# РАЗРАБОТКА ПРОГРАММНОГО ИНСТРУМЕНТАЛЬНОГО СРЕДСТВА ДЛЯ ПРОИЗВОДСТВА КОМПЬЮТЕРНО – ТЕХНИЧЕСКИХ ЭКСПЕРТИЗ

Студент 2 курса 5 группы Берёзкин А.

Научный руководитель: Ливак Е. Н.

г. Гродно, 2004

# Актуальность проблемы компьютерных преступлений

- Огромный, сложно локализуемый ущерб.
- Тяжёлые экономические последствия.
- Более 44% пользователей Internet в США совершают компьютерные преступления различной степени тяжести – от нелегального распространения сообщений электронной почты (спам) до размещения в сети Internet материалов порнографического содержания.
- Этот показатель намного выше в странах с более низким уровнем жизни.

# Базовые сведения о компьютерно – технической экспертизе

- Выявление роли объекта в преступлении.
- Получение доступа к компьютерной информации на носителях данных с её последующим исследованием.

## Виды экспертизы

- Аппаратно – компьютерная.
- Программно – компьютерная (ПО).
- Информационно – компьютерная(данных).
- Компьютерно – сетевая.

# Существующие инструментальные средства

- EnCase: Коммерческий пакет. Позволяет снимать образ и анализировать данные с жестких дисков и сменных носителей. ($149).

- SafeBack: Коммерческий продукт. Используется для снятия образов жестких дисков компьютерных систем с архитектурой Intel и восстановления этих образов на других жестких дисках.

Недостатки:

- Высокая стоимость.
- Отсутствие универсальности.
- Нацеленность на выполнение узкого круга задач.

# Существующие инструментальные средства

- TASKTASK и Autopsy - свободно распространяемая альтернатива EnCase с открытым кодом.
- CookieViewCookieView. Анализ файлов Cookies. Доступна с Digital-Detective.co.uk.
- NetAnalysisNetAnalysis. Еще одна утилита с Digital-Detective.co.uk. Инструмент для исследования Windows-машин в поисках улик, касающихся Web - активности.

Недостатки:

- Open Source Product(Отсутствуют любые гарантии).
- Отсутствие универсальности.
- Нацеленность на выполнение узкого круга задач.

# Средства(артефакты) Windows, полезные при производстве КТЭ

- Системные директории Cookies, SendTo, Favorites, History и другие.
- Файлы, которые имеют расширение .spl или .shd, содержат множество информации о задаче печати.
- Start Menu ОС Windows и директория Recent.
- Файл NTUSER.DAT (содержит конфигурационную информацию пользователя и расположен в корне структуры каталогов пользователя).

# Цели исследования

- Изучение вопросов, связанных с производством компьютерно – технической экспертизы .
- Изучение основных возможностей системы программирования Visual C++.
- Разработка автоматизированной системы, которая бы позволила осуществить необходимые при производстве компьютерно – технической экспертизы операции.
- Разработка интерфейса, удовлетворяющего заказчика, дополненного всплывающими подсказками и советами.

# Обоснованный выбор среды программирования

## Среда Visual C++ :

- Высокая надёжность.
- Хорошая совместимость с другими продуктами Microsoft.
- Наличие конфигурации Win 32 Release, обеспечивающей работу программы и при отсутствии некоторых требуемых ей DLL-библиотек на исследуемом компьютере.

Перечисленные преимущества в контексте проведения компьютерно- технической экспертизы представляются ключевыми.

# разработанного инструментального средства

## Операции с файлами

### Поиск файлов по:

- имени;
- расширению;
- дате и времени создания;
- дате и времени модификации;
- дате и времени последнего обращения к файлу;
- другим атрибутам;

# Основные возможности разработанного инструментального средства

## Операции с файлами

- просмотр всех перечисленных сведений о файлах, включая информацию об их местонахождении;
- возможность выбора директории поиска;
- просмотр содержимого файлов;
- сортировка найденных файлов в соответствии с указанными пользователем критериями;
- помещение найденных данных полностью или частично в буфер обмена для их дальнейшей обработки средствами Microsoft Office, в частности Microsoft Excel (требование заказчика);
- сохранение результатов в отдельный файл;
- вывод результатов на печать;

