ТЕМА 4.2. АДМИНИСТРИРОВАНИЕ В ОПЕРАЦИОННОЙ СИСТЕМЕ WINDOWS

В данной теме рассматриваются следующие вопросы:

- Настройка ОС Windows.
- Получение сведений о компьютере.
- Управление конфигурацией системы, порядком запуска и загрузки.
- Восстановление системы.
- Системный реестр Windows, его назначение и использование.
- Использование Панели управления для изменения параметров ОС.
- Использование Планировщика задач.
- Планирование и назначение разрешений NTFS.
- Командное консольное окно.
- BAT-файлы.
- PowerShell.
- WMI.
- ETW.
- Групповые политики.
- Административные шаблоны.
- Файловые системы.
- Динамические диски.
- Управление сжатием на дисках NTFS.
- Шифрование файлов.
- Управление дисковыми квотами.
- Использование Консоли восстановления.

Лекции – 2 часа, лабораторные занятия – 4 часа, самостоятельная работа – 2 часа.

Экзаменационные вопросы по теме:

- Системный реестр ОС Windows, его назначение и использование.
- ОС Windows: планирование и назначение разрешений NTFS (в теме 5.2).
- Средства автоматической настройки в ОС Windows.

4.2.1. Настройка ОС Windows

Сразу после установки Windows система настроена по рекомендованным значениям от производителя продукта. У пользователя есть возможность изменить некоторые предложенные параметры во время процесса инсталляции ОС на компьютер.

Вы можете внести изменения в настройки по умолчанию, чтобы оптимизировать работу операционной системы Windows 11 на ПК. Настройка Windows 11 после установки поможет вам решить проблемы непривычного или неудобного интерфейса, а также отключить некоторые ненужные функции.

Ниже перечислены настройки Windows 11, которые может изменить пользователь [1]:

- Место расположения кнопки «Пуск» и значков на панели задач.
- Удаление рекомендуемых элементов в меню «Пуск».
- Закрепление избранных папок в меню «Пуск».
- Удаление ненужных приложений с панели задач.
- Добавление приложений на панель задач.
- Отключение надоедливых уведомлений.
- Отключение рекламы Microsoft.
- Изменение браузера по умолчанию.
- Отключение ненужных программ в автозагрузке.
- Выбор режима электропитания.
- Вход в систему с локальной учетной записью.

По ссылке в конце этой темы можно найти последовательность действий для каждой из перечисленных настроек.

В корпоративной среде, как правило, права пользователя по настройке системы ограничены. Администраторы предприятия используют групповые политики и другие инструменты для выполнения необходимых настроек.

Для управления мобильными устройствами широко используются технологии MDM и MAM.

MDM (Mobile Device Management) — это системы, которые позволяют ИТ-службам компаний управлять мобильными устройствами, находящимися у сотрудников. Речь не только о мобильных телефонах, но также о планшетах, ноутбуках и другой технике, используемой в рабочих целях [2].

Важнейшая функция MDM-систем – MAM (Mobile Application Management).

MDM-система даёт корпоративным ИТ-службам весьма широкие возможности, например:

- разрешает установку на устройства и удаление приложений и сертификатов безопасности;
- запрещает использовать неблагонадёжные приложения и сервисы;
- разрешает удалённую настройку устройства в соответствии с принятыми в компании политиками;
- допускает шифрование данных на устройстве;
- обеспечивает работу с утерянными устройствами: поиск их местонахождения, блокирование, уничтожение конфиденциальных данных в памяти.

4.2.2. Получение сведений о компьютере

Прежде чем устанавливать операционную систему, необходимо проверить, удовлетворяет ли компьютер минимальным требованиям к оборудованию.

Минимальные требования для Windows 11 [3]:

- Процессор: совместимый, 64-разрядный, 2 ядра или более, минимум 1 ГГц
- ОЗУ: 4 ГБ
- Хранилище: 64 ГБ минимум

- Тип BIOS: UEFI с поддержкой безопасной загрузки
- Наличие TPM: минимум 2.0
- Видеоадаптер: DirectX 12 с драйвером WDDM 2.0
- Дисплей: HD-разрешение, более 9 дюймов, 8 бит
- Windows 11 Home требует подключения к Интернету

Получить информацию о компьютере можно с помощью:

- апплета Система в Панели управления
- графической утилиты msinfo32.exe
- утилиты командной строки systeminfo.exe
- WMI-запросов

4.2.3. Управление конфигурацией системы, порядком запуска и загрузки

При запуске компьютера система BIOS начинает проверять список предварительно заданных накопителей и устройств, на которых может находиться операционная система. Компьютер может загружать операционную систему с жесткого диска, оптического дисковода, устройства хранения данных USB или сети. Порядок, в котором выполняется проверка таких устройств, задается в меню настройки BIOS [4].

Порядок загрузки по умолчанию для компьютера задается производителем. Порядок загрузки по умолчанию определяет, загрузка каких компонентов выполняется компьютером в первую очередь.

Порядок загрузки UEFI:

- Диспетчер загрузки ОС
- Накопитель USB
- CD или DVD-привод USB
- Сетевой адаптер

Порядок загрузки в устаревшем режиме (legacy mode):

- Диспетчер загрузки ОС
- Жесткий диск
- Накопитель USB
- CD или DVD-привод USB
- Сетевой адаптер USB
- Сетевой адаптер

Для загрузки с устройства USB, DVD или CD необходимо, чтобы на нем были установлены загрузочные файлы, или компьютер может обойти устройство и загрузить файлы, установленные на локальном компьютере.

Менеджер загрузки Windows (Windows Boot Manager) – это программа, которая отвечает за процесс загрузки операционной системы Windows на компьютере. Он является неотъемлемой частью Windows и выполняет роль посредника между аппаратным обеспечением компьютера и операционной системой [5].

Основная задача менеджера загрузки Windows — запуск операционной системы, выбранной пользователем. Во время загрузки компьютера, менеджер загрузки Windows проверяет файлы операционной системы, конфигурацию и устройства компьютера и управляет процессом загрузки.

