ЗОЛОТОЕ СЕЧЕНИЕ
ФОНД ПОДДЕРЖКИ ТАЛАНТЛИВЫХ ДЕТЕЙ И МОЛОДЕЖИ

ВСОШ

# Разбор заданий муниципального этапа всероссийской олимпиады школьников по труду (технологии) (информационная безопасность) для 7-8 классов

## 2024/2025 учебного года в Свердловской области

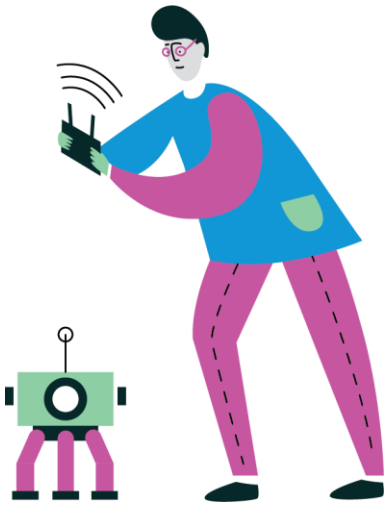
Разработчик:
Алексеевский Петр Иванович
ст. преп. каф. ИИТиМОИ, УрГПУ

Вопрос 5

**Как называется наука о методах дешифрования зашифрованной информации без знания соответствующего ключа?**

А) стеганография; — занимается сокрытием факта передачи сообщения.
Б) криптография; — занимается сокрытием содержания сообщения.
В) криптоанализ; — занимается методами дешифрования без знания ключа.
Г) криптомерия. — вечнозелёное дерево семейства Кипарисовые

Правильный ответ — В.

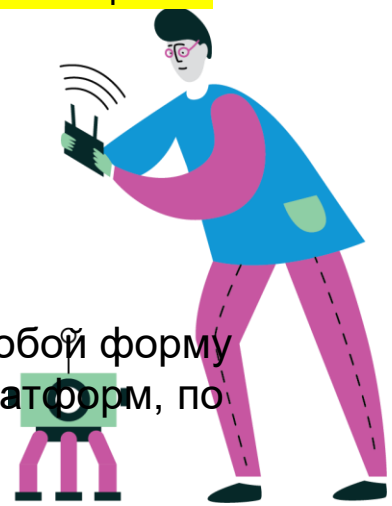


Вопрос 6

**Пользователь получил электронное письмо, содержащее ссылку на веб-страницу: https://ru.wikipedia.org/wiki/%D0%9A%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D0%B8%D1%8F.**
**Что это за странный набор букв и цифр в конце адреса?**

а) Пароль для доступа к секретной области сайта
б) Испорченный адрес ссылки
в) Коды русских букв, представленные в такой форме для нормальной работы в средах, где кириллица не поддерживаются
г) Вредоносный программный код
д) Перенаправление на мошеннический сайт

Правильный ответ — В.



- Последовательности вида %XX, где XX — пара шестнадцатеричных цифр, представляют собой форму записи кодов символов, отображение и/или ввод которых может быть затруднён на ряде платформ, по той или иной причине.
- В данном случае это коды русских букв, составляющих слово «Криптография».

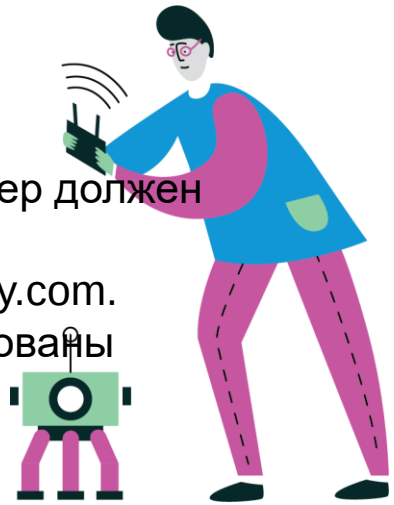
Вопрос 7

**Пользователь отправляет два электронных письма, одно — на адрес info+a@company.com, другое — на info+b@company.com. Какова дальнейшая судьба этих двух писем?**

а) Письма будут доставлены одному пользователю — «info»
б) Письма будут доставлены двум разным пользователям — «a» и «b»
в) Письма будут доставлены двум разным пользователям — «info+a» и «info+b»
г) Письма будут доставлены трём разным пользователям — «info», «a» и «b»
д) Письма не будут доставлены из-за запрещённых символов в адресе

Правильный ответ - А

- По имеющимся спецификациям протоколов передачи почтовых сообщений, почтовый сервер должен игнорировать часть имени почтового ящика, начинающуюся со знака «+».
- Таким образом, оба письма будут доставлены по одному и тому же адресу — info@company.com.
- Однако, суффиксы «+a» и «+b» останутся в поле адреса получателя, и могут быть использованы почтовым ПО, например, для автоматической сортировки писем.



