МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ

Учреждение образования «Полоцкий государственный университет»

Факультет информационных технологий

Кафедра технологий программирования

**ОТЧЕТ**

**ПРАКТИЧЕСКАЯ РАБОТА №4**

По дисциплине: «Основы защиты информации»

Тема: «Правовое и нормативное обеспечение защиты информации»

ВЫПОЛНИЛ студент группы 16-ИТ-3

Яблонский А.С.

ПРОВЕРИЛ ст. препод. Кафедры ТП

Бурачёнок И.Б.

Полоцк 2018 г.

**ТЕМА**: Изучить содержание основных нормативных актов сферы защиты

информации в Республике Беларусь. Расследование преступлений в сфере

компьютерной информации и иных преступлений, связанных с

использованием компьютерной техники в Республике Беларусь.

**ЦЕЛЬ РАБОТЫ**: Систематизация и закрепление знаний о характеристике

преступлений в сфере информационной безопасности и формирование основ

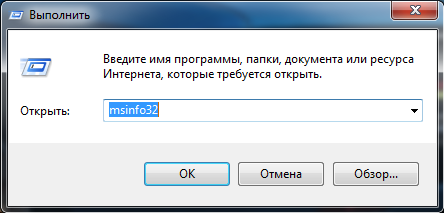
умения их расследовать; выработка навыков выявления и фиксации следов

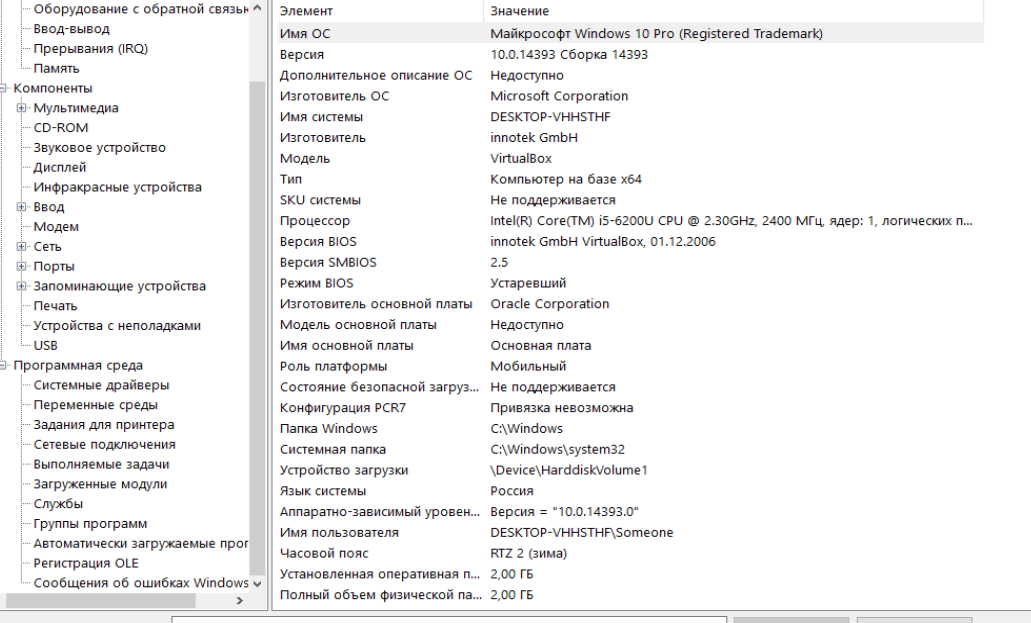
противоправной деятельности при расследовании иных преступлений,

связанных с использованием компьютерной техники.