Менеджер загрузки Windows может быть установлен на одном из разделов жесткого диска компьютера, либо на MBR (Master Boot Record) — первом секторе жесткого диска, который содержит код, необходимый для запуска процесса загрузки.

Один из важных элементов менеджера загрузки Windows — это загрузочное меню (Boot Menu), которое предоставляет пользователю выбор операционной системы для загрузки.

Если на компьютере установлены несколько операционных систем, загрузочное меню позволяет выбрать нужную ОС и запустить ее.

Менеджер загрузки Windows также позволяет управлять настройками загрузки, изменять порядок загрузки, устанавливать задержку перед загрузкой, а также выполнять другие действия, связанные с процессом загрузки операционной системы.

Важно отметить, что менеджер загрузки Windows может быть заменен или дополнен другими программами, такими как GRUB или EasyBCD, что позволяет добавлять дополнительные функции и настраивать процесс загрузки по своему усмотрению.

В Windows для изменения параметров загрузки используется **BCDEdit**. Ее нужно запускать в окне командной строки с повышенными привилегиями (выберите и удерживайте (или щелкните правой кнопкой мыши) **Командную строку** и выберите в контекстном меню пункт **Запуск от имени администратора**).

Практическое руководство по редактированию параметров загрузки на компьютере и пошаговые инструкции по настройке основных элементов параметров загрузки можно найти по ссылке:

https://learn.microsoft.com/ru-ru/windows-hardware/drivers/devtest/editing-boot-options.

4.2.4. Восстановление системы

Основные методы восстановления

- Загрузка последней успешной конфигурации
- Восстановление из резервной копии
- Переустановка операционной системы
- Операция Refresh

Операция Refresh

Если ваша Windows 11 является загрузочной и все установленные программы в порядке, вы можете использовать первый метод, который заключается в обновлении Windows 11 без потери программ и данных путем восстановления обновления. Вы можете выполнить восстановление, запустив Windows Setup.exe в Windows 11 [6].

Помимо первого метода, вы также можете обновить Windows 11 без потери файлов, выполнив **Сброс компьютера** (Reset PC)

Если вы не форматируете системный диск и не устанавливаете Windows 11, вы можете вручную получить файл и приложения из папки Window.old. Этот метод довольно прост: вам нужно установить ОС, просмотреть папку и скопировать нужный файл на рабочий стол или куда угодно. Вот конкретные шаги.

Если ваша система загружается нормально, вы можете выполнить настройки, чтобы перезагрузить компьютер. Нажмите **Win+I**, чтобы открыть Настройки, и выберите **Система** > **Восстановление** > **Сбросить настройки этого компьютера**.

Если ваша система не загружается, вы можете создать диск восстановления и загрузиться с него. Затем выберите язык и другие настройки и нажмите **Далее** > **Восстановить компьютер** > **Устранение неполадок** > **Сбросить настройки этого компьютера**.

Если вы хотите обновить Windows 11 без потери данных, вам следует выбрать первый вариант. Если вы хотите выполнить чистую установку, выберите второй вариант.

4.2.5. Системный реестр Windows, его назначение и использование

Реестр — это база данных, в которой Windows хранит параметры конфигурации пользователя и компьютера. Всякий раз, когда вы вносите изменения в конфигурацию Windows, это изменение фиксируется в реестре [7].

Реестр Windows организован иерархически. На верхнем уровне имеется пять кустов реестра, которые представляют собой отдельный набор связанных параметров, структурированных как серия ключей, подразделов и значений: HKEY_CLASSES_ROOT, HKEY_CURRENT_USER, HKEY_LOCAL_MACHINE, HKEY_USERS и HKEY_CURRENT_CONFIG.

HKEY_CLASSES_ROOT

Этот куст содержит информацию о ассоциации файлов и определяет, какое приложение открывается, когда пользователь дважды щелкает определенный тип файла в файловой системе. Например, он определяет, что приложением для файлов .xlsx является Microsoft Excel. Этот куст заполняется на основе настроек, связанных с компьютером и пользователем, которые хранятся в разделах HKEY_LOCAL_MACHINE\Software\Classes и HKEY_CURRENT_USER\Software\Classes. Обычно вы не будете вносить изменения в этот куст.

HKEY_CURRENT_USER

Этот куст содержит информацию о конфигурации для текущего пользователя, вошедшего в систему. Такие элементы, как цветовая схема Windows пользователя и настройки шрифта, хранятся в соответствующих значениях под этим кустом. При ссылке на этот куст при редактировании реестра этот куст иногда называют HKCU. Этот куст представляет собой ярлык ключа, хранящегося в HKEY_USERS.

HKEY_LOCAL_MACHINE

Вероятно, это самый важный куст, в который вы, вероятно, будете вносить больше всего изменений. Этот куст, иногда называемый сокращенно HKLM, хранит все параметры конфигурации, связанные с компьютером.

HKEY_USERS

Этот куст содержит коллекцию всей информации о конфигурации для всех пользователей, выполнивших вход локально на компьютер, включая текущего пользователя, вошедшего в систему. Фактически, один из ключей под этим кустом — это ключ текущего пользователя, вошедшего в систему, который отображается как куст HKEY_CURRENT_USER. Важно знать, что вы, скорее всего, будете вносить прямые изменения в настройки пользователя только для текущего пользователя, вошедшего в систему.

HKEY_CURRENT_CONFIG

Этот куст содержит информацию о текущем профиле оборудования, который локальный компьютер использовал во время запуска системы. Обычно вы не вносите изменения в этот куст.

Ключи и подразделы

Для поддержания структуры базы данных аналогичные настройки хранятся в папках и подпапках, известных как ключи и подразделы. Это упрощает ссылку на определенное значение реестра. Вы можете указать путь, объявив соответствующий куст, ключ, подразделы и значение, как показано в следующем примере:

- `HKCU\Control Panel\Desktop\Wallpaper` — это значение (Wallpaper), в котором хранится имя и расположение обоев рабочего стола пользователя.
- `HKLM\Software\Microsoft\Windows\CurrentVersion\Run` — это ключ, содержащий значения, относящиеся к программам, которые запускаются автоматически при запуске компьютера и входе пользователя в систему. Обычно эти программы находятся на панели задач.