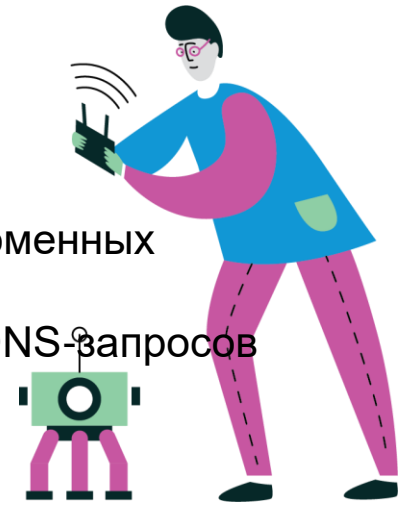
Вопрос 8

**Пользователь ввёл в адресную строку браузера адрес сайта. При переходе по введённому адресу он автоматически изменился, приняв вид https://xn--b1aew.xn--p1ai/**
**Какова наиболее вероятная причина такого поведения браузера?**

а) Компьютер заражён вирусом, который подменяет адреса
б) Пользователь ввёл адрес кириллицей
в) Доступ к сайту осуществляется через зашифрованное соединение
г) Отсутствует подключение к интернету
д) Доступ к сайту заблокирован

Правильный ответ - Б

- Такой вид доменного имени называется PunyCode. Он используется для представления доменных имён, написанных знаками, отличными от латиницы.
- Перекодирование доменных имён в такую форму необходимо для корректной обработки DNS-запросов серверами, которые могут работать только с запросами в кодировке ASCII.
- В данном случае с помощью PunyCode закодировано доменное имя «мвд.рф».



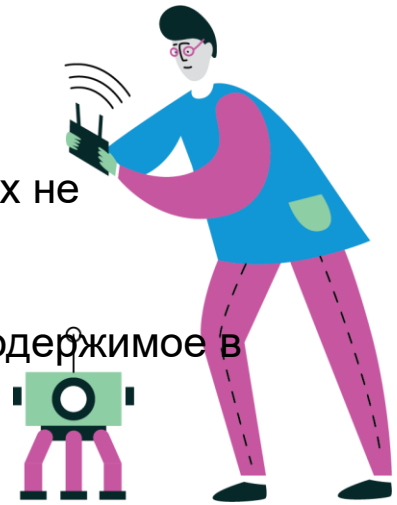
Вопрос 9

**При работе с некоторым сайтом после перехода по ссылке веб-браузер выдал сообщение об ошибке, при этом в строке адреса URL начинается со слова ftp. Что это такое?**

а) Ссылка на вредоносное программное обеспечение, приводящее к ошибкам в работе веб-браузера
б) Ошибка в ссылке, допущенная администратором сайта
в) Протокол передачи файлов, использование которого запрещено действующим законодательством
г) Протокол передачи файлов, поддержка которого в некоторых современных браузерах прекращена
д) Повреждение ссылки, вызванное попыткой доступа к запрещённому ресурсу

Правильный ответ — Г.

- Протокол передачи файлов (FTP, File Transfer Protocol) в некоторых современных браузерах не поддерживается.
- В качестве главной причины отключения поддержки протокола FTP обычно упоминают его небезопасность — протокол передаёт имена пользователей, пароли, имена файлов и их содержимое в открытой форме, без шифрования.
- Работа с FTP-сайтами по-прежнему возможна с помощью соответствующего специального программного обеспечения.

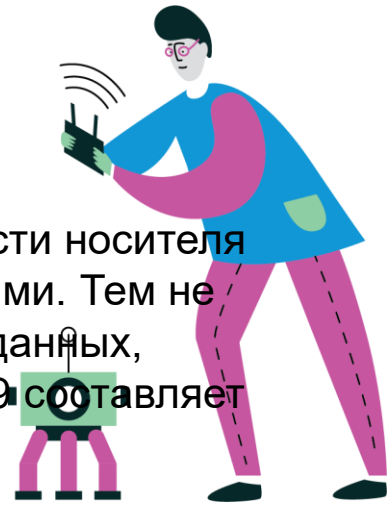


Вопрос 10

**Какой из перечисленных носителей информации, используемых для резервного копирования, имеет наименьшую стоимость хранения информации (отношение стоимости носителя к его объёму)?**

а) Записываемые компакт-диски
б) Твердотельные накопители
в) Жёсткие магнитные диски
г) Перфокарты
д) Магнитная лента
е) Гибкие магнитные диски

Правильный ответ — Д.



- Современные решения на основе магнитной ленты имеют наименьшее отношение стоимости носителя к объёму. К сожалению, нельзя сказать то же об устройствах для работы с такими носителями. Тем не менее, в отраслях, где требуется осуществлять резервное копирование больших объёмов данных, магнитная лента активно применяется. Например, вместимость картриджа стандарта LTO-9 составляет 18ТБ (45ТБ при использовании сжатия).

