Министерство образования и науки РФ

ФГБОУ ВО «Томский государственный университет
систем управления и радиоэлектроники»
Кафедра комплексной информационной безопасности
электронно-вычислительных систем (КИБЭВС)

А.А. Конев, А.Ю. Якимук

БЕЗОПАСНОСТЬ ОПЕРАЦИОННЫХ СИСТЕМ

(Часть 1)

Лабораторный практикум
для студентов специальностей и направлений
10.03.01 – «Информационная безопасность»,
10.05.02 – «Информационная безопасность
телекоммуникационных систем»,
10.05.03 – «Информационная безопасность
автоматизированных систем»,
10.05.04 – «Информационно-аналитические системы безопасности»

В-Спектр
Томск, 2017

УДК 004.056
ББК 32.973.26-018.2
К 64

К 64 **Конев А.А., Якимук А.Ю.** Безопасность операционных систем: лабораторный практикум. Ч. 1. – Томск: В-Спектр, 2017. – 118 с.
ISBN 978-5-91191-366-3

Практикум содержит описания лабораторных работ по дисциплине «Безопасность операционных систем» для специальностей 10.05.02 – «Информационная безопасность телекоммуникационных систем», 10.05.03 – «Информационная безопасность автоматизированных систем», 10.05.04 – «Информационно-аналитические системы безопасности» и направления 10.03.01 – «Информационная безопасность», задания, методические указания по выполнению, требования по представлению отчётности, вопросы для самоконтроля.

УДК 004.056
ББК 32.973.26-018.2

Работа выполнена при финансовой поддержке Министерства образования и науки РФ в рамках базовой части государственного задания ТУСУР на 2017–2019 годы (проект № 2.8172.2017/8.9)

ISBN 978-5-91191-366-3

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Лабораторный практикум подготовлен с целью обучения студентов специальностей 10.05.02 – «Информационная безопасность телекоммуникационных систем», 10.05.03 – «Информационная безопасность автоматизированных систем», 10.05.04 – «Информационно-аналитические системы безопасности» и направления 10.03.01 – «Информационная безопасность» работе с базовыми механизмами администрирования операционных систем. Выполнив лабораторные работы, студенты приобретут умения и навыки управления функционированием и ресурсами системы и освоят ряд профессиональных компетенций по обеспечению корректной и надежной работы операционной системы.

В процессе выполнения лабораторных работ студенты используют виртуальные операционные системы, созданные для каждого из занятий. За счет использования технологии виртуализации достигается интерактивность проведения занятий. Данная технология позволяет предоставить студентам полнофункциональную тестовую учебную среду, содержащую локальную операционную систему с установленным программным обеспечением. Использование виртуализации дает ряд преимуществ, например, студент может работать с операционной системой, имея права администратора системы. Гибкость применения технологии виртуализации заключается в возможности простой интеграции учебной среды в любую компьютеризированную аудиторию. Дополнительная возможность – использование полнофункционального учебного стенда при самостоятельной работе вне вуза.

Практикум содержит в себе работы, которые позволят студентам на примере операционной системы Windows освоить основные принципы по управлению параметрами безопасности. Данная среда была выбрана ввиду высокой популярности среди пользователей и удобства в плане наглядного представления настройки систем. Почти во всех лабораторных работах данной части руководства используется Windows 10. Эта версия операционной системы позволяет изучить как технологию управления параметрами безопасности, существовавшими в старых версиях, так и добавленными после выхода Windows Vista. В лабораторной работе по восстановлению операционной системы после сбоя, действия осуществляются на базе Windows XP в связи с тем, что встроенные функции по восстановлению с выходом новых версий существенно не менялись, а средства, включенные в Hiren’s BootCD, работают во всех версиях одинаковым образом.

Помимо средств Windows в лабораторных работах применяются программные продукты Process Explorer и Process Monitor, позволяющие студентам детально ознакомиться со структурой и особенностями процессов и потоков. Кроме того, в рамках изучения методов восстановления операционной системы после сбоев изучается загрузочный диск Hiren's BootCD. Наличие данной сборки утилит избавляет своего владельца от необходимости держать при себе множество дисков с необходимыми для ежедневной работы программами.

В процессе выполнения комплекса лабораторных работ студенты в интерактивной форме освоят профессиональные компетенции, обозначенные в основной образовательной программе по данной дисциплине. Так студенты специальности 10.03.01 – «Информационная безопасность», выполняя задания по настройке политик учетных записей и групповых политик, смогут освоить компетенцию ПК-10 – способность администрировать подсистемы информационной безопасности объекта.

Обучающиеся по направлению 10.05.02 – «Информационная безопасность телекоммуникационных систем», сделав задания по шифрованию каталогов, организации дисковых квот и настройке политик безопасности, получат способность обеспечить эффективное применение средств защиты информационно-технологических ресурсов телекоммуникационных систем, что является профессиональной компетенцией ПК-33.

Выполнив те же действия, студенты специальности 10.05.03 – «Информационная безопасность автоматизированных систем» получат должные навыки по компетенции ПК-36 – способность обеспечить эффективное применение средств защиты информационно-технологических ресурсов автоматизированной системы. Кроме того, изучение мониторинга производительности и детальное рассмотрение процессов и потоков разовьют компетенцию ПК-37 – способность администрировать подсистему информационной безопасности автоматизированной системы. А выполнив лабораторную работу по восстановлению операционной системы после сбоя, освоят профессиональную компетенцию ПК-40 – способность обеспечить восстановление работоспособности систем защиты информации при возникновении нештатных ситуаций.

В свою очередь, студенты направления 10.05.04 – «Информационно-аналитические системы безопасности», рассмотрев автоматизацию выполнения административных задач и настройку политик безопасности, приобретут способность применять основные защитные механизмы и средства обеспечения безопасности операционных систем, составляющую компетенцию ПК-8.

ЛАБОРАТОРНАЯ РАБОТА №1
Администрирование Windows 10

1. Цель работы

Целью работы является освоение средств администрирования учётных записей пользователей и групп пользователей в ОС Windows 8, изучение основных параметров, определяющих взаимодействие пользователей с операционной системой, консолью управления и групповой политикой.

2. Краткие теоретические сведения

В операционной системе Windows 10 существует 2 группы пользователей:

– локальные учетные записи;

– учетные записи Microsoft.

Первая группа называется локальной, по причине того, что аутентификация происходит на локальном компьютере. Все учетные данные необходимые для этого (имя пользователя, пароль и параметры учетной записи) хранятся в нем.

В случае работы с учетной записью Microsoft — аутентификация пользователей происходит на сервере сети, то есть удаленно. Преимущество данного способа в том, что любой сотрудник предприятия может зайти в сеть с любого компьютера, а не только с закрепленного за ним. Сервер хранит все параметры пользователя, а также при необходимости и документы, с которыми он работает. Однако второй тип пользователей имеет свой недостаток – при отсутствии интернет-соединения или коммутируемом (не устанавливаемом автоматически) соединении аутентификация будет невозможна.

Локальные учетные записи бывают трех видов:

– учетная запись администратора, создаваемая при установке системы и используемая при изменении параметров системы;

– учетная запись пользователя, позволяющая использовать установленные администратором из внешних источников программы и изменять параметры персонализации;

– гостевая учетная запись.

Консоль управления Microsoft Management Console (MMC) – это компонент операционных систем семейства Windows NT, предоставляющий администраторам графический интерфейс для настройки системных приложений и прикладных программ.

Оснастка – компонент для MMC, включающий набор параметров какого-либо модуля операционной системы (файловой системы, управления пользователями и т.д.) или прикладного приложения.

Набор параметров для прикладных программ может быть добавлен в оснастку при помощи административных шаблонов – особым образом структурированных файлов с расширением *.adm.

Групповая политика – это набор правил или настроек, в соответствии с которыми производится настройка рабочей среды Windows.

3. Ход работы

3.1. Управление учётными записями локальных пользователей

Рассмотрите механизм работы с учетными записями пользователей, предлагаемых Windows 10. Для этого через меню «Пуск» перейдите к параметрам системы (рис. 1).

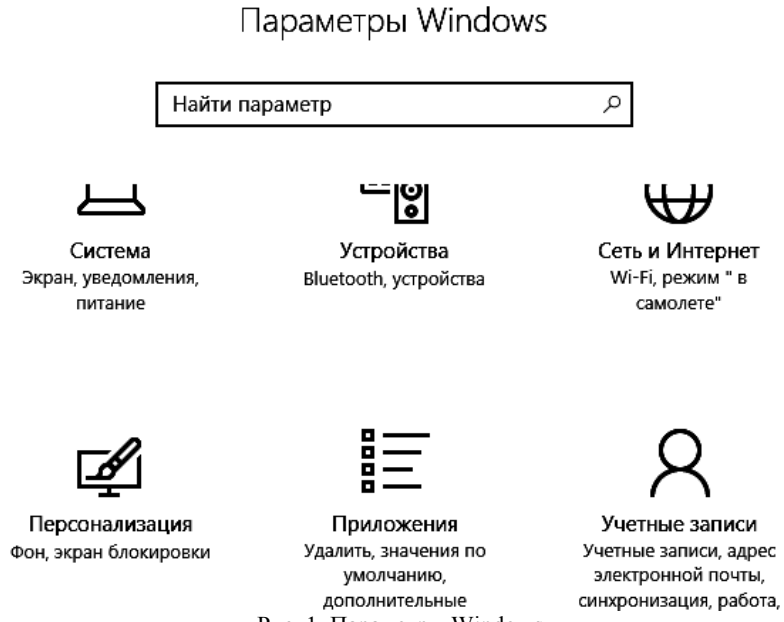

Рис. 1. Параметры Windows

Перейдите в раздел «Учётные записи». В данном разделе будет представлена информация о том, под какой учетной записью был осуществлен вход, представлены функции по изменению параметров входа, представлены учетные записи на данном компьютере (если таковые имеются) и предложено создать новых пользователей (рис. 2).

Рис. 2. Вкладка управления пользователями

Перейдите во вкладку «Семья и другие люди», нажмите на «Добавить нового пользователя для этого компьютера». В результате поступит предложение ввести электронный адрес или номер телефона для авторизации. Чтобы добавить локального пользователя нажмите на «У меня нет данных для данного человека» (рис. 3).

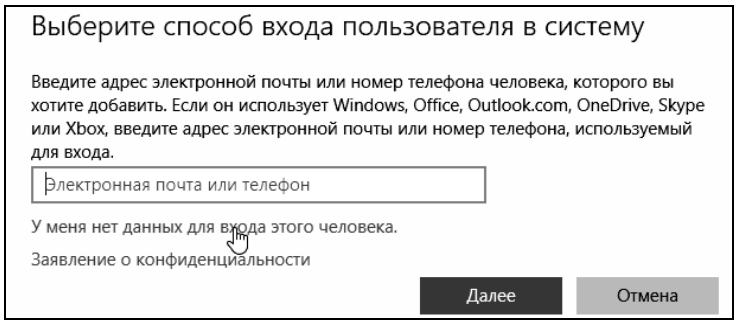

Рис. 3. Выбор способа входа в систему

Потом кликните по надписи: «Добавить пользователя без учётной записи» (рис. 4).

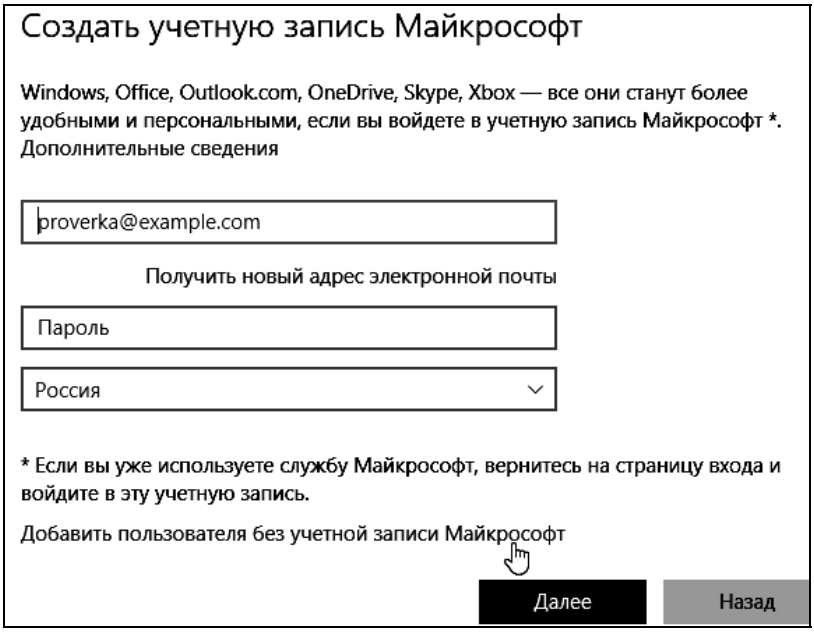

Рис. 4. Добавление локального пользователя

После этого потребуется задать имя пользователя и пароль для него, а также подсказку для пароля. После завершения создания пользователя – соответствующая запись появится в перечне учетных записей на данном компьютере.

Запустите Microsoft Management Console (mmc) – компонент Windows, позволяющий администрировать систему. Откройте меню «Пуск – Выполнить – mmc». Для добавления необходимого набора оснасток в меню консоли выберите «Файл – Добавить или удалить оснастку». В результате будет предложен перечень, из которого пользователь может выбрать одну или несколько оснасток.

Нажмите «Файл» и перейдите в пункт «Параметры». Здесь можно выбрать режим работы пользователя с этой консолью: авторский режим, предоставляющий пользователю полный доступ ко всем функциям MMC, и пользовательский режим.

Существует три вида пользовательского режима:

– полный доступ (full access) даёт пользователю доступ ко всем командам MMC, но не позволяет добавлять или удалять оснастки, или изменять свойства консоли;

– ограниченный доступ, много окон (Limited Access Multiple Windows) позволяет пользователю осуществлять доступ только к областям дерева консоли, которые отображались при сохранении консоли, а также открывать новые окна;

– ограниченный доступ, одно окно (Limited Access Single Window) работает так же, как многооконный ограниченный доступ с той разницей, что пользователь не может открывать новые окна.

Сохраните консоль в авторском и пользовательских режимах (рис. 5). Выявите отличия работы консоли в различных режимах.

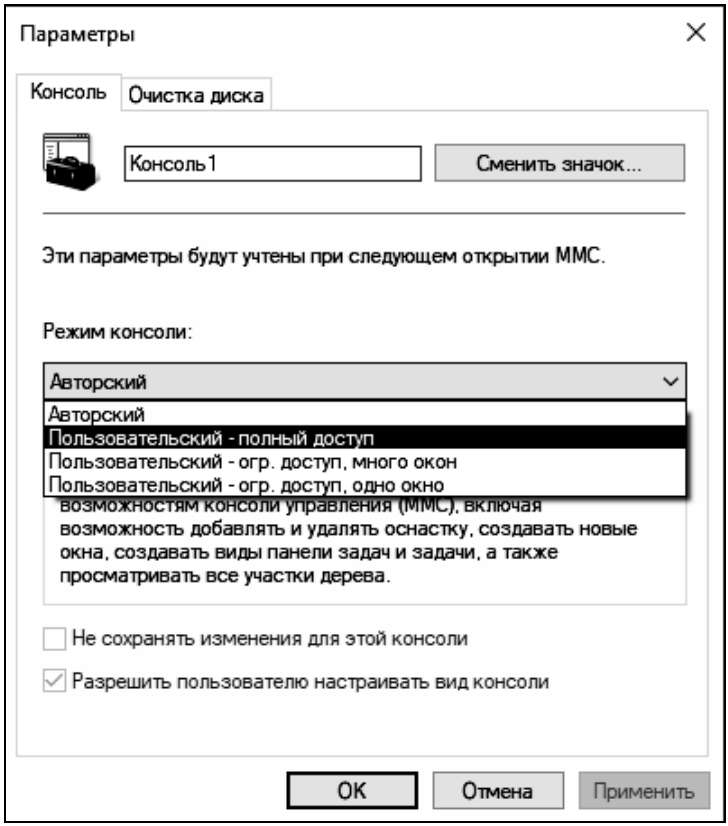

Рис. 5. Параметры режима консоли

Через пункт «Добавить или удалить оснастку» добавьте «Локальные пользователи и группы» (рис. 6).

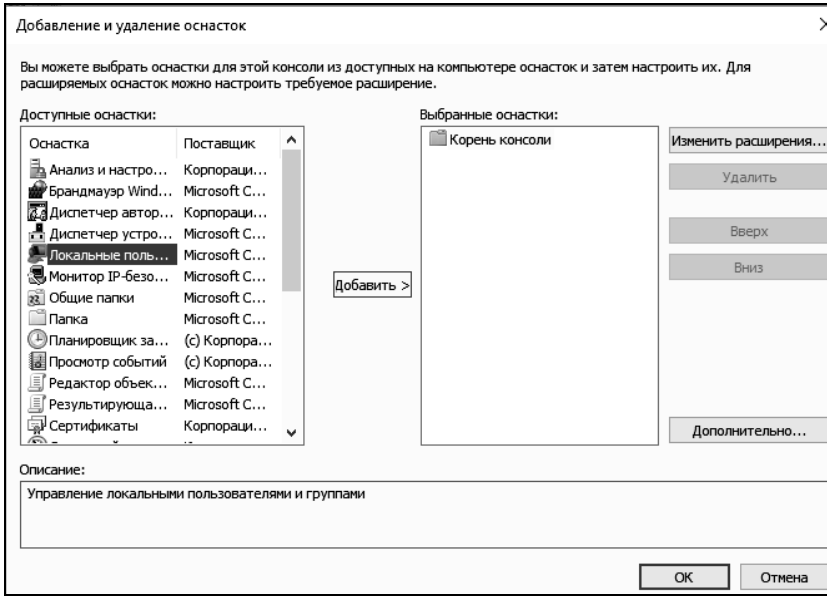

Рис. 6. Добавление оснастки

Через данную оснастку также возможно добавить нового пользователя (рис. 7).

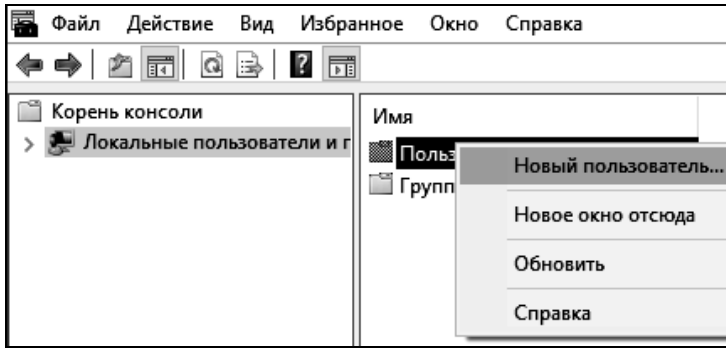

Рис. 7. Добавление пользователя через оснастку

В появившемся окне (рис. 8) введите имя учётной записи, а также пароль и его подтверждение. Если администратор устанавливает пользователю временный пароль, то для обязательной смены пароля необходимо включить параметр «Потребовать смену пароля при следующем входе в систему». Сразу после успешной аутентификации пользователь

получает запрос на смену пароля, в ответ на который он должен задать новый пароль. Этот подход необходимо использовать в тех случаях, когда администратор системы не должен знать пароли пользователей.

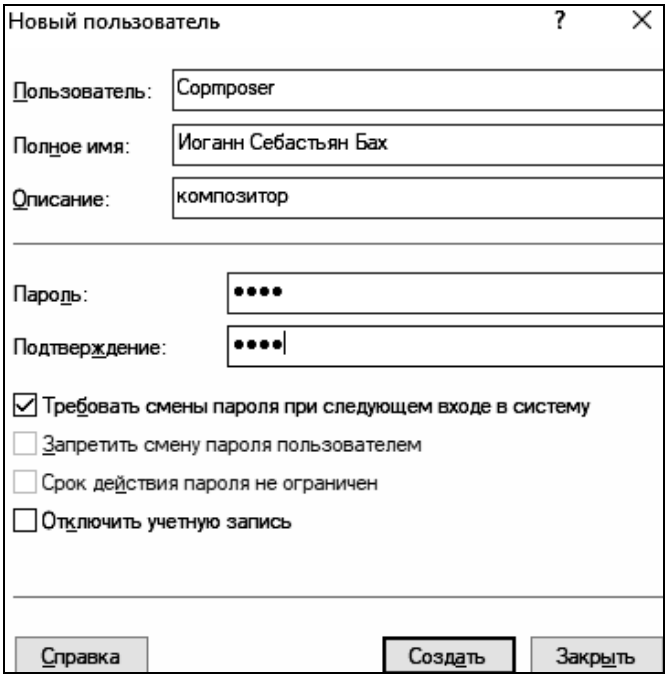

Рис. 8. Настройка параметров учётной записи при её создании

Если пользователь забыл свой пароль, то член группы «Администраторы» может сбросить его старый пароль при помощи функции «Задать пароль», доступной в контекстном меню учётной записи этого пользователя (рис. 8). Смените пароль у созданной учётной записи.

В данный момент времени учетная запись «Администратор» является заблокированной (рис. 10). Разблокируйте её, выбрав соответствующий пункт в свойствах учетной записи. Посмотрите какие еще параметры можно настроить через свойства.

Войдите в систему под созданной учётной записью. При первом входе пользователю будет выдано сообщение о необходимости ввести пароль (рис. 11) и окно смены пароля (рис. 12). Смените пароль созданной учётной записи. Здесь подтверждение действий осуществляется клавишей «Enter».

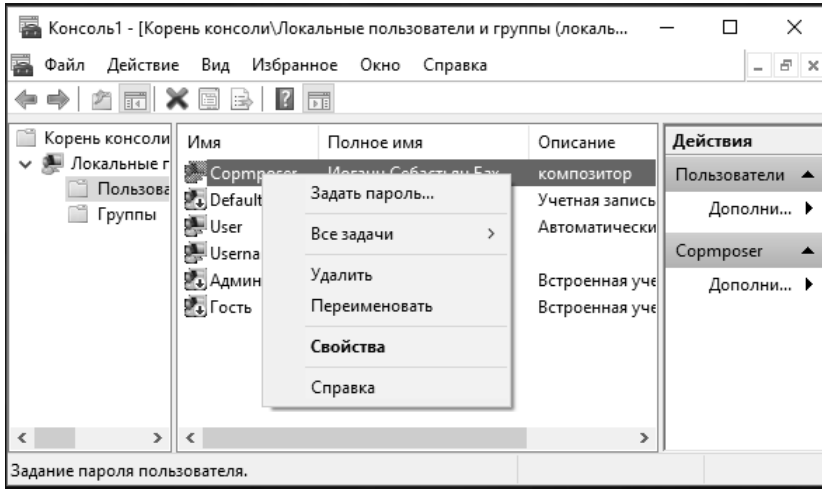

Рис. 9. Задание пароля пользователя администратором

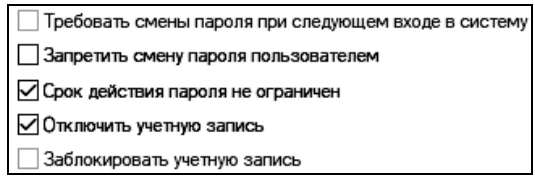

Рис. 10. Изменение свойств администратора

Рис. 11. Сообщение пользователю о необходимости смены пароля

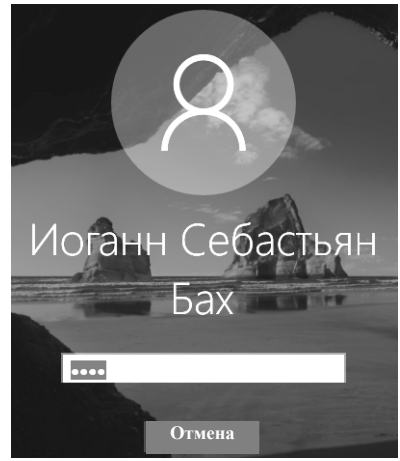

Рис. 12. Окно «Смена пароля»

Для применения к пользователю набора прав и ограничений можно включить его учётную запись в группу пользователей с соответствующим набором прав и ограничений.

Войдите в систему под учётной записью «Администратор». Откройте «Свойства» созданной учётной записи. На вкладке «Членство в группах» добавьте пользователя в группу «Опытные пользователи» (рис. 13). Имя группы можно ввести самостоятельно или выбрать из списка, предоставляемого после последовательного нажатия кнопок «Дополнительно» и «Поиск».

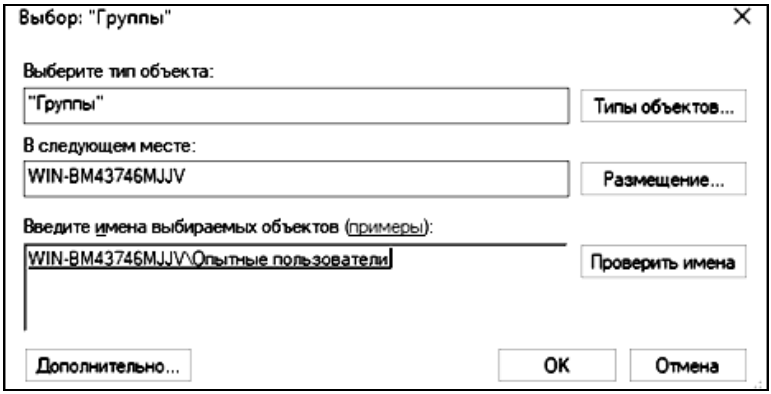

Рис. 13. Добавление группы

В разделе «Группы» откройте «Свойства» группы «Опытные пользователи» и проверьте наличие в группе добавленной учётной записи. Создайте новую группу и добавьте в неё этого же пользователя.

Вызовите командную строку и выполните команду «net user». Консоль выведет перечень всех имеющихся учетных записей (рис. 14)

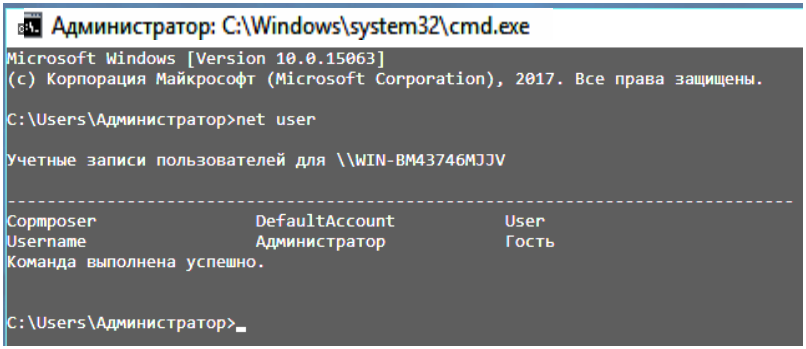

Рис. 14. Список пользователей в командной строке

Создание и изменение учётных записей осуществляется при помощи команды «net user». Подробную информацию о команде можно получить, введя «net user /help» (рис. 15). Изучите предлагаемые функции команды.

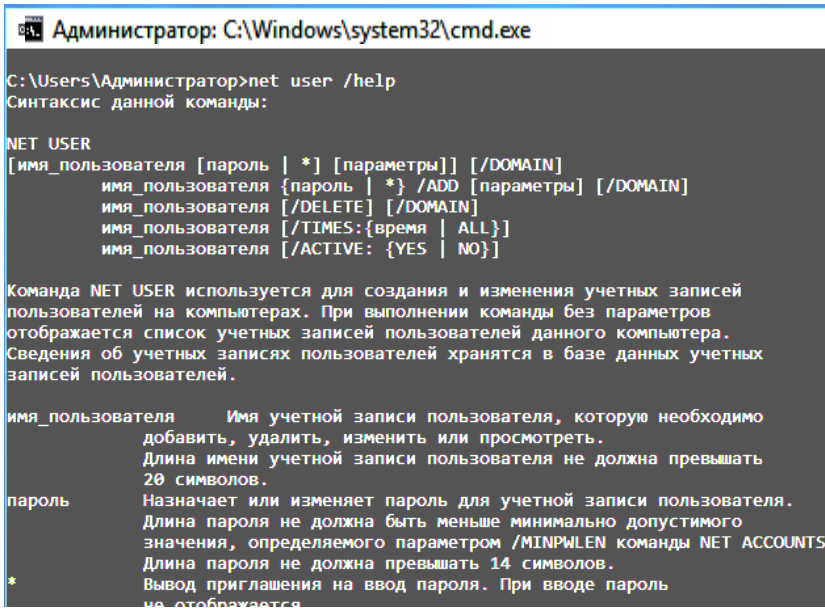

Рис. 15. Справка по команде Net user

Создайте учётную запись пользователя с именем, совпадающим с Вашим именем в кафедральной сети, явно указав пароль. При создании дополнительно к логину укажите полное имя пользователя (рис. 16).

Синтаксис команды Net user при создании учётной записи пользователя:

Net user имя_пользователя {пароль | *} /ADD [параметры].

Для добавления полного имени пользователя нужно в качестве параметра ввести: /FULLNAME: «имя».

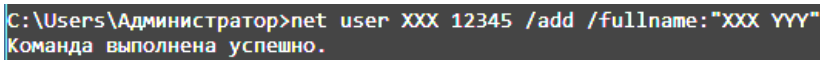

Рис. 16. Создание нового пользователя

Проверьте наличие созданной учётной записи в списке пользователей при помощи команды Net user. Команда Net user имя_пользователя, введённая без параметров, позволяет просмотреть информа-

цию об указанном пользователе. Просмотрите информацию о созданной учетной записи.

Возможен ввод пароля без отображения на экране – для этого вместо пароля нужно ввести «*». Измените пароль созданного пользователя при помощи команды Net user имя_пользователя * (рис. 17).

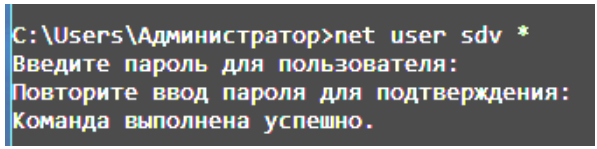

Рис. 17. Изменение пароля пользователя

Существует возможность установки ограничений на работу пользователя в операционной системе по времени. Для этого используется параметр /TIMES:{промежуток | ALL}. Значение ALL указывает, что пользователь может войти в систему в любое время, а пустое значение указывает, что пользователь не может войти в систему никогда. Ограничьте время работы созданного пользователя рамками рабочего времени (рис. 18). Переведите часы на время, не входящее в интервал рабочего, и протестируйте возможность входа пользователя в операционную систему.

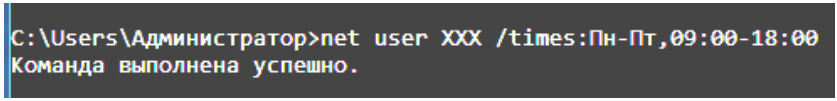

Рис. 18. Задание интервала действия учетной записи

В случае необходимости администратор может заблокировать учётную запись пользователя. Заблокируйте учётную запись созданного пользователя при помощи параметра /ACTIVE:{YES | NO} (рис. 19).

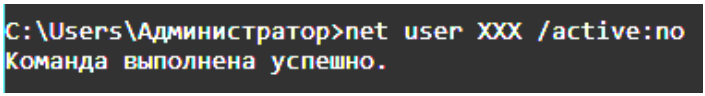

Рис. 19. Блокирование учетной записи

Проверьте применение блокирования к учётной записи при помощи команды Net user имя_пользователя. В выдаваемой о пользователе информации есть графа «Учётная запись активна», показывающая состояние блокирования учётной записи. Разблокируйте учётную запись пользователя.

Если пользователь временно работает в организации, то администратор может ограничить время действия учётной записи пользователя. Для этого служит параметр: /EXPIRES:{дата | NEVER}. Если используется значение NEVER, то время действия учётной записи не имеет ограничений срока действия. Ограничьте время действия учётной записи созданного пользователя (рис. 20). Установите системное время на срок более поздний, чем установленное ограничение. Попытайтесь войти в систему под данной учётной записью – операционная система выдаст ошибку (рис. 21).

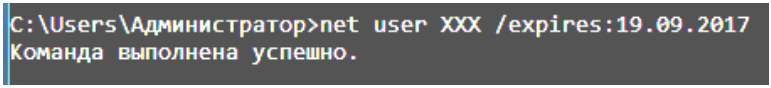

Рис. 20. Ограничение времени действия учётной записи

Рис. 21. Ошибка при попытке входа под просроченной учётной записью

Команда Net localgroup служит для создания локальных групп и управления ими. При использовании этой команды без указания параметров выводится перечень групп пользователей, существующих в операционной системе (рис. 22). Выведите список всех существующих групп.

Синтаксис команды Net net при создании локальной группы: Net localgroup имя_группы {/ADD }. Создайте локальную группу Students (рис. 23).

Проверьте наличие созданной группы пользователей при помощи команды Net localgroup. Добавление пользователей в группу осуществляется командой Net localgroup имя_группы имя [...] {/ADD }, где имя [...] – имя одного или нескольких пользователей (имена разделяются пробелами).

Добавьте ранее созданного пользователя в группу Students. Команда Net localgroup имя_группы выводит список пользователей, входящих в указанную группу. Выведите список пользователей группы Students (рис. 24).

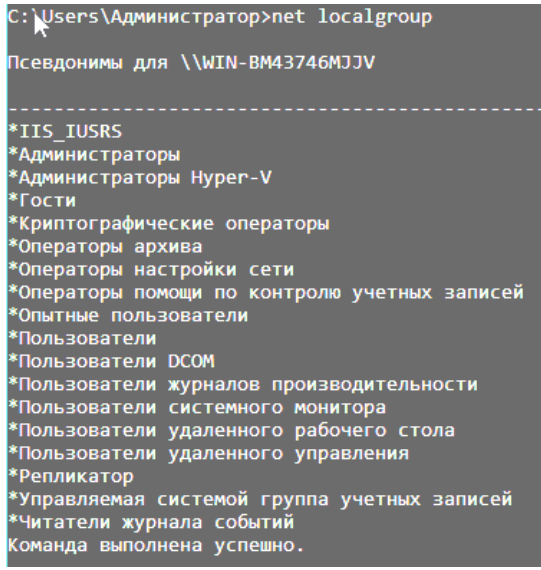

Рис. 22. Список групп

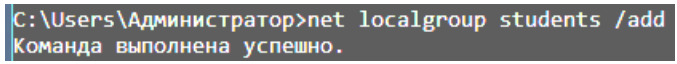

Рис. 23. Создание группы

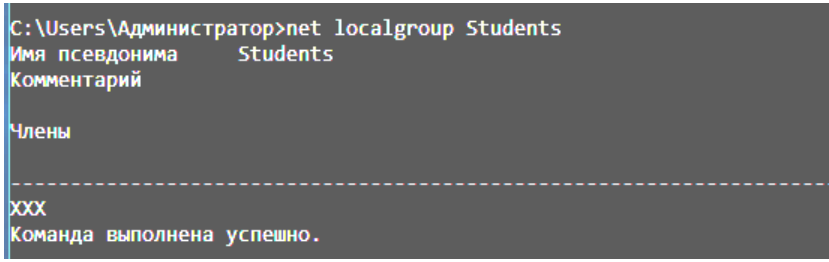

Рис. 24. Просмотр списка пользователей заданной группы

Для удаления пользователя из группы используется команда Net localgroup имя_группы имя_пользователя {/DELETE}. Удалите группу Students (рис. 25).

