МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РФ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

Методические указания

по выполнению лабораторных работ
по дисциплине
«КОМПЬЮТЕРНАЯ КРИМИНАЛИСТИКА»
для студентов специальности 10.05.03 Информационная безопасность автоматизированных систем, специализация Анализ безопасности информационных систем

Ставрополь
2026

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Цель и задачи освоения дисциплины

Целью освоения дисциплины «Компьютерная криминалистика» является формирование у будущего специалиста по специальности 10.05.03 Информационная безопасность автоматизированных систем специализация «Анализ безопасности информационных систем» знаний в области компьютерной криминалистики, сбора и анализа цифровых доказательств.

Задачи преподавания дисциплины:

изучение этапов, методов и средств проведения компьютерно-технических экспертиз;

освоение способов и методов средств сбора цифровых доказательств;

освоение методов организации и управления деятельности служб защиты информации на предприятии.

СТРУКТУРА И СОДЕРЖАНИЕ ЛАБОРАТОРНЫХ ЗАНЯТИЙ

1. ИССЛЕДОВАНИЕ ПОЛИТИКИ БЕЗОПАСНОСТИ

Цель – исследовать соответствие политики безопасности и настроек ОС.

Формируемые компетенции: ПК-4, ПК-9, ПК-24, ПК-25, ПК-30.»

«Пример выполнения работы

1. Пакет KB3096447 (это обновление для системы безопасности устраняет уязвимости в Windows. Более серьезная из этих уязвимостей делает возможным несанкционированное получение прав при входе на уязвимой системе злоумышленником и запускает специально созданное приложение).

2. Пакет KB3096443 (это обновление для системы безопасности устраняет уязвимости в Windows. Эти уязвимости делают возможным удаленное выполнение кода, если пользователь открывает специально созданный инструментов объект в Windows или злоумышленник побуждает пользователя посетить специально созданного содержимого в Интернете).

3. Пакет KB3096448 (это обновление для системы безопасности устраняет уязвимость в Microsoft края. Уязвимость делает» возможным удаленное выполнение кода при просмотре специально созданной веб страницы в Microsoft края).4. Пакет KB3096441 (данное обновление устраняет несколько уязвимостей, обнаруженных в обозревателе Internet Explorer. Наиболее серьезная из этих уязвимостей делает возможным удаленное выполнение кода при просмотре специально созданной веб страницы в обозревателе Internet Explorer).5. Пакет KB3080446 (это обновление для системы безопасности устраняет уязвимость в Windows. Такие уязвимости делают возможным удаленное выполнение кода, если пользователь откроет специально созданный объект на панели инструментов в Windows, или если злоумышленник убеждает пользователя для просмотра специальное содержимое в Интернете).6. Пакет KB3105216 (обновление для уязвимости в Adobe Flash Player в Internet Explorer и Microsoft Edge).7. Пакет KB3087390 (исправляет баг в файле ядра Windows8.1 / RT 8.1 и системных файлах, включая, Ntoskrnl.exe, Ntdll.dll,Ntvdm64.dll, Wow64.dll, Advapi32.dll. Исправляемый баг приводил к неправильному поведению компонентов ОС при работе программ с разделом системного реестра для COM объектов).8. Пакет KB3075249 (это обновление добавляет телеметрии, указывает на User Account Control (UAC) особенность собирать информацию о высотах, которые приходят от низких уровней целостности).9. Пакет KB3074228 (это обновление устраняет уязвимости вMicrosoft.NET Framework, которые могут привести к несанкционированному получению прав, если пользователь работает специально созданный .NET Framework приложения).10. Пакет KB3065822 (это обновление для системы безопасности устраняет несколько уязвимостей в Internet Explorer. Наиболее серьезная из этих уязвимостей делает возможным удаленное выполнение кода, если пользователь просматривает специально созданный веб страницы в Internet Explorer).

Задание

Получить и привести описание перечня установленных обновлений безопасности исследуемой ОС.

Содержание отчета

Форма отчета должна соответствовать требованиям к оформлению простого реферата. Титульный лист должен включать на «звание дисциплины, название лабораторной работы, фамилию и инициалы сдающего, номер группы, фамилию и инициалы принимающего преподавателя. Основная часть работы должна содержать:− описание проведенной работы;− выводы о проделанной работе.

Контрольные вопросы

1. Как производится исследование компьютерной техники при криминалистической экспертизе?

2. С помощью каких средств можно получить перечень установленных программ на ЭПК?

2. ИЗУЧЕНИЕ КЛАССИФИКАЦИИИ УПРАВЛЕНИЕ РЕСУРСАМИПО ОГРАНИЧЕНИЮ ИНЦИДЕНТОВ ИБ

Цель – исследовать организационные меры по обеспечению безопасности.

Формируемые компетенции: ПК-4, ПК-9, ПК-24, ПК-25, ПК-30.

Задание

Получить перечень установленных программ на исследуемой ОС.

Содержание отчета

Форма отчета должна соответствовать требованиям к оформлению простого реферата. Титульный лист должен включать на «звание дисциплины, название лабораторной работы, фамилию и инициалы сдающего, номер группы, фамилию и инициалы принимающего преподавателя. Основная часть работы должна содержать:

− описание проведенной работы;

− выводы о проделанной работе.

Контрольные вопросы

1. Дайте описание способов совершения компьютерного преступления, предмет посягательства;
2. Какова личность вероятного компьютерного преступника ивероятные его мотивы?
3. Какова личность вероятного компьютерного потерпевшего от компьютерных преступлений?
4. Какие бывают механизмы образования компьютерных следов?
5. Какими бывают обстановка и другие типичные обстоятельства при совершении компьютерных преступлений

3. ИССЛЕДОВАНИЕ ИСТОРИИ РАБОТЫ ШТАТНОГО И НЕШТАТНОГО ПО

Цель – исследовать историю запуска штатного ПО, а также историю запуска нештатного и специального ПО.

Формируемые компетенции: ПК-4, ПК-9, ПК-24, ПК-25, ПК-30

Задание

Получить перечень запускаемых программ на ПК с помощью программы Executed Programs List. Выполнить лабораторную работу в соответствии с полученным заданием и примером выполнения работы

Содержание отчета

Форма отчета должна соответствовать требованиям к оформлению простого реферата. Титульный лист должен включать на «звание дисциплины, название лабораторной работы, фамилию и инициалы сдающего, номер группы, фамилию и инициалы принимающего преподавателя. Основная часть работы должна содержать:

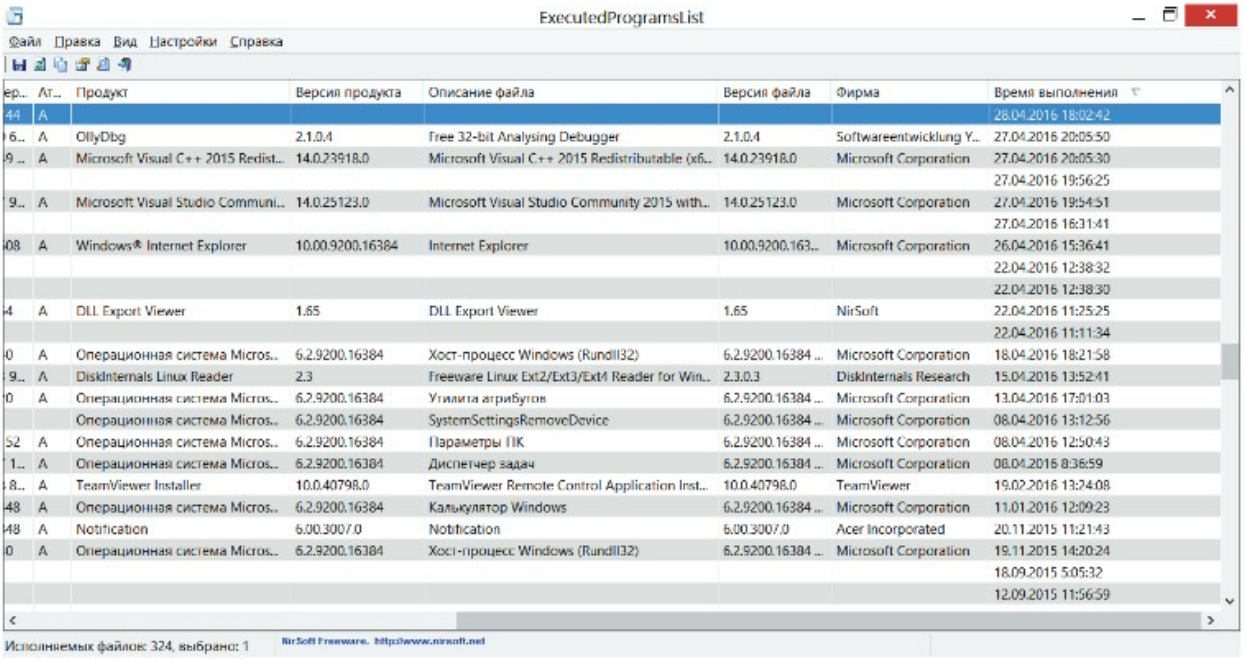
− описание проведенной работы;

− выводы о проделанной работе.

