

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.

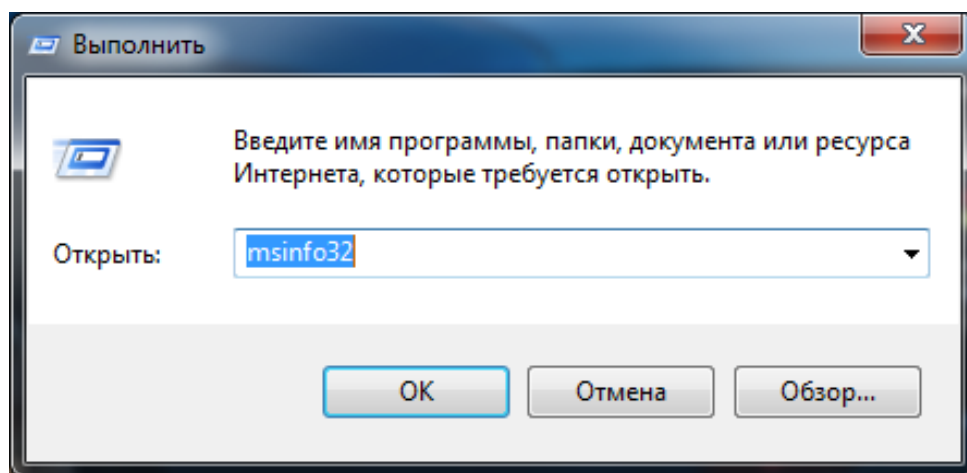
Полоцк 2018 г.

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 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



Оборудование с обратной связью		Элемент	Значение
Ввод-вывод		Имя ОС	Майкрософт Windows 10 Pro (Registered Trademark)
Прерывания (IRQ)		Версия	10.0.14393 Сборка 14393
Память		Дополнительное описание ОС	Недоступно
Компоненты		Изготовитель ОС	Microsoft Corporation
Мультимедиа		Имя системы	DESKTOP-VNHSTHF
CD-ROM		Изготовитель	innotek GmbH
Звуковое устройство		Модель	VirtualBox
Дисплей		Тип	Компьютер на базе x64
Инфракрасные устройства		SKU системы	Не поддерживается
Ввод		Процессор	Intel(R) Core(TM) i5-6200U CPU @ 2.30GHz, 2400 МГц, ядер: 1, логических п...
Модем		Версия BIOS	innotek GmbH VirtualBox, 01.12.2006
Сеть		Версия SMBIOS	2.5
Порты		Режим BIOS	Устаревший
Запоминающие устройства		Изготовитель основной платы	Oracle Corporation
Печать		Модель основной платы	Недоступно
Устройства с неполадками		Имя основной платы	Основная плата
USB		Роль платформы	Мобильный
Программная среда		Состояние безопасной загруз...	Не поддерживается
Системные драйверы		Конфигурация PCR7	Привязка невозможна
Переменные среды		Папка Windows	C:\Windows
Задания для принтера		Системная папка	C:\Windows\system32
Сетевые подключения		Устройство загрузки	\Device\HarddiskVolume1
Выполняемые задачи		Язык системы	Россия
Загруженные модули		Аппаратно-зависимый уровен...	Версия = "10.0.14393.0"
Службы		Имя пользователя	DESKTOP-VNHSTHF\Someone
Группы программ		Часовой пояс	RTZ 2 (зима)
Автоматически загружаемые прог		Установленная оперативная п...	2,00 ГБ
Регистрация OLE		Полный объем физической па...	2,00 ГБ
Сообщения об ошибках Windows			

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**.

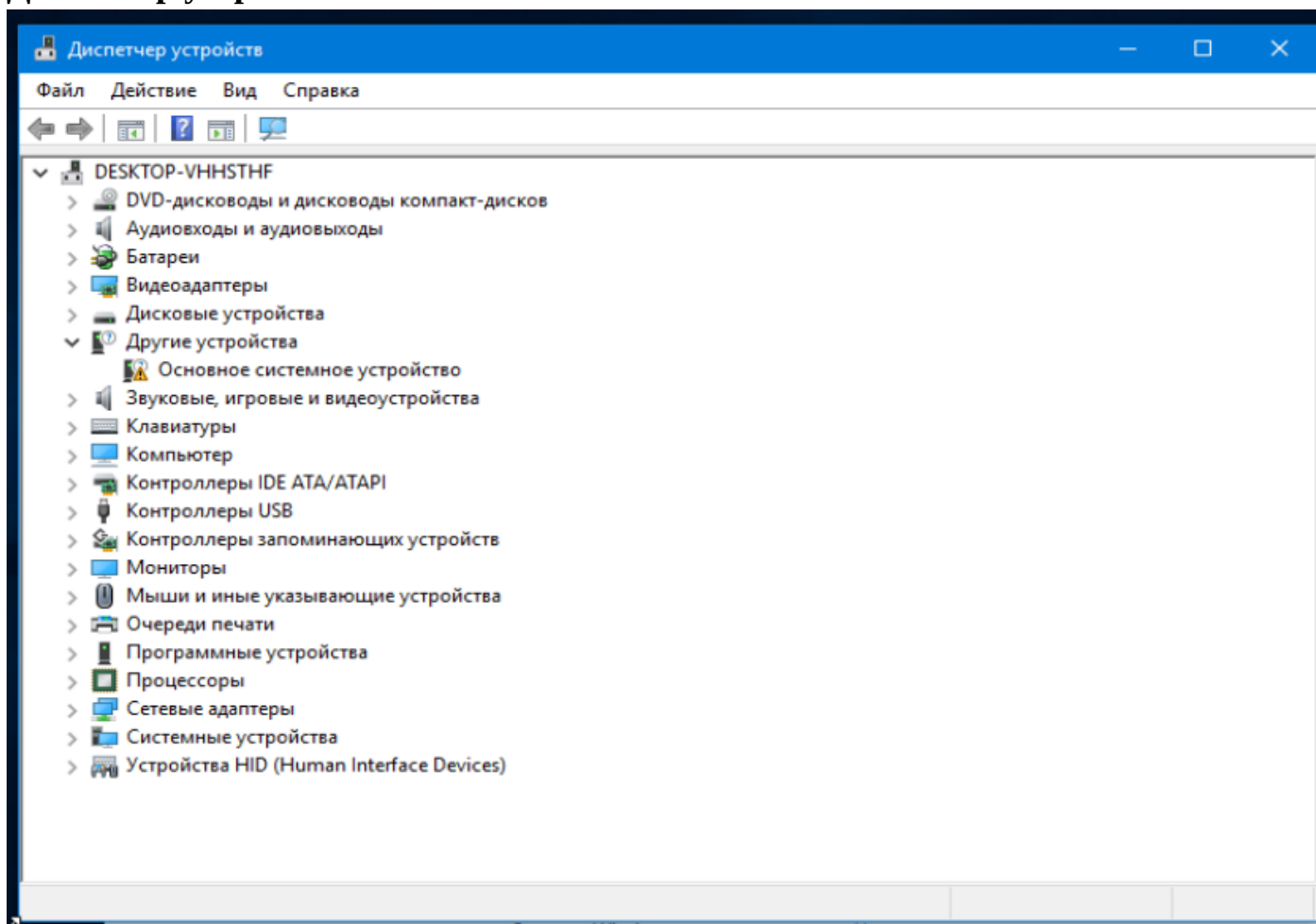
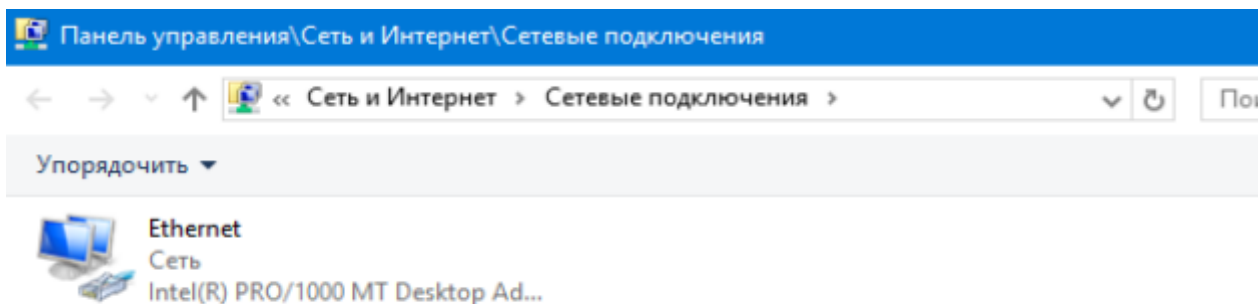