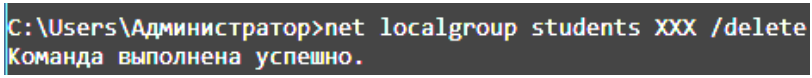

Рис. 25. Исключение пользователя из группы

Для удаления группы используется команда Net localgroup имя_группы {/DELETE}. Удалите группу Students (рис. 26).

```
C:\Users\Администратор>net localgroup students /delete
Команда выполнена успешно.
```

Рис. 26. Удаление группы пользователей

Проверьте отсутствие группы Students, используя команду вывода списка существующих групп пользователей.

3.2. Настройка политики учётной записи

Откройте «Локальную политику безопасности», вызвав её запросом secpol.msc в меню «Пуск». Основное окно «Локальной политики безопасности» представлено на рисунке 27. Значения параметров, заданные при настройке политики, будут применяться ко всем пользователям локального компьютера.

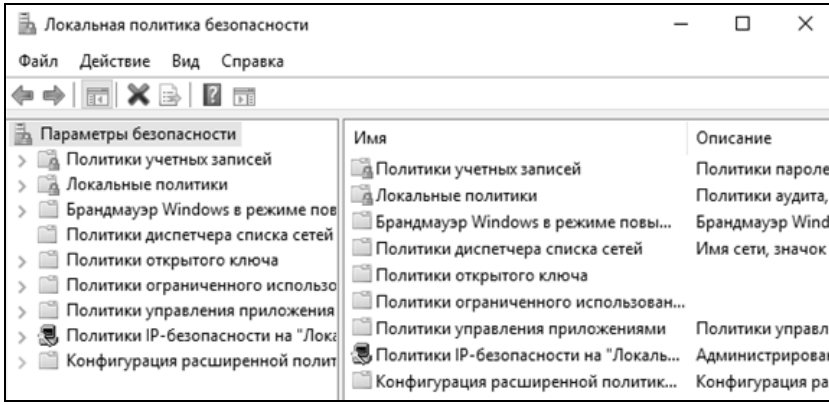

Рис. 27. Локальная политика безопасности

Раздел «Политики учётных записей» «Локальной политики безопасности» включает в себя настройки, применяющиеся к паролям пользователей.

Выберите раздел «Политика паролей» («Параметры безопасности – Политики учётных записей – Политика паролей»). Настройки, входящие в раздел «Политика паролей», представлены на рис. 28.

Выполните следующие задания:

– установите максимальный срок действия пароля – 30 дней;

– установите минимальную длину пароля – 10 символов;

– для параметра «Вести журнал паролей» установите значение 3 хранимых пароля, означающее, что новый пароль должен отличаться от 3 последних паролей пользователя;

– включите параметр «Пароль должен отвечать требованиям сложности».

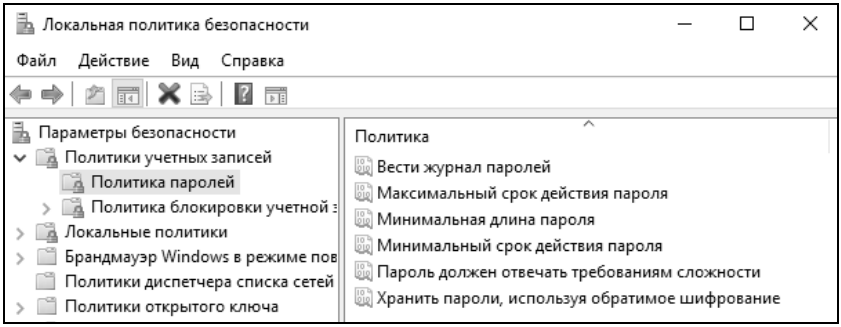

Рис. 28. Политика паролей

Параметр «Пароль должен отвечать требованиям сложности» определяет требования сложности для паролей. Если эта политика включена, то пароли должны удовлетворять следующим минимальным требованиям:

– пароль не может содержать имя учётной записи пользователя или какую-либо его часть;

– пароль должен состоять не менее чем из шести символов;

– в пароле должны присутствовать символы трёх категорий из числа следующих четырёх:

а) прописные буквы английского алфавита от A до Z;

б) строчные буквы английского алфавита от a до z;

в) десятичные цифры (от 0 до 9);

г) неалфавитные символы (например !, $, #, %).

Проверка соблюдения этих требований выполняется при изменении или создании паролей. При помощи этого параметра можно избавиться от легко подбираемых паролей типа «111», «qwerty», «12345» и т.д.

Убедитесь, что для пользователя не включена опция «Срок действия пароля неограничен» в оснастке «Локальные пользователи и группы». Переведите системное время более чем на 30 дней вперёд. Попытайтесь войти под созданной учётной записью. Пользователю будет выдано сообщение об истечении срока действия пароля (рис. 29). При сме-

не пароля попытайтесь заменить пароль на более простой (например, abc12345 или включающий имя учётной записи).

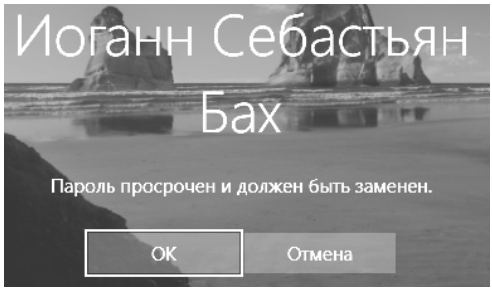

Рис. 29. Сообщение об истечении срока действия пароля

В этом случае пользователю будет выдано сообщение об ошибке при смене пароля (рис. 30). Введите пароль, удовлетворяющий требованиям.

Рис. 30. Сообщение о несоответствии пароля требованиям

Войдите в систему под учётной записью «Администратор». Переведите системное время в исходное состояние. Выберите раздел «Политика блокировки учётной записи» («Параметры безопасности – Политики учётных записей – Политика блокировки учётной записи»). Настройки, входящие в раздел «Политика блокировки учётной записи», представлены на рисунке 31.

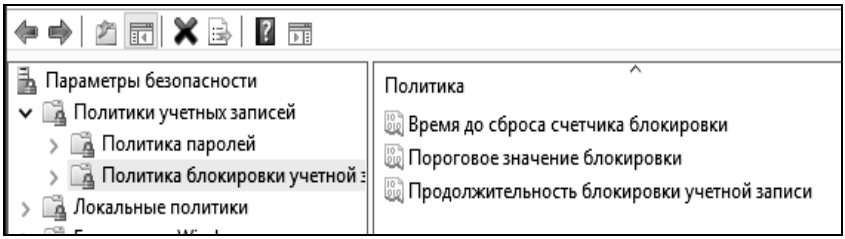

Рис. 31. Политика блокировки учетной записи

Настройте параметры следующим образом:

– установить пороговое значение блокировки, равное 3 ошибкам входа в систему (после 3 неудачных попыток входа учётная запись блокируется);

– установить длительность блокировки в параметре «Блокировка учётной записи на», равную 30 мин (значение 0 означает, что блокировку может снять только администратор);

– установите сброс счётчика блокировки через 15 мин. Если в течение установленного времени будет 3 неудачных попытки входа, то учётная запись блокируется. Если неудачных попыток в течение установленного времени будет меньше, то опять допускается 3 неудачных попытки (значение этого параметра не должно превышать длительность блокировки учётной записи).

Завершите сеанс учётной записи «Администратор». При входе в систему под созданной учётной записью три раза введите неправильный пароль. При следующей попытке входа в систему будет выдано сообщение о блокировании созданной учётной записи (рис. 32).

Рис. 32. Сообщение о блокировке учетной записи

Войдите в систему под учётной записью «Администратор». Разблокируйте созданную учётную запись. Для этого в окне «Свойства» этой учётной записи отключите настройку «Заблокировать учётную запись».

Вызовите командную строку. Net accounts используется для обновления базы данных регистрационных записей и изменения параметров входа в сеть (LOGON) и требований к паролям для всех регистрационных записей. При использовании этой команды без указания параметров выводятся текущие значения параметров, определяющих требования к паролям и другие параметры. Выведите текущие параметры входа в систему (рис. 33).

Задайте следующие требования к паролю:

– минимальную длину – 6 символов;

– максимальный срок действия пароля – 40 дней;

– запрет использования 3 последних паролей пользователя.

```
C:\Users\Администратор>net accounts
Принудительный выход по истечении времени через:        Никогда
Минимальный срок действия пароля (дней):                0
Максимальный срок действия пароля (дней):               10
Минимальная длина пароля:                               10
Хранение неповторяющихся паролей:                       3
Блокировка после ошибок ввода пароля:                   3
Длительность блокировки (минут):                        30
Сброс счетчика блокировок через (минут):                15
Роль компьютера:                                        РАБОЧАЯ СТАНЦИЯ
Команда выполнена успешно.
```

Рис. 33. Просмотр информации о требованиях к качеству паролей

Применение этих требований (рис. 34) производится при помощи следующих параметров команды Net accounts:

/MINPWLEN:длина

/MAXPWAGE:дни

/UNIQUEPW:число

```
C:\Users\Администратор>net accounts /minpwlen:6 /maxpwage:40 /uniquepw:3
Команда выполнена успешно.
```

Рис. 34. Изменение требований к качеству паролей

3.3. Групповые политики

Откройте оснастку «Групповая политика» («Пуск – Выполнить – gpedit.msc»). Оснастка «Групповая политика» состоит из двух основных частей: конфигурация компьютера и конфигурация пользователя (рис. 35).

«Конфигурация компьютера» используется для задания политики, применяемой к компьютерам, вне зависимости от того, какой пользователь работает на них. «Конфигурация пользователя» используется для задания политики, применяемой к пользователям независимо от того, какой компьютер используется для входа в систему.

Созданная групповая политика может быть экспортирована на другой локальный компьютер. Для того чтобы произвести экспорт данных необходимо в оснастке «Групповая политика» выделить нужный узел и во вкладке «Действие» выбрать пункт «Экспортировать список». В появившемся окне выбрать путь сохранения и указать имя файла.

«Конфигурация компьютера» по умолчанию состоит из следующих разделов: конфигурация программ, конфигурация Windows и административные шаблоны (рис. 36).

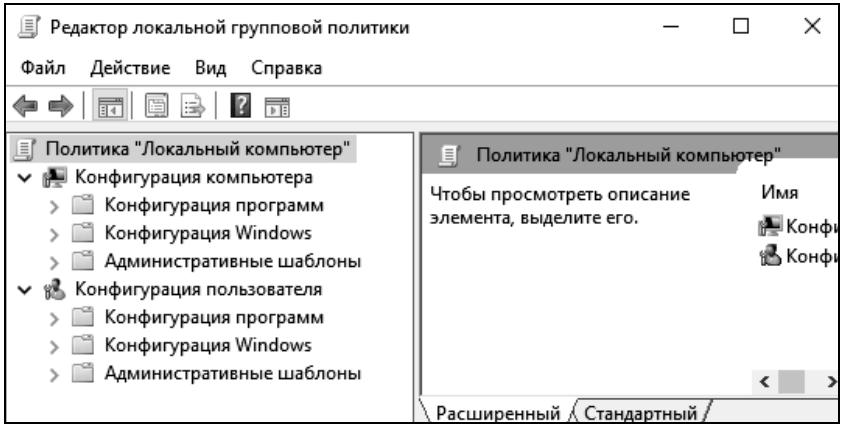

Рис. 35. Редактор групповых политик

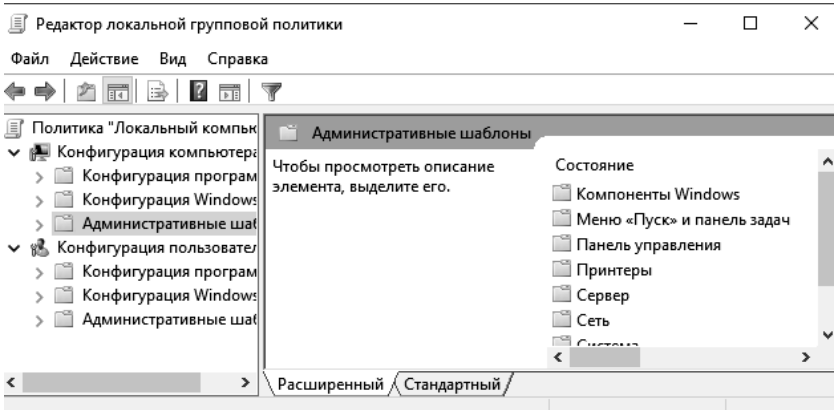

Рис. 36. Раздел «Административные шаблоны»

Средствами виртуальной машины подключите компакт-диск. В разделе «Административные шаблоны» выберите подраздел «Компоненты Windows» – «Политики автозапуска». Включите параметр «Выключение автозапуска» (рис. 37). Чтобы проверить выполнение данного параметра, необходимо повторно вставить диск в CD-привод. Система не будет производить его автозапуск, как это делалось раньше.

В разделе «Система» откройте подраздел «Вход в систему» и выберите параметр «Выполнять эти программы при входе в систему». Включите этот параметр и добавьте несколько программ, которые будут запускаться при входе пользователя в систему (рис. 38).

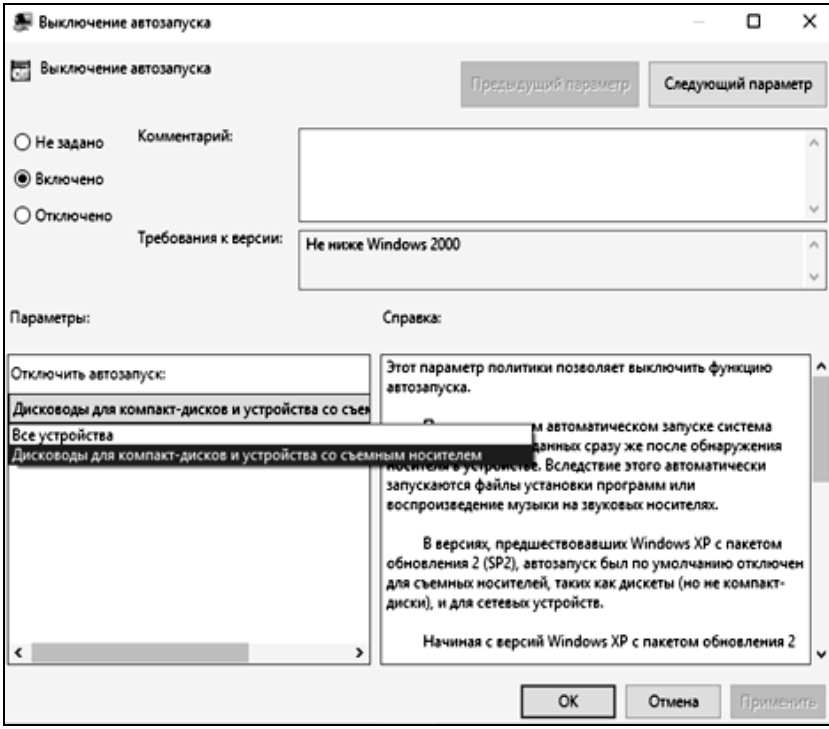

Рис. 37. Выключение автозапуска носителя

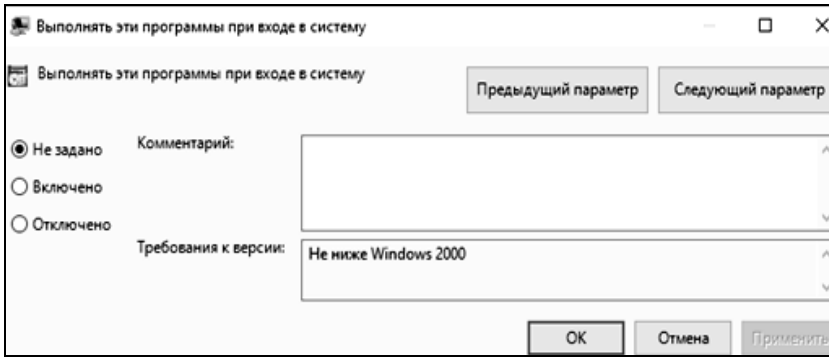

Рис. 38. Включение параметра

Добавленные программы (рис. 39) будут запускаться при каждом входе пользователя в систему. Для проверки повторно войдите в систему.

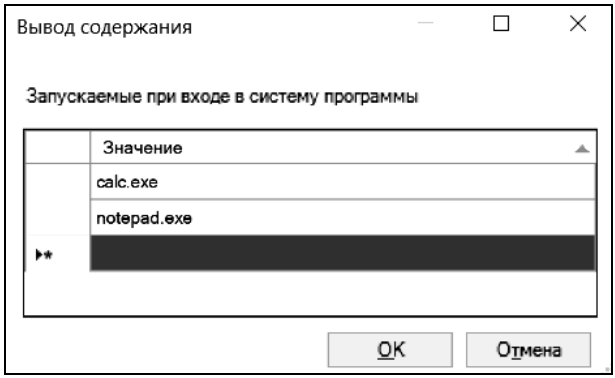

Рис. 39. Список запускаемых программ

«Конфигурация пользователя» по умолчанию состоит из тех же разделов, что и «Конфигурация компьютера». При помощи параметров групповой политики существует возможность ограничения доступа пользователя к логическим дискам. Можно скрыть выбранный диск из «Проводника», а также запретить доступ к нему.

Выберите параметр «Запретить доступ к дискам через «Мой компьютер», расположенный в подразделе «Компоненты Windows – Проводник» и запретите доступ к логическому диску C:\ (рис. 40).

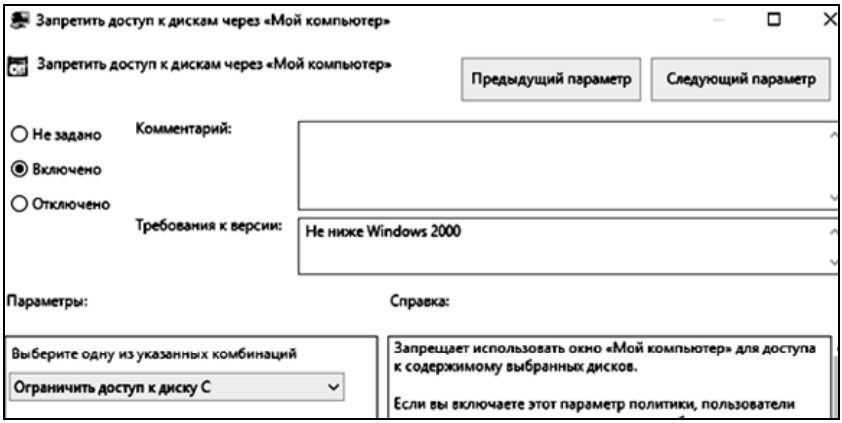

Рис. 40. Включение ограничения доступа к диску D

Попытайтесь открыть диск D:\ через «Мой компьютер» (рис. 41) и командную строку (рис. 42). В первом случае система откажет в дос-

тупе, а во втором – доступ будет предоставлен (т.к. доступ запрещён только через «Проводник»).

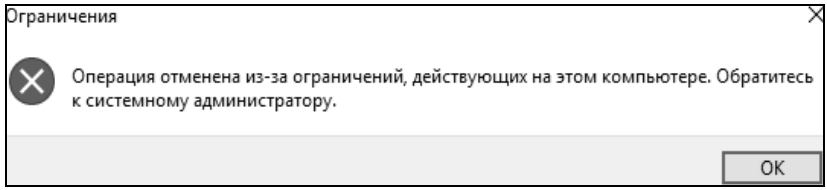

Рис. 41. Попытка доступа через проводник

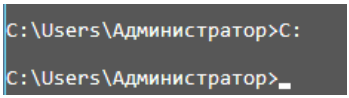

Рис. 42. Попытка доступа через командную строку

Ограничение доступа к средствам администрирования возможно за счёт запрета доступа к «Панели управления». Включите параметр «Запретить доступ к панели управления», находящийся в подразделе «Панель управления» (рис. 43). Попытайтесь открыть «Панель управления».

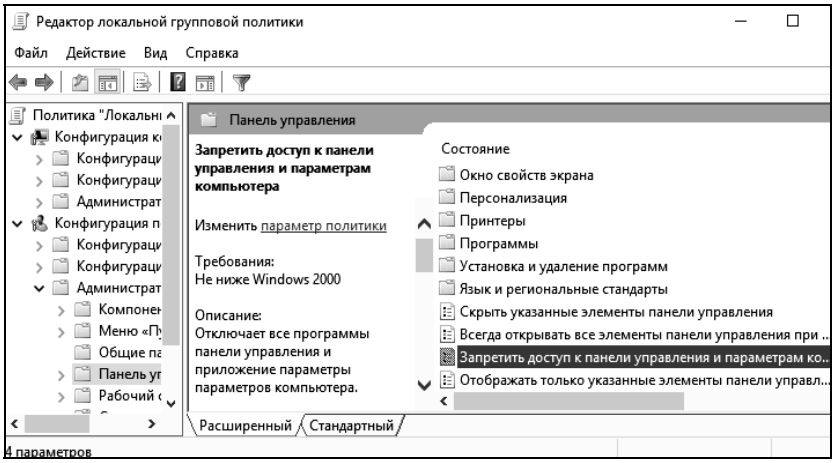

Рис. 43. Ошибка при открытии панели управления

Для полного запрета использования командной строки включите параметр «Запретить использование командной строки» в подразделе «Система». Попытайтесь запустить cmd.exe (рис. 44).

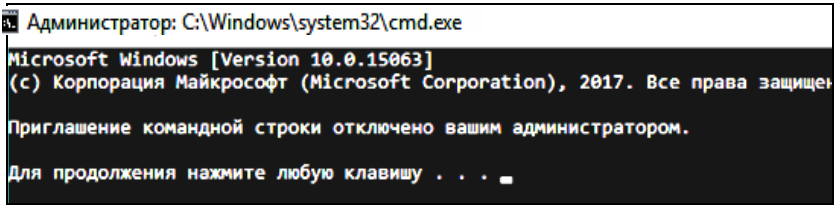

Рис. 44. Попытка запуска командной строки

Кроме того, в подразделе «Система» можно запретить использование редактора реестра. Для этого нужно включить параметр «Сделать недоступными средства редактирования реестра». Включите данный параметр и попытайтесь запустить редактор реестра C:\Windows\regedit.exe.

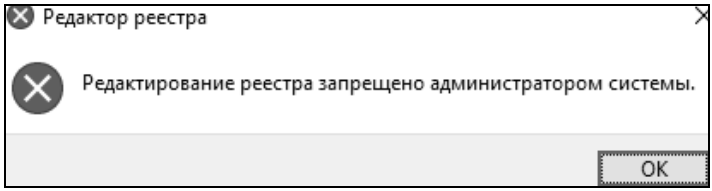

Рис. 45. Попытка запуска реестра

Добавление и удаление шаблонов может производиться через контекстное меню раздела «Административные шаблоны» (рис. 46). В появившемся контекстном меню выберите «Добавление и удаление шаблонов». В появившемся окне можно удалить любой шаблон, а также добавить новый шаблон политики.

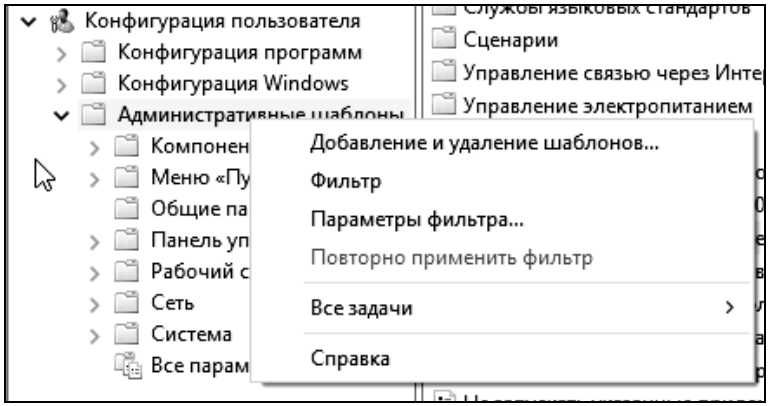

Рис. 46. Контекстное меню административных шаблонов

4. Задание на лабораторную работу

1. Ознакомьтесь с теорией.
2. Выполните представленные задания и составьте по проделанной работе отчет.
3. В оснастке «Локальные пользователи и группы» создайте новую группу пользователей. В качестве имени группы пользователей используйте номер Вашей учебной группы.
4. Создайте учётную запись с именем Вашей учётной записи в кафедральной сети и включите её в созданную группу.
5. Примените к созданной учётной записи настройки, указанные в Вашем варианте (табл. 1).
6. Создайте новую консоль. Добавьте в корень консоли оснастки «Редактор объекта групповой политики» и «Результирующая политика». Сохраните консоль в режиме, указанном в Вашем варианте (табл. 2.).

Таблица 1

Варианты заданий работы с пользователями

Параметр \ Вариант	1	2	3	4	5	6	7	8	9	10
Максимальный срок действия пароля	30	90	60	30	90	60	30	90	60	30
Минимальная длина пароля	6	7	8	9	10	6	7	8	9	10
Требовать неповторяемости паролей	6	5	4	3	2	6	5	4	3	2
Отвечать требованиям сложности	+	–	–	+	–	–	+	–	+	+
Пороговое значение блокировки	3	4	5	6	7	3	4	5	6	7
Блокировка учётной записи на…	10	20	30	45	60	10	20	30	45	60
Сброс счётчика блокировки через…	5	10	15	20	30	10	20	30	45	60
Завершение работы системы	+	+			+		+		+	
Локальный вход в систему	+	+	+	+	+	+	+	+	+	+
Изменение системного времени	+		+		+		+		+	

Таблица 2

Варианты работы с групповыми политиками

Вар.	Режим работы с консолью	Параметры групповой политики
1	*2*	*3*
1	Авторский	Запретить редактирование реестра. Ограничить размер профиля пользователя значением 5 МБ
2	Пользовательский – полный доступ	Запретить использование командной строки. Запретить изменение рисунка рабочего стола
3	Пользовательский – многооконный	Запретить использование сочетаний клавиш, включающих кнопку «Windows». Удалить имя пользователя из меню «Пуск»

Продолжение табл. 2

1	2	3
4	Пользовательский – однооконный	Запретить использование диспетчера задач. Установить обязательный запрос пароля при выходе из спящего режима
5	Авторский	Запретить доступ к «Панели управления». Запретить запуск «Блокнота»
6	Пользовательский – полный доступ	Установить обязательный запрос пароля при выходе из экранной заставки. Удалить «Завершение сеанса» из меню «Пуск»
7	Пользовательский – многооконный	Скройте диск D: (CD-привод) из окна «Мой компьютер». Удалить значок «Мои документы» с «Рабочего стола»
8	Пользовательский – однооконный	Удалите «Общие документы» из окна «Мой компьютер». Скрыть общие группы программ из меню «Пуск»
9	Авторский	Запретите доступ к диску C: из окна «Мой компьютер». Удалить «Сетевые подключения» из меню «Пуск»
10	Пользовательский – полный доступ	Запретить вызов «Свойств» объекта «Мой компьютер». Установить очистку списка последних использовавшихся документов при выходе из системы

7. Установите параметры групповой политики, указанные в Вашем варианте (табл. 2), и продемонстрируйте преподавателю результат применения параметров (например, невозможность запуска редактора реестра).

8. Продемонстрируйте преподавателю изменённые параметры при помощи «Результирующей политики» для пользователя «user».

5. Контрольные вопросы

1. Поясните параметр «Пароль должен отвечать требованиям сложности» и перечислите минимальные требования, которым должны удовлетворять пароли, если параметр включен.

2. Какие параметры входят в политику блокировки учётной записи?

3. Возможно ли, что учётная запись не будет блокирована при количестве ошибок большем, чем установленное пороговое значение?

4. Что такое и для чего применяется MMC?

5. Что такое оснастка?

6. В чём состоит отличие конфигурации компьютера от конфигурации пользователя в групповой политике?

7. Каким образом можно включить автозапуск программ через групповую политику?

8. При помощи какой команды можно получить список пользователей операционной системы?

9. При помощи какой команды можно получить список групп пользователей операционной системы?

10. При помощи какой команды можно создать нового пользователя?

ЛАБОРАТОРНАЯ РАБОТА №2
Управление системными службами и процессами Windows

1. Цель работы

Целью работы является освоение способов управления службами в ОС Windows 10, изучение специфики работы планировщика задач, а также ознакомление со структурой и особенностями работы процессов и потоков в операционных системах.

2. Краткие теоретические сведения

Служба Windows – программа или процесс, который выполняется в фоновом режиме, т.е. без прямого общения с пользователем, и обеспечивает поддержку других программ. Службы могут запускаться при загрузке операционной системы и находиться в оперативной памяти вплоть до завершения работы. Каждая служба имеет определённые характеристики: тип запуска, условия восстановления и другие, которые будут рассмотрены ниже.

Параметры настройки служб хранятся в реестре Windows.

Процесс services.exe, запущенный от имени пользователя SYSTEM, отвечает за запуск, остановку и управление службами. Services.exe автоматически запускает службы во время загрузки ОС и останавливает все службы при завершении работы Windows. Другое название этого процесса – диспетчер управления службами (Service control manager, SCM).

Отдельные службы запускаются в процессе svchost.exe, который является дочерним для services.exe. На компьютере может быть запущено несколько экземпляров процесса svchost.exe, при этом каждый из них содержит различные службы. Один экземпляр процесса svchost.exe может содержать одну службу для программы, а другой – несколько служб, относящихся к работе Windows.

Не только система, но и сам пользователь может управлять службами. В Windows предусмотрено управление службами через графический интерфейс и через командную строку, а также при помощи изменения ключей реестра.

3. Ход работы

3.1. Управление службами

Запустите диспетчер задач, нажав Ctrl+Alt+Del. Перейдите на вкладку «Службы» (рис. 1), чтобы увидеть все службы, установленные в операционной системе.

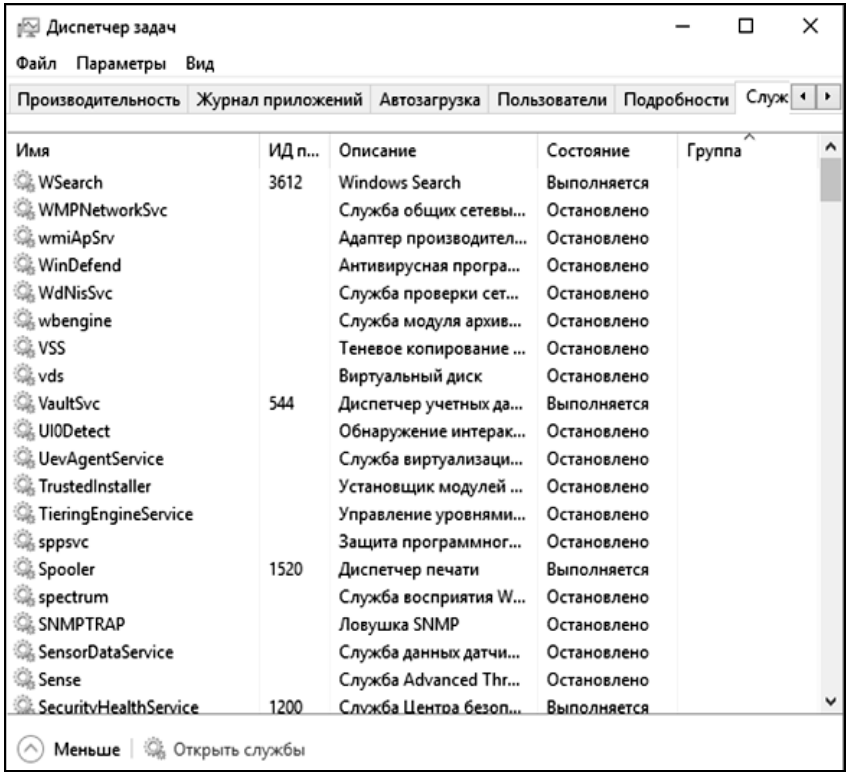

Рис. 1. Просмотр установленных служб в диспетчере задач

Для каждой службы в диспетчере задач показывается её имя, идентификатор процесса, в рамках которого она запущена (если такой имеется), краткое описание, текущее состояние и группа.

Диспетчер задач позволяет запускать и останавливать службы, если это возможно. Щёлкните правой кнопкой на службе из списка, чтобы увидеть возможные действия (рис. 2).

Запустите и остановите службу Parental Controls (WPCSvc). Приложения, выполняющие функции, аналогичные диспетчеру задач, также зачастую позволяют просматривать, запускать и останавливать службы. Например, эти возможности доступны в Process Explorer.

Оснастка !Службы! – другое средство управления службами, имеющее графический интерфейс, но обладающее большими возможностями, чем диспетчер задач. Оснастка «Службы» представляет собой оснастку консоли MMC.

Оснастку «Службы» можно запустить из диспетчера задач (начиная с Windows 7). Для этого нужно нажать кнопку «Открыть службы» на вкладке «Службы» (рис. 3).

Чтобы запустить оснастку «Службы» из командной строки, нужно выполнить services.msc. Окно оснастки представлено на рис. 4.