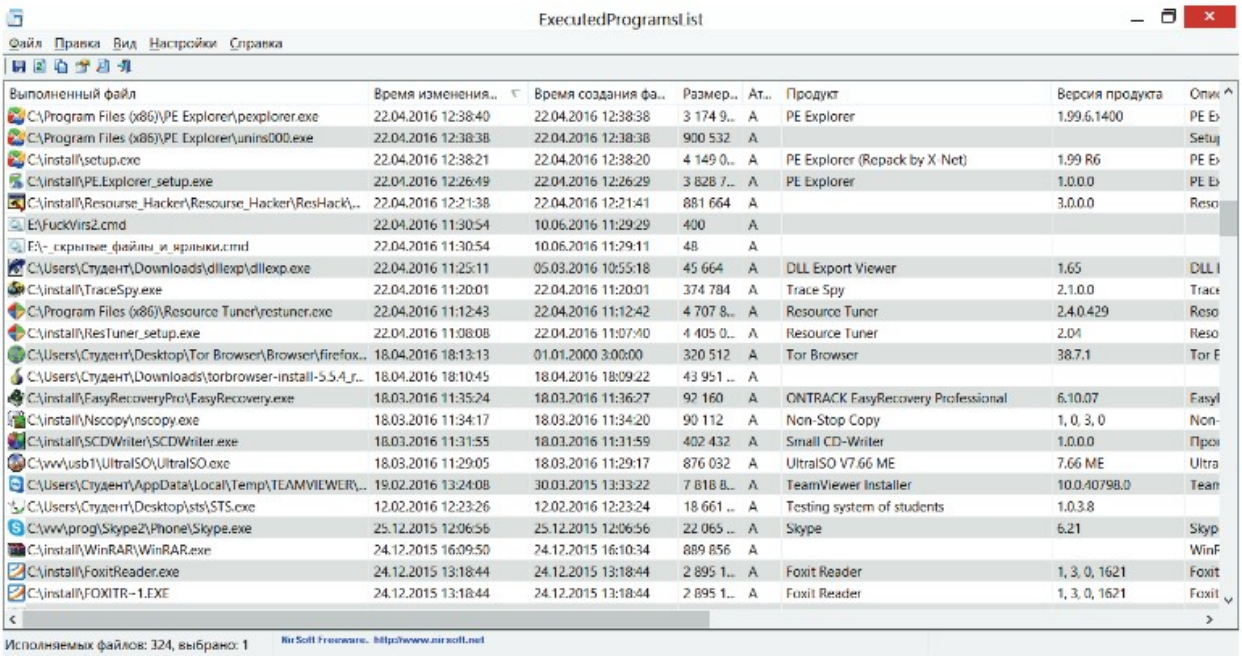
Пример выполнения работы

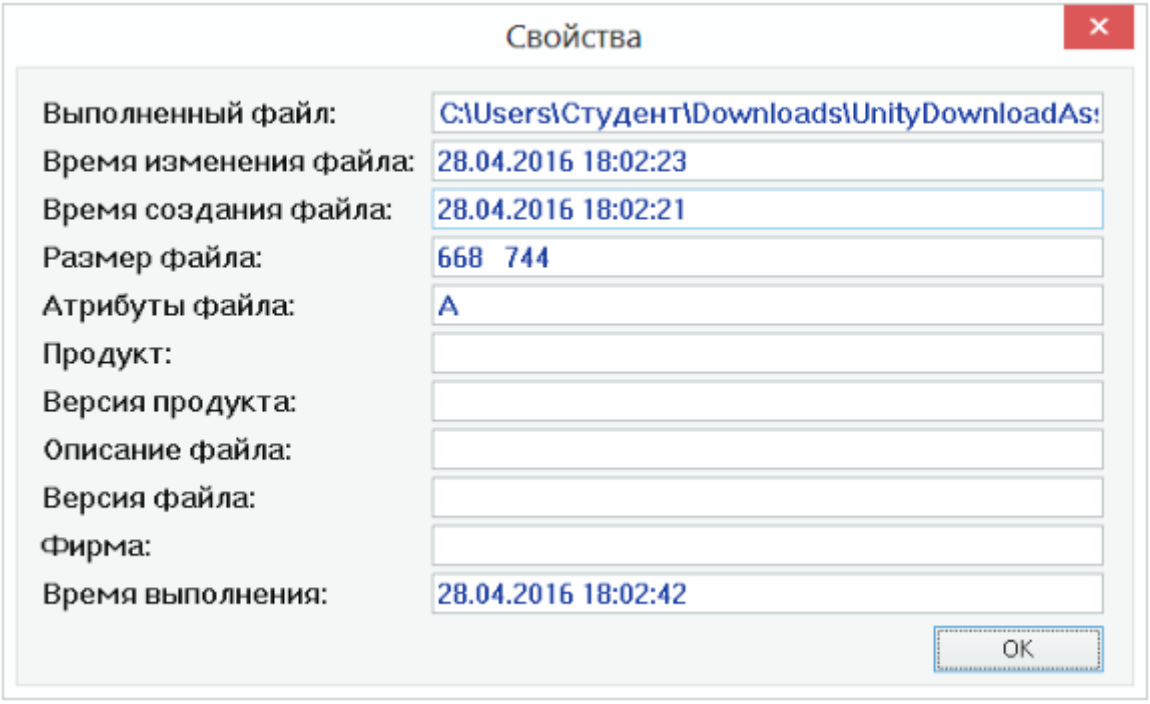
Перечень запущенных программ на ПК

Наименование программы	Описание, цель	Размер программы	Дата последнего запуска
C:\Program Files (x86)\Microsoft Office\Office15\WINWORD.EXE	Microsoft Word	1 922 720	23.12.2015 4:49:45
C:\Program Files (x86)\Google\ Chrome\Application\chrome.exe	Google Chrome	741 704	23.12.2015 4:47:41
C:\Program Files (x86)\Steam\Steam. exe	Steam Client Bootstrapper	3 013 712	23.12.2015 4:35:13
C:\Program Files\WinRAR\WinRAR. exe	WinRAR archiver	1 481 816	22.12.2015 19:37:54
C:\Program Files\Windows NT\ Accessories\WORDPAD.EXE	Текстовый редактор Wordpad Windows	4 517 888	22.12.2015 1:12:25
C:\Program Files (x86)\Photoshop CS6\Photoshop.exe	Adobe Photoshop CS6	43 005 320	21.12.2015 23:22:50
C:\WINDOWS\Explorer.exe	Проводник	4 502 864	08.12.2015 10:11:46
C:\PROGRAM FILES\ (X86)\Steam\STEAMAPPS\common\ Viridi\Viridi.exe		16 180 224	23.12.2015 4:35:40
C:\Windows\SysWOW64\notepad.exe	Блокнот	232 448	22.12.2015 19:33:15
C:\PROGRAM FILES\WINDOWS DEFENDER\MSASCui.exe	Windows Defender User Interface	1 332 224	22.12.2015 5:19:40
C:\Windows\splwow64.exe	Print driver host for applications	128 000	22.12.2015 2:30:02
C:\Windows\SYSTEMAPPS\ MICROSOFT.MICROSOFTEDGE_ 8WEKYB3D8BBWE\ MICROSOFTEDGE.EXE	Microsoft Edge	7 319 408	21.12.2015 16:54:17



ер..	Ат..	Продукт	Версия продукта	Описание файла	Версия файла	Фирма	Время выполнения
44	A						28.04.2016 18:02:42
6..	A	OllyDbg	2.1.0.4	Free 32-bit Analysing Debugger	2.1.0.4	Softwareentwicklung Y..	27.04.2016 20:05:50
9 ..	A	Microsoft Visual C++ 2015 Redist..	14.0.23918.0	Microsoft Visual C++ 2015 Redistributable (x6..	14.0.23918.0	Microsoft Corporation	27.04.2016 20:05:30
							27.04.2016 19:56:25
9..	A	Microsoft Visual Studio Communi..	14.0.25123.0	Microsoft Visual Studio Community 2015 with..	14.0.25123.0	Microsoft Corporation	27.04.2016 19:54:51
							27.04.2016 16:31:41
08	A	Windows® Internet Explorer	10.00.9200.16384	Internet Explorer	10.00.9200.163..	Microsoft Corporation	26.04.2016 15:36:41
							22.04.2016 12:38:32
							22.04.2016 12:38:30
4	A	DLL Export Viewer	1.65	DLL Export Viewer	1.65	NirSoft	22.04.2016 11:25:25
							22.04.2016 11:11:34
0	A	Операционная система Micros..	6.2.9200.16384	Хост-процесс Windows (Rundll32)	6.2.9200.16384 ...	Microsoft Corporation	18.04.2016 18:21:58
9..	A	DiskInternals Linux Reader	2.3	Freeware Linux Ext2/Ext3/Ext4 Reader for Win..	2.3.0.3	DiskInternals Research	15.04.2016 13:52:41
0	A	Операционная система Micros..	6.2.9200.16384	Утилита атрибутов	6.2.9200.16384 ...	Microsoft Corporation	13.04.2016 17:01:03
		Операционная система Micros..	6.2.9200.16384	SystemSettingsRemoveDevice	6.2.9200.16384 ...	Microsoft Corporation	08.04.2016 13:12:56
S2	A	Операционная система Micros..	6.2.9200.16384	Параметры ПК	6.2.9200.16384 ...	Microsoft Corporation	08.04.2016 12:50:43
1..	A	Операционная система Micros..	6.2.9200.16384	Диспетчер задач	6.2.9200.16384 ...	Microsoft Corporation	08.04.2016 8:36:59
8..	A	TeamViewer Installer	10.0.40798.0	TeamViewer Remote Control Application Inst..	10.0.40798.0	TeamViewer	19.02.2016 13:24:08
48	A	Операционная система Micros..	6.2.9200.16384	Калькулятор Windows	6.2.9200.16384 ...	Microsoft Corporation	11.01.2016 12:09:23
48	A	Notification	6.00.3007.0	Notification	6.00.3007.0	Acer Incorporated	20.11.2015 11:21:43
0	A	Операционная система Micros..	6.2.9200.16384	Хост-процесс Windows (Rundll32)	6.2.9200.16384 ...	Microsoft Corporation	19.11.2015 14:20:24
							18.09.2015 5:05:32
							12.09.2015 11:56:59


