ЗОЛОТОЕ СЕЧЕНИЕ
ФОНД ПОДДЕРЖКИ ТАЛАНТЛИВЫХ ДЕТЕЙ И МОЛОДЕЖИ

ВСОШ

Разбор заданий муниципального этапа всероссийской олимпиады школьников по труду (технологии) (информационная безопасность) для 9 класса

2024/2025 учебного года в Свердловской области

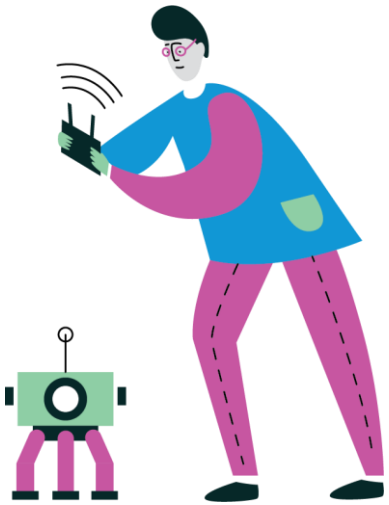
Разработчик:
Алексеевский Петр Иванович
ст. преп. каф. ИИТиМОИ, УрГПУ

Вопрос 5

Как называется способ передачи или хранения информации, предполагающий сохранение в тайне факта существования секретного сообщения в передаваемой или хранимой информации?

а) клептография; — предполагает исследование возможности организации скрытых каналов связи.
б) стеганография; — предполагает сокрытие факта существования сообщения.
в) криптография; — предполагает сокрытия содержания сообщения, но не факта его существования.
г) стенография; — способ быстрой записи сообщений

Правильный ответ — Б.



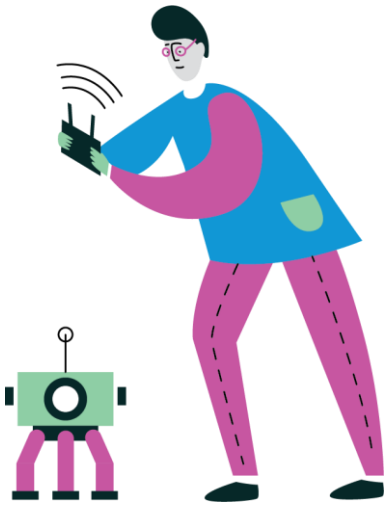
Вопрос 6

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?

а) Сведения об операциях по лицевому счёту клиента
б) Информация о составе личного имущества клиента
в) Паспортные данные клиента — физического лица
г) Сведения о наличии или отсутствии у клиента банковских счетов

Правильный ответ — Б.

- Информация о составе личного имущества клиента — не сообщается банку, поэтому не может быть объектом банковской тайны.
- Все остальные сведения, перечисленные в вопросе, согласно ст. 26 закона «О банках и банковской деятельности», составляют банковскую тайну, и для доступа к ним требуются специальные процедуры.



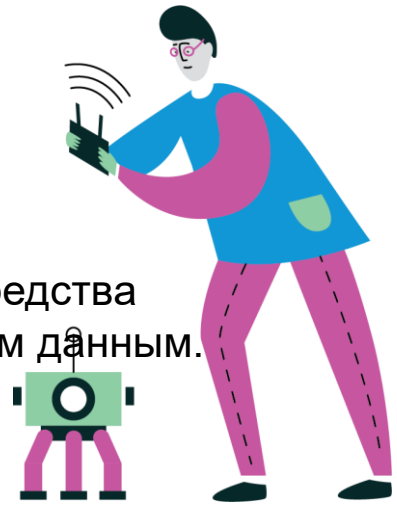
Вопрос 7

Персональные данные — это сведения, позволяющие однозначно определить личность субъекта или отнести его к определённой группе. Какие из перечисленных сведений не относятся к персональным данным?

а) Размер заработной платы
б) Национальная принадлежность
в) Расовая принадлежность
г) Госномер транспортного средства
д) Состояние здоровья
е) Всё перечисленное относится к персональным данным

Правильный ответ — Г.

- Госномер транспортного средства — является средством идентификации транспортного средства (например, автомобиля), а не его владельца, и таким образом не относится к персональным данным.