Вопрос 11

**Какой из перечисленных уровней RAID имеет наибольшую устойчивость к сбоям?**

а) RAID 0

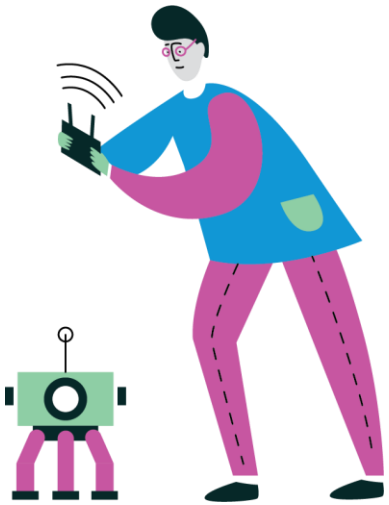
б) RAID 5

в) RAID 6

г) RAID 1+0

д) RAID 5+0

Правильный ответ — В.



- Из перечисленных в вопросе уровней наибольшую устойчивость к сбоям имеет RAID-6, допускающий одновременный выход из строя любых двух дисков в массиве.

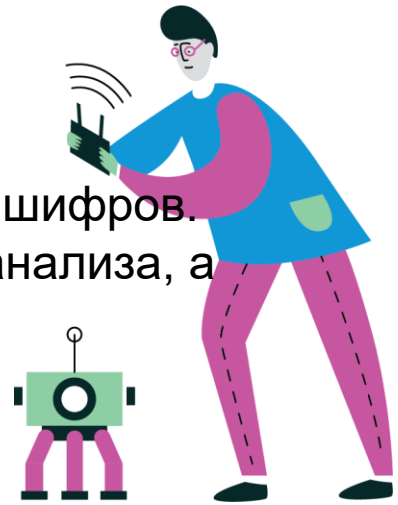
Вопрос 12

**Какой из перечисленных шифров имеет наименьшую устойчивость к атакам?**

а) Потоковый шифр с квантовым распределением ключей
б) Потоковый шифр с нерегулярным тактированием сдвиговых регистров, формирующих ключ
в) Блочный шифр с очень большим размером блока
г) Блочный шифр с малым размером блока
д) Блочный шифр с переменной длиной ключа

Правильный ответ — Г.

- Блочные шифры с малым размером блока — подмножество наиболее уязвимых шифров. Небольшой размер блока делает шифр уязвимым к атакам методом частотного анализа, а также ограничивает полезную длину ключа шифрования.



Вопрос 13

**Какой из перечисленных шифров имеет математически доказанную абсолютную устойчивость к атакам?**

а) Криптосистема Эль-Гамаля
б) Сеть Фейстеля
в) Подстановочно-перестановочная сеть
г) Шифр Вернама
д) Шифр Цезаря

Правильный ответ — Г.

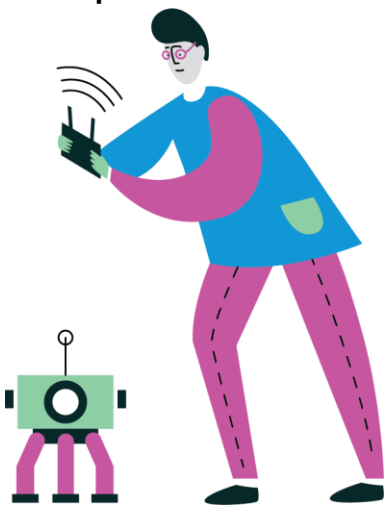
- Доказанную абсолютную устойчивость к атакам имеет шифр Вернама.
- Несмотря на это его достоинство, шифр Вернама является крайне непрактичным, что делает его бесполезным для решения каких-либо задач криптографии.

Вопрос 14

**Какова минимальная длина пароля пользователя Samba в режиме контроллера домена Active Directory по-умолчанию?**

Правильный ответ — 7.

- Согласно документации на актуальную версию Samba, минимальная длина пароля составляет 7 символов. Это значение может быть изменено при настройке контроллера домена.



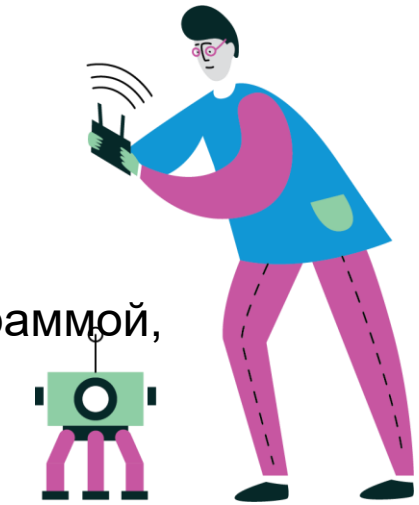
Вопрос 15

**Как называется программа, которая использует обнаруженную уязвимость в информационной системе с целью нарушения элементов информационной безопасности?**

а) атака
б) эксплойт
в) вирус
г) троянский конь
д) ботнет

Правильный ответ — Б.