ExecutedProgramsList
Файл Правка Вид Настройки Справка
Выполненный файл | Время изменения.. | Время создания фа.. | Размер.. | Ат.. | Продукт | Версия продукта | Опис
C:\Program Files (x86)\PE Explorer\pexplorer.exe | 22.04.2016 12:38:40 | 22.04.2016 12:38:38 | 3 174 9.. | A | PE Explorer | 1.99.6.1400 | PE Ex
C:\Program Files (x86)\PE Explorer\unins000.exe | 22.04.2016 12:38:38 | 22.04.2016 12:38:38 | 900 532 | A | | | Setup
C:\install\setup.exe | 22.04.2016 12:38:21 | 22.04.2016 12:38:20 | 4 149 0.. | A | PE Explorer (Repack by X-Net) | 1.99 R6 | PE Ex
C:\install\PE.Explorer_setup.exe | 22.04.2016 12:26:49 | 22.04.2016 12:26:29 | 3 828 7.. | A | PE Explorer | 1.0.0.0 | PE Ex
C:\install\Resourse_Hacker\Resourse_Hacker\ResHack\... | 22.04.2016 12:21:38 | 22.04.2016 12:21:41 | 881 664 | A | | 3.0.0.0 | Reso
E:\FuckVirs2.cmd | 22.04.2016 11:30:54 | 10.06.2016 11:29:29 | 400 | A | | | |
F:\- скрытые файлы и ярлыки.cmd | 22.04.2016 11:30:54 | 10.06.2016 11:29:11 | 48 | A | | | |
C:\Users\Студент\Downloads\dllexp\dllexp.exe | 22.04.2016 11:25:11 | 05.03.2016 10:55:18 | 45 664 | A | DLL Export Viewer | 1.65 | DLL E
C:\install\TraceSpy.exe | 22.04.2016 11:20:01 | 22.04.2016 11:20:01 | 374 784 | A | Trace Spy | 2.1.0.0 | Trace
C:\Program Files (x86)\Resource Tuner\restuner.exe | 22.04.2016 11:12:43 | 22.04.2016 11:12:42 | 4 707 8.. | A | Resource Tuner | 2.4.0.429 | Reso
C:\install\ResTuner_setup.exe | 22.04.2016 11:08:08 | 22.04.2016 11:07:40 | 4 405 0.. | A | Resource Tuner | 2.04 | Reso
C:\Users\Студент\Desktop\Tor Browser\Browser\firefox... | 18.04.2016 18:13:13 | 01.01.2000 3:00:00 | 320 512 | A | Tor Browser | 38.7.1 | Tor B
C:\Users\Студент\Downloads\torbrowser-install-5.5.4_r... | 18.04.2016 18:10:45 | 18.04.2016 18:09:22 | 43 951 .. | A | | | |
C:\install\EasyRecoveryPro\EasyRecovery.exe | 18.03.2016 11:35:24 | 18.03.2016 11:36:27 | 92 160 | A | ONTRACK EasyRecovery Professional | 6.10.07 | Easy
C:\install\Nscopy\nscopy.exe | 18.03.2016 11:34:17 | 18.03.2016 11:34:20 | 90 112 | A | Non-Stop Copy | 1, 0, 3, 0 | Non-
C:\install\SCDWriter\SCDWriter.exe | 18.03.2016 11:31:55 | 18.03.2016 11:31:59 | 402 432 | A | Small CD-Writer | 1.0.0.0 | Прог
C:\vw\usb1\UltraISO\UltraISO.exe | 18.03.2016 11:29:05 | 18.03.2016 11:29:17 | 876 032 | A | UltraISO V7.66 ME | 7.66 ME | Ultra
C:\Users\Студент\AppData\Local\Temp\TEAMVIEWER\... | 19.02.2016 13:24:08 | 30.03.2015 13:33:22 | 7 818 8.. | A | TeamViewer Installer | 10.0.40798.0 | Team
C:\Users\Студент\Desktop\sts\STS.exe | 12.02.2016 12:23:26 | 12.02.2016 12:23:24 | 18 661 .. | A | Testing system of students | 1.0.3.8 |
C:\vw\prog\Skype2\Phone\Skype.exe | 25.12.2015 12:06:56 | 25.12.2015 12:06:56 | 22 065 .. | A | Skype | 6.21 | Skyp
C:\install\WinRAR\WinRAR.exe | 24.12.2015 16:09:50 | 24.12.2015 16:10:34 | 889 856 | A | | | WinR
C:\install\FoxitReader.exe | 24.12.2015 13:18:44 | 24.12.2015 13:18:44 | 2 895 1.. | A | Foxit Reader | 1, 3, 0, 1621 | Foxit
C:\install\FOXITR~1.EXE | 24.12.2015 13:18:44 | 24.12.2015 13:18:44 | 2 895 1.. | A | Foxit Reader | 1, 3, 0, 1621 | Foxit
Исполняемых файлов: 324, выбрано: 1
NirSoft Freeware. http://www.nirsoft.net


Свойства
Выполненный файл: C:\Users\Студент\Downloads\UnityDownloadAs
Время изменения файла: 28.04.2016 18:02:23
Время создания файла: 28.04.2016 18:02:21
Размер файла: 668 744
Атрибуты файла: A
Продукт:
Версия продукта:
Описание файла:
Версия файла:
Фирма:
Время выполнения: 28.04.2016 18:02:42
OK

4. ИССЛЕДОВАНИЕ ЖУРНАЛОВ СОБЫТИЙ В ОС

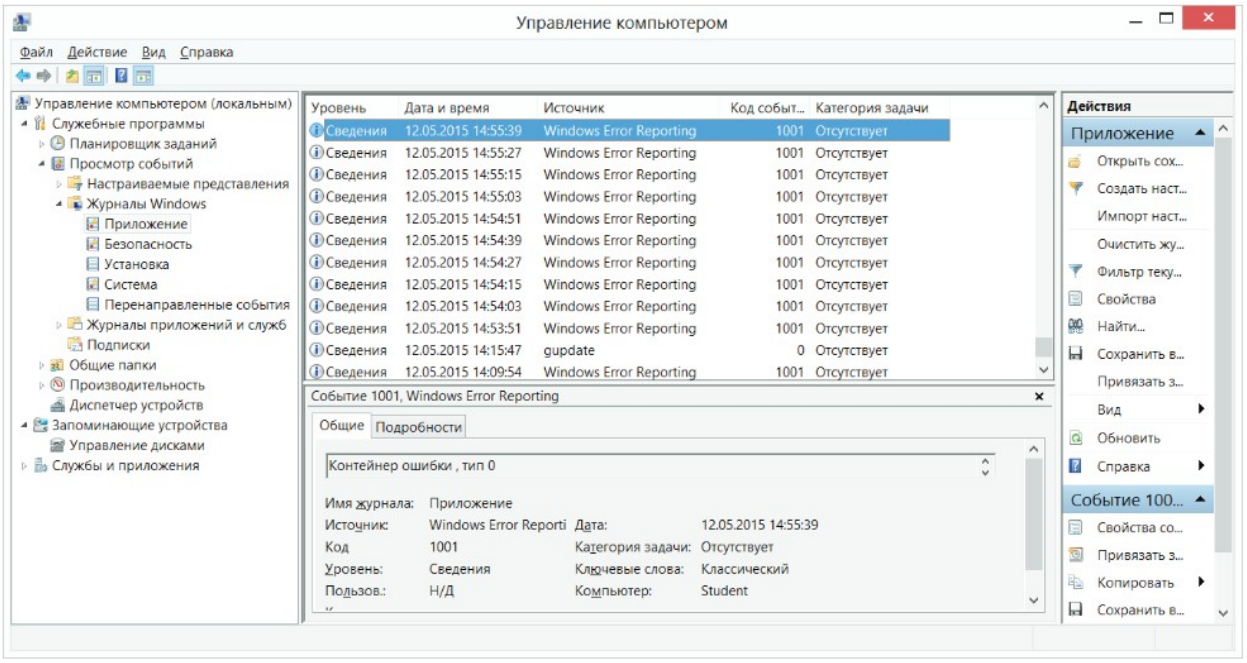
Цель – изучить следующие журналы в ОС: системный журнал событий и журнал приложений.

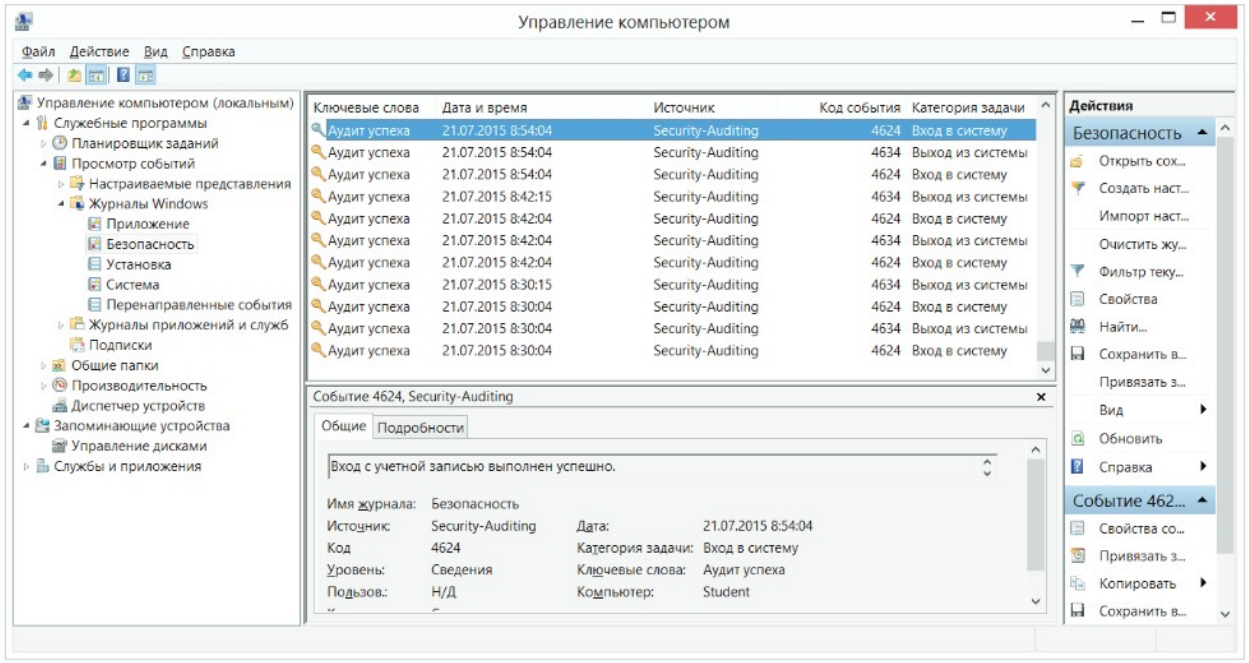
Формируемые компетенции: ПК-4, ПК-9, ПК-24, ПК-25, ПК-30