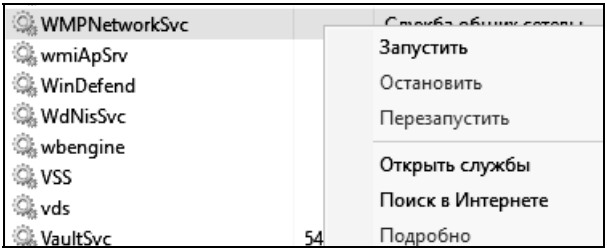

Рис. 2. Действия со службами в диспетчере задач

Рис. 3. Вызов оснастки из диспетчера задач

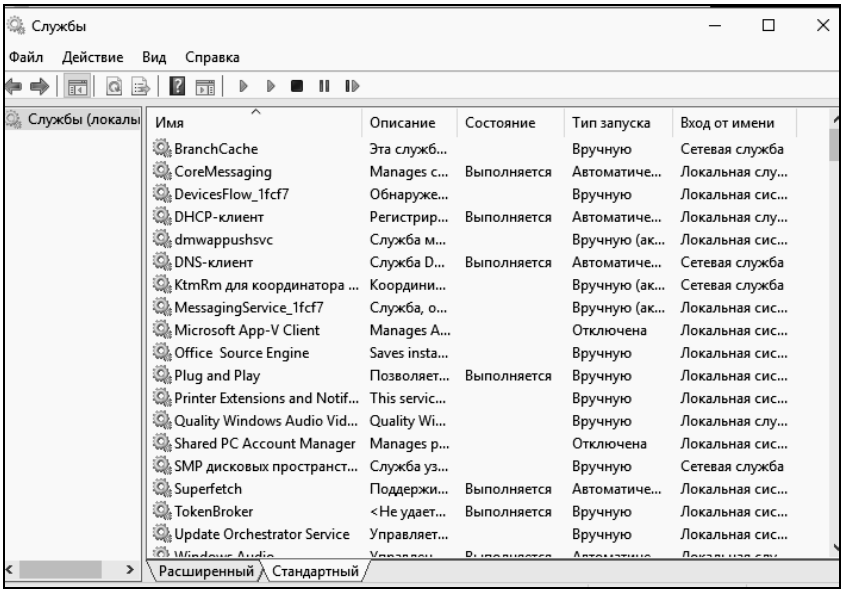

Рис. 4. Оснастка «Службы»

Если два раза щёлкнуть левой кнопкой мыши по любой из доступных служб, откроется окно свойств этой службы (рис. 5).

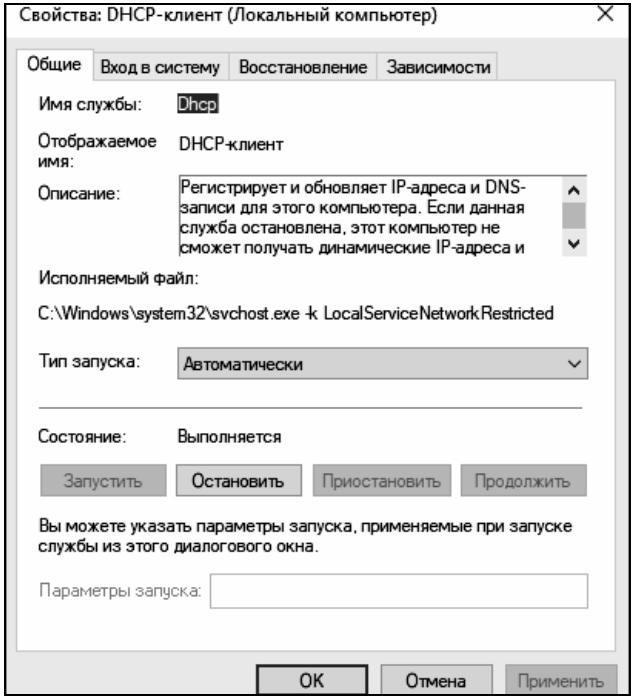

Рис. 5. Окно свойств службы

Служба может находиться в одном из следующих состояний: работает, приостановлена и остановлена. Соответственно, для службы доступно 4 команды: запустить, остановить, приостановить, продолжить. Эти команды для выбранной службы отображаются в оснастке слева от списка доступных служб (при выборе «расширенного» вида внизу окна), либо в окне свойств выбранной службы на вкладке «Общие». Команды также отображаются, если щёлкнуть правой кнопкой на службе в списке.

Не все службы могут быть приостановлены – некоторые могут быть только запущены и остановлены. Некоторые службы нельзя ни приостановить, ни остановить.

Остановите службу «Windows Audio» и попробуйте запустить звуковой файл. Затем запустите службу и убедитесь, что файл проигрывается.

Служба может зависеть от других служб и при этом могут быть службы, зависящие от неё. Если служба, от которой зависит данная

служба, не запущена, то данная служба может работать некорректно или вообще не запуститься.

Одна служба может иметь несколько зависимых служб. Также сама служба может быть зависима от нескольких служб. Службы могут зависеть не только от других служб, но и от некоторых драйверов. Зависимые службы можно просмотреть на вкладке «Зависимости» окна свойств службы (рис. 6).

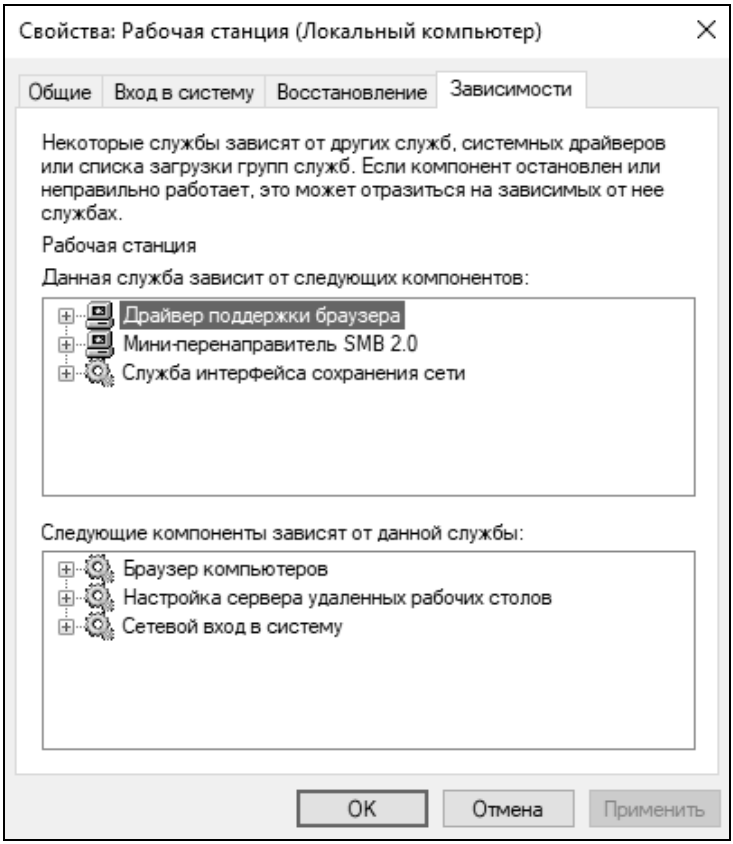

Рис. 6. Просмотр зависимостей службы

Остановите службу «Система событий COM+», которая имеет зависимую службу «Служба уведомления о системных событиях». Система выведет предупреждение о том, что зависимые службы будут также остановлены (рис. 7).

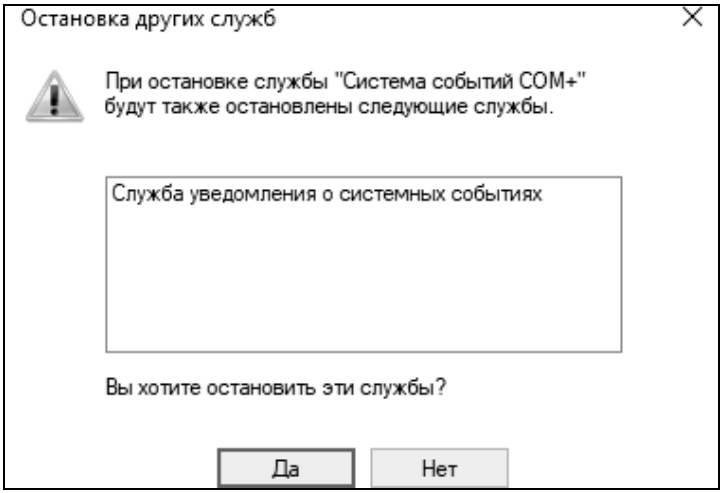

Рис. 7. Попытка остановить службу с зависимостями

Каждая служба может иметь один из следующих типов запуска:

– автоматически: служба запускается при загрузке Windows;

– вручную: служба запускается пользователем в оснастке «Службы» или любым другим способом;

– отключена: служба не может быть запущена, пока тип запуска не будет сменён на другой.

Кроме того, имеются также два дополнительных типа запуска: первый – запуск на этапе загрузке ядра Windows (низкоуровневые драйверы), второй – запуск сразу после инициализации ядра. Для таких служб сменить тип запуска в оснастке нельзя (например, служба «Удалённый вызов процедур»).

Примечание: начиная с Windows Vista, у служб присутствует ещё один тип запуска – «Автоматически (отложено)». Он аналогичен типу «Автоматически», но запускает службу через некоторое время после загрузки для оптимизации запуска Windows.

Тип запуска можно сменить на вкладке «Общие» окна свойств службы. Для службы «Темы» установите тип запуска «Вручную», перезагрузите компьютер и убедитесь, что окна Windows имеют «классический» вид, так как служба не запущена.

Если работа службы была некорректно завершена, Windows может перезапустить её или выполнить другие действия. Настройка параметров восстановления находится на вкладке «Восстановление» окна свойств службы (рис. 8).

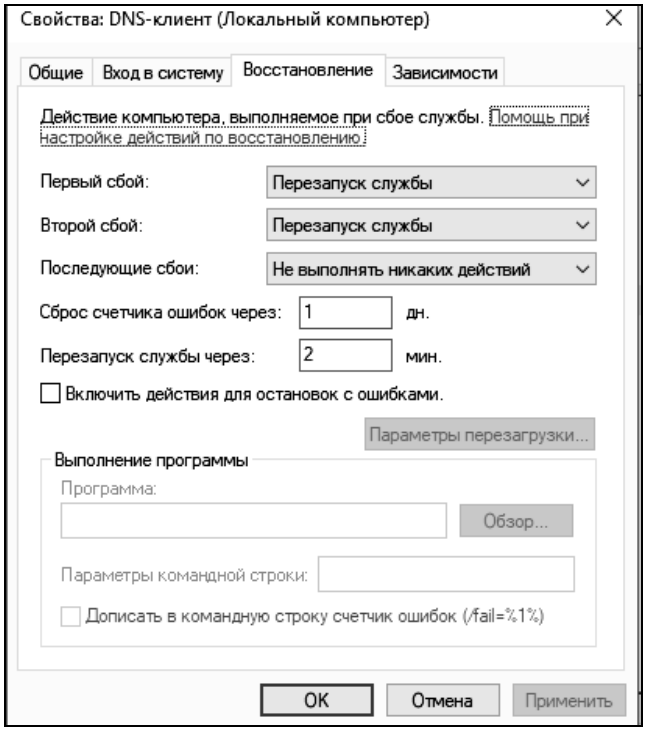

Рис. 8. Параметры восстановления службы

Можно задать действия, которые будут выполняться при первом, втором и последующих сбоях службы. Среди доступных действий:

– перезапуск службы: перезапускает службу через указанное время после сбоя;

– запуск программы: запускает выбранную ниже программу с заданными параметрами командной строки. Можно включить в параметры командной строки номер очередного сбоя службы;

– перезагрузка компьютера: перезагружает компьютер немедленно или по истечении заданного времени. При этом можно вывести на экран сообщение о неминуемой перезагрузке;

– не выполнять никаких действий: никакие действия после сбоя выполнены не будут.

Некоторые службы, например «Plug'n'play», не поддерживают параметры восстановления. Обычно при сбое этих служб компьютер перезагружается.

Установите параметры восстановления для службы «Диспетчер печати» («Диспетчер очереди печати») следующим образом: при первом сбое служба должна мгновенно перезапускаться, при втором – перезагружать компьютер с выводом сообщения через 2 минуты.

Завершите процесс spoolsv.exe, в котором запущена эта служба. Убедитесь, что процесс тут же запускается снова. Завершите процесс второй раз и убедитесь, что Windows выводит сообщение о неминуемой перезагрузке и через 2 минуты компьютер перезагружается.

Каждая служба имеет определённые права при запуске. Служба может запускаться:

– с системной учётной записью;

– как локальная служба;

– как сетевая служба;

– с правами какого-либо пользователя.

Права службы можно сменить на вкладке «Вход в систему» окна свойств службы (рис. 9).

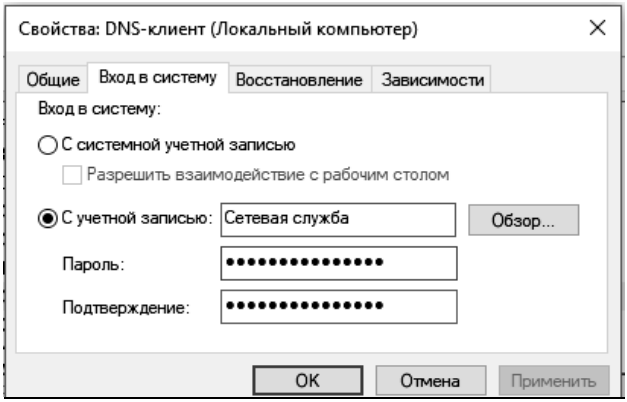

Рис. 9. Права службы при входе в систему

Чтобы выбрать вход с системной учётной записью, выберите соответствующий вариант вверху окна. Для выбора локальной службы нужно ввести в качестве имени пользователя «NT AUTHORITY / LocalService» («Локальная служба» в Windows Vista и 7) без кавычек, а пароль не вводить.

Для выбора сетевой службы – «NT AUTHORITY/NetworkService» («Сетевая служба» в Windows Vista и 7) и пароль так же не вводить.

Для работы со службами из командной строки предусмотрены команды семейств net и sc. Семейство net в основном используется для

других целей и имеет базовые команды работы со службами. Семейство sc, введённое в Windows XP, целиком посвящено работе со службами.

Запустите командную строку, выбрав «Пуск > Выполнить» и набрав cmd.

Для просмотра запущенных на данный момент служб введите команду net start. Обратите внимание, что она выводит список отображаемых имён служб, а не сами имена служб (рис. 10).

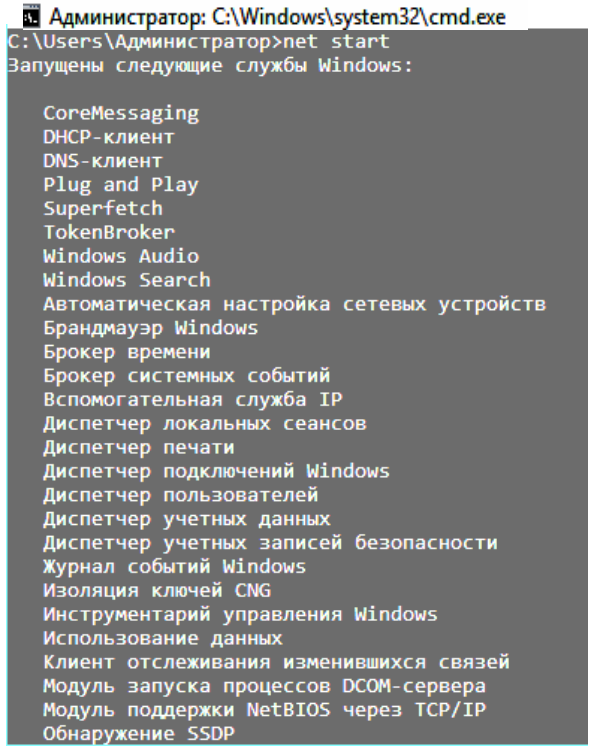

Рис. 10. Выполнение команды net start

Чтобы запустить службу, введите команду net start с последующим именем службы. Запустите службу SysmonLog (pla начиная с Windows 7) – «Журналы и оповещения производительности» (рис. 11).

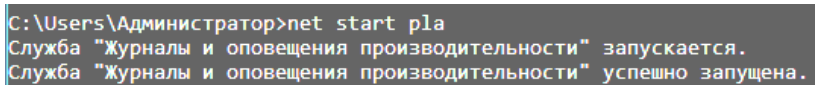

Рис. 11. Запуск службы с помощью net start

Если служба имеет тип запуска «Отключена» или уже запущена, об этом будет выведено соответствующее сообщение.

Для остановки службы используется команда net stop с последующим именем службы. Если служба не запущена или не может быть остановлена, об этом будет выведено сообщение. Остановите службу MpsSvc – «Брандмауэр Windows». Зайдите в панель управления и убедитесь, что брандмауэр Windows отключен.

Команды семейства net не позволяют, например, выводить все установленные в системе службы. Для этого используются команды семейства sc.

Семейство sc позволяет просматривать и изменять подробную информацию о каждой службе, а также регистрировать в системе новые службы и удалять установленные. Если ввести sc без параметров, можно просмотреть справку по этому семейству. То же самое относится к большинству команд этого семейства.

Для вывода списка служб используются команды sc query и sc queryex. Первая команда выводит такие данные о службе, как имя (SERVICE_NAME), отображаемое имя (DISPLAY_NAME), состояние (STATE) и другие данные, не рассматриваемые в данной работе. Вторая команда дополнительно выводит идентификатор процесса (PID), в рамках которого запущена служба (рис. 12).

```
C:\Users\Администратор>sc queryex

Имя_службы: AudioEndpointBuilder
Выводимое_имя: Средство построения конечных точек Windows Audio
        Тип                : 20  WIN32_SHARE_PROCESS
        Состояние          : 4  RUNNING
                                (STOPPABLE, NOT_PAUSABLE, IGNORES_SHUTDOWN)
        Код_выхода_Win32   : 0  (0x0)
        Код_выхода_службы  : 0  (0x0)
        Контрольная_точка  : 0x0
        Ожидание           : 0x0
        ID_процесса        : 8
        Флаги              :
```

Рис. 12. Команды sc query и sc queryex

Команды позволяют использовать фильтр для вывода списка служб. Фильтр задаётся в виде параметров, введённых после команды. Среди параметров:

– type: имеет значение driver (драйвер), service (служба), interact (интерактивная служба, которая обменивается информацией с пользователем) или all (и то, и другое). По умолчанию – service;

– state: имеет значение inactive (незапущенные службы) или all (и запущенные, и остановленные службы). Если параметр не задан, он принимается равным значению active (запущенные службы).

Таким образом, чтобы, например, вывести список незапущенных служб драйверов, нужно ввести команду sc query type= all state= inactive.

Соответственно, если не задано никаких параметров, выводятся все запущенные службы.

Если после команды sc query или sc queryex ввести имя службы, будет выведена информация только об этой службе.

Выведите список всех установленных интерактивных служб. Затем выведите расширенную информацию об одной из запущенных служб из этого списка.

Кроме перечисленных команд, для вывода информации о конкретной службе используются также команды sc qc, sc qdescription, sc qfailure и другие. После команды пишется имя соответствующей службы (рис. 13).

```
C:\Users\Администратор>sc qc Spooler
[SC] QueryServiceConfig: успех

Имя_службы: Spooler
        Тип                : 110  WIN32_OWN_PROCESS (interactive)
        Тип_запуска        : 2   AUTO_START
        Управление_ошибками  : 1   NORMAL
        Имя_двоичного_файла  : C:\Windows\System32\spoolsv.exe
        Группа_запуска     : SpoolerGroup
        Тег                : 0
        Выводимое_имя      : Диспетчер печати
        Зависимости        : RPCSS
                           : http
        Начальное_имя_службы : LocalSystem

C:\Users\Администратор>sc qdescription Spooler
[SC] QueryServiceConfig2: успех

Имя_службы: Spooler
Описание:  Эта служба позволяет ставить задания печати в очередь и обеспечивает взаимодей
ствие с принтером. Если ее отключить, вы не сможете выполнять печать и видеть свои принте
ры.

C:\Users\Администратор>sc qfailure Spooler
[SC] QueryServiceConfig2: успех

Имя_службы: Spooler
        Период_сброса (в секундах)    : 3600
        Сообщение_при_перезагрузке    :
        Командная_строка              :
        Действия_при_сбое             : перезапуск -- задержка = 5000 мс.
```

Рис. 13. Команды просмотра информации о службах

sc qc выводит такую информацию: тип запуска службы (START_TYPE), имя исполняемого файла (BINARY_PATH_NAME), отображаемое имя (DISPLAY_NAME), зависимости (DEPENDENCIES) и имя учётной записи, правами которой обладает служба при запуске (или начальное имя службы, SERVICE_START_NAME).

sc qdescription выводит описание службы (DESCRIPTION).

sc qfailure выводит действия при сбое службы (FAILURE_ ACTIONS), период сброса счётчика сбоев в секундах (RESET_PERIOD), сообщение при неминуемой перезагрузке (REBOOT_MESSAGE) и путь к файлу программы для запуска (COMMAND_LINE).

Кроме того, можно вывести список служб, зависящих от данной службы. Для этого используется команда sc enumdepend.

Выведите информацию с помощью этих команд о службе CryptSvc – «Службы криптографии».

Для изменения состояния службы используются следующие команды:

– sc start: запуск службы;

– sc pause: приостановка службы, если возможно;

– sc continue: продолжение работы службы, если она была приостановлена;

– sc stop: остановка службы, если возможно.

После команды пишется имя службы, состояние которой нужно изменить.

Для изменения типа запуска определённой службы используется команда sc config с последующим именем службы и списком изменяемых параметров. Эта команда также позволяет, в частности, изменять имя учётной записи для службы, отображаемое имя, путь к исполняемому файлу и даже зависимости, что недоступно в диспетчере управления службами.

Для изменения типа запуска используется параметр start. Его значения:

– boot: запуск при инициализации ядра Windows;

– system: запуск сразу после инициализации ядра Windows;

– auto: запуск сразу после загрузки Windows (соответствует типу «Автоматически» в диспетчере управления службами);

– demand: запуск по требованию пользователя (соответствует типу «Вручную» в диспетчере управления службами);

– disabled: служба отключена (соответствует типу «Отключена» в диспетчере управления службами).

Примечание: для Windows Vista и выше, типу «Автоматически (отложено)» соответствует значение параметра delayed-auto.

Примечание: как и в оснастке «Службы», первые два типа запуска изменять не допускается.

Таким образом, чтобы, например, установить службе «DNS-клиент» тип запуска «Вручную», нужно ввести sc config Dnscache start= demand.

С помощью этой команды измените тип запуска службы Themes – «Темы» на «Автоматически». Перезагрузите компьютер и убедитесь, что окна Windows имеют обычный вид.

Для изменения параметров восстановления определённой службы используется команда sc failure с последующим именем службы и списком изменяемых параметров. Параметры следующие:

– actions: действия, выполняемые при сбое и задержки перед их выполнением в миллисекундах. Сначала пишется действие при первом сбое, затем задержка, отделяемая от него косой чертой («/»). Если нужно задать действия при следующих сбоях, далее снова ставится косая черта и пишется следующее действие и задержка. Возможные действия:

– run: запуск программы. При использовании этого значения должен быть задан параметр command;

– reboot: перезагрузка компьютера. Используется совместно с параметром reboot;

– restart: перезапуск службы.

Чтобы при сбое не выполнялось никаких действий, просто не вводите следующее действие и его задержку.

К примеру, если службу при первом и втором сбое нужно перезапустить через 2 секунды, а при следующих сбоях – перезагрузить компьютер через 30 секунд, значение параметра actions будет равно restart/2000/restart/2000/reboot/30000;

– reset: продолжительность периода (в секундах), после которого счётчик сбоев сбрасывается. Если значение равно INFINITE, счётчик никогда не сбрасывается;

– reboot: сообщение, выводимое перед перезагрузкой;

– command: путь и параметры командной строки для файла запускаемой при сбое программы.

Для службы Spooler установите следующие параметры восстановления: при первом сбое служба должна перезапуститься через 5 секунд, при втором

– через 10 секунд, при третьем – компьютер должен перезагрузиться через 20 секунд с выводом соответствующего сообщения. Счётчик сбоев должен быть сброшен через 1 час.

Завершите процесс spoolsv.exe три раза, чтобы убедиться в правильности введённой команды.

Команда sc interrogate используется совместно с открытой оснасткой «Службы». При изменении состояния службы с помощью командной строки оно не сразу обновляется в оснастке. Чтобы принудительно обновить его, вводится эта команда с последующим именем службы.

Откройте оснастку «Службы». Остановите с помощью sc stop службу TapiSrv – «Телефония», а затем обновите её состояние в оснастке с помощью sc interrogate и убедитесь в том, что в оснастке её состояние показывается правильно.

Для регистрации новой службы в реестре используется команда sc create. При этом после команды требуется указать имя создаваемой службы и путь к исполняемому файлу (параметр binPath). Дополнительно можно указать тип запуска (start), зависимости (depend), отображаемое имя (DisplayName), имя (obj) и пароль (password) учётной записи для входа и другое.

Создайте новую службу, выбрав в качестве исполняемого файла Notepad.exe (блокнот) (рис. 14). Задайте ему автоматический тип запуска и произвольное отображаемое имя. Пусть служба обладает правами пользователя «Система» (LocalSystem).

```
C:\Users\Администратор>sc create Notepad binPath=C:\Windows\notepad.exe start=
auto DisplayName= Блокнот obj= LocalSystem
[SC] CreateService: успех
```

Рис. 14. Создание новой службы

Откройте оснастку «Службы» и убедитесь, что созданная служба отображается в списке.

Примечание: не пытайтесь запустить созданную службу. Она не отвечает требованиям, предъявляемым к службам, и приведена только в качестве примера.

Чтобы удалить службу, используется команда sc delete с последующим именем службы. Если служба запущена или используется другим процессом, она будет помечена для удаления и удалена позже.

Удалите только что созданную службу. Перейдите в оснастку «Службы», выберите «Действие > Обновить» и убедитесь, что служба в списке отсутствует.

Приведём описание некоторых системных служб Windows:

– DHCP-клиент: управляет конфигурацией сети посредством регистрации и обновления IP-адресов и DNS-имен.

– DNS-клиент: разрешает для данного компьютера DNS-имена в адреса и помещает их в кэш. Если служба остановлена, не удастся разрешить DNS-имена и разместить службу каталогов Active Directory контроллеров домена.

– Plug'n'play: позволяет компьютеру распознавать изменения в установленном оборудовании и подстраиваться под них, либо не требуя вмешательства пользователя, либо сводя его к минимуму.

– Windows audio: управление звуковыми устройствами для Windows-программ.

– Автоматическое обновление: загрузка и установка обновлений Windows. Если служба отключена, то на этом компьютере нельзя будет использовать возможности автоматического обновления или веб-узел Windows Update.

– Веб-клиент: позволяет Windows-программам создавать, получать доступ и изменять файлы, хранящиеся в Интернете.

– Диспетчер логических дисков: обнаружение и наблюдение за новыми жесткими дисками и передача информации о томах жестких дисков службе управления диспетчера логических дисков.

– Журнал событий: обеспечивает поддержку сообщений журналов событий, выдаваемых Windows-программами и компонентами системы, и просмотр этих сообщений.

– Обозреватель компьютеров/браузер компьютеров: обслуживает список компьютеров в сети и выдает его программам по запросу.

– Планировщик заданий: позволяет настраивать расписание автоматического выполнения задач на компьютере.

– Поставщик поддержки безопасности NT LM: аутентификация на серверах NT и доступ к ресурсам домена.

– Рабочая станция: обеспечивает поддержку сетевых подключений и связь. Если служба остановлена, программа, данные подключения будут недоступны.

– Сервер: обеспечивает поддержку общий доступ к файлам, принтерам и именованным каналам для данного компьютера через сетевое подключение.

– Сетевые подключения: управляет объектами папки «Сеть и удаленный доступ к сети», отображающей свойства локальной сети и подключений удаленного доступа.

– Служба восстановления системы: выполняет функции восстановления системы.

– Службы криптографии: предоставляет три службы управления: службу баз данных каталога, которая проверяет цифровые подписи файлов Windows; службу защищенного корня, которая добавляет и удаляет сертификаты доверенного корня центра сертификации с этого компьютера; и службу ключей, которая позволяет подавать заявки на сертификаты с этого компьютера. Начиная с Windows Vista, предоставляет также четвёртую службу: службу автоматического обновления корневых сертификатов, которая получает корневые сертификаты из центра обновления Windows и разрешает сценарии, такие как SSL.

– Теневое копирование тома: управляет созданием теневых копий (контрольных точек состояния) дисковых томов, которые используются для архивации и восстановления или для иных целей.

– Удалённый вызов процедур: выполняет запросы активации объектов, разрешение экспортера объектов и распределенный сбор мусора для серверов COM и DCOM.

– Управление приложениями: обеспечивает службы установки программного обеспечения, такие как назначение, публикация и удаление.

– Центр обеспечения безопасности: ведет наблюдение за настройками и параметрами безопасности системы.

3.2. Автоматизация выполнения административных задач

Планировщик заданий – это оснастка MMC, позволяющая назначать автоматически выполняемые задания, запуск которых производится в определенное время или при возникновении определенных событий.

Планировщик заданий содержит библиотеку всех назначенных заданий, обеспечивая возможность быстрого просмотра и удобного управления заданиями. Из библиотеки можно запустить, отключить, изменить и удалить задание.

Для того чтобы запустить планировщик задач, необходимо проверить, включена ли данная служба, как показано на рис. 15.

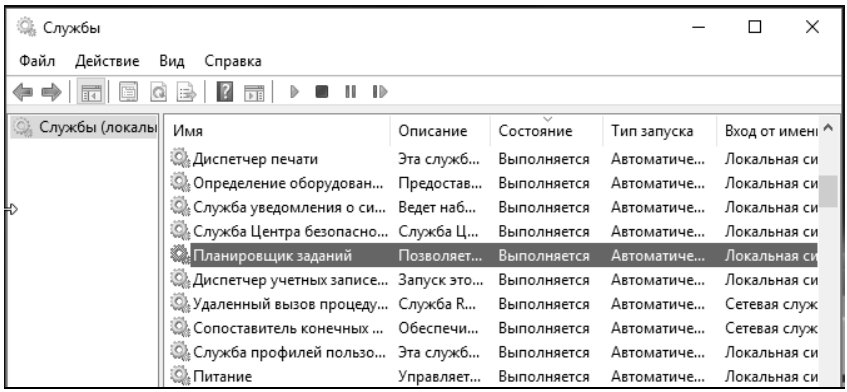

Рис. 15. Службы

Если служба Планировщик задач не включена, нужно вызвать контекстное меню, кликнув правой кнопкой мыши на данную службу и выбрать Свойства. Во вкладке Общее, если в поле Состояние стоит статус «Работает», значит служба планировщик задач запущена. Если нет, необходимо нажать кнопку «Запустить», тип запуска выбрать «Автоматически» и сохранить настройки (рис. 16).

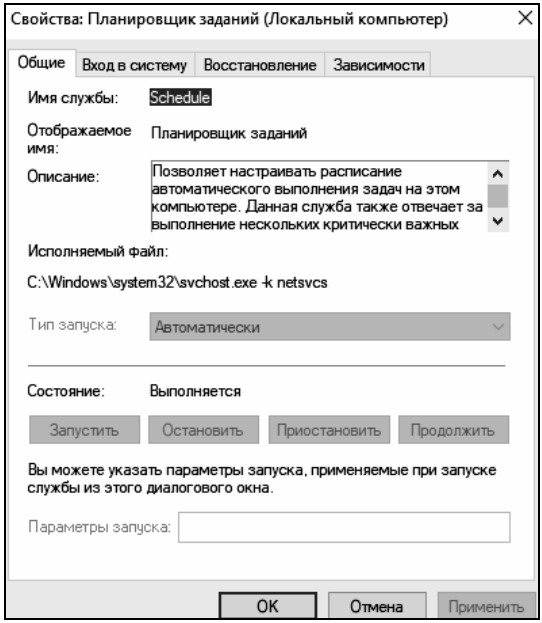

Рис. 16. Планировщик заданий

После того, как служба запущена и тип запуска автоматический, служба будет стартовать при загрузке системы, и задания будут выполняться в соответствии с выбранным расписанием.

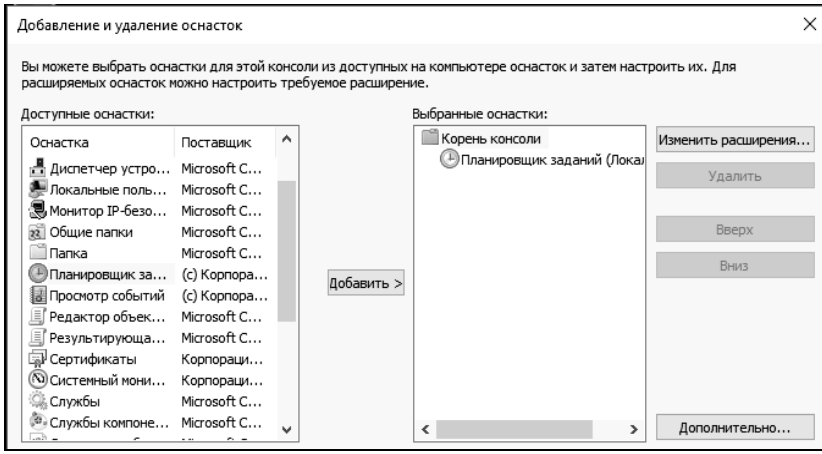

Рис. 17. Добавление оснастки

Чтобы создать задачу, потребуется сперва вызвать консоль управления ММС и добавить в нее оснастку «Планировщик заданий» (рис. 17). После чего в меню действий к данной оснастке выбрать пункт «Создать задачу…» или «Создать простую задачу…» (рис. 18).

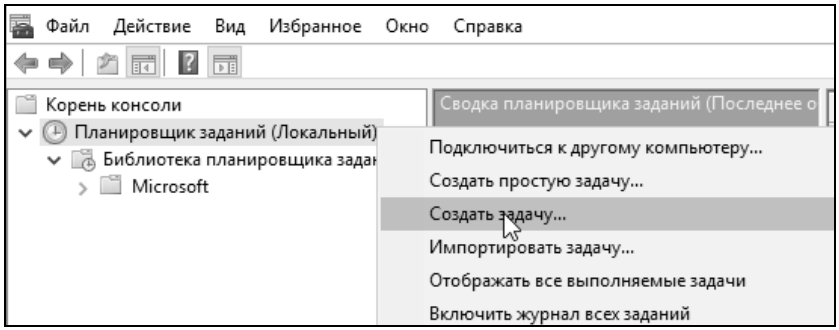

Рис. 18. Добавить задание

В случае выбора создания простой задачи – будет запущен «Мастер создания простой задачи», в котором по шагам будет предложено создать необходимое задание. Создайте задачу по запуску командной строки. Для удобства работы с создаваемыми задачами – каждой из них присваивается имя (рис. 19).