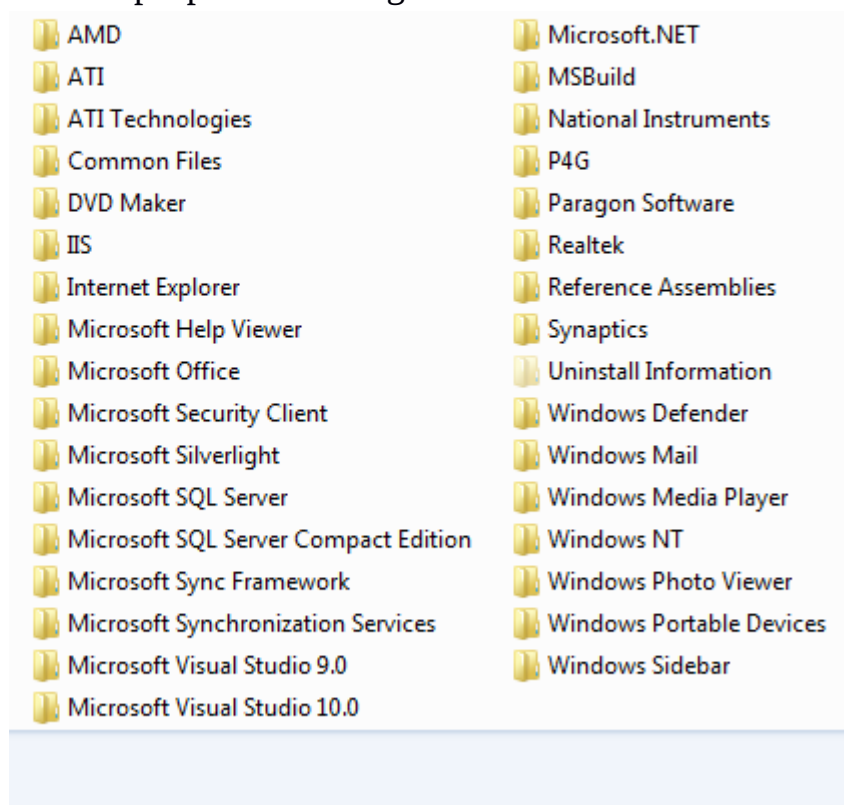
Рисунок 2 – «Список устройств ПЭВМ»