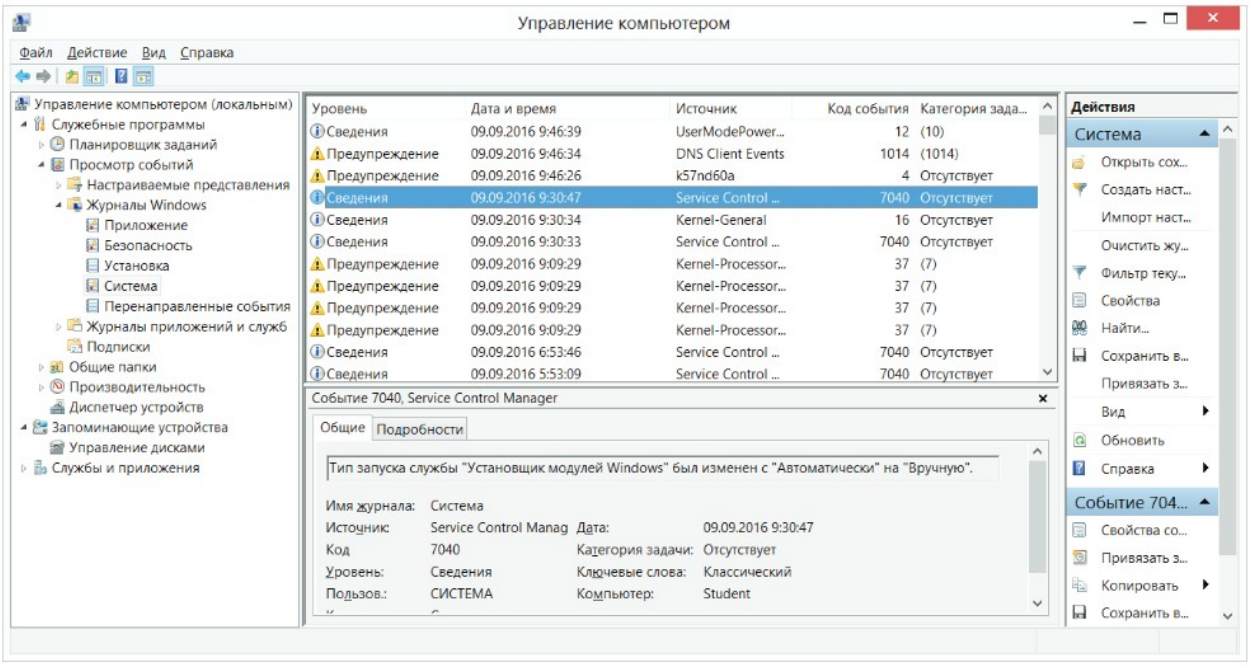
Пример выполнения работы

Журнал событий «Приложения»

Код	Дата	Сведения
16384	23.12.2015 5:11:41	Перезапуск службы защиты программного обеспечения успешно запланирован на 2015-12-23T03:35:41Z.
903	23.12.2015 5:11:41	Служба защиты программного обеспечения остановлена.
1003	23.12.2015 5:09:57	Служба защиты программного обеспечения завершила проверку состояния лицензирования.
900	23.12.2015 4:50:07	Выполняется запуск службы защиты программного обеспечения.
8233	23.12.2015 2:36:03	Обработчик правил сообщил о сбое попытки активации корпоративной лицензии.
8224	22.12.2015 7:20:51	Служба VSS выключается из-за тайм-аута простоя.
1066	21.12.2015 17:36:31	Состояние инициализации объектов службы.
5973	19.12.2015 19:56:40	Сбой активации приложения Microsoft.Windows.Cortana_cw5n1h2txyewy!CortanaUI. Ошибка: Сбой при удаленном вызове процедуры..
326	19.12.2015 5:58:49	svchost (1048) DS_Token_DB: Ядро СУБД присоединило базу данных (1, C:\WINDOWS\system32\config\systemprofile\AppData\Local\DataSharing\Storage\DSTokenDB2.dat). (Время=0 с) Последовательность внутренней синхронизации: [1] 0.000, [2] 0.015, [3] 0.000, [4] 0.000, [5] 0.000, [6] 0.500, [7] 0.235, [8] 0.125, [9] 0.000, [10] 0.000, [11] 0.000, [12] 0.000. Сохраненный кэш: 1 0


Управление компьютером
Файл Действие Вид Справка
Управление компьютером (локальным)
Служебные программы
Планировщик заданий
Просмотр событий
Настраиваемые представления
Журналы Windows
Приложение
Безопасность
Установка
Система
Перенаправленные события
Журналы приложений и служб
Подписки
Общие папки
Производительность
Диспетчер устройств
Запоминающие устройства
Управление дисками
Службы и приложения
Уровень Дата и время Источник Код событ... Категория задачи
Сведения 12.05.2015 14:55:39 Windows Error Reporting 1001 Отсутствует
Сведения 12.05.2015 14:55:27 Windows Error Reporting 1001 Отсутствует
Сведения 12.05.2015 14:55:15 Windows Error Reporting 1001 Отсутствует
Сведения 12.05.2015 14:55:03 Windows Error Reporting 1001 Отсутствует
Сведения 12.05.2015 14:54:51 Windows Error Reporting 1001 Отсутствует
Сведения 12.05.2015 14:54:39 Windows Error Reporting 1001 Отсутствует
Сведения 12.05.2015 14:54:27 Windows Error Reporting 1001 Отсутствует
Сведения 12.05.2015 14:54:15 Windows Error Reporting 1001 Отсутствует
Сведения 12.05.2015 14:54:03 Windows Error Reporting 1001 Отсутствует
Сведения 12.05.2015 14:53:51 Windows Error Reporting 1001 Отсутствует
Сведения 12.05.2015 14:15:47 gupdate 0 Отсутствует
Сведения 12.05.2015 14:09:54 Windows Error Reporting 1001 Отсутствует
Событие 1001, Windows Error Reporting
Общие Подробности
Контейнер ошибки , тип 0
Имя журнала: Приложение
Источник: Windows Error Reporti
Дата: 12.05.2015 14:55:39
Код 1001
Категория задачи: Отсутствует
Уровень: Сведения
Ключевые слова: Классический
Пользов.: Н/Д
Компьютер: Student
Действия
Приложение
Открыть сох...
Создать наст...
Импорт наст...
Очистить жу...
Фильтр теку...
Свойства
Найти...
Сохранить в...
Привязать з...
Вид
Обновить
Справка
Событие 100...
Свойства со...
Привязать з...
Копировать
Сохранить в...





«Задание

Получить содержимое следующих файлов журналов ОС:

1) системный журнал событий;

2) журнал событий безопасности;

3) журнал приложений.

Содержание отчета

Форма отчета должна соответствовать требованиям к оформлению простого реферата. Титульный лист должен включать на «звание дисциплины, название лабораторной работы,

фамилию и инициалы сдающего, номер группы, фамилию и инициалы принимающего преподавателя. Основная часть работы должна содержать:

− описание проведенной работы;

− выводы о проделанной работе.

Контрольные вопросы

1. Какая информация отображается в следующих журналах ОС:

– системный журнал событий;

– журнал событий безопасности;

– журнал приложений.

5 ИССЛЕДОВАНИЕ ЖУРНАЛОВСОБЫТИЙ БЕЗОПАСНОСТИ

Цель – изучить и проанализировать журнал событий безопасности.

Формируемые компетенции: ПК-4, ПК-9, ПК-24, ПК-25, ПК-30.

Пример выполнения работы

Журнал событий «Безопасность»

Код	Дата	Сведения
4797	24.12.2015 1:55:32	Попытка запроса существования пустого пароля для учетной записи
4624	23.12.2015 22:09:13	Вход в учетную запись выполнен успешно
4798	23.12.2015 10:42:53	Перечислено участие пользователя в локальных группах
4672	22.12.2015 18:37:44	Новому сеансу входа назначены специальные привилегии
5058	15.12.2015 21:22:53	Операция с файлом ключей
5061	15.12.2015 21:22:53	Операция шифрования
6281	15.12.2015 10:13:39	Средство проверки целостности кода обнаружило, что хэш-данные страниц файла образа недопустимы. Возможно, файл неправильно подписан без использования хэш-данных страниц либо поврежден из-за несанкционированного изменения. Недопустимые хэш-данные могут указывать на возможную ошибку дискового устройства
4905	15.12.2015 9:55:09	Произведена попытка отмены регистрации источника событий безопасности
4799	19.12.2015 5:58:49	Перечислено участие в защищенных локальных группах

Журнал событий «Система»

Код	Дата	Сведения
19	10.12.2015 18:29:04	Установка завершена: следующее обновление было успешно установлено: Get Office
6006	10.12.2015 3:57:06	Служба журнала событий остановлена
98	10.12.2015 3:57:30	Том \\?\Volume{b3ddb939-db00-4147-a752-1c46579402b5} (\Device\HarddiskVolume1) работоспособен. Не требуется никаких действий
10114	10.12.2015 3:57:29	WUDFPf (часть UMDF) еще не загружена. После ее загрузки Windows снова запустит устройство
44	15.12.2015 21:22:53	Центр обновления Windows начал скачивать обновление
6013	14.12.2015 10:49:18	Время работоспособного состояния 19 сек.
2	12.12.2015 21:20:24	Intel(R) Management Engine Interface driver has started successfully
16	15.12.2015 9:55:09	Журнал доступа в кусте \??\C:\Users\Ermolaeva\AppData\Local\Packages\microsoft.windowscommunicationsapps_8wekyb3d8bbwe\microsoft.windowscommunicationsapps_17.6509.64001.0_x64__8wekyb3d8bbwe\ActivationStore\ActivationStore.dat очищен; обновлено разделов: 0; создано измененных страниц: 0
43	19.12.2015 5:58:49	Установка начата: ОС Windows начала устанавливать следующее обновление: TuneIn Radio

Задание

Привести содержимое журнала событий безопасности в отсортированном виде по датам событий

Содержание отчета

Форма отчета должна соответствовать требованиям к оформлению простого реферата. Титульный лист должен включать на «звание дисциплины, название лабораторной работы, фамилию и инициалы сдающего, номер группы, фамилию и инициалы принимающего преподавателя. Основная часть работы должна содержать:

− описание проведенной работы;

− выводы о проделанной работе.

Контрольные вопросы

1. Какие событие приводятся в журнале безопасности OCWindows?

2. Какие события отражают время доступа к файловой системе?