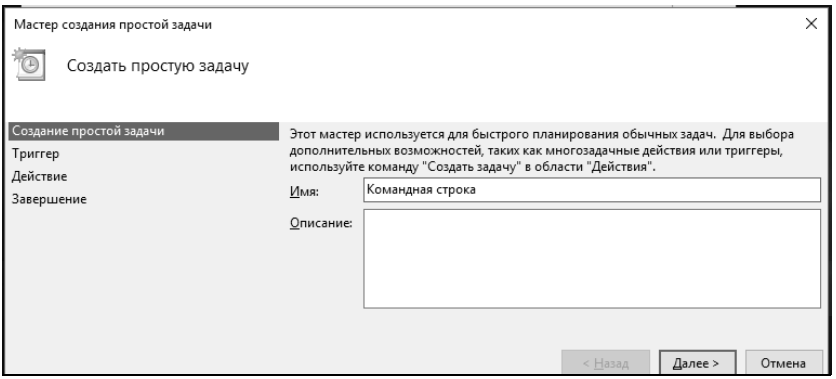

Рис. 19. Задание имени задаче

Мастер предложить указать период запуска этого задания. Возможны следующие варианты периода запуска задания:

– Ежедневно. Задание будет запускаться ежедневно, либо только по рабочим дням или через несколько дней в указанное время.

– Еженедельно. Указывается, каждую ли неделю нужно запускать задание и выбирать дни недели, по которым задание будет запущено в определенное время.

– Ежемесячно. В какие месяцы года надо запускать задание и выбирать по каким числам месяца, либо по каким дням месяца в определенное время будет запущено задание.

– Однократно. Можно выбрать дату и время запуска задания. Больше это задание выполняться не будет.

– При загрузке компьютера. При таком типе запуска задание будет выполняться каждый раз при загрузке компьютера. Данный тип запуска не требует входа пользователя.

– При входе в Windows. Этот тип запуска похож на предыдущий с тем отличием, что задание будет выполнено только когда пользователь войдет в Windows, то есть введет свои логин и пароль.

Выберите «При входе в Windows» и нажмите «Далее» (рис. 20).

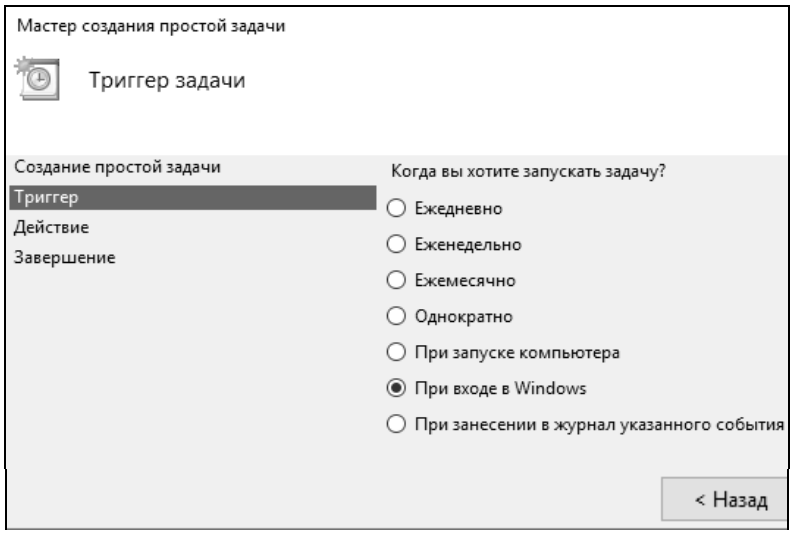

Рис. 20. Задание триггера запуска

Затем будет предложено выбрать действие, выполняемое задачей. Выберите «Запуск программы» (рис. 21). Будет предложено через «Проводник» указать файл программы, который будет необходимо запустить. Выберите из списка Командную строку (C:\Windows\System32\cmd.exe) и нажмите «Далее» (рис. 22).

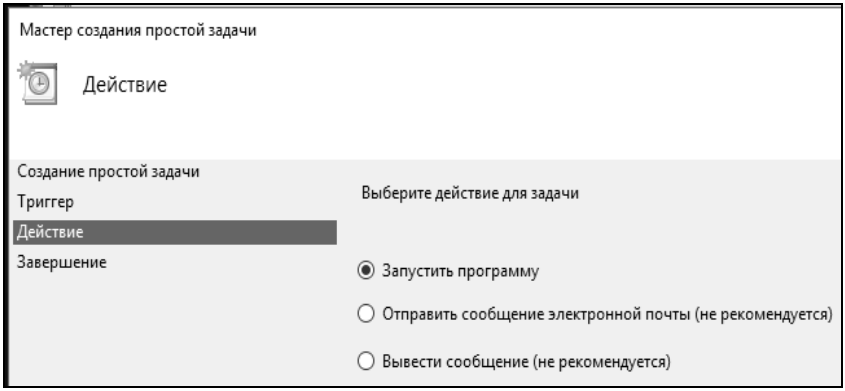

Рис. 21. Выбор действия

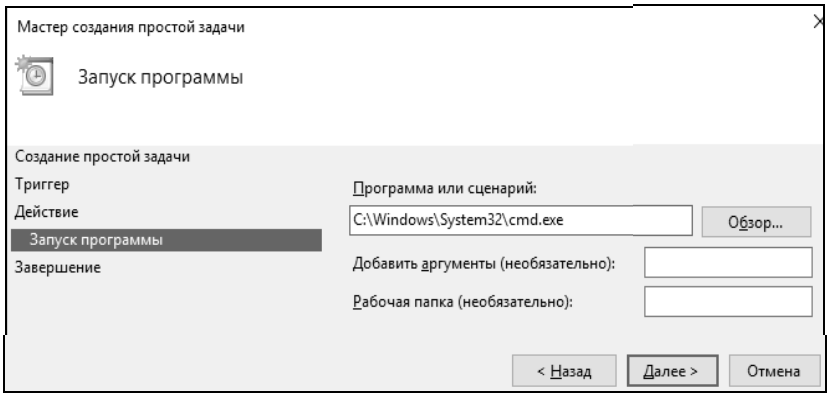

Рис. 22. Выбор программы для запуска

После проделанных действий «Мастер создания простой задачи» предоставит информацию по заданной задаче. Убедитесь, что все соответствует выбранным параметрам и нажмите «Готово» (рис. 23).

В библиотеке планировщика заданий появится новая задача с указанным Вами именем. Выделите задачу правой кнопкой и в меню действий (рис. 24) выберите пункт «Выполнить». Убедитесь, что задача осуществляется, после чего откройте ее свойства (рис. 25).

Ознакомьтесь с содержимым вкладок свойств созданной задачи. После чего запустите через меню действий планировщика «Создать задачу…». В данном формате создания задачи – мастер отличается от меню свойств созданной задачи только отсутствием вкладки «Журнал». Создайте через данный мастер задачу по запуску «Блокнота».

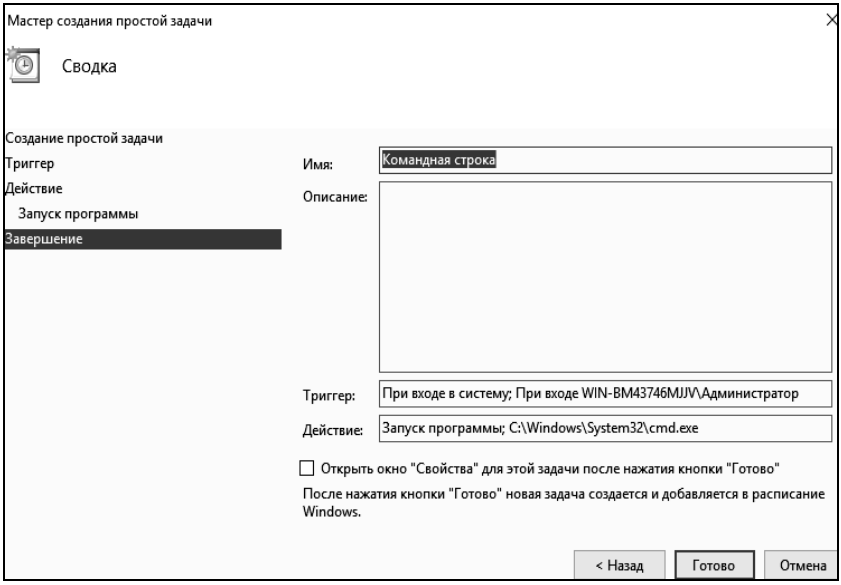

Рис. 23. Завершение работы мастера создания простой задачи

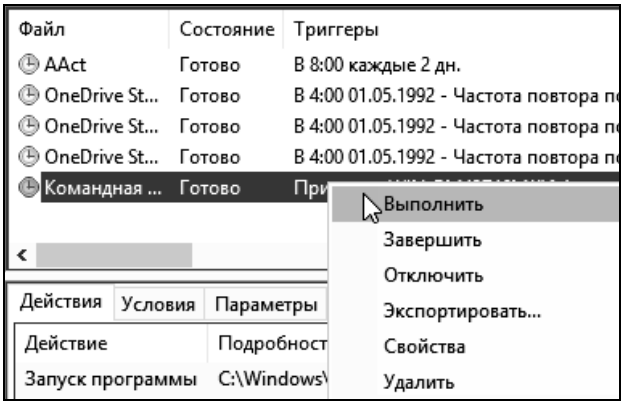

Рис. 24. Выбор действий с созданной задачей.

Добавьте в планировщик заданий Дефрагментацию диска. Для этого в Мастере планирования задания необходимо нажать Обзор и выбрать программу Defrag.exe, находящуюся в каталоге C:\Windows\System32\Defrag.exe (рис. 27). Выберите ежедневное выполнение задания.

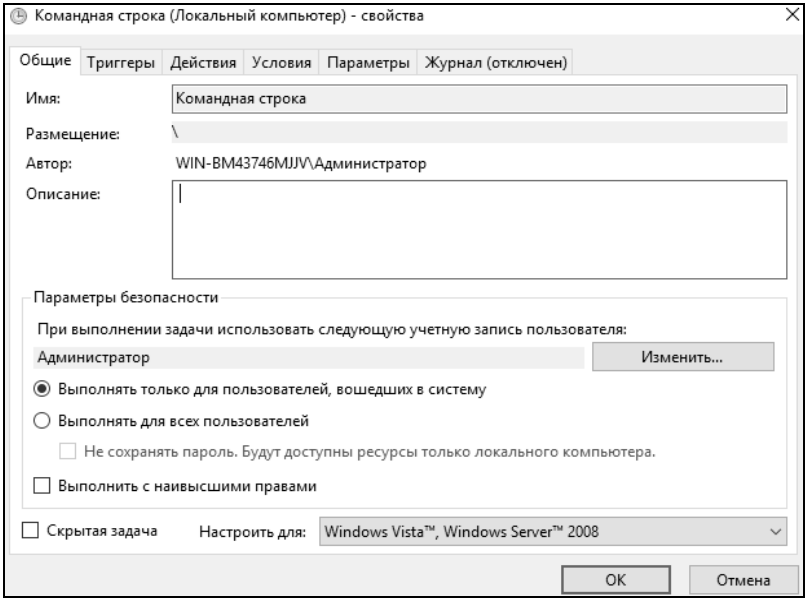

Рис. 25. Свойства задачи

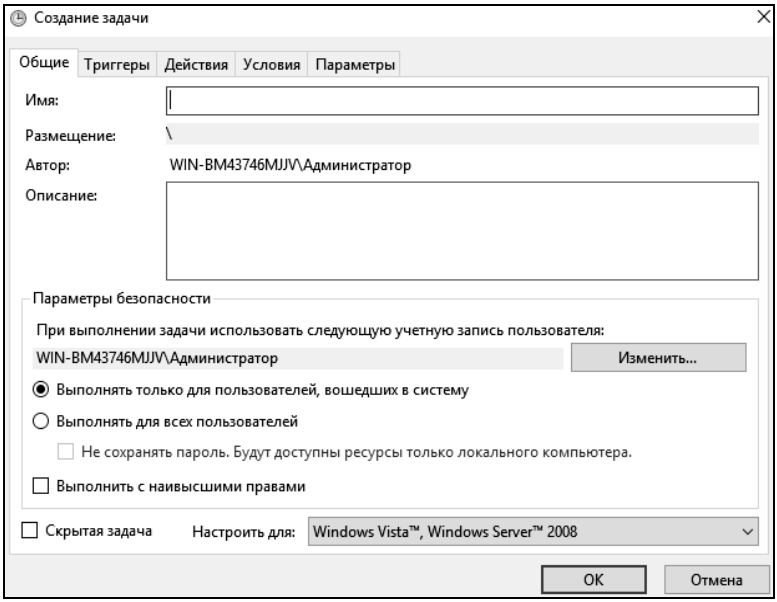

Рис. 26. Общие параметры создаваемой задачи

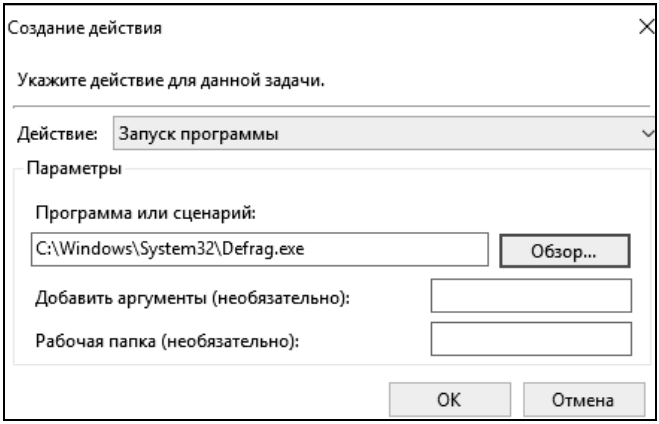

Рис. 27. Мастер планирования заданий

Ошибки при создании задачи, которые приводят к незапуску задачи в указанное время – неправильно введенный пароль, либо пароль не введен вообще. Путь к программе или скрипту, которые запускаются задачей, указан неправильно. Если в пути к запускаемой программе или скрипту есть пробелы, то путь должен быть заключен в кавычки. Еще необходимо проверить статус службы планировщика. Он должен быть запущен и режим запуска службы планировщик заданий должен быть «Авто».

3.3. Работа с процессами и потоками

Запустите «Process Explorer» (файл procexp.exe). В главном окне перечислены все работающие в системе процессы, представленные в виде древовидной структуры (рис. 28).

Двойной щелчок по имени процесса открывает окно его свойств (рис. 29). Свойства процесса предоставляют информацию о работе выбранного процесса. На вкладке «Образ» указаны путь к программе, родительский процесс, текущий рабочий каталог, предоставляется возможность уничтожения процесса и др. На вкладке «Производительность» выводится информация об использовании процессора, описание процесса, объем занятой памяти, на основе которых на вкладке «График производительности» построены графики.

Существует два режима работы программы. В режиме дескрипторов и в режиме библиотек DLL, переключение между режимами осуществляется с помощью сочетания клавиш Ctrl+H – переключение в режим отображения описателей и Ctrl+D – переключение в режим отображения DLL.

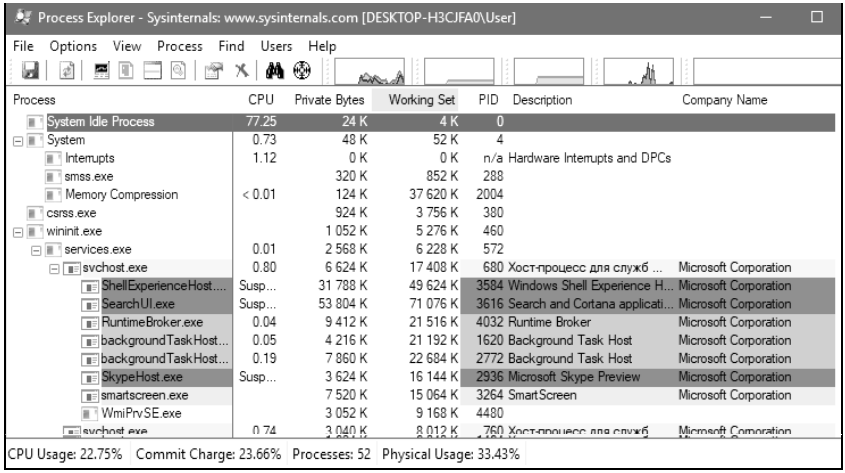

Рис. 28. Главное окно Process Explorer

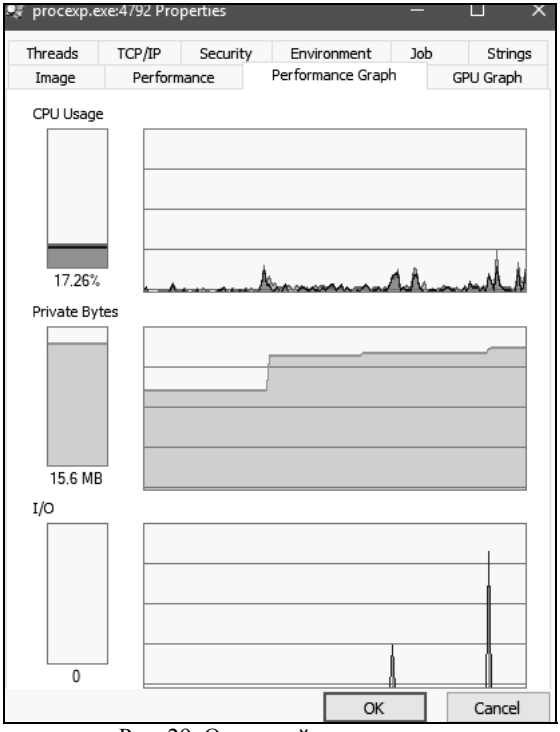

Рис. 29. Окно свойств процесса

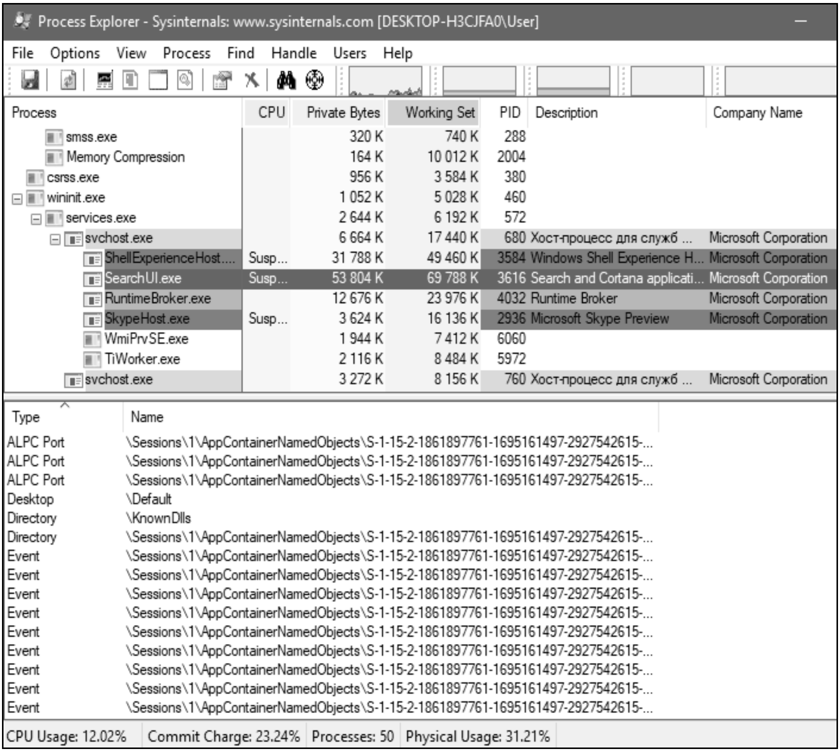

Рис. 30. Режим отображения дескрипторов

В режиме дескрипторов (рис. 30), в нижнем окне, отображаются все открытые дескрипторы выбранного в верхнем окне процесса, в данном случае, посмотрим дескрипторы открытые процессом procexp.exe: Section – диспетчер памяти объект «Секция» для общей памяти. Semaphore – исполнительная система определяет объекты «семафор». File – диспетчер ввода/вывода определяет объект «файл» для представления открытых экземпляров ресурсов драйверов устройств, которые включают в себя файлы файловой системы. Key – «ключ» для представления открытого ключа системного реестра. Диспетчер процессов создает объекты «поток» (Thread) и «процесс» (Process). Mutant – «мутант» внутреннее название для мьютекса.

В режиме библиотек DLL (рис. 31) отображаются все загруженные процессом динамические библиотеки и отображенные в память файлы.

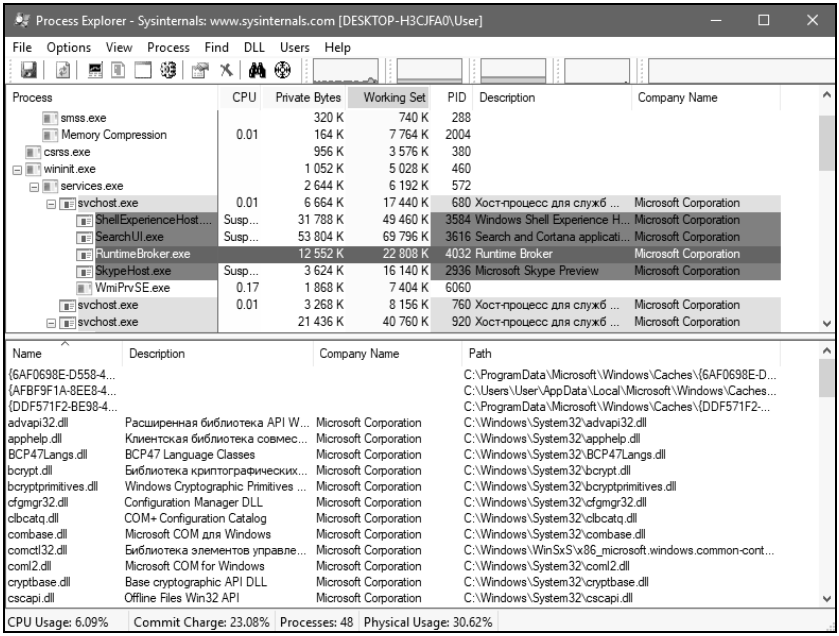

Рис. 31. Режим отображения библиотек DLL

Process Explorer позволяет приостановить/возобновить работу процесса, изменить приоритет, уничтожить процесс или уничтожить процесс и его дерево. Для этого необходимо щелкнуть на нужный процесс правой кнопкой мыши и в открывшемся контекстном меню выбрать необходимое действие. Например, в процесс explorer.exe, входит процесс procexp.exe, можно уничтожить это дерево процессов (рис. 32). Приостановка работы процесса может временно освободить занятые им ресурсы для использования другими приложениями.

Process Explorer предоставляет в распоряжение пользователя удобный инструмент, с помощью которого очень просто определить то, каким процессом открыто определенное окно. Для этого следует перетащить с панели инструментов Process Explorer кнопку в любое место открывшегося окна. После этого в верхней части главного окна будет подсвечено имя искомого процесса (рис. 33).

При помощи пункта меню «Параметры – Вместо диспетчера задач» можно заменить стандартный Диспетчер задач Windows на Process Explorer (рис. 34). Информация о системе, вызываемая из Process Explorer более полная, чем аналогичная вкладка Диспетчера задач Windows.

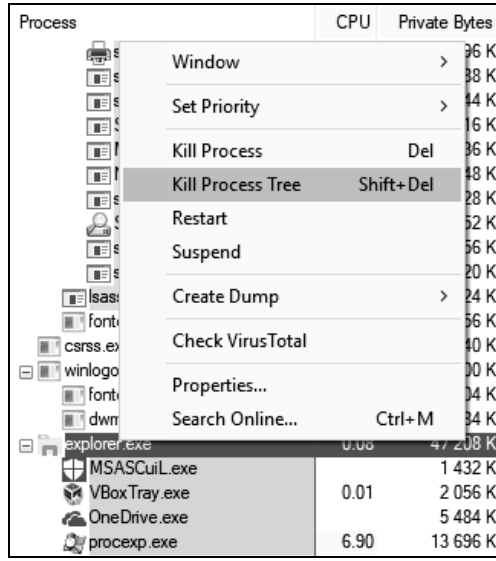

Рис. 32. Уничтожение дерева процессов

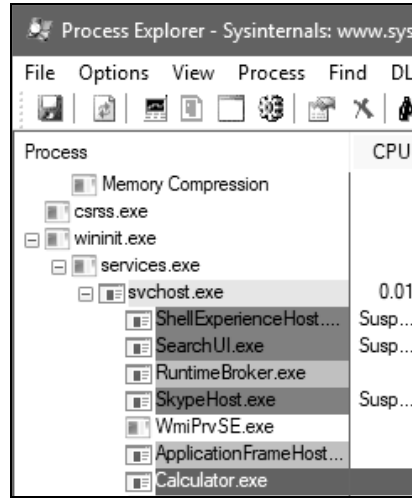

Рис. 33. Подсветка имени искомого процесса

При помощи пункта меню «Файл – Сохранить» (рис. 35), сохранить в текстовый файл список всех процессов с описаниями и объемом занятой каждым из них памяти.

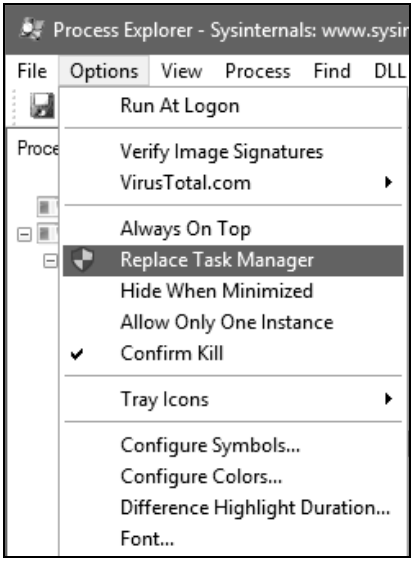

Рис. 34. Замена стандартного диспетчера задач

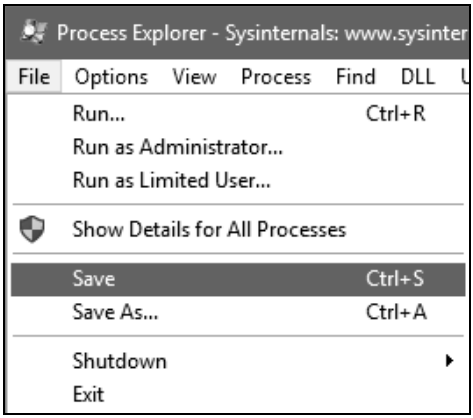

Рис. 35. Сохранение в текстовый файл списка всех процессов

Можно рассчитать влияние приоритета процесса на количество выделяемого процессорного времени, а также задать приоритет (приоритет можно выбрать при помощи нажатия правой кнопки мыши по процессу). На рис. 36 видно, сколько выделяется суммарного времени за одну минуту при заданном приоритете «Реального времени: 24» и 4 соответственно.

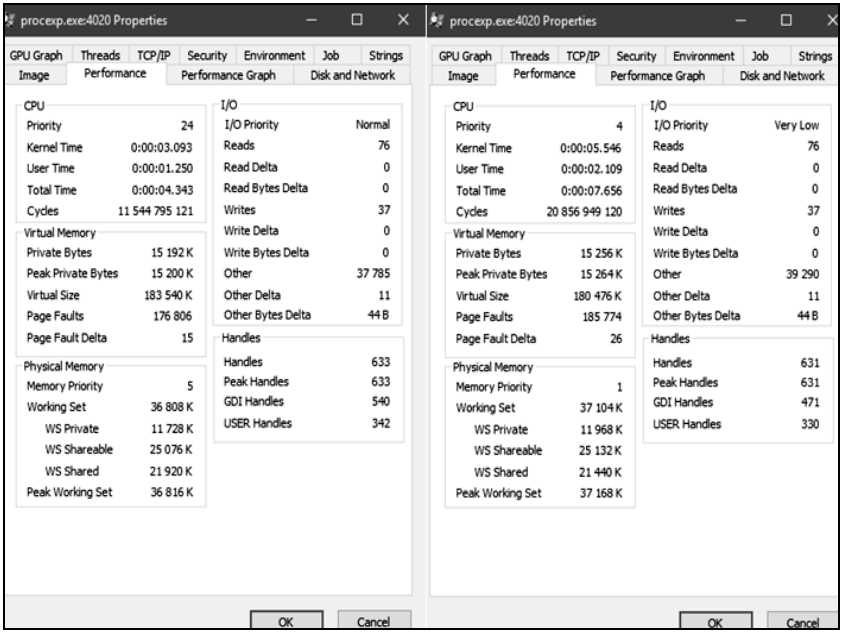

Рис. 36. Влияние приоритета на выделяемые ресурсы

У потоков, также как и у процессов, существует возможность менять приоритет, приоритет потока изменяется путем изменения приоритета у процесса. Аналогично процессам, потокам выделяется процессорное время, также потоки можно приостановить и уничтожить.

Чтобы просмотреть потоки, исполняемые в рамках процесса, необходимо открыть вкладку потоки в окне свойств процесса (рис. 37).

Чтобы просмотреть стек потока процесса, необходимо нажать клавишу «Stack» (рис. 38).

Запустите «Process Monitor» (файл ProcmonRus.exe). Откроется главное окно утилиты (рис. 39). В этом окне можно отследить действия процессов во время их работы.

При помощи меню «Файл – Сохранить» можно сохранить информацию о процессах в журнал (рис. 40).

С помощью утилиты Process Monitor можно отследить действия (включая «чтение» и «запись») процесса с файлами, реестром, сетью. Для этого необходимо зайти в меню «Настройки – Выбор колонок» и выбрать колонку «Категория» (рис. 41). В результате в колонке «Категория» можно увидеть действия процесса (рис. 42).

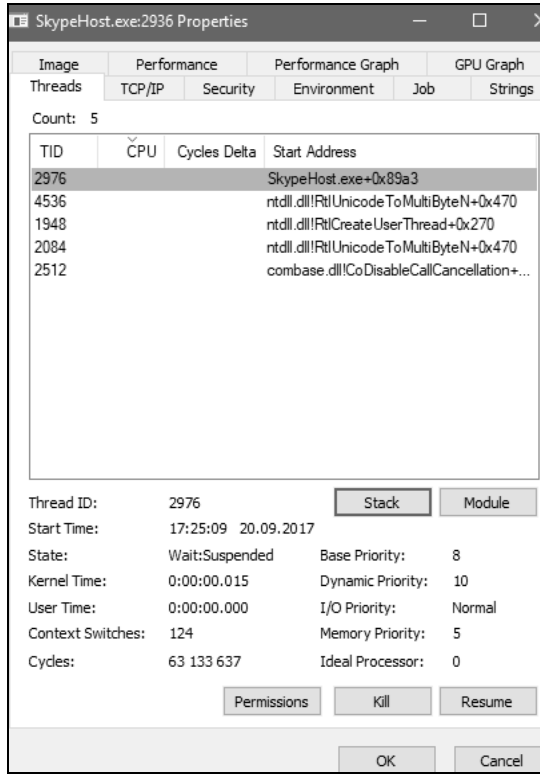

Рис. 37. Потоки

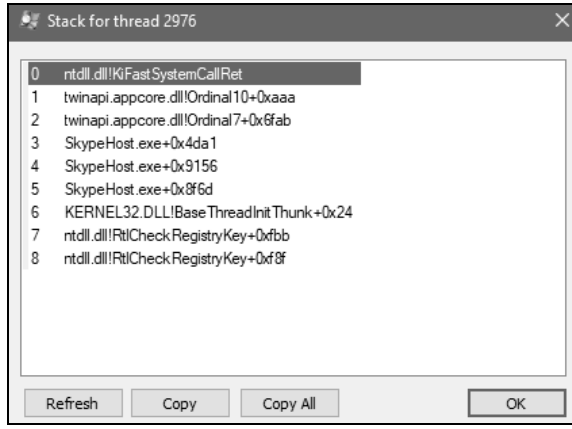

Рис. 38. Стек потока

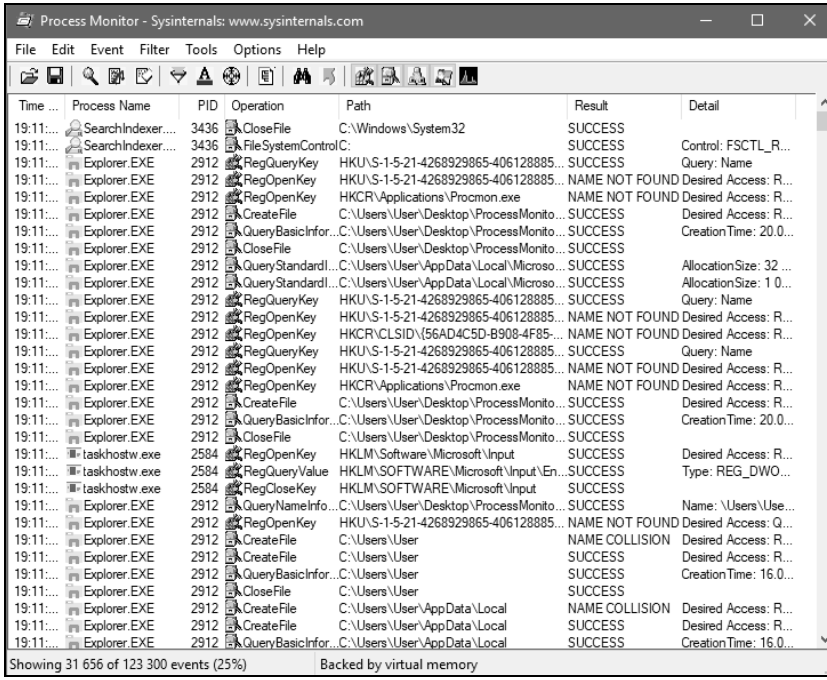

Рис. 39. Главное окно Process Monitor

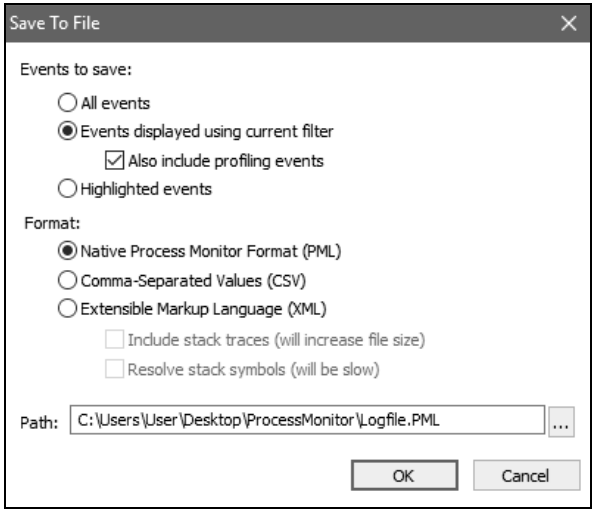

Рис. 40. Сохранение в журнал

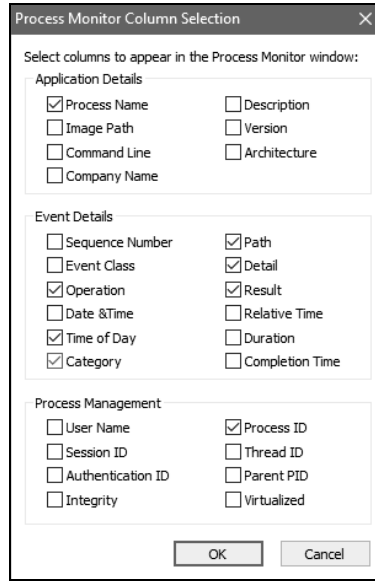

Рис. 41. Выбор колонок

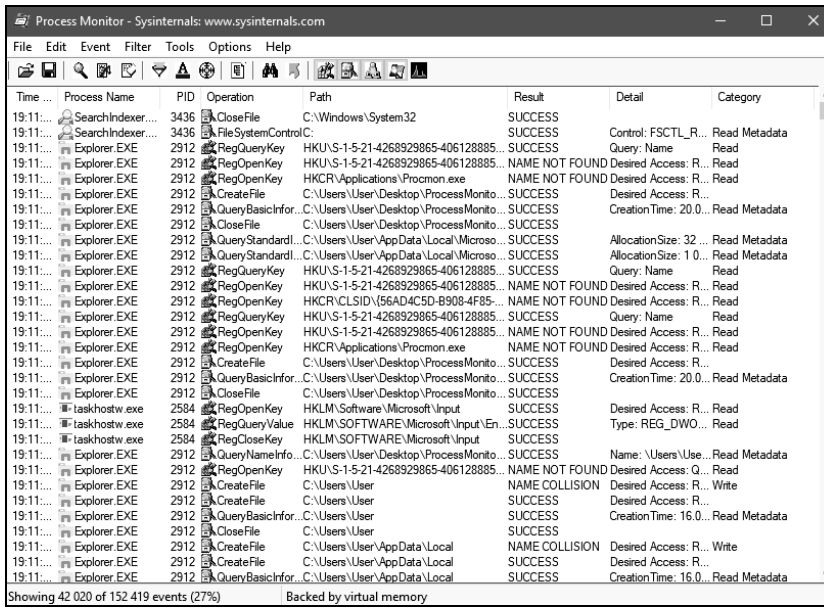

Рис. 42. Отслеживание действий процесса

Также можно отследить активность процессов при помощи меню «Инструменты – Лог активных процессов» (рис. 43).