**Ход работы**:

Нажмем комбинацию клавиш Win + R для запуска окна **Выполнить.** Вводим команду msinfo32



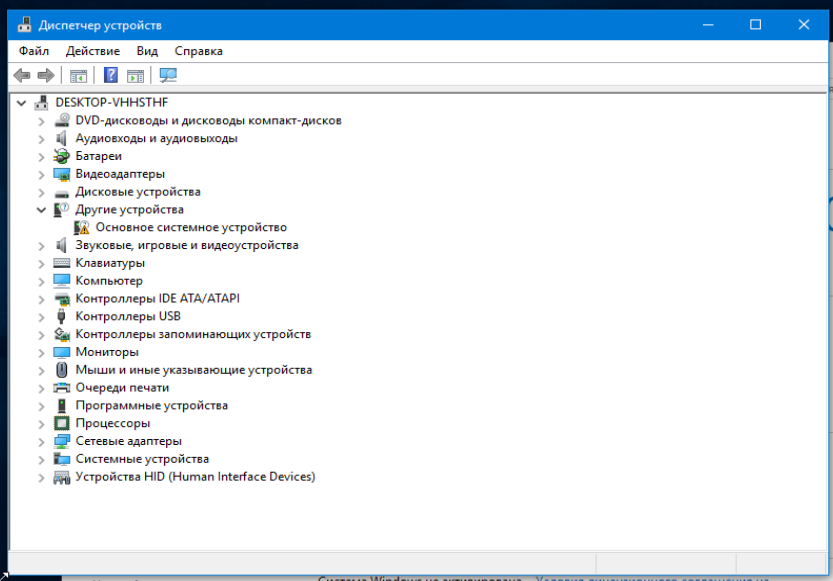
Сведения о данной ЭВМ отображены на рисунке 1.

**Рисунок 1 –** «Сведения о системе»

Подробные сведения о системе можно изучить раскрывая:

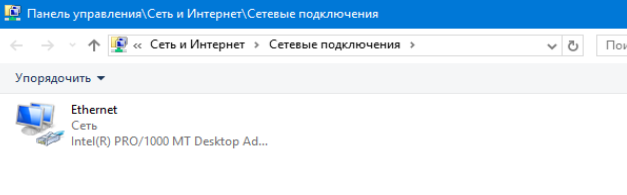
1. Аппаратные ресурсы
2. Компоненты
3. Запоминающие устройства и пр.

Чтобы определить какие устройства подключены к ЭВМ, необходимо выбрать команду **Диспетчер устройств.**



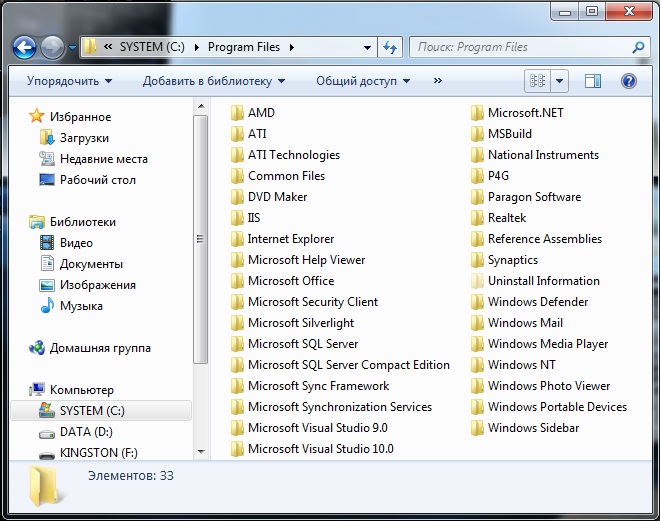
**Рисунок 2 –** «Список устройств ПЭВМ»

Чтобы определить какие имеются сетевые подключения к ЭВМ, необходимо выбрать команду **Сетевые подключения.**