Значения

Значения определяют поведение операционной системы и хранятся в разделах и подразделах. Существует много типов значений, в зависимости от типа данных, которые каждое из них хранит. Например, вы можете захотеть хранить текстовые значения, числовые данные, переменные и подобные данные. Ниже перечислены наиболее распространенные типы значений реестра.

REG_BINARY. Необработанные двоичные данные. Эти значения обычно отображаются в шестнадцатеричном формате. Информация об оборудовании часто хранится в значениях REG_BINARY.

REG_DWORD. 4-байтовые числа (32-битное целое число). Многие значения, связанные с драйверами устройств и службами, хранятся в значениях REG_DWORD. Например, значения START и TYPE для драйверов устройств всегда определяются в значениях типа REG_DWORD.

REG_SZ. Текстовая строка фиксированной длины.

REG_EXPAND_SZ. Текстовая строка переменной длины.

REG_MULTI_SZ. Несколько строковых значений.

4.2.6. Использование Панели управления для изменения параметров ОС

Панель управления (Control Panel) — компонент Microsoft Windows, позволяющий выполнять основные действия по настройке системы, такие как добавление, удаление и настройка устройств, установка и деинсталляция программ, управление учётными записями, включение специальных возможностей, а также многие другие действия, связанные с управлением системой. Присутствует в системе с момента её выхода в 1985 году [8].

Все элементы (или же апплеты, с англ. applet — мини-приложение) Панели управления, с помощью которых можно выполнять определенные системные действия, представляют собой файлы с расширением `.cpl`. Каждый такой апплет запускает системную утилиту, которая нужна для выполнения конкретных задач по настройке системы. Большинство апплетов в Панели управления созданы Microsoft, но в некоторых случаях сторонние производители (например, NVidia) также создавали свои апплеты для Панели управления. С выходом Windows XP, ввиду увеличившегося количества апплетов, была создана их сортировка по категориям, при этом «классический вид» по всем апплетам сразу также сохранился.

В Windows 8, а затем и в Windows 10 появилось приложение «Параметры», заменяющее собой Панель управления. Панель управления в системе при этом осталась. В Windows 10 некоторые функции, такие как Персонализация или Свойства системы, частично или полностью перемещены в «Параметры», и более не работают в Панели управления.

В Windows 11 панель управления недоступна.

4.2.7. Использование Планировщика задач

Планировщик заданий (Task Scheduler) — компонент Microsoft Windows, который предоставляет возможность запланировать запуск программ или скриптов в определённые моменты времени или через заданные временные интервалы. Компонент впервые появился в Windows 95 Plus! pack под названием System Agent, но был переименован в Task Scheduler в Windows 98. Данный сервис для запуска требует включённого Event Log service [9].

Примеры задач, которые можно выполнить с помощью планировщика задач: запуск приложения; отправка сообщения электронной почты; или отображение окна сообщения.

Можно запланировать выполнение задачи в ответ на следующие триггеры:

- При возникновении определенного системного события
- В определенное время
- В определенное время по ежедневному расписанию
- В определенное время в еженедельном расписании
- В определенное время по ежемесячному расписанию
- В определенное время в ежемесячном расписании недели
- Когда компьютер переходит в состояние простоя
- При регистрации задачи
- При загрузке системы
- Когда пользователь входит в систему
- При изменении состояния сеанса сервера терминалов

4.2.8. Планирование и назначение разрешений NTFS

Эта тема рассматривается в теме 5.2.

4.2.9. Командное консольное окно

Все поддерживаемые версии Windows и Windows Server имеют встроенный набор команд консоли Win32.

В Windows есть две оболочки командной строки: командная оболочка cmd и PowerShell.

Каждая оболочка — это программная программа, которая обеспечивает прямую связь между оператором и операционной системой или приложением, предоставляя среду для автоматизации ИТ-операций.

Командная оболочка **`cmd`** была первой оболочкой, встроенной в Windows, для автоматизации повседневных задач, с пакетными (`.bat` или `.cmd`) файлами. С помощью Windows Script Host можно запускать более сложные скрипты в командной оболочке (команды **`cscript`** и **`vscript`**).

PowerShell был разработан для расширения возможностей командной оболочки для выполнения команд PowerShell, называемых командлетами. Командлеты похожи на команды Windows, но предоставляют более расширяемый язык сценариев. Команды Windows и командлеты PowerShell можно запускать в PowerShell, но командная оболочка может выполнять только команды Windows, а не командлеты PowerShell.

Есть несколько способов открыть командную строку в Windows. Ниже представлены наиболее удобные:

- Введите «командная строка» в меню «Пуск», чтобы найти его. Вы также можете ввести «cmd» (краткое имя исполняемого файла, запускающего командную строку), если хотите.
- Нажмите Win + R, чтобы открыть окно «Выполнить», затем введите «cmd» и нажмите Enter, чтобы открыть его.
- Нажмите Win + X (или щелкните правой кнопкой мыши кнопку «Пуск») и выберите в меню «Командная строка».
    - *В зависимости от ваших настроек Windows вместо этого может отображаться Windows PowerShell или Windows Terminal. Новый терминал Windows и PowerShell более мощные, чем командная строка, но обратно совместимы со всеми командами CMD.*

Примеры команд командной строки:

dir – вывод содержимого каталога

copy – копирование файла или папки

ren – переименование файла или папки

cd – сменить текущий каталог

mkdir – создать подкаталог

Полный список команд можно найти по ссылке:

https://learn.microsoft.com/ru-ru/windows-server/administration/windows-commands/windows-commands

4.2.10. BAT-файлы

Текстовые файлы с расширением .cmd или .bat (от слова batch)

