Лабораторные работы по дисциплине

«ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ»

направление 050100 «Педагогическое образование»

профиль «Информатика»,

профили «Математика», «Информатика»,

профили «Информатика», «Физика»

Волгоград,

2013

СОДЕРЖАНИЕ

ВВОДНАЯ ЛАБОРАТОРНАЯ РАБОТА «ОПЕРАЦИОННАЯ СИСТЕМА WINDOWS: УПРАВЛЕНИЕ МЫШЬЮ, РАБОТА С ОКНАМИ И ПРИЛОЖЕНИЯМИ».

Содержание занятия:

1. В текстовом документе заполните следующую таблицу, сохраняя форматирование:

Таблица 1 Основные приемы работы с мышью

Действие	Выполнение действия	Назначение действия
Щелчок		
Двойной щелчок		
Перетаскивание		
Протягивание		
Щелчок правой кнопкой мышью		
Зависание		

2. Сделайте скриншот окна любого приложения, добавьте в текстовый документ и опишите его структуру – подпишите следующие элементы окна:

− строка заголовка;

− кнопки управления размером окна;

− строка меню;

− панель инструментов;

− строка состояния;

− полосы прокрутки;

− рабочая область.

3. Выполните поиск файлов на локальных дисках компьютера (либо в одной из сетевых папок) по следующим критериям:

− файлы с расширением .doc;

− файлы с последними изменениями (сохраненные) на прошедшей неделе;

− файлы, размер которых менее 1 МБ.

Результаты поиска оформить в виде таблицы:

Таблица 2. Результаты поиска файлов.

Критерий	Результат
Файлы с расширением .doc;	
Файлы с последними изменениями (сохраненные) на прошедшей неделе	
Файлы, размер которых менее 1 МБ	

Указание: После полной загрузки ОС Windows, откройте ГЛАВНОЕ МЕНЮ и выберите команду НАЙТИ, затем в открывшемся подменю щелкните на пиктограмме ФАЙЛЫ И ПАПКИ. Откроется окно РЕЗУЛЬТАТЫ ПОИСКА, в левой части этого окна находится панель помощника по выполнению поиска. Ознакомьтесь со всеми разделами панели помощника.

Возможно также выполнить поиск следующим образом: открыть диск или папку, в которой будет осуществляться поиск, и воспользоваться опцией ПОИСК на панели инструментов.

Для поиска файлов на дисках ПК необходимо знать все критерии поиска или некоторые из них:

- часть имени файла или имя файла целиком;
- слово или фразу в файле;
- дату последних изменений;
- размер файла;

Дополнительные параметры:

- тип файла;

- поиск в системных папках;
- поиск в скрытых файлах и папках;
- просмотреть вложенные папки;
- с учетом регистра;
- поиск во внешних хранилищах.

Для выполнения задания необходимо задать соответствующие критерии поиска.

4. Сделайте скриншоты окон приложений OpenOffice.org Impress, OpenOffice.org Calc, OpenOffice.org Writer (или же, в зависимости от установленного программного обеспечения, MS PowerPoint, MS Excel, MS Word). Опишите и укажите на рисунках общие элементы операционных меню указанных приложений.

ЛАБОРАТОРНАЯ РАБОТА № 1
«УЧЕТНЫЕ ЗАПИСИ ПОЛЬЗОВАТЕЛЕЙ. НАСТРОЙКА ПАРАМЕТРОВ АУТЕНТИФИКАЦИИ»

Учетные записи пользователей в Windows XP

Теоретические сведения

Учётная запись пользователя – это запись, которая содержит сведения, необходимые для идентификации[1] пользователя при подключении к системе, а также информацию для авторизации и учёта. Это имя пользователя и пароль (или другое аналогичное средство аутентификации[2] — например, биометрические характеристики). Пароль или его аналог, как правило, хранится в зашифрованном виде (в целях его безопасности).

Для повышения надёжности могут быть, наряду с паролем, предусмотрены альтернативные средства аутентификации — например, специальный секретный вопрос (или несколько вопросов) такого содержания, что ответ может быть известен только пользователю. Такие вопросы и ответы также хранятся в учётной записи.

В операционной системе Windows XP можно создавать несколькими способами как учетные записи пользователей для компьютеров, состоящих в рабочих группах, так и учетные записи пользователей для компьютеров, которые входят в состав домена. Домены, рабочие группы и домашние группы представляют разные методы организации компьютеров в сети. Основное их различие состоит в том, как осуществляется управление компьютерами и другими ресурсами.

Рабочая группа – это группа компьютеров, подключенных к сети, которые совместно используют ресурсы. При настройке сети операционная система Windows автоматически создает рабочую группу и присваивает ей имя по умолчанию.

Домен — это группа компьютеров одной сети, имеющих единый центр, использующий единую базу пользователей, единую групповую и локальную политики, единые параметры безопасности, ограничение времени работы учётной записи и прочие параметры, значительно упрощающие работу системного

---

[1] Идентификация – присвоение субъектам и объектам доступа личного идентификатора и сравнение его с заданным.

[2] Аутентификация – проверка подлинности.

администратора организации, если в ней эксплуатируется большое количество компьютеров.

При работе в компьютерной сети существуют два типа учетных записей.

Локальные учетные записи создаются на данном компьютере. Информация них хранится локально (в локальной базе безопасности компьютера) и локально же выполняется аутентификация такой учетной записи (пользователя).

Доменные учетные записи создаются на контроллерах домена[3]. И именно контроллеры домена проверяют параметры входа такого пользователя в систему.

Все учетные записи условно делятся на два типа.

Администраторы компьютера. Администраторы наделены всеми правами для настройки системы и имеют доступ ко всем файлам и папкам на разделах NTFS. Они могут создавать, изменять и удалять учетные записи других пользователей, а также наделять их теми или иными правами.

Ограниченные учетные записи. Пользователь с такой учетной записью может запускать программы, создавать, редактировать и удалять документы, но у него будут существенно ограничены возможности изменения системных настроек. При использовании файловой системы NTFS пользователи с ограниченной учетной записью не могут получить доступ к файлам и папкам других пользователей, также им нельзя изменять файлы, находящиеся в системных папках, например WINDOWS или Program Files.

Для каждой учетной записи система создает *профиль пользователя* — набор папок, в которых хранится личная информация пользователя. По умолчанию профили хранятся в папках с именами учетных записей, которые находятся в папке DOCUMENTS AND SETTINGS системного раздела.

Каждый профиль содержит личные папки пользователя: РАБОЧИЙ СТОЛ, МОИ ДОКУМЕНТЫ, ГЛАВНОЕ МЕНЮ И ИЗБРАННОЕ. Кроме них, в конфигурации есть несколько скрытых папок и файлов, содержащих настройки данного профиля. После

[3] Контроллер домена – главный компьютер, на котором находятся параметры учетных записей пользователей. Применяются в крупных организациях для централизованного управления.

входа пользователя в систему автоматически загружаются его настройки, элементы ГЛАВНОГО МЕНЮ и РАБОЧЕГО СТОЛА. Таким образом, каждый пользователь работает в своей индивидуальной среде независимо от других.

Задания

1) Создание новой учетной записи

Создание учетной записи пользователя с помощью диалога «Учетные записи пользователей»

1) Войдите в систему под учетной записью администратора.

2) Войдите в меню ПУСК, выберите пункт ПАНЕЛЬ УПРАВЛЕНИЕ – УЧЕТНЫЕ ЗАПИСИ ПОЛЬЗОВАТЕЛЕЙ

3) Просмотрите, какие учетные записи уже есть на данном компьютере, изучите свойства каждой учетной записи.

4) Добавьте нового пользователя с именем TEST. Для этого необходимо выбрать СОЗДАНИЕ УЧЕТНОЙ ЗАПИСИ.

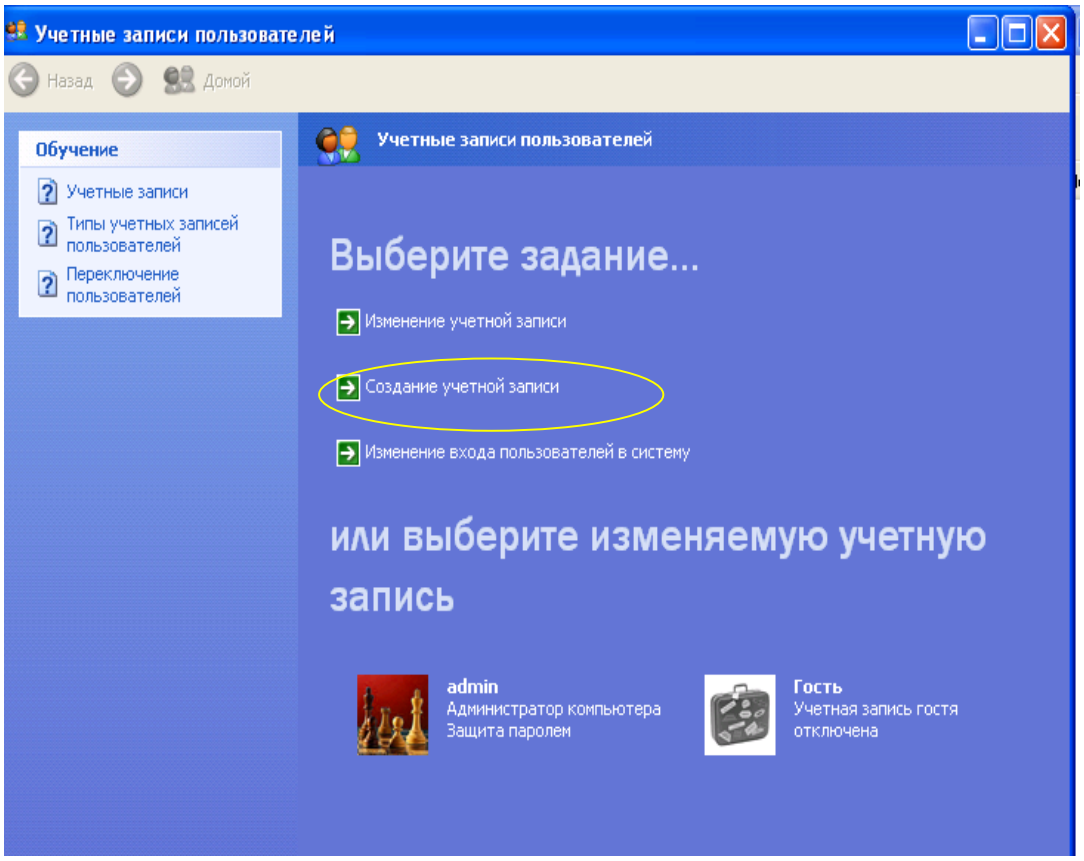

Рис. 1. Создание учетной записи пользователя

Далее нужно будет ввести имя для учетной записи, далее - выбрать тип учетной записи.

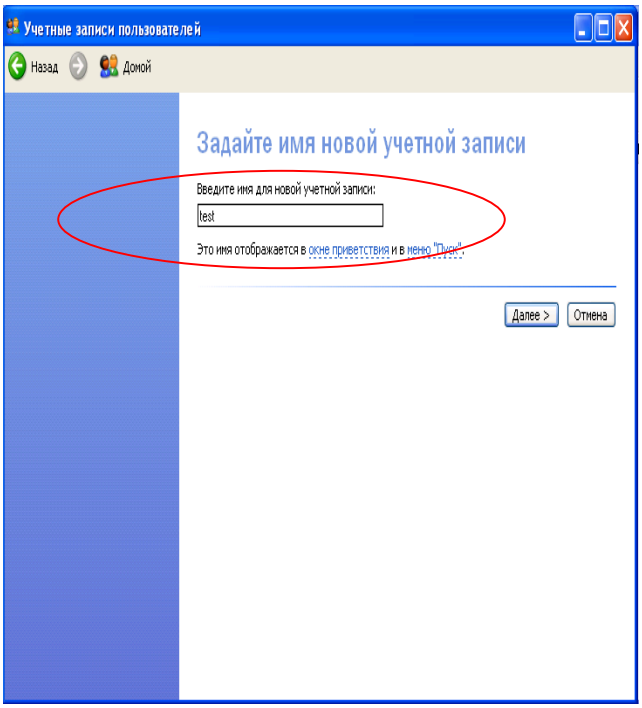

Рис. 2. Задание имени учетной записи

Имя пользователя не должно совпадать с любым другим именем пользователя или группы на данном компьютере. Оно может содержать до 20 символов верхнего или нижнего регистров, за исключением следующих: " / \ [ ] : ; | = , + * ? <> @, а также имя пользователя не может состоять только из точек и пробелов.