3. В каких событиях находится описание доступа к настройкам связанным с безопасностью ОС

6 ИССЛЕДОВАНИЕ ИСТОРИИ БРАУЗЕРОВ

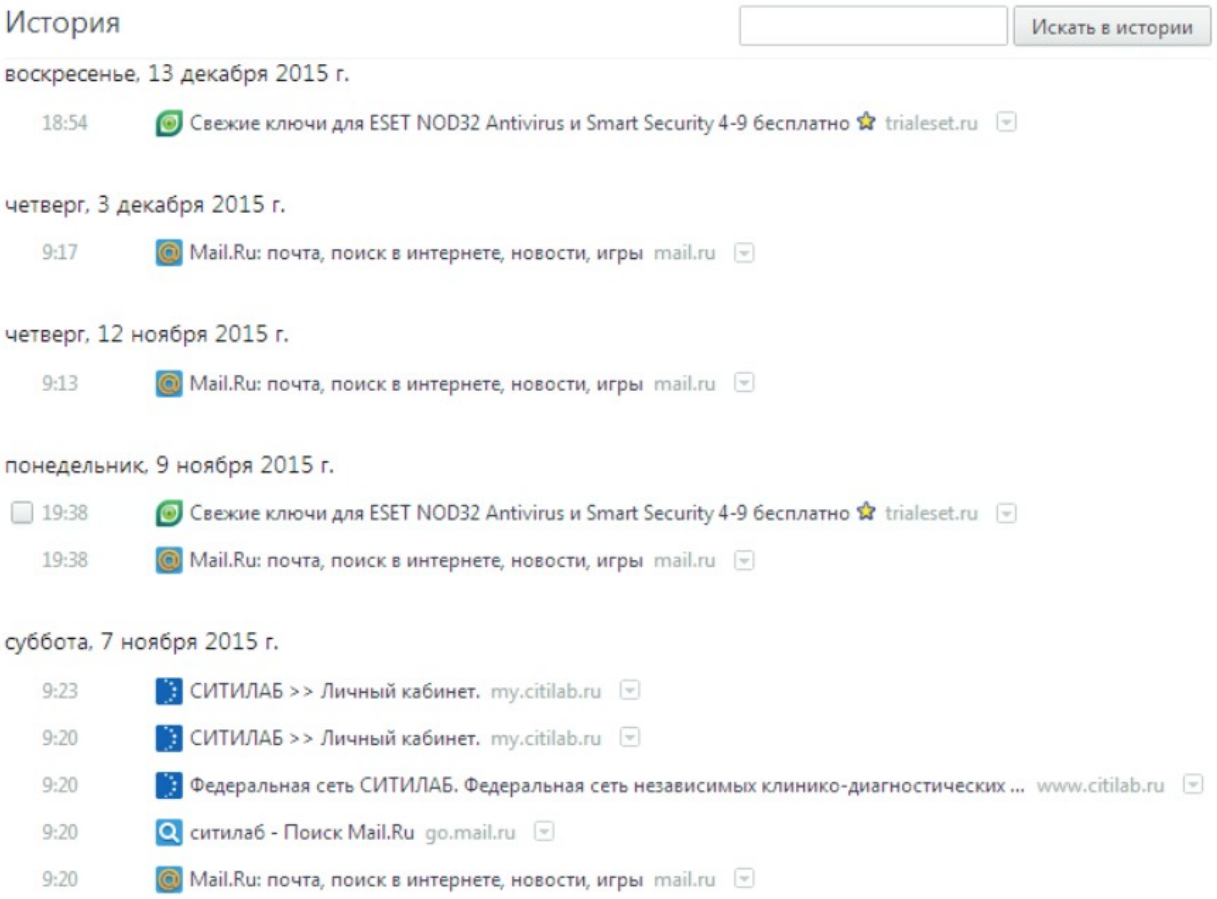
Цель – научиться исследовать журналы посещенных ресурсов в интернет-браузерах.

Формируемые компетенции: ПК-4, ПК-9, ПК-24, ПК-25, ПК-30

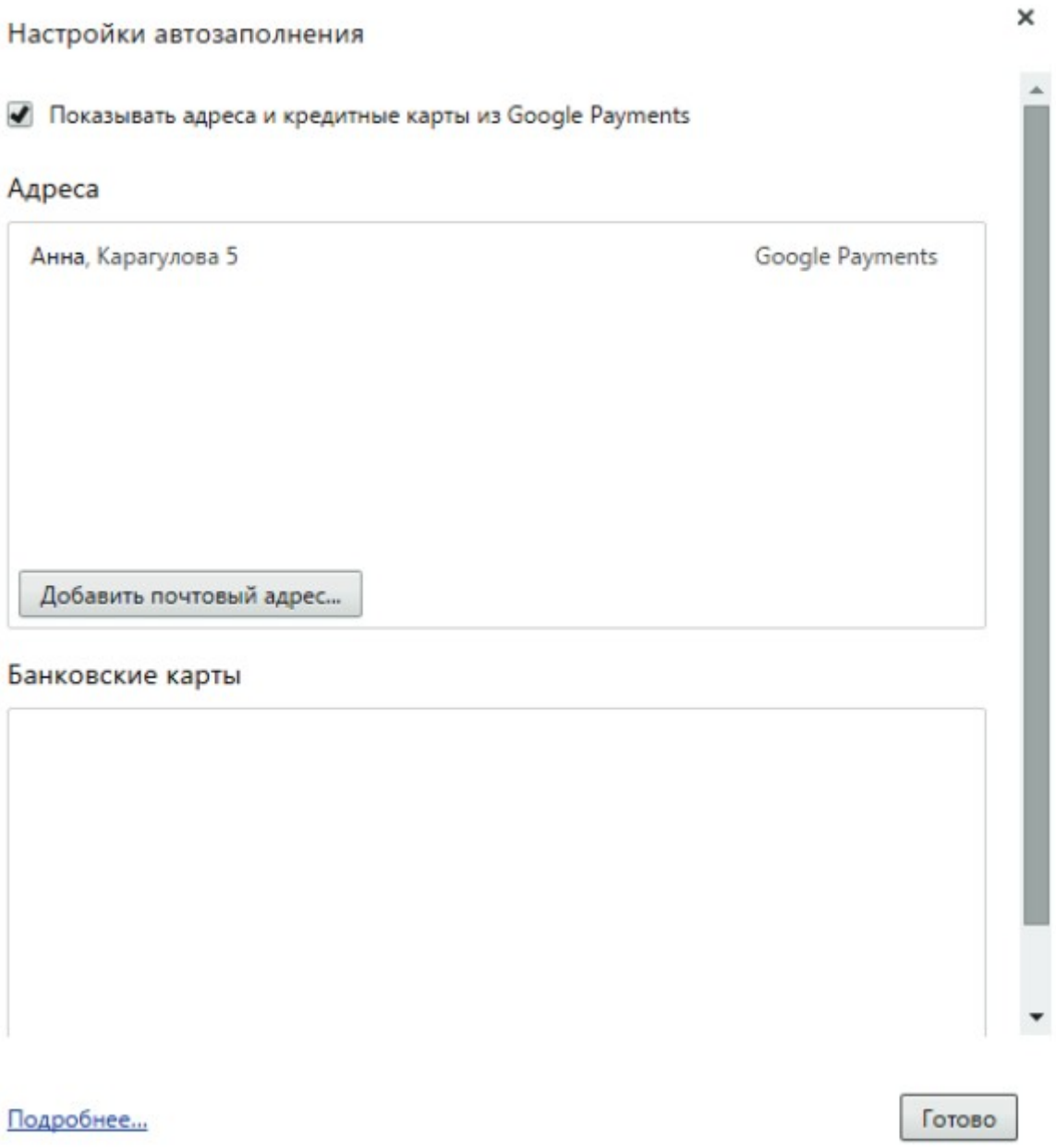
Пример выполнения работы

Просмотр истории в браузере Google Chrome

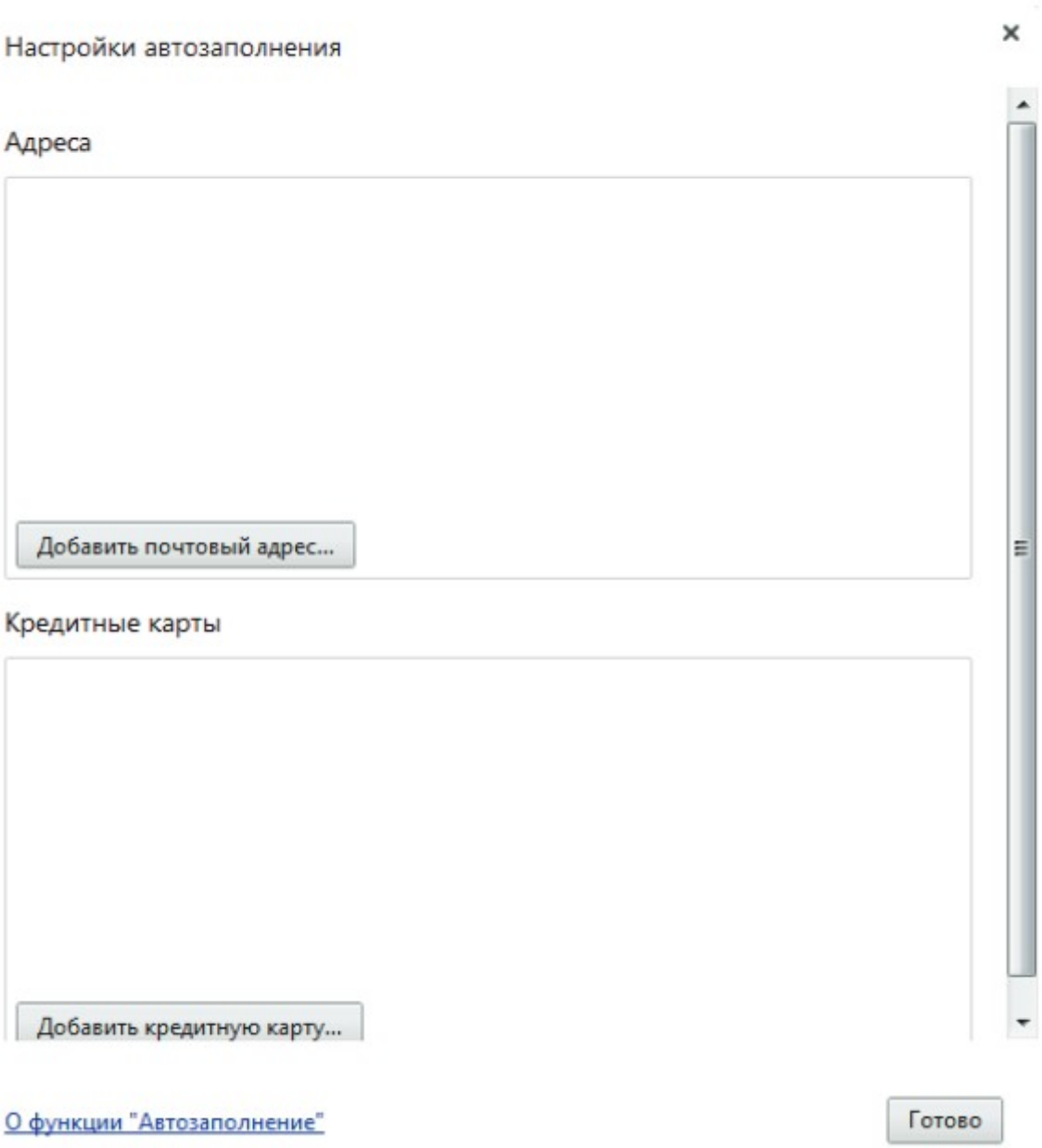
Просмотр история в браузере «Интернет»