- Использование (эксплуатация) обнаруженной уязвимости осуществляется программой, которую принято называть «эксплойт» (от англ. exploit).



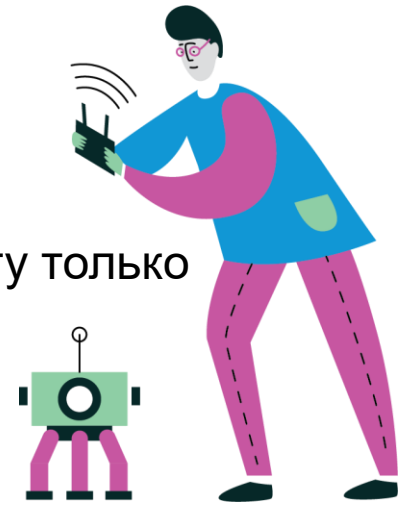
Вопрос 16

**Что из перечисленного отличает кибербезопасность от информационной безопасности?**

а) Кибербезопасность включает защиту только цифровых данных
б) Кибербезопасность не включает защиту персональных данных
в) Кибербезопасность включает использование технических средств защиты информации
г) Кибербезопасность не включает защиту от угроз, зависящих от человека

Правильный ответ — А.

- Информационная безопасность — очень широкое понятие, включающее защиту информации любого рода.
- Кибербезопасность — часть информационной безопасности, включающая защиту только цифровой информации.



ЗОЛОТОЕ СЕЧЕНИЕ
ФОНД ПОДДЕРЖКИ ТАЛАНТЛИВЫХ ДЕТЕЙ И МОЛОДЕЖИ

ВСОШ
ТЕХНОЛОГИЯ ВСЕРОССИЙСКАЯ ОЛИМПИАДА ШКОЛЬНИКОВ

# Вопросы 17, 18

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

Правильный ответ — КЛЮЧ.

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

Правильный ответ — ШИФР.

- 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 - «ЛМ» → «КЛ» → «ЙК» и т. д. Существуют слова, начинающиеся с букв «КЛ», а вот со словами на «ЙК», например, проблема. Попробуем сдвинуть на одну позицию в алфавите остальные буквы, получаем слово «КЛЮЧ».
- Аналогично, попробуем сдвинуть буквы «ЦЖ», в этот раз — вперёд. Получим последовательности - «ЦЖ» → «ЧЗ» → «ШИ» → «ЩЙ» и т. д. Слова на «ШИ» существуют, если сдвинуть остальные буквы на две позиции в алфавите, получаем слово «ШИФР».

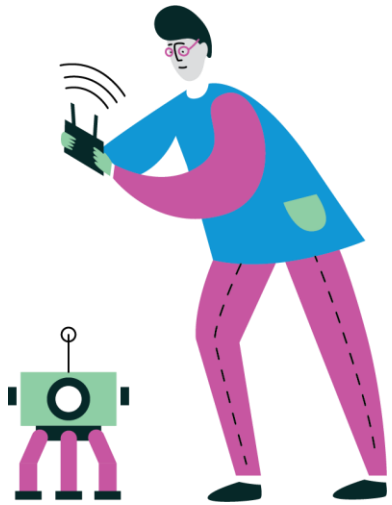
Вопросы 19, 20

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

19. «ЁГЯЁЫБЙ» Правильный ответ — «АЛФАВИТ».

20. «УКАБЫГЮЧ» Правильный ответ — «АЛГОРИТМ».

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



Задание 21 (кейс)

**Каковы возможные сценарии утечки макетов?**

- Наиболее вероятные сценарии - утечка реквизитов ресурса, неосторожность пользователей, умысел сотрудника рекламной компании, шпионаж, нарушения безопасности поставщика услуг облачного хранилища.

**Как можно было это предотвратить?**

- Подход к организации безопасности выбирается в зависимости от возможного сценария утечки. Сервис обмена файлами мог бы быть организован средствами самой компании. Либо можно было бы ввести более жёсткие требования для доступа к ресурсу.

**Варианты взаимодействия клиентов с рекламной компанией, при которых риск утечки конфиденциальных данных был бы ниже.**

- Организовать хранение файлов с доступом только на запись, без возможности загрузки отправленного макета.
- Обязательное использование асимметричного шифрования, чтобы отправленные макеты могли быть расшифрованы только сотрудниками компании.
- Использование облачного ресурса, поддерживающего многофакторную аутентификацию и ведение журнала доступа.