Далее необходимо выбрать тип учетной записи:

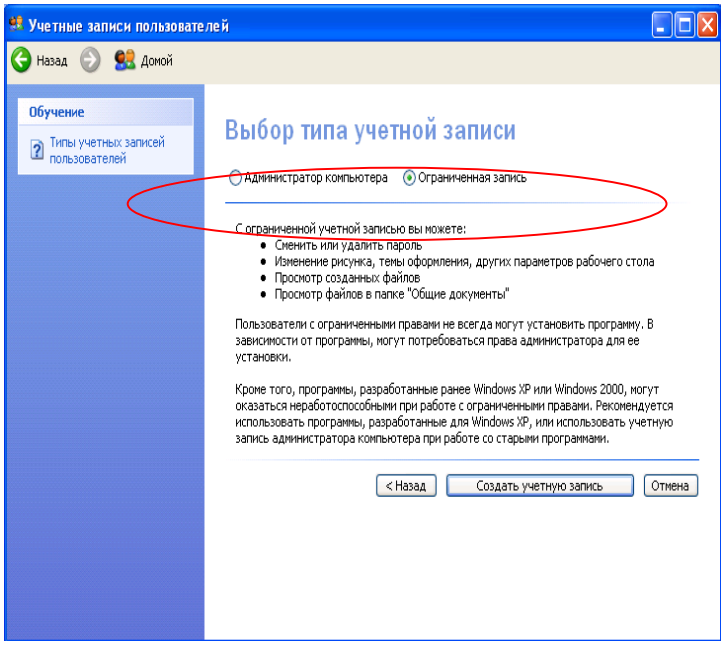

Рис. 3. Выбор типа учетной записи

В этом диалоге, можно выбрать одну из двух типов учетных записей:

− АДМИНИСТРАТОР КОМПЬЮТЕРА.

Пользователь с данной учетной записью будет обладать правами администратора, т.е. получит полный контроль над системой и сможет изменять любые ее настройки.

− ОГРАНИЧЕННАЯ ЗАПИСЬ.

Права обладателя данной учетной записи будут существенно ограничены. Пользователь не получит доступа к основным настройкам системы, а также не сможет запускать или устанавливать некоторые программы.

Обратите внимание на следующие аспекты создания учетной записи указанными способом:

- тип учетной записи пользователя, предлагаемый по умолчанию;
- существующие ограничения создания учетной записи пользователя указанным способом.

5) С помощью ПРОВОДНИКА откройте содержимое папки C:\ DOCUMENTS AND SETTINGS. Что можно сказать о профиле нового пользователя?

6) Зайдите в систему под именем нового пользователя. Убедитесь, что в папке C:\ DOCUMENTS AND SETTINGS.. Создан профиль нового пользователя TEST.

7) Сравните содержимое папки C:\ DOCUMENTS AND SETTINGS \ TEST\РАБОЧИЙ СТОЛ и РАБОЧЕГО СТОЛА как области экрана. Создайте ярлык на РАБОЧЕМ СТОЛЕ, убедитесь, что изменилось содержимое папки C:\ DOCUMENTS AND SETTINGS \ TEST\РАБОЧИЙ СТОЛ.

8) Создайте ярлык в папке C:\ DOCUMENTS AND SETTINGS \ TEST\РАБОЧИЙ СТОЛ, убедитесь, что изменился вид РАБОЧЕГО СТОЛА как области экрана.

9) Попробуйте войти в профили других пользователей, убедитесь, что персональные данные защищены.

Создание учетной записи при помощи оснастки
ЛОКАЛЬНЫЕ ПОЛЬЗОВАТЕЛИ И ГРУППЫ

1) Войдите в систему под учетной записью администратора.

2) Войдите в меню ПУСК, далее выберите ПАНЕЛЬ УПРАВЛЕНИЯ — АДМИНИСТРИРОВАНИЕ – УПРАВЛЕНИЕ КОМПЬЮТЕРОМ – ЛОКАЛЬНЫЕ ПОЛЬЗОВАТЕЛИ И ГРУППЫ.

3) Откройте папку ПОЛЬЗОВАТЕЛИ и изучите список пользователей данного компьютера.

4) Используя либо меню ДЕЙСТВИЕ, либо контекстное меню, выберите команду НОВЫЙ ПОЛЬЗОВАТЕЛЬ.

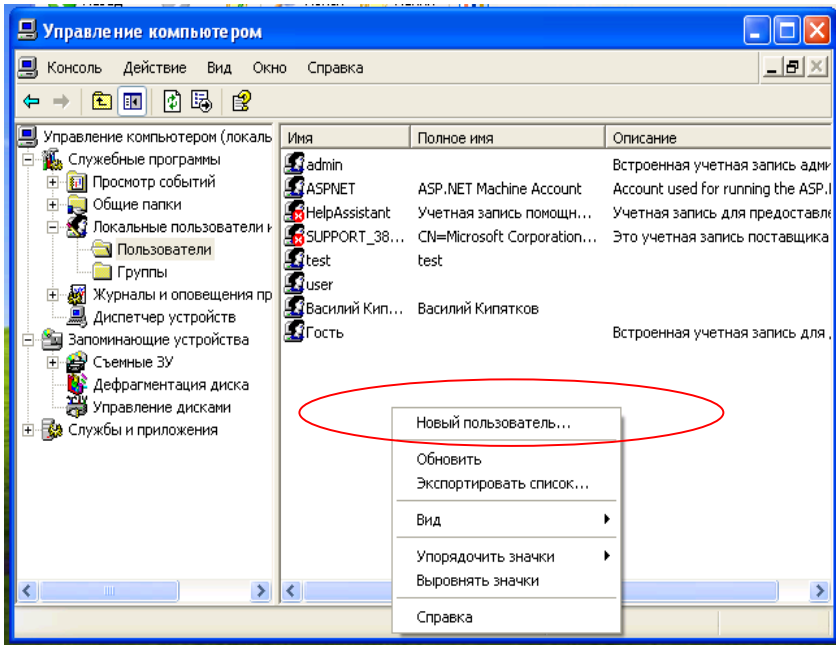

Рис. 4. Добавление нового пользователя

5) Добавьте нового пользователя, следуя инструкциям системы.

6) Для вновь созданного пользователя добавьте членство в группе, выполнив следующие действия в контекстном меню данного пользователя: СВОЙСТВА – ЧЛЕНСТВО В ГРУППАХ – ДОБАВИТЬ. В появившемся окне в поле ввода выбираемых имен введите имя необходимо группы и нажмите кнопку ПРОВЕРИТЬ ИМЕНА.

Изменения членства в группах вступят в силу после следующего входа пользователя в систему.

2. <u>Изучение параметров учетной записи пользователя.</u>

1) Войдите в систему под учетной записью администратора.

2) Выполните следующие действия: ПУСК – ПАНЕЛЬ УПРАВЛЕНИЯ – УЧЕТНЫЕ ЗАПИСИ ПОЛЬЗОВАТЕЙ – ИЗМЕНЕНИЕ УЧЕТНОЙ ЗАПИСИ ПОЛЬЗОВАТЕЛЯ.

3) Изучите параметры учетной записи пользователя.

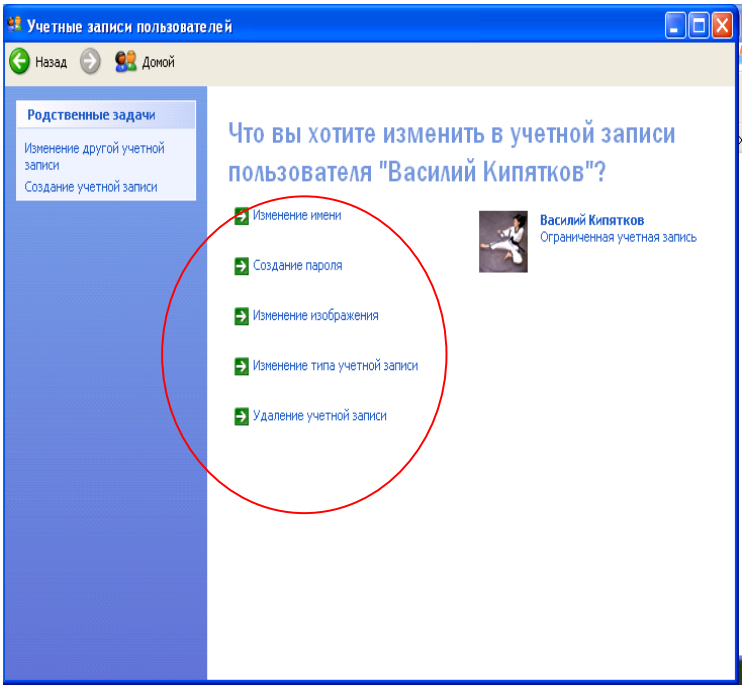

Рис. 5. Параметры учетной записи пользователя рабочей станции.

3. <u>Создание новой группы пользователей.</u>

1) Войдите в меню ПУСК, далее выберите ПАНЕЛЬ УПРАВЛЕНИЯ – АДМИНИСТРИРОВАНИЕ – УПРАВЛЕНИЕ КОМПЬЮТЕРОМ – ЛОКАЛЬНЫЕ ПОЛЬЗОВАТЕЛИ И ГРУППЫ.

2) Откройте папку ГРУППЫ и изучите список групп.

В данной папке отображаются все встроенные группы и группы, созданные пользователем. Встроенные группы создаются автоматически при установке Windows XP. Принадлежность к группе предоставляет пользователю права и возможности для выполнения различных задач на компьютере. Рассмотрим свойства некоторых встроенных групп.

АДМИНИСТРАТОРЫ

Членство в этой группе по умолчанию предоставляет самый широкий набор разрешений и возможность изменять собственные разрешения. Администраторы имеют полные, ничем неограниченные права доступа к компьютеру или домену. Работа в Windows XP в качестве администратора делает систему уязвимой для троянских коней и других программ, угрожающих безопасности. Простое посещение веб-узла может очень сильно повредить систему. На незнакомом

веб-узле может находиться троянская программа, которая будет загружена в систему и выполнена. Если в это время находиться в системе с правами администратора, такая программа может переформатировать жесткий диск, стереть все файлы, создать новую учетную запись пользователя с административным доступом и т. д.

Рекомендуется использовать административный доступ только для выполнения следующих действий:

− установки операционной системы и ее компонентов (например, драйверов устройств, системных служб и так далее);

− установки пакетов обновления;

− обновления операционной системы;

− восстановления операционной системы;

− настройки важнейших параметров операционной системы (политики паролей, управления доступом, политики аудита, настройки драйверов в режиме ядра и так далее);

− вступления во владение файлами, ставшими недоступными;

− управления журналами безопасности и аудита;

− архивирования и восстановления системы.

На практике учетные записи администраторов часто должны использоваться для установки и запуска программ, написанных для предыдущих версий Windows.

ОПЫТНЫЕ ПОЛЬЗОВАТЕЛИ

Эта группа поддерживается, в основном, для совместимости с предыдущими версиями для выполнения несертифицированных приложений. Разрешения по умолчанию, предоставленные этой группе, позволяют членам группы изменять параметры компьютера. Если необходима поддержка несертифицированных приложений, конечные пользователи должны быть членами группы «Опытные пользователи».

Члены группы «Опытные пользователи» имеют больше разрешений, чем члены группы «Пользователи», и меньше, чем члены группы «Администраторы». Опытные пользователи могут выполнять любые задачи с операционной системой, кроме задач, зарезервированных для группы «Администраторы».

Опытные пользователи могут:

− выполнять приложения, сертифицированные для Windows 2000 и Windows XP Professional, а также устаревшие приложения;

− устанавливать программы, не изменяющие файлы операционной системы, и системные службы;

− настраивать ресурсы на уровне системы, включая принтеры, дату и время, параметры электропитания и другие ресурсы панели управления;

− создавать и управлять локальными учетными записями пользователей и групп;

− останавливать и запускать системные службы, не запущенные по умолчанию.

Опытные пользователи не могут добавлять себя в группу «Администраторы». Они не имеют доступа к данным других пользователей на томе NTFS, если соответствующие разрешения этих пользователей не получены. Поскольку опытные пользователи могут устанавливать и изменять программы, работа под учетной записью группы «Опытные пользователь» при подключении к Интернету может сделать систему уязвимой для троянских коней и других программ, угрожающих безопасности.

ПОЛЬЗОВАТЕЛИ

Члены этой группы не могут организовывать общий доступ к каталогам или создавать локальные принтеры. Группа «Пользователи» предоставляет самую безопасную среду для

выполнения программ. Пользователи могут выключать рабочие станции, но не серверы. Пользователи могут создавать локальные группы, но управлять могут только теми, которые они создали. Однако разрешения на уровне пользователя часто не допускают выполнение пользователем устаревших приложений. Участники группы «Пользователи» гарантированно могут запускать только сертифицированные для Windows приложения.