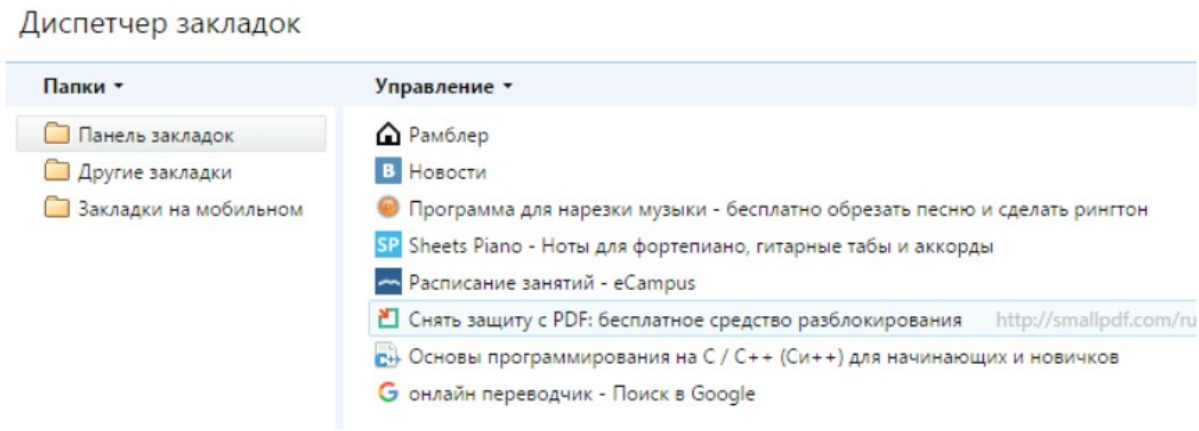
Автозаполнение браузера Google Chrome



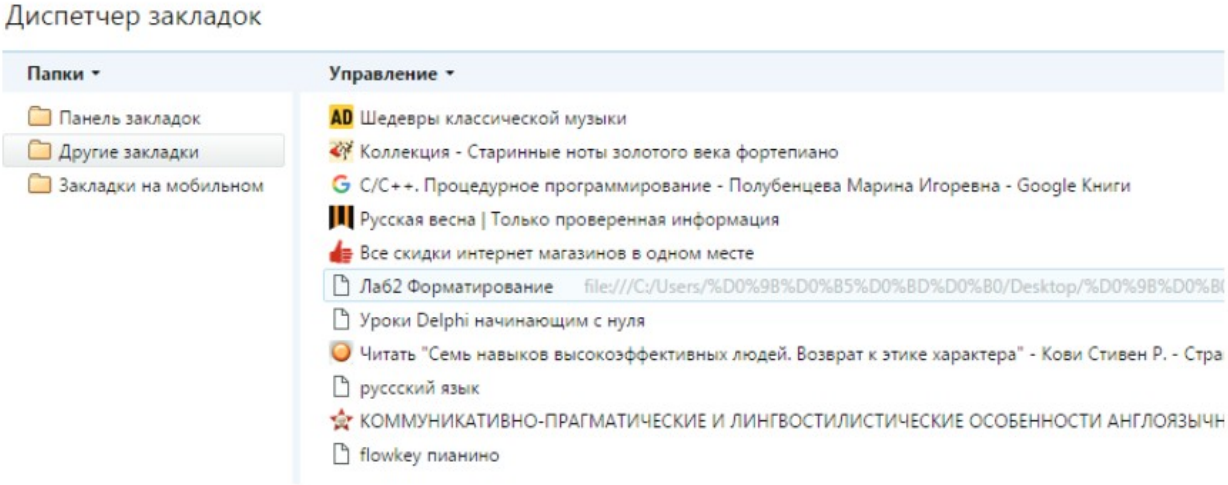
Автозаполнение браузера «Интернет»



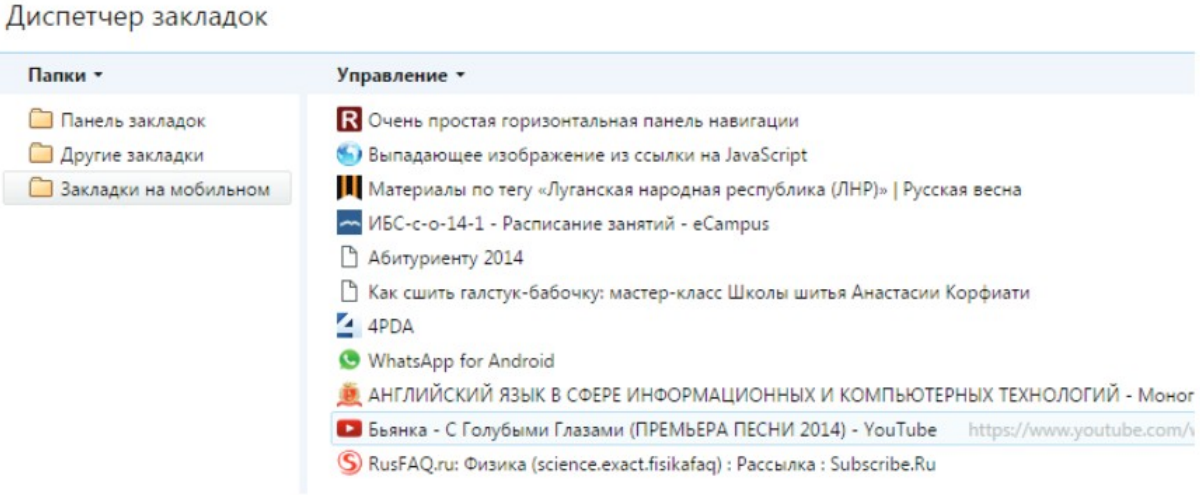
Закладки браузера Google Chrome



Закладки браузера Google Chrome



Закладки браузера Google Chrome



Задание

Произвести анализ посещенных страниц из исследуемых бра-узеров

Содержание отчета

Форма отчета должна соответствовать требованиям к оформлению простого реферата. Титульный лист должен включать на «звание дисциплины, название лабораторной работы, фамилию и инициалы сдающего, номер группы, фамилию и инициалы принимающего преподавателя. Основная часть работы должна содержать:

− описание проведенной работы;

− выводы о проделанной работе.

Контрольные вопросы

1. Где хранится история просмотра веб-страниц.

2. Что хранится в кэше браузера (временные файлы).

3. Что содержится в cookie-файлах.

4. Как установить, когда пользователь просматривал веб-сайт.

5. Где хранятся посещенные страницы и загрузки.

6. Где хранятся поисковые запросы и данные форм.

7. Где хранятся настройках для посещаемых сайтов.

8. Где хранятся Информация об авторизации на сайтах.

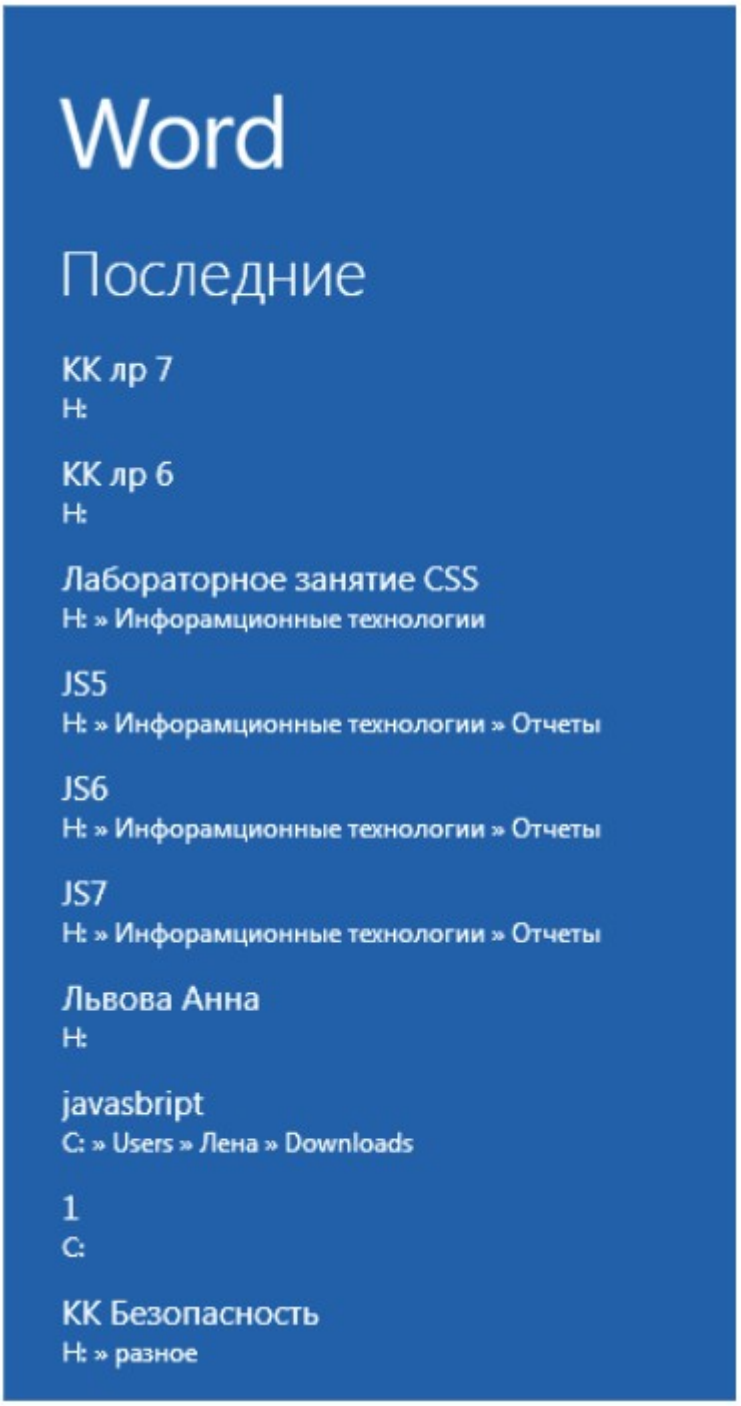
9. Где хранятся кэшированные данные посещенных страниц (картинки, скрипты и прочее)