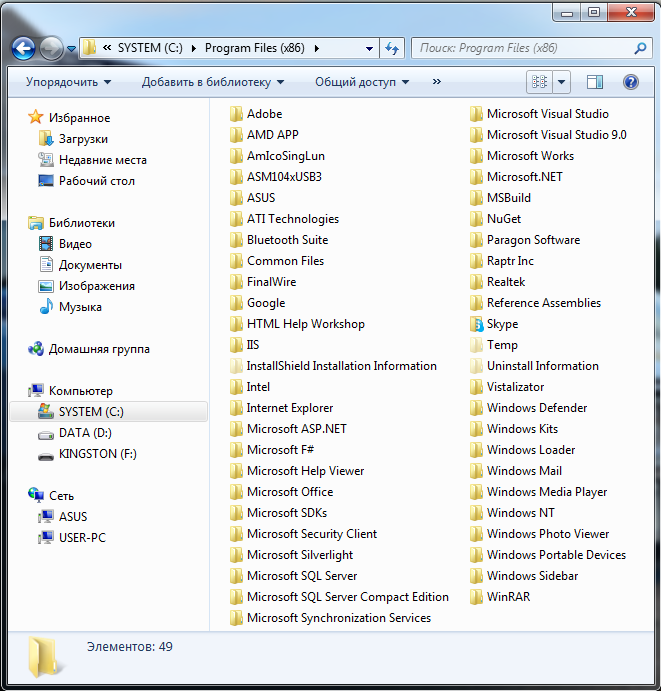


Установленные программы находятся в папках C:\Program Files и C:\Program Files(x86).

Список установленных программ: C:\Program Files

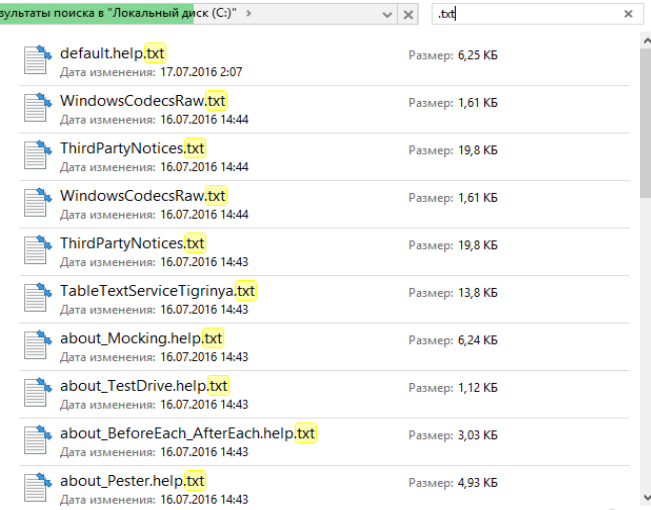


Список установленных программ: C:\Program Files (x86)



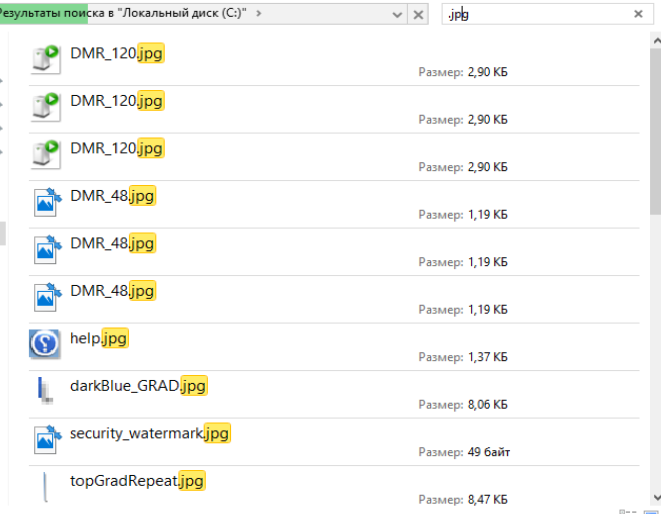
На данном компьютере установлено различно ПО для обработки изображений, текстовых файлов. Средства разработки программных продуктов.

Поиск текстовых файлов:

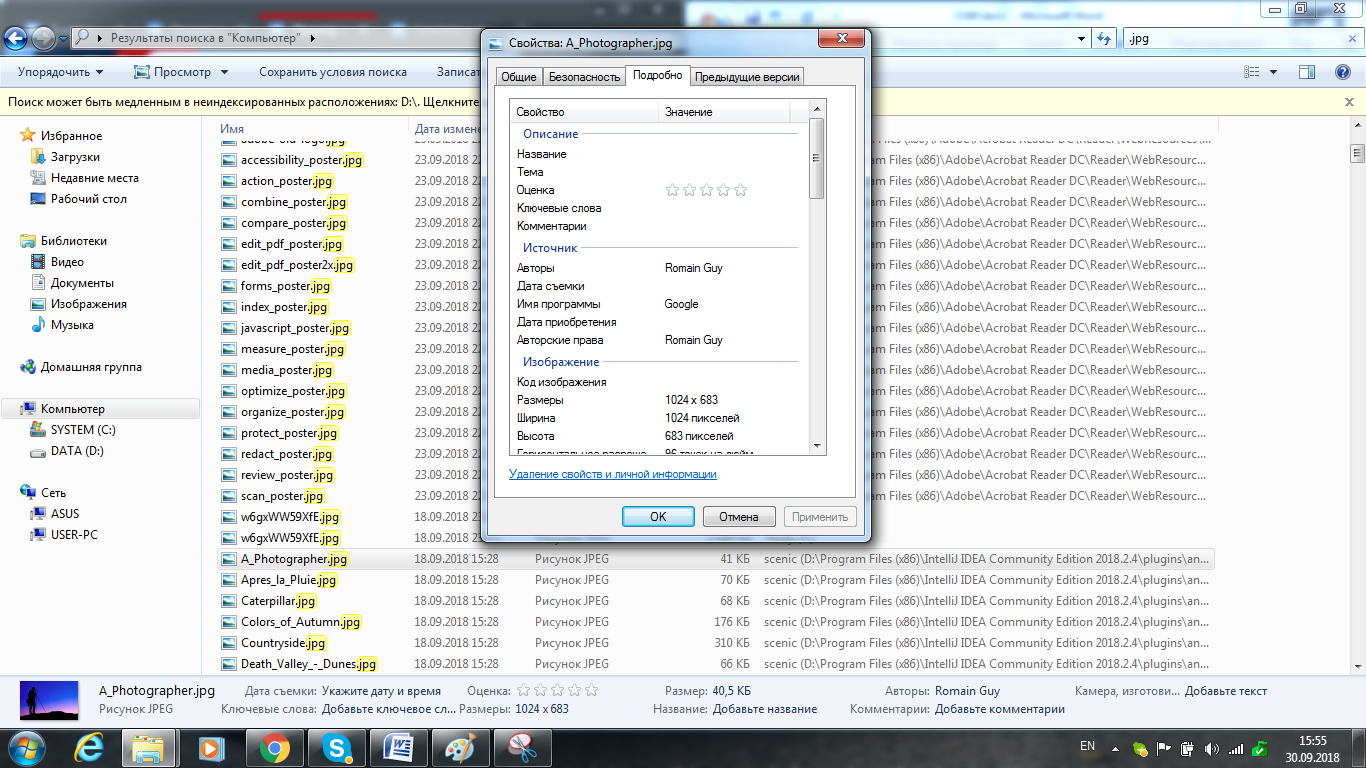


**Рисунок 3 –** «Поиск документов по указанной маске ввода»

Поиск графической информации:



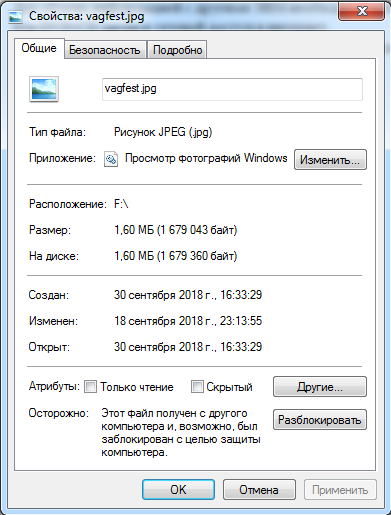
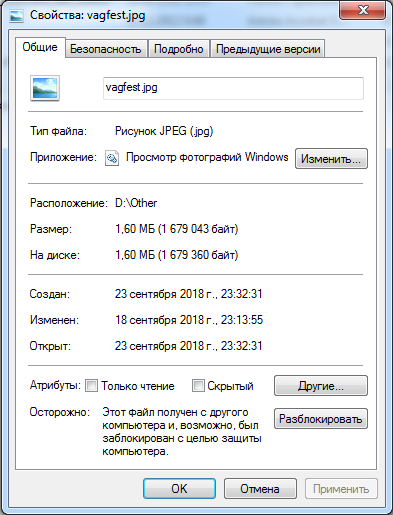
Можно проверить источник, выбрав свойства файла



**Рисунок 3.1 –** «Свойства, Подробно»

Для обмена информацией с другими ЭВМ необходимо использовать флэш накопители или DVD/CD диски и сетевой доступ в интернет.