ОПЕРАТОРЫ АРХИВА

Члены этой группы могут архивировать и восстанавливать файлы на компьютере независимо от всех разрешений, которыми защищены эти файлы. Они могут также входить в систему и завершать работу компьютера, но не могут изменять параметры безопасности. Для архивирования и восстановления файлов данных и системных файлов требуются разрешения на чтение и запись. Разрешения по умолчанию для операторов архива, позволяющие им архивировать и восстанавливать файлы, делают для них возможным использование разрешений группы для других целей, например для чтения файлов других пользователей и установки программ с троянскими вирусами.

ГОСТИ

Члены этой группы по умолчанию имеют те же права, что и пользователи, за исключением учетной записи «Гость», еще более ограниченной в правах.

ОПЕРАТОРЫ НАСТРОЙКИ СЕТИ

Члены этой группы могут иметь некоторые административные права для управления настройкой сетевых параметров.

ПОЛЬЗОВАТЕЛИ УДАЛЕННОГО РАБОЧЕГО СТОЛА

Члены этой группы имеют право на выполнение удаленного входа в систему.

3) Используя либо меню ДЕЙСТВИЕ, либо контекстное меню, выберите команду НОВАЯ ГРУППА, добавьте имя и описание группы.

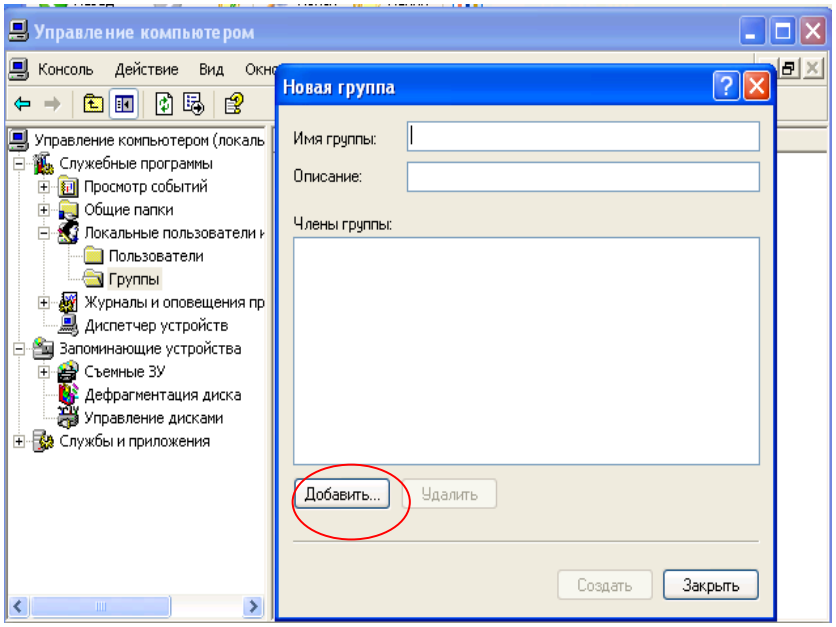

Рис. 6. Создание новой группы

4) Для добавления пользователей в группу выбираем кнопку ДОБАВИТЬ. Пользователей в группу выбираем из списка уже созданных, воспользовавшись функцией проверки имен.

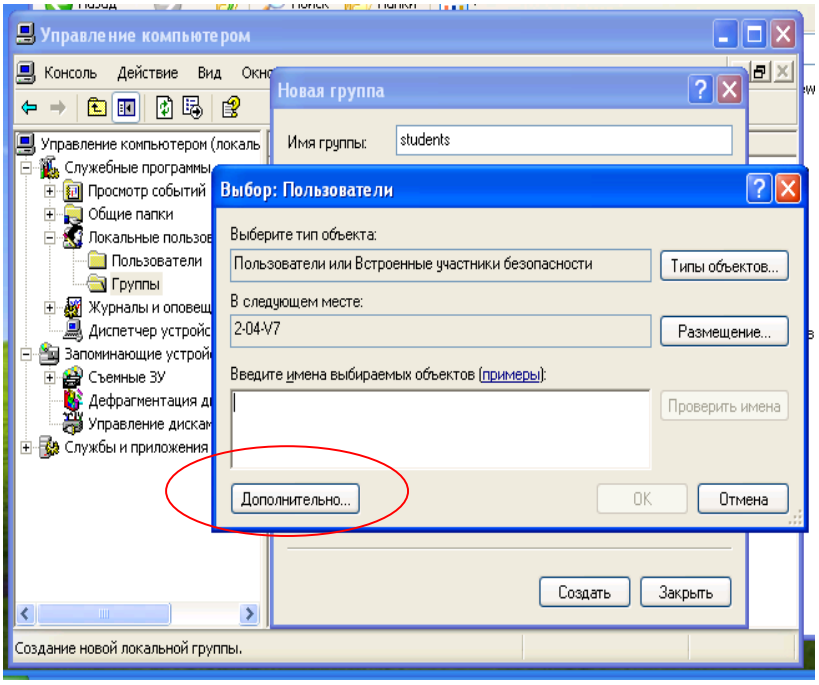

Рис.7. Добавление пользователей в новую группу.

4. Создание сетевого ресурса

1) Запустите утилиту УПРАВЛЕНИЕ КОМПЬЮТЕРОМ, выберите ветвь ОБЩИЕ ПАПКИ.

2) Изучите содержимое папок ОБЩИЕ РЕСУРСЫ, СЕАНСЫ, ОТКРЫТЫЕ ФАЙЛЫ. Определите назначение каждой из них.

3) В рабочей директории (например, D:\STUDENTS) создайте папку, в нее пометите какой-нибудь документ. Используя команды контекстного меню, сделайте созданную папку сетевым ресурсом, дайте разрешение для пользователей и групп.

5. Удаление учетной записи пользователя

Удаление учетной записи пользователя происходит с использованием опции УПРАВЛЕНИЕ УЧЕТНЫМИ ЗАПИСЯМИ ПОЛЬЗОВАТЕЛЯ.

Удалите созданные тестовые учетные записи пользователей.

Настройка параметров аутентификации в Windows XP

Теоретические сведения

В соответствии с сертификационными требованиями к системам безопасности операционных систем при подключении пользователей должен реализовываться

механизм аутентификации и/или идентификации. Настройка параметров аутентификации рассматриваемых систем выполняется в рамках локальной политики безопасности.

Оснастка «ЛОКАЛЬНАЯ ПОЛИТИКА БЕЗОПАСНОСТИ» используется для изменения политики учетных записей и локальной политики на локальном компьютере. При помощи оснастки «ЛОКАЛЬНАЯ ПОЛИТИКА БЕЗОПАСНОСТИ» можно определить:

– кто имеет доступ к компьютеру;

– какие ресурсы могут использовать пользователи на компьютере;

– включение и отключение записи действий пользователя или группы в журнале событий.

Задания

1. Настройка параметров политики паролей.

1) Зайдите в систему, используя учетную запись администратора.

2) Выберите ПУСК – ПАНЕЛЬ УПРАВЛЕНИЯ – АДМИНИСТРИРОВАНИЕ - ЛОКАЛЬНАЯ ПОЛИТИКА БЕЗОПАСНОСТИ:

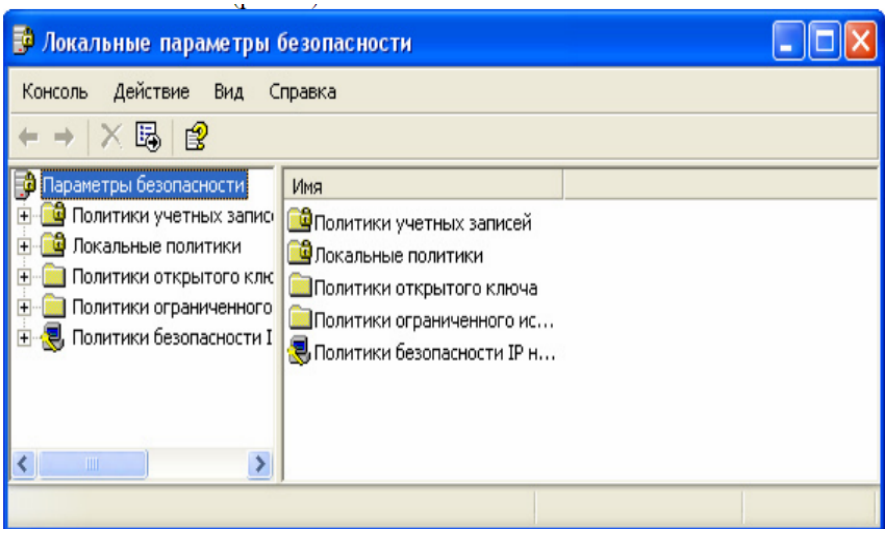

Рис. 1. Оснастка «Локальные параметры безопасности»

3) Выберите пункт ПОЛИТИКИ УЧЕТНЫХ ЗАПИСЕЙ – ПОЛИТИКА ПАРОЛЕЙ, появится список настраиваемых параметров:

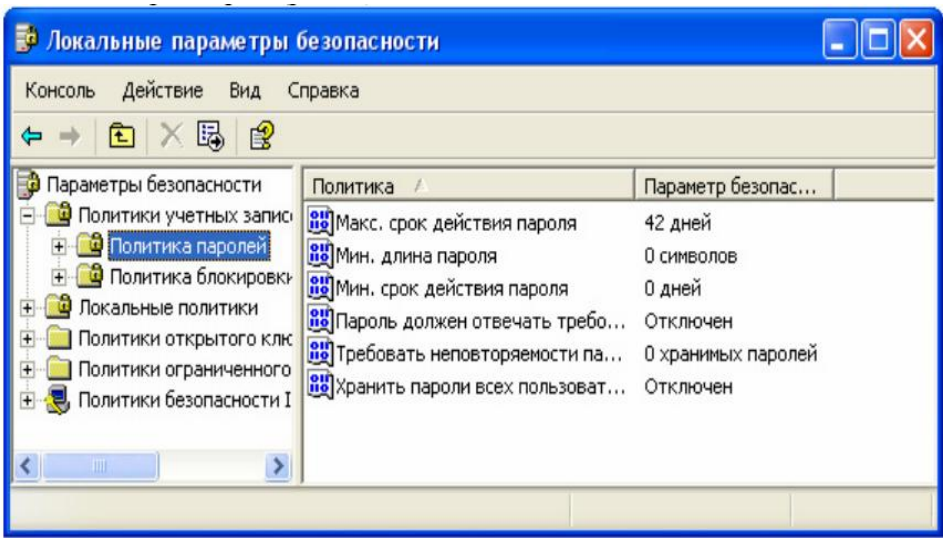

Рис. 2. Список параметров политики паролей

4) Ознакомьтесь с состоянием параметров политики паролей, значения параметров приведены в таблице 1.

Таблица 1

Значения параметров ПОЛИТИКИ ПАРОЛЕЙ

ПАРАМЕТР	ЗНАЧЕНИЕ
Требовать повторяемости паролей	Определяет число новых паролей, которые должны быть сопоставлены учетной записи пользователя, прежде чем можно будет снова использовать старый пароль. Это значение должно принадлежать диапазону от 0 до 24.
Максимальный срок действия пароля	Определяет период времени (в днях), в течение которого можно использовать пароль, прежде чем система потребует от пользователя заменить его. Можно задать значение в диапазоне от 1 до 999 дней или снять всякие ограничений срока действия, установив число дней равным 0.
Минимальный срок действия пароля	Определяет период времени (в днях), в течение которого можно использовать пароль, прежде чем пользователь сможет заменить его. Можно задать значение в диапазоне от 1 до 999 дней или разрешить немедленное изменение, установив число дней равным 0.
Минимальная длина пароля	Определяет наименьшее число символов, которые может содержать пароль учетной записи пользователя. Можно задать значение в диапазоне от 1 до 14 символов или отменить использование пароля, установив число символов равным 0.
Пароль должен отвечать требованиям сложности	Определяет, должны ли пароли соответствовать требованиям сложности. Если эта опция включена, пароли должны удовлетворять следующим минимальным требованиям: – пароль не может содержать имя учетной записи пользователя или какую-либо его часть; – пароль должен состоять не мене чем из 6 символов; – в пароле должны присутствовать символы трех категорий из числа следующих четырех: 1) прописные буквы английского алфавита от A до Z; 2) строчные буквы английского алфавита от a до z;

	3) десятичные цифры от 0 до 9; 4) символы, не принадлежащие алфавитно-цифровому набору (например, !, %, #). Проверка соблюдения этих требований выполняется при изменении или создании паролей.
Хранить пароли всех пользователей в домене, используя обратимое шифрование	Определяет, следует ли в системах Windows 2000 Server, Windows 2000 Professional и Windows XP хранить пароли, используя обратимое шифрование[4]. Эта политика обеспечивает поддержку приложений, использующих протоколы[5], которым для проверки подлинности надо знать пароли пользователя. Хранить пароли, зашифрованные обратимыми методами, - это все равно, что хранить их открытым текстом. Поэтому данную политику следует использовать лишь в исключительных случаях, если потребности приложения оказываются важнее, чем защита пароля.