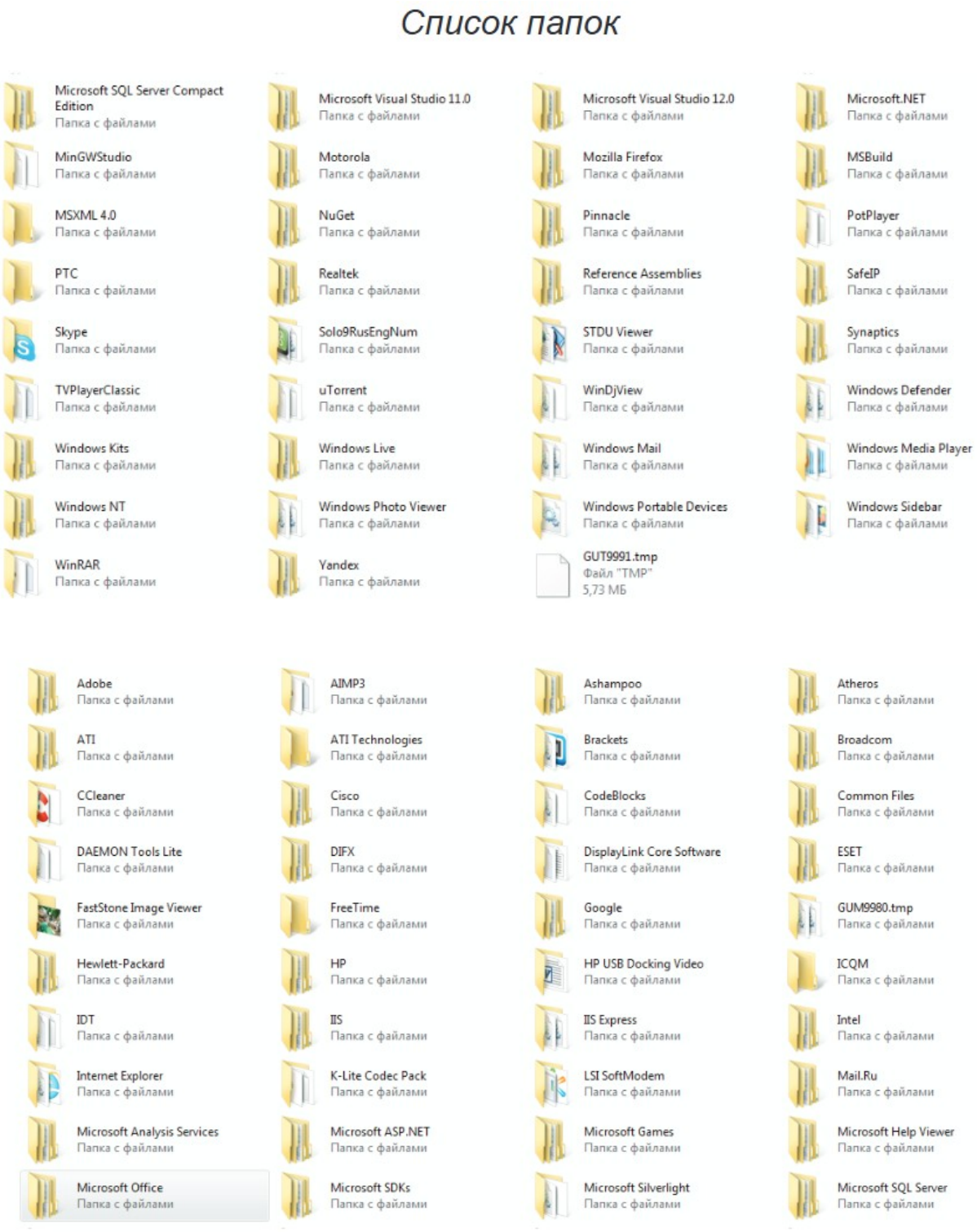
7. ИССЛЕДОВАНИЕ ИСТОРИИ ТЕКСТОВОГО РЕДАКТОРА MS WORD

Цель – исследовать получение истории текстового редактора MS Word.

Формируемые компетенции: ПК-4, ПК-9, ПК-24, ПК-25, ПК-30

Пример выполнения работы


Word
Последние
КК лр 7
H:
КК лр 6
H:
Лабораторное занятие CSS
H: » Инфорамционные технологии
JS5
H: » Инфорамционные технологии » Отчеты
JS6
H: » Инфорамционные технологии » Отчеты
JS7
H: » Инфорамционные технологии » Отчеты
Львова Анна
H:
javasbript
C: » Users » Лена » Downloads
1
C:
КК Безопасность
H: » разное



Задания

1. Получить перечень файлов, в которых хранится история от-крываемых документов.

2. Получить перечень открываемых документов

Содержание отчета

Форма отчета должна соответствовать требованиям к оформлению простого реферата. Титульный лист должен включать на «звание дисциплины, название лабораторной работы, фамилию и инициалы сдающего, номер группы, фамилию и инициалы принимающего преподавателя. Основная часть работы должна содержать:

− описание проведенной работы;

− выводы о проделанной работе.

Контрольные вопросы:

1. Где хранятся история открываемых документов в MS WORD?

8. ИССЛЕДОВАНИЕ СОДЕРЖАНИЯ ФАЙЛОВОЙ СТРУКТУРЫ ПК

Цель – исследовать файловую структуру на примере ПК и провести анализ файлов и директорий.

Формируемые компетенции: ПК-4, ПК-9, ПК-24, ПК-25, ПК-30

Пример выполнения работы

C:\1.txt

C:\calc.exe

C:\inetpub

C:\Intel

C:\masm32

C:\NuGet.exe

C:\NVIDIA

C:\ PDOXUSRS.NET

C:\PerfLogs

C:\Program Files

C:\Program Files (x86)

C:\Python31

C:\SolomonData.dat

C:\SolomonLog.dat

C:ISSA

C:\Stonesoft

C:\Transaq

C:\Users

C:\VirtualBox

C:\VkNet.1.0.0.nupkg

C:\WebServers

C:\Windows

C:\SINPLACE.~TR\Data

C:\SINPLACE.~TR\Machine

C:\SINPLACE.~TR\Data\DATA

C:\SINPLACE.~TR\Data\DATA\Windows

C:\WebServers

C:\Windows

C:\$INPLACE.~TR\Data

C:\$INPLACE.~TR\Machine

C:\$INPLACE.~TR\Data\DATA

C:\$INPLACE.~TR\Data\DATA\Windows

C:\$INPLACE.~TR\Data\DATA\Windows\Media

C:\$INPLACE.~TR\Data\DATA\Windows\System32

C:\$INPLACE.~TR\Data\DATA\Windows\Media\chimes.wav

C:\$INPLACE.~TR\Data\DATA\Windows\Media\chord.wav

C:\$INPLACE.~TR\Data\DATA\Windows\Media\ding.wav

C:\$INPLACE.~TR\Data\DATA\Windows\Media\flourish.mid

C:\$INPLACE.~TR\Data\DATA\Windows\Media\notify.wav

C:\$INPLACE.~TR\Data\DATA\Windows\Media\onestop.mid

C:\$INPLACE.~TR\Data\DATA\Windows\Media\recycle.wav

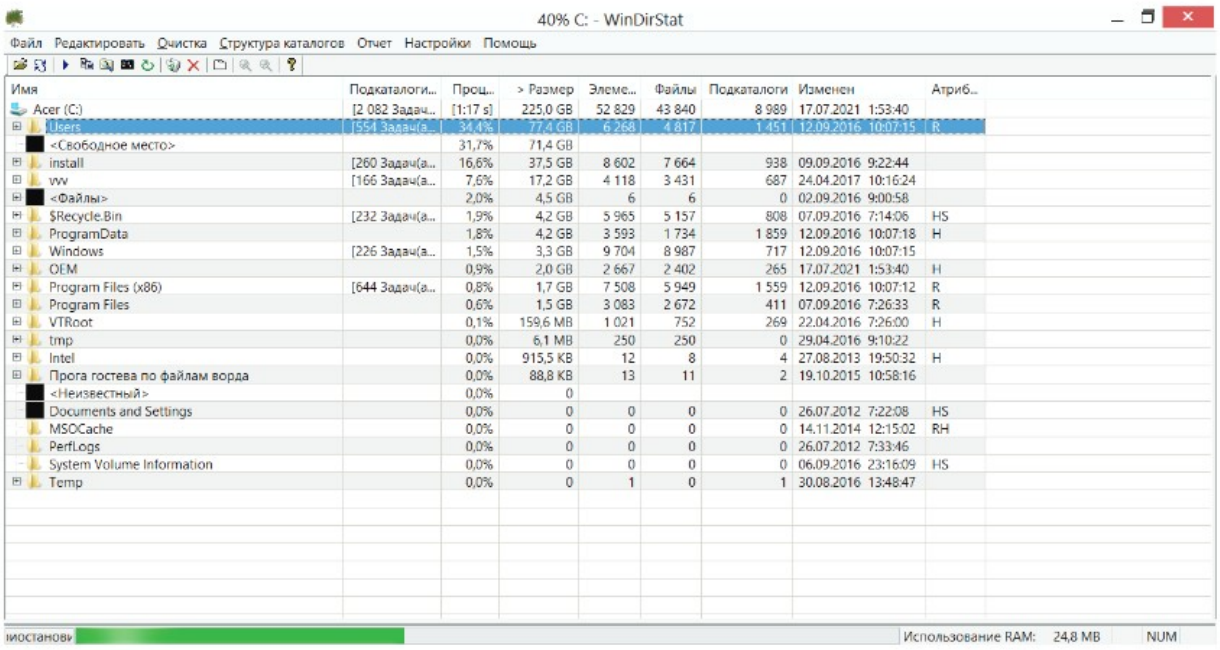
C:\$INPLACE.~TR\Data\DATA\Windows\Media\ringout.wav

