**Практическое задание. Решение проблем конфигурации с помощью групповых политик.**

**Цели работы:**

1. освоение умений у обучающихся по настройке, изменению и созданию групповых политик

**Задачи:**

1. Изучить Требования
2. Установить образ Windows 7(при необходимости)
3. Редактор групповой политики
4. Запуск редактора групповой политики
5. Работа в редакторе
6. Настройки политики
7. Фильтры политик
8. Экспорт списка политик
9. Применение фильтрации
10. Принцип работы с групповыми политиками
11. Изменение окна безопасности Windows
12. Изменения панели мест
13. Слежение за завершением работы компьютера
14. Применение инструмента «Локальная политика безопасности»
15. Использование инструмента «Редактор локальной групповой политики»
16. Выполнить способы, когда включался компьютер
17. Способ 1: Командная строка
18. Способ 2: Журнал событий
19. Способ 3: Локальные групповые политики
20. Способ 4: Реестр
21. Способ 5: TurnedOnTimesView

**План урока:**

1. Объяснение практической работы
2. Разбить людей на команды
3. Выполнение практической работы
4. Составить отчет о проделанной работе

**Для проведения практического занятия используется следующее обеспечение:**

1. Персональный компьютер
2. VirtualBox
3. Windows 7

**Порядок выполнения:**

1. Изучить Требования
2. Установить образ Windows 7(при необходимости)
3. Редактор групповой политики
4. Запуск редактора групповой политики
5. Работа в редакторе
6. Настройки политики
7. Фильтры политик
8. Экспорт списка политик
9. Применение фильтрации
10. Принцип работы с групповыми политиками
11. Изменение окна безопасности Windows
12. Изменения панели мест
13. Слежение за завершением работы компьютера
14. Применение инструмента «Локальная политика безопасности»
15. Использование инструмента «Редактор локальной групповой политики»
16. Выполнить способы, когда включался компьютер
17. Способ 1: Командная строка
18. Способ 2: Журнал событий
19. Способ 3: Локальные групповые политики
20. Способ 4: Реестр
21. Способ 5: TurnedOnTimesView
22. Составить отчет о проделанной работе

**Теоретическая часть**

Одним из самых эффективных способов управления компьютерной сетью является использование групповых политик. Групповая политика позволяет централизованно устанавливать единые параметры для настройки как операционной системы, так и прикладного программного обеспечения.

Политика представляет собой набор настроек и правил, которые могут быть применены к группе компьютеров (состав группы может регулироваться администратором). [an error occurred while processing this directive]

При помощи политики возможно:

* автоматически установить на компьютер программное обеспечение;
* настроить права доступа к файлам и папкам на дисках с файловой системой NTFS;
* лимитировать членство пользователей в группах безопасности (например, жестко фиксировать состав группы администраторов);
* изменить параметры реестра, внести настройки в режимы запуска служб компьютера;
* установить параметры использования прикладных программ и т. п.

Количество настроек, которые можно регулировать при помощи групповых политик, растет с каждой версией операционной системы. Число доступных для настройки параметров перевалило уже за несколько тысяч. Поэтому описать подробно работу с групповыми политиками практически нереально. Опишем только основные моменты использования данной технологии.

Настраивать все параметры, существующие в групповой политике, не имеет смысла. После их применения работать на локальной системе станет практически не возможно из-за введенных ограничений. В каждой конкретной организации перечень параметров управления должен определяться индивидуально.

Чтобы применение групповых политик, прежде всего, облегчало работу как пользователя, так и администратора. Например, если есть постоянный канал доступа в Интернет, то целесообразно централизованно настроить программу обозревателя на использование соответствующих параметров доступа. Таким образом, новому пользователю не придется вносить никаких индивидуальных настроек в систему, а администратору объяснять, как это нужно сделать.

**К чему и как применяются групповые политики**

Правила групповой политики могут быть назначены для различных объектов: локальный компьютер, сайт, домен, любое организационное подразделение, причем к каждому такому объекту может быть привязано несколько политик.

**Примечание**

В Windows 2008/Windows 7 групповая политика может применяться раздельно для пользователей из группы администраторов (локальная политика администратора) и остальных пользователей (неадминистративная локальная политика).

В разных политиках один и тот же параметр может быть определен с отличающимися значениями. Например, в связи со спецификой обрабатываемой информации администратор подразделения может потребовать использования более строгих правил создания паролей, чем те, которые заданы администратором домена. Какие правила действуют при разрешении подобных ситуаций?

Очередность применения политик. Политики применяются в соответствии с иерархической структурой организации (структурой службы каталогов). Сначала используется локальная политика, а потом последовательно применяются политики с самого верхнего структурного уровня до самого нижнего (от общего к частному). При наличии на одном уровне нескольких политик, они применяются по очереди снизу вверх списка (самая верхняя политика в списке будет применена на данном уровне последней).

**Разрешение конфликтов политик.**

Значение параметра, регулируемого одной политикой, может противоречить аналогичному значению, но в другой политике, также применяемой к объекту. При наличии конфликтующих значений будет использован параметр, задаваемой следующей по очереди политикой. На практике это соответствует применению политики подразделения — "непосредственного начальника". Если существует конфликт параметров политики компьютер и пользователь одного уровня, то обычно больший вес имеет параметр, заданный для компьютера.

В случае необходимости администраторы могут устанавливать для политик признаки запрета перезаписи и/или обязательного значения параметра. Если политика описана как не допускающая изменения параметров, то ее настройки будут иметь преимущество и не смогут быть изменены значениями следующей применяемой политики.

Администратор может также указать, что значения политики не должны наследоваться от политики более высокого уровня. В этом случае "отсекаются" настройки политик, которые применялись до данного уровня.

Примечание

Если возникает конфликт требований "не переписывать" и "не наследовать", то преимущество имеет установка "не переписывать". Фактически это означает, что администратор подразделения более высокого уровня всегда сможет применить свои настройки.

**Последствия отключений политик**

Параметры политик условно можно разделить на две группы. Первая группа — это параметры настройки, существующие во временных ключах реестра системы. Действует политика — есть ключи. Политика отключена — ключи не создаются. Иными словами, отключение политики осуществится "безболезненно".

Вторая группа параметров задает значения существующих ключей реестра или создает такие ключи при первом применении. Главное, что такие параметры не будут удалены при снятии политики. В первую очередь это свойственно настройкам, импортируемым из файлов административных шаблонов.

Если политика устанавливает такой параметр, то снятие политики ничего не меняет в настройках системы. Ведь параметр реестра уже создан, а отсутствие политики означает просто сохранение его в том значении, которое было установлено политикой. Чтобы восстановить значения по умолчанию для таких параметров, администратору недостаточно просто снять политику. Нужно создать новые настройки, которые соответствуют значениям настройки по умолчанию, и применить их к компьютерам (пользователям).

Поэтому если необходимость применения какой-либо политики отпала, то рекомендуется просто отключить привязку (link) данной политики к конкретному подразделению, а саму политику не удалять. Во-первых, эти настройки могут вам опять понадобиться. А во-вторых, наличие ранее выполнявшихся настроек может помочь проанализировать действующие в подразделении параметры компьютеров и пользователей.

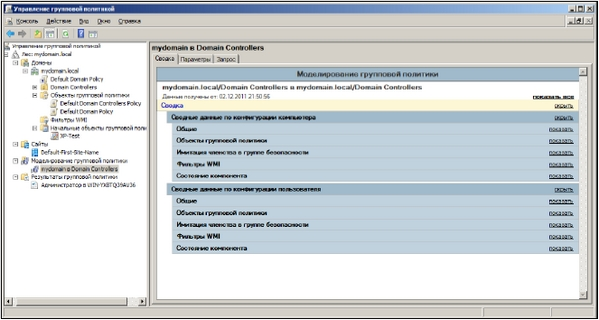
**Чем редактировать групповую политику**

Групповые политики домена Windows 2008 (R2) можно создавать и редактировать как на серверах Windows 2008 (R2), так и с рабочих станций Windows 7.

Консоль редактирования групповой политики входит в состав сервера, но ее необходимо установить в диспетчере сервера как дополнительный компонент управления групповыми политиками. Если необходимо управлять групповыми политиками с рабочей станции, то на компьютер сначала следует установить средства удаленного администрирования сервера (RSAT — Remote Server Administration Tool), которые бесплатно доступны со страницы http://go.microsoft.com/fwlink/ ?LinkId=130862. После установки RSAT нужно включить новые компоненты в Панели управления: для этого надо выбрать Программы и компоненты | Включение или отключение компонентов Windows, затем установить флажок Средства управления групповыми политиками по пути Средства удаленного администрирования сервера | Средства администрирования возможностей.

После этих операций в составе программ меню Администрирование появляется задача Управление групповыми политиками.

В оснастке Управление групповыми политиками четко видна иерархическая структура политик, с помощью которой удобно назначать ("привязывать", создавать линк) политики к подразделениям. Можно воспользоваться специализированными интерфейсами, которые покажут, какие параметры политики реально заданы администратором (в отличие от параметров по умолчанию). При наличии разветвленной структуры групповых политик определить, какие параметры будут применены из создаваемой политики, крайне затруднительно. В оснастке есть два интерфейса: моделирование политики и просмотр результирующего значения, позволяющие сформировать отчет о применяемых показателях. Для этого достаточно вызвать команду Создать... и далее следовать указаниям мастера (выбрать анализируемую политику, подразделение, пользователей и т. д.). На рис. показан пример окна моделирования политики (для отображения конкретных значений параметров нужно перейти по ссылкам показать).



**Фильтрация при помощи WMI-запросов**

Существует возможность уточнять область применения политики на основе WMI-фильтров. Администратор, знакомый с основами программирования и использования WMI (см. разд. "Windows Management Interface” далее в этой главе), может создать фильтры применения политики, учитывающие любые параметры конфигурации систем (как аппаратного, так и программного обеспечения).

При помощи фильтров можно выполнить сколь угодно точную фильтрацию, однако интерфейс назначения фильтров в групповой политике не содержит никаких средств проверки правильности запроса (это можно сделать уже при моделировании или проверке результирующих значений). Поэтому, чтобы исключить ошибки в настройках, WMI-запросы должны быть предварительно проверены другими средствами.

**Настройка параметров безопасности групповых политик**

Фильтровать доступ к групповой политике можно с помощью настройки ее параметров безопасности. Достаточно соответствующим образом определить те группы (или индивидуально) безопасности, которые будут иметь или не иметь право доступа и установки групповой политики.

Метод не требует дополнительных разъяснений. Но фактически при его использовании мы вместо усложнения структуры каталогов создаем соответствующую структуру групп безопасности.

**Предпочтения групповых политик**

В групповых политиках Windows появился дополнительный раздел — Предпочтения. Параметры этого раздела позволяют управлять подключением дисков, параметрами реестра, локальными пользователями и группами, службами, файлами и папками.

Главное преимущество раздела Предпочтения — легкость назначения параметров без обращения к каким-либо сценариям, составлению сложных запросов и т. д. Это позволяет, с одной стороны, облегчить настройку групповой политики, с другой — упростить структуру службы каталогов, поскольку не нужно будет создавать дополнительных контейнеров для выборки компьютеров.

Для использования раздела Предпочтения не нужно знать языки программирования, правила составления запросов в них и т. п. Все операции проводятся при помощи графического интерфейса. При этом возможности отбора крайне велики.

**Практическая часть**

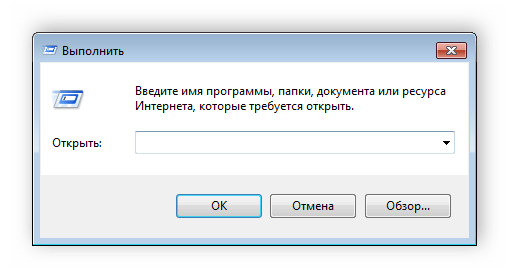
**Редактор групповой политики**

В Windows 7 Домашняя Базовая/Расширенная и Начальная редактор групповых политик просто отсутствует. Разработчики позволяют использовать его только в профессиональных версиях Виндовс, например, в Windows 7 Максимальная. Если вы не обладаете этой версией, то те же действия вам придется выполнять через изменения параметров реестра. Давайте подробнее рассмотрим редактор.

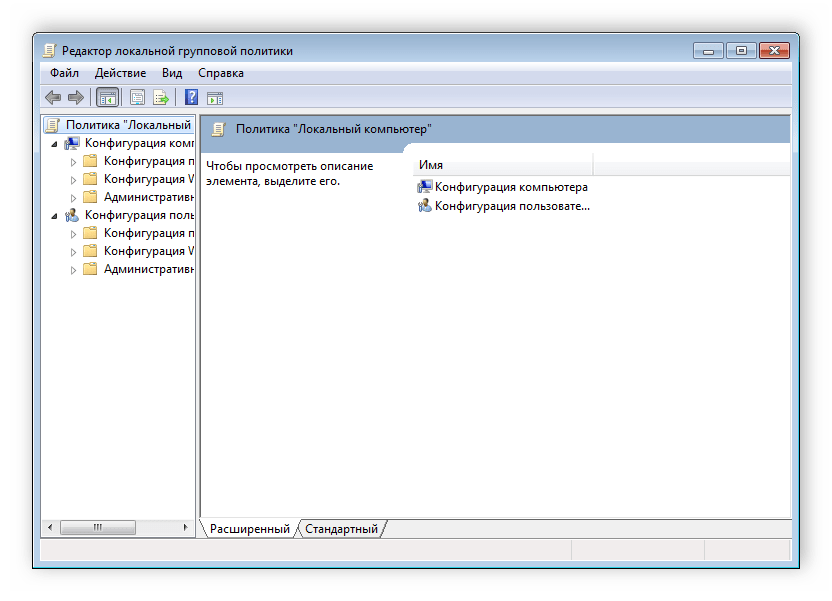
Запуск редактора групповой политики

Переход к среде работы с параметрами и настройками осуществляется за несколько простых действий. Вам только необходимо:

1. Зажать клавиши **Win + R**, чтобы открыть **«Выполнить»**.



