



**ЗОЛОТОЕ
СЕЧЕНИЕ**

ФОНД ПОДДЕРЖКИ
ТАЛАНТЛИВЫХ ДЕТЕЙ
И МОЛОДЕЖИ

Разбор заданий муниципального этапа всероссийской олимпиады школьников по труду (технологии) (информационная безопасность) для 10-11 классов

2024/2025 учебного года в Свердловской области

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

ВС{ }Ш

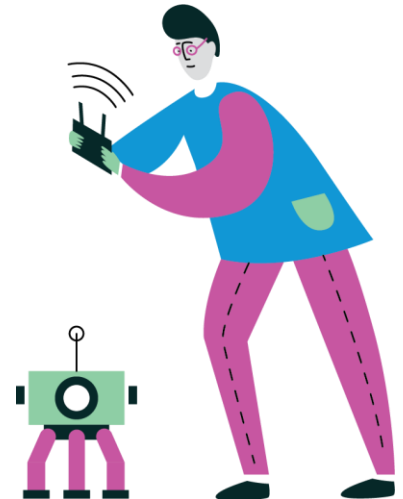


Вопрос 5

Как называется набор данных, используемый для внедрения в него секретного сообщения при стеганографии?

- а) цифровой водяной знак
- б) носитель информации
- в) шифротекст
- г) стегоконтейнер**
- д) криптоконтейнер

Правильный ответ — Г.



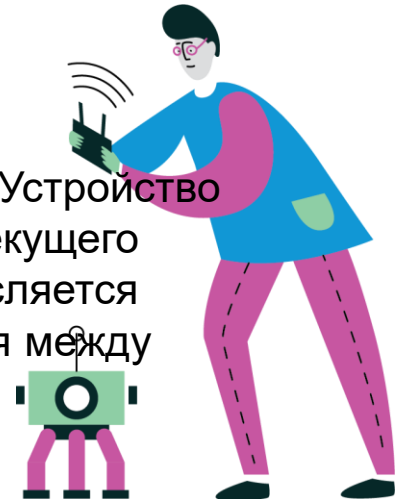
Вопрос 6

В некоторых организациях при работе с банком используется устройство, обычно имеющее вид брелока с дисплеем и единственной кнопкой. Никаких других органов управления у устройства нет. При нажатии на кнопку на дисплее отображается некоторое число. Что это за устройство?

- а) Доверенный USB Flash-накопитель для хранения ключей шифрования.
- б) Пульт дистанционного управления сигнализацией.
- в) Генератор одноразовых паролей.**
- г) Справочник PIN-кодов банковских карт.

Правильный ответ — В.

- Это устройство — генератор одноразовых паролей. Порядок его работы достаточно прост. Устройство имеет встроенные часы, синхронизированные с таковыми на серверах банка. На основе текущего времени и индивидуального номера устройства с помощью специального алгоритма вычисляется некоторое число. Точно такое же число вычисляется сервером банка. Никакая информация между устройством и серверами не передаётся, что исключает перехват пароля.



Вопрос 7

В некоторых организациях используется устройство под названием RuToken, обычно имеющее вид USB Flash-накопителя. Что это за устройство?

- а) Доверенный USB Flash-накопитель для хранения файлов.
- б) Хранилище реквизитов, используемых для аутентификации владельца.**
- в) Ключ для предотвращения использования нелегальных копий ПО.
- г) Устройство для безопасного подключения беспроводных устройств ввода.

Правильный ответ — Б.

- Это устройство является вариантом смарт-карты в форм-факторе USB-брелока. Оно предназначено для хранения криптографических реквизитов и алгоритмов, и обычно используется для аутентификации владельца.



Вопрос 8

Во многих организациях используется та или иная система электронного документооборота. Документы, циркулирующие в такой системе, часто содержат реквизит под названием «Электронная подпись». Для чего из перечисленного электронная подпись не предназначена?

- а) Подтверждение достоверности сведений, содержащихся в подписанном документе.
- б) Определение неизменности подписанного документа с момента создания подписи.
- в) Доказательство принадлежности подписи конкретному субъекту.
- г) Контроль целостности документа и его подписи в случае, если он был передан по какому-либо каналу связи.

Правильный ответ — А.

- Электронная подпись позволяет обнаружить факт изменения (преднамеренного или случайного) документа с момента создания подписи.
- Также электронная подпись позволяет идентифицировать создателя этой подписи.
- Достоверность сведений, содержащихся в документе, электронная подпись гарантировать не может.