5) Изучите свойства этих параметров, для изменения требуемого параметра необходимо воспользоваться его свойством из контекстного меню. В результате появится одно из окон, представленных на рисунке:

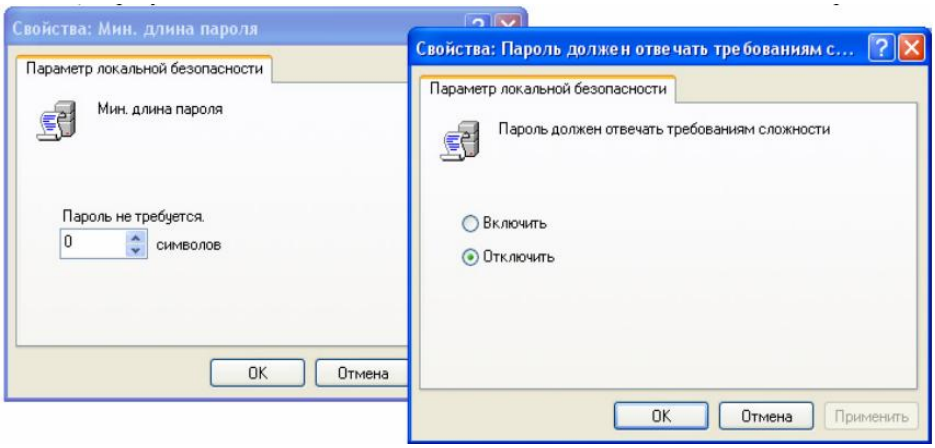

Рис.3. Настройка параметров пароля

6) Измените следующие значения:

– выберите параметр ТРЕБОВАТЬ НЕПОВТОРЯЕМОСТИ ПАРОЛЕЙ и измените его значение на 1;

---

[4] Шифрование – это процесс изменения информации по определённому алгоритму, при котором теряется возможность её нормального восприятия. Обратимое шифрование – это процесс, при котором возможно полное восстановление информации.

[5] Протокол – набор правил определяющих формат и очередность сообщений, которыми обмениваются два или более устройства, а также действия, выполняемые при передаче и/или приеме сообщений либо при наступлении иных событий.

− сделайте включенным параметр ПАРОЛЬ ДОЛЖЕН ОТВЕЧАТЬ ТРЕБОВАНИЯМ СЛОЖНОСТИ и после этого попробуйте изменить пароль своей учетной записи, введите допустимый пароль;

− снова изменить пароль своей учетной записи, а в качестве нового пароля укажите прежний пароль; зафиксируйте все сообщения, проанализируйте и объясните поведение системы безопасности.

2. Настройка параметров политики блокировки учетных записей

1) Зайдите в систему, используя учетную запись администратора.

2) Выберите ПУСК – ПАНЕЛЬ УПРАВЛЕНИЯ – АДМИНИСТРИРОВАНИЕ - ЛОКАЛЬНАЯ ПОЛИТИКА БЕЗОПАСНОСТИ – ПОЛИТИКА БЛОКИРОВКИ УЧЕТНЫХ ЗАПИСЕЙ.

3) Ознакомьтесь с состоянием параметров политики паролей, значения параметров приведены в таблице 2.

Таблица 2

Значения параметров ПОЛИТИКИ БЛОКИРОВКИ УЧЕТНЫХ ЗАПИСЕЙ

ПАРАМЕТР	ЗНАЧЕНИЕ
Пороговое значение блокировки	Определяет число неудачных попыток входа в систему, после которых учетная запись пользователя блокируется. Блокированную учетную запись нельзя использовать до тех пор, пока блокировка не будет сброшена администратором или пока не истечет период ее блокировки. Можно задать значение в диапазоне от 1 до 999 или запретить блокировку данной учетной записи, установив значение 0.
Блокировка учетной записи на	Определяет число минут, в течение которого учетная запись остается блокированной, прежде чем будет автоматически разблокирована. Этот параметр может принимать значения от 1 до 99 999 минут. Если установить значение 0, то учетная запись будет заблокирована до тех пор, пока администратор не разблокирует ее явным образом. Если пороговое значение блокировки определено, данный интервал блокировки должен быть больше или равен интервалу сброса.
Сброс счетчика блокировки через	Определяет число минут, которые должны пройти после неудачной попытки входа в систему, прежде чем, счетчик неудачных попыток будет сброшен в 0. Этот параметр может принимать значения от 1 до 99 999 минут. Если определенно пороговое значение блокировки, данный интервал сброса не должен быть больше интервала БЛОКИРОВКА УЧЕТНОЙ ЗАПИСИ НА.

4) Изучите и измените параметры ПОЛИТИКИ БЛОКИРОВКИ УЧЕТНЫХ ЗАПИСЕЙ.

3. Отслеживание попыток доступа и изменения параметров компьютера

Можно отслеживать все происходящее на компьютере (эта операция также называется *аудит*) для повышения его безопасности. Если на компьютере ведется аудит, всегда можно определить, какие пользователи входили в систему, создавали новые учетные записи пользователей, изменяли политику безопасности, открывали документы. Аудит не предотвращает изменения настроек компьютера хакерами или пользователями, имеющими учетную запись на компьютере, но дает возможность определить, какие и кем были сделаны изменения. Существует несколько видов событий, за которыми можно вести наблюдение: управление учетными записями, вход в систему, доступ к объектам, изменение политики, системные события. Если включить аудит любого из этих событий, то Windows будет их регистрировать в соответствующем журнале событий[6], который можно просматривать в окне просмотра событий.

Таблица 3

События, за которыми можно вести наблюдение

СОБЫТИЕ	ОПИСАНИЕ
Управление учетными записями	Наблюдение за данным событием позволяет определить, когда и кем были сделаны изменения имени учетной записи, когда она была включена или выключена, создана или удалена, когда был изменен пароль или изменена группа пользователей.
События входа в систему	Контроль за этими событиями позволяет определить, когда кто-либо входил или покидал систему (непосредственно на компьютере или через сеть).
Доступ к службе каталогов	Наблюдение за данным событием позволяет отследить факт обращения к объекту Active Directory[7], имеющему собственный системный список управления доступом (SACL).
Доступ к объектам	Аудит этого события позволяет определить, когда и кем использовались файлы, папки, принтеры или другие объекты. Также можно производить аудит ключей реестра, но это рекомендуется делать только опытным пользователям, имеющим опыт работы с системным реестром.
Изменение политик	Наблюдение за данным событием позволяет отслеживать попытки изменения локальной политики безопасности, политик аудита и доверия, прав пользователей.
Использование привилегий	Контроль этого события позволяет отследить применение права пользователя.
Отслеживание процессов	Наблюдение за этим событием позволяет определить такие события, как активация программ или завершение процесса.

[6] Журнал событий - это специальный журнал в Microsoft Windows, который содержит записи о входах и выходах из операционной системы и других, связанных с безопасностью событиях. Служба журналов событий запускается автоматически при запуске Windows.

[7] Active Directory — это централизованное хранилище информации обо всех ресурсах организации, таких как компьютеры, пользователи, группы, приложения, общие папки, принтеры и другие объекты.

Системные события	Аудит данных событий позволяет отслеживать выключение и перезагрузку компьютера, попытки программ совершать неразрешенные действия. Например, если шпионская программа попытается изменить параметры компьютера, не имея на то разрешения, контроль за системными событиями зафиксирует это.

1) Зайдите в систему, используя учетную запись администратора.

2) Включите локальную политику безопасности:

ПУСК – ПАНЕЛЬ УПРАВЛЕНИЯ – АДМИНИСТРИРОВАНИЕ - ЛОКАЛЬНАЯ ПОЛИТИКА БЕЗОПАСНОСТИ — ЛОКАЛЬНЫЕ ПОЛИТИКИ — ПОЛИТИКА АУДИТА

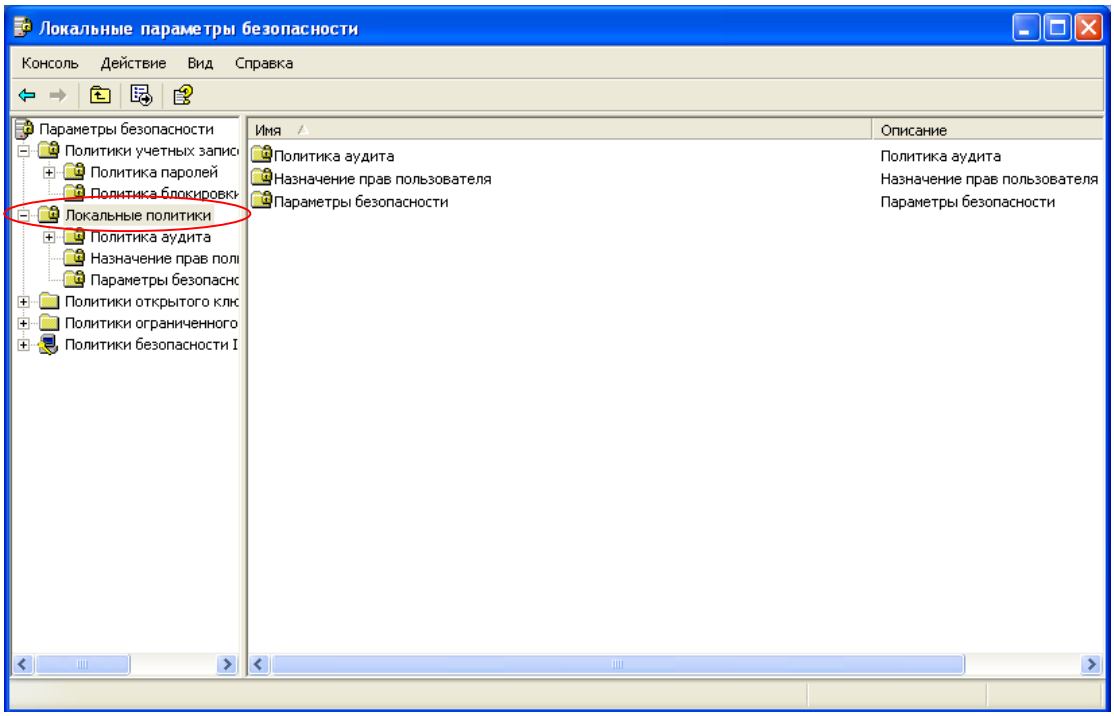

Рис. 4. Локальные политики

3) Двойным щелчком выберите событие, за которым надо наблюдать и установите флажки УСПЕХ или ОТКАЗ (или оба одновременно)[8].

[8] Если установить флажок УСПЕХ Windows будет фиксировать все успешные попытки выполнения события выбранного типа. Если установить флажок ОТКАЗ, будут зафиксированы все безуспешные попытки выполнения события. Количество фиксируемых событий ограничено, поскольку слишком большой журнал аудита событий может замедлить работу компьютера. Чтобы освободить место, можно удалить события из журнала, используя окно просмотра событий.