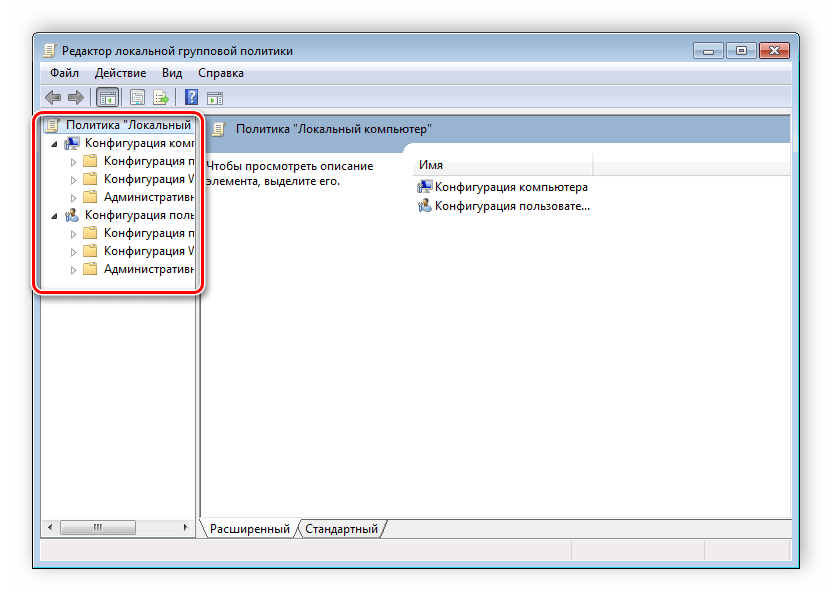
1. Напечатать в строке **gpedit.msc** и подтвердить действие, нажав **«ОК»**. Далее запустится новое окно.



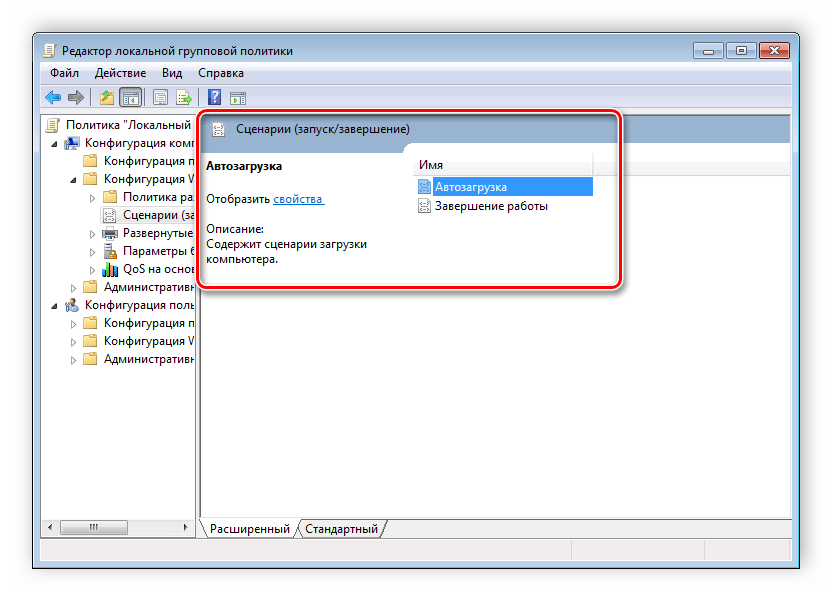
Теперь можно приступать к работе в редакторе.

Работа в редакторе

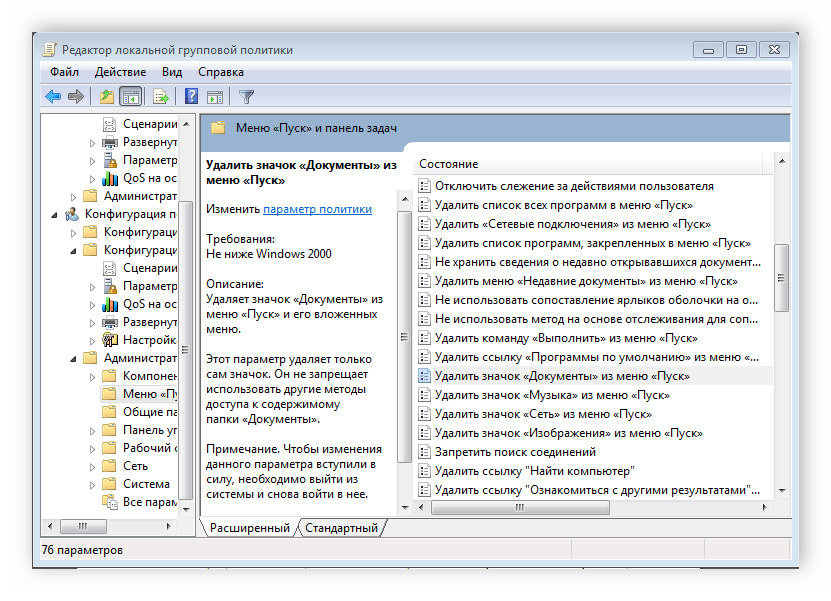
Разделяется главное окно управления на две части. Слева располагается структурированные категории политик. Они в свою очередь делятся еще на две различные группы – настройка компьютера и настройка пользователя.



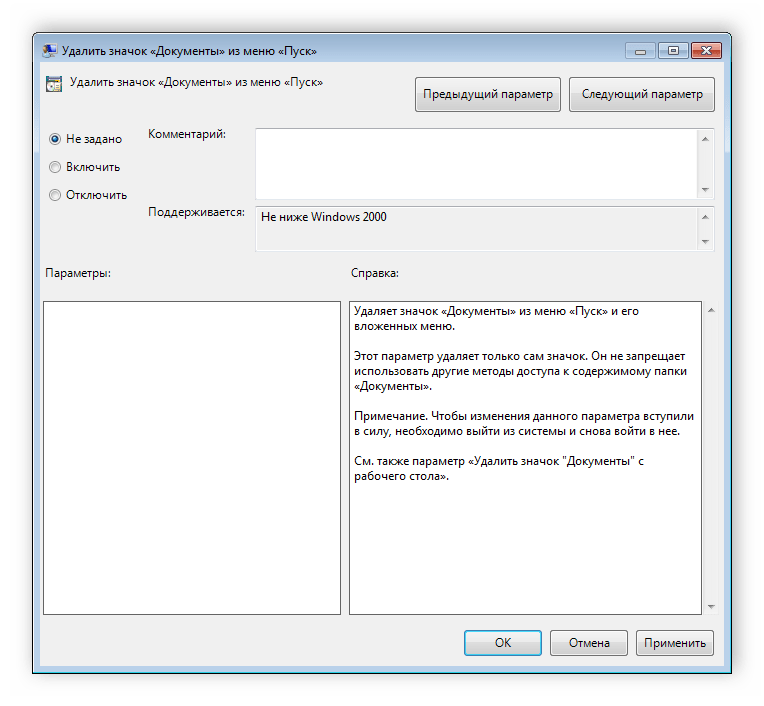
В правой части отображается информация о выбранной политике из меню слева.



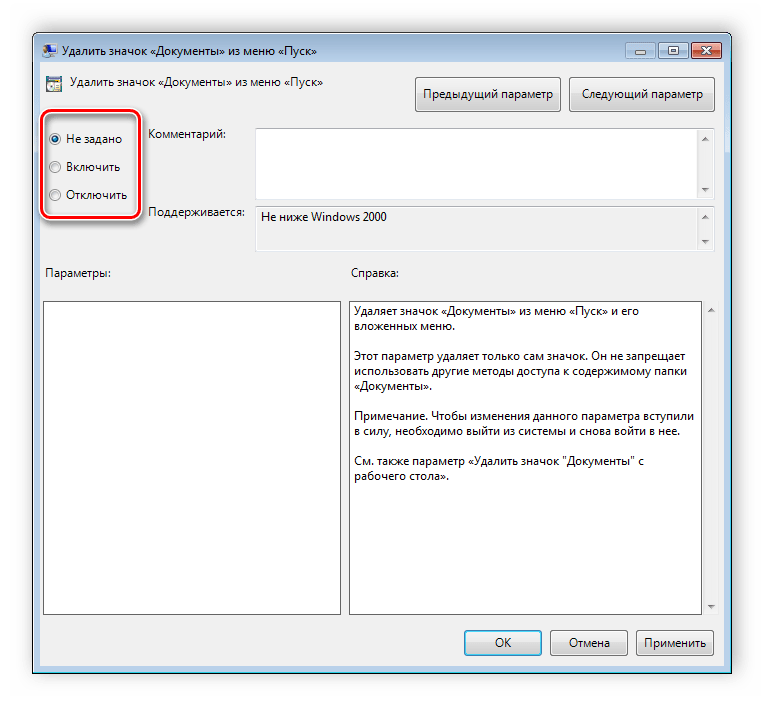
Из этого можно сделать вывод, что работа в редакторе осуществляется путем перемещения по категориям для поиска необходимой настройки. Выберите, например, **«Административные шаблоны»** в **«Конфигурации пользователя»** и перейдите в папку **«Меню «Пуск» и диспетчер задач»**. Теперь справа отобразятся параметры и их состояния. Нажмите на любую строку, чтобы открыть ее описание.

Настройки политики

Каждая политика доступна для настройки. Открывается окно редактирования параметров по двойному щелчку на определенную строку. Вид окон может отличаться, все зависит от выбранной политики.



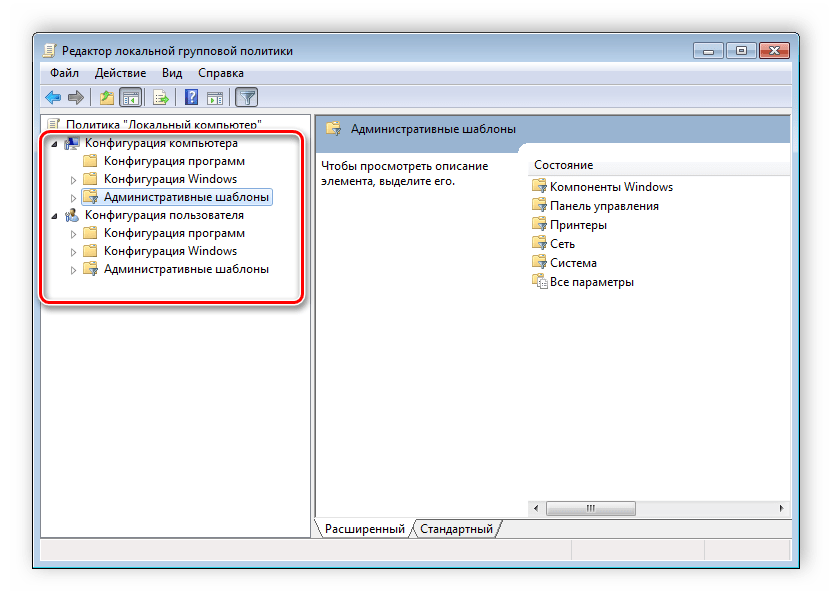
Стандартное простое окно имеет три различных состояния, которые настраиваются пользователем. Если точка стоит напротив **«Не задано»**, то политика не действует. **«Включить»** – она будет работать и активируются настройки. **«Отключить»** – находится в рабочем состоянии, однако параметры не применяются.



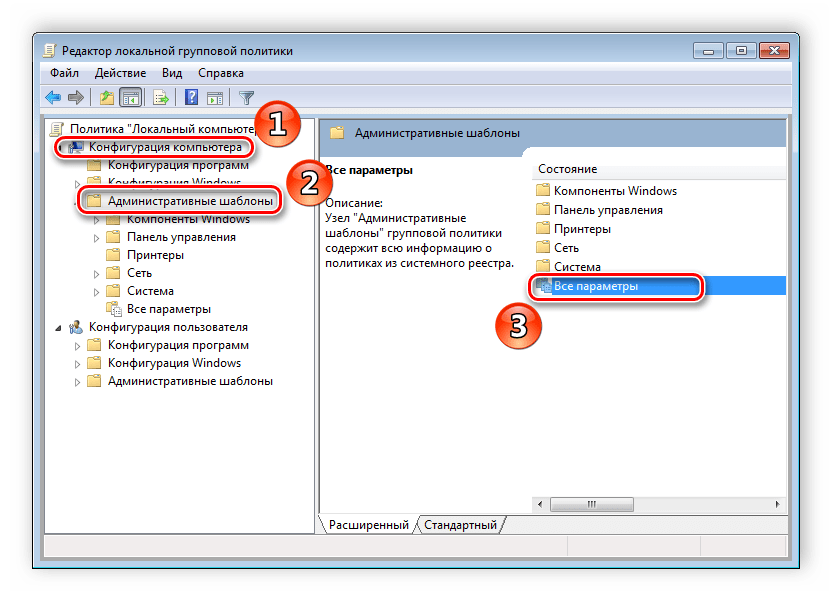
Рекомендуем обратить внимание на строку **«Поддерживается»** в окне, она показывает, на какие версии Windows распространяется политика.

Фильтры политик

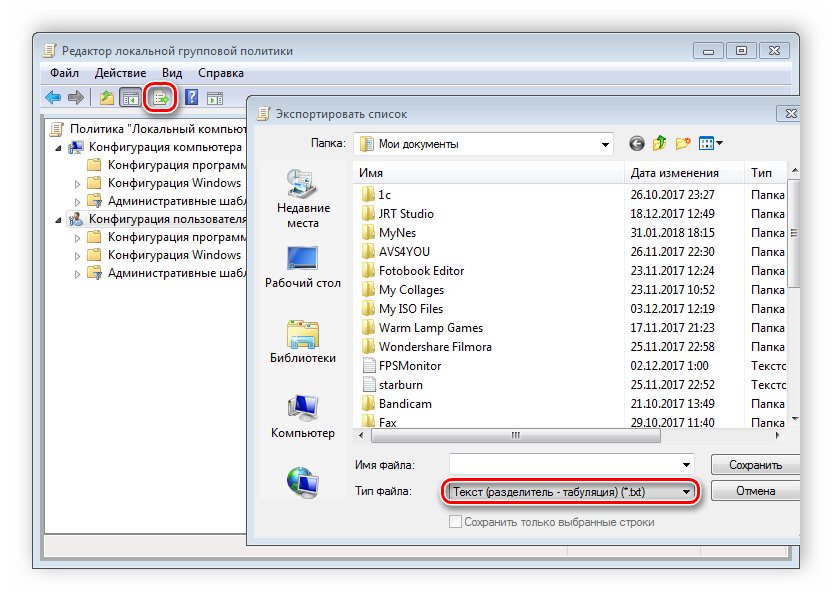
Минусом редактора является отсутствие функции поиска. Существует множество различных настроек и параметров, их больше трех тысяч, все они разбросаны по отдельным папкам, а поиск приходится осуществлять вручную. Однако данный процесс упрощается благодаря структурированной группе из двух ветвей, в которых расположились тематические папки.