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

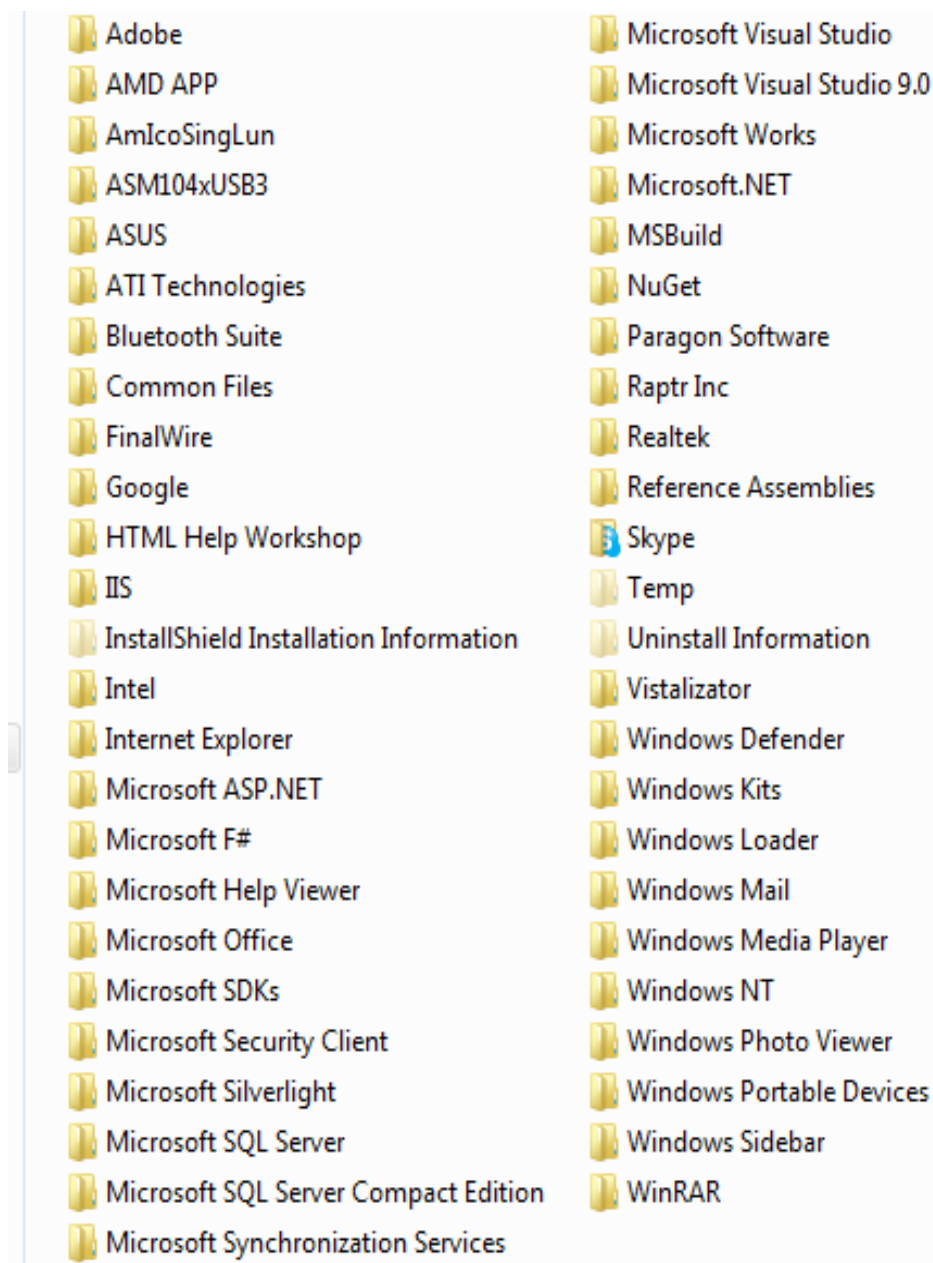


Установленные программы находятся в папках C:\Program Files и C:\Program Files(x86).

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:

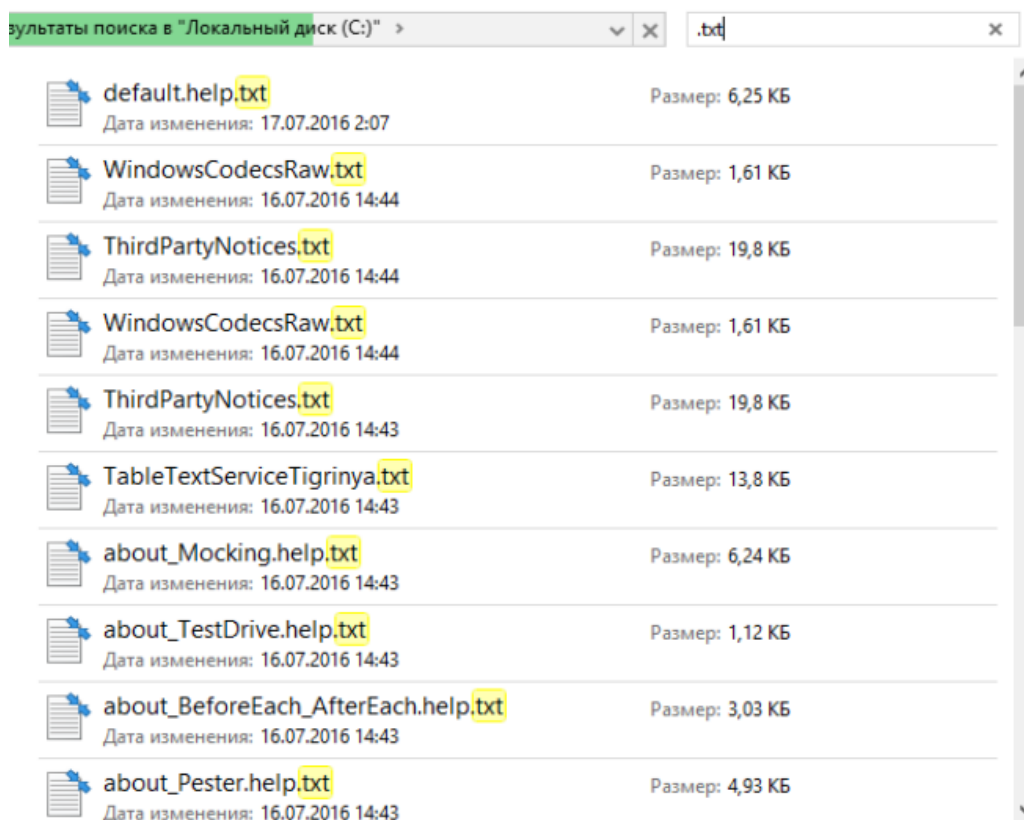
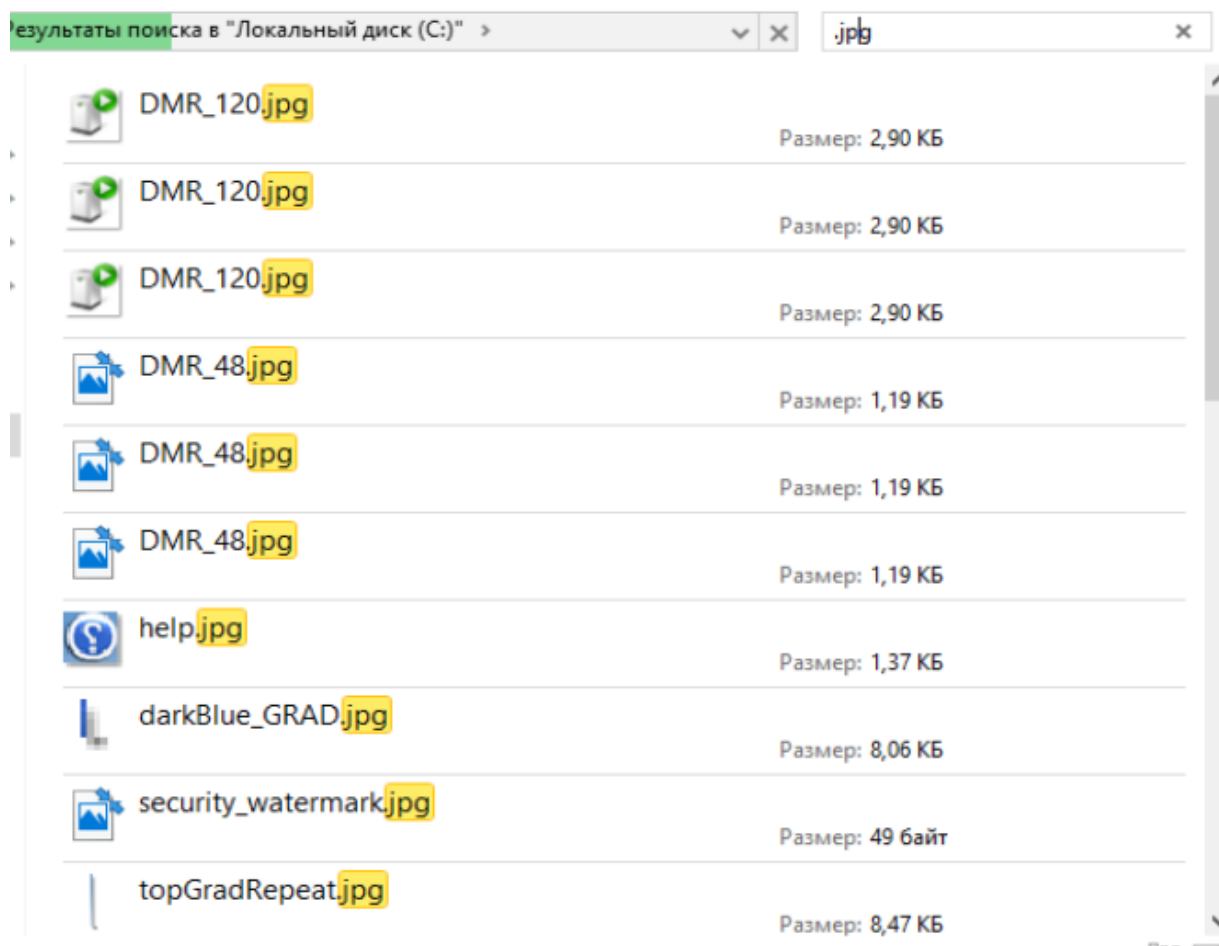