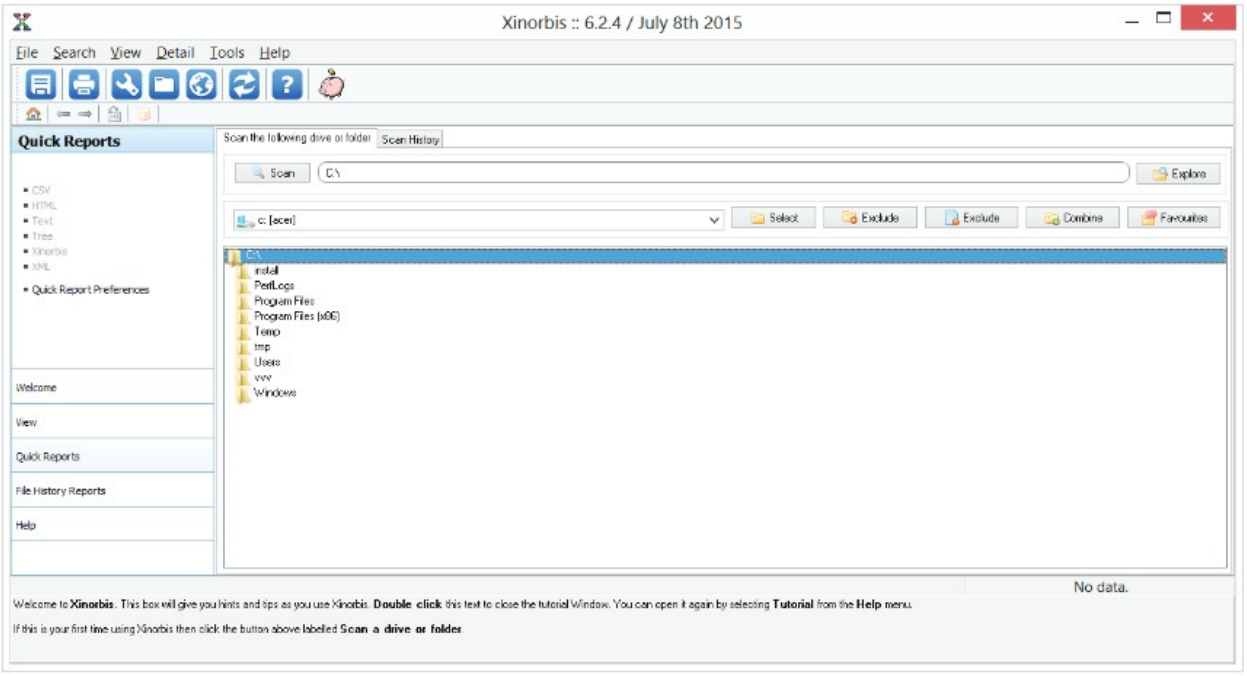
C:\$INPLACE.~TR\Data\DATA\Windows\Media\tada.wav

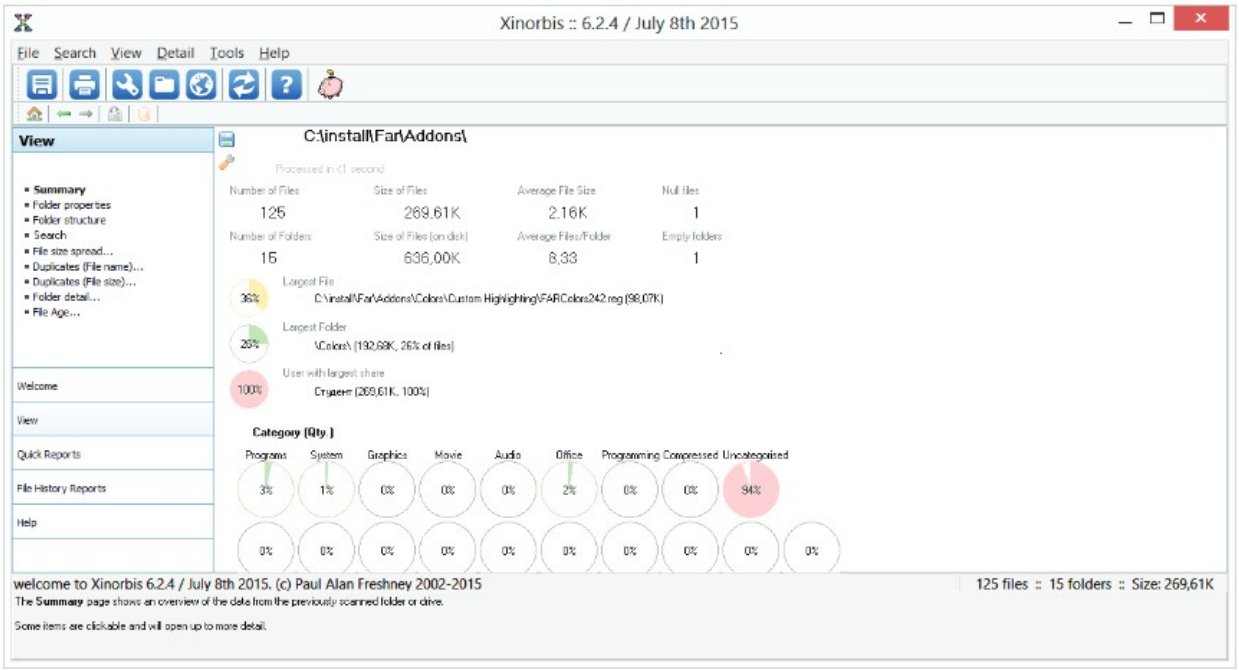
C:\$INPLACE.~TR\Data\DATA\Windows\Media\town.mid

C:\$INPLACE.~TR\Data\DATA\Windows\Media\Windows Balloon.wav

C:\$INPLACE.~TR\Data\DATA\Windows\Media\Windows Battery Critical.wav


40% C: - WinDirStat
Файл Редактировать Очистка Структура каталогов Отчет Настройки Помощь
Имя Подкаталоги... Проц... > Размер Элеме... Файлы Подкаталоги Изменен Атриб...
Acer (C:) [2 082 Задач... [1:17 s] 225,0 GB 52 829 43 840 8 989 17.07.2021 1:53:40
Users [554 Задач(а... 34,4% 77,4 GB 6 268 4 817 1 451 12.09.2016 10:07:15 R
<Свободное место> 31,7% 71,4 GB
install [260 Задач(а... 16,6% 37,5 GB 8 602 7 664 938 09.09.2016 9:22:44
vvv [166 Задач(а... 7,6% 17,2 GB 4 118 3 431 687 24.04.2017 10:16:24
<Файлы> 2,0% 4,5 GB 6 6 0 02.09.2016 9:00:58
$Recycle.Bin [232 Задач(а... 1,9% 4,2 GB 5 965 5 157 808 07.09.2016 7:14:06 HS
ProgramData 1,8% 4,2 GB 3 593 1 734 1 859 12.09.2016 10:07:18 H
Windows [226 Задач(а... 1,5% 3,3 GB 9 704 8 987 717 12.09.2016 10:07:15
OEM 0,9% 2,0 GB 2 667 2 402 265 17.07.2021 1:53:40 H
Program Files (x86) [644 Задач(а... 0,8% 1,7 GB 7 508 5 949 1 559 12.09.2016 10:07:12 R
Program Files 0,6% 1,5 GB 3 083 2 672 411 07.09.2016 7:26:33 R
VTRoot 0,1% 159,6 MB 1 021 752 269 22.04.2016 7:26:00 H
tmp 0,0% 6,1 MB 250 250 0 29.04.2016 9:10:22
Intel 0,0% 915,5 KB 12 8 4 27.08.2013 19:50:32 H
Прога гостева по файлам ворда 0,0% 88,8 KB 13 11 2 19.10.2015 10:58:16
<Неизвестный> 0,0% 0
Documents and Settings 0,0% 0 0 0 0 26.07.2012 7:22:08 HS
MSOCache 0,0% 0 0 0 0 14.11.2014 12:15:02 RH
PerfLogs 0,0% 0 0 0 0 26.07.2012 7:33:46
System Volume Information 0,0% 0 0 0 0 06.09.2016 23:16:09 HS
Temp 0,0% 0 1 0 1 30.08.2016 13:48:47
иостанови
Использование RAM: 24,8 MB
NUM


Xinorbis :: 6.2.4 / July 8th 2015
File Search View Detail Tools Help
Quick Reports
CSV
HTML
Text
Tree
Xinorbis
XML
Quick Report Preferences
Welcome
View
Quick Reports
File History Reports
Help
Scan the following drive or folder
Scan History
Scan
C:\
Explore
c: [acer]
Select
Exclude
Exclude
Combine
Favourites
C:\
install
PerfLogs
Program Files
Program Files (x86)
Temp
tmp
Users
vvv
Windows
No data.
Welcome to Xinorbis. This box will give you hints and tips as you use Xinorbis. Double click this text to close the tutorial Window. You can open it again by selecting Tutorial from the Help menu.
If this is your first time using Xinorbis then click the button above labelled Scan a drive or folder.



Задание

Получить перечень файлов с помощью штатных и нештатных

программ для работы с файловой системой и структурой каталогов.

Содержание отчета

Форма отчета должна соответствовать требованиям к оформлению простого реферата. Титульный лист должен включать название дисциплины, название лабораторной работы, фамилию и инициалы сдающего, номер группы, фамилию и инициалы принимающего преподавателя.

Основная часть работы должна содержать:

- описание проведенной работы;

- выводы о проделанной работе.

Контрольные вопросы

1. Как получить информацию о файловой структуре?

2. Как получить информацию о перечне файлов на ПК?

3. Что отражается в статистике запуска файлов и анализе перечня директорий?

Рекомендуемая литература

1. Вехов В. Б. Компьютерные преступления. Способы совершения и методика расследования. М.: 1996. 182 с.

2. Середа С. А., Федотов Н. Н. Ответственность за распространение вредоносных программ для ЭВМ // Право и экономика. 2007, № 3. С. 50-55.

3. Середа С. А., Федотов Н. Н. Расширительное толкование терминов «вредоносная программа» и «неправомерный доступ» //Закон. 2007, июль. С. 191.

4. Середа С. А., Федотов Н. Н. Сложности толкования терминов «вредоносная программа» и «неправомерный доступ» // Российская юстиция. 2007, № 2. С. 58-62.

5. Федотов Н. Н. Форензика - компьютерная криминалистика.М.: Юридический Мир, 2007. 432 с.