Например, в разделе **«Административные шаблоны»**, в любой конфигурации, находятся политики, которые никак не связаны с безопасностью. В этой папке находится еще несколько папок с определенными настройками, однако можно включить полное отображение всех параметров, для этого нужно нажать на ветвь и выбрать пункт в правой части редактора **«Все параметры»**, что приведет к открытию всех политик данной ветви.

Экспорт списка политик

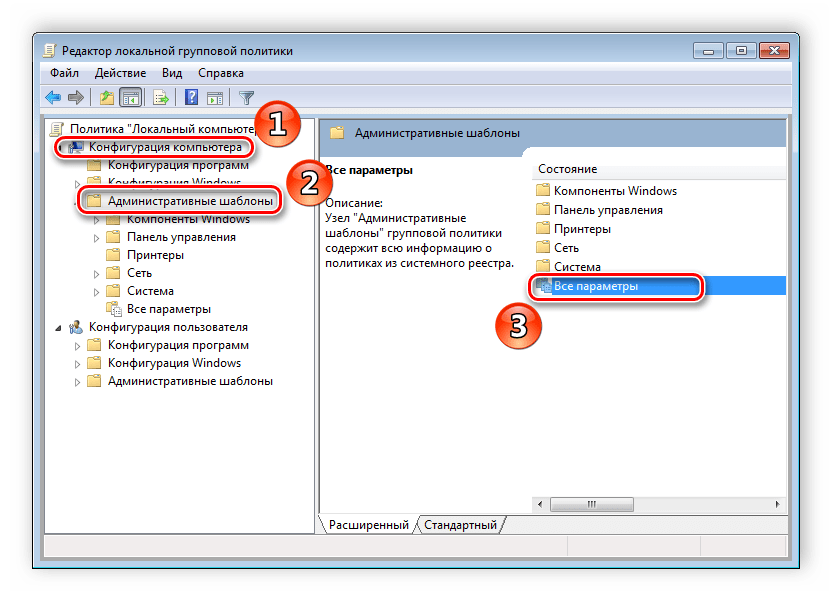
Если все-таки появляется необходимость найти определенный параметр, то сделать это можно только путем экспорта списка в текстовый формат, а потом уже через, например Word, осуществлять поиск. В главном окне редактора есть специальная функция **«Экспорт списка»**, он переносит все политики в формат TXT и сохраняет в выбранном месте на компьютере.



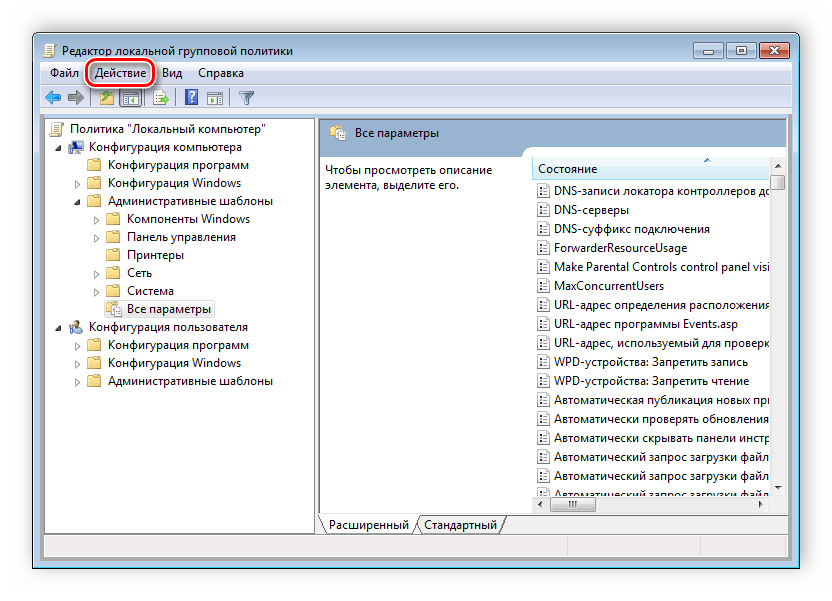
Применение фильтрации

Благодаря появлению ветви**«Все параметры»** и улучшению функции фильтрации поиск практически не нужен, ведь лишнее откидывается путем применения фильтров, а отображаться будут только необходимые политики. Давайте подробнее рассмотрим процесс применения фильтрации:

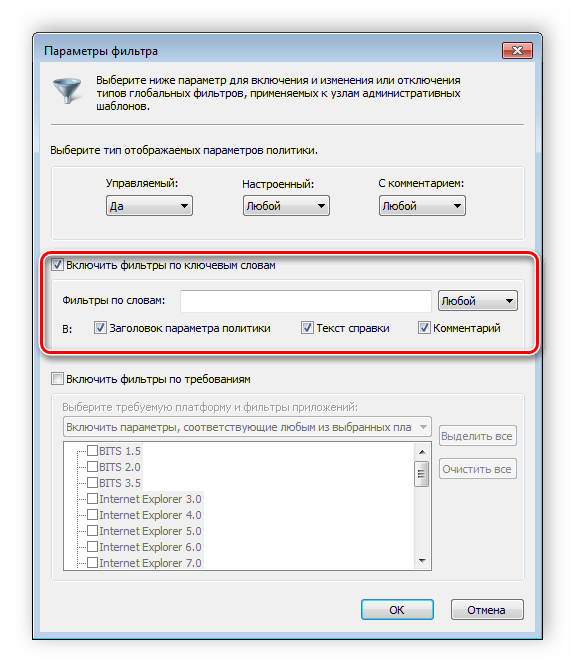
1. Выберите, например, **«Конфигурация компьютера»**, откройте раздел **«Административные шаблоны»** и перейдите в **«Все параметры»**.



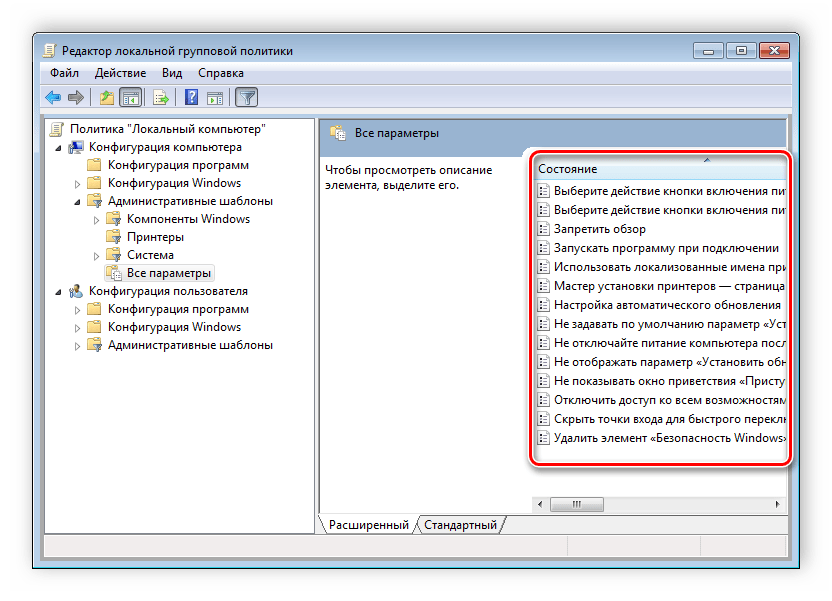
1. Разверните всплывающее меню **«Действие»** и перейдите в **«Параметры фильтра»**.



1. Поставьте галочку возле пункта **«Включить фильтры по ключевым словам»**. Здесь имеется несколько вариантов подбора соответствий. Откройте всплывающее меню напротив строки ввода текста и выберите **«Любой»** – если нужно отображать все политики, которые соответствуют хотя бы одному указанному слову, **«Все»** – отобразит политики, содержащие текст из строки в любом порядке, **«Точный»** – только параметры, точно соответствующие заданному фильтру по словам, в правильном порядке. Флажками снизу строки соответствий отмечаются места, где будет осуществляться выборка.



1. Нажмите **«ОК»** и после этого в строке **«Состояние»** отобразятся только подходящие параметры.



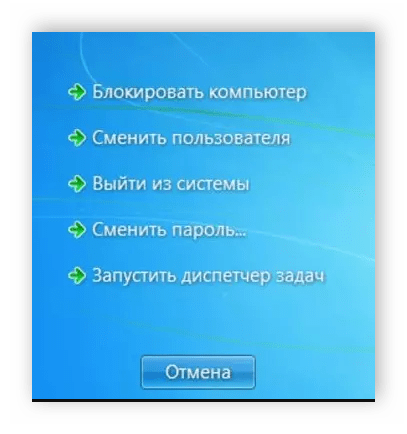
В том же всплывающем меню **«Действие»** ставится или убирается галочка напротив строки **«Фильтр»**, если нужно применить или отменить заранее заданные настройки подбора соответствий.

Принцип работы с групповыми политиками

Рассматриваемый в этой статье инструмент позволяет применять множество самых разнообразных параметров. К сожалению, большинство из них понятно только профессионалам, использующим групповые политики в рабочих целях. Однако и обычному пользователю есть что настроить, используя некоторые параметры. Разберем несколько простых примеров.

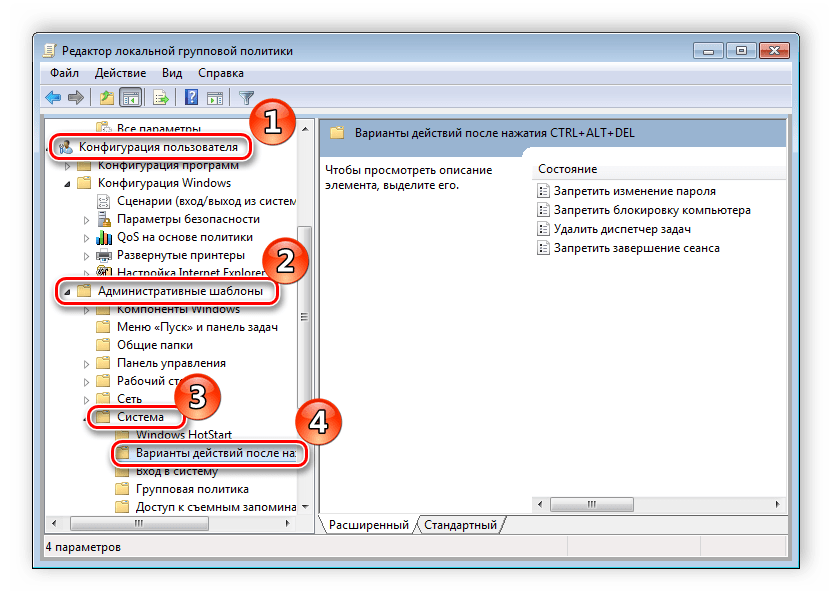
Изменение окна безопасности Windows

Если в Виндовс 7 зажать сочетание клавиш **Ctrl + Alt + Delete**, то будет запущено окно безопасности, где осуществляется переход к диспетчеру задач, блокировка ПК, завершение сеанса системы, смена профиля пользователя и пароля.

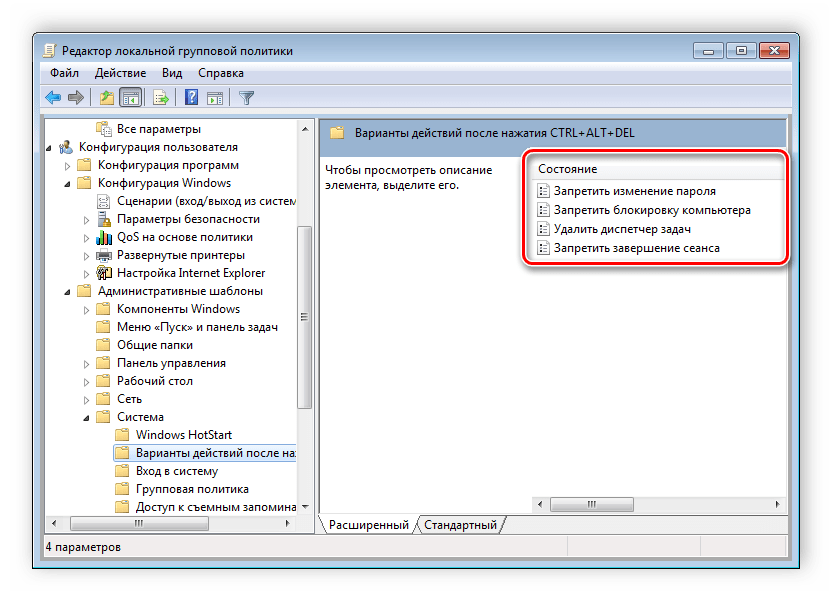


Каждая команда за исключением **«Сменить пользователя»** доступна для редактирования путем изменения нескольких параметров. Выполняется это в среде с параметрами или путем изменения реестра. Рассмотрим оба варианта.