Рисунок 3 – «Поиск документов по указанной маске ввода»

Поиск графической информации:



Можно проверить источник, выбрав свойства файла

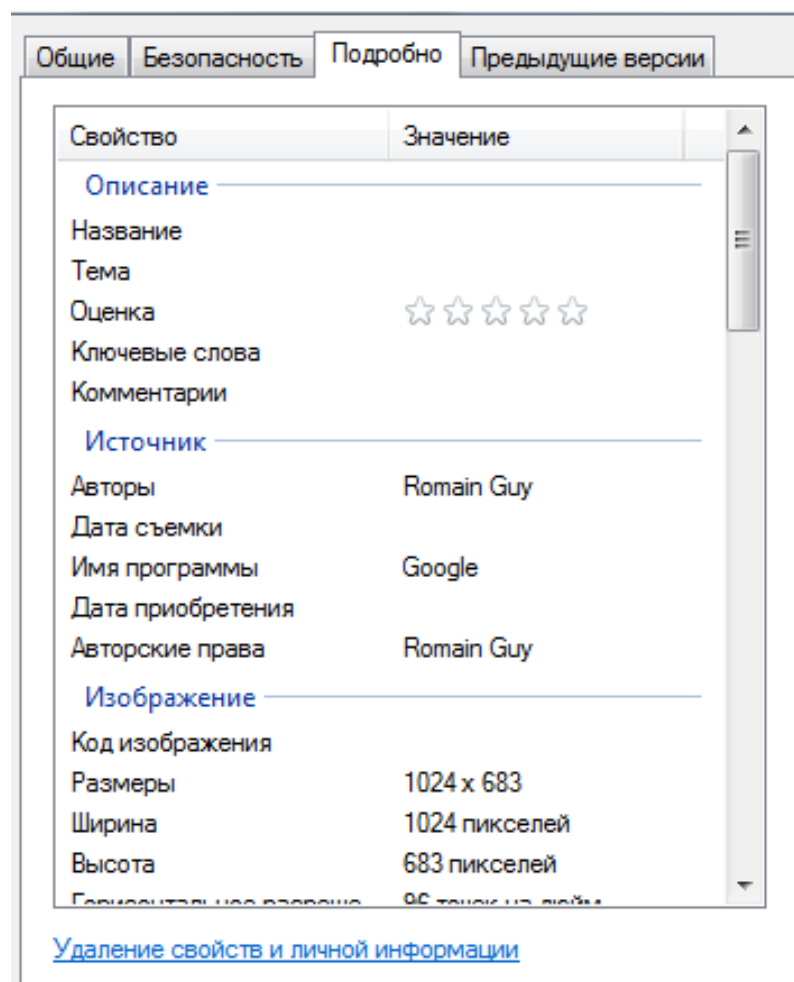


Рисунок 3.1 – «Свойства, Подробно»

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).