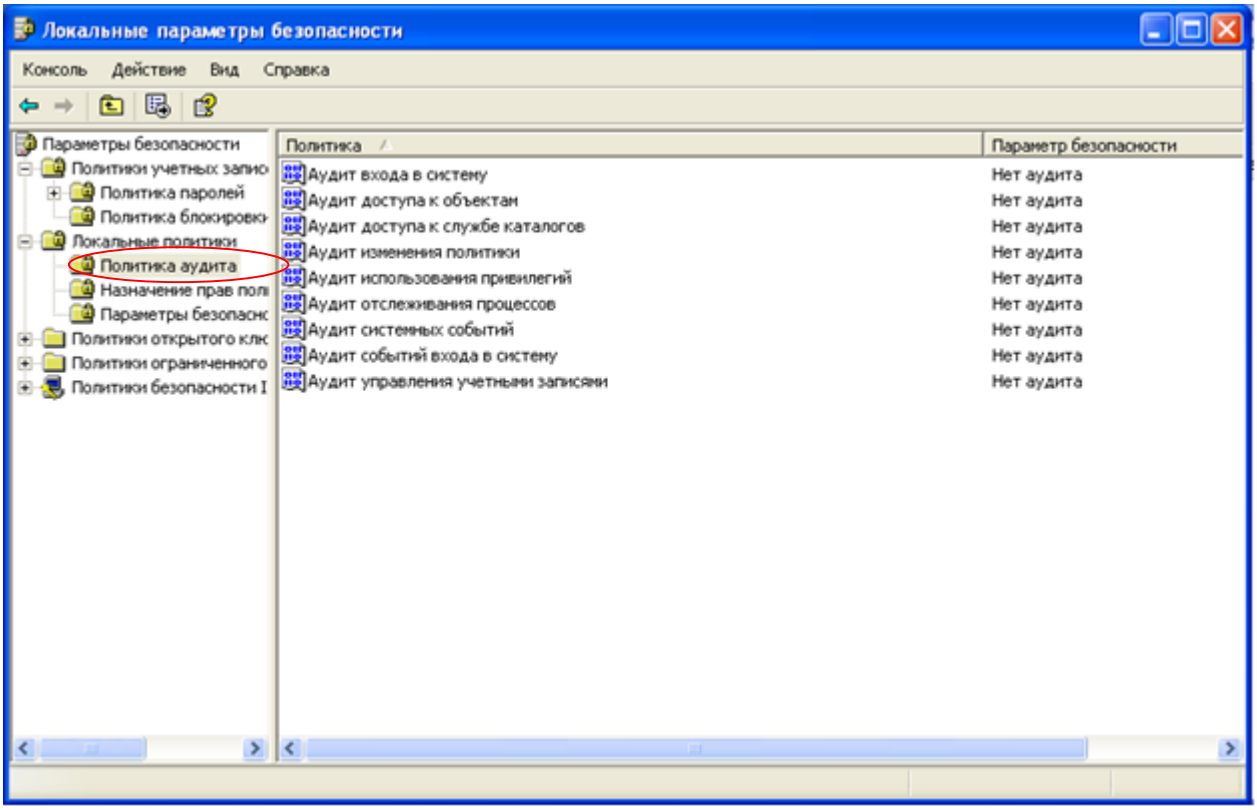

Рис. 5. Политика аудита

4) Измените параметры аудита отслеживаемых событий, настройте аудит входа пользователей в систему.

5) Настройте аудит пользователей, открывающих документ:

5.1. Вызовите контекстное меню для документа, контроль за которым надо установить и выберите СВОЙСТВА;

5.2. выберите БЕЗОПАСНОСТЬ – ДОПОЛНИТЕЛЬНО – АУДИТ.

5.3. Нажмите ПРОДОЛЖИТЬ, введите пароль администратора и, при необходимости, подтверждение пароля, выберите ДОБАВИТЬ.

5.4. Введите имя пользователя или группы, за которыми надо установить наблюдение. Если необходимо контролировать всех, введите *Everyone*, если необходимо производить наблюдение за конкретным пользователем, введите имя компьютера, а затем — имя пользователя: *компьютер\имя пользователя*.

5.5. Выберите те действия, которые нужно контролировать:

Таблица 4.

Действия над файлами, для которых можно установить аудит

ДЕЙСТВИЕ	ОПИСАНИЕ
Обзор папок или выполнение файлов	Отслеживание попыток запустить программный файл.

Просмотр содержания папки или чтение данных	Отслеживание попыток просмотра данных в файле.
Чтение атрибутов	Отслеживание попыток просмотра атрибутов файла или папки, таких как «Только чтение» или «Скрытый».
Чтение дополнительных атрибутов	Отслеживание попыток просмотра дополнительных атрибутов файла. Дополнительные атрибуты определяются программами, создавшими файл.
Создание файлов или запись данных	Отслеживание попыток изменения содержания файла.
Создание папок или добавление данных	Отслеживание попыток добавления данных в конец файла.
Запись атрибутов	Отслеживание попыток изменения атрибутов файла.
Запись дополнительных атрибутов	Отслеживание попыток изменения дополнительных атрибутов файла.
Удаление подпапок и файлов	Отслеживание попыток удаления папок.
Удаление	Отслеживание попыток удаления файлов.
Чтение разрешений	Отслеживание попыток просмотра разрешений файла.
Изменение разрешений	Отслеживание попыток изменения разрешений файла.
Смена владельца	Отслеживание события, когда пользователь становится владельцем файла.

Установка флажка ПОЛНЫЙ ДОСТУП выберет все действия, доступные для наблюдения.

6) Просмотрите журнал событий.

6.1. Выберите ПУСК – ПАНЕЛЬ УПРАВЛЕНИЯ – АДМИНИСТРИРОВАНИЕ, а затем двойным щелчком выберите ПРОСМОТР СОБЫТИЯ.

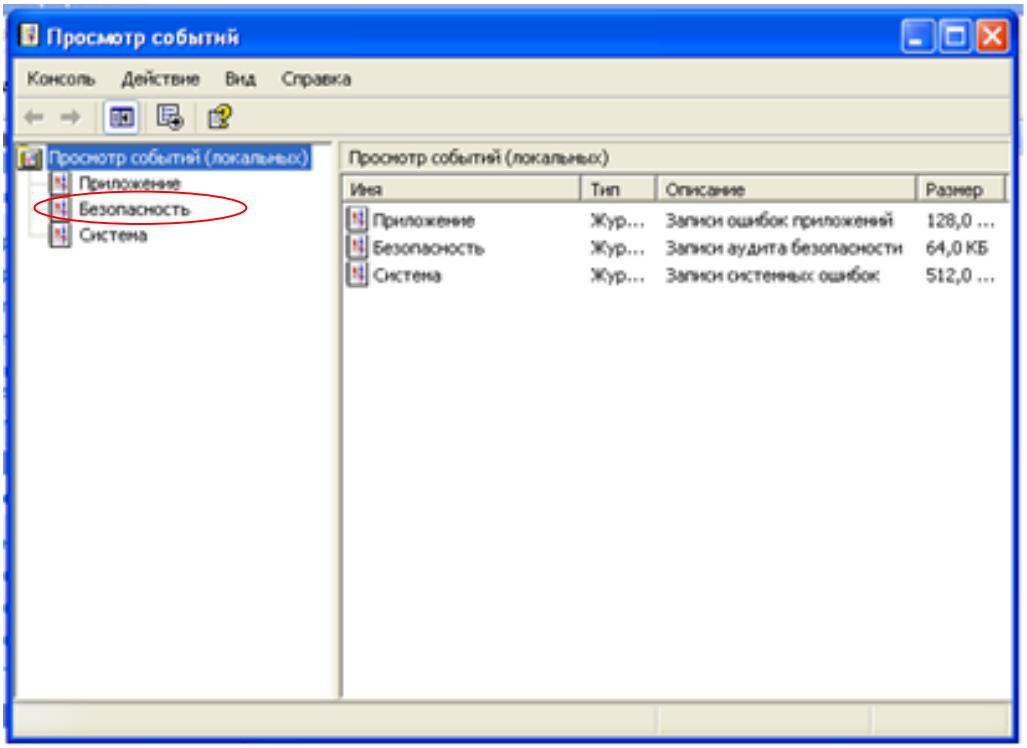

Рис. 5 Просмотр событий

6.2. При необходимости введите пароль администратора или подтверждение пароля.

6.3. Выберите пункт БЕЗОПАСНОСТЬ.

6.4. Изучите представленные события, с помощью двойного щелчка можно просмотреть подробности о событии.

ЛАБОРАТОРНАЯ РАБОТА № 2
«АРХИВИРОВАНИЕ И ВОССТАНОВЛЕНИЕ СИСТЕМЫ. РАБОТА С ДИСКАМИ. СЛУЖБЫ WINDOWS XP»

Содержание занятия:

1. Архивация данных

1) Зайдите в систему, используя учетную запись администратора.

2) Запустите утилиту АРХИВАЦИЯ ДАННЫХ:

ПУСК – ВСЕ ПРОГРАММЫ – СТАНДАРТНЫЕ – СЛУЖЕБНЫЕ – АРХИВАЦИЯ

Выберите МАСТЕР АРХИВАЦИИ, обратите внимание на то, какие объекты можно архивировать с помощью этой утилиты.

3) Создайте архив некоторой рабочей папки, следуя указаниям утилиты. Изучите возможности, предоставляемые после нажатия кнопки ДОПОЛНИТЕЛЬНО.

4) Внесите изменения в файлы, хранящиеся в вашей рабочей папке.

5) Запустите утилиту АРХИВАЦИЯ ДАННЫХ, выберите пункт ВОССТАНОВЛЕНИЕ ФАЙЛОВ И ПАРАМЕТРОВ и восстановите архив, созданный в 4.

6) Убедитесь, что содержимое рабочей папки соответствует более раннему состоянию – состоянию до внесения изменений в файлы, хранящиеся в этой папке.

Указание: выясните, какие группы пользователей наделены правами для архивации и восстановления системы.

2. Восстановление системы

Теоретические сведения

Установка новых программ и драйверов, изменения в оборудовании компьютера и настройках, а также другие причины могут привести к нестабильной работе операционной системы. В такой ситуации можно воспользоваться программой

ВОССТАНОВЛЕНИЕ СИСТЕМЫ для отмены изменений и восстановления предыдущего состояния компьютера без потери личных данных.

Программа ВОССТАНОВЛЕНИЕ СИСТЕМЫ ведет наблюдение за изменениями операционной системы и некоторыми файлами приложений и автоматически создает легко идентифицируемые *точки восстановления*. Эти точки восстановления позволяют вернуть систему к тому состоянию, которое было в момент создания контрольной точки восстановления. Такие точки создаются регулярно, а также во время существенных системных событий, таких как установка приложений или драйверов. Пользователь также имеет возможность в любое время создавать именованные точки восстановления для моментов времени, отличных от выбираемых системой. Создание собственной точки восстановления может оказаться полезным при внесении изменений, которые могут привести к нестабильной работе компьютера.

Таким образом, появляется возможность восстановить предыдущее состояние компьютера, выбирая по дате или времени точку восстановления, после которой были произведены изменения. Например, если случайно были удалены или повреждены наблюдаемые программные файлы, такие как файлы с расширением exe или dll, то можно восстановить состояние компьютера, предшествующее внесению изменений.

Программа ВОССТАНОВЛЕНИЕ СИСТЕМЫ по умолчанию отслеживает и восстанавливает все разделы и диски на компьютере. Программа также отслеживает настройку всех приложений и дисков, которые осуществляют пользователи с помощью CD-ROM или гибкого диска.

Восстановление системы не приводит к потере личных файлов или паролей. Такие элементы, как документы, сообщения электронной почты, перечень просмотренных страниц и пароли, сохраняются при восстановлении системы.

Программа ВОССТАНОВЛЕНИЕ СИСТЕМЫ обеспечивает сохранение личных файлов, не выполняя восстановление файлов в папке МОИ ДОКУМЕНТЫ. Кроме того, данная программа не восстанавливает файлы данных с часто используемыми расширениями, такими как doc и xls. Если вы не уверены, что ваши личные файлы имеют часто используемые расширения имен, и необходимо исключить эти файлы из

операции восстановления системы, то следует поместить все такие файлы в папку МОИ ДОКУМЕНТЫ.

В некоторых случаях при восстановлении системы восстанавливается папка, имя которой совпадает с именем существующей папки. Чтобы не переписывать существующие файлы, программа ВОССТАНОВЛЕНИЕ СИСТЕМЫ переименовывает папку, добавляя к имени числовой суффикс.

Если после создания точки восстановления была установлена какая-либо программа, то в процессе восстановления эта программа может быть удалена. Файлы данных, созданные этой программой, не теряются. Однако для открытия этих файлов необходимо будет установить удаленную программу.

1) Зайдите в систему, используя учетную запись администратора.
2) Запустите утилиту ВОССТАНОВЛЕНИЕ СИСТЕМЫ:

ПУСК – ВСЕ ПРОГРАММЫ – СТАНДАРТНЫЕ – СЛУЖЕБНЫЕ – ВОССТАНОВЛЕНИЕ СИСТЕМЫ

3) Создайте точку восстановления системы, следуя указаниям утилиты.
4) Создайте нового пользователя рабочей станции известным вам способом.
5) Запустите утилиту ВОССТАНОВЛЕНИЕ СИСТЕМЫ и восстановите более раннее состояние системы, выбрав контрольную точку восстановления, созданную в п.3.
6) Убедитесь, что конфигурация компьютера возвращена в более раннее состояние – состояние до создания нового пользователя.
7) Посмотрите список контрольных точек восстановления на вашем ПК. Есть ли среди них системные, пользовательские и установочные?

3. Проверка дисков на наличие ошибок

Теоретические сведения

Сохраняемые файлы и устанавливаемые программы записываются на диск с использованием так называемой *кластерной структуры хранения данных*. Эта структура подразумевает дробление дискового пространства на небольшие пронумерованные участки - кластеры, каждый из которых может содержать строго определенный объем информации. Записываемый на диск файл также разделяется на большое количество составляющих, каждая из которых помещается в собственный кластер вместе со сведениями о том, где система должна искать «продолжение» файла.

При загрузке программ или считывании какого-либо документа головка жесткого диска последовательно проходит все кластеры диска, «собирая» считываемую информацию в оперативной памяти воедино.