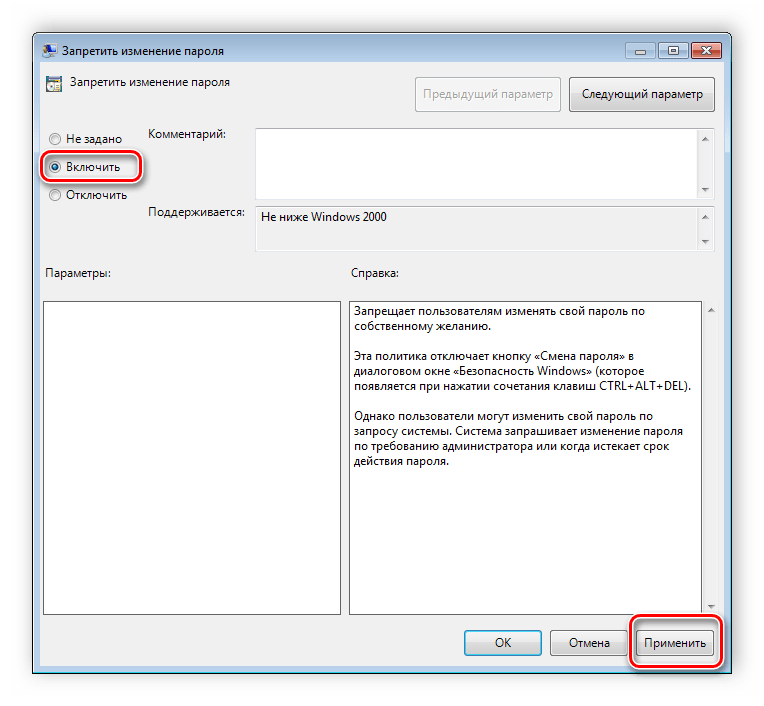
1. Откройте редактор.
2. Перейдите в папку **«Конфигурация пользователя»**, **«Административные шаблоны»**, **«Система»** и **«Варианты действий после нажатия Ctrl + Alt + Delete»**.



1. Откройте любую необходимую политику в окне справа.



1. В простом окне управления состоянием параметра поставьте галочку напротив **«Включить»** и не забудьте применить изменения.

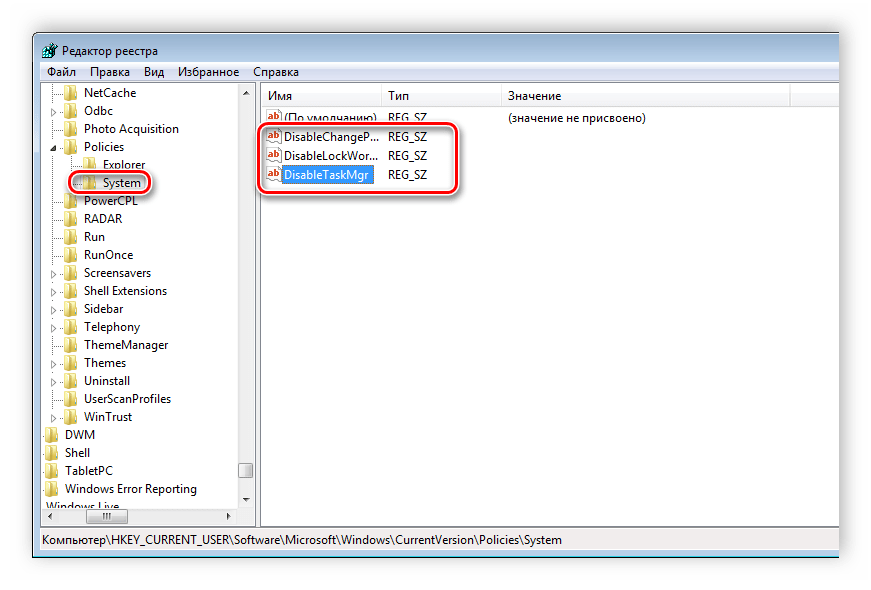


Пользователям, у которых нет редактора политик, все действия нужно будет выполнять через реестр. Давайте рассмотрим все действия пошагово:

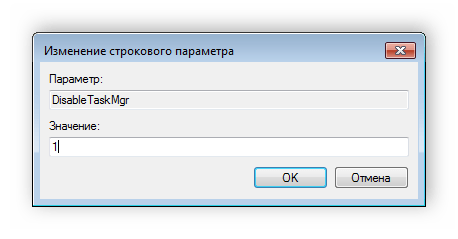
1. Перейдите к редактированию реестра.
2. Перейдите к разделу **«System»**. Он находится по этому ключу:

HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\System

1. Там вы увидите три строки, отвечающие за появление функций в окне безопасности.



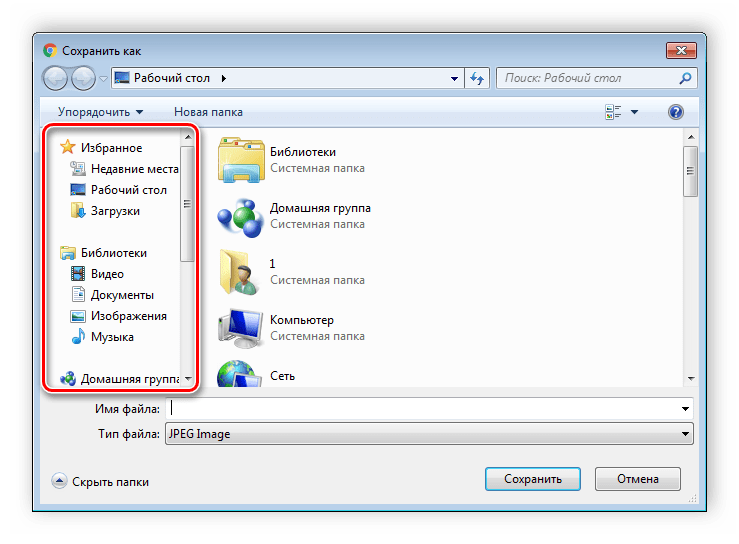
1. Откройте необходимую строку и поменяйте значение на **«1»**, чтобы активировать параметр.



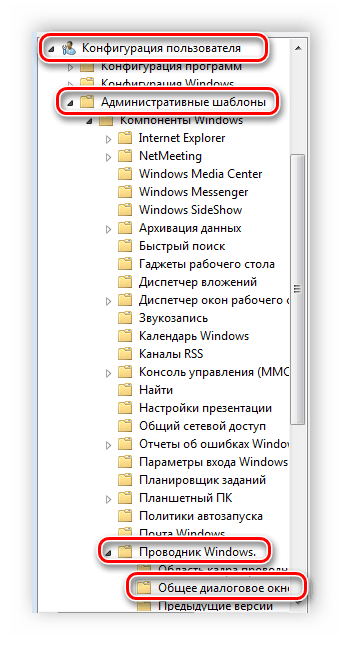
После сохранения изменений деактивированные параметры больше не будут отображаться в окне безопасности Windows 7.

Изменения панели мест

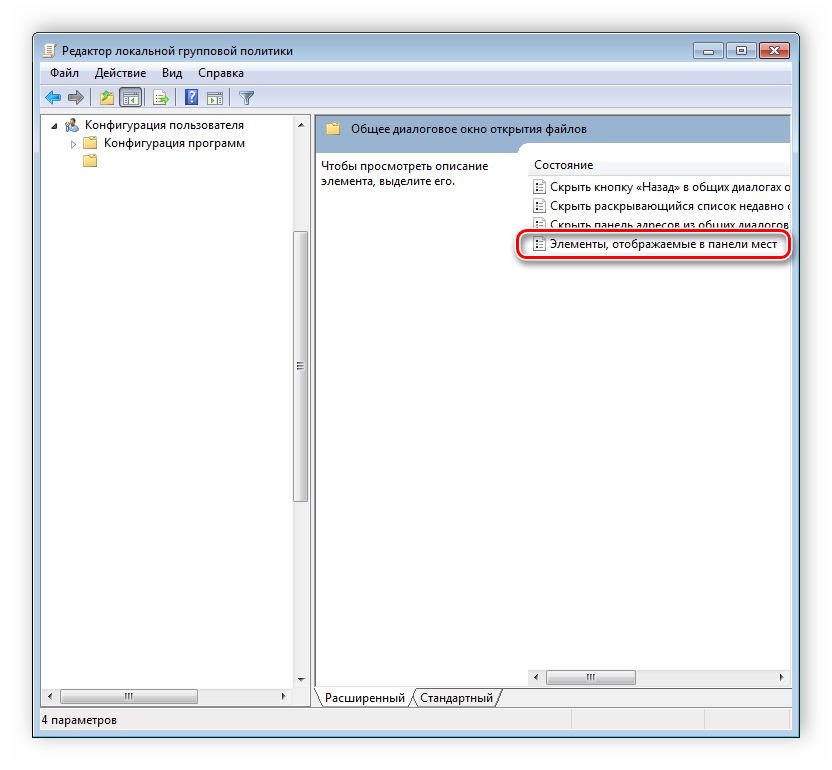
Многие используют диалоговые окна **«Сохранить как»** или **«Открыть как»**. Слева отображается навигационная панель, включая раздел **«Избранное»**. Данный раздел настраивается стандартными средствами Windows, однако это долго и неудобно. Поэтому лучше воспользоваться групповыми политиками для редактирования отображения значков в данном меню. Редактирование происходит следующим образом:



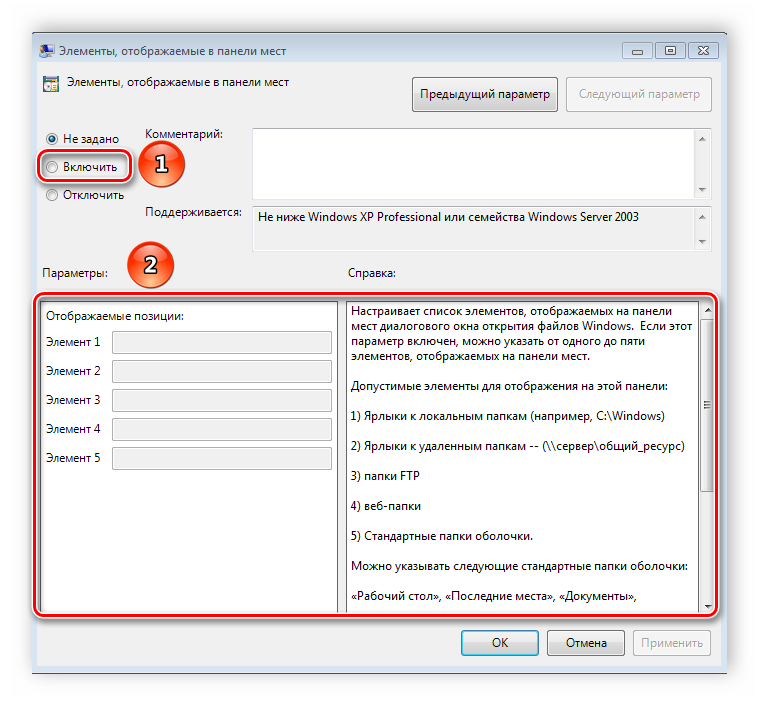
1. Перейдите в редактор, выберите **«Конфигурация пользователя»**, перейдите к **«Административные шаблоны»**, **«Компоненты Windows»**, **«Проводник»** и конечной папкой будет «**Общее диалоговое окно открытия файлов»**.



1. Здесь вас интересует **«Элементы, отображаемые в панели мест»**.



1. Поставьте точку напротив **«Включить»** и добавьте до пяти различных путей сохранения в соответствующие строки. Справа от них отображается инструкция правильного указания путей к локальным или сетевым папкам.

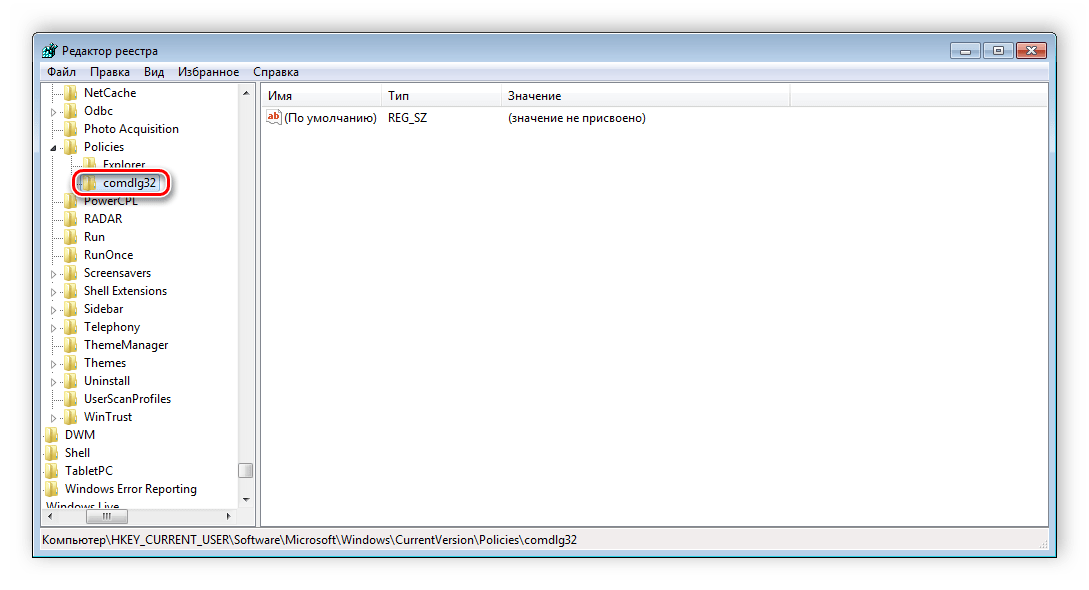


Теперь рассмотрим добавление элементов через реестр для пользователей, у которых отсутствует редактор.

