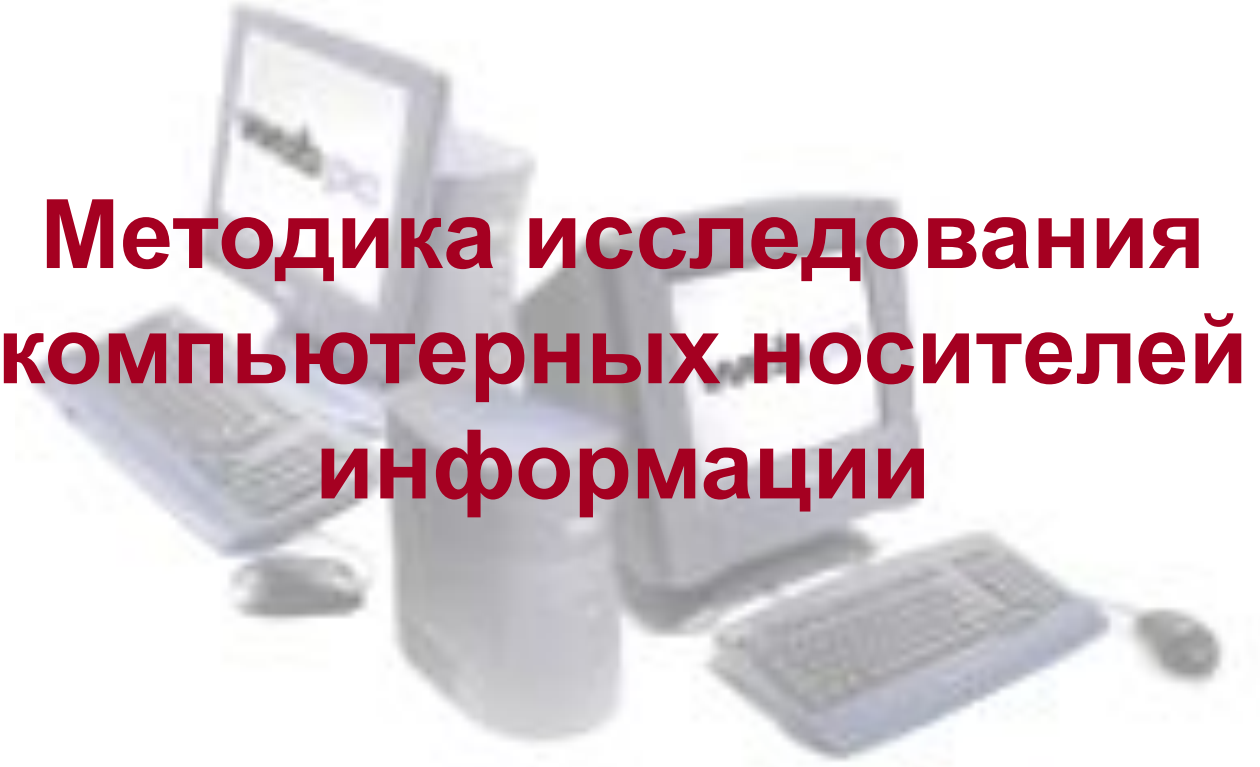

Методика исследования компьютерных носителей информации

Учебные вопросы

1. Общая характеристика компьютерных носителей информации
2. Основные задачи и этапы исследования компьютерных носителей информации

Рекомендуемые сокращения

- КНИ – компьютерный носитель информации
- ОС – операционная система
- И т.д.

Учебный вопрос №1

1. Общая характеристика компьютерных носителей информации
2. Основные задачи и этапы исследования

Понятие компьютерных носителей информации

Компьютерный носитель информации

– физическое устройство, входящее в состав компьютерной системы и предназначенное для хранения информации

Классификация компьютерных носителей информации

- По физическому принципу хранения информации:
  - магнитные, электронные, оптические, магнитооптические
- По зависимости от электропитания:
  - энергозависимые, энергонезависимые
- По конструктивному исполнению:
  - сменные, внутренние

Характеристики носителей

- Объем
- Быстродействие
  - время доступа к данным
  - скорость операций чтения/записи
- Размер блока данных

- и т.д.

Представление информации в компьютерных системах

- в цифровой форме
- в двоичной системе счисления

- Любая информация может быть представлена в числовом виде
  - оцифровка
  - кодирование

Организация данных

- Физический уровень
  - Организация данных зависит от типа носителя
  - Основные понятия:
    - устройства, блоки, адресация блоков ...

- Логический уровень
  - Организация данных зависит от применяемого программного обеспечения
  - Основные понятия:
    - файлы, папки, записи, документы …

Организация данных на жестком диске компьютера

- см. отдельную презентацию

Учебный вопрос №2

1. Общая характеристика компьютерных носителей информации
2. Основные задачи и этапы исследования компьютерных носителей информации

Цели исследования

- Обнаружение свидетельств противоправной деятельности
  - Следы информационных преступлений
  - Вредоносные программы
  - Контрафактные программы и данные
  - Финансовые документы

- Получение необходимых сведений для розыскной работы
  - Подготовленные пользователем документы
  - Парольная информация
  - Электронная переписка
  - Адресная книга
  - Посещенные сайты Интернет

Задачи исследования

- Обеспечение условий для исследования
- Поиск информации
- Восстановление данных
- Ревизия данных на носителе
- Фиксация данных
- Исследование данных
- Анализ данных

Обеспечение условий для исследования

- Обеспечение доступности данных
  - Подключение устройства
  - Нейтрализация механизмов защиты
  - Восстановление информации с поврежденных носителей
- Обеспечение сохранности информации
  - Создание копий
- Снятие организационных ограничений
  - Техническое оснащение (оборудование + программы)
  - Привлечение специалистов

Поиск информации на носителях

- Формулировка критериев поиска в соответствии с задачей исследования
- Поиск
- Анализ результатов

- Корректировка критериев
- Поиск

Критерии поиска

- объекты поиска
  - документы,
  - программы,
  - сообщения электронной почты,
  - отдельные фрагменты текста,
  - числовые последовательности
- ограничивающие условия
  - вид информации
  - формат данных
  - дата и время
  - размер

Методы поиска информации на носителях

- просмотр дерева каталогов
- поиск файлов
- поиск в архивах
- поиск в стертых данных
- поиск на физическом уровне

Фиксация данных

- Копирование данных на другие носители
  - Клонирование носителей
- Изъятие носителей

Анализ информации

- Чаще всего выходит за рамки компьютерной разведки
  - Изучение исполняемого программного кода
  - Анализ документов
  - Решение диагностических задач

Вопросы?