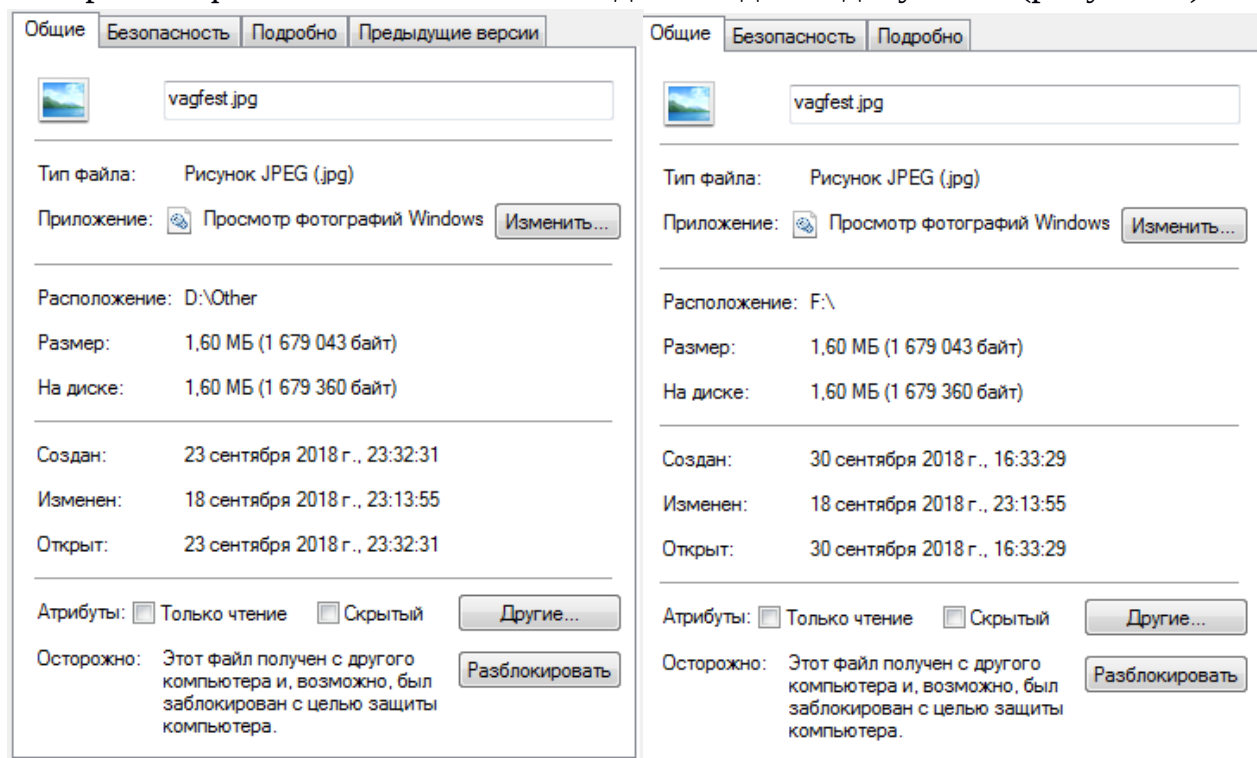
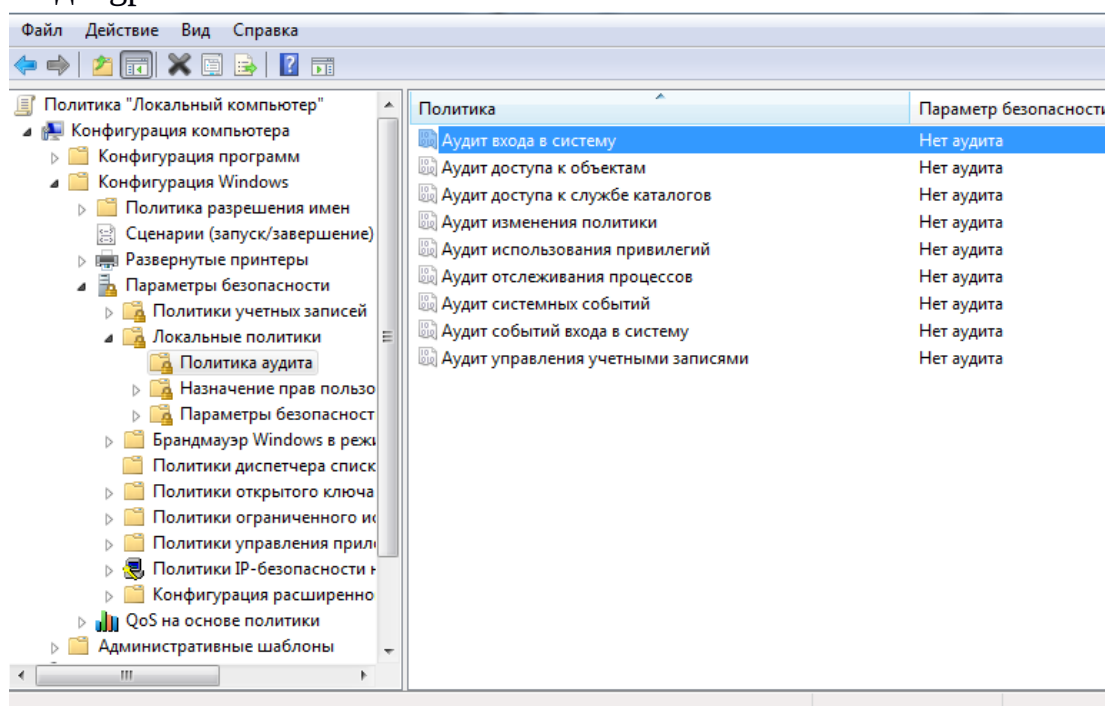


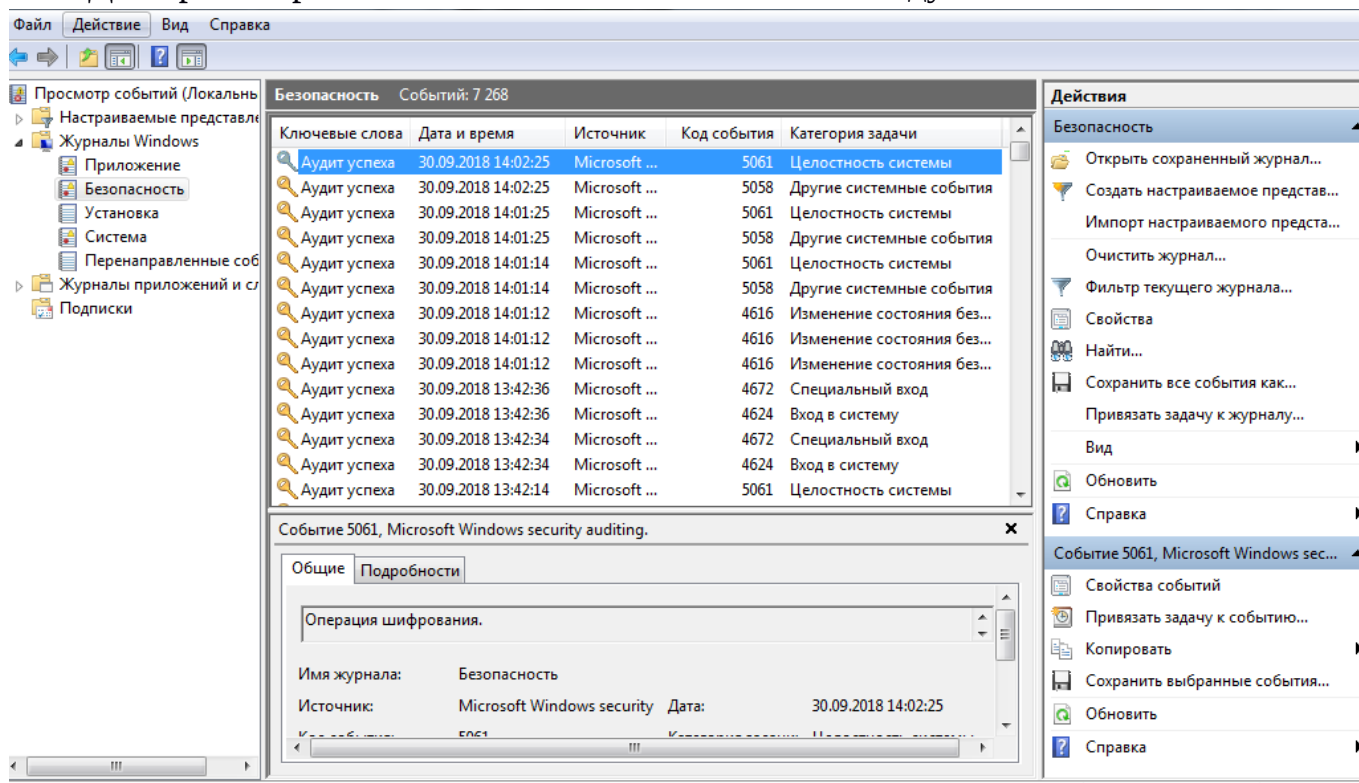
Рисунок 4 – «Свойства файла до и после переноса на другую ПЭВМ»