Комментарии начинаются с REM (remark)

Строки, начинающиеся с @, не выводятся на экран

Допускаются программные конструкции, например:

```
for %%i in (1 1 5) do echo %%i
if a equ 0 echo 0 else echo notzero
```

Для вызова другого скрипта используется команда **call**

Для создания переменной используется команда **set**

```
set a=0
```

4.2.11. Powershell

PowerShell — расширяемое средство автоматизации от Microsoft с открытым исходным кодом [10], состоящее из оболочки с интерфейсом командной строки и сопутствующего языка сценариев. Впервые публично язык был продемонстрирован на Профессиональной конференции разработчиков (англ. Professional Developers Conference, PDC) в сентябре 2003 года под кодовым названием Monad. Изначально средство выпущено как компонент Windows под названием Windows PowerShell. Открытый исходный код был выпущен с началом разработки PowerShell Core в августе 2016 года.

Windows PowerShell 2.0 был выпущен в составе Windows 7, Windows 8 и Windows Server 2008 R2, а также Windows Server 2012 R2 как неотъемлемый компонент системы. Кроме того, вторая версия доступна и для других систем, таких, как Windows XP SP3, Windows Server 2003 SP2, Windows Vista SP1, Windows Vista SP2, Windows Server 2008 и Windows Server 2012.

Изначально PowerShell построен на базе Microsoft .NET Framework, а позднее — на .NET, и интегрирован с ними. Дополнительно PowerShell предоставляет удобный доступ к COM, WMI и ADSI, равно как и позволяет выполнять обычные команды командной строки, чтобы создать единое окружение, в котором администраторы смогли бы выполнять различные задачи на локальных и удалённых системах.

Эти административные задачи обычно выполняются с помощью командлетов (в оригинале — «cmdlets»), которые являются специализированными классами .NET. Пользователь может комбинировать их в скриптах (сценариях), используя различные конструкции, утилиты командной строки и обращения к обычным классам .NET, объектам WMI или COM. Кроме того, можно использовать различные хранилища данных, такие, как файловая система или реестр Windows, которые предоставляются PowerShell посредством поставщиков (англ. providers).

PowerShell также предоставляет механизм встраивания, благодаря которому исполняемые компоненты PowerShell могут быть встроены в другие приложения. Эти приложения затем могут использовать функциональность PowerShell для реализации различных операций, включая предоставляемые через графический интерфейс. Этот

подход применён в Microsoft Exchange Server 2007 для реализации управляющей функциональности в виде командлетов PowerShell и графических утилит управления в виде оболочек PowerShell, которые вызывают необходимые командлеты. Таким образом, графический интерфейс управления находится поверх промежуточного слоя — PowerShell. Другие приложения Microsoft, включая Microsoft SQL Server 2008, System Center Operations Manager и System Center Data Protection Manager, так же предоставляют доступ к своим интерфейсам управления через командлеты PowerShell.

PowerShell имеет свою собственную расширяемую справку, доступную (в том числе из командной строки) через командлет **`Get-Help`**.

4.2.12. WMI

Инструментарий управления Windows (WMI) — это инфраструктура для управления данными и операциями в операционных системах Windows.

Это расширенная и адаптированная под Windows реализация стандарта WBEM, принятого многими компаниями, в основе которого лежит идея создания универсального интерфейса мониторинга и управления различными системами и компонентами распределённой информационной среды предприятия с использованием объектно-ориентированных идеологий и протоколов HTML и XML [11].

В основе структуры данных в WBEM лежит Common Information Model (CIM), реализующая ООП-подход к представлению компонентов системы. CIM является расширяемой моделью, что позволяет программам, системам и драйверам добавлять в неё свои классы, объекты, методы и свойства.

WMI, основанный на CIM, также является открытой унифицированной системой интерфейсов доступа к любым параметрам операционной системы, устройствам и приложениям.

`wbemtest.exe` — графическая утилита для взаимодействия со структурой WMI на локальном или удаленном компьютере.

`wmic.exe` — консольная утилита для взаимодействия со структурой WMI на локальном или удаленном компьютере.

4.2.13. ETW

Event Tracing for Windows (ETW) — это служба, которая позволяет получать события от одного или нескольких поставщиков событий в режиме реального времени или из файла *.etl за некоторый временной период [12].

Архитектура ETW включает в себя 4 элемента (рис. 4.2.1):

- поставщики событий (providers)
- потребители событий (consumers)
- контроллеры ETW (controllers)
- сессии ETW (event tracing sessions)

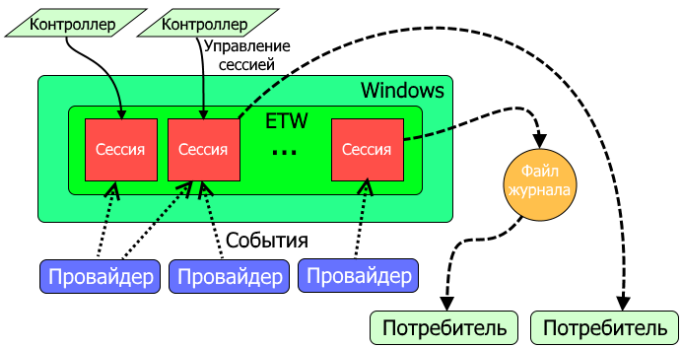

Рис. 4.2.1. Архитектура ETW

Поставщики событий — это приложения, содержащие инструменты отслеживания событий. После того, как поставщик зарегистрировался, контроллер может включить или отключить отслеживание событий в поставщике. Поставщик определяет свою интерпретацию включения или выключения. Как правило, включенный поставщик генерирует события, а отключенный поставщик нет. Это позволяет добавлять отслеживание событий в наше приложение, не требуя, чтобы оно генерировало события все время.

Один поставщик может делиться своими событиями сразу с несколькими сессиями ETW.