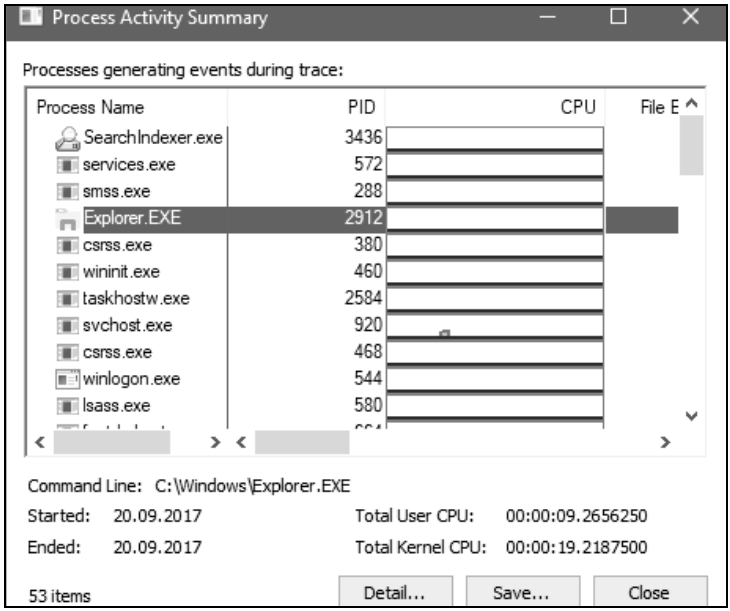

Рис. 43. Лог активных процессов

Process Monitor предоставляет возможность создавать фильтры, позволяющие делать выборки из журналов. Попасть в меню фильтров можно нажатием сочетания клавиш Ctrl+L. Фильтры можно создавать по многим параметрам, например, по имени процесса, времени, категории, операций и др. Создадим фильтр, который делает выборку процессов по операции записи в файл (рис. 44).

Также можно отследить работу процессов с файловой системой и реестром при установке программного обеспечения. Рассмотрим данную функцию на примере установки 7-zip. Установите программу. После установки выведите на экран информацию о записи ключей в реестр при установке программы. Для этого необходимо создать фильтр, который делает выборку процессов по операции записи в RegCreateFile. Определите, в каких разделах реестра 7-zip сохранил свою информацию. По аналогии определите, в каких каталогах диска были созданы новые данные.

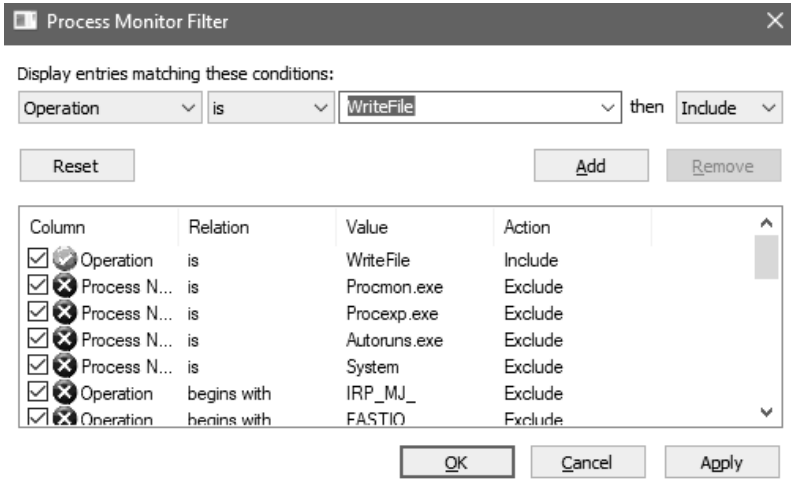

Рис. 44. Создание фильтра

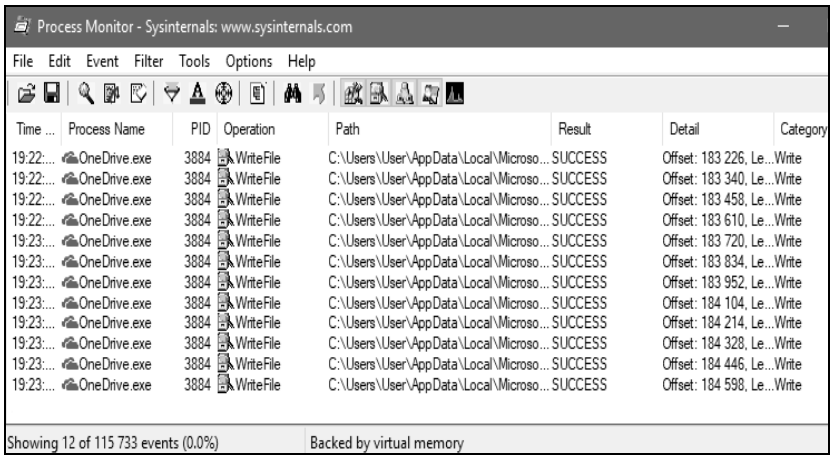

Рис. 45. Результат действия фильтра

4. Задание на лабораторную работу

1. Задать через командную строку перезагрузку компьютера через минуту после первого сбоя.
2. Назначить автоматический запуск калькулятора после входа в Windows.
3. Заменить стандартный диспетчер задач на Process Explorer.
4. Определить какой раздел реестра «Сапер» делает записи о рекордах.
5. Вывести информацию о Cookies при работе Internet Explorer.
6. Определить какие файлы реестра открывает косынка.
7. Определить какие системные файлы читает при работе WMPlayer.
8. Определить какой процесс запускается при открытии “Установки и удаления программ”.
9. Определить в какой файл записываются данные при работе с калькулятором.

5. Контрольные вопросы

1. Что такое служба Windows?
2. Какие средства для управления службами предусмотрены в Windows?
3. В каких состояниях может находиться служба?
4. Какие действия могут применяться при сбое службы?
5. Правами каких учётных записей может обладать служба при запуске?
6. Чем отличаются команды для управления службами семейств net и sc?
7. Какие команды используются для изменения состояния и типа запуска служб?
8. Чем отличается процесс от потока?
9. Как с помощью Process Explorer определить, каким процессом открыто определенное окно?
10. По каким параметрам можно создавать фильтры в Process Monitor?

ЛАБОРАТОРНАЯ РАБОТА №3
Управление ресурсами в ОС Windows

1. Цель работы

Целью данной работы является изучение основ работы с логическими дисками. Изучение функциональных возможностей файловых систем (на примере NTFS): шифрование файлов, управление дисками, дисковые квоты, дефрагментация и резервное копирование данных. А также работа с оснасткой «Системный монитор», журналами и оповещениями производительности.

2. Краткие теоретические сведения

Файловая система NTFS (New Technology File System) разрабатывалась Microsoft как основная файловая система для серверных версий операционных систем Windows.

Данный тип файловой системы включает в себя ряд возможностей:

- восстанавливаемость – способность файловой системы возвращаться к работоспособному состоянию после возникновения сбоя;
- безопасность – защищенность файлов от несанкционированного доступа;
- шифрование – преобразование файла в зашифрованный код, который невозможно прочесть без ключа;
- дисковые квоты для пользователей – возможность выделения для каждого пользователя определенного пространства на диске (квоты). NTFS не позволяет пользователю записывать данные на диск сверх выделенной квоты.

Системный монитор Windows используется для анализа влияния работы программ на производительность компьютера как в реальном времени, так и посредством сбора данных журнала для последующей обработки. Для этого используются счетчики производительности, данные трассировки событий и сведения о конфигурации, которые можно объединять в группы сборщиков данных.

Счетчики производительности являются инструментами оценки состояния или активности системы. Они могут входить в состав операционной системы или быть частью отдельных приложений. Системный монитор Windows запрашивает текущие показания счетчиков производительности через определенные промежутки времени.

Данные трассировки событий собираются от поставщиков трассировки, которые являются компонентами операционной системы или отдельных приложений, оповещающими о выполнении действий или

возникновении событий. Выходные данные нескольких поставщиков трассировки могут объединяться в сеанс трассировки.

Сведения о конфигурации содержат значения параметров реестра Windows. Системный монитор Windows сохраняет значения параметров реестра в файле журнала в определенные моменты или через определенные интервалы времени.

3. Ход работы

3.1. Управление дисками

Войдите в систему под учетной записью «Администратор». Вызовите консоль управления MMC и добавьте оснастку «Управление дисками» (рис. 1).

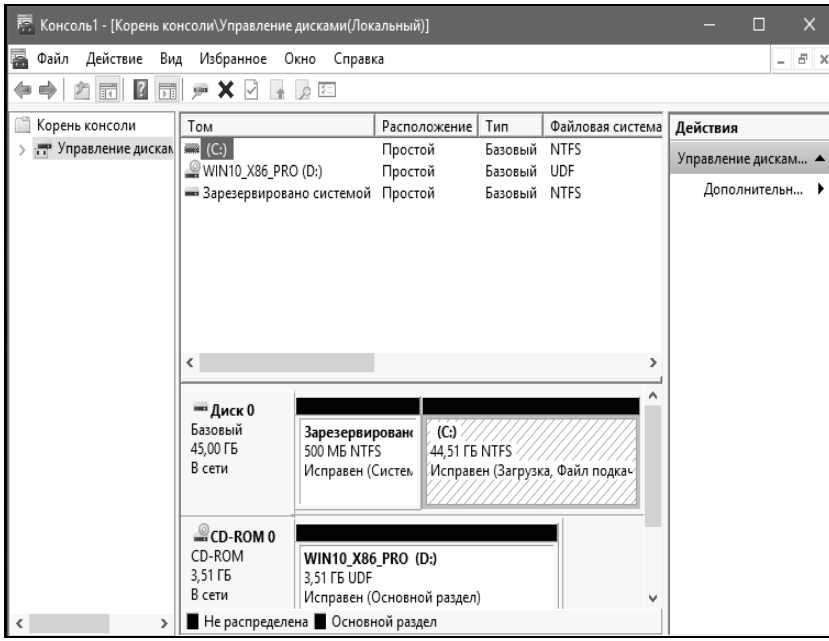

Рис. 1. Управление дисками

При создании логического диска необходимо отформатировать раздел в файловой системе NTFS. В открывшемся окне можно установить размер кластера на диске, присвоить диску собственную метку и др. Добавить раздел можно с помощью контекстного меню (рис. 2). При форматировании диска метку раздела назначить как «Docs» (рис. 3).

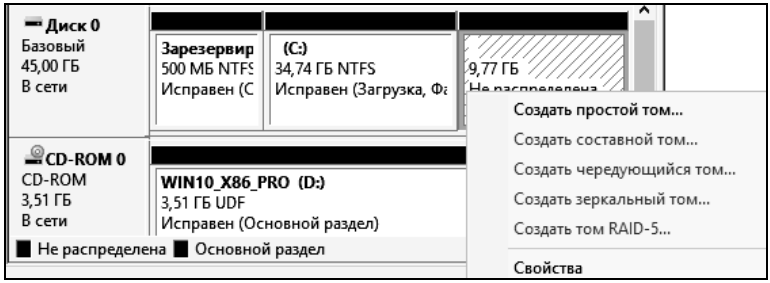

Рис. 2. Создание логического диска

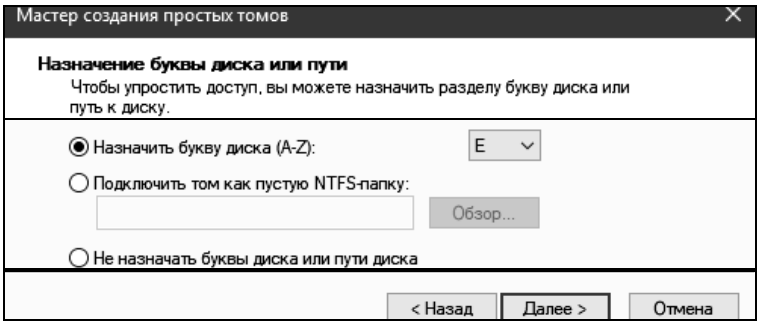

Рис. 3. Создание нового тома

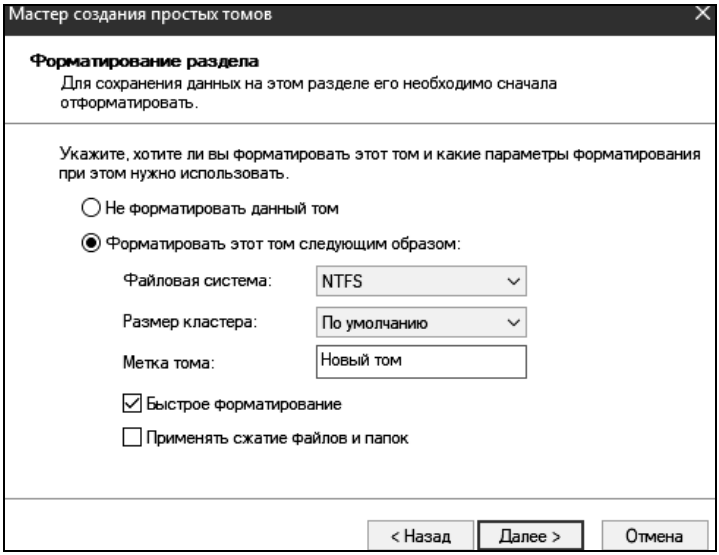

Рис. 4. Форматирование нового логического диска

Измените метку логического диска C:\ на «System». Метка существующего диска изменяется на вкладке «Общие» свойств диска (рис. 5).

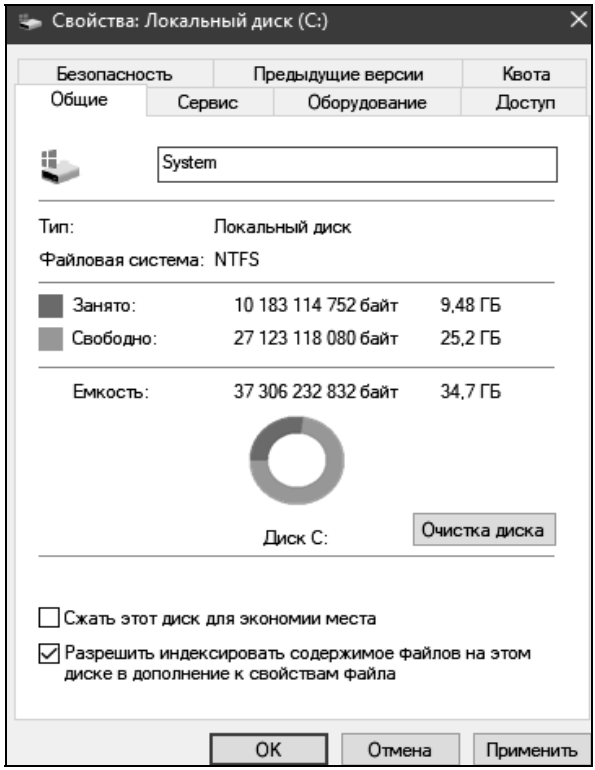

Рис. 5. Окно «Свойства логического диска»

Измените букву диска CD-ROM на E:\. Чтобы изменить букву диска, в контекстном меню диска выберите «Изменить букву диска или путь к диску» (рис. 6). При изменении буквы диска необходимо убедиться, что эта буква не задействована.

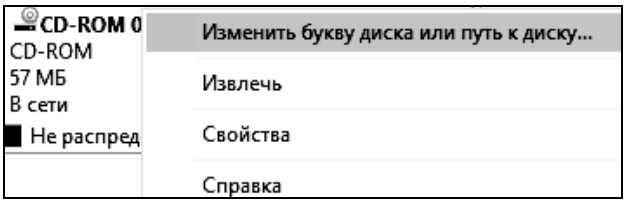

Рис. 6. Контекстное меню управления логическим диском

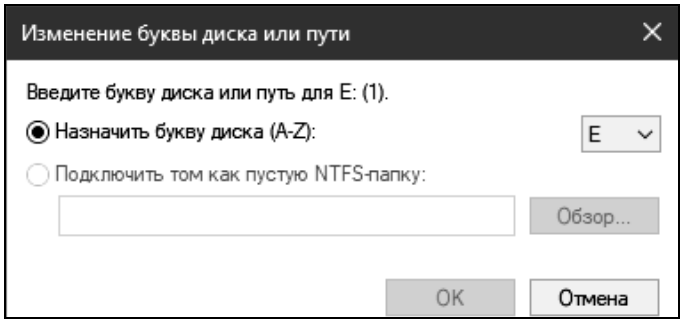

Рис. 7. Изменение буквы диска

Создайте папку с данными и зашифруйте её (Свойства папки – Общие – Другие – Шифровать содержимое для защиты данных). Атрибут, показывающий зашифрована ли папка, представлен на рис. 8.

Проверьте отсутствие возможности просмотреть файл под учётной записью «User».

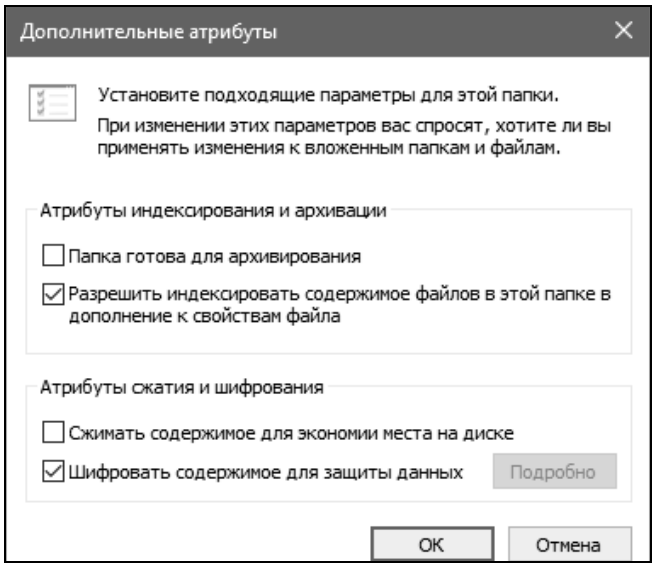

Рис. 8. Шифрование папки

Под учётной записью пользователя, зашифровавшего папку, скопируйте файл из зашифрованной папки в незашифрованную (рис. 7). Проверьте состояние атрибута шифрования у скопированного файла.

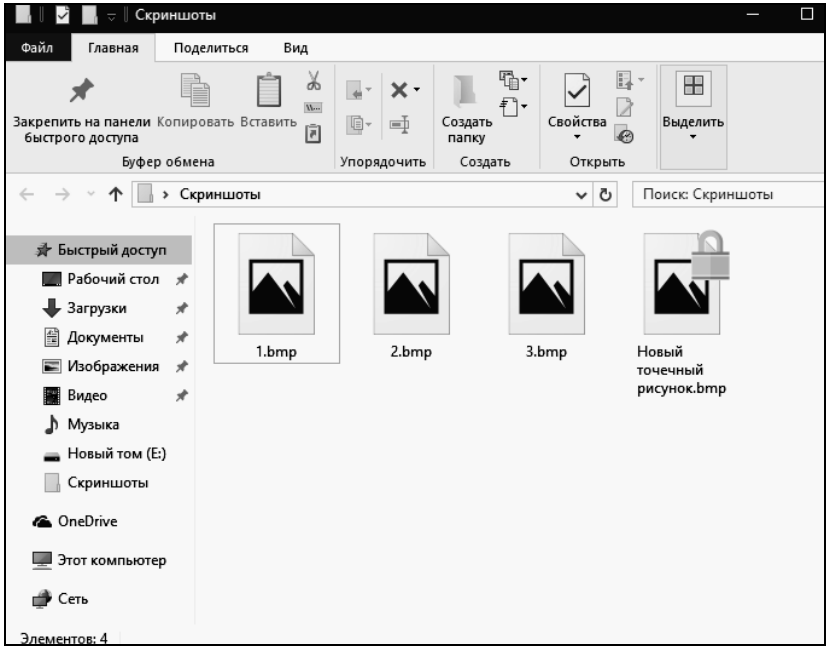

Рис. 9. Список файлов

Под учётной записью пользователя, зашифровавшего папку, скопируйте файл из незашифрованной папки в зашифрованную. Проверьте состояние атрибута шифрования у скопированного файла.

Войдите под учетной записью «User». Создайте и зашифруйте файл. Для предоставления доступа к зашифрованному файлу другим пользователям откройте окно «Дополнительные атрибуты» у выбранного файла (Свойства – Общие – Другие – Подробно).

В разделе «Атрибуты сжатия и шифрования» нажмите кнопку «Подробно» и нажмите кнопку «Добавить» (рис. 10). Выберите пользователя, которому необходимо предоставить доступ к данному зашифрованному файлу.

Под учётной записью «Администратор» в свойствах диска E:\ выберите вкладку «Квота» (рис. 11). Включите управление квотами.

Ограничьте место, выделяемое на диске значением 10 МБ, установите порог выдачи предупреждения, равным 5 МБ. Включите регистрацию превышения квоты и порога предупреждения (рис. 12).

Под учётной записью «User» создайте данные размером более 5 и менее 10 МБ. Под учётной записью «Администратор» просмотрите записи квот – проверьте наличие записи о превышении порога предупреждения.

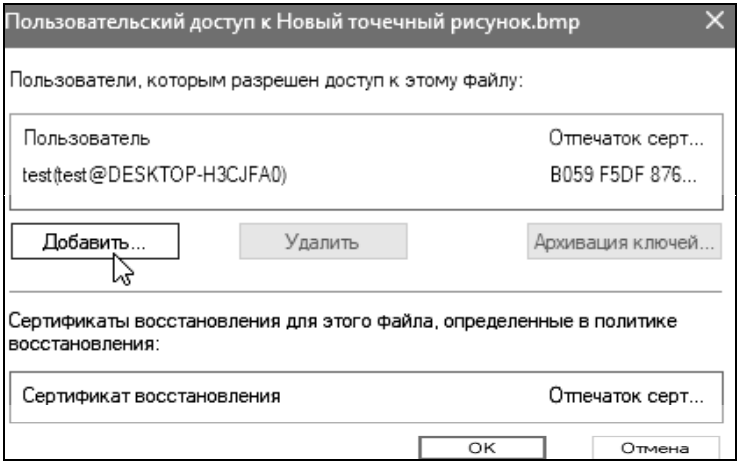

Рис. 10. Выбор пользователя

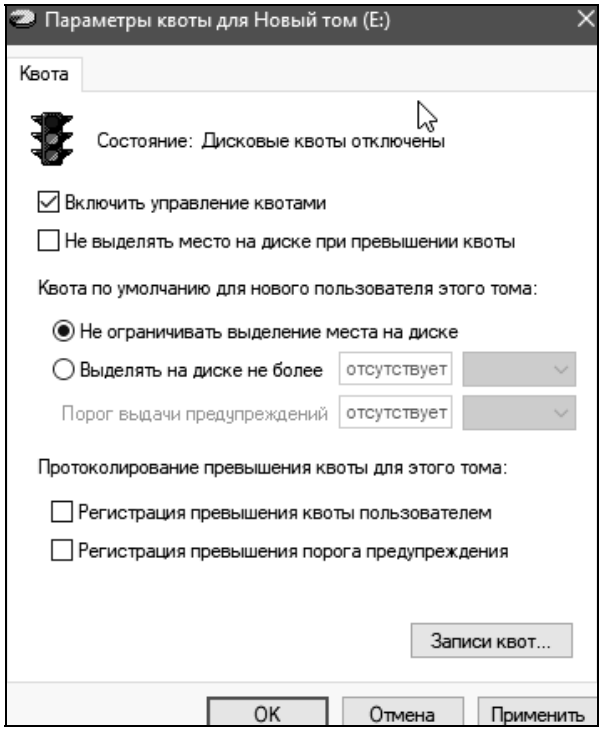

Рис. 11. Управление дисковыми квотами

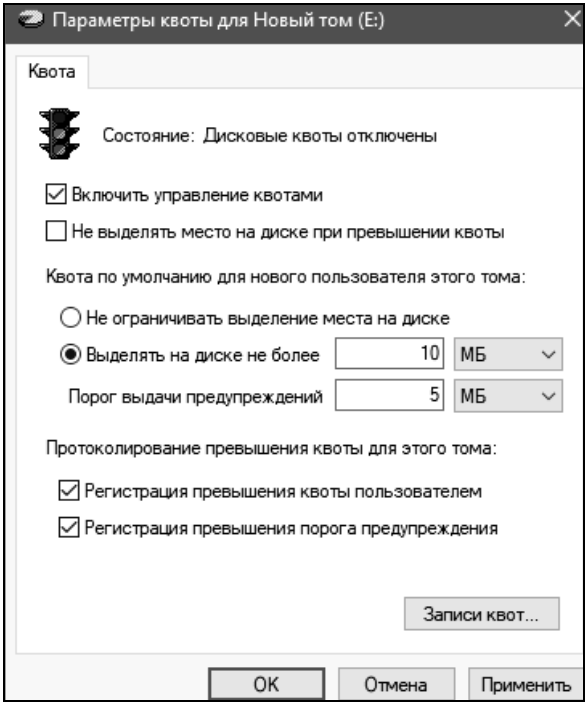

Рис. 12. Управление дисковыми квотами

Под учётной записью «User» создайте данные размером более 10 МБ. Под учётной записью «Администратор» просмотрите записи квот – проверьте наличие записи о превышении квоты. Записи квот предоставляют возможность просматривать только текущее состояние использования квот (рис. 13).

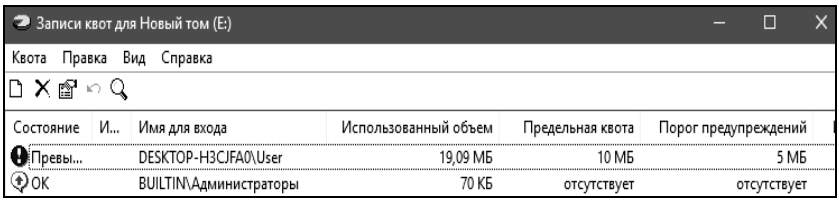

Рис. 13. Записи квот

Удалите данные, созданные под учётной записью «User». Установите запрет на превышение квоты на вкладке «Квоты». Под учётной записью «User» попытайтесь создать данные размером более 10 МБ.

В случае, когда пользователь исчерпал выделенное ему пространство на диске, можно выделить дополнительное пространство на диске. Откройте вкладку «Квота» и затем щелкните на «Записи квот». Вызовите контекстное меню нужного пользователя и затем нажмите «Свойства» для изменения границы квоты данного пользователя (рис. 14).

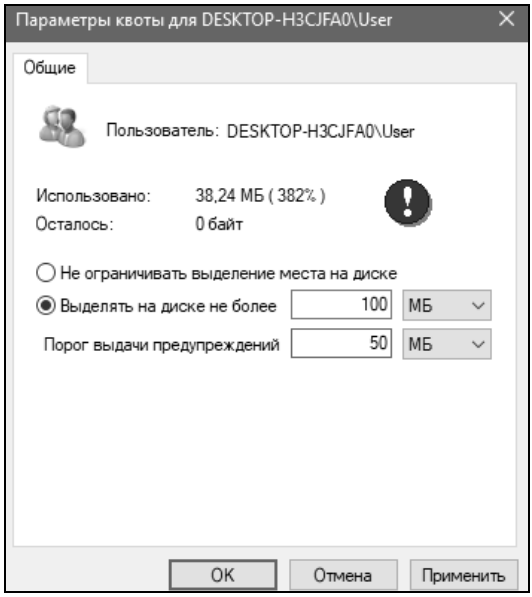

Рис. 14. Изменение границы квоты для пользователя

Для того чтобы открыть утилиту «Архивация и восстановление файлов», откройте Панель управления и выберите пункт «Резервное копирование и восстановление (Windows 7)» (рис. 15).

С выходом Windows 7 изменения в возможностях архивации затронули не только технологии, но и пользовательский интерфейс. В частности:

– переработан интерфейс главного окна элемента панели управления «Архивация и восстановление»;

– создан новый пользовательский интерфейс для управления пространством, занятым под резервные копии;

– упрощено восстановление файлов, выполняющееся с помощью мастера;

– реализована интеграция с центром поддержки для своевременного уведомления пользователей о необходимости создания резервной копии.

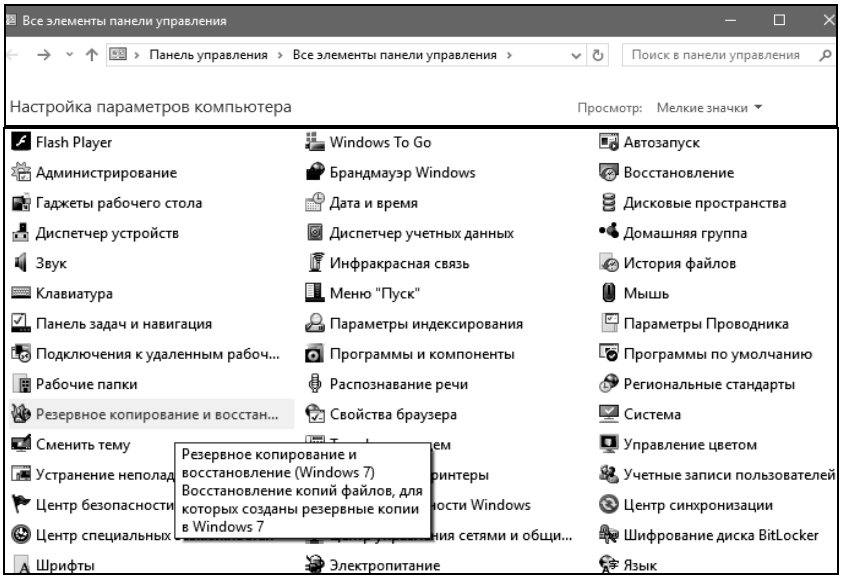

Рис. 15. Вызов восстановления файлов из Панели управления

Для того, чтобы организовать на данном компьютере резервирование данных, нажмите на кнопку «Настроить резервное копирование» (рис. 16).

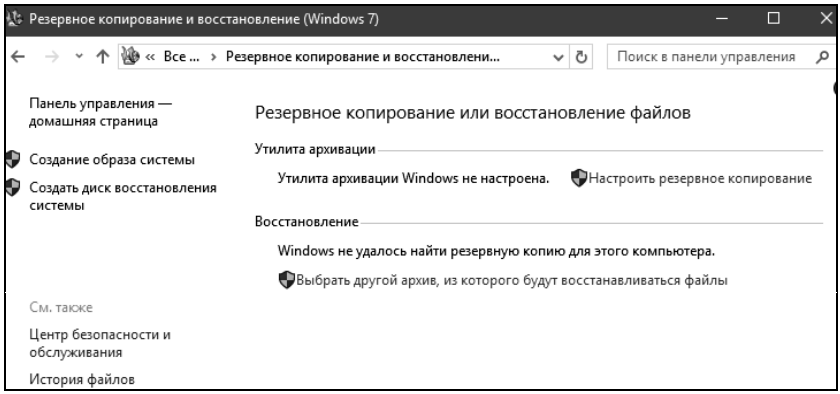

Рис. 16. Интерфейс восстановления файлов

В результате будет запущено окно настройки архивации. В первую очередь от пользователя потребуется указать место для хранения архивов с зарезервированными файлами. Чтобы задать его, нажмите кнопку «Сохранить в сети» (рис. 17). Для указания сетевого окружения нажмите «Обзор».