Поскольку содержимое жестких дисков компьютера непрерывно изменяется в связи с созданием, удалением и копированием различных файловых объектов, кластеры, в которых записана та или иная программа, могут оказаться на значительном расстоянии друг от друга, то есть хранящаяся в них информация становится фрагментированной. Очевидно, что в этом случае операционной системе требуется довольно много времени для того, чтобы загрузить такую программу - ведь считывающая головка жесткого диска должна просмотреть множество кластеров, постоянно перемещаясь над различными участками диска. Чтобы заметно ускорить загрузку приложений, необходимо «собрать» кластеры, в которых хранятся фрагменты программ, разместив их на диске по возможности близко друг к другу. Этот процесс называется *дефрагментацией диска*. Поскольку любая информация, хранящаяся на вашем жестком диске, с течением времени фрагментируется, дефрагментацию необходимо периодически повторять, не реже одного раза в несколько месяцев.

Если в процессе работы с Windows XP неожиданно начались какие-то сбои или стало невозможно открыть один или несколько файлов, необходимо проверить диски вашего компьютера и устранить ошибки, если они будут обнаружены. Утилита проверки диска запускается автоматически в ходе аварийной перезагрузки компьютера и в случае некорректного завершения работы с Windows XP.

1) Зайдите в систему под учетной записью администратора.

2) Перед началом дефрагментации необходимо проанализировать логическую структуру диска. Выделите в окне ДЕФРАГМЕНТАЦИЯ ДИСКА (ПУСК – ВСЕ ПРОГРАММЫ – СТАНДАРТНЫЕ – СЛУЖЕБНЫЕ) диск, который хотите дефрагментировать, и нажмите на кнопку АНАЛИЗ. Программа автоматически протестирует файловую структуру диска и покажет вам сводную информацию о характеристиках размещенных на диске данных, а также создаст список наиболее фрагментированных файлов.

3) Откройте системное окно Мой компьютер и щелкните на значке диска, который хотите проверить, правой кнопкой мыши.

4) В появившемся меню выберите пункт СВОЙСТВА и перейдите ко вкладке СЕРВИС диалогового окна СВОЙСТВА: ДИСК.

5) Щелкните на кнопке ВЫПОЛНИТЬ ПРОВЕРКУ и в появившемся окне ПРОВЕРКА ДИСКА установите флажок рядом с пунктом АВТОМАТИЧЕСКИ ИСПРАВЛЯТЬ СИСТЕМНЫЕ ОШИБКИ.

6) Если вы хотите, чтобы программа CHECK DISK полностью проверила диск на наличие сбойных секторов, установите флажок рядом с пунктом ПРОВЕРЯТЬ И ВОССТАНАВЛИВАТЬ СБОЙНЫЕ СЕКТОРЫ. Щелкните мышью на кнопке ЗАПУСК.

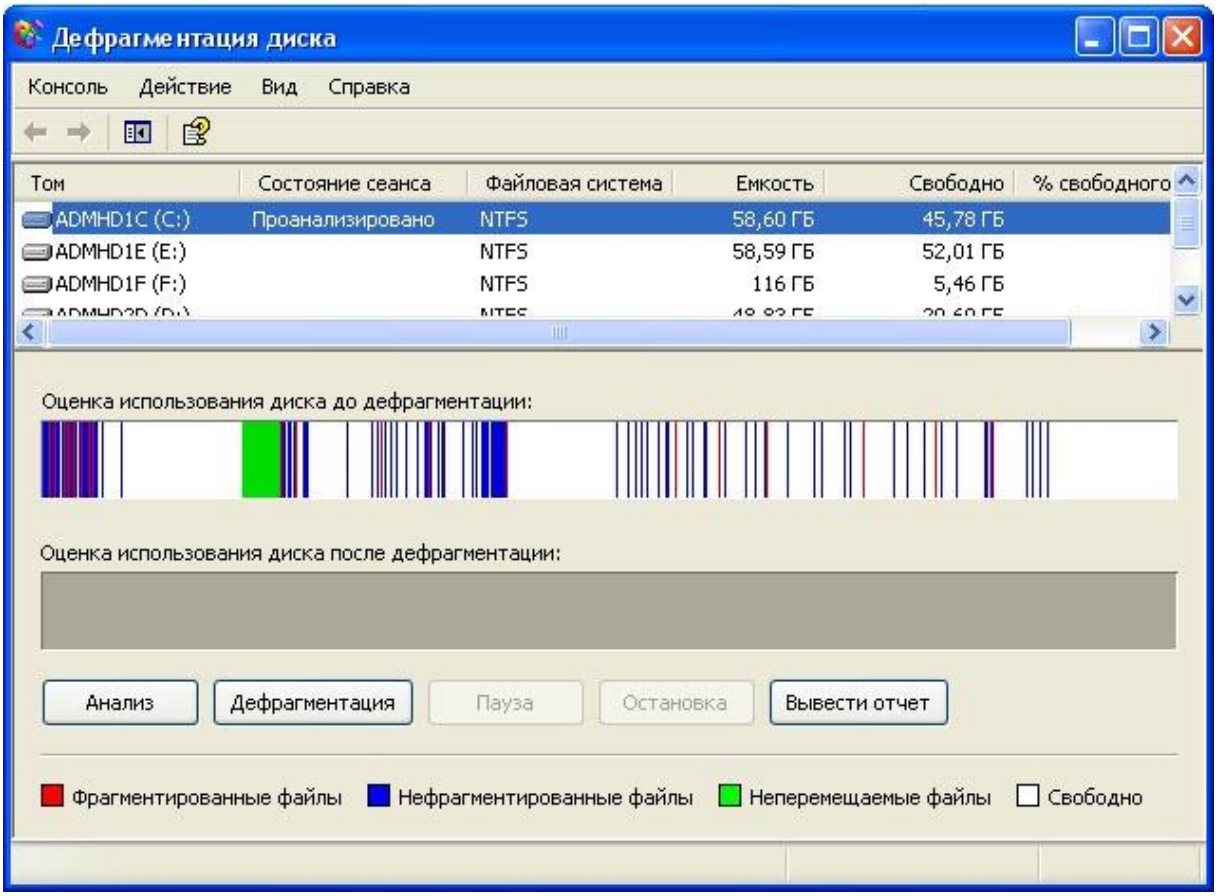

Рис.1. Интерфейс программы дефрагментации диска

Процедура дефрагментации диска может занять от восьми до сорока минут. Дефрагментация диска сообщит вам, когда она будет завершена.

4. Очистка дисков

Теоретические сведения

При заполнении 95 % дискового пространства различными файловыми объектами Windows XP сообщает пользователю о том, что свободное пространство на данном диске отсутствует. Можно освободить определенное место на диске вручную, удалив ряд неиспользуемых программ или уничтожив ненужные вам больше файлы, но можно также попытаться очистить диск с помощью специальной программы ОЧИСТКА ДИСКА.

1) Выберите меню ПУСК - ВСЕ ПРОГРАММЫ – СТАНДАРТНЫЕ – СЛУЖЕБНЫЕ - ОЧИСТКА ДИСКА.

2) Выберите в меню ДИСКИ диск, который хотите очистить от ненужной информации.

3) Программа проанализирует вашу систему и в следующем окне предложит список компонентов, удаление которых может высвободить определенный объем дискового пространства.

Среди подлежащих удалению данных программой могут быть предложены следующие варианты:

DOWNLOADED PROGRAM FILES - интерактивные компоненты ActiveX[9] и апплеты Java[10], загруженные из Интернета в процессе просмотра web-страниц и хранящиеся в одноименной системной папке.

TEMPORARY INTERNET FILES- web-страницы, помещенные при просмотре в кэш[11] браузера.

УСТАРЕВШИЕ ФАЙЛЫ CHKDISK (OLD CHKDISK FILES)- ФАЙЛЫ, АВТОМАТИЧЕСКИ СОЗДАВАЕМЫЕ ПРОГРАММОЙ CHECK DISK при проверке диска на наличие ошибок. Они могут содержать информацию о потерянных кластерах диска, а также сведения об обнаруженных программой неполадках в файловой системе. После штатной загрузки Windows и исправления выявленных ошибок эти файлы более не используются системой.

КОРЗИНА - содержимое Корзины Windows XP.

ВРЕМЕННЫЕ ФАЙЛЫ (TEMPORARY FILES)- некоторые программы, работающие под управлением Windows XP, создают на диске временные файлы с расширением .tmp. Такие файлы обычно автоматически уничтожаются при закрытии программ, но далеко не всегда.

Временные файлы WEBCLIENT/PUBLISHER (WEBCLIENT/PUBLISHER TEMPORARY FILES)- программы WebClient и Publisher при запуске создают на диске временные файлы, которые используются только в процессе работы данных приложений. Удаление этих файлов не может повредить операционной системе.

Файлы каталога для индексатора содержимого (CATALOG FILES FOR THE CONTENT INDEXER)- встроенная поисковая система Windows XP Помощник по поиску (Search Companion) может использовать функцию Indexing Service, позволяющую индексировать хранящиеся на дисках файлы с целью ускорения поиска информации. Удалить содержимое индекса программы Помощник по поиску можно вполне безболезненно.

4) Изучите дополнительные возможности на вкладке ДОПОЛНИТЕЛЬНО в окне программы DISK CLEANUP:

- Компоненты WINDOWS - удаляет неиспользуемые компоненты Windows.

---

[9] ActiveX – технология, предназначенная для написания сетевых приложений.

[10] Апплет Java – прикладная программа, написанная на языке программирования Java.

[11] Кеш – промежуточная область памяти с быстрым доступом, информация в ней может быть запрошена с высокой вероятностью.

− УСТАНОВЛЕННЫЕ ПРОГРАММЫ - вызывает на экран диалоговое окно установки и удаления программ.

− ВОССТАНОВЛЕНИЕ СИСТЕМЫ - удаляет хранящиеся на дисках резервные копии системных файлов, создаваемых программой ВОССТАНОВЛЕНИЕ СИСТЕМЫ.

5) Щелкните мышью на кнопке OK, чтобы начать процесс очистки жестких дисков.

5. Назначенные задания

1) Запустите утилиту «Назначенные задания»:

ПАНЕЛЬ УПРАВЛЕНИЯ - НАЗНАЧЕННЫЕ ЗАДАНИЯ.

2) Добавьте новое задание, используя пункт «Добавить задание» и следуя указаниям Мастера планирования заданий. Обратите внимание на то, какие задания можно запланировать. Запланируйте выполнение задания на ближайшее время.

3) Убедитесь в выполнении созданного вами задания в назначенное время.

6. Повторение: аудит и регистрация событий.

1) Установите аудит успеха действий с учетными записями.

2) Удалите ранее созданную пробную учетную запись.

3) Найдите все события в системном журнале, связанные с этим действием.

ЛАБОРАТОРНАЯ РАБОТА № 3
«СИСТЕМНЫЙ РЕЕСТР WINDOWS»

Указание

Ход выполнения лабораторной работы необходимо оформить в виде отчета с ответом на вопросы к заданиям, выводами и скриншотами выполняемых действий.

Теоретические сведения

Реестр операционной системы Windows – это большая база данных, где хранится информация о конфигурации системы. Этой информацией пользуются как операционная система Windows, так и другие программы. В некоторых случаях восстановить работоспособность системы после сбоя можно, загрузив работо способную версию реестра, но для этого необходимо иметь копию реестра.

Реестр можно рассматривать как записную книжку Windows - как только системе нужна какая-то информация, она ищет ее в реестре. Реестр очень обширен, и дать однозначное его определение невозможно.

В целом реестр очень напоминает файловую систему с той разницей, что вместо файлов на нижнем уровне содержатся *параметры.*

Информация, хранящаяся в иерархической базе данных реестра, собрана в *разделы* (ключи, key), которые содержат один или более *подразделов* (subkey). Каждый подраздел содержит *параметры* (значения, value):

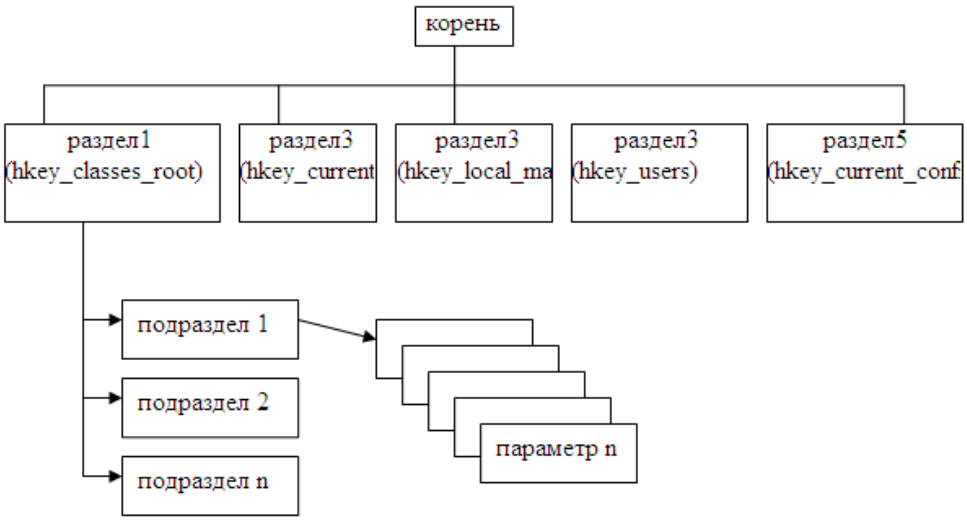

Рис.1. Архитектура реестра Windows

Основным средством для просмотра и редактирования записей реестра служит специализированная утилита «РЕДАКТОР РЕЕСТРА».