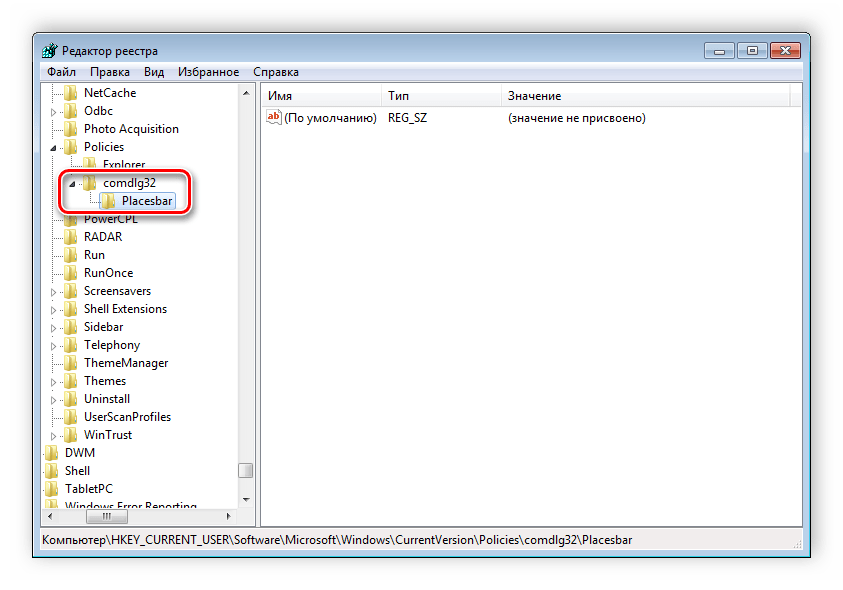
1. Перейдите по пути:

HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\

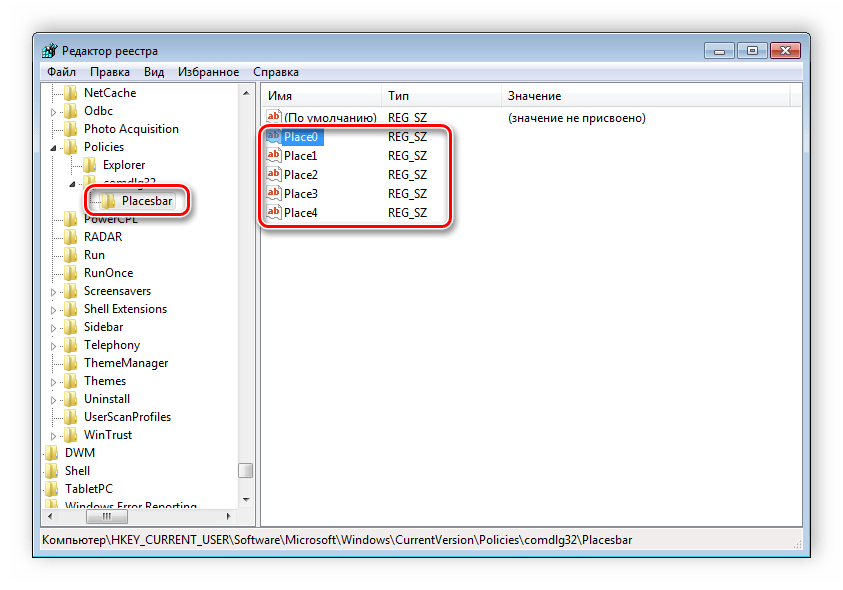
1. Выберите папку **«Policies»** и сделайте в ней раздел **comdlg32**.



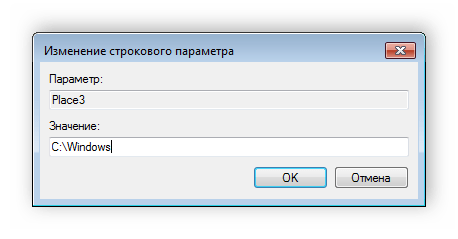
1. Перейдите в созданный раздел и сделайте внутри него папку **Placesbar**.



1. В этом разделе потребуется создать до пяти строковых параметров и назвать их от **«Place0»** до **«Place4»**.

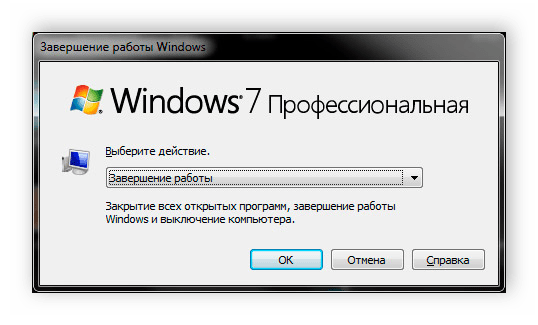


1. После создания откройте каждый из них и в строку введите необходимый путь к папке.

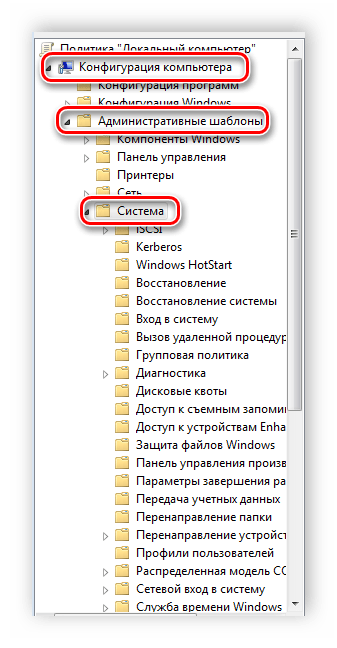


Слежение за завершением работы компьютера

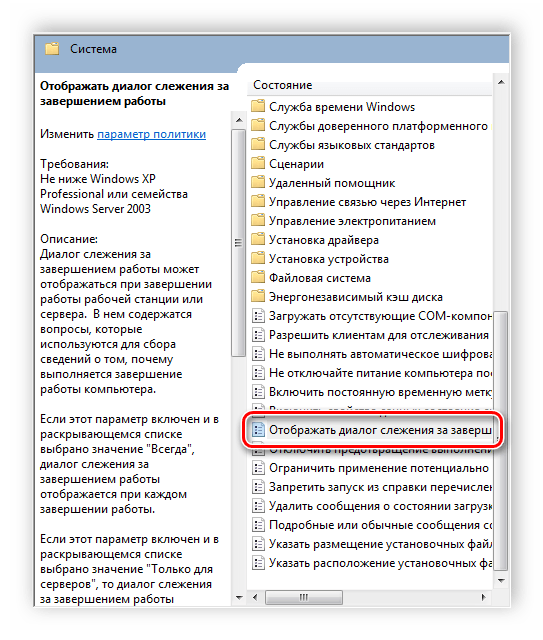
Когда вы завершаете работу за компьютером, выключение системы происходит без показа дополнительных окон, что позволяет не быстрее выключить ПК. Но иногда требуется узнать почему происходит выключение или перезапуск системы. В этом поможет включение специального диалогового окна. Включается оно с помощью редактора или путем изменения реестра.



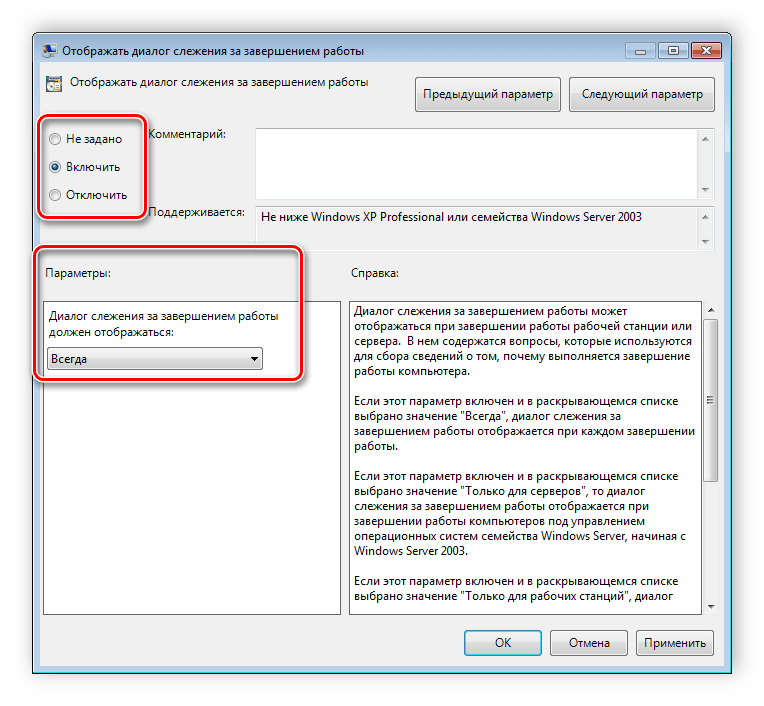
1. Откройте редактор и перейдите к **«Конфигурация компьютера»**, **«Административные шаблоны»**, после чего выберите папку **«Система»**.



1. В ней нужно выбрать параметр **«Отображать диалог слежения за завершением работы»**.



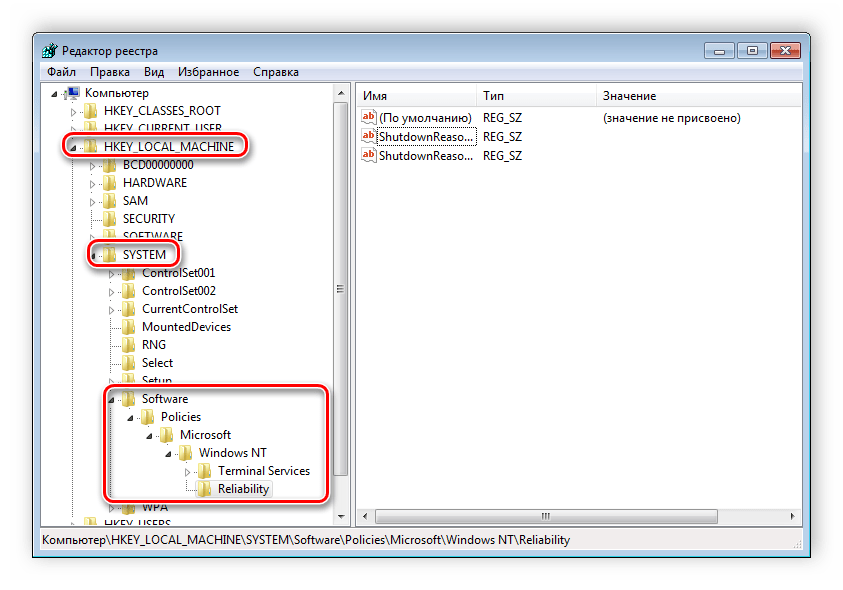
1. Откроется простое окно настройки, где необходимо поставить точку напротив **«Включить»**, при этом в разделе параметры во всплывающем меню необходимо указать **«Всегда»**. После не забудьте применить изменения.



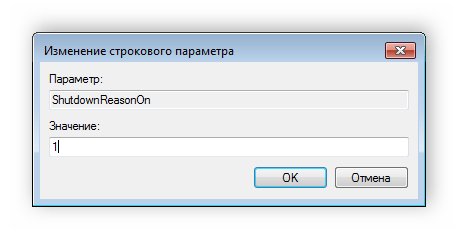
Данная функция включается и через реестр. Вам нужно совершить несколько простых действий:

1. Запустите реестр и перейдите по пути:

HKLM\Software\Policies\Microsoft\Windows NT\Reliability



1. Найдите в разделе две строки: **«ShutdownReasonOn»** и **«ShutdownReasonUI»**.
2. Введите в строку с состоянием **«1»**.



**Настраиваем локальную политику безопасности в Windows 7**

Варианты настройки политики безопасности

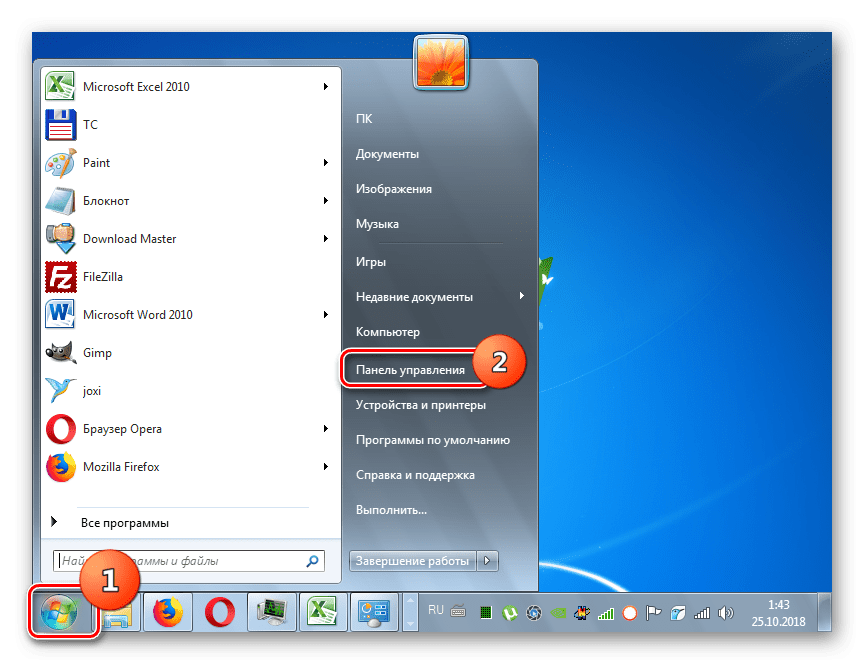
Прежде всего, нужно отметить, что по умолчанию политика безопасности настроена оптимально для выполнения повседневных задач рядового юзера. Производить манипуляции в ней нужно только в случае возникновения необходимости решить конкретный вопрос, требующий корректировки данных параметров.

Изучаемые нами настройки безопасности регулируются с помощью GPO. В Виндовс 7 сделать это можно, используя инструменты **«Локальная политика безопасности»** либо **«Редактор локальных групповых политик»**. Обязательным условием является вход в профиль системы с полномочиями администратора. Далее мы рассмотрим оба этих варианта действий.