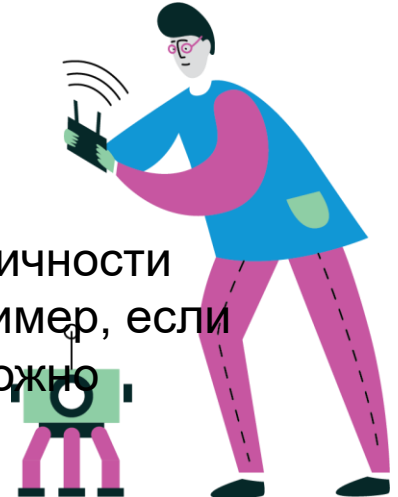
Вопрос 9

В настоящее время клиенты ряда организаций используют так называемую «упрощённую электронную подпись». Для чего из перечисленного она предназначена?

- а) Подтверждение достоверности сведений, содержащихся в подписанном документе.
- б) Определение неизменности подписанного документа с момента создания подписи.
- в) Удостоверение личности клиента с помощью реквизитов подписанного документа.**
- г) Контроль целостности документа и его подписи в случае, если он был передан по какому-либо каналу связи.

Правильный ответ — В.

- Упрощённая электронная подпись предназначена для быстрого удостоверения личности клиента на основе данных, которые содержатся в подписанном документе. Например, если документ содержит номер личного мобильного телефона клиента, то личность можно установить, проверив фактор владения этим номером.



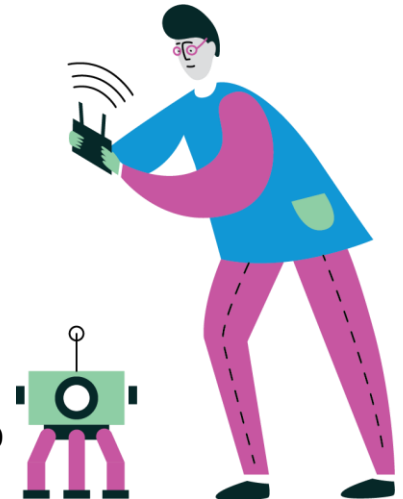
Вопрос 10

Сотрудник компании решил прибраться в серверной и обнаружил, что к одному из серверов подключено устройство, похожее на USB Flash-накопитель. Полагая, что это Flash-накопитель, забытый системным администратором, сотрудник отключил это устройство. В результате в компании перестало работать бухгалтерское ПО. Что за устройство по незнанию отключил сотрудник?

- а) Модуль TPM
- б) Модуль доверенной загрузки
- в) Сетевой адаптер
- г) Аппаратный ключ проверки лицензии**
- д) Модуль оперативной памяти

Правильный ответ — Г.

- Скорее всего, это был ключ защиты бухгалтерского ПО от несанкционированного копирования.



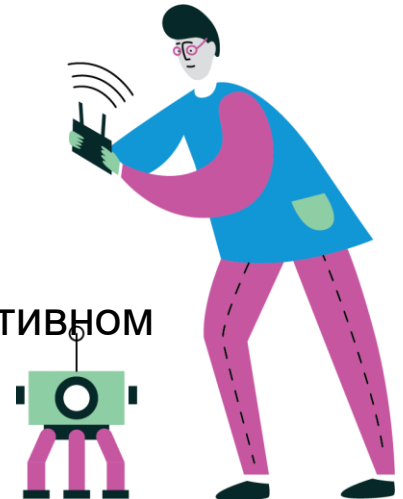
Вопрос 11

При использовании операционной системы Windows можно столкнуться с ситуацией, когда при открытии исполняемого файла система предупреждает о том, что файл был загружен из недоверенного источника. Где хранится информация об этом?

- а) В заголовке самого файла в соответствующем поле
- б) В альтернативном потоке данных файла в файловой системе NTFS**
- в) В атрибутах файла
- г) В системном реестре Windows
- д) В отдельном файле

Правильный ответ — Б.

- Информация об источнике, из которого был загружен файл, хранится в альтернативном потоке данных в файловой системе NTFS.



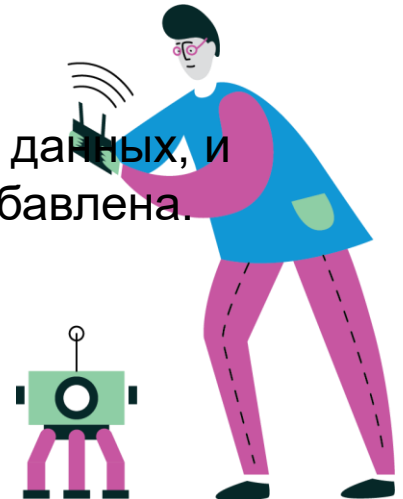
Вопрос 12

Какое из перечисленных утверждений о протоколе SSL является неверным?