Файл редактор реестра находится в папке C:\Windows. Называется он REGEDIT.EXE. после запуска появится окно редактора реестра. Вы увидите список из 5 разделов:

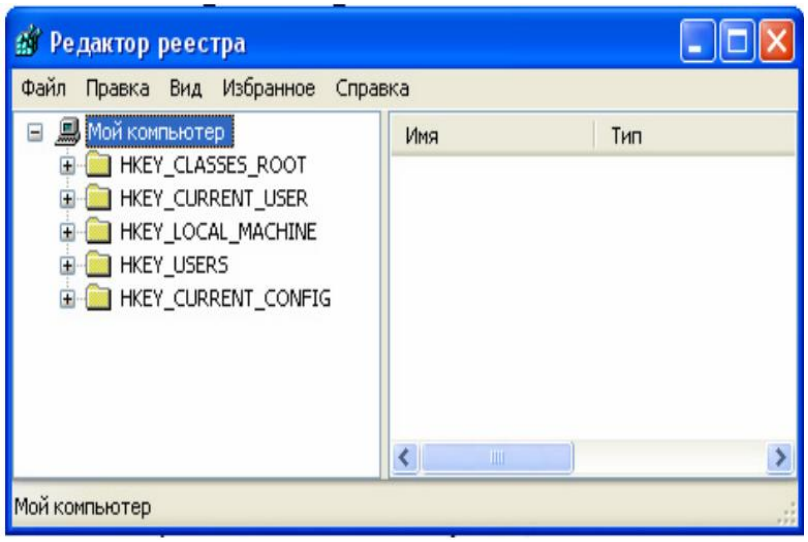

Рис.2. Редактор реестра

Работа с разделами реестра аналогична работе с папками в ПРОВОДНИКЕ. Конечным элементом дерева реестра являются ключи или параметры.

Реестр содержит шесть корневых разделов (ветвей), каждый из них включает подразделы, отображаемые в левой части окна в виде значка папки.

Указания:

Перед выполнением заданий создайте точку восстановления системы.

Задания

1. С помощью редактора реестра изучить корневые разделы системного реестра.

Таблица 1. Корневые разделы реестра:

Имя корневого раздела	*Описание*
HKEY_CLASSES_ROOT	В этом разделе содержится информация о зарегистрированных в

	Windows типах файлов, что позволяет открывать их по двойному щелчку мыши, а также информация для **OLE**[12] и операций **drag-and-drop**[13]. Параметры этого раздела совпадают с параметрами, расположенными в разделе HKEY_LOCAL_MACHINE\Software\Classes.
HKEY_CURRENT_USER	Здесь содержатся настройки оболочки пользователя (например, «Рабочего стола», меню «Пуск», ...), вошедшего в **Windows**. Они дублируют содержимое подраздела **«HKEY_USER\name»**, где **«name»**— имя пользователя, вошедшего в **Windows**. Если на компьютере работает один пользователь и используется обычный вход в **Windows** , то значения раздела берутся из подраздела **«HKEY_USERS\.DEFAULT»**. Содержит, профиль пользователя, на данный момент зарегистрировавшегося в системе, включая переменные окружения, настройку рабочего стола, параметры настройки сети, принтеров и приложений. Этот раздел представляет собой ссылку на раздел HKEY USERS\username, где username — имя пользователя, зарегистрировавшегося в системе на текущий момент
HKEY_LOCAL_MACHINE	Этот раздел содержит информацию, относящуюся к компьютеру: драйверы, установленное программное обеспечение и его настройки. Содержит глобальную информацию о компьютерной системе, включая такие данные об аппаратных средствах и операционной системе, в том числе: тип шины, системная память, драйверы устройств и управляющие данные, используемые при запуске системы. Информация, содержащаяся в этом разделе, действует применительно ко всем пользователям, регистрирующимся в системе Windows NT/2000/XP.
HKEY_USERS	Содержит настройки оболочки **Windows** для всех пользователей. Как было сказано выше, именно из этого раздела информация копируется в раздел **«HKEY_CURRENT_USER»**. Все изменения в**«HKEY_CURRENT_USER»** автоматически переносятся в**«HKEY_USERS»**.
HKEY_CURRENT_CONFIG	В этом разделе содержится информация о конфигурации устройств**Plug&Play**[14] и сведения о конфигурации компьютера с переменным составом аппаратных средств.

Регистр букв в ключах и параметрах не имеет значения. Прописные буквы употребляются только для удобства восприятия информации.

2. Экспорт реестра

[12] OLE (Object Linking and Embedded) – технология, обеспечивающая совместную работу нескольких приложений при подготовке одного документа.

[13] Drag-and-drop – способ оперирования элементами интерфейса, заключающийся в возможности их захвата и перемещения с использования мыши.

[14] PlugandPlay – технология быстрого определения устройств в компьютере.

Указание: по ходу выполнения заданий сделайте несколько скриншотов, добавьте в них комментарии и пояснения, внесите в отчет.

Экспорт Реестра ОС или его части это одна из тех вещей, которые достаточно часто приходится делать системным администраторам и опытным пользователям. Экспорт - копирование данных в другой файл. По отношению к Реестру, этот файл имеет расширение .reg.

Экспорт настроек в **Reg**-файл может использоваться для следующих целей.

Прежде всего, это хороший способ создать резервную копию системных настроек на случай их экстренного восстановления при необходимости. Также появляется возможность передавать настройки другим пользователям на другие компьютеры сети. Имея несколько **Reg**-файлов с различными настройками системы, возможно импортировать их одним двойным щелчком мышью.

Для экспорта ветвей реестра выполните следующие действия:

1) щелкните мышью на разделе (ключе), находящемся в вершине ветви, выбранной самостоятельно, которую необходимо экспортировать (например, HKEY_CURRENT_USER);

2) в меню «ФАЙЛ» выберите пункт «ЭКСПОРТ», чтобы вывести на экран диалоговое окно «ЭКСПОРТ ФАЙЛА РЕЕСТРА»;

3) в поле «ИМЯ ФАЙЛА» введите имя файла для экспорта;

4) выберите диапазон экспорта: чтобы создать копию всего реестра, щелкните на «ВЕСЬ РЕЕСТР», чтобы создать копию выделенной ветви, щелкните на «ВЫБРАННАЯ ВЕТВЬ»;

5) в выпадающем списке «Тип файла» выберите тип файла для экспорта: «Файлы Реестра *.reg», «Файлы кустов Реестра *.*», «Текстовые файлы *.txt» или «Файлы Реестра Win9x/NT4 *.reg»;

6) экспортируйте ветвь, мышью щелкнув на кнопке «СОХРАНИТЬ».

Последовательность вышеописанных действий фактически представляет собой один из способов создания резервной копии Реестра ОС. Сохранение Реестра перед его редактированием является принципиальным, поскольку обеспечивает дополнительный шанс на его восстановление в случае выхода системы из строя посредством непродуманных действий пользователя.

Обратная процедура импорта Реестра практически ни чем не отличается от простого открытия Reg-файла. Для этого необходимо щелкнуть мышью на пункте «ИМПОРТ» в меню «ФАЙЛ», далее в выпадающем списке «ТИП ФАЙЛА» выбрать тип файла, который предполагается импортировать, а затем в поле «ИМЯ ФАЙЛА» ввести полный путь **Reg**-файла и подтвердить операцию, щелкнув по кнопке «ОТКРЫТЬ».

Важно! Файлы Реестра ОС Windows XP представляют собой пятую версию **Reg**-файлов. Другие ОС семейства Windows имеют другие версии **Reg**-файлов. Поэтому не импортируйте **Reg**-файл, созданный в одной версии ОС Windows, в другую версию этой ОС. Это может привести к неработоспособности последней.

3. Внесение в системный реестр настроек, запрещающих пользователю полное или частичное изменение свойств Рабочего стола.

Указание: в отчет внести скриншот и полученные выводы.

1) С помощью ПРОВОДНИКА найти в папке Windows файл regedit.exe и запустить его.

2) Перейти в раздел реестра

HKEY_CURRENT_USERS\SOFTWARE\ MICROSOFT\WINDOWS\CURRENT VERSION\POLICIES\SYSTEM.

Если при открытии раздела POLICIES окажется, что в нем отсутствует раздел SYSTEM, создать его, используя команду

ПРАВКА – СОЗДАТЬ – РАЗДЕЛ.

3) Свернуть окно редактирования реестра и, щелкнув правой кнопкой мыши в свободном месте Рабочего стола, с помощью контекстного меню открыть окно *СВОЙСТВА: ЭКРАН*. Записать перечень закладок окна с настройками экрана, доступными для пользователя, и закрыть окно.

4) Развернуть окно редактирования реестра и в разделе SYSTEM с помощью команды

ПРАВКА – СОЗДАТЬ – ПАРАМЕТР DWORD

создать ключ *NODISPSettingsPage* и, щелкнув по его имени правой кнопкой мыши, выбрать в появившемся меню команду ИЗМЕНИТЬ. Используя окно ИЗМЕНЕНИЕ ПАРАМЕТРА DWORD (вызов осуществляется через контекстное меню), присвоить созданному ключу значение «1» в шестнадцатеричной системе.

5) Свернуть окно редактирования реестра и вновь открыть окно *СВОЙСТВА: ЭКРАН.* Изучить перечень закладок, доступных пользователю, и сделать вывод о назначении ключа *NODISPSettingsPage.* Закрыть окно свойств экрана.

6) Повторить действия, описанные в пунктах 4 и 5, присваивая значение «1» следующим ключам:

- NODISPBackgroundPage;
- NODISPAppearancePage;
- NODISPScrSavPage;
- NODISPCPL .

Сделать вывод об их назначении.

4. Создание файлов редактирования реестра, один из которых разрешает, а другой запрещает пользователю изменение настроек Рабочего стола.

Указание: внести в отчет скриншот и полученные выводы.

1) Хотя файлы редактирования реестра могут создаваться в любом текстовом редакторе (например, *Блокнот*), удобнее получить шаблон такого файла, используя *regedit.* Для этого, не закрывая редактор *regedit* после выполнения задания 3, в разделе *System* удалить все ключи кроме последнего *NODISPCPL*.

2) Щелкнув мышью по строке с названием раздела *System,* выполнить команду

ФАЙЛ – ЭКСПОРТ

и, указав имя создаваемого файла *file1,* сохранить его в папке *Мои документы.*

3) Закрыть программу *regedit.*

4) Перейти в папку *Мои документы* и, щелкнув правой кнопкой мыши по файлу *file1.reg,* выполнить команду

ОТКРЫТЬ С ПОМОЩЬЮ – БЛОКНОТ

5) Изучить структуру файла *file1.reg.* Его содержимое должно быть примерно следующим:

```
Windows Registry Editor Version 5.00
[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\System]
"NODISPCPL"=dword:00000001
```

6) Заменить в последней строке файла значение параметра DWORD с 00000001 на 00000000 и, используя команду ФАЙЛ – СОХРАНИТЬ КАК, сохранить внесенные изменения в файле *file2.reg.*

7) Закрыть *Блокнот.* Поочередно запуская двойным щелчком на выполнение файлы *file1.reg* и *file2.reg*, произвести попытку редактирования настроек Рабочего стола. Сделать выводы, удалить оба файла.

5. Настройка визуальных опций ОС с помощью системного Реестра.

Указание: в отчет внести выводы по задачам № 1 и 2, скриншоты по заданиям № 3 и 4.

1. В диалоговом окне «ИЗМЕНЕНИЕ СТРОКОВОГО ПАРАМЕТРА» ключа *HKCU\Control Panel\Desktop* измените значение параметра *MenuShowDelay* на любое число, менее 400. Сделайте вывод о том, как различные значения этого параметра влияют на раскрытие вложенных списков меню ПУСК.

2. Скрыть все значки с рабочего стола. Для этого в разделе *HREY_CURRENT_USER\ Software\ Microsoft\ Windows\ CurrentVersion\ Policies\ Explorer* создать параметр *DWORD NoDesktop =1* (=0 - все значки видны). При необходимости выполните перезагрузку виртуальной машины.