Каждое событие состоит из двух элементов: заголовка и данных. Заголовок события включает информацию о событии: идентификатор провайдера, идентификатор события, временную метку и т.д. Остальные данные определяются конкретным провайдером: ETW принимает любые данные и записывает их в буфер, а их интерпретация возлагается на потребителей информации.

Контроллер — это приложение, которое отвечает за функционирование одной или нескольких сессий ETW. Именно контроллер определяет размер и местоположение файла журнала, запускает и останавливает сеансы трассировки событий (сессии ETW), позволяют поставщикам регистрировать события в сеансе. Именно контроллер разрешает провайдеру делиться своими событиями.

Потребители — это приложения, которые получают и обрабатывают события от одного или нескольких сеансов трассировки одновременно. Потребители могут получать события, хранящиеся в файлах журналов или из сеансов, которые доставляют события в режиме реального времени. Как мы уже знаем, у одной сессии ETW может быть несколько поставщиков. Возникает вопрос: а не будет ли путаницы? Как события из различных сессий ETW будут располагаться друг относительно друга? События сортируются по времени их появления, т.е. система доставляет события в хронологическом порядке!

Сеансы отслеживания событий (**сессии** ETW) записывают события от одного или нескольких провайдеров, которые разрешает контроллер. Сессия также отвечает за управление и очистку буферов.

4.2.14. Групповые политики

Групповая политика — важный элемент любой среды Microsoft Active Directory (AD). Её основная цель — дать ИТ-администраторам возможность централизованно управлять пользователями и компьютерами в домене [13]. Групповая политика, в свою очередь, состоит из набора политик, называемых объектами групповой политики (GPO). При создании домена AD автоматически создаются два объекта групповой политики:

- политика домена по умолчанию устанавливает базовые параметры для всех пользователей и компьютеров в домене в трех плоскостях: политика паролей, политика блокировки учетных записей и политика Kerberos;
- политика контроллеров домена по умолчанию устанавливает базовые параметры безопасности и аудита для всех контроллеров домена в рамках домена.

Для вступления настроек в силу, объект групповой политики необходимо применить (связать) с одним или несколькими контейнерами Active Directory: сайт, домен или подразделение (OU). Например, можно использовать групповую политику, чтобы потребовать от всех пользователей в определённом домене использовать более сложные пароли или запретить использование съемных носителей на всех компьютерах только в финансовом подразделении данного домена.

Объект групповой политики не действует, пока не будет связан с контейнером Active Directory, например, сайтом, доменом или подразделением. Любой объект групповой политики может быть связан с несколькими контейнерами, и, наоборот, с конкретным

контейнером может быть связано несколько объектов групповой политики. Кроме того, контейнеры наследуют объекты групповой политики, например, объект групповой политики, связанный с подразделением, применяется ко всем пользователям и компьютерам в его дочерних подразделениях. Аналогичным образом, объект групповой политики, применяемый к OU, применяется не только ко всем пользователям и компьютерам в этом OU, но и наследуется всем пользователям и компьютерам в дочерних OU.

Настройки различных объектов групповой политики могут перекрываться или конфликтовать. По умолчанию объекты групповой политики обрабатываются в следующем порядке (причем примененные позднее имеют приоритет над примененными ранее):

- Локальный (индивидуальный компьютер)
- Сайт
- Домен
- Организационное подразделение.

В эту последовательность можно и нужно вмешиваться, выполнив любое из следующих действий:

- **Изменение последовательности GPO**. Объект групповой политики, созданный позднее, обрабатывается последним и имеет наивысший приоритет, перезаписывая настройки в созданных ранее объектах. Это работает в случае возникновения конфликтов.
- **Блокирование наследования**. По умолчанию дочерние объекты наследуют все объекты групповой политики от родительского, но вы можете заблокировать это наследование.
- **Принудительное игнорирование связи GPO**. По умолчанию параметры родительских политик перезаписываются любыми конфликтующими политиками дочерних объектов. Вы можете переопределить это поведение.
- **Отключение связей GPO**. По умолчанию, обработка включена для всех связей GPO. Вы можете предотвратить применение объекта групповой политики для конкретного контейнера, отключив связь с объектом групповой политики этого контейнера.

Для управления групповыми политиками Microsoft предоставляет консоль управления групповыми политиками (GPMC). Используя этот бесплатный редактор групповой политики, ИТ-администраторы могут создавать, копировать, импортировать, создавать резервные копии и восстанавливать объекты групповой политики, а также составлять отчеты по ним. Microsoft также предлагает целый набор интерфейсов GPMC, которые можно использовать для программного доступа ко многим операциям, поддерживаемым консолью.

По умолчанию любой член группы администраторов домена может создавать объекты групповой политики и управлять ими. Кроме того, существует глобальная группа под названием «Владельцы-создатели групповых политик»; его члены могут создавать объекты групповой политики, но они могут изменять только созданные ими политики, если им специально не предоставлены разрешения на редактирование других объектов групповой политики.

В этой же консоли можно делегировать вспомогательным ИТ-администраторам разрешения для различных действий: создание, редактирование и создание связей для определенных объектов групповой политики. Делегирование — ценный инструмент; например, можно предоставить группе, ответственной за управление Microsoft Office, возможность редактировать объекты групповой политики, используемые для управления настройками Office на рабочем столе пользователей.

4.2.15. Административные шаблоны

Административные шаблоны представляют собой XML-файлы на разных языках, которые определяют основанные на значениях реестра параметры групповых политик, отображаемые в редакторе локальных групповых политик [14].

Административные шаблоны представляют собой иерархическую структуру категорий и подкатегорий политики, которые определяют, каким образом параметры политики отображаются в редакторе локальных групповых политик, включая:

- расположение каждого параметра в реестре;
- возможные значения и ограничения для каждого параметра;
- значение по умолчанию для многих параметров;
- текстовые объяснения о каждом параметре.