- а) Протокол может использоваться для взаимной аутентификации клиента и сервера
- б) Протокол может использоваться для шифрования передаваемых данных**
- в) Протокол может использоваться совместно с другими протоколами, такими как HTTP
- г) Протокол устарел, и в настоящее время вытеснен более совершенными протоколами.

Правильный ответ — Б.

- Протокол SSL изначально не был предназначен для шифрования передаваемых данных, и это одна из причин создания протокола TLS, в котором эта возможность была добавлена.



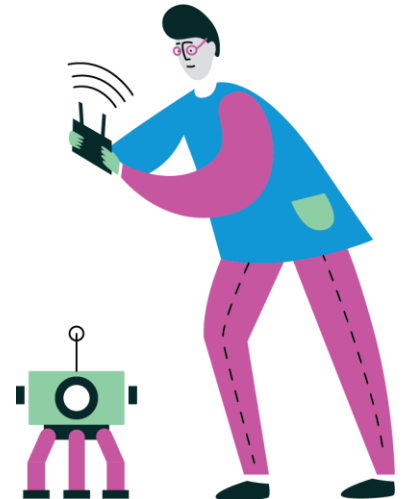
Вопрос 13

К какому классу ПО относятся HIDS и NIDS решения?

- а) Антивирусы
- б) Сетевые сканеры
- в) Межсетевые экраны
- г) Системы обнаружения вторжений**
- д) Системы предотвращения вторжений

Правильный ответ — Г.

- HIDS и NIDS относятся к IDS — Intrusion Detection System, системы обнаружения вторжений.



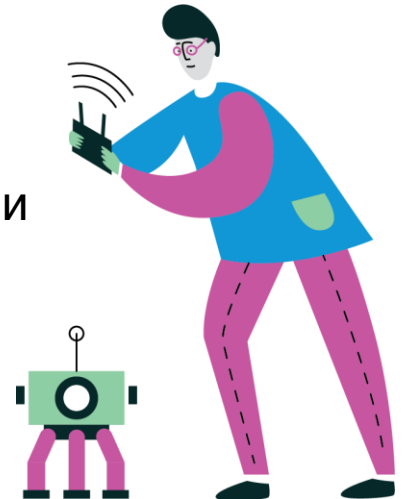
Вопрос 14

Какая из перечисленных уязвимостей не входит явно в текущий список OWASP Top 10?

- а) Небезопасный дизайн
- б) Неправильная конфигурация безопасности
- в) Межсайтовый скриптинг**
- г) Уязвимые и устаревшие компоненты
- д) Нарушение целостности ПО и данных

Правильный ответ — В.

- Уязвимость «Межсайтовый скриптинг» была объединена с другими родственными уязвимостями, как отдельная более не выделяется.



Вопросы 15, 16

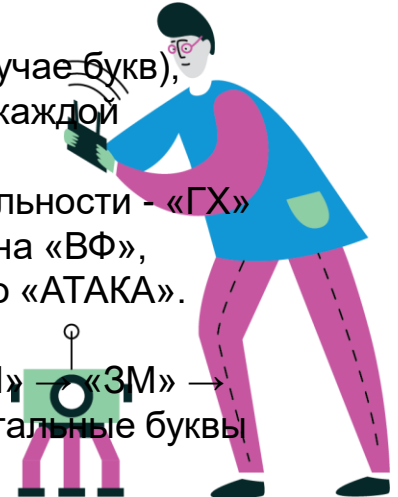
В ящике стола обнаружилась записка с буквами «ГХГНГ». По-видимому, шифровка. Известно, что шифрование осуществлялось путём сдвига алфавита на некоторое количество позиций. Какое слово было зашифровано?

Правильный ответ — «АТАКА».

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

Правильный ответ — «ИНЦИДЕНТ».

- 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 назад, то получаем следующие последовательности - «ГХ» → «ВФ» → «БУ» → «АТ» и т. д. Существуют слова, начинающиеся с букв «БУ» и «АТ», а вот со словами на «ВФ», например, проблема. Попробуем сдвинуть на три позиции в алфавите остальные буквы, получаем слово «АТАКА». Повтор в слове первой буквы помогает выбрать правильный вариант.
- Аналогично, попробуем сдвинуть буквы «ЖЛ», в этот раз — вперёд. Получим последовательности - «ЖЛ» → «ЗМ» → «ИН» → «ЙО» и т. д. Наиболее правдоподобным сочетанием букв является «ИН». Если сдвинуть все остальные буквы на 2 позиции, то получится слово «ИНЦИДЕНТ».