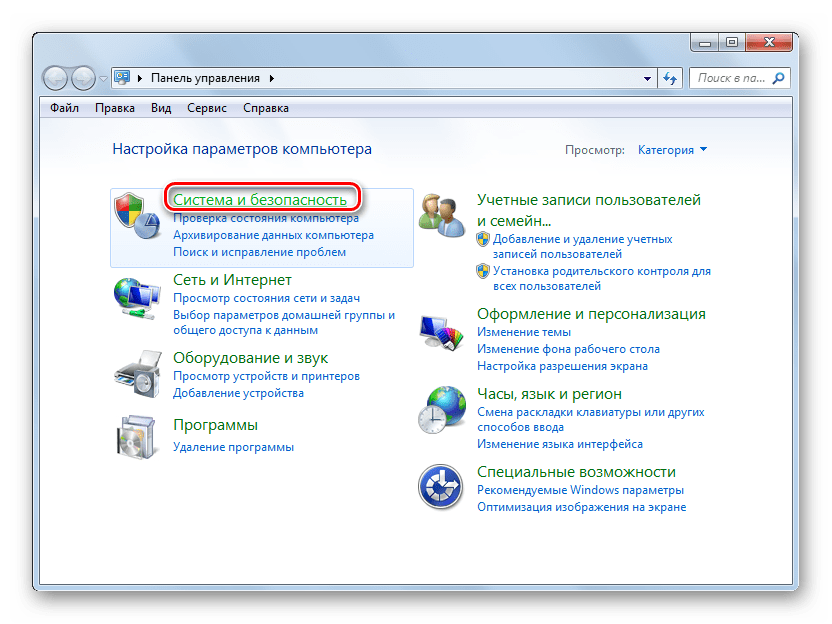
Способ 1: Применение инструмента «Локальная политика безопасности»

Прежде всего, изучим, как решить поставленную задачу с помощью инструмента **«Локальная политика безопасности»**.

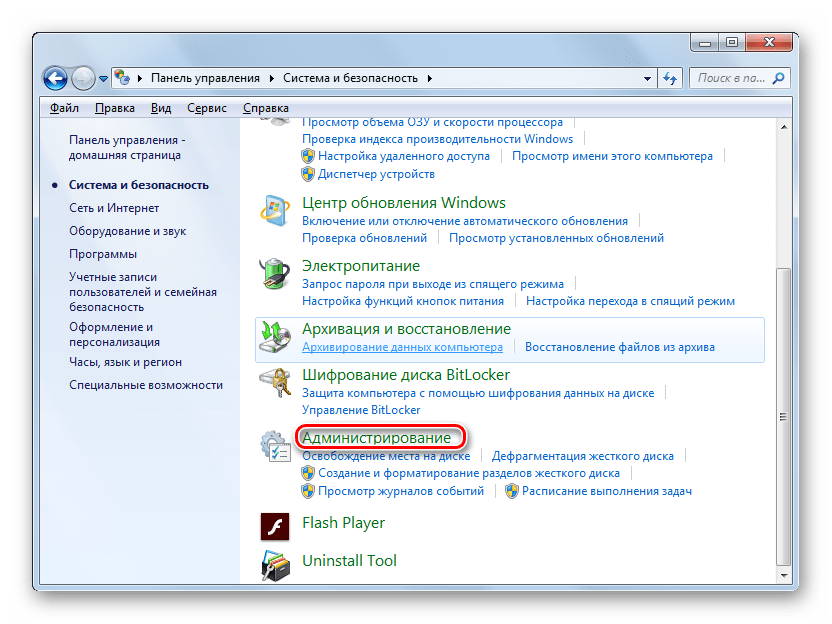
1. Чтобы запустить указанную оснастку, щелкните **«Пуск»** и перейдите в **«Панель управления»**.

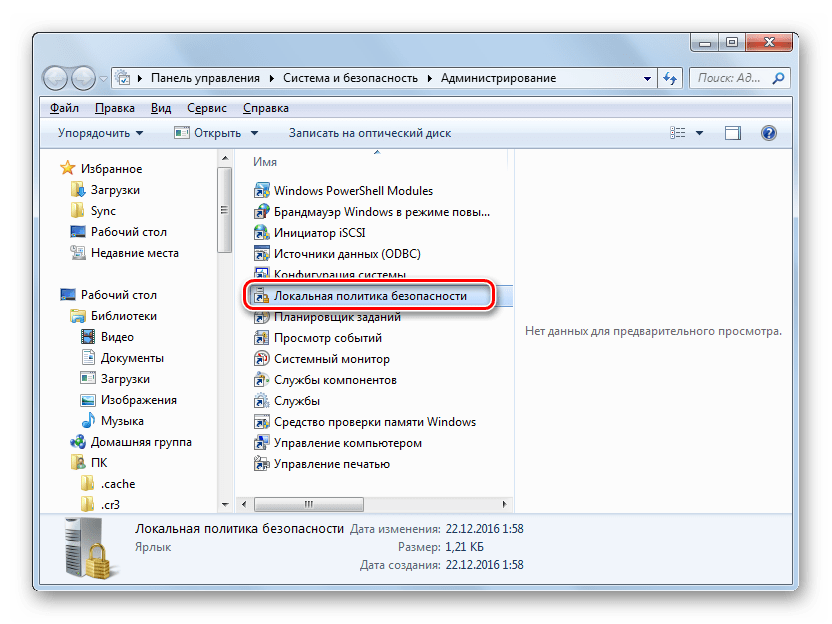


1. Далее откройте раздел **«Система и безопасности»**.



1. Щелкните **«Администрирование»**.

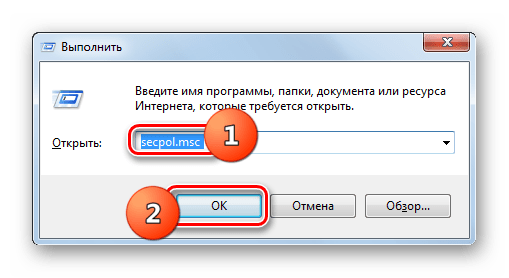


1. Из предложенного набора системных инструментов выберите вариант **«Локальная политика безопасности»**.

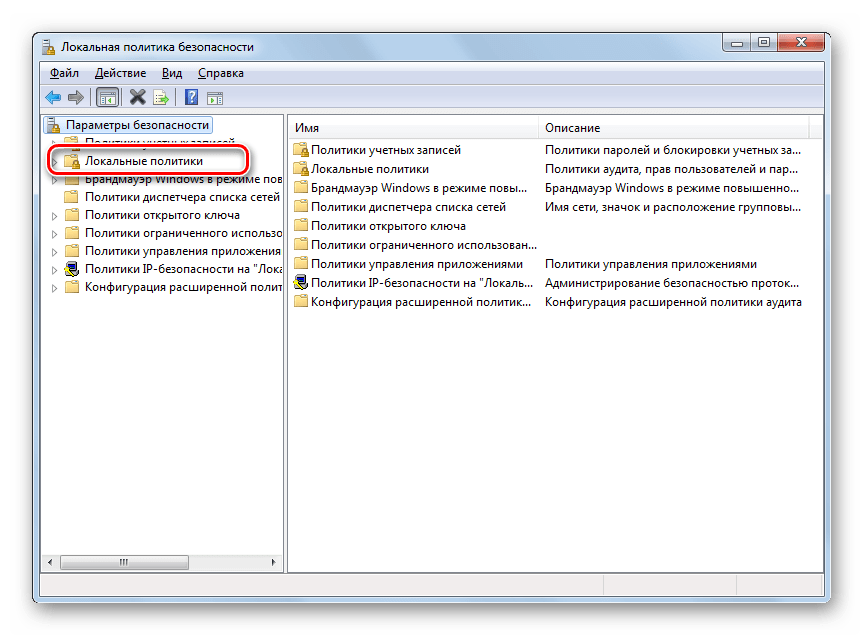
Также оснастку можно запустить и через окно **«Выполнить»**. Для этого наберите **Win+R** и введите следующую команду:

secpol.msc

Затем щелкните **«OK»**.



1. Указанные выше действия приведут к запуску графического интерфейса искомого инструмента. В подавляющем большинстве случаев возникает необходимость откорректировать параметры в папке **«Локальные политики»**. Тогда нужно щелкнуть по элементу с этим наименованием.

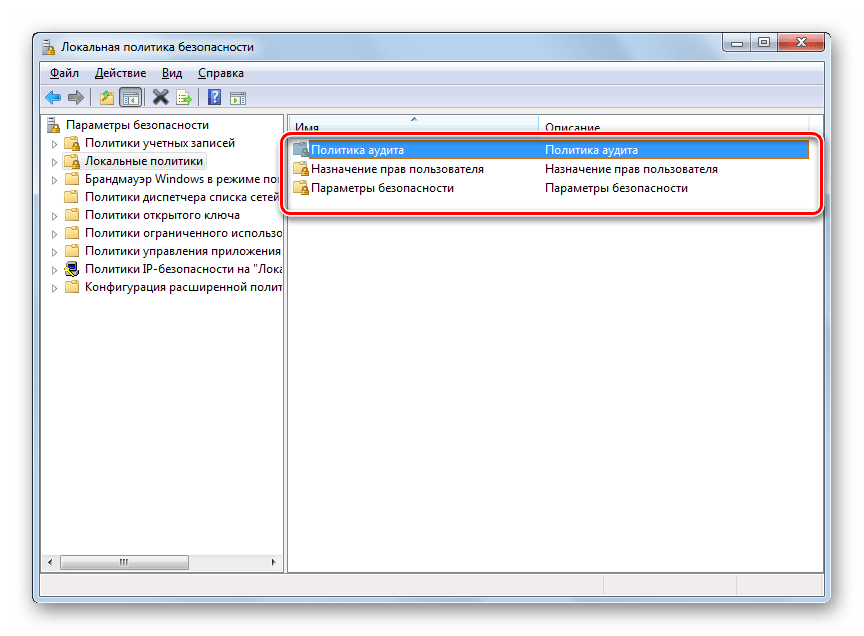


1. В данном каталоге располагается три папки.

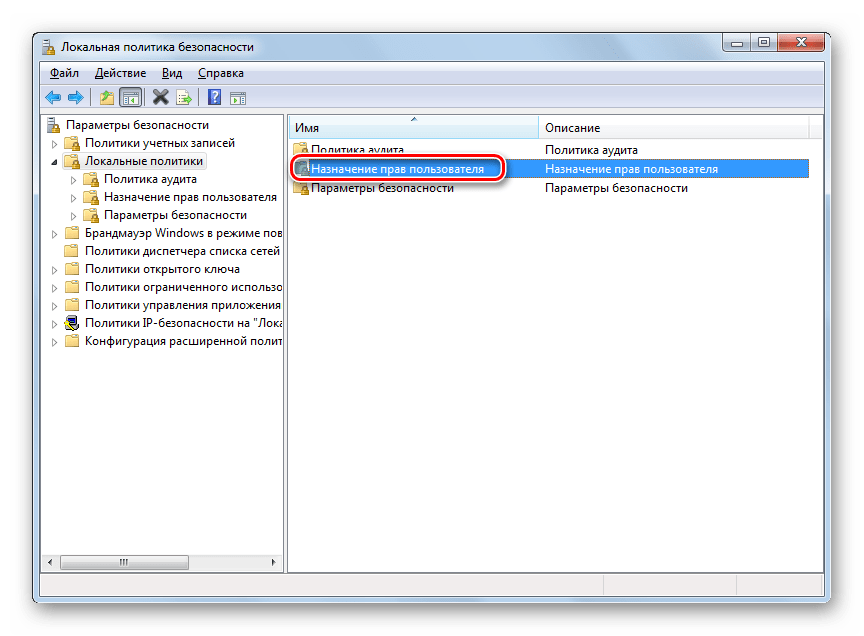
В директории**«Назначение прав пользователя»** определяются полномочия отдельных пользователей или групп юзеров. Например, можно указать, запрет или разрешение для отдельных лиц или категорий пользователей на выполнение конкретных задач; определить, кому разрешен локальный доступ к ПК, а кому только по сети и т.д.

В каталоге **«Политика аудита»** указываются события, предназначенные для записи в журнале безопасности.

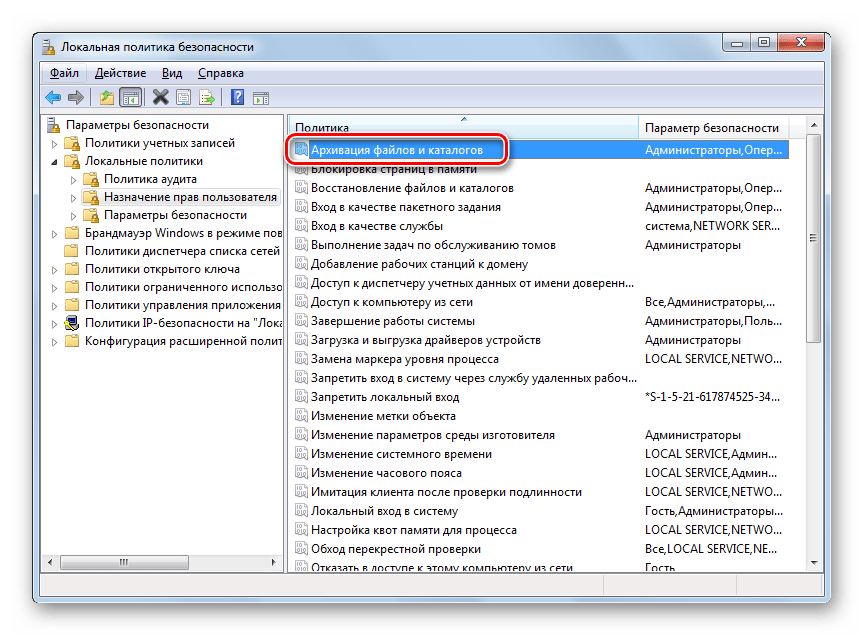
В папке **«Параметры безопасности»** указываются разнообразные административные настройки, которые определяют поведение ОС при входе в неё как локально, так и через сеть, а также взаимодействие с различными устройствами. Без особой необходимости данные параметры изменять не стоит, так как большинство соответствующих задач можно решить через стандартную настройку учетных записей, родительский контроль и разрешения NTFS.