# Основные возможности разработанного инструментального средства

## Операции с Интернет-адресами

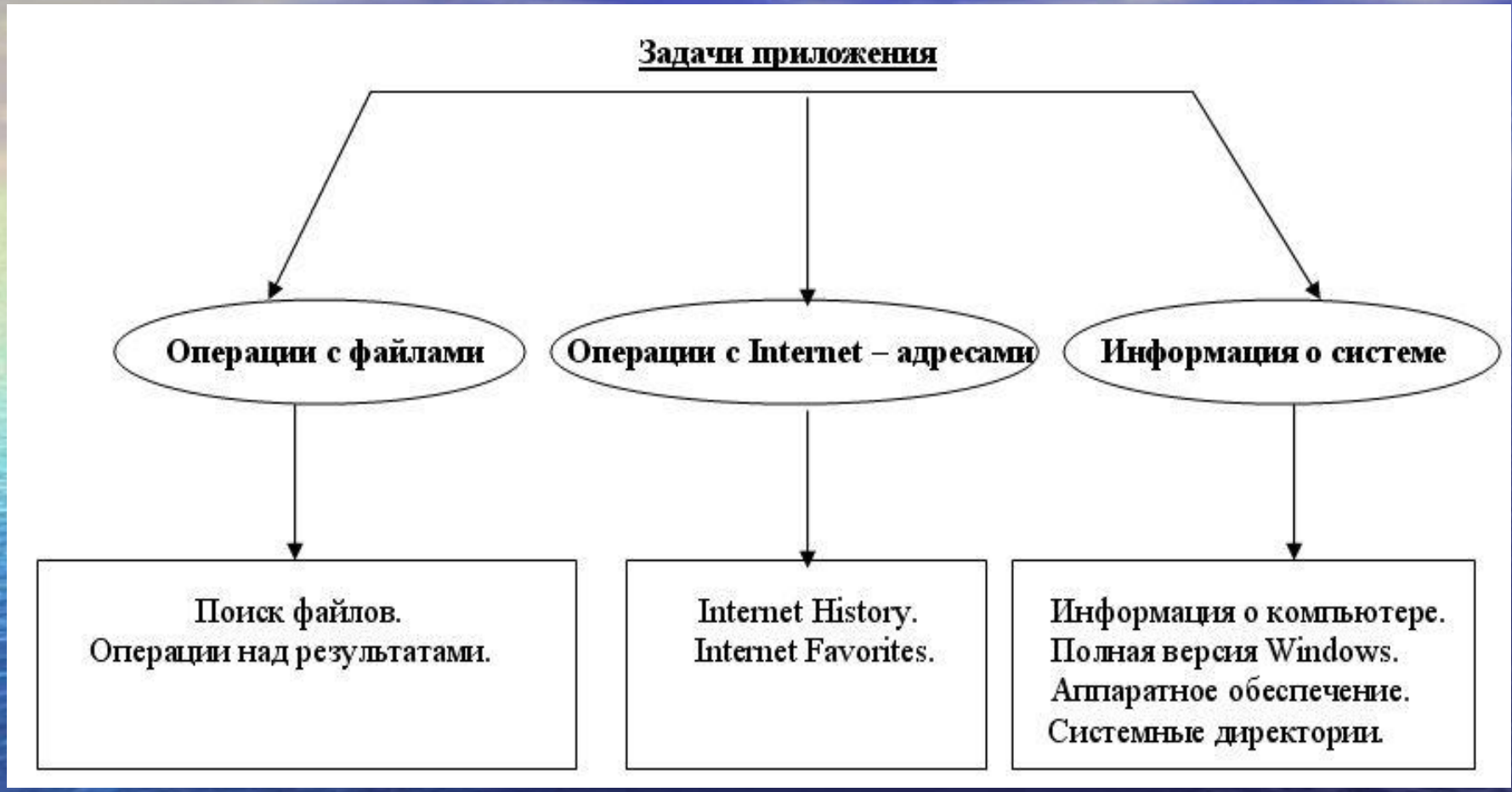
- Получение списка последних посещённых Internet – адресов (History) Microsoft Internet Explorer.
- Получение списка избранных Internet – страниц (Favorites) Microsoft Internet Explorer.
- Возможность сортировки, печати, сохранения в файл и копирования в буфер списка результатов.

# Основные возможности разработанного инструментального средства

## Системная информация

- Версия Microsoft Windows, включая номер сборки (Build number) и спецификатор.
- Получение адресов важнейших системных директорий.
- Получение системной информации (имя компьютера, имя пользователя и т.д.).
- Базовая информация об аппаратном обеспечении;

# Схема приложения




Данное логическое деление было удобно перенести на программный продукте, реализовав его в форме окна с тематическими вкладками.