Для того, чтобы определить пользовались ли ЭВМ, необходимо:

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



2. Для просмотра событий Windows выполните команду eventvwr.msc

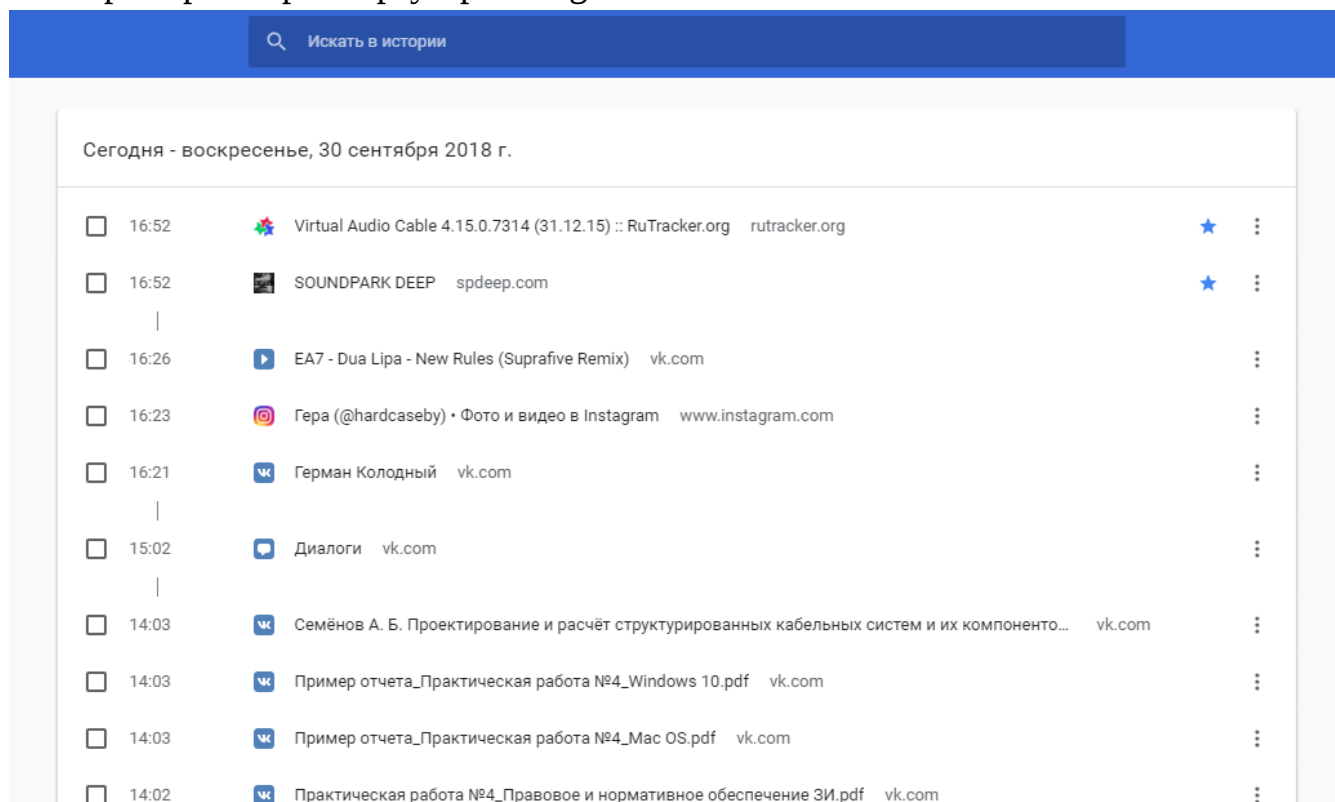


3. Последние открытые файлы доступны по адресу:

C:\Users\USERNAME\AppData\Roaming\Microsoft\Windows\Recent

4. История посещения WEB страниц в разных браузерах доступна по разному.

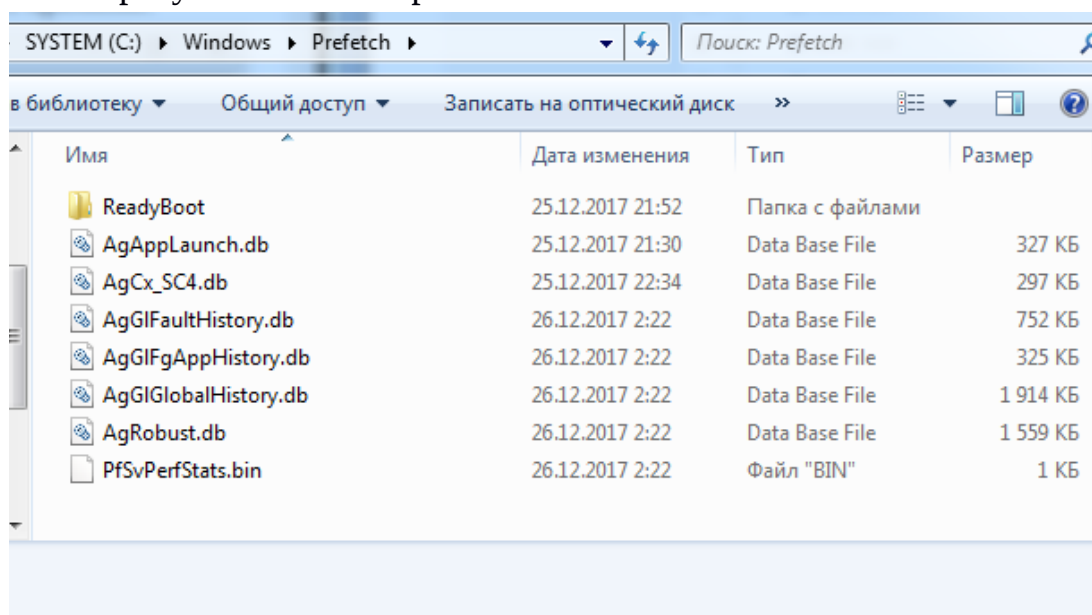
Пример историю браузера Google Chrome:



5. 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

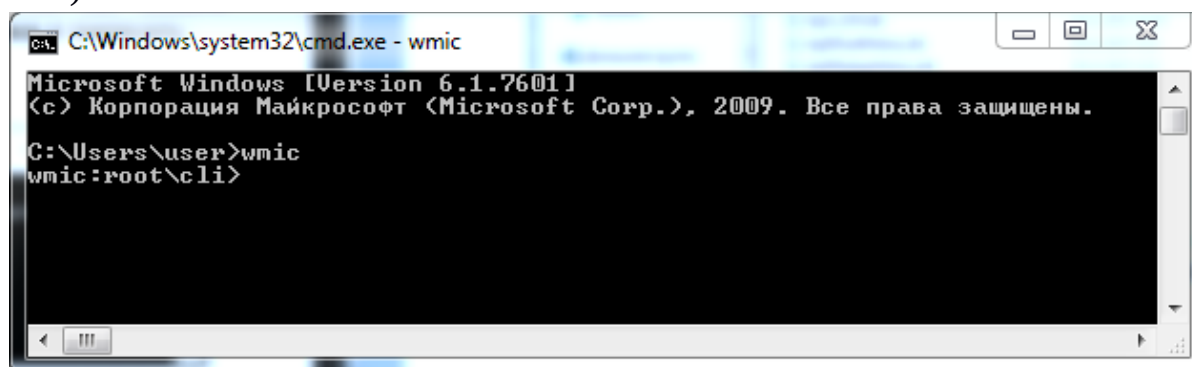
компьютера Windows обращается к данным файлам для ускорения процесса запуска. Папка Prefetch вложена в системную папку Windows и поддерживается самостоятельно, поэтому нет необходимости в ее удалении или очистке содержимого. Если эту папку очистить, то в следующий раз для загрузки Windows и запуска приложений потребуется больше времени.



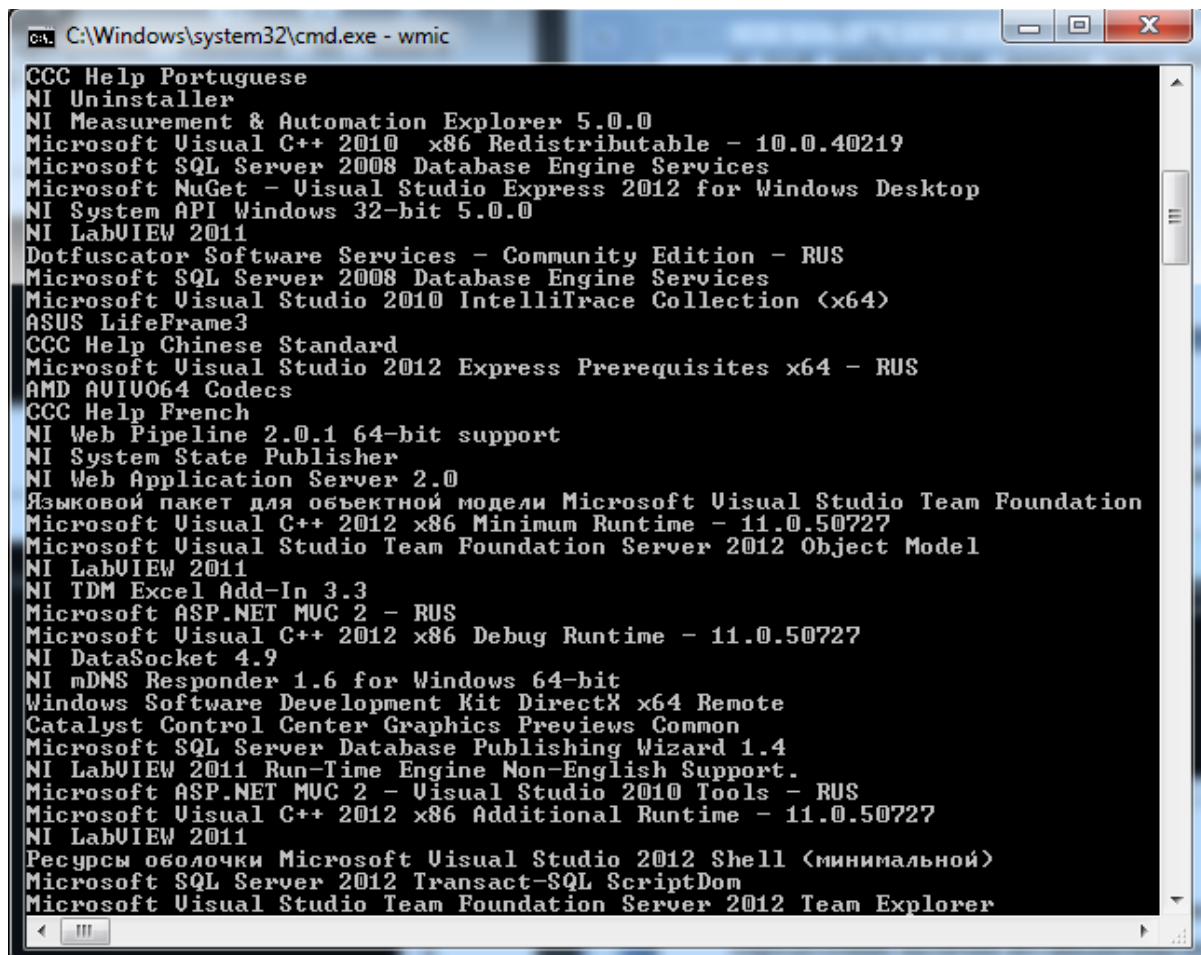
В ходе анализа этих данных было выявлено, что несанкционированного доступа к ЭВМ не было.