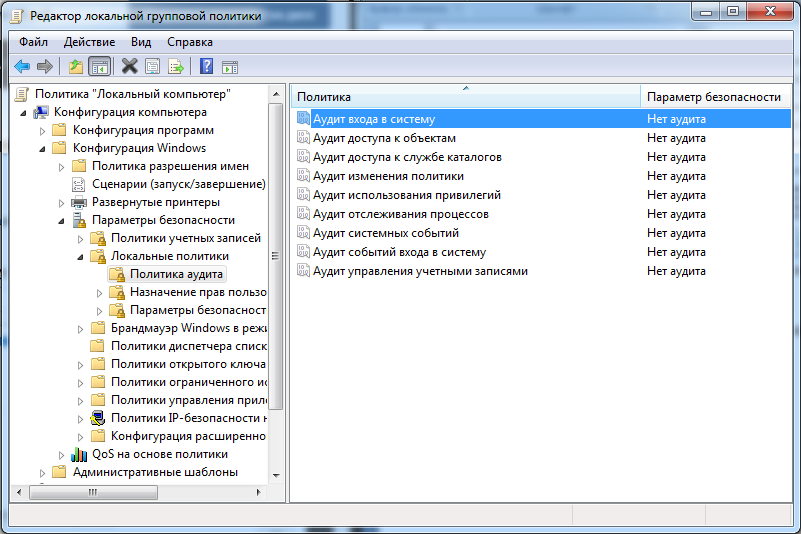
После переноса файла изменилась только дата создания документа (рисунок 4).



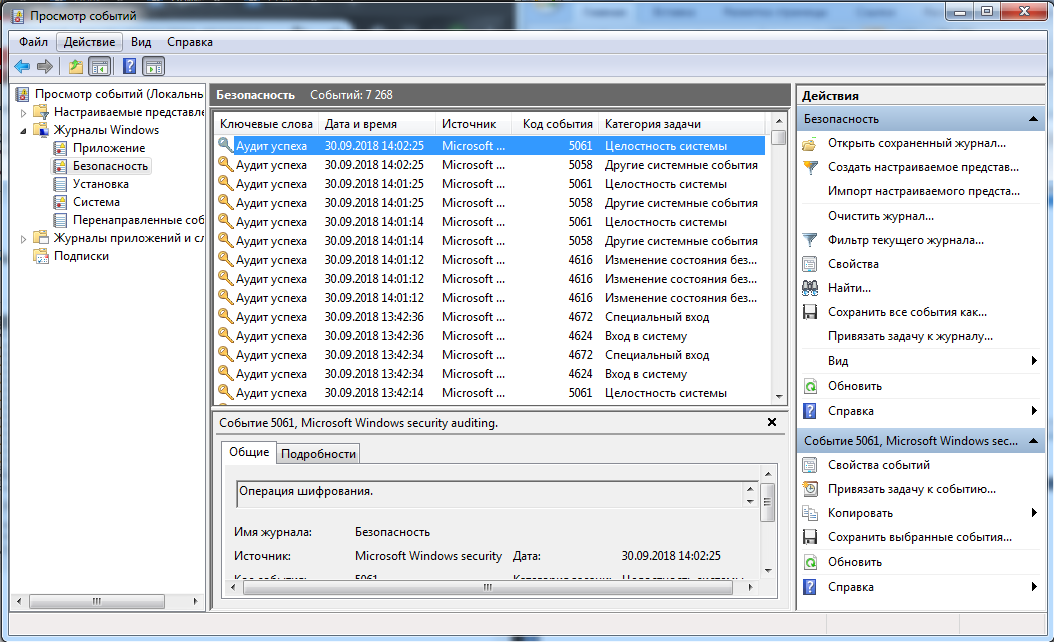
**Рисунок 4 –** «Свойства файла до и после переноса на другую ПЭВМ»