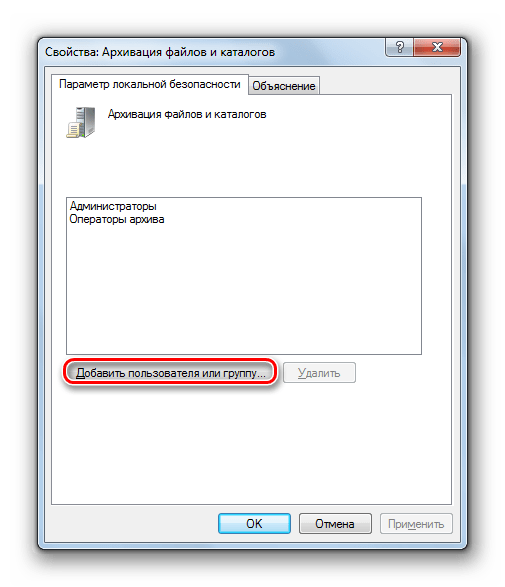


1. Для дальнейших действий по решаемой нами задаче щелкните по наименованию одного из указанных выше каталогов.

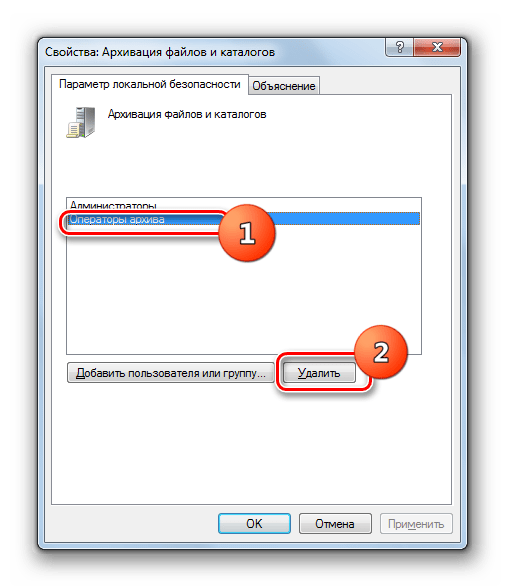


1. Откроется перечень политик выбранного каталога. Кликните по той из них, которую желаете изменить.

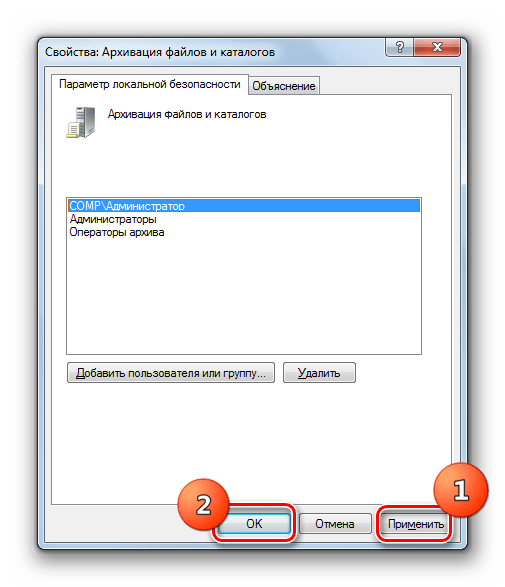


1. После этого откроется окошко редактирования политики. Его вид и действия, которые необходимо произвести, существенно отличаются от того, к какой именно категории она принадлежит. Например, для объектов из папки **«Назначение прав пользователя»** в открывшемся окне необходимо добавить или удалить имя конкретного пользователя либо группы юзеров. Добавление производится путем нажатия кнопки **«Добавить пользователя или группу…»**.

Если же необходимо произвести удаление элемента из выбранной политики, то выделите его и нажмите **«Удалить»**.



1. После завершения манипуляций в окне редактирования политики для сохранения внесенных корректировок не забудьте нажать кнопки **«Применить»** и **«OK»**, а иначе изменения не вступят в силу.



Мы описали изменение настроек безопасности на примере действий в папке **«Локальные политики»**, но по такой же аналогии можно производить действия и в других каталогах оснастки, например в директории **«Политики учетных записей»**.

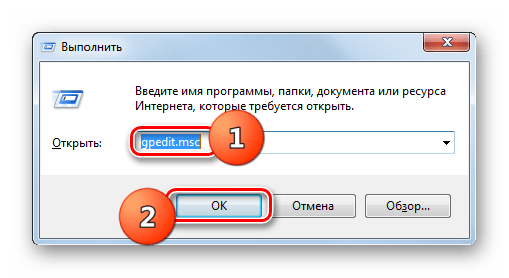
Способ 2: Использование инструмента «Редактор локальной групповой политики»

Настроить локальную политику можно также при помощи оснастки **«Редактор локальной групповой политики»**. Правда, данный вариант доступен не во всех редакциях Windows 7, а только в Ultimate, Professional и Enterprise.

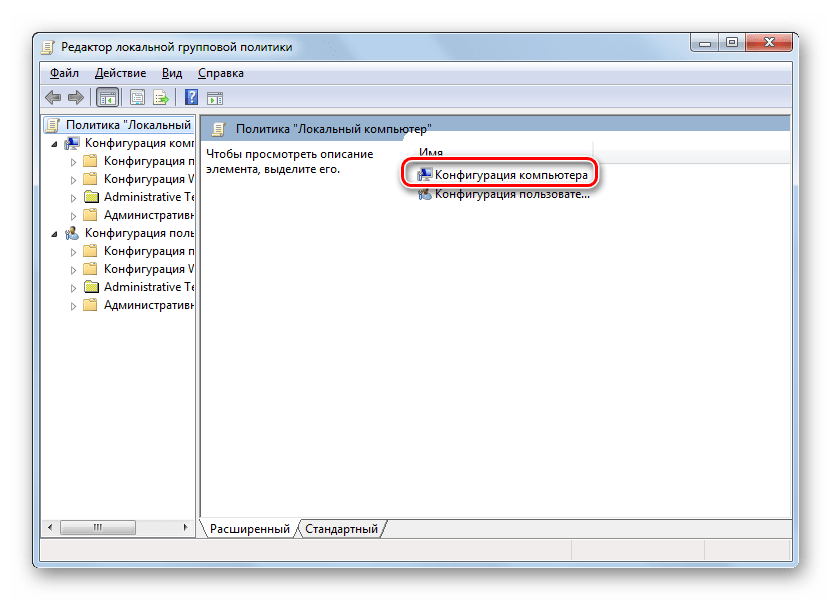
1. В отличие от предыдущей оснастки, данный инструмент нельзя запустить через **«Панель управления»**. Его можно активировать только путем введения команды в окно **«Выполнить»** или в **«Командную строку»**. Наберите **Win+R** и введите в поле такое выражение:

gpedit.msc

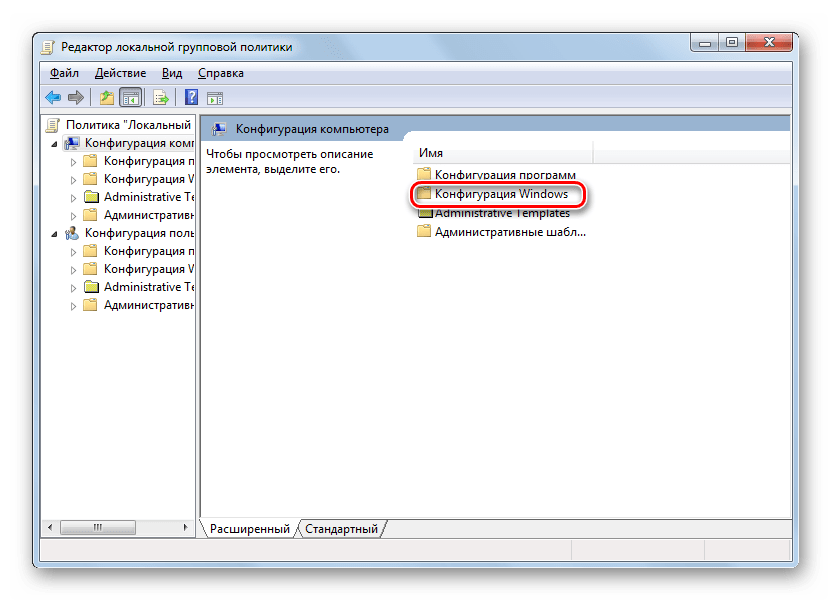
Затем щелкните **«OK»**.



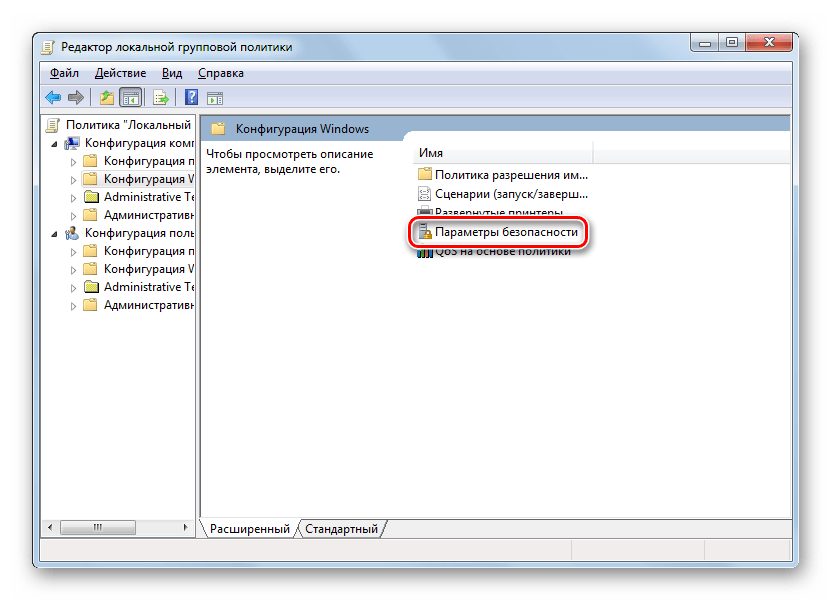
1. Откроется интерфейс оснастки. Перейдите в раздел **«Конфигурация компьютера»**.

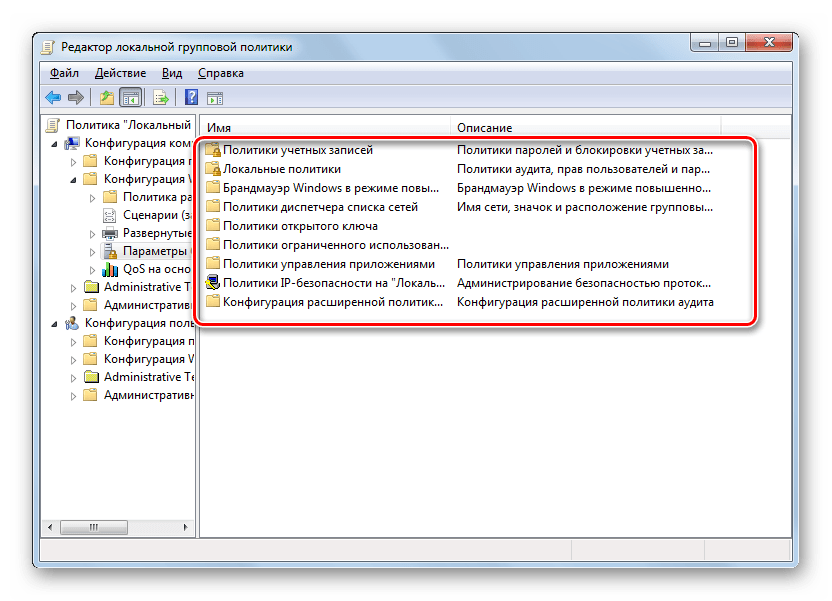


1. Далее щелкните по папке **«Конфигурация Windows»**.



1. Теперь щелкните по элементу **«Параметры безопасности»**.



1. Откроется директория с уже знакомыми нам по предыдущему методу папками: **«Политики учетных записей»**, **«Локальные политики»** и т.д. Все дальнейшие действия проводятся по точно такому же алгоритму, который указан при описании **Способа 1**, начиная с пункта 5. Единственное отличие состоит в том, что манипуляции будут выполняться в оболочке другого инструмента.

Настроить локальную политику в Виндовс 7 можно путем использования одной из двух системных оснасток. Порядок действий в них довольно схожий, отличие заключается в алгоритме доступа к открытию данных инструментов. Но изменять указанные настройки рекомендуем только тогда, когда вы полностью уверены, что это нужно сделать для выполнения определенной задачи. Если же таковой нет, эти параметры лучше не корректировать, так как они отрегулированы на оптимальный вариант повседневного использования.

**Настройка контроля пользователей путем включения ПК**

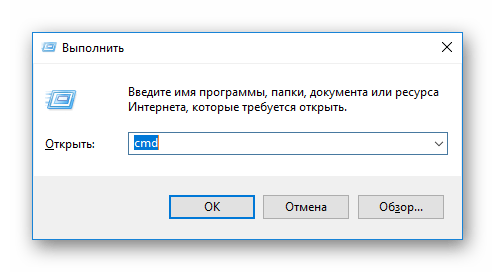
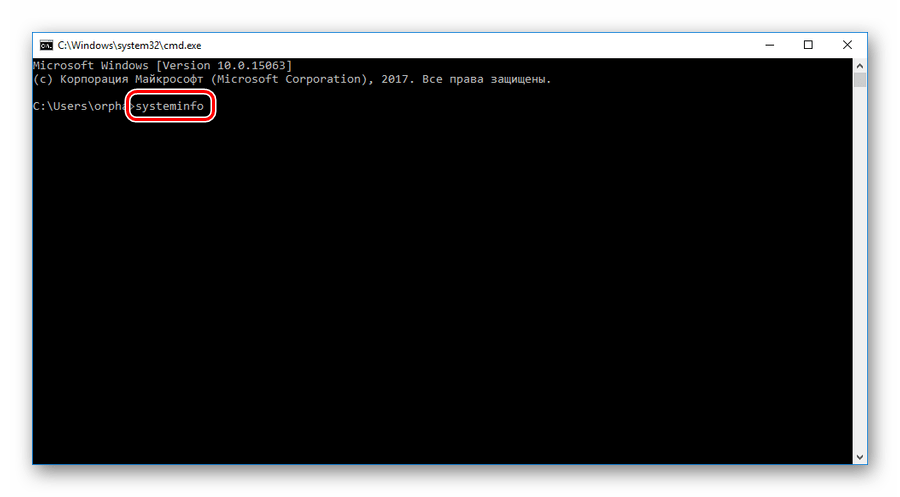
Одним из проявлений беспокойства о целостности своей информации является то, что все больше пользователей желают знать, не включался ли их ПК во то время, когда они отсутствовали. И это не какие-нибудь параноидальные проявления, а жизненная необходимость — от желания проконтролировать время нахождения за компьютером ребенка до попыток уличить в недобросовестности коллег, работающих в одном офисе. Поэтому этот вопрос заслуживает более детального рассмотрения.