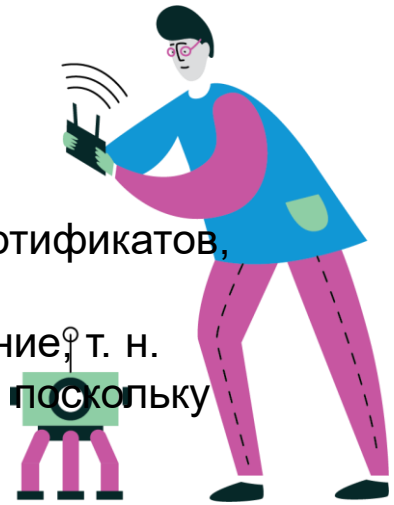


Вопрос 8

В некоторых организациях обязательным требованием является установка в компьютеры модулей TPM, причём, независимо от используемой операционной системы. Что является основным мотивом использования TPM в организации?

а) Обеспечение возможности установки Windows 11 на эти компьютеры
б) Обеспечение возможности безопасного хранения криптографических реквизитов
в) Повышение производительности компьютера
г) Прохождение сертификации платформы в государственных ведомствах
д) Безопасная работа в сети Интернет

Правильный ответ — Б.



- Модули TPM предназначены для безопасного хранения криптографических реквизитов (сертификатов, ключей и т. п.), это основная причина их использования.
- Заметим, что некоторые современные компьютеры могут использовать программное решение, т. н. fTPM — в этом случае всё равно может потребоваться установка аппаратного модуля TPM, поскольку программный fTPM принципиально не может быть сертифицирован.

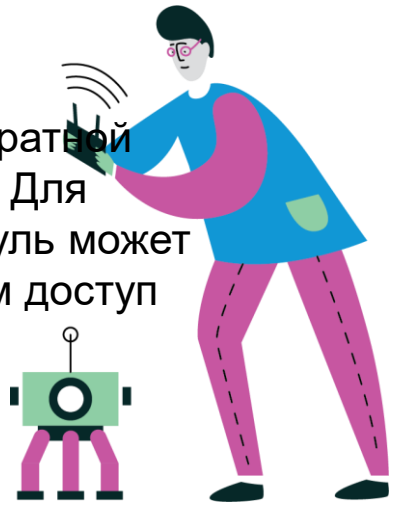
Вопрос 9

В некоторых организациях обязательным требованием является установка в компьютеры модулей МДЗ. Для чего из перечисленного такие модули не предназначены?

а) Повышение производительности криптографических алгоритмов в прикладном ПО.
б) Предотвращение запуска ОС со съёмного носителя.
в) Предотвращение запуска ОС без установленного модуля.
г) Контроль целостности технических и программных средств компьютера.

Правильный ответ — А.

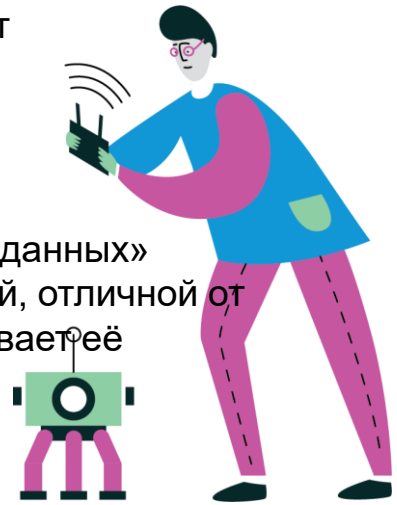
- В задачи МДЗ входит обеспечение доверенной среды, т. е. не допускается изменение аппаратной конфигурации компьютера, замена операционной системы или отключение самого модуля. Для прикладного ПО модуль доверенной загрузки, как правило, невидим. И даже если сам модуль может выполнять какие-либо криптографические алгоритмы, прикладное ПО к этим возможностям доступ получить не может.



Вопрос 10

Сотрудник компании загрузил из сети программу, при запуске которой ОС Windows вывела сообщение о запрете на запуск программ из недоверенных источников. Тем не менее, программа пользователю известна, и для выполнения работы необходимо её выполнить. Каким из перечисленных способом сотрудник может удалить информацию о недоверенном источнике в обход всех политик безопасности?

а) Открыть файл с помощью текстового редактора и пересохранить
б) Сбросить атрибуты файла
в) Переименовать файл
г) Скопировать файл на носитель, отформатированный в файловой системе FAT
д) Установить стороннюю программу, предназначенную для удаления альтернативных потоков, и удалить этот дополнительный поток.



Правильный ответ — Г.