Существует два вида административных шаблонов:

- **ADMX** — не зависящий от языка файл установки, который указывает количество и тип параметров политики, а также расположение по категориям согласно отображению файла в редакторе локальных групповых политик.
- **ADML** — файл установки на определенном языке, который предоставляет связанные с языком сведения для ADMX-файла. Этот файл позволяет параметру политики отображаться в редакторе локальных групповых политик на нужном языке. Вы можете добавлять новые языки, добавляя новые ADML-файлы на нужных языках.

В качестве администратора вы можете создать центральную папку хранения в каталоге SYSVOL с названием PolicyDefinitions. Например, %SystemRoot%\PolicyDefinitions. В этой папке будут централизованно храниться файлы административных шаблонов (как ADMX, так и ADML), чтобы их могли использовать доменные объекты групповой политики.

4.2.16. Файловые системы

Файловая система – это способ организации и хранения файлов на жестком диске компьютера. В операционной системе Windows используется несколько различных типов файловых систем, которые обеспечивают удобное хранение и управление данными [15].

Одним из основных типов файловых систем в Windows является NTFS (New Technology File System). NTFS обладает высокой степенью надежности, поддерживает шифрование и права доступа к файлам и папкам. Кроме того, NTFS позволяет работать с файлами размером до 16 терабайт.

Другим распространенным типом файловой системы в Windows является FAT (File Allocation Table). FAT поддерживает работу с файлами менее 4 гигабайт и не обеспечивает такую высокую степень надежности, как NTFS. Однако FAT более совместима с различными операционными системами и устройствами.

Операционная система Windows использует файловую систему NTFS по умолчанию. Это обеспечивает высокую степень совместимости и надежности при работе с файлами и папками. Однако, если необходимо, пользователь может выбрать другую файловую систему при установке операционной системы или форматировании жесткого диска.

Операционная система Windows также предоставляет удобный интерфейс для управления файлами и папками. Пользователь может создавать, копировать, перемещать и удалять файлы, а также организовывать их в папки и подпапки. Для этих целей используются команды и функции операционной системы, а также графический интерфейс, предоставляемый проводником Windows.

Кроме того, операционная система Windows поддерживает работу с различными типами файлов, включая текстовые документы, изображения, музыку, видео и другие файлы.

Для каждого типа файлов может быть установлена программа, которая будет открывать и обрабатывать этот тип файлов по умолчанию.

В целом, файловая система операционной системы Windows обеспечивает удобство и надежность при работе с файлами и папками. Она позволяет организовывать данные на жестком диске, управлять ими и работать с различными типами файлов. Это позволяет пользователям эффективно использовать ресурсы своего компьютера и обеспечивает комфортное использование операционной системы Windows.

Функциональность файловой системы NTFS

NTFS (New Technology File System) — это файловая система, разработанная компанией Microsoft и введенная в операционных системах Windows NT. NTFS предлагает ряд функциональных возможностей, которые делают его одной из самых мощных и надежных файловых систем для операционной системы Windows.

Безопасность и доступы: NTFS обеспечивает механизмы безопасности и защиты данных. Есть возможность установить различные уровни доступа к файлам и папкам для разных пользователей и групп пользователей. Можно назначить права на чтение, запись, выполнение и удаление файлов.

Журналирование: NTFS основан на журнализации, что означает, что каждая операция записи или изменения данных записывается в журнал перед выполнением. Это позволяет снизить вероятность повреждения файловой системы в случае сбоя питания или других непредвиденных ситуаций.

Поддержка больших дисков и файлов: NTFS поддерживает работу с большими жесткими дисками и файлами. Максимальный размер диска на NTFS составляет несколько петабайт, а максимальный размер файла — 16 эксабайт. E61 — последняя часть кода.

Сжатие данных: NTFS предлагает возможность сжимать файлы и папки в режиме реального времени. Это может помочь сэкономить дисковое пространство, особенно для файлов, которые содержат много текстовой информации или повторяющихся блоков данных.

Шифрование: NTFS поддерживает шифрование файлов и папок с помощью технологии EFS (Encrypting File System). Это позволяет защитить конфиденциальные данные от несанкционированного доступа.

Ограничения имени файла: NTFS поддерживает более широкий набор допустимых символов в именах файлов и папок, по сравнению с другими файловыми системами, такими как FAT32. Он также позволяет использовать длинные имена файлов.

4.2.17. Динамические диски

Динамические диски предоставляют функции, которых нет у базовых дисков. Вы можете создавать тома, охватывающие несколько дисков, и отказоустойчивые тома. Динамические диски также могут использовать стили разделов MBR или GPT [16].

Динамические диски используют базу данных для отслеживания информации о томах на динамических дисках компьютера. На каждом динамическом диске компьютера хранится копия базы данных динамического диска, что полезно в случае повреждения базы данных динамического диска. Windows может восстановить поврежденный динамический диск, используя базу данных на другом динамическом диске. Стиль разделов диска определяет расположение базы данных. В разделах MBR Windows хранит базу данных в последнем 1 МБ диска. В разделах GPT база данных расположена в зарезервированном скрытом разделе размером 1 МБ.

Следующие операции можно выполнять только на динамических дисках:

- Создание и удаление составных, чередующихся и зеркальных томов.

- Расширьте простой том до несмежного пространства или составного тома.
- Удалите зеркало из зеркального тома.
- Восстановление зеркальных томов.
- Повторно активируйте отсутствующий или отключенный диск.

Вам следует учитывать следующие соображения, касающиеся динамических дисков:

- Вы не можете преобразовать базовый диск в динамический диск, если на диске не имеется хотя бы 1 МБ неиспользуемого пространства из-за базы данных диспетчера логических дисков.
- Вы не можете преобразовать динамический диск в базовый без потери данных. Вам необходимо удалить все динамические тома на диске. Управление дисками автоматически преобразует диск в базовый при удалении последнего тома.
- Вы не можете использовать Windows PowerShell для управления динамическими дисками. Командлеты хранилища не распознают динамические диски.

4.2.18. Управление сжатием на дисках NTFS

Впервые встроенная функции сжатия появилась в ОС Windows XP, в последующих версиях Windows эта функция неизменно присутствует. Поддерживаются два типа сжатия:

- NTFS-сжатие на уровне файловой системы,
- Сжатые ZIP-папки (Compressed Folders).