Для того, чтобы определить пользовались ли ЭВМ, необходимо:

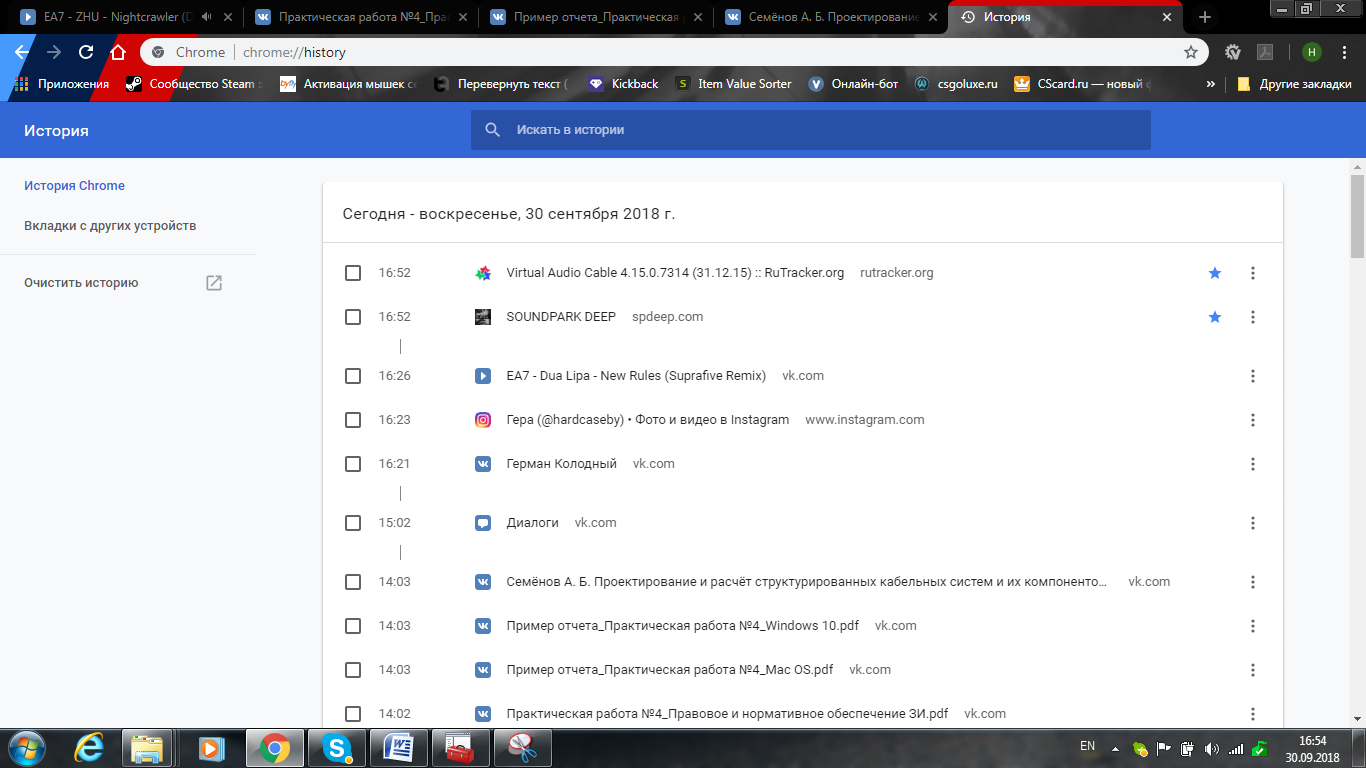
1. Просмотреть аудита входа в систему производиться при помощи выполнения команды gpedit.msc