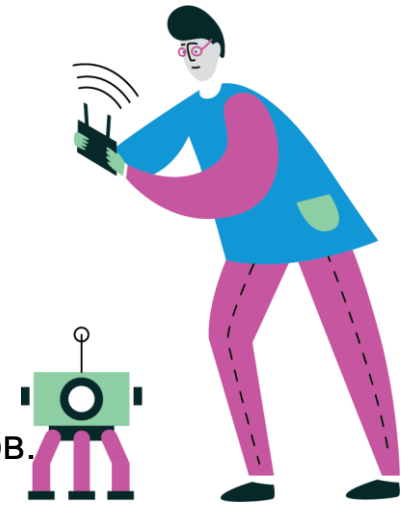
- Информация о том, откуда был загружен файл, сохраняется в так называемом «альтернативном потоке данных» файла. Это особенность файловой системы NTFS. При копировании файла на том с файловой системой, отличной от NTFS (например, FAT32), эта информация теряется, поскольку целевая файловая система не поддерживает её хранение.
- Какие-либо стандартные манипуляции с файлом не влияют на содержимое альтернативных потоков.
- Установка сторонних программ пользователями, как правило, запрещена политикой безопасности.

Вопрос 11

Сотрудник компании решил почистить компьютер на своём рабочем месте от пыли. Во время чистки он обнаружил внутри компьютера незнакомую плату расширения с непонятным предназначением. На всякий случай, он отключил этот модуль. Однако, после чистки и сборки, компьютер отказался загружать операционную систему. Более того, при попытке загрузиться с загрузочного носителя обнаружилось, что все жёсткие диски полностью заполнены данными, выглядящими как случайные числа. Что за модуль по незнанию отключил сотрудник?

а) Модуль TPM
б) Сетевой адаптер
в) Модуль доверенной загрузки
г) Контроллер жёсткого диска
д) Модуль оперативной памяти

Правильный ответ — В.



- Описанное в вопросе поведение — результат отключения модуля доверенной загрузки.
- Некоторые МДЗ имеют возможность прозрачного шифрования содержимого жёстких дисков.

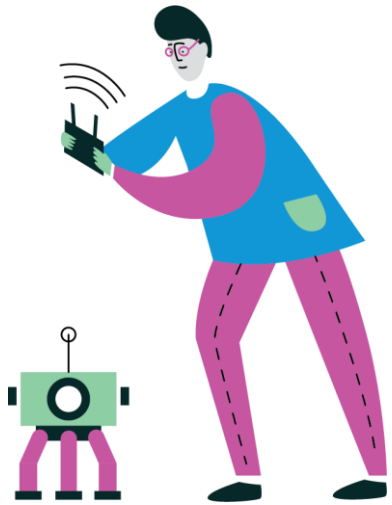
Вопрос 12

Какое из перечисленных утверждений о протоколе TLS является неверным?

а) Протокол может использоваться для шифрования передаваемых данных
б) Протокол может использоваться для взаимной аутентификации клиента и сервера
в) Использование протокола включено в протокол HTTPS
г) Протокол устарел, и в настоящее время вытеснен более совершенными протоколами.

Правильный ответ — Г.

- Протокол TLS актуален и активно применяется на практике, в отличие от устаревшего и не рекомендованного к использованию протокола SSL.

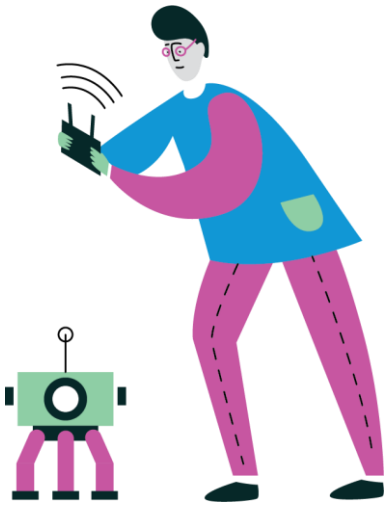


Вопрос 13

Как расшифровывается название класса программного обеспечения «EDR»?

а) Extended Data Rate
б) Endpoint Detection and Response
в) Enhanced Data Recovery
г) Error Detection and Recovery
д) Electronic Digital Recorder

Правильный ответ — Б.