Сжатие NTFS – это архивирование на уровне файловой системы NTFS, выполняется оно прозрачно драйвером файловой системы. NTFS сжатие может применяться к файлам, папкам и дискам целиком. Для этого каждому сжатому объекту присваивается специальный атрибут сжатия (compression state), который указывает, сжат файл или нет. У этого типа сжатия есть свои особенности:

- Сжатие NTFS возможно только на разделах с файловой системы NTFS
- При доступе к сжатому файлу или папке осуществляется прозрачная декомпрессия, т.е. пользователь не видит различий между сжатыми и обычными файлами в Windows, и спокойно может копировать, добавлять или удалять файлы в сжатой папке.
- Для отображения объектов, сжатых на NTFS, применяется специальная цветовая схема (по умолчанию, в проводнике имена сжатых файлов отображаются синим цветом)
- Скорость доступа к сжатому файлу ниже, т.к. систем требуется некоторое время на его распаковку (для современных систем такая операция сложностей не создает, так что задержка практически не видна невооруженным взглядом).
- Сжатие более слабое, чем при использовании ZIP-папок или других архиваторов, но скорость его выполнения гораздо выше

Сжатые ZIP-папки подразумевают архивацию файлов встроенной в систему функцией создания zip архивов. Сжатые папки очень похожи на обычные, иногда даже можно забыть, что на самом деле работаешь с ZIP-архивом. Особенности ZIP-папок в Windows:

- Сжатые ZIP-папки можно создавать как на томах NTFS, так и на томах FAT.
- Из сжатой Zip-папки можно открывать файлы и даже запускать некоторые приложения
- Zip-папку можно передать на другой компьютер, где ее можно распаковать любой другой программой сжатия.
- Для сжатия файла нужно просто переместить его в сжатую Zip-папку. Когда файл перемещается их такой Zip-папки в обычную, он автоматически распаковывается.

4.2.19. Шифрование файлов

Windows поддерживает две технологии шифрования:

- EFS — на уровне файлов и папок;
- BitLocker — на уровне томов.

Encrypting File System (EFS) — система шифрования данных, реализующая шифрование на уровне файлов в современных операционных системах Microsoft Windows, за исключением «домашних» версий. Данная система предоставляет возможность «прозрачного шифрования» данных, хранящихся на разделах с файловой системой NTFS, для защиты потенциально конфиденциальных данных от несанкционированного доступа при физическом доступе к компьютеру и дискам.

Аутентификация пользователя и права доступа к ресурсам, имеющие место в NT, работают, когда операционная система загружена, но при физическом доступе к системе возможно загрузить другую ОС, чтобы обойти эти ограничения. EFS использует симметричное шифрование для защиты файлов, а также шифрование, основанное на паре открытый/закрытый ключ для защиты случайно сгенерированного ключа шифрования для каждого файла. По умолчанию закрытый ключ пользователя защищён с помощью шифрования пользовательским паролем, и защищённость данных зависит от стойкости пароля пользователя.

EFS работает, шифруя каждый файл с помощью алгоритма симметричного шифрования, зависящего от версии операционной системы и настроек. При этом используется случайно сгенерированный ключ для каждого файла, называемый File Encryption Key (FEK).

FEK защищается путём асимметричного шифрования, использующего открытый ключ пользователя, шифрующего файл, и алгоритм RSA. Зашифрованный таким образом ключ FEK сохраняется в альтернативном потоке $EFS файловой системы NTFS. Для расшифрования данных драйвер шифрованной файловой системы прозрачно для пользователя расшифровывает FEK, используя закрытый ключ пользователя, а затем и необходимый файл с помощью расшифрованного файлового ключа.

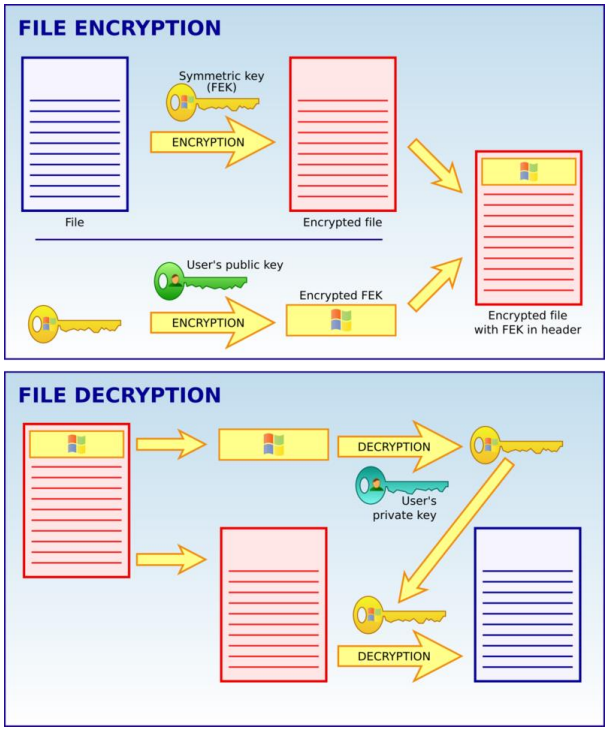

Рис. 4.2.2. Схема шифрования в EFS

BitLocker — это функция безопасности Windows, которая обеспечивает шифрование для целых томов, устраняя угрозы кражи или раскрытия данных с потерянных, украденных или неправильно списанных устройств.

BitLocker обеспечивает максимальную защиту при использовании с доверенным платформенным модулем (TPM), который является общим аппаратным компонентом, установленным на устройствах Windows. TPM работает с BitLocker, чтобы убедиться, что устройство не было изменено, пока система находится в автономном режиме.

4.2.20. Управление дисковыми квотами

Дисковые квоты позволяют администраторам Windows контролировать сколько места используют пользователи на файловой системе серверов и рабочих станций. ОС Windows Server поддерживает два типа квотирования:

- квотирование на базе File Server Resource Manager (дисковые квоты FSRM);
- NTFS квоты.