# Использованные MFC - классы

- CSheet, CPropertyPage;
- CDialog, CAboutDlg;
- CFileFind;
- CListCtrl;
- CEdit;
- CImageList;
- CString;
- CProgressCtrl;
- CButton;
- CFileDialog, CPrintDialog;

# Использованные функции Win32API

- UpdateData(), UpdateWindow();
- MessageBox();
- GetLogicalDriveStrings();
- GetDriveType();
- PeekMessage();
- TranslateMessage();
- SHGetSpecialFolderPath();
- ShellExecute();
- GetDlgItem();
- OpenClipboard(), EmptyClipboard();
- CloseClipboard(), SetClipboardData();
- и другие.

# Классы, разработанные самостоятельно

- CSearchWindow
  Самый объёмный класс в программе(SearchWindow.cpp = 1809 строк). Содержит все функции работы с файлами. Предусмотрена возможность выбора директории поиска.

  Поиск осуществляется по:

  - Имени.
  - Дате модификации, создания, последнего просмотра (задаётся какой – либо временной промежуток).
  - Типу файла (видео, документы, рисунки, музыка). Возможно задание другого типа, т.е. поиск по расширению.
  - Атрибутам (скрытый файл, файл только для чтения).
  - Различным комбинациям перечисленных параметров.

# Важнейшие функции класса CSearchWindow

- DatePass(CFileFind &FoundFile);
- DisplayItem(CFileFind &FoundFile);
- FindAllCheck(LPCTSTR pstr), FindHidden(LPCTSTR pstr), FindHiddenName(LPCTSTR pstr), FindNameAndReadOnly(LPCTSTR pstr), FindReadOnly(LPCTSTR pstr), FindReadOnlyAndHidden(LPCTSTR pstr), OneRadioOnly(LPCTSTR pstr);
- OnAllDrives();
- OnClickAllfiles();
- OnColumnclickFoundFiles(NMHDR* pNMHDR, LRESULT* pResult);
- OnComeToTree();
- SearchFunction();

# Важнейшие функции класса CSearchWindow

- OnMyMenuPrint();
- OnMyMenuSaveInFile();
- OnOtherType() ;
- OnStartSearch();
- Recurse(LPCTSTR pstr);
- TypePass(CFileFind &FoundFile);
- WaitLoop();
- static int CALLBACK NameCompare (LPARAM lparam1, LPARAM lparam2, LPARAM lparamsort);
- OnDblclkFoundFiles(NMHDR* pNMHDR, LRESULT* pResult);
- OnInitDialog();
- OnMenuCopyToBuffer();
- OnMenuSortCreation();

# Классы, разработанные самостоятельно

- **CHistoryDisplay**
  Класс для получения последних посещённых Internet – страниц и даты их посещения

- **CInternetFavorites**
  Назначение методов этого класса – поиск и обработка избранных Интернет – адресов пользователя (Favorites).

- **CBrowse**
  Инициализируется структура TreeView для построения дерева директорий компьютера.

- **CExtension**
  Данный класс соответствует окну , в котором вводится расширение файлов, которые необходимо найти.

# Классы, разработанные самостоятельно

- **CPage1**

  Первая вкладка главного окна. Содержит в качестве ActiveX-компонента фоновый рисунок, приветствие и кнопку “Поиск файлов”.

- **CPage2**

  Вторая вкладка главного окна. Содержит кнопки “Internet History” и “Internet Favorites.

- **CPage3**

  Третья вкладка главного окна. Содержит кнопки “Информация о версии ОС Windows”, “Информация об аппаратном обеспечении”, “Системная информация Windows” и “Основные системные директории”.

- **CSplashScreen**

  Отображение при загрузке программы окна Splash Screen.

# Основные алгоритмы программы

- Организация поиска файлов.
- Копирование в буфер обмена.
- Сортировка.
- Получение адресов Internet History.

# Заключение

В ходе курсовой работы выполнены следующие задачи:

- Изучены возможности библиотеки классов MFC, а также особенности языка C++ и среды Microsoft Visual C++;
- Изучены теоретические основы компьютерно-технической экспертизы;
- Реализованы алгоритмы сортировки, поиска файлов, копирования в буфер, получения системной информации Windows, посещённых Internet – адресов.
- Разработана автоматизированная система, позволяющая производить компьютерно- техническую экспертизу по ряду параметров, оговоренных целями выполнения курсовой работы.

Спасибо за внимание!