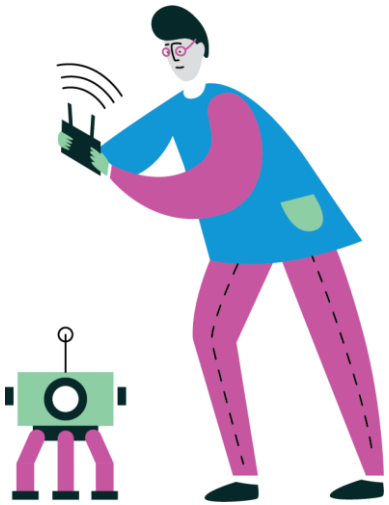


Вопрос 14

Какой трёхбуквенной аббревиатурой обозначается сегмент сети, в котором располагаются службы, доступные извне локальной сети, и не имеющий прямого доступа к внутренним ресурсам локальной сети?

Правильный ответ — DMZ.

- Такой сегмент сети называется «демилитаризованная зона» (demilitarized zone). Сокращённо — DMZ.



ЗОЛОТОЕ СЕЧЕНИЕ
ФОНД ПОДДЕРЖКИ ТАЛАНТЛИВЫХ ДЕТЕЙ И МОЛОДЕЖИ

ВСОШ
ТЕХНОЛОГИЯ ВСЕРОССИЙСКАЯ ОЛИМПИАДА ШКОЛЬНИКОВ

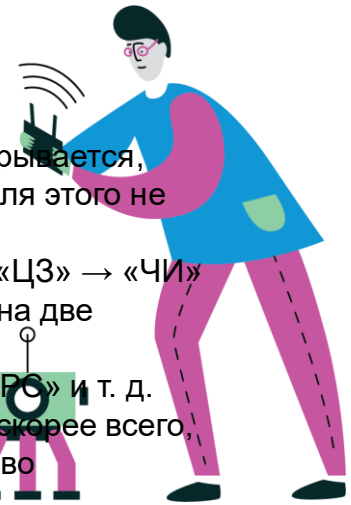
Вопросы 15, 16

15. В ящике стола обнаружилась записка с буквами «ХЖПЙМ». По-видимому, шифровка. Известно, что шифрование осуществлялось путём сдвига алфавита на некоторое количество позиций. Какое слово было зашифровано?

Правильный ответ — «ЧИСЛО».

16. В другом ящике стола нашлась ещё одна записка, в этот раз со словом «УФТРМВ». Известно, что шифрование осуществлялось путём сдвига алфавита на некоторое количество позиций. Какое слово было зашифровано?

Правильный ответ — «СТРОКА».



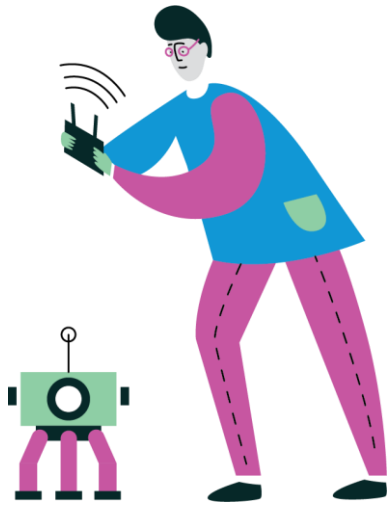
- Подобный шифр, где известна закономерность, по которой осуществляется замена блоков (в данном случае букв), легко вскрывается, если анализировать «правдоподобность» последовательностей блоков (букв) после каждой попытки подбора ключа. Часто для этого не требуется даже обрабатывать все блоки.
- Если попробовать сдвигать первые две буквы по алфавиту вперёд, то получаем следующие последовательности - «ХЖ» → «ЦЗ» → «ЧИ» и т. д. Существуют слова, начинающиеся с букв «ЧИ», а вот со словами на «ЦЗ», например, проблема. Попробуем сдвинуть на две позиции в алфавите остальные буквы, получаем слово «ЧИСЛО».
- Аналогично, попробуем сдвинуть буквы «УФ», в этот раз — назад. Получим последовательности - «УФ» → «ТУ» → «СТ» → «РС» и т. д. Слова на «ТУ» существуют, но если сдвинуть остальные буквы на одну позицию в алфавите, получаем «ТУСПЛБ», т. е. это, скорее всего, не то слово, и это становится понятно уже на четвёртой букве. Но если все буквы сдвинуть на две позиции, то получится слово «СТРОКА».

Вопросы 17, 18

Для шифрования сообщения был использован ключ, приведённый в таблице. Что здесь зашифровано?

17. «РАБНЙЦДАЁЯБЩ» Правильный ответ — «КРИПТОГРАФИЯ».
18. «ЖЮЩАУРБАЫУЛГЭ» Правильный ответ — «СТЕГАНОГРАФИЯ».