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

а) **wmic**



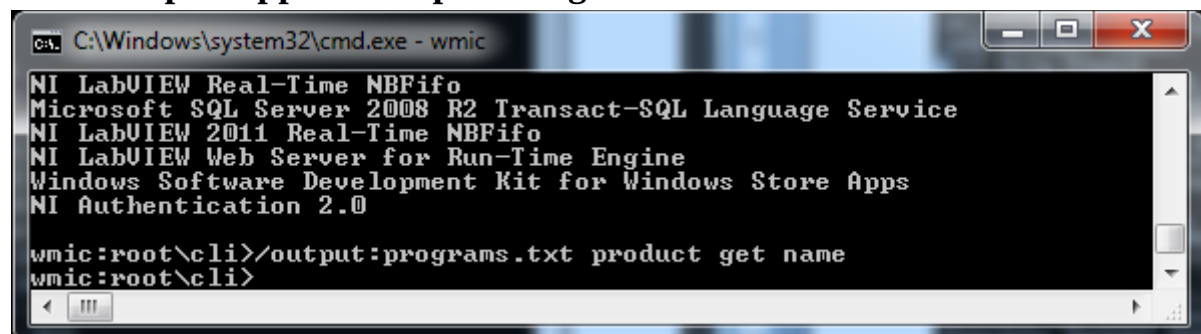
б) **product get name**



```
C:\Windows\system32\cmd.exe - wmic
CCC Help Portuguese
NI Uninstaller
NI Measurement & Automation Explorer 5.0.0
Microsoft Visual C++ 2010 x86 Redistributable - 10.0.40219
Microsoft SQL Server 2008 Database Engine Services
Microsoft NuGet - Visual Studio Express 2012 for Windows Desktop
NI System API Windows 32-bit 5.0.0
NI LabVIEW 2011
Dotfuscator Software Services - Community Edition - RUS
Microsoft SQL Server 2008 Database Engine Services
Microsoft Visual Studio 2010 IntelliTrace Collection (x64)
ASUS LifeFrame3
CCC Help Chinese Standard
Microsoft Visual Studio 2012 Express Prerequisites x64 - RUS
AMD AVIVO64 Codecs
CCC Help French
NI Web Pipeline 2.0.1 64-bit support
NI System State Publisher
NI Web Application Server 2.0
Языковой пакет для объектной модели Microsoft Visual Studio Team Foundation
Microsoft Visual C++ 2012 x86 Minimum Runtime - 11.0.50727
Microsoft Visual Studio Team Foundation Server 2012 Object Model
NI LabVIEW 2011
NI TDM Excel Add-In 3.3
Microsoft ASP.NET MVC 2 - RUS
Microsoft Visual C++ 2012 x86 Debug Runtime - 11.0.50727
NI DataSocket 4.9
NI mDNS Responder 1.6 for Windows 64-bit
Windows Software Development Kit DirectX x64 Remote
Catalyst Control Center Graphics Previews Common
Microsoft SQL Server Database Publishing Wizard 1.4
NI LabVIEW 2011 Run-Time Engine Non-English Support.
Microsoft ASP.NET MVC 2 - Visual Studio 2010 Tools - RUS
Microsoft Visual C++ 2012 x86 Additional Runtime - 11.0.50727
NI LabVIEW 2011
Ресурсы оболочки Microsoft Visual Studio 2012 Shell (минимальной)
Microsoft SQL Server 2012 Transact-SQL ScriptDom
Microsoft Visual Studio Team Foundation Server 2012 Team Explorer
```

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

с) **/output:AppList .txt product get name**



```
C:\Windows\system32\cmd.exe - wmic
NI LabVIEW Real-Time NBFifo
Microsoft SQL Server 2008 R2 Transact-SQL Language Service
NI LabVIEW 2011 Real-Time NBFifo
NI LabVIEW Web Server for Run-Time Engine
Windows Software Development Kit for Windows Store Apps
NI Authentication 2.0

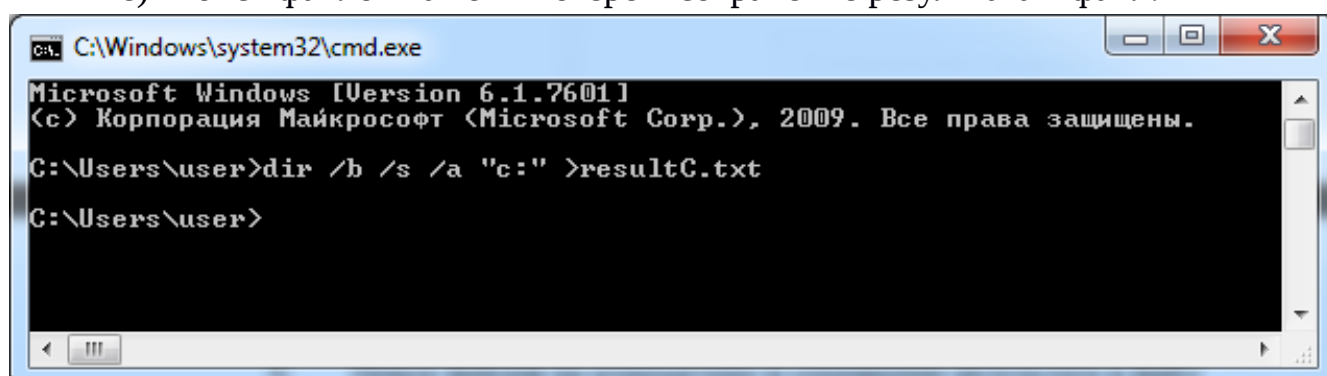
wmic:root\cli>/output:programs.txt product get name
wmic:root\cli>
```

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

Файл Правка Формат Вид Справка

Name
Microsoft Help viewer 1.0 Language Pack - RU
Microsoft Office Professional Plus 2007
Microsoft Office Visio Professional 2007
Microsoft Office Standard 2007
Microsoft Office InfoPath MUI (Russian) 2007
Microsoft Office Visio MUI (Russian) 2007
Microsoft Office Access MUI (Russian) 2007
Microsoft Office Excel MUI (Russian) 2007
Microsoft Office PowerPoint MUI (Russian) 2007
Microsoft Office Publisher MUI (Russian) 2007
Microsoft Office Outlook MUI (Russian) 2007
Microsoft Office Office 64-bit Components 2007
Microsoft Office Shared 64-bit MUI (Russian) 2007
Microsoft Office Word MUI (Russian) 2007
Microsoft Office Proofing (Russian) 2007
Microsoft Office Shared MUI (Russian) 2007
Microsoft Office Proof (Ukrainian) 2007
Microsoft Office Proof (German) 2007
Microsoft Office Proof (English) 2007
Microsoft Office Proof (Russian) 2007
Microsoft Application Error Reporting
Microsoft Application Error Reporting
Microsoft Visual F# 2.0 Runtime
Paragon Alignment Tool™ 4.0 Professional
Microsoft Visual Studio Ultimate 2012 XAML UI Designer Core
CCC Help Japanese
Microsoft Sync Services for ADO.NET v2.0 SP1 (x64) ru
CCC Help English
Microsoft ASP.NET MVC 2
Объекты SMO Microsoft SQL Server 2008 R2
Microsoft SQL Server 2008 Database Engine Shared
NI VC2005MSMs x64
WIF Core Dependencies windows 5.0.0
NI Measurement Studio Recipe Processor
Microsoft SQL Server 2008 R2 Data-Tier Application Project
NI LabVIEW 2011 VIPM Helper

е) Поиск файлов на компьютере и сохранение результата в файл.



```
C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7601]
(c) Корпорация Майкрософт (Microsoft Corp.), 2009. Все права защищены.
C:\Users\user>dir /b /s /a "c:.*" >resultC.txt
C:\Users\user>
```


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.