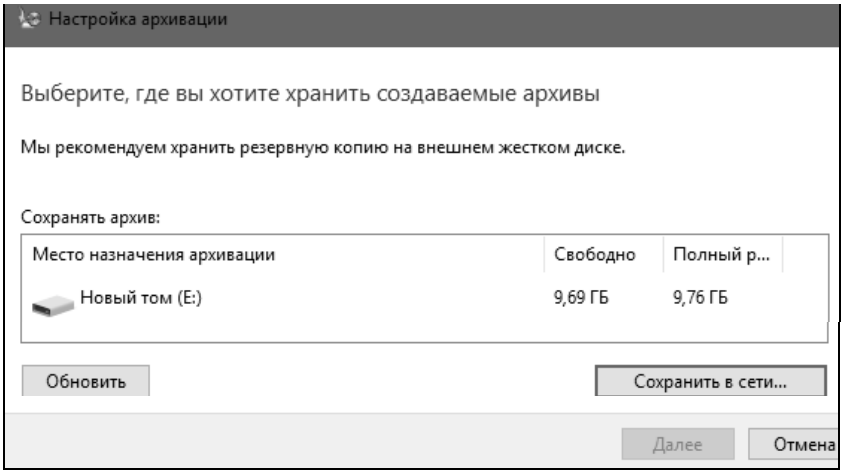

Рис. 17. Начало организации резервирования

Среди дерева папок выберите ту, в которую будете сохранять резервируемые данные, и нажмите «Ок» (рис. 18). После задайте данные для пользователя, имеющего доступ к данной директории, и перейдите к дальнейшей работе (рис. 19).

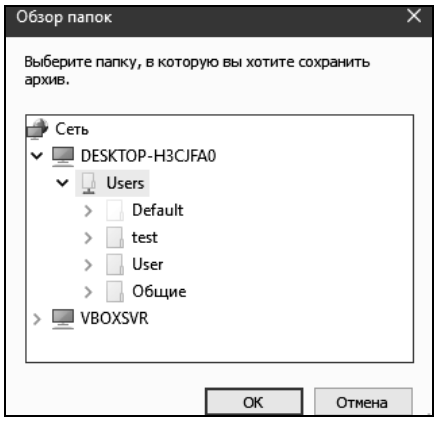

Рис. 18. Выбор директории для сохранения архива

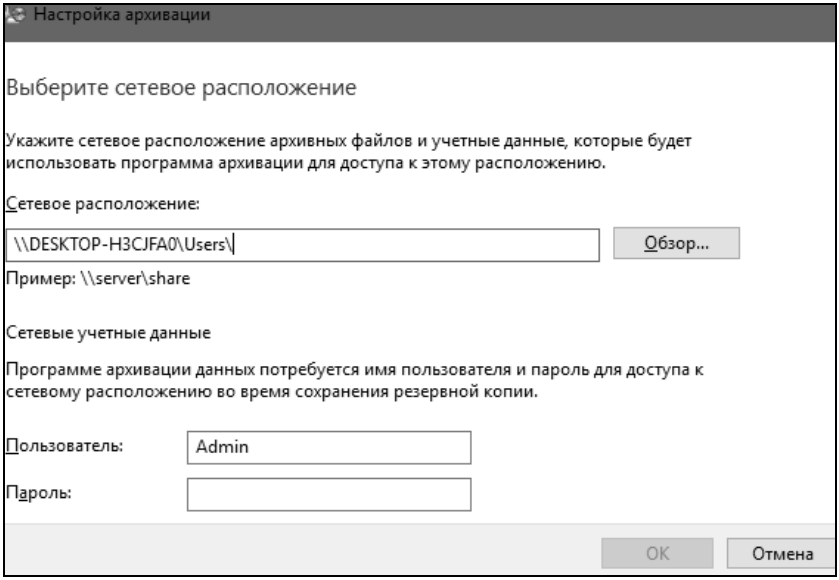

Рис. 19. Настройка сетевого положения

После этого в окне настройки архивации появится вариант сохранения в директорию, указанную Вами в ходе предыдущих действий, с уведомлением о состоянии памяти на данном жестком диске (рис. 20). Выберите в списке архивов для сохранения зарегистрированную директорию и нажмите «Далее».

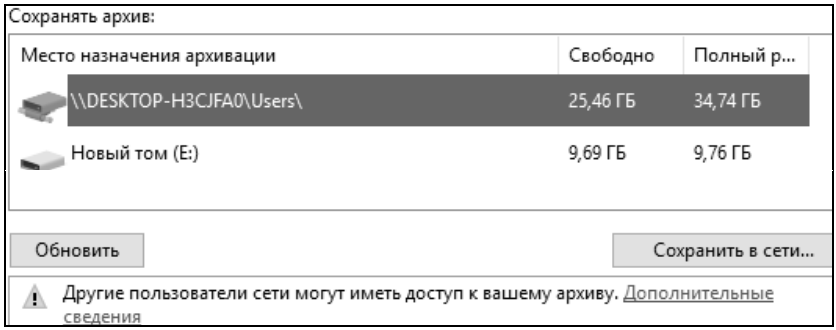

Рис. 20. Заданная директория в настройках архивации

Windows 10 позволяет создавать как резервные копии папок, так и полный образ разделов жесткого диска.

В случае сохранения пользовательских файлов – сохранение происходит на уровне файлов путем добавления к первоначальному архиву (если таковой уже был) только изменившихся файлов. Сохранение резервных копий возможно на разделы NTFS и FAT32. Для сжатия используется формат .ZIP. В данном формате возможно восстановление отдельных папок и библиотек.

Если создается образ раздела жесткого диска, то архивация производится на уровне блоков (в архив включаются только используемые блоки), а сохранение резервных копий возможно только на разделы NTFS. Полный образ сохраняется в формате VHD, при этом сжатия файлов не происходит.

В дальнейшем образы создаются инкрементно, т.е. добавляются только изменившиеся блоки. Для этого используются теневые копии. Последующее создание полных образов также возможно. Образы разделов дают возможность быстрого восстановления ОС и файлов в случае выхода из строя жесткого диска.

Выберите пункт «Предоставить мне выбор» и перейдите к следующему шагу.

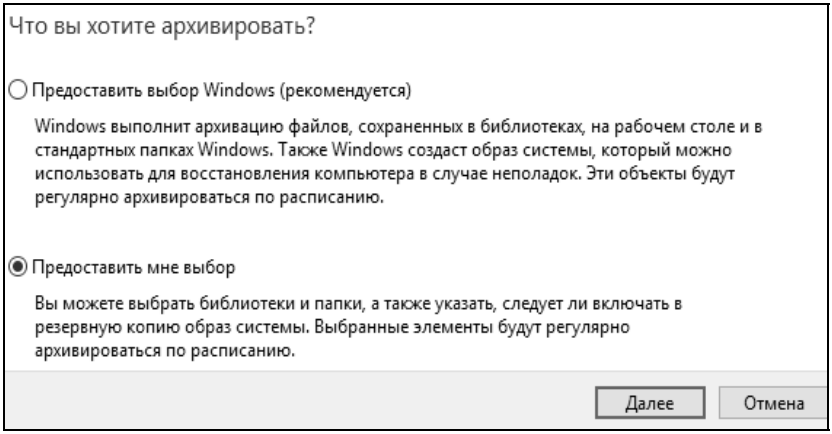

Рис. 21. Выбор шаблона по типу резервирования

При самостоятельном выборе Вы можете создать резервные копии:

– пользовательских файлов, включая библиотеки;

– папок локального диска;

– полного образа системы.

Укажите данные, необходимые для резервирования, и перейдите к дальнейшей работе.

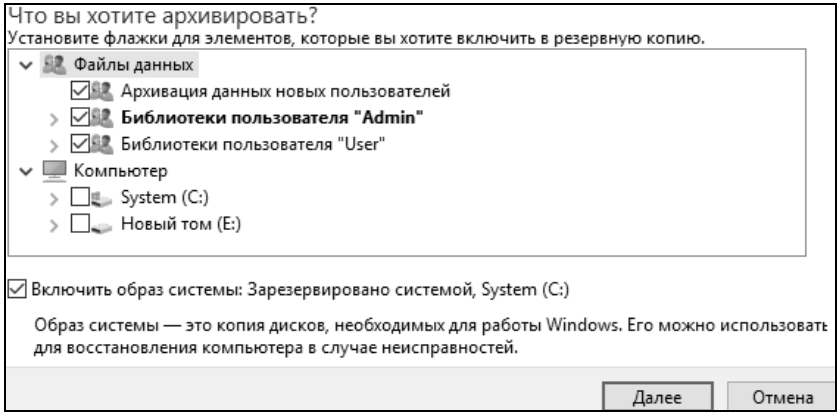

Рис. 22. Выбор файлов для резервирования

В конце средство восстановления файлов Windows 7 выводит сводку параметров резервного копирования. Проверьте правильность заданных Вами параметров и запустите архивацию (рис. 23).

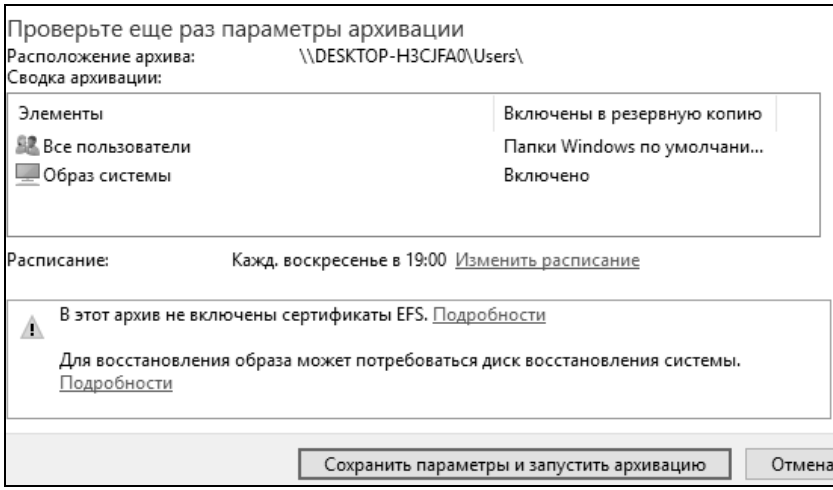

Рис. 23. Проверка заданных параметров

После запуска архивации – ее прогресс можно будет отследить в открывшемся окне. В случае возникновения ошибки – из него можно будет посмотреть сведения о происходящем и изменить параметры (рис. 24).

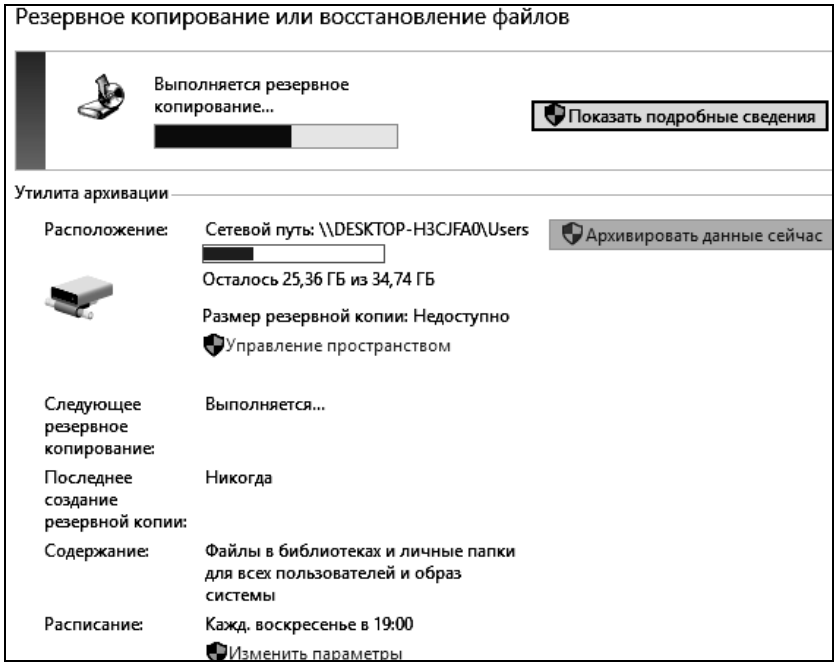

Рис. 24. Отслеживание прогресса архивации и восстановления

Из данного окна, в частности, можно изменить параметры расписания запуска архивации (рис. 25), указав периодичность и время начала архивации либо задав единовременное резервирование.

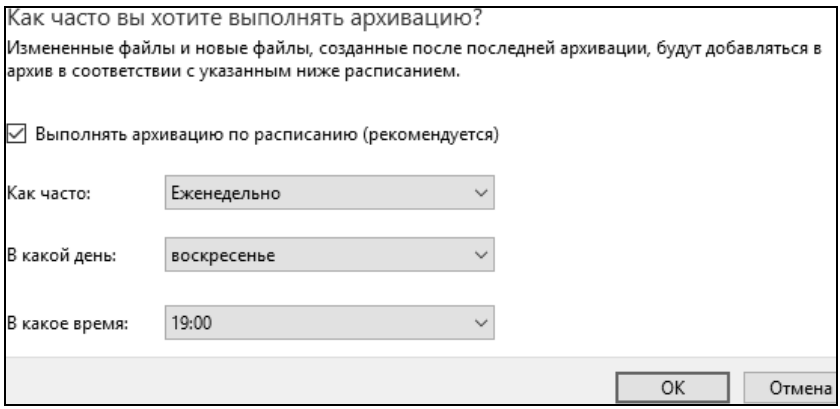

Рис. 25. Задание расписания резервирования

После завершения архивирования нажмите на кнопку «Восстановить мои файлы». Будет предложено выбрать источник для восстановления (рис. 26).

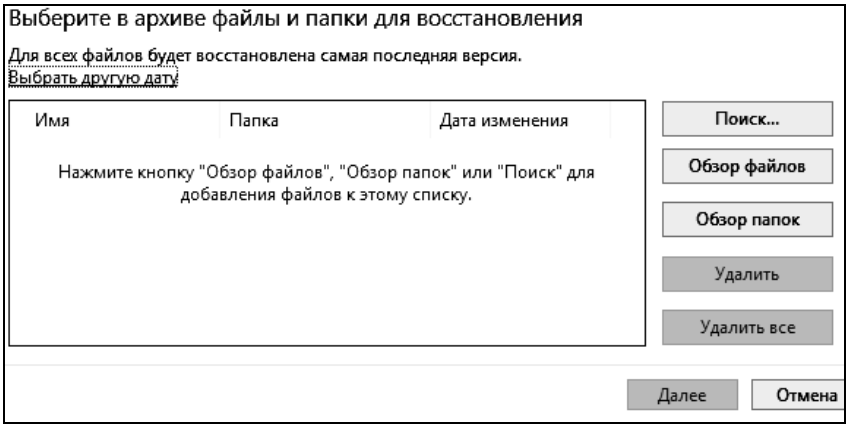

Рис. 26. Выбор архива для восстановления

Также в главном окне возможно удаление ненужных архивов с зарезервированными данными, для этого нужно кликнуть на ссылку «Управление пространством» и нажать на кнопку «Просмотреть архивы» (рис. 27).

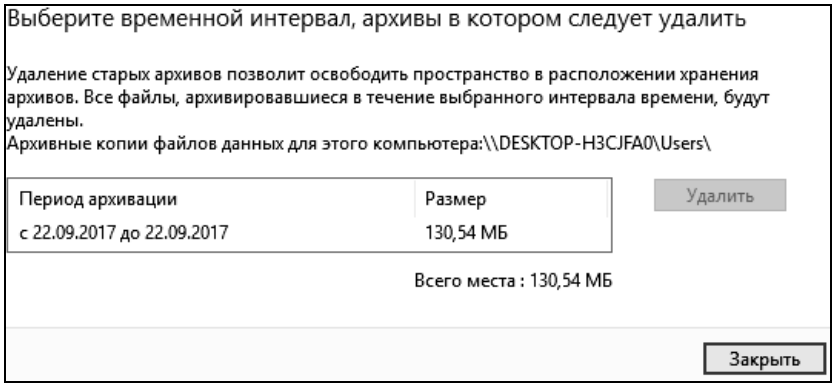

Рис. 27. Управление дисковым пространством архивации

При запуске восстановления из архива, будет показан поиск файлов в данном архиве, необходимых для восстановления.

Откройте через «Проводник» папку, в которую был сохранен архив с зарезервированными Вами данными (рис. 28). Запустите файл с архивом. В результате, будет выведено окно программы по архивации данных с предложением восстановить файлы из текущей резервной копии (рис. 29).

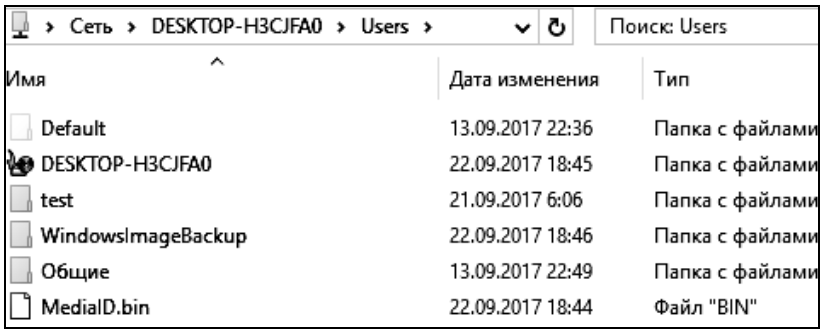

Рис. 28. Директория с архивом файлов

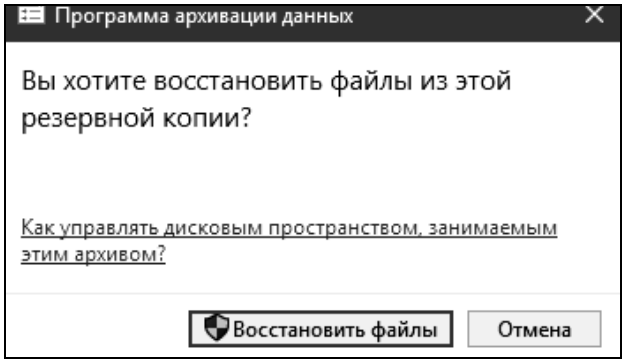

Рис. 29. Предложение восстановления из архива

Высокая степень фрагментации файлов заставляет жесткий диск совершать дополнительные действия, что приводит к замедлению работы компьютера. Файлы на съемных запоминающих устройствах таких, как USB-устройства флэш-памяти, также могут стать фрагментированными. Программа дефрагментации диска производит упорядочение фрагментированной информации для более эффективной работы дисков и дисководов. Программа дефрагментации диска работает по заданному расписанию, но можно запускать анализ и дефрагментацию дисков вручную.

В Windows 10 дефрагментация диска называется «Дефрагментация и оптимизация ваших дисков». Для запуска данной программы наберите ее название в поиске меню «Пуск» (рис. 30) или выберите соответствующий пункт в меню «Свойства» для необходимого диска (рис. 31).

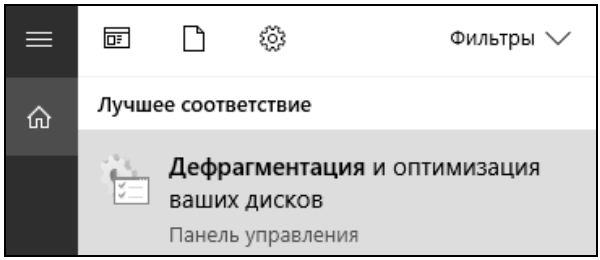

Рис. 30. Вызов дефрагментации из меню «Пуск»

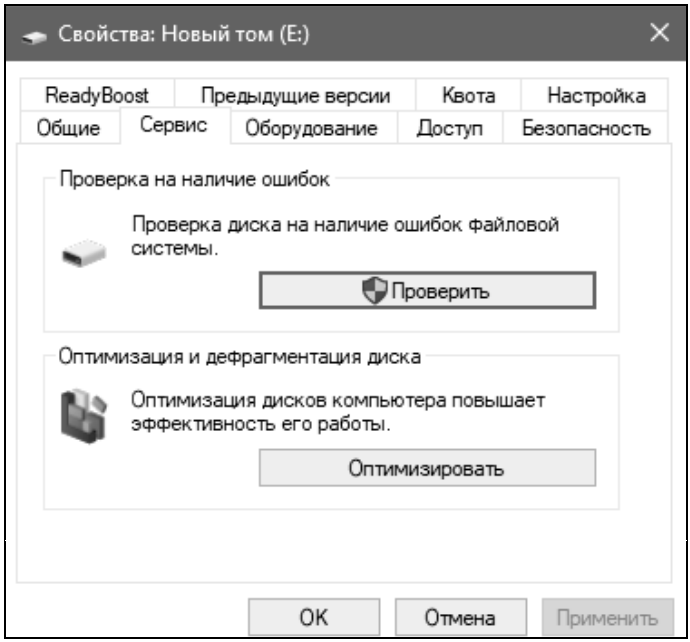

Рис. 31. Вызов дефрагментации из меню свойств диска

Откроется программа, где вы увидите список ваших дисков, тип носителя, прошлый запуск и текущие состояние (фрагментировано %) (рис. 32).

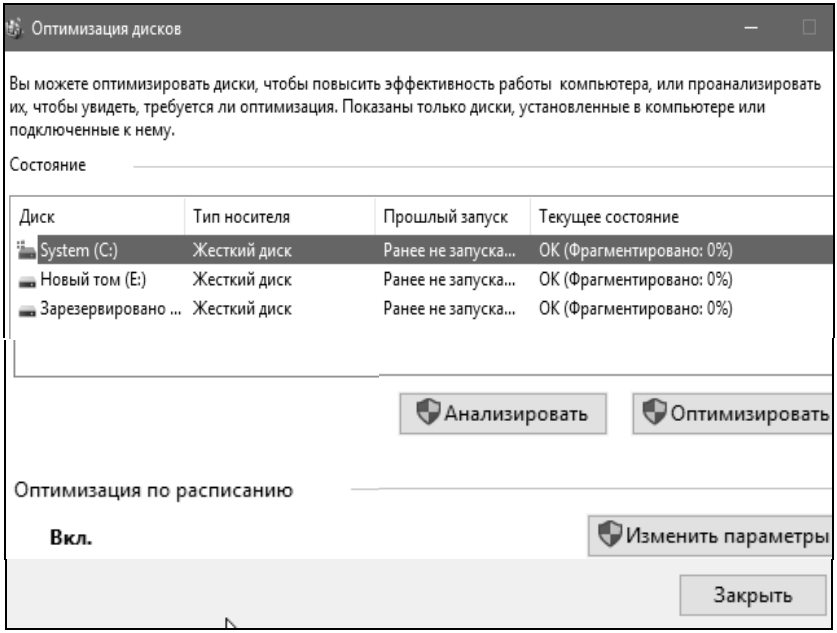

Рис. 32. Интерфейс оптимизации дисков

В Windows 10 диски автоматически запланированы для оптимизаций на еженедельной основе (оптимизация дисков происходит в фоновом режиме, поэтому пользователи её могут не замечать). Также можно вручную оптимизировать или дефрагментировать диски в Windows 10, выбрав диск и нажав на кнопку «Оптимизировать». В зависимости от размера диска и степени фрагментации файлов для дефрагментации может потребоваться от нескольких минут до нескольких часов. Во время дефрагментации работу с компьютером можно не прерывать.

Если вы хотите изменить расписание оптимизаций, то нажмите на кнопку «Изменить параметры».

Вы можете отключить автоматическую дефрагментацию, убрав галочку рядом с надписью «Выполнять по расписанию», или вы можете изменить её от еженедельной до ежедневной или ежемесячной (рис. 33).

Также вы можете выбрать все диски или конкретный для автоматической дефрагментации, нажав кнопку «Выбрать». Ещё можно поставить галочку рядом с надписью «Автоматически оптимизировать новые диски» для того, чтобы новые диски, которые подключены к компьютеру, тоже оптимизировались по расписанию (рис. 34).

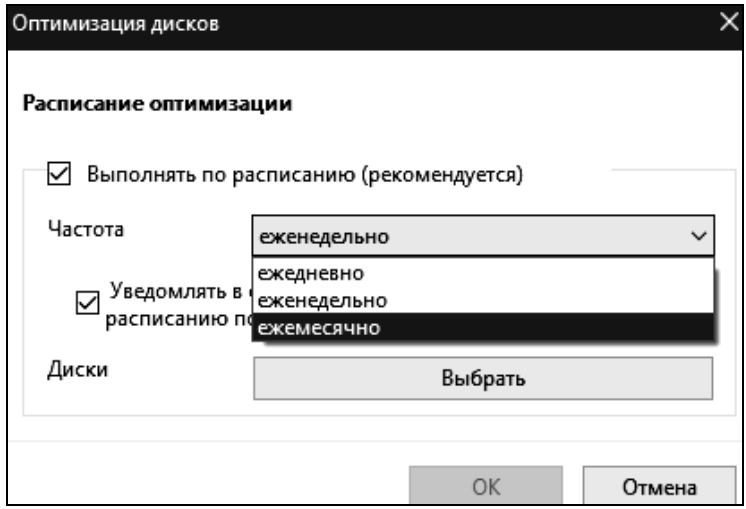

Рис. 33. Изменение частоты проведения дефрагментации

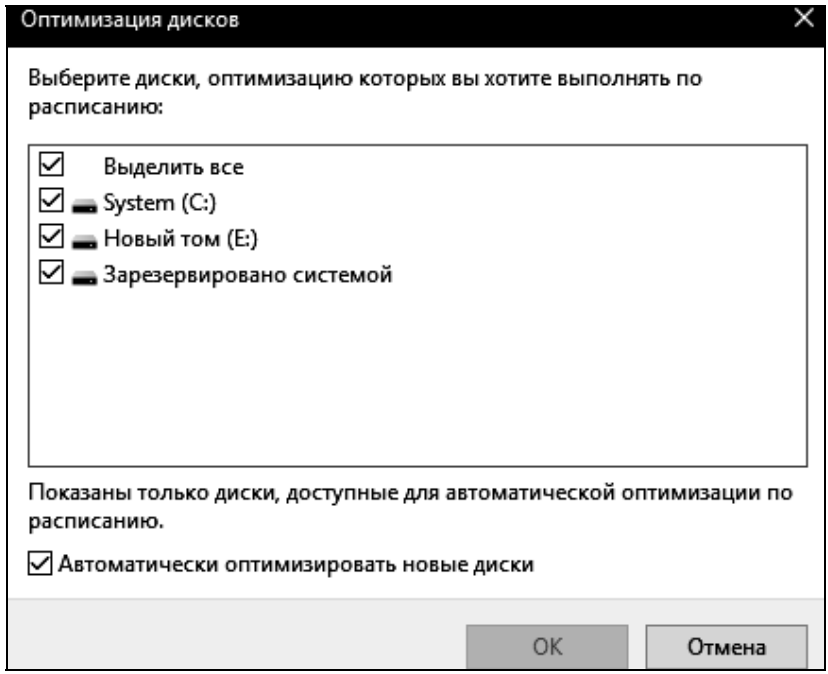

Рис. 34. Выбор дисков подлежащих дефрагментации по расписанию

3.2. Мониторинг производительности

Значения счетчиков объектов сохранять как таблицу результатов (например: MS Excel).

Для работы с системным монитором в меню «Пуск» выберите пункт «Выполнить», в диалоговом окне «Выполнить» введите «perfmon» и нажмите кнопку «OK» (рис. 35).

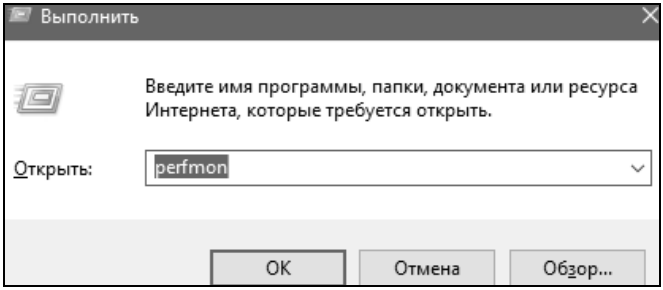

Рис. 35. Вызов системного монитора

По умолчанию отображается график загруженности процессора. Вертикальная красная линия на графике указывает на текущий момент времени. Также пользователю предоставляется инструментальная панель; область значений (с текущим, минимальным, максимальным и средним значением выбранного счётчика); легенда, отображающая отображаемые счётчики.

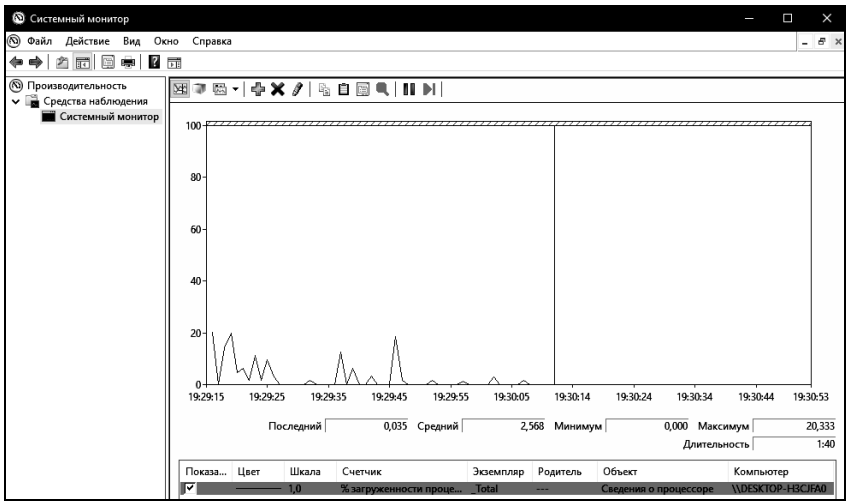

Рис. 36. Системный монитор

На инструментальной панели доступны следующие возможности: просмотр текущей активности  , просмотр данных журнала  , изменение типа диаграммы  (на строку, линейчатую диаграмму и отчет), добавление  , удаление  и выделение счетчика цветом на графике  . Возможно копирование свойств выбранных счётчиков  , и возможна вставка в другое окно системного монитора скопированных счётчиков и их свойств  . Опробуйте возможности, предоставляемые инструментальной панелью.

Свойства системного монитора предоставляют следующие возможности:

– изменение периода съёма информации (вкладка «Общие», рис. 37);

– изменение цвета, масштаба и других характеристик выбранного графика (вкладка «Данные», рис. 38);

– изменение диапазона значений вертикальной оси (вкладка «График», рис. 39).

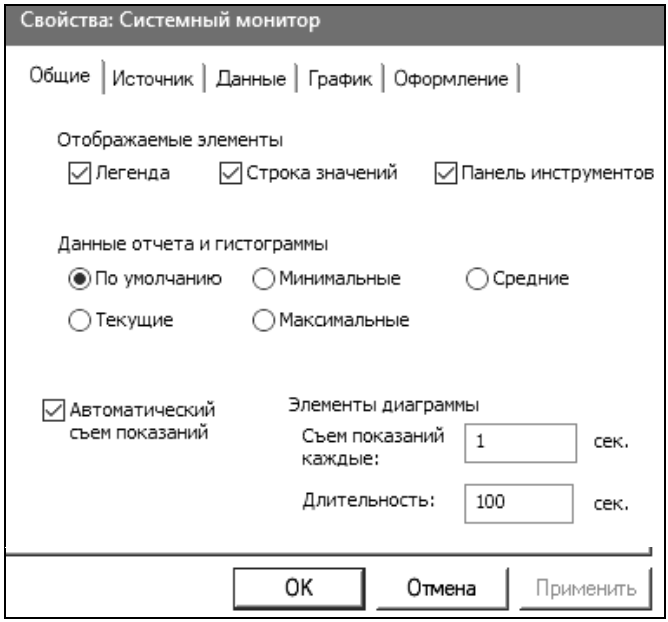

Рис. 37. Свойства системного монитора «Общие»

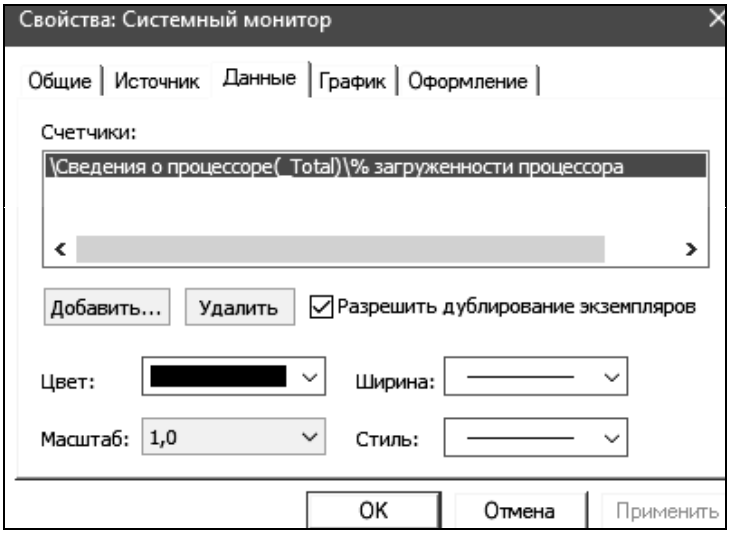

Рис. 38. Свойства системного монитора «Данные»

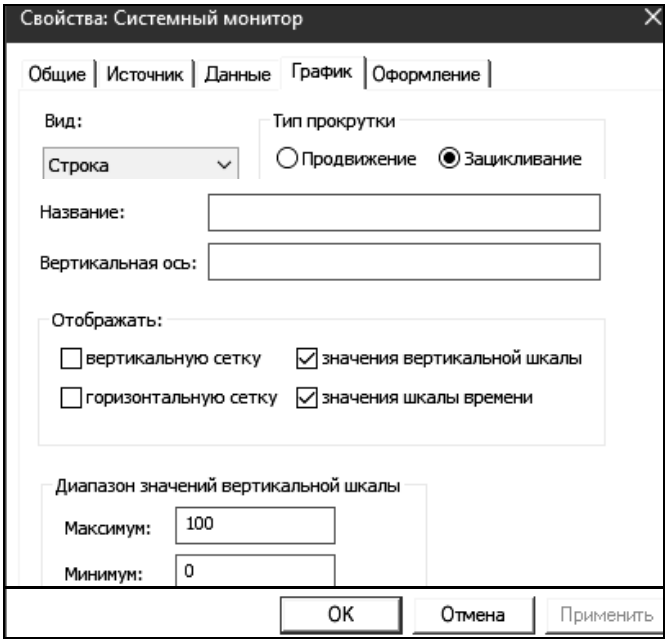

Рис. 39. Свойства системного монитора «График»

Опробуйте перечисленные возможности.