- В заданиях приведены таблицы замены символов. Первая строка — знак открытого текста, вторая строка — знак шифротекста.



Вопрос 19

Один из наиболее распространённых вариантов Base64-кодирования, RFC 4648 p4, использует алфавит, содержащий, по порядку, заглавные латинские буквы A-Z, строчные латинские буквы a-z, цифры 0-9 и символы «+» и «/». В качестве символа заполнения используется знак «=». Кодовая таблица ASCII содержит заглавные буквы латиницы в алфавитном порядке, начиная с кода 65. Какое слово, записанное заглавными латинскими буквами, закодировано в строке «U0hJRlQK»?

Правильный ответ — «SHIFT».

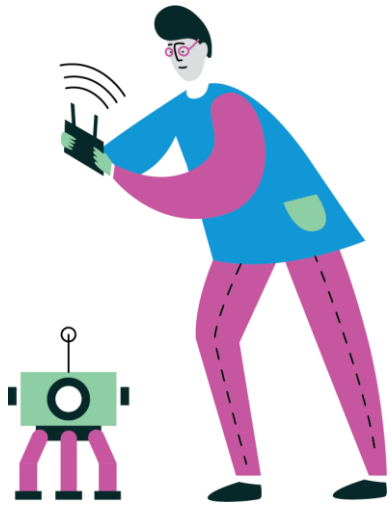
- Заменим каждый символ строки на его номер в описанном алфавите: 20, 52, 33, 9, 17, 37, 16, 10.
- Переведём эти номера в двоичную систему счисления и запишем как шестиразрядные числа:
  010100 110100 100001 001001 010001 100101 010000 001010
- Перегруппируем разряды так, чтобы получились восьмиразрядные числа:
  01010011 01001000 01001001 01000110 01010100 00001010
- Переведём эти числа в десятичную систему счисления:
  83, 72, 73, 68, 84, 10
- Заменим их на соответствующие символы таблицы ASCII:
  S, H, I, F, T, перевод строки
- Получится слово «SHIFT»

Вопрос 20

Один из наиболее распространённых вариантов Base64-кодирования, RFC 4648 p4, использует алфавит, содержащий, по порядку, заглавные латинские буквы A-Z, строчные латинские буквы a-z, цифры 0-9 и символы «+» и «/». В качестве символа заполнения используется знак «=». Кодовая таблица ASCII содержит заглавные буквы латиницы в алфавитном порядке, начиная с кода 65. Закодируйте методом Base64 слово «ROTATE».

Правильный ответ — «Uk9UQVRF».

- Заменим буквы на их коды по таблице ASCII:
  82, 79, 84, 65, 84, 69
- Переведём их в двоичную систему счисления и запишем как восьмиразрядные числа:
  01010010 01001111 01010100 01000001 01010100 01000101
- Перегруппируем разряды, чтобы получились шестиразрядные числа:
  010100 100100 111101 010100 010000 010101 010001 000101
- Переведём числа в десятичную систему счисления:
  20, 36, 61, 20, 16, 21, 17, 5
- Выполним замену по алфавиту для Base64-кодирования.
- Результатом будет строка «Uk9UQVRF»



Вопрос 21 (кейс-задание)

Имеет ли место нарушение безопасности информационной среды компании?

- Да, имеет

Есть ли для таких обнаруженных предметов специальное название?

- Такие предметы называются «Дорожное яблоко»

Если имело место нарушение безопасности, то что именно могло произойти после подключения накопителя?

- Наиболее вероятный вариант — заражение сети предприятия сетевым червём, поскольку вышли из строя несколько компьютеров в сети при отсутствии воздействия извне.

Какие угрозы это может создать для компании?

- Заражение сетевым червём несёт риск нарушения всех компонентов информационной безопасности. Это может привести к утечке персональных данных, повреждению хранимых данных, отказу в обслуживании и другим проблемам, вплоть до полной остановки деятельности предприятия.

Как предотвратить дальнейшие негативные последствия?

- Провести аудит системы безопасности, устранить непосредственные причины сбоев, устранить вредоносное ПО.

Как избежать повторения данной ситуации?

- Поскольку в данном случае имел место человеческий фактор, первоочередной задачей будет проведение инструктажа сотрудников. Также, после устранения последствий заражения, возможно, следует усилить политики сетевой безопасности.