1. Для просмотра событий Windows выполните команду eventvwr.msc

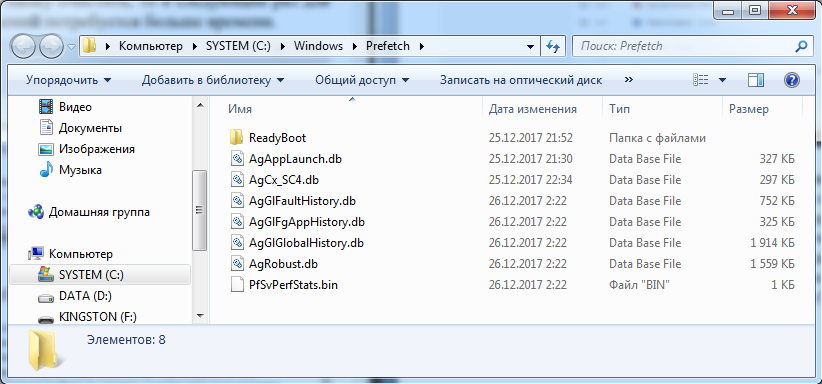


1. Последние открытые фалы доступны по адресу: **C:\Users\USERNAME\AppData\Roaming\Microsoft\Windows\Recent**
2. История посещения WEB страниц в разных браузерах доступна по разному. Пример историю браузера Google Chrome:



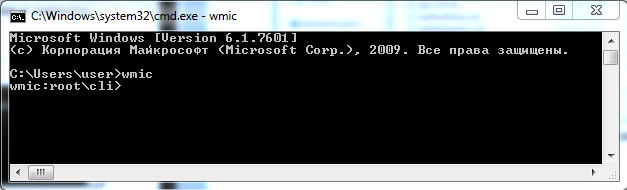
1. Работа с папкой **Prefetch**

Всякий раз при включении компьютера Windows отслеживает способ его запуска и приложения, которые обычно открываются. Эти сведения сохраняются Windows в папке Prefetch в виде файлов небольшого размера. При следующем включении компьютера Windows обращается к данным файлам для ускорения процесса запуска. Папка Prefetch вложена в системную папку Windows и поддерживается самостоятельно, поэтому нет необходимости в ее удалении или очистке содержимого. Если эту папку очистить, то в следующий раз для загрузки Windows и запуска приложений потребуется больше времени.

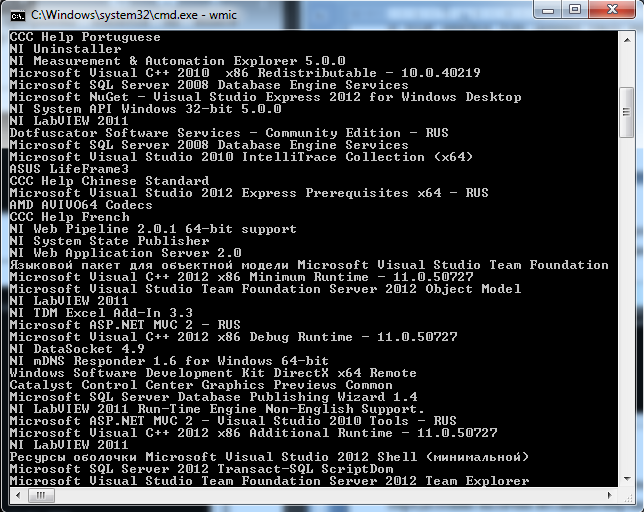


В ходе анализа этих данных было выявлено, что несанкционированного доступа к ЭВМ не было.

1. Чтобы определить какие программы имеются на вашем компьютере, необходимо открыть **Командную строку** и ввести:
   1. **wmic**

