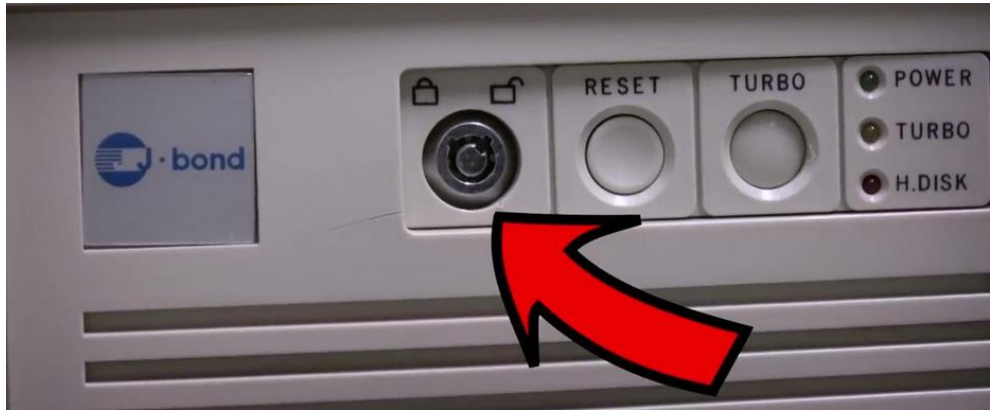
Технические средства обеспечения информационной безопасности

- Kensington Lock – используется для предотвращения кражи устройства

Вариант I, 17 – Б

Технические средства обеспечения информационной безопасности

- Key Lock – используется для блокировки ввода с клавиатуры (отсюда название). Изначально использовался для предотвращения доступа к компьютеру, но стал в этой роли бесполезным, как только в организациях стало использоваться более одного ПК (ключи везде одинаковые). Аналогичный замок иногда также использовался для предотвращения запуска компьютера или доступа внутрь корпуса, но в настоящее время утратил и эту роль. Иногда до сих пор встречается в промышленных ПК, в основном – для предотвращения случайных нажатий на клавиши встроенной клавиатуры.
- Выглядит так:



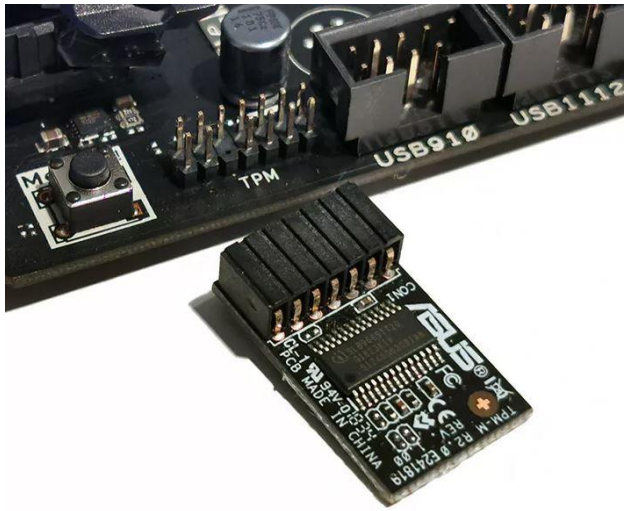
Вариант II, 17 - B

Программные средства защиты информации

- На серверах в Интернете наиболее распространены UNIX-подобные операционные системы, в частности — GNU/Linux. (Вариант I, 18 - Б)
- ОС Аврора является одной из немногих мобильных ОС, полностью соответствующих требованиям законодательства РФ к обеспечению конфиденциальности данных. (Вариант I, 19 — Г)
- Oracle VirtualBox является решением для «настольной» виртуализации. Несмотря на возможность использования данной платформы на серверах, такой режим работы не имеет полноценной технической поддержки, стабильность работы платформы в целом не гарантируется, а интеграция с распространёнными средствами администрирования зачастую отсутствует (несмотря на наличие соответствующего API). (Вариант II, 18 — В)
- 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, 19- 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 I, 24)

Технические средства обеспечения информационной безопасности

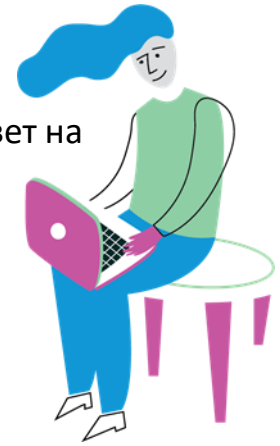
- TPM-модуль – специализированное устройство, реализующее функции доверенного хранилища ключей, криптопроцессора и датчика случайных чисел.
- Если какое-либо криптографическое ПО использует этот модуль, то его извлечение приводит к невозможности работы этого ПО, в том числе, к невозможности загрузки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



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,
- ИМОАГР → КОРВЕТ (2 позиции назад), НКПМРТ → ЛИНКОР (2 позиции вперёд), (Вариант I и II, вопрос 20)



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, 21 — «БАЗА ДАННЫХ»
Вариант II, 21 — «ТЕКСТОВЫЙ ФАЙЛ»

ЗОЛОТОЕ СЕЧЕНИЕ
ФОНД ПОДДЕРЖКИ ТАЛАНТЛИВЫХ ДЕТЕЙ И МОЛОДЕЖИ


Благодарю за внимание!