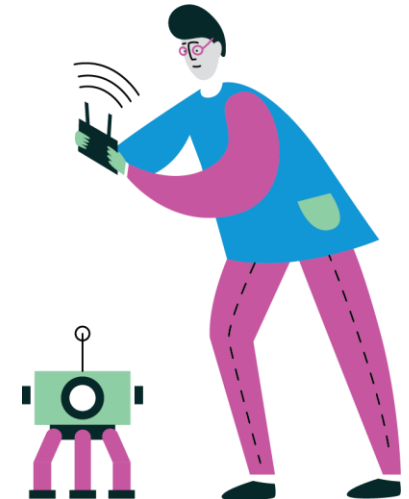
Вопросы 17,18

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

Задание 17. «ФАЁЬЛЧЁЗША» Правильный ответ — «**БРАНДМАУЭР**».

Задание 18. «УРЮГЦГЫИЖ» Правильный ответ — «**АНТИВИРУС**».

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

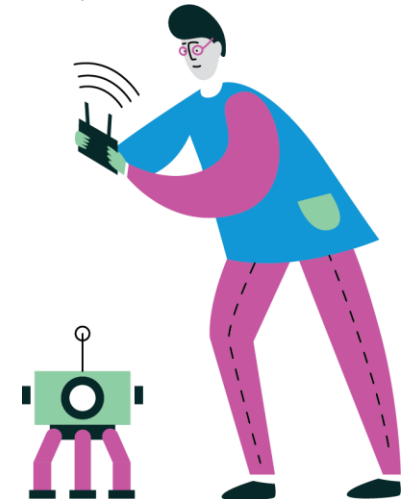


Вопрос 19

Один из наиболее распространённых вариантов Base64-кодирования, RFC 4648 р4, 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 «REVDTRFUgo=»?

Правильный ответ — «**DECODER**».

- Заменяем каждый символ строки на его номер в описанном алфавите: 17, 4, 21, 3, 19, 52, 17, 5, 20, 32, 40, =. (просто запомним, что в конце один знак «=»)
- Переведём эти номера в двоичную систему счисления и запишем как шестизначные числа:
010001 000100 010101 000011 010011 110100 010001 000101 010100 100000 101000 000000
- Перегруппируем разряды так, чтобы получились восьмизначные числа:
01000100 01000101 01000011 01001111 01000100 01000101 01010010 00001010 00000000
- Переведём эти числа в десятичную систему счисления, удалив одно последнее:
68, 69, 67, 79, 68, 69, 82, 10
- Заменяем их на соответствующие символы таблицы ASCII:
D, E, C, O, D, E, R, перевод строки
- Получится слово «DECODER»

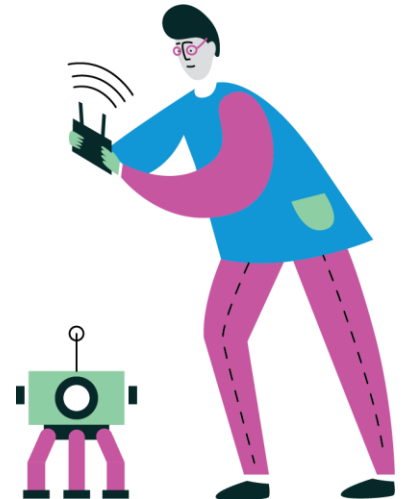


Вопрос 20

Один из наиболее распространённых вариантов Base64-кодирования, RFC 4648 р4, 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 «SECURITY».

Правильный ответ — «U0VDVVJJVFk=».

- Заменяем буквы на их коды по таблице ASCII:
83, 69, 67, 85, 82, 73, 84, 89
- Переведём их в двоичную систему счисления и запишем как восьмиразрядные числа:
01010011 01000101 01000011 01010101 01010010 01001001 01010100 01011001
- Перегруппируем разряды, чтобы получились шестиразрядные числа, дополняя нулями:
010100 110100 010101 000011 010101 010101 001001 001001 010101 000101 100100
- Переведём числа в десятичную систему счисления:
20, 52, 21, 3, 21, 21, 9, 9, 21, 5, 36
- Выполним замену по алфавиту для Base64-кодирования, добавив знак «=».
- Результатом будет строка «U0VDVVJJVFk=»



Задание 21 (кейс)

Имеет ли место нарушение безопасности информационной среды магазина?

- 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 компьютера трояном, возможно — вирусом. Поскольку вышел из строя только один компьютер, наличие сетевого червя маловероятно.

Какие угрозы это может создать для магазина?

- Заражение вирусом несёт риск нарушения всех компонентов информационной безопасности применительно к данному компьютеру. Это может привести к утечке персональных данных, повреждению хранимых данных, отказу в обслуживании и другим проблемам, вплоть до полной остановки рабочего места.

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. Следует установить или обновить антивирусное программное обеспечение. Также, после устранения последствий заражения, возможно, следует усилить политики сетевой безопасности.