При добавлении счётчиков производительности (рис. 40) возможен выбор: целевого компьютера (локального или в локальной сети); объекта, информацию о котором будет снимать счётчик; типа счётчика, регистрирующего конкретный параметр работы объекта; одного или всех экземпляров выбранного объекта (одного из существующих процессоров, логических дисков и т.д.). Также возможен вызов объяснения по выбранному счётчику. Добавление счётчика производится нажатием кнопки «Добавить».

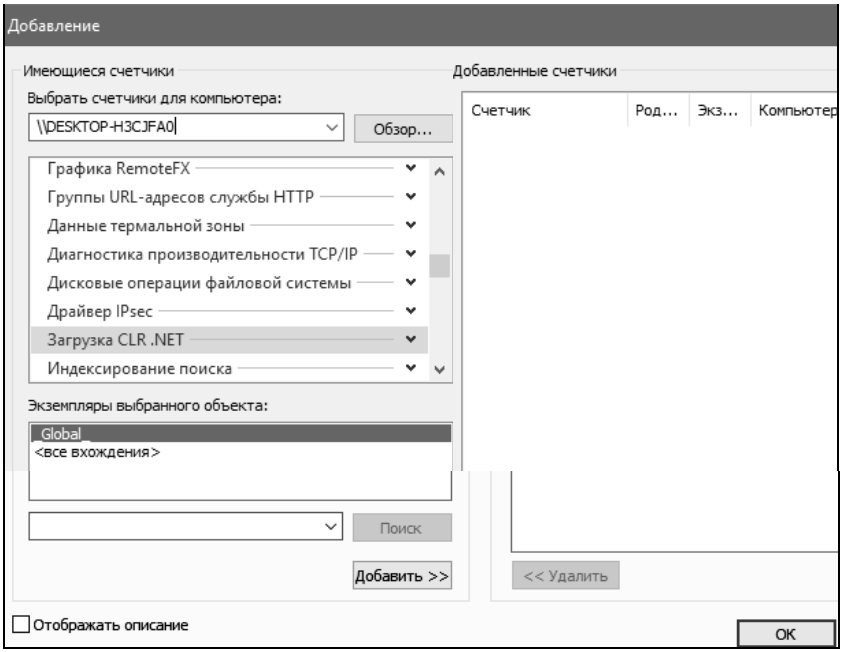

Рис. 40. Добавление счетчиков

Объект «Кэш». Добавьте счётчик «% попаданий при отображении данных». Зафиксируйте среднее значение при бездействии системы, при копировании данных и запуске программ. Удалите счётчик.

Значения счетчика смотреть в области значений (с текущим, минимальным, максимальным и средним значением выбранного счётчика). Остальные счетчики добавить по аналогии.

Объект «Логический диск». Добавьте следующие счётчики: обращений чтения с диска/сек, обращений записи на диск/сек.

Данные счетчики отражают частоту выполнения операций чтения с диска и записи на диск.

Зафиксируйте максимальные значения счётчиков при бездействии системы и при копировании данных. Удалите все выбранные счётчики.

Объект «Логический диск». Добавьте следующий счётчик: расщепления ввода-вывода/сек.

Вычисляет частоту, с которой операции ввода-вывода диска оказываются расщепленными на несколько операций ввода-вывода. Расщепление операций ввода-вывода может происходить либо из-за того, что запрошен слишком большой блок данных, который не может быть передан за одну операцию, либо из-за фрагментации диска. На расщепление I/O запроса влияет дизайн прикладных программ, файловая система или драйверы. Высокая норма расщеплений I/O не может сама по себе представлять проблему. Если речь идёт о единичном диске, высокая норма для этого счетчика может указывать на фрагментацию диска.

Зафиксируйте минимальные, средние и максимальные значения счётчиков. Удалите счётчик.

Объект «Физический диск». Добавьте следующие счётчики: скорость записи на диск, скорость чтения с диска. Зафиксируйте максимальные значения счётчиков при бездействии системы и при копировании файловых наборов. Удалите все выбранные счётчики.

Объект «Память». Добавьте следующие счётчики:

– «% использования выделенной памяти» показывает отношение значения «байт выделенной виртуальной памяти» к значению «предел выделенной виртуальной памяти». Если это значение очень велико (более 90 %), могут возникать сбои при фиксации. Это явный признак того, что в системе недостаточно памяти;

– «доступно МБ» показывает объем физической памяти в мегабайтах (МБ), непосредственно доступной для выделения процессу или использования системой. Эта величина равна сумме памяти, выделенной для резервной памяти (кэша), свободной памяти и обнуленных страниц памяти.

Запустите какие-либо программы. Зафиксируйте минимальные, средние и максимальные значения счётчиков. Удалите все выбранные счётчики.

Объект «Файл подкачки». Добавьте счётчик «% использования». Запустите какие-либо программы. Зафиксируйте минимальное, среднее и максимальное значения счётчика. Удалите счётчик.

Объект «Объекты» (рис. 41). Добавьте следующие счётчики: счётчик процессов и счётчик потоков, счётчик мьютексов, счётчик семафоров в разделе «Объекты». Запустите какую-либо программу (на-

пример, Internet Explorer). Зафиксируйте минимальные и максимальные значения счётчиков. Зафиксируйте количество потоков у выбранной программы, а также количество используемых мьютексов и семафоров. Удалите все выбранные счётчики.

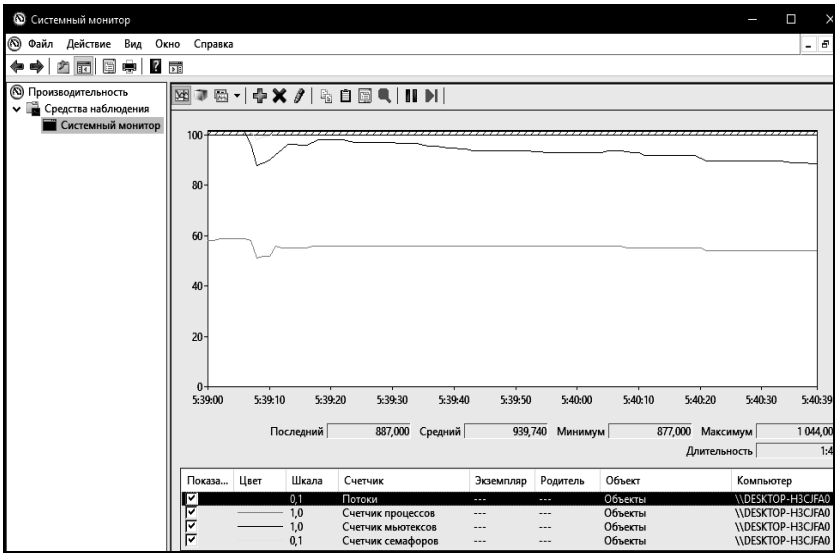

Рис. 41. Добавление счетчиков объекта «Объекты»

Объект «Процессор». Добавьте следующие счётчики: «% времени прерываний», «% работы в пользовательском режиме», «% работы в привилегированном режиме». Запустите какую-либо программу (например, калькулятор) и поработайте с ней. Зафиксируйте максимальные значения счётчиков до запуска программы и после запуска. Удалите все выбранные счётчики.

Объект «Процесс». Запустите какую-либо программу (например, Internet Explorer). Добавьте следующие счётчики: «% загруженности процессора», «базовый приоритет», «рабочее множество», «счётчик потоков», «I/O – обмен данными», «I/O – операций с данными в сек». Поработайте с программой. Зафиксируйте минимальные и максимальные значения счётчиков. Удалите все выбранные счётчики.

Объект «Система». Добавьте следующие счётчики: «длина очереди процессора, контекстных переключений/сек, системных вызовов/сек», «счётчик процессов». Зафиксируйте средние и максимальные значения счётчиков. Удалите все выбранные счётчики.

Для работы с журналами производительности в контекстном меню объекта «Системный монитор» выберите «Создать», «Группа сборщиков данных» (рис. 42).

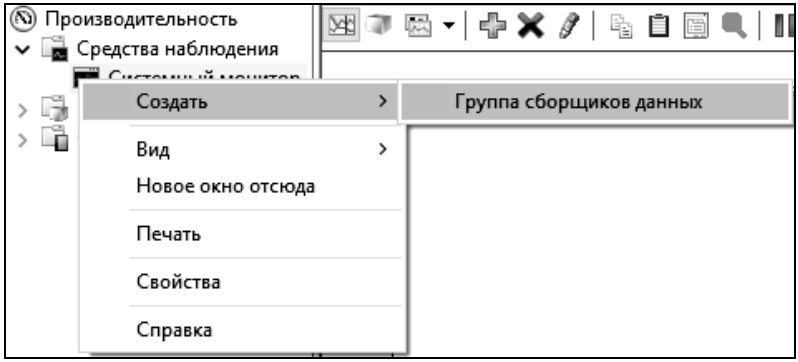

Рис. 42. Создание журнала

Введите имя новой группы (рис. 43), выберите папку для сохранения данных (рис. 44), пользователя и дальнейшее действие после создания группы (рис. 45).

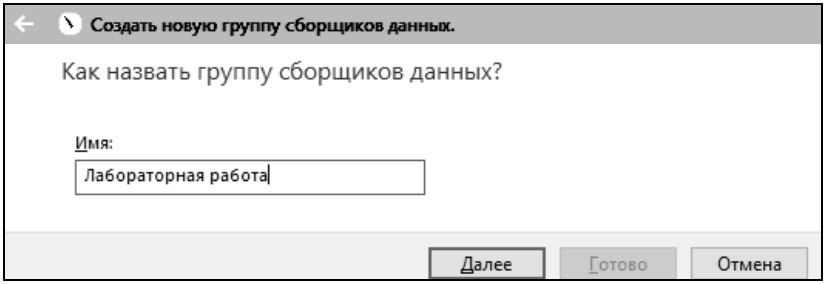

Рис. 43. Задание имени группы

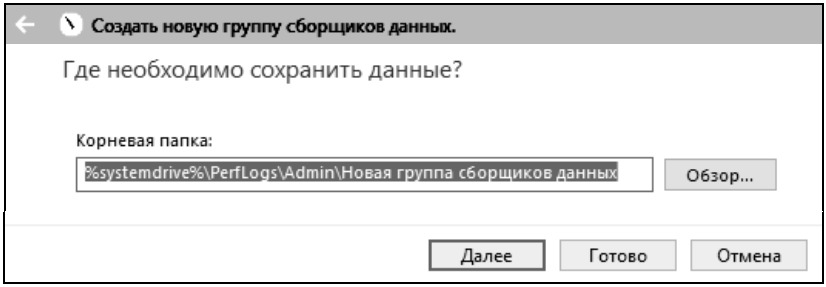

Рис. 44. Выбор папки для сохранения данных

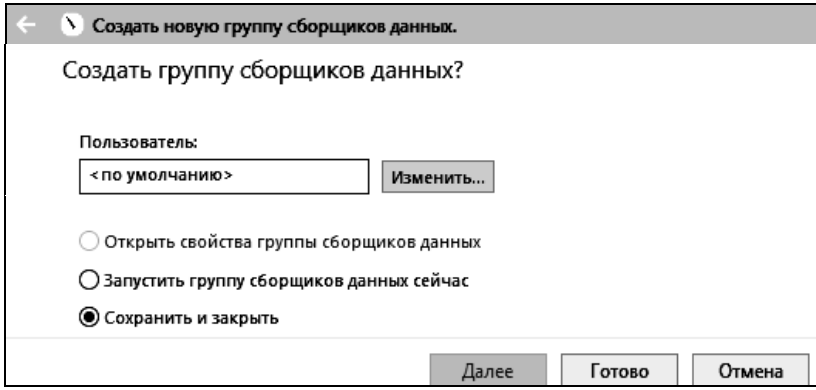

Рис. 45. Выбор пользователя и дальнейшего действия

После этого потребуется задать журнал данных. В свойствах журнала системного монитора (рис. 46) добавьте 5–6 счётчиков, установите интервал снятия данных, равным 1 сек. После этого нажмите «Ок».

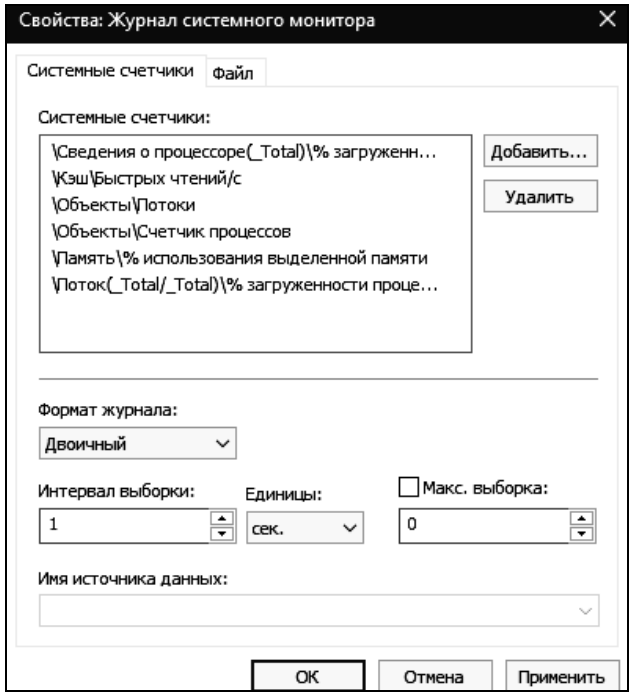

Рис. 46. Выбор счетчиков для записи

Запустите группу сборщиков данных, кликнув на значок . Через некоторое время остановите его и просмотрите полученный файл журнала в «Системном мониторе» (в свойствах «Системного монитора выберите просмотр файла журнала и откройте созданный журнал, после чего добавьте необходимый счётчик).

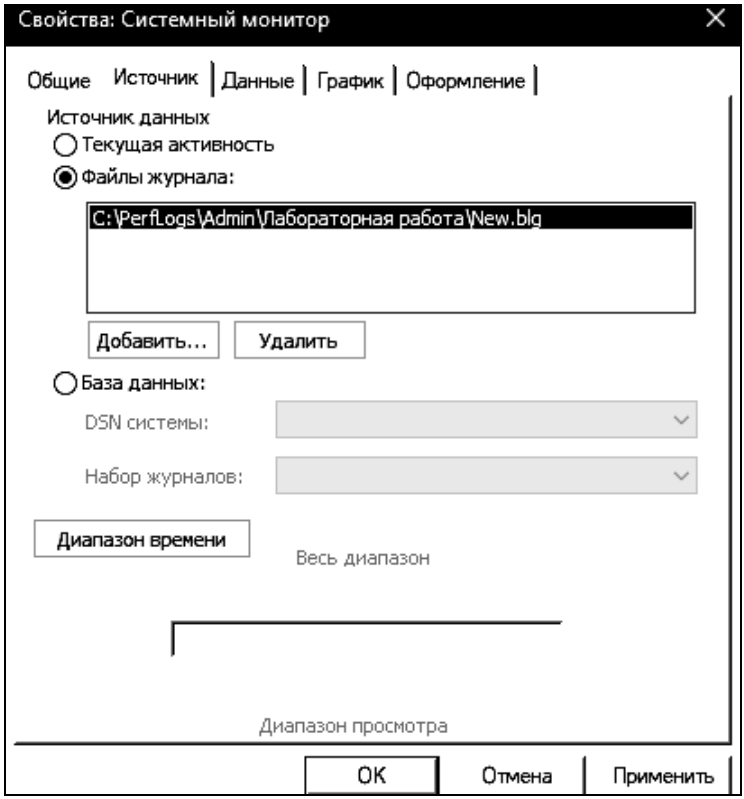

Рис. 47. Запуск журнала

4. Задание на лабораторную работу

1. Установите квоты на диске D:\ для указанных пользователей в соответствии с вариантом (см. таблицу). Осуществите архивирование в соответствии со своим вариантом и продемонстрируйте их отличие.

Варианты заданий

Вариант	Дисковые квоты		Параметры архивирования
	Администратор, МБ	Пользователь, МБ	
1	100	50	Обычное и ежедневное архивирование
2	200	75	Копирующее и разностное архивирование
3	500	500	Восстановление с исходным и альтернативным размещением
4	50	25	Обычное и копирующее архивирование
5	20	10	Добавочное и разностное архивирование
6	500	200	Восстановление в одну папку и с исходным размещением
7	50	50	Копирующее и ежедневное архивирование
8	250	100	Восстановление в одну папку и с альтернативным размещением
9	10	10	Обычное и разностное архивирование
10	10	5	Обычное и добавочное архивирование

2. Проведите диагностику работы виртуальной машины с помощью оснастки «Системный монитор».

5. Контрольные вопросы

1. Как сменить букву системного диска?
2. Что случится, если в зашифрованную папку одного пользователя добавить файлы другого пользователя? Возможна ли расшифровка этих файлов и папок. Если возможна, то каким образом?
3. Можно ли предоставить общий доступ к зашифрованной папке?
4. Для чего нужны квоты?
5. Каким образом можно назначить квоту конкретному пользователю?
6. Фиксируются ли попытки превышения квоты пользователем? Если «да», то где? Если «нет», то почему?
7. Для чего нужна архивация?
8. В чём особенности восстановления «В одну папку»?
9. Каково назначение атрибута «файл готов для архивирования»?
10. Чем отличаются обычное и добавочное резервное копирование?

ЛАБОРАТОРНАЯ РАБОТА №4
Восстановление работоспособности ОС Windows

1. Цель работы

Целью данной работы является изучение методики восстановления ОС «Windows», освоение практических навыков восстановления работоспособности ОС, технологии восстановления операционной системы после сбоя с помощью загрузочного диска Hiren.

2. Краткие теоретические сведения

Наиболее часто встречаются следующие причины сбоев при загрузке Windows:

– повреждение или удаление важных системных файлов, например, файлов системного реестра, ntoskrnl.exe, ntdetect.com, hal.dll, boot.ini;

– установка несовместимых (или неисправных) служб или драйверов;

– повреждение или удаление необходимых для системы служб или драйверов;

– физическое повреждение или разрушение диска;

– повреждение файловой системы, в том числе нарушение структуры каталогов, главной загрузочной записи (MBR) и загрузочного сектора;

– появление неверных данных в системном реестре (при физически не поврежденном реестре записи содержат логически неверные данные, например, выходящие за пределы допустимых значений для служб или драйверов);

– неверно установленные или слишком ограниченные права доступа к папке \%systemroot%.

Следует четко понимать, что всегда проще восстановить работоспособность упавшей ОС из ее резервной копии, чем проводить восстановление, копаясь в файлах или реестре. Однако бывают ситуации, когда делать их уже поздно, а проблему восстановления нужно решить.

Одним из наиболее популярных представителей данного варианта решения проблем восстановления системы – является инструмент Hiren’s BootCD, представляющий собой загрузочный CD-диск с десятками популярных программ и утилит, необходимых для работы с жестким диском, его восстановления и диагностики, диагностики всех узлов компьютера, файловыми менеджерами, утилитами для работы в сети и многими другими.

Наличие данной сборки утилит избавляет своего владельца от необходимости держать при себе множество дисков с необходимыми для ежедневной работы программами.

3. Ход работы

3.1. Восстановление реестра

Попробуйте запустить 1-ю виртуальную машину в обычном режиме с помощью программы VMware Player. Поскольку она была повреждена заранее – пользователем будет получена ошибка, свидетельствующая об этом. Будет сообщено, что некий файл, а именно файл реестра, соответствующий настройкам локального компьютера, был испорчен или утерян (рис. 1).

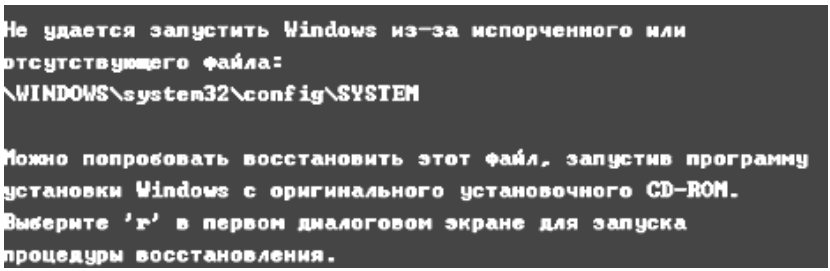

Рис. 1. Ошибка при запуске

Через меню VMware Player, необходимо выбрать в качестве диска, с которого будет происходить чтение – диск Hiren's BootCD (рис. 2).

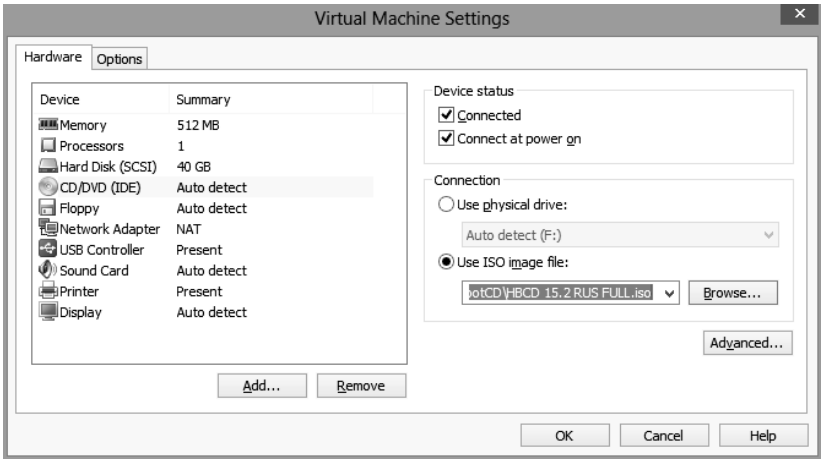

Рис. 2. Выбор диска для загрузки

Чтобы исправить сложившуюся ситуацию, необходимо запустить диск восстановления Hiren's BootCD 15.2. Для этого следует перезапустить виртуальную машину и до того, как загрузится Windows нажать на F2. В результате проделанной операции откроется меню настроек BIOS (рис. 3).

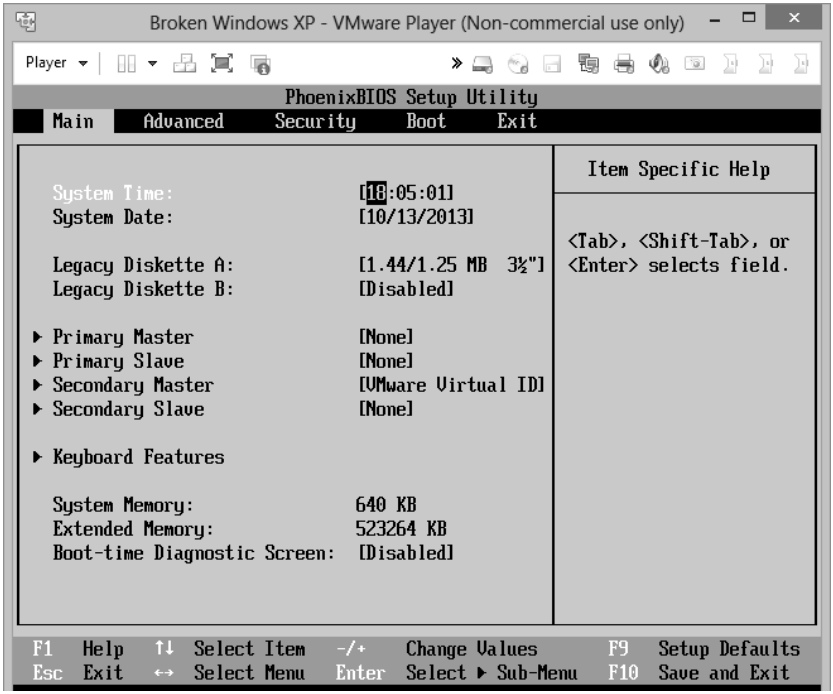

Рис. 3. Меню настроек BIOS

С помощью стрелок «←» и «→» нужно выбрать вкладку «Boot». После чего следует задать порядок восстановления, при котором в первую очередь загрузка будет идти с оптического диска, а уже после с жесткого диска и других носителей, выбрав соответствующий пункт с помощью стрелок «↑» и «↓», а после повысив уровень значимости с помощью «+» (рис. 4). После этого останется нажать на F10 и выйти, сохранив полученные изменения.

При последующем запуске Windows, уже будет видно, что запуск с диска имеет первостепенное значение, о чем свидетельствует запись с названием запускаемого диска в верхней части экрана. Ниже будет перечень возможных вариантов развития событий. Если попытаться загру-

зиться с жесткого диска, система выдаст ту же ошибку, что появлялась ранее. Чтобы восстановить реестр необходимо выбрать пункт «Mini Windows XP» (рис. 5). Это минимальный образ операционной системы, запускаемый с диска.

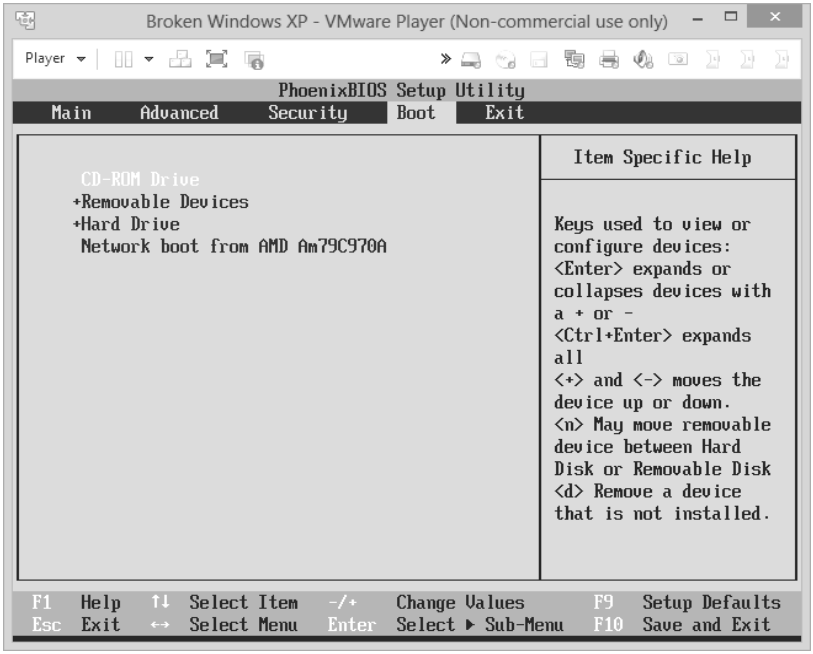

Рис. 4. Настроенный порядок запуска

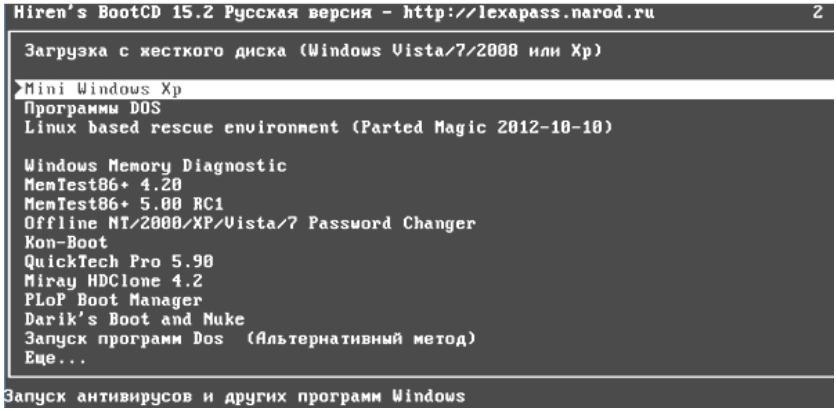

Рис. 5. Загрузка с диска Hiren's BootCD

Загрузится образ минимизированной операционной системы Windows XP, откуда были удалены все ненужные программы, неиспользуемые в повседневной жизни. Данный образ создан специально для того, чтобы восстанавливать операционную систему после сбоя (рис. 6).

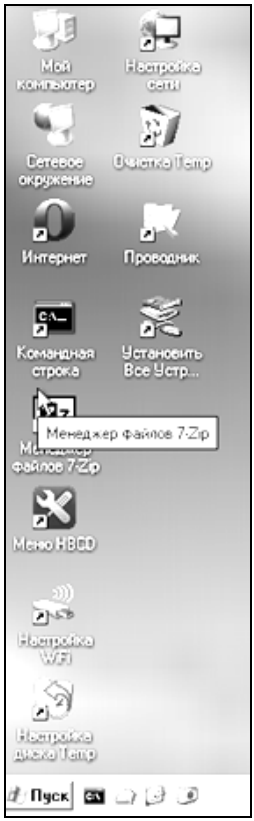

Рис. 6. Рабочий стол Mini Windows XP

Когда «Mini Windows XP» уже загружена, следует открыть «Проводник» и найти на диске «C» папку с названием «System Volume Information». Это скрытая от глаз пользователя (при настройках вида папок и файлов «по умолчанию») папка, куда система копирует программные файлы, подвергшиеся изменениям, хранит отчеты по процедурам очистки диска от мусора (при запуске менеджера очистки), информацию о сжатии файловых массивов (при формате NTFS), хранит

бэкапы определенных компонентов Windows и пользовательских программ (в подкаталогах «restore»).

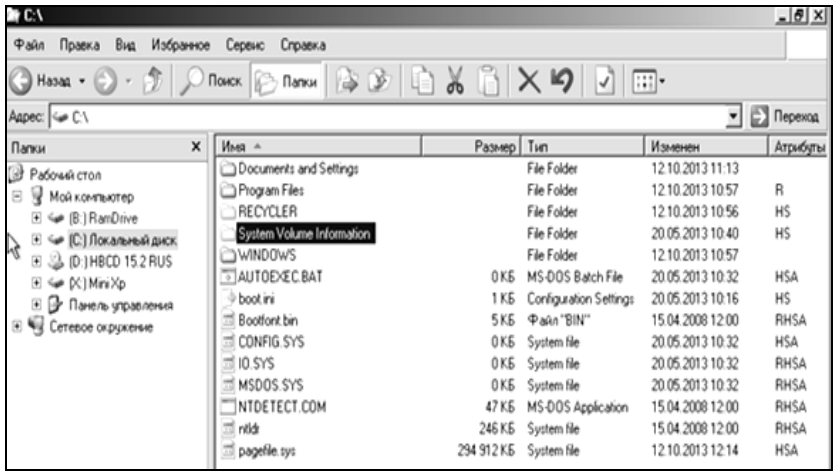

Рис. 7. Расположение папки «System Volume Information»

Далее следует открыть папку «System Volume Information». Внутри неё можно увидеть другую папку с именем, похожим на «_restore{*}», где вместо * – может быть любая комбинация символов (рис. 8).

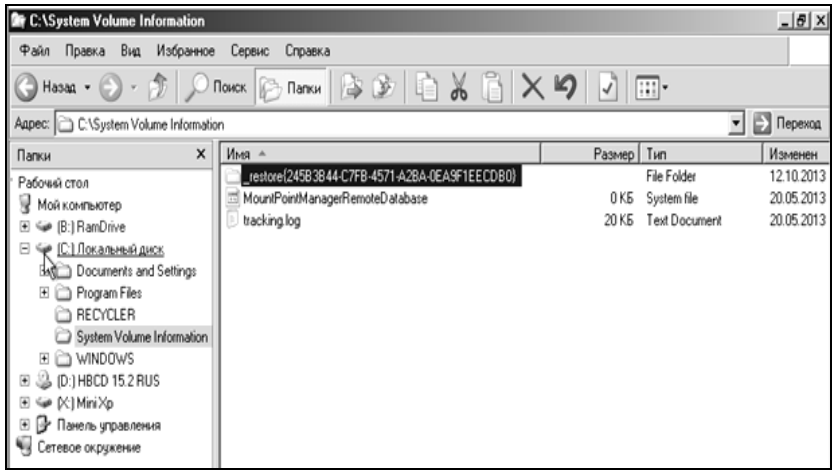

Рис. 8. Содержимое папки «System Volume Information»

Внутри папки «restore», находится некоторое количество папок с именем в формате **RPxx** (RP2, RP3 и др.). Необходимо выбрать папку с новейшей модификацией данных (последний порядковый номер) и открыть её (рис. 9).

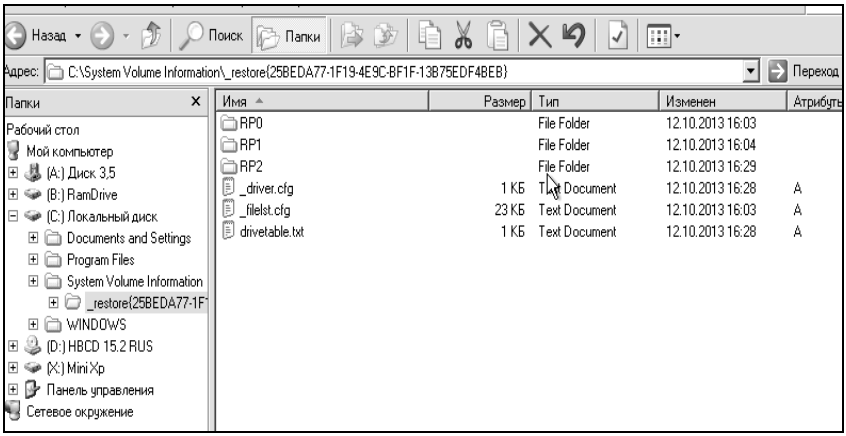

Рис. 9. Папки в формате RPxx

Внутри папки с названием «RPxx» с последней модификацией находится папка «snapshot». Именно она представляет для восстановления особый интерес. В ней будут находится файлы с последней успешной конфигурацией реестра (рис. 10).