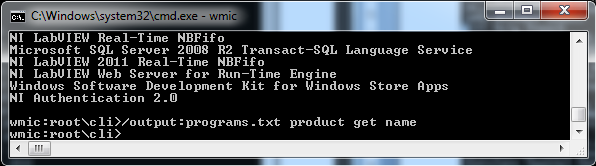


* 1. **product get name**

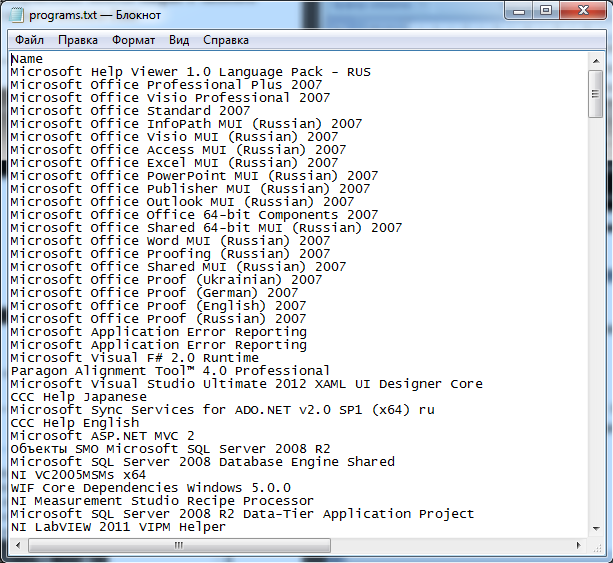


Для удобства последующего анализа списка установленных программ можно воспользоваться командой перенаправления вывода **output** и записать в текстовый файл, например в текущей папке с именем A**ppList.txt**.

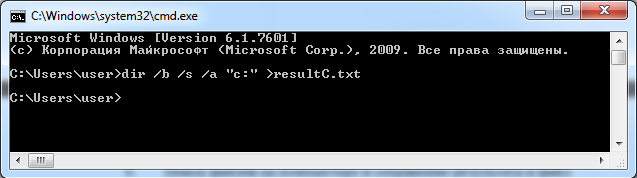
* 1. /**output:AppList .txt product get name**

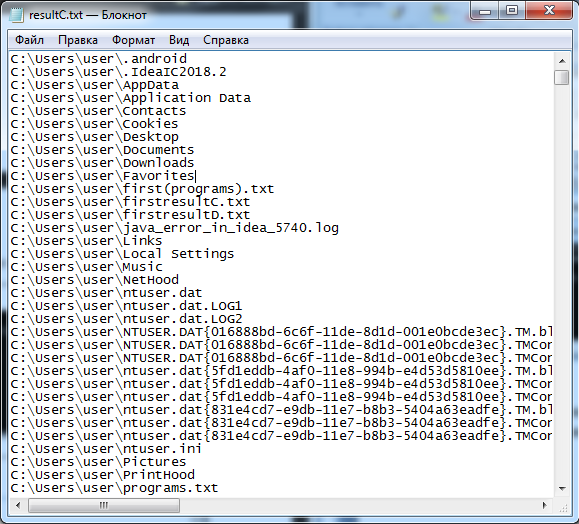


* 1. Список установленных программ сохранится в файле **AppList.txt** в текущей папке.

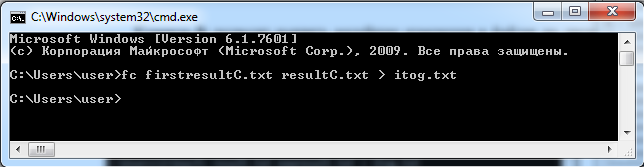


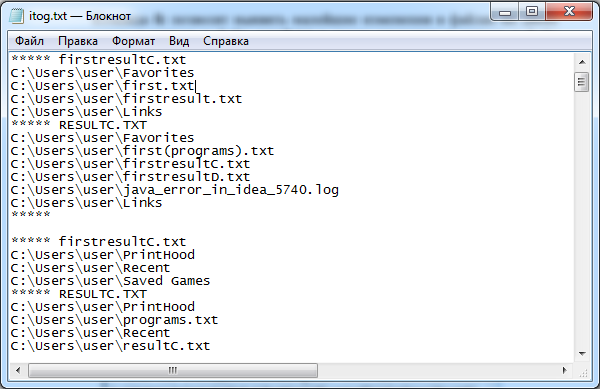
* 1. Поиск файлов на компьютере и сохранение результата в файл.





Команда **fc** позволяет выявить малейшие изменения в файлах на диске до проверки и записи в файл **serach.txt** и после проверки и записи в файл **serach.txt**. Все изменения, происходящие в системе, будут внесены в файл **itog.txt**.





**Вывод:** В ходе выполнения данной практической работы был приобретен навык определения наличия несанкционированного доступа к ЭВМ. Закреплены знания о характеристике преступлений в сфере информационной безопасности и получили понятие о методах и порядке расследований преступлений в Республике Беларусь, связанных с использованием компьютерной техники.