Хотя FSRM-квотирование и является более гибким и удобным, но в некоторых простых случаях эффективно можно использовать и NTFS квоты.

С помощью дисковых квот Windows вы можете ограничить максимальный размер файлов и папок каждого пользователя так, чтобы он не превысил установленного лимита и не занял своими данными весь диск. Принадлежность фалов и каталогов определяется в соответствии с владельцем объекта файловой системы NTFS. Дисковые квоты работают как на северных, так и на клиентских версиях Windows.

Основные особенности и ограничения NTFS-квот:

- Квотирование может быть применено только целиком к конкретному тому (разделу), отформатированному в файловой систем NTFS (на ReFS томах квотирование не работает).
- Квоты действуют на всех пользователей, хранящих свои данные на данном разделе. Нельзя применить квоту на группу пользователей или отдельный каталог.
- Принадлежность файлов пользователю определяется по его владельцу (owner) файла, заданного в дескрипторе защиты NTFS.
- По умолчанию Windows сканирует раздел с включенным квотированием и пересчитывает суммарный размер файлов каждого пользователя 1 раз в час
- При использовании NTFS-компрессии, учитывается оригинальный размер файлов (до сжатия).

Опции (рис. 4.2.3) следует выбрать в зависимости от желаемого сценария использования квот:

- **Deny disk space to users exceeding quota limit** – запретить запись на диск пользователям, превысившим лимит;
- **Limit disk space to** — задать лимит на суммарный размер файлов одного пользователя;
- **Log event when a user exceeds their quota limit** – записывать в Event Viewer событие при превышении квоты пользователем;
- **Log event when a user exceeds their warning level** – записывать в журнал события при приближении к указанному порогу.

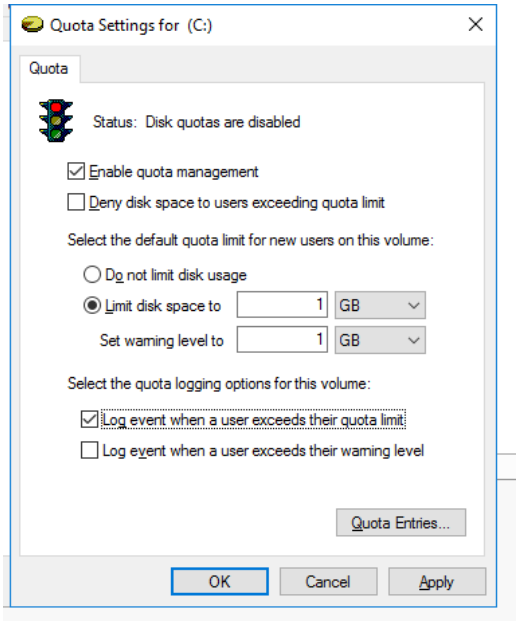

Рис. 4.2.3. Окно настройки квот NTFS

4.2.21. Использование консоли восстановления

Среда восстановления Windows 10 позволяет производить различные операции, имеющие отношение к восстановлению работоспособности системы: использовать особые варианты загрузки (например, безопасный режим или отключение проверки цифровой подписи драйверов), выполнять сброс ОС или автоматическое восстановление загрузчика Windows 10 и многое другое. В статье по следующей ссылке описаны способы входа в среду восстановления и работу в ней:

https://remontka.pro/run-windows-10-recovery-environment/

Список использованных источников

1. Как настроить Windows 11 после установки на компьютер
https://vellisa.ru/change-windows-11-settings-after-installation

2. Что такое MDM-системы и зачем компаниям управлять техникой сотрудников
https://vc.ru/macaroon/185491-chto-takoe-mdm-sistemy-i-zachem-kompaniyam-upravlyat-tehnikoy-sotrudnikov

3. Windows 11 System Requirements
https://support.microsoft.com/en-us/windows/windows-11-system-requirements-86c11283-ea52-4782-9efd-7674389a7ba3

4. ПК HP - Настройка порядка загрузки в системе BIOS
https://support.hp.com/kz-ru/document/ish_3936081-3910542-16

5. Что такое Windows Boot Manager и как он работает?
Источник: https://uchet-jkh.ru/i/cto-takoe-windows-boot-manager-i-kak-on-rabotaet

6. How to Refresh Windows 11 without Losing Programs (3 Ways)
https://www.ubackup.com/windows-11/refresh-windows-11-without-losing-programs.html

7. Examine the Windows registry
https://learn.microsoft.com/ru-ru/training/modules/explore-windows-architecture/4-examine-windows-registry

8. Панель управления Windows
https://ru.wikipedia.org/wiki/Панель_управления_Windows

9. Планировщик заданий (Windows)
https://ru.wikipedia.org/wiki/Планировщик_заданий_(Windows)

10. PowerShell
https://ru.wikipedia.org/wiki/PowerShell

11. WMI
https://ru.wikipedia.org/wiki/WMI

12. Изучаем Event Tracing for Windows: теория и практика
https://habr.com/ru/articles/502362/

13. Групповые политики (GPO) Active Directory: разбираемся почему это важно и как ими управлять в GPOAdmin

https://habr.com/ru/companies/galssoftware/articles/543588/

14. Административные шаблоны и Internet Explorer 11

https://learn.microsoft.com/ru-ru/internet-explorer/ie11-deploy-guide/administrative-templates-and-ie11

15. Как работает операционная система Windows: принципы и функциональность

Источник: https://uchet-jkh.ru/i/kak-rabotaet-operacionnaya-sistema-windows-principy-i-funkcionalnost

16. Describe dynamic disks

https://learn.microsoft.com/en-us/training/modules/manage-storage-windows-clients/5-describe-dynamic-disks

17. Немного про сжатые папки в Windows

https://winitpro.ru/index.php/2012/08/06/nemnogo-pro-szhatye-papki-v-windows