3. Запретить следующие команды в меню ПУСК. В разделе *HKEY_CURRENT_USER\ Software\ Microsoft\ Windows\ CurrentVersion\ Policies\ Explorer* если параметр имеет равен 1, то команда запрещена, 0 - разрешена

- *NoTrayContextMenu* - запретить контекстное меню панели задач,
- *NoChangeStartMenu* - запретить контекстное меню в меню ПУСК
- *NoStartMenuSubfolders*- скрыть подкаталоги в меню ПУСК.
- *NoRun* - скрыть меню ВЫПОЛНИТЬ в меню ПУСК.
- *NoFind* скрыть меню НАЙТИ в меню ПУСК.
- *NoLogOff* скрыть меню ЗАВЕРШЕНИЕ СЕАНСА в меню ПУСК.

− *NoClose* скрыть меню ЗАВЕРШЕНИЕ РАБОТЫ в меню ПУСК.

4. Удалить стрелки у ярлыков:

HKLM\SOFTWARE\Classes\lnkfile - ярлыки Windows XP

STRING IsShortcut - удаление этого параметра - отключает стрелки на ярлыках.

Не добавлять "ЯРЛЫК ДЛЯ..." для создаваемых ярлыков:

HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer BINARY link, значение hex:00,00, 00,00 - не добавлять.

6. Настройка меню ПУСК посредством системного реестра.

Указания:

− перенесите последовательность выполняемых действий по каждому из пунктов 1-4 в отчет (возможно приведение графических фрагментов, сделанных с экрана, в качестве демонстрационного материала),

− результаты применения новых значений системных параметров Реестра ОС перенесите в отчет,

− сделайте вывод о проделанной работе и запишите его в отчет.

Все настройки главного меню «Пуск» находятся в системном Реестре в одном месте *HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\ Advanced.*

Таблицы 2 и 3 описывают значения, которые можно добавлять в этот ключ. Причем первая таблица содержит значения для классического меню «Пуск», а вторая – для нового меню, соответственно. Большинство из этих значений принадлежит к типу REG_DWORD (данные имеют вид 0x01, 0x02 и т.д.), но некоторые из них имеют тип REG_SZ (символьные данные вида «NO» или «YES»).

Для настройки меню «Пуск» посредством Реестра ОС Windows XP, выполните следующие действия:

1) самостоятельно выберите вид главного меню «ПУСК» (классический или новый), соответствующие параметры которого будут применяться в Реестре ОС (табл. 2 или 3),

2) самостоятельно определите, какие именно параметры будут применены для конфигурирования меню «ПУСК» (в количестве не менее пяти штук),

3) самостоятельно конфигурируйте меню «ПУСК» с применением выбранных параметров,

4) результаты конфигурирования меню «ПУСК» зафиксируйте в виде графических фрагментов, сделанных с экрана командой PrintScreen.

Таблица 2. Настройка классического меню ПУСК в Windows XP.

№п/п	Параметр	Описание
1	SrartMenuAdminTools	Администрирование, YES – отобразить, NO - скрыть
2	CascadeControlPanel	Панель управления YES – отобразить как меню, NO – отобразить как ссылку
3	CascadeMyDocuments	Мои документы YES – отобразить как меню, NO – отобразить как ссылку
4	CascadeMyPictures	Мои рисунки YES – отобразить как меню, NO – отобразить как ссылку
5	CascadePrinters	Принтеры YES – отобразить как меню, NO – отобразить как ссылку
6	IntelliMenus	Персонифицированное меню 0x00 – не использовать; 0x01 – использовать;
7	CascadeNetwork-Connections	Сетевые подключения» NO – Отобразить как ссылку; YES – Отобразить как меню;
8	Start_LargeMFUIcons	Пиктограммы в меню «Пуск» 0x00 – Отобразить маленькими; 0x01 – Отобразить большими;
9	StartMenuChange	DRAG-AND-DROP 0x00 – Отключить; 0x01 – Включить;
10	StartMenuFavorites	Избранное 0x00 – Скрыть; 0x01 – Отобразить;
11	StartMenuLogoff	Завершение сеанса 0x00 – Скрыть; 0x01 – Отобразить;
12	StartMenuRun	Команда «Выполнить» 0x00 – Скрыть; 0x01 – Отобразить;
13	StartMenuScrollPrograms	Прокрутка меню «Программы» NO – Не использовать; YES – Использовать

Таблица 3. Настройка классического меню ПУСК в Windows XP.

№ п/п	Параметр	Описание
1	Start_ShowControlPanel	«Панель управления» 0x00 – Скрыть; 0x01 – Отобразить как ссылку; 0x02 – Отобразить как меню;
2	Start_EnableDragDrop	DRAG AND DROP 0x00 – Отключить: 0x01 – Включить;
3	StartMenuFavorites	«Избранное» 0x00 – Скрыть; 0x01 – Отобразить;
4	Start_ShowMyComputer	«Мой компьютер» 0x00 – Скрыть; 0x01 – Отобразить как ссылку; 0x02 – Отобразить как меню;
5	Start_ShowMyDocs	«Мои документы» 0x00 – Скрыть; 0x01 – Отобразить как ссылку; 0x02 – Отобразить как меню;
6	Start_ShowMyMusic	«Моя музыка» 0x00 – Скрыть; 0x01 – Отобразить как ссылку; 0x02 – Отобразить как меню;
7	Start_ShowMyPics	«Мои рисунки» 0x00 – Скрыть; 0x01 – Отобразить как ссылку; 0x02 – Отобразить как меню;
8	Start_ShowNetConn	«Сетевые подключения» 0x00 – Скрыть; 0x01 – Отобразить как ссылку; 0x02 – Отобразить как меню;
9	Start_AdminToolsTemp	«Администрирование» 0x00 – Скрыть; 0x01 – Отобразить в меню «Все программы» 0x02 – Отобразить в меню «Все программы» и меню «Пуск»;
10	Start_ShowHelp	«Справка и поддержка» 0x00 – Скрыть; 0x01 – Отобразить;
11	Start_ShowNetPlaces	«Сетевое окружение» 0x00 – Скрыть; 0x01 – Отобразить;
12	Start_ShowOEMLink	«Производитель» 0x00 – Скрыть; 0x01 – Отобразить;
13	Start_ShowPrinters	«Принтеры и факсы» 0x00 – Скрыть; 0x01 – Отобразить;
14	Start_ShowRun	Команда «Выполнить» 0x00 – Скрыть; 0x01 – Отобразить;

15	Start_ShowSearch	Команда «Найти» 0x00 – Скрыть; 0x01 – Отобразить;
16	Start_ScrollPrograms	Прокрутка меню «Программы» 0x00 – не использовать; 0x01 – использовать;

7. Создание в системном реестре собственного обработчика произвольного расширения.

Указание: внести в отчет скриншот полученного результата

1. выберите самостоятельно произвольное расширение, состоящее из трех символов, обработчик которого предполагается создать,

2. в разделе HKCR Реестра ОС создайте новый раздел с названием выбранного ранее расширения; при этом обратите внимание на то, как это уже сделано для других расширений в системе,

3. значение строкового параметра (по умолчанию), соответствующего созданному разделу, должно содержать ссылку вида ****file*, где *** – символы выбранного расширения, на раздел обработчика данного расширения,

4. в разделе HKCR Реестра ОС создайте новый раздел обработчика расширения следующего вида ***file\shell\open\command* – для команды открытия и ***file\shell\list\command* – для команды просмотра файла;

5. в разделах *command*, каждой из ветвей, создайте по одному расширяемому строковому параметру типа REG_EXPAND_SZ с наименованием (*по умолчанию*),

6. удалите старые строковые параметры REG_SZ, создаваемые в разделе *command* по умолчанию,

7. в расширяемом строковом параметре раздела ***file\shell\list* измените данные значения по умолчанию на «*Мой просмотр*»,

8. в соответствующих разделах command измените значения расширяемых строковых параметров на команды для открытия файла и его просмотра. В частности, для открытия текстового файла можно воспользоваться приложением WORDPAD.EXE, а для его просмотра выбрать NOTEPAD.EXE,

9. проверьте работоспособность обработчика, выполнив следующее:

   − выберите какой-либо файл с его стандартным расширением,

− поменяйте стандартное расширение на то, обработчик которого Вы только что создали,

− правой кнопкой манипулятора мышь выберите из контекстного меню команду с именем того файла (*filename.****),* который Вы собираетесь открыть или команду «Мой просмотр», чтобы просмотреть файл; при этом должно загрузиться соответствующее приложение обработчика.

ЛАБОРАТОРНАЯ РАБОТА № 4

«СЕРВИСНОЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ: АРХИВАТОРЫ»

Указание

Скопируйте в свою папку папки с файлами к заданию.

1. Создание и просмотр архивов

Создание архива

1. Откройте программу **7Zip File Manager**.[**Пуск→Программы→7zip →7Zip File Manager**]

2. Откройте свою рабочую папку.

3. Выделите все файлы этой папки. **[Edit→Select All].**

4. Дайте команду **Добавить [Add]**.

5. Изучите открывшееся диалоговое окно. Добейтесь того, чтобы вам был понятен каждый пункт.

6. Запустите процесс добавления в архив щелчком на кнопке **ОК**.

7. Убедитесь, что новый архив создан.

8. Просмотрите его содержимое.

9. Закройте программу **7Zip File Manager**.

Создание самораспаковывающихся архивов

1. Откройте программу **7Zip File Manager**.[**Пуск→Программы→7zip →7Zip File Manager**]

2. Как в предыдущем задании создавайте архив всех файлов своей рабочей папки.

3. Дойдя до диалогового окна, установите флажок **Create SFX archive**.

4. Запустите процесс добавления в архив щелчком на кнопке **ОК**.

5. Закройте программу **7Zip File Manager**.

6. Найдите только что созданный архив.

7. Запустите его как обычную программу.

8. Установите путь к рабочей папке в строке **Extract to** и нажмите кнопку **Extract**.

9. Наблюдайте за процессом распаковывания.

10. Попробуйте распаковать архив в другую папку.

11. После все файлы можно удалить.

Просмотр архивного файла

1. Двойным щелчком на файле **arc.rar** запустите программу.

2. В окне программы откроется список файлов, входящих в архив.

3. Выделите файл **ReadMe.txt**. Дважды щёлкните на этом значке, и файл откроется.

4. Закройте все окна работающих программ.

Извлечение файлов из архива

1. Запустите программу **7Zip File Manager.**

2. Выделите файлы ReadMe.txt и Гимн РФ.doc. При групповом выделении пользуйтесь левой кнопкой мыши совместно с клавишей **Ctrl.**

3. С помощью панели инструментов дайте команду **Extract** – откроется диалоговое окно.

4. Изучите содержание окна, установите необходимые переключатели, проверьте путь извлечения.

5. Запустите процесс извлечения файлов щелчком на кнопке **ОК**.

6. По окончании процесса закройте окно программы **7Zip File Manager.**

7. Убедитесь в том, что файлы, извлечённые из архива, действительно поступили в заданную папку.

8. Удалите только что распакованные файлы.

2. Оценка коэффициента сжатия

1. Скопируйте в свою папку файлы к заданию 2.

2. Создайте два архива. В первый поместите графические файлы, во второй — текстовые. Оцените коэффициент сжатия.

3. Сравнение сжатия различных типов данных

Сравнительная характеристика сжатия различных типов данных

(при использовании архиватора 7Zip File Manager)

файл	**Тип файла**	**Размер кбайт**	**Normal сжатие**	**Maximum. сжатие**	**Ultra сжатие**
01 - Alles Luge.mp3	mp3				
brndlog.txt	txt				
Calc.exe	exe				
Установка.bmp	bmp				
Imgocxd.hlp	hlp				
1089714161_6.jpg	jpg				
Дерево.jpg	jpg				
Biography.doc	doc				

Проанализируйте таблицу и сделайте выводы о сжатии различных типов данных.

ЛАБОРАТОРНАЯ РАБОТА № 5
«СРАВНЕНИЕ АНТИВИРУСНЫХ ПРОГРАММ»

1. Если не установлено – установить на компьютер одну из испытуемых антивирусных программ.

2. Распаковать архив с вирусами (пароль - virus).

3. Сравнить работу антивирусных программ по следующим параметрам:

- дата последнего обновления сигнатур;
- количество обнаруженных вирусов при распаковке зараженного архива;
- действия программы при обнаружении вируса;
- время сканирования;
- типы файлов, отмеченных как подозрительные;
- ложные срабатывания антивирусов (например, для программ FreePascal и Turbo Delphi).

Антивирусы для выполнения задания:

- Avira;
- Avast;
- AVG;
- NOD 32;
- Panda Cloud.