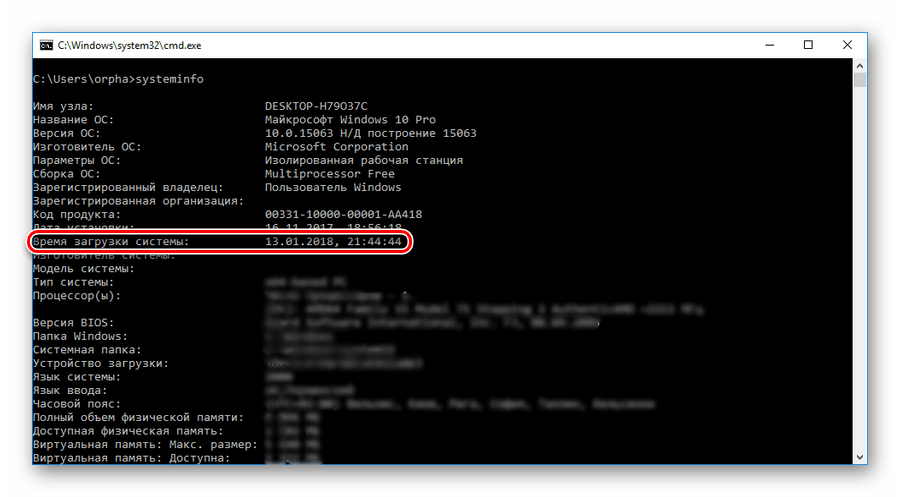
Способы узнать, когда включался компьютер

Существует несколько способов узнать, когда компьютер включался последний раз. Это можно сделать как средствами, предусмотренными в операционной системе, так и с помощью программного обеспечения сторонних производителей. Остановимся на них подробнее.

Способ 1: Командная строка

Этот способ является простейшим из всех и не потребует от пользователя каких-либо особых ухищрений. Все делается в два шага:

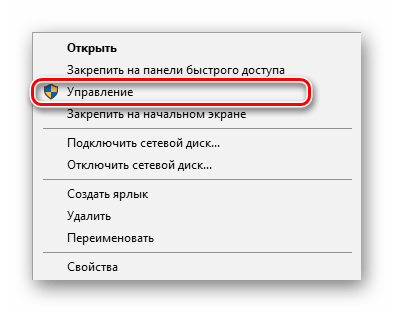
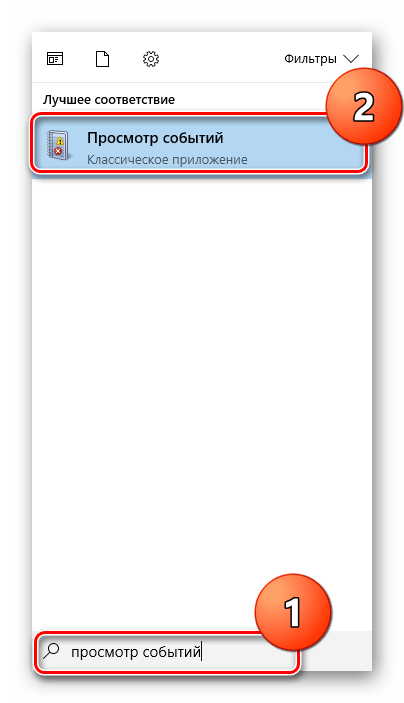
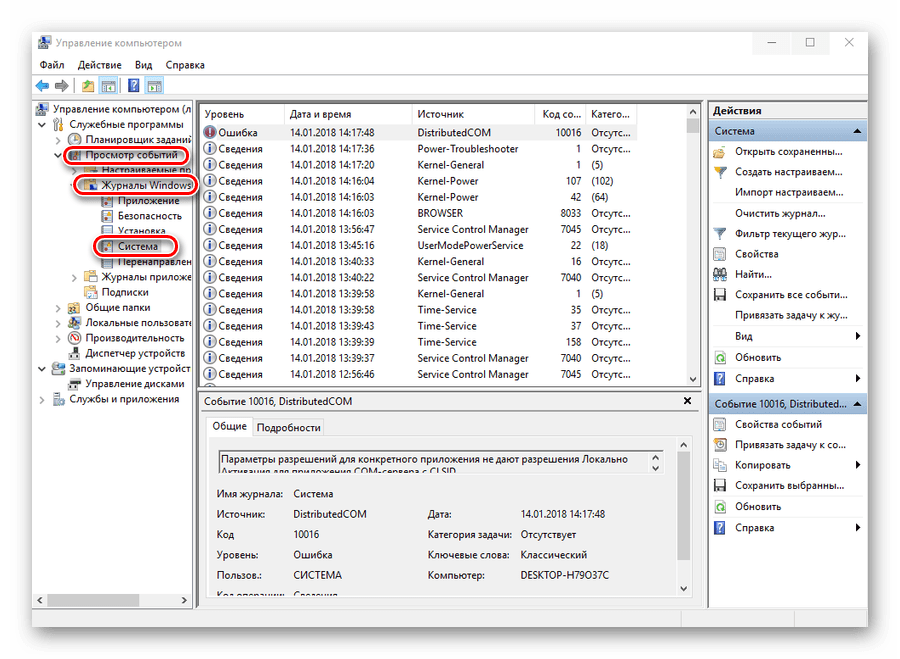
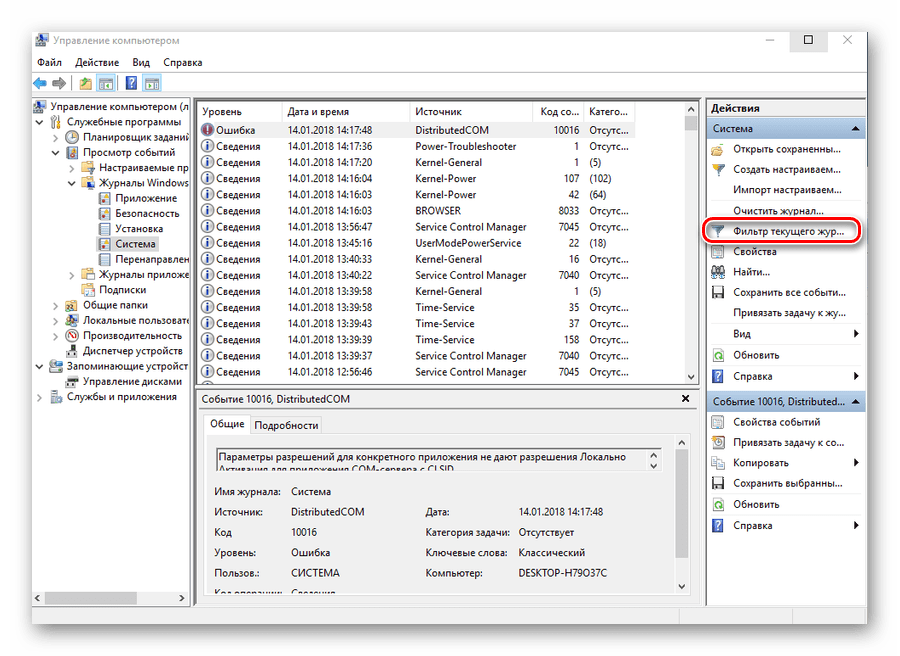
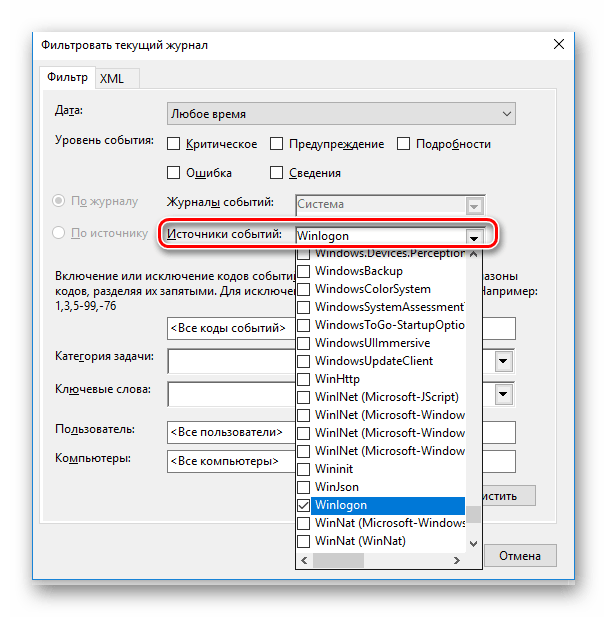
1. Открыть командную строку любым удобным для пользователя способом, например, вызвав с помощью комбинации **«Win+R»** окно запуска программ и введя там команду cmd.  
   
2. Ввести в строке команду systeminfo.  
   

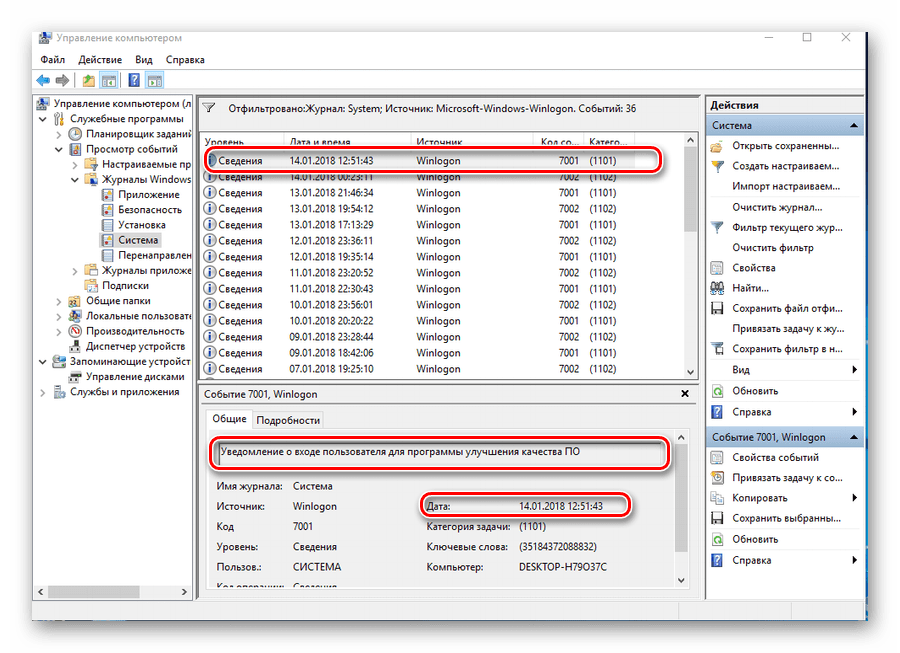
Результатом выполнения команды будет вывод на экран полной и информации о системе. Для получения интересующих нас сведений следует обратить внимание на строку **«Время загрузки системы»**.  
  
Сведения, содержащиеся в ней, и будут временем последнего включения компьютера, не считая текущей сессии. Сопоставив их с временем своей работы за ПК, пользователь легко сможет определить, включал ли его кто-нибудь посторонний, или нет.

Пользователям, у которых установлена Windows 8 (8.1), или Windows 10, следует иметь в виду, что полученные таким образом данные отображают сведения о реальном включении компьютера, а не о выводе его из состояния гибернации. Поэтому для того чтобы получать неискаженную информацию, необходимо выключать его полностью через командную строку.

Способ 2: Журнал событий

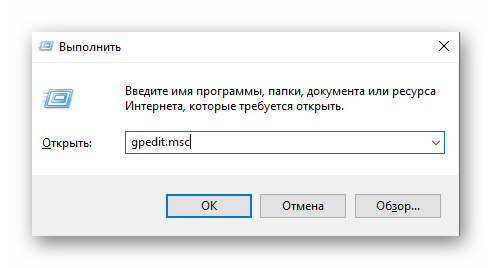
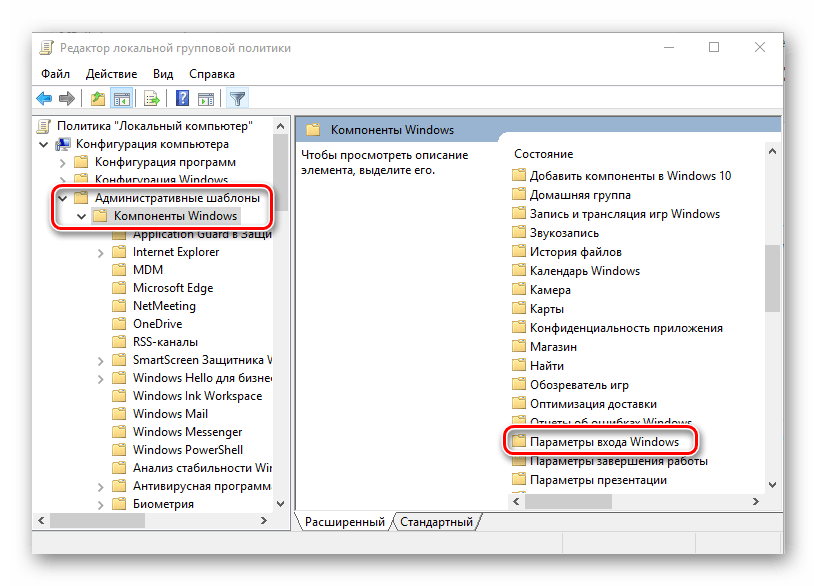