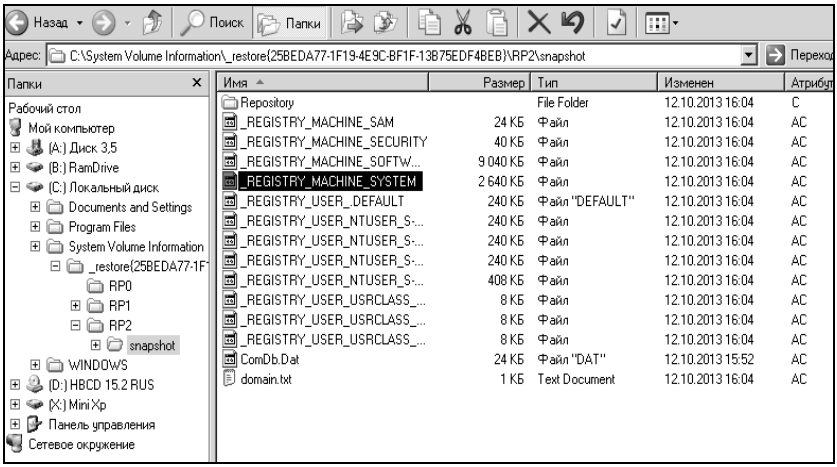

Рис. 10. Содержимое папки «snapshot»

Если бы система не смогла запуститься из-за ошибки, говорящей, что «\WINDOWS\SYSTEM32\CONFIG\SOFTWARE» был поврежден, понадобился бы файл с именем «_REGISTRY_MACHINE_SOFTWARE». Но поскольку ошибка была связана с проблемой системы, а именно «\WINDOWS\SYSTEM32\CONFIG\SOFTWARE SYSTEM» – необходим файл «_REGISTRY_MACHINE_SYSTEM».

Все, что пользователю необходимо сделать, это скопировать файл «_REGISTRY_MACHINE_SYSTEM», содержащий бэкап по последней удачной конфигурации реестра касательно настроек системы локального компьютера, в папку «C:\WINDOWS\System32\Config». После этого удалить имеющийся в папке файл «system» и переименовать скопированную резервную копию, дав ей имя удаленного файла.

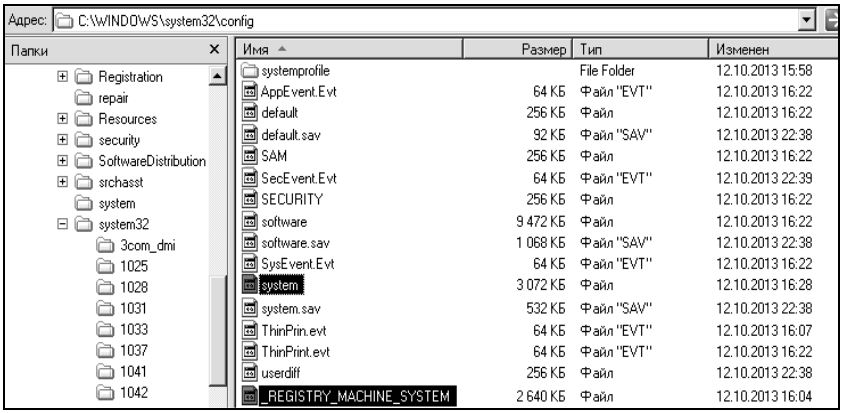

Рис. 11. Заменяемый и заменяющий файлы

Следующим шагом потребуется зайти в свойства файла и убрать атрибут «Сжимать содержимое для экономии места на диске» (рис. 12). В противном случае – файл не будет прочитан системой и ошибка останется.

После перезагрузки, при выборе загрузки с жесткого диска, ранее полученной ошибки уже не будет. И в итоге – операционная система будет запущена. Пользователю будет предложено вести логин и пароль для входа.

Переключитесь на снимок «Step 2». В результате при запуске пользователем будет получена ошибка, говорящая о том, что запустить Windows не удается ввиду каких-то аппаратных настроек. К сожалению, это никоим образом не говорит о природе возникновения ошибки. Поддержка Microsoft по данной проблеме предполагает только выход из строя какого-либо из аппаратных элементов системы.

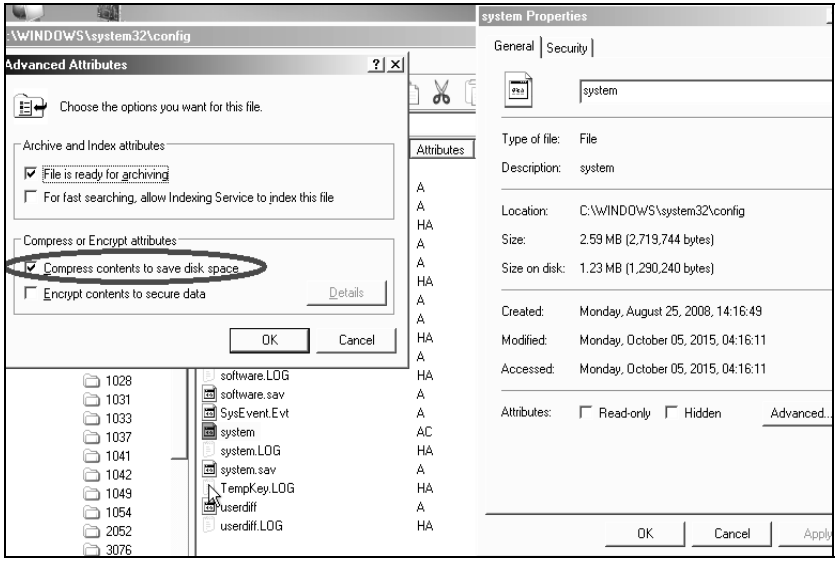

Рис.12. Свойства файла резервной копии реестра

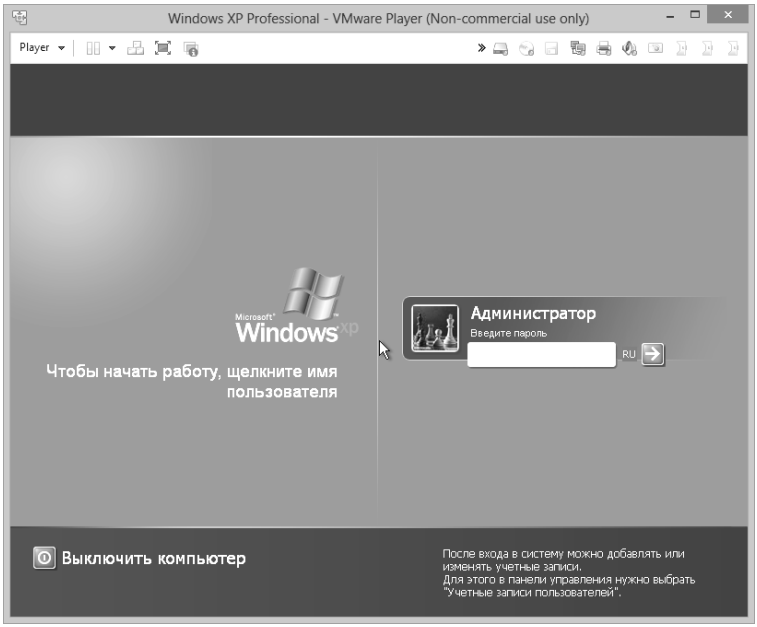

Рис. 13. Предложение входа в систему

3.2. Восстановление boot.ini

Однако, в этот раз источник проблемы создан искусственно и известен нам. Поэтому существует возможность применить конкретный инструмент для ее скорейшего решения.

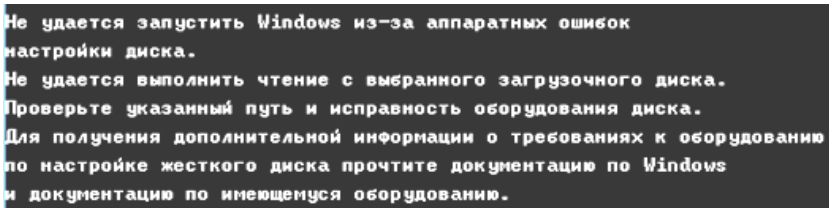

Рис. 14. Текст ошибки после изменений

Для этого следует осуществить следующий переход в меню загрузки с диска. «Программы DOS» → «Дальше…» → «Утилиты NTFS, Ext2FS, Ext3FS (Файловые системы)…». В открывшемся после этого списке выбрать пункт «EditBini». Данная программа позволяет исправлять файл boot.ini на разделах NTFS (рис. 15).

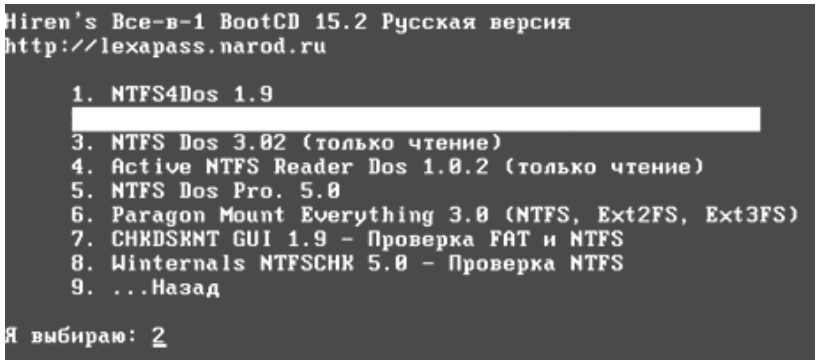

Рис. 15. Необходимая программа

После запуска программы, необходимо будет выбрать раздел диска, на котором находится искомый файл. Поскольку в данной виртуальной машине он один – это не составит проблем (рис. 16 и 17). В результате проделанных действий откроется редактор файла boot.ini (рис. 18). Теперь следует исправить совершенные изменения, восстановив возможность входа в систему.

Пользователю остается изменить обратно «9» на «1» и нажать F10. На вопрос о сохранении изменений в файле ответить положительно (рис. 19).

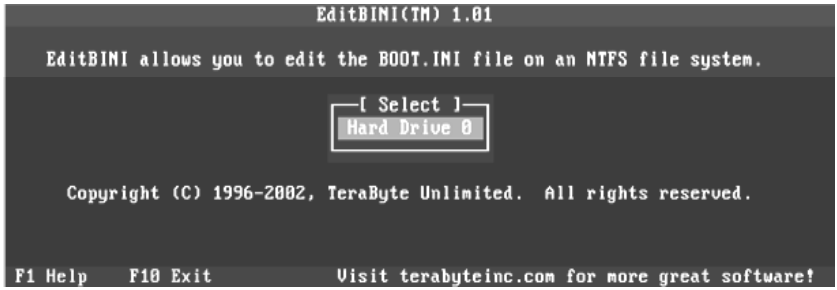

Рис. 16. Выбор жесткого диска

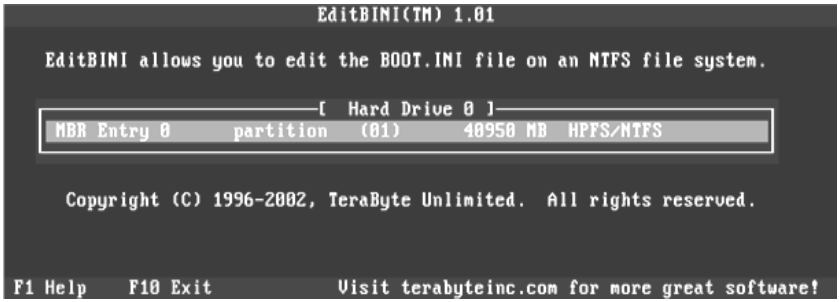

Рис. 17. Выбор логического диска

Рис. 18. Редактор содержимого файла boot.ini

Рис. 19. Запрос на сохранение изменений в файле boot.ini

Совершите перезапуск системы и загрузимся с жесткого диска, чтобы убедиться в полезности совершенных исправлений (рис. 20).

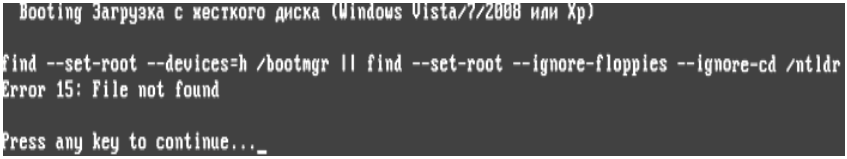

Рис. 20. Сообщение об ошибке

3.3. Восстановление MBR

Попробуйте запустить 2-ю виртуальную машину в обычном режиме с помощью программы VMware Player. На данной виртуальной машине была повреждена главная загрузочная запись (MBR). Данная запись является кодом и данными, необходимыми для последующей загрузки операционной системы и расположена она в первых физических секторах (чаще всего в самом первом) на жёстком диске или другом устройстве хранения информации. Системой будет выдано сообщение о том, что файл не был найден (рис. 20).

Для решения данной проблемы пользователю необходимо загрузиться с Hiren's BootCD, где выбрать пункт «Программы DOS». После чего проделав переход «Дальше…» → «Утилиты MBR», запустить программу «MBR Work». В результате будет выведена информация о текущем содержимом MBR, где будет видно, что вся информация затерта (рис. 21).

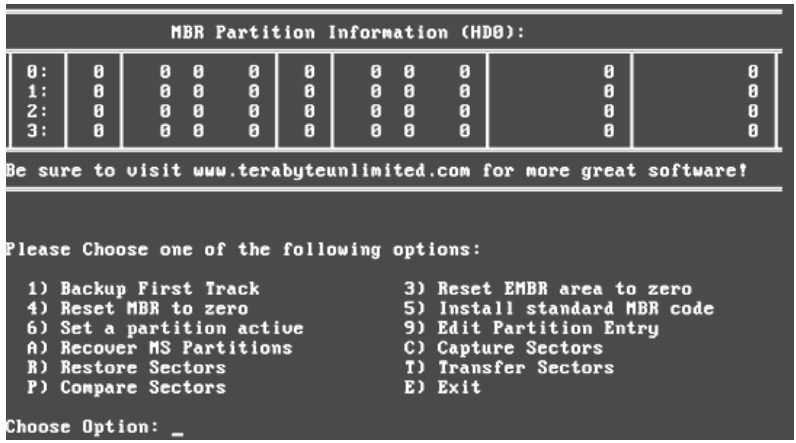

Рис. 21. Начальный вид утилиты

В нижней части экрана будет отображен список опций запуска программы, среди которых первым делом понадобится запустить опцию «A», восстанавливающую разделы. Программа сообщит о своих возможностях и спросит о том данные скольких из разделов необходимо восстановить сейчас.

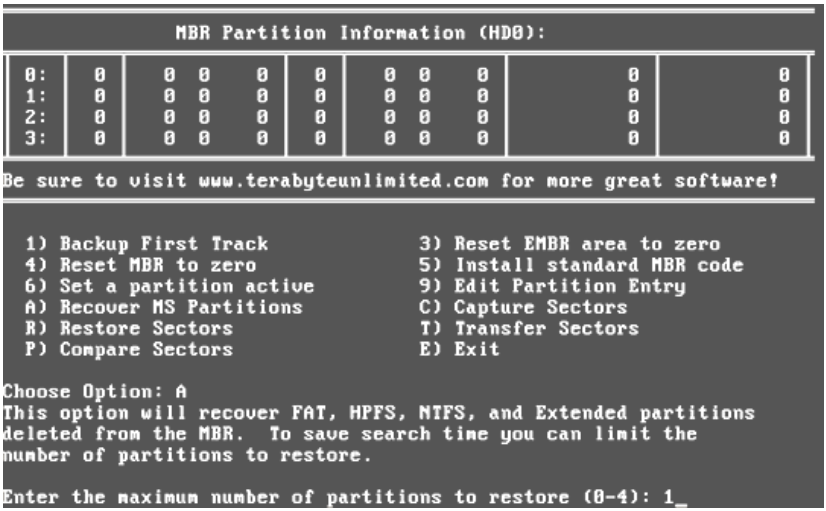

Рис. 22. Восстановление раздела

После успешного восстановления будет сообщено об этом, а также предложено запустить после этого опцию «5» (рис. 23), чтобы установить стандартный для определенной версии ОС MBR код (рис. 23).

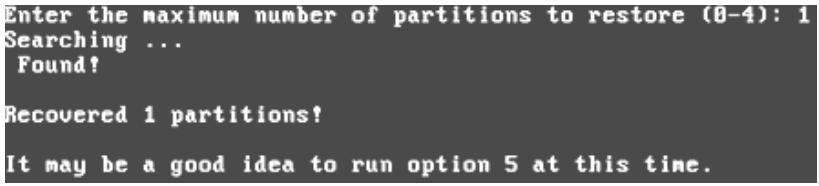

Рис. 23. Результат восстановления

В качестве вариантов установки стандартного MBR кода будет предложено выбрать между стандартным и специальным для Windows 7. После выбора варианта событий – будет задан вопрос о том, действительно ли пользователь желает внести изменения. После – достаточно будет перезапустить виртуальную машину и убедиться, что восстановление прошло успешно.

3.4. Сброс пароля

Бывают ситуации, когда пароль утерян, а пользователю необходимо получить доступ к своему профилю. Для этого вновь потребуется загрузиться с диска «Hiren's BootCD», где в уже знакомом меню «Программы DOS» выбрать пункт «Пароли и реестр…», содержащий утилиты для паролей и реестра. Запустите программу «Offline NT/ 2000/ XP/ Vista/7 Password Changer» (рис. 24). С помощью данной программы будет можно решить проблему.

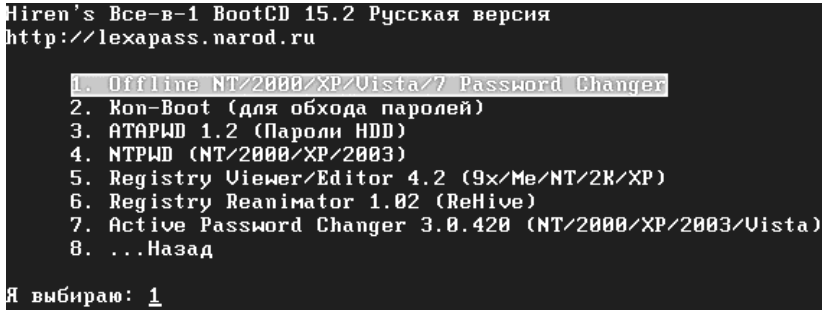

Рис. 24. Выбор программы

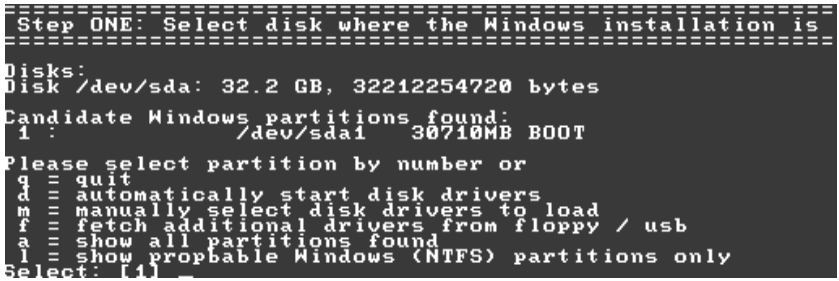

Рис. 25. Выбор раздела жесткого диска

После того как программа загрузится, перед пользователем появится окно выбора раздела жесткого диска, на котором находится операционная система. Так как программа работает в режиме DOS, все что от него требуется это ввести нужный пункт меню и нажать «Enter». В данном случае (рис. 25) программа обнаружила один единственный локальный диск, который стоит под номером «1». Далее согласимся на изменения (рис. 26).

На втором шаге программа предлагает выбрать путь до файла реестра системы (рис. 27). По умолчанию это – «Windows/system32/ config» поэтому в этом окне ничего не нужно изменять.

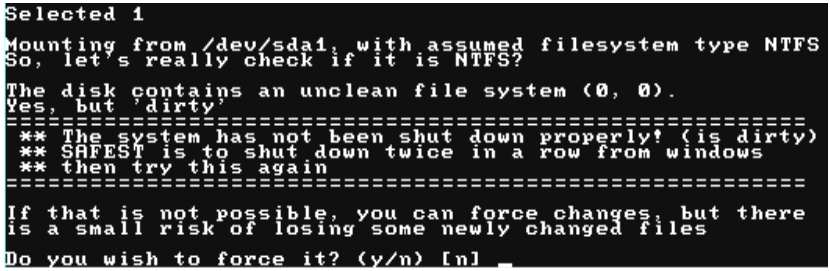

Рис. 26. Проверка на необходимость дальнейших действий

Рис. 27. Проверка пути реестра

В следующем окне программа предлагает выбрать цель загрузки реестра. Под пунктом «1» – это сброс пароля, а под пунктом «2» – консоль восстановления параметров (рис. 28). Далее необходимо выбрать метод использования полученного файла. Следует выбрать пункт «1» – Edit user data and password – Редактировать данные пользователя и пароль (рис. 29).

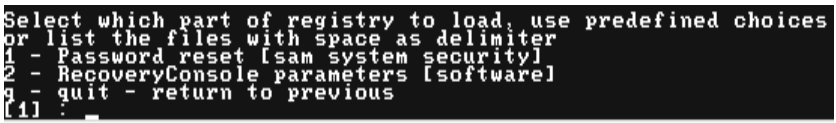

Рис. 28. Выбор раздела регистра

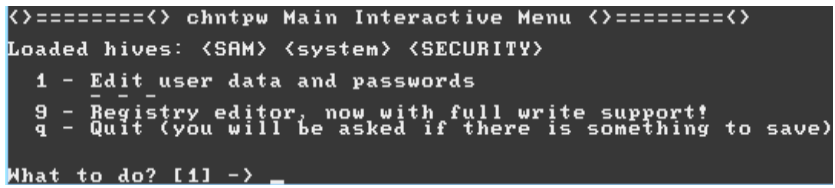

Рис. 29. Выбор действия в реестре

Далее программа выводит полученный список пользователей. Остается выбрать пользователя, у которого был утерян пароль. В данном случае это «Forgotten» (рис. 30).

Рис. 30. Список пользователей

В следующем окне (рис. 31) программа выводит информацию о пользователе и предлагает на выбор несколько вариантов действий.

1. «1» – очистить пароль пользователя;
2. «2» – назначить новый пароль пользователю;
3. «3» – назначить пользователю права администратора);
4. «4» – разблокировать учетную запись пользователя;
5. «q» – закончить правку и вернуться в меню выбора пользователя.

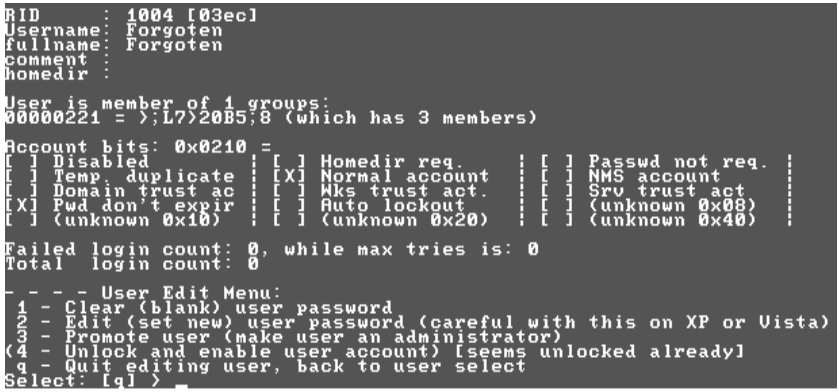

Рис. 31. Выбор метода изменения

Пункт номер «2» не всегда срабатывает, в связи с чем следует использовать пункт «1» для очистки истории паролей пользователя. Если после потребуется назначить пользователю новый пароль, это можно будет реализовать непосредственно в системе. Далее на экран будет выведено сообщение о том, что пароль очищен, и программа предложит ввести «!» для выхода из режима редактирования пользователя (рис. 32).

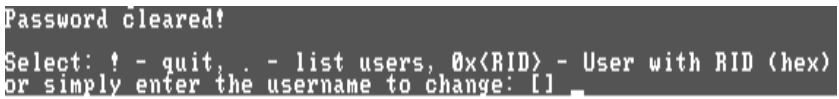

Рис. 32. Сообщение об успешности очистки

После того, как пользователь выйдет из редактирования, он окажется в уже знакомом меню выбора действий с файлом реестра. Если необходимо изменить или сбросить пароль еще одному пользователю, то следует пройти описанную выше последовательность действий для него. Для выхода необходимо выбрать «q».

Рис. 33. Внесение изменений

На следующем этапе программа выдает запрос на запись измененного файла реестра. Чтобы внести изменения необходимо выбрать «Y» (в противном случае «N»). Далее пользователю выдается сообщение, о том что редактирование завершено, и выдается запрос на повторный запуск этой программы (рис. 34). Далее остается запустить Windows и попробовать зайти под измененным пользователем в систему.

Рис. 34. Сообщение о внесении изменений

3.5. Штатные средства восстановления

В данном разделе потребуется рассмотреть создание резервных копий, которые позволят избежать поиска необходимых для восстановления утилит. Будет рассмотрено создание набора ASR. Для этого необходимо запустить программу «Архивация данных», набрав ntbackup.exe из меню «Пуск – Выполнить» (рис. 35).

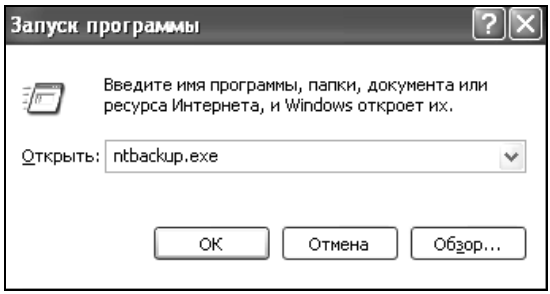

Рис. 35. Запуск программы

В открывшемся окне «Мастера архивации и восстановления» следует выбрать «Расширенный режим» (рис. 36). Это позволит воспользоваться настройкой создаваемого образа восстановления.

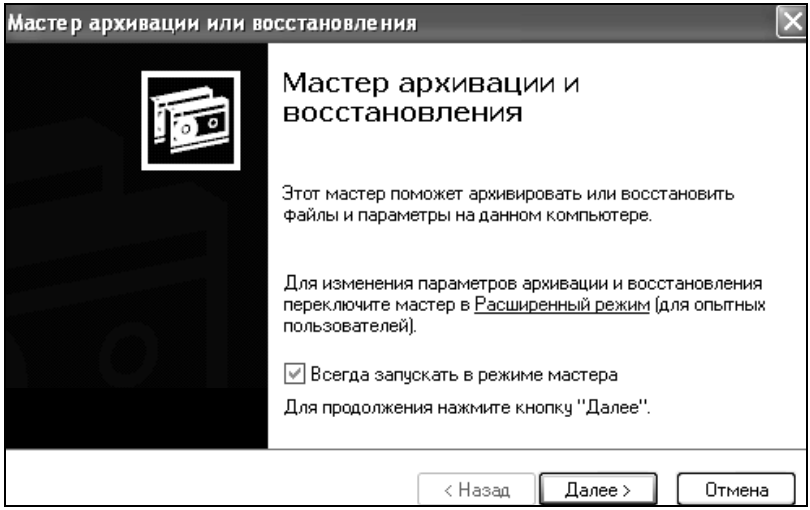

Рис. 36. Выбор расширенного режима

По умолчанию не все файлы включаются в создаваемый архив. Поэтому перед созданием набора ASR стоит посмотреть список исключенных файлов. Для этого осуществляется переход «Сервис – Параметры – Исключение файлов» (рис. 37).

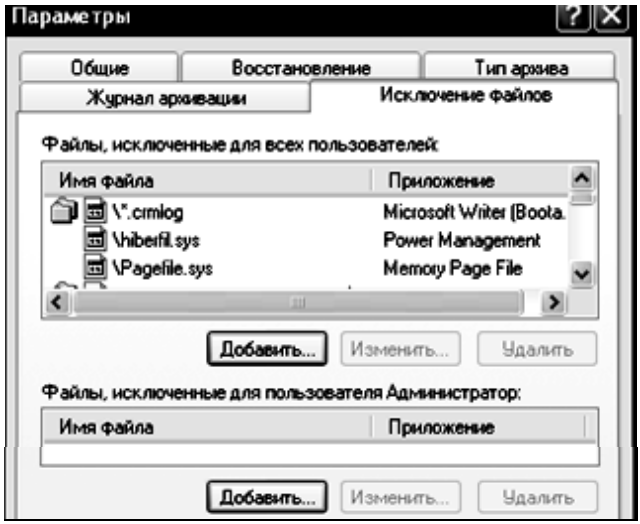

Рис. 37. Список исключенных файлов

По умолчанию в этом списке находятся: файл подкачки (pagefile.sys), файл создаваемый при использовании спящего режима (hiberfil.sys), контрольные точки восстановления, временные файлы и некоторые файлы журналов. Когда все необходимы изменения будут произведены – в главном меню программы (рис. 38) необходимо выбрать пункт «Мастер аварийного восстановления системы».

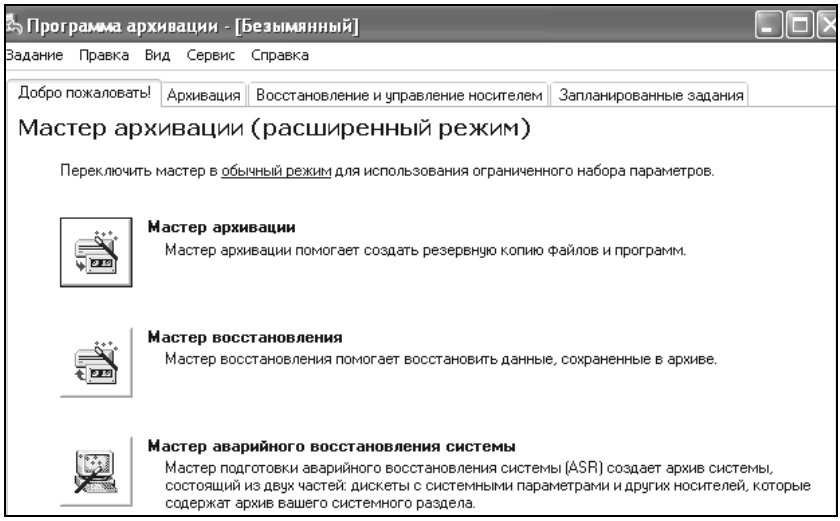

Рис. 38. Расширенный режим мастера

Потребуется указать носитель архива или имя файла. Желательно в качестве носителя использовать дискету (рис. 39).

После сбора необходимой информации начнется процесс архивации. После создания архива будет предложено вставить дискету для записи на нее параметров восстановления. На этом создание набора ASR закончено.

Для восстановления системы потребуется набор ASR (архив+дискета) и загрузочный диск Windows XP. Пользователю понадобится загрузиться с помощью загрузочного диска, выбрав установку Windows XP. При появлении в строке состояния приглашения нажать клавишу F2 – в ответ на что будет получено сообщение «Вставьте диск под названием Диск автоматического восстановления системы Windows в дисковод для гибких дисков». После считывания с дискеты необходимых для восстановления данных и загрузки основных драйверов будет произведено форматирование системного раздела и начальная установка Windows XP.

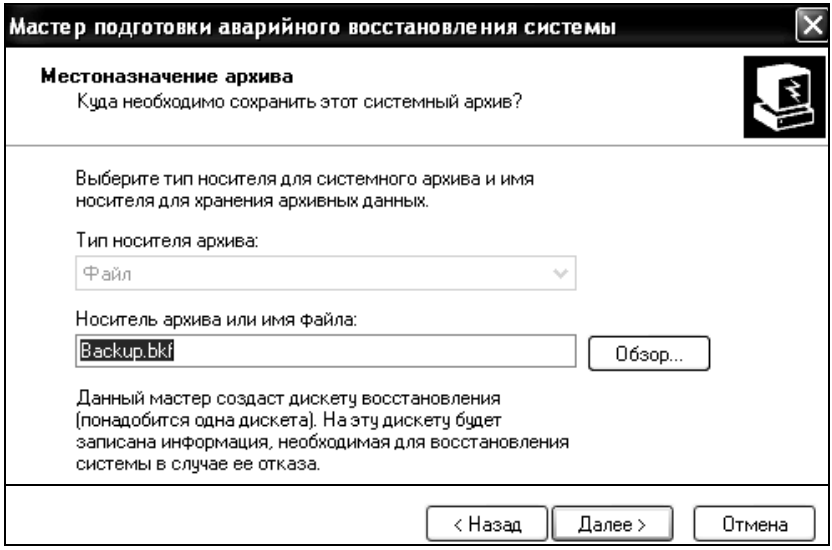

Рис. 39. Выбор носителя

Далее будет запущен мастер аварийного восстановления системы и произведено восстановление файлов из архива набора ASR. После восстановления файлов будет произведена перезагрузка и получена Windows XP со всеми установленными программами, документами и системными настройками на момент создания набора ASR.

Контрольные вопросы

1.Какие основные причины сбоев операционной системы?

2.На какие две группы делятся средства восстановления ОС?

3.Какие средства восстановления в Windows XP вам известны?

4.Какие возможности дает использование Hiren's BootCD?

5.Каким образом можно восстановить утерянные или поврежденные файлы реестра?

6.Какое изменение файла boot.ini может помешать запуститься Windows? Почему?

7.Каким образом можно восстановить файл boot.ini?

8.Что такое MBR?

9.С помощью какой программы можно исправить ошибки MBR?

10. Каким образом можно восстановить возможность входа в систему, если пароль пользователя был утерян?

Литература

1. Станек У.Р. Microsoft Windows 8.1. Справочник администратора. СПб.: БХВ-Петербург, 2015. 400 с.

2. Руссинович М., Соломон Д., Ионеску А. Внутреннее устройство Microsoft Windows. Ч. 1.: Основные подсистемы ОС. 6-е изд. / Пер. Н. Вильчинский. СПб.: Питер, 2013. 800 с.

Для заметок

Учебное издание

Антон Александрович Конев,
Алексей Юрьевич Якимук

БЕЗОПАСНОСТЬ ОПЕРАЦИОННЫХ СИСТЕМ

(Часть 1)

Лабораторный практикум
для студентов специальностей и направлений
10.03.01 – «Информационная безопасность»,
10.05.02 – «Информационная безопасность телекоммуникационных систем»,
10.05.03 – «Информационная безопасность автоматизированных систем»,
10.05.04 – «Информационно-аналитические системы безопасности»

Верстка – В.М. Бочкаревой
Текст дан в авторской редакции, без корректуры

Издательство «В-Спектр»
Подписано к печати 20.11.2017.
Формат $60\times84^{1}/_{16}$. Печать трафаретная.
Печ. л. 7,4. Тираж 250 экз. Заказ 31.

Тираж отпечатан ИП Бочкаревой В.М.
ИНН 701701817754
634055, г. Томск, пр. Академический, 13-24, тел. 49-09-91.
E-mail: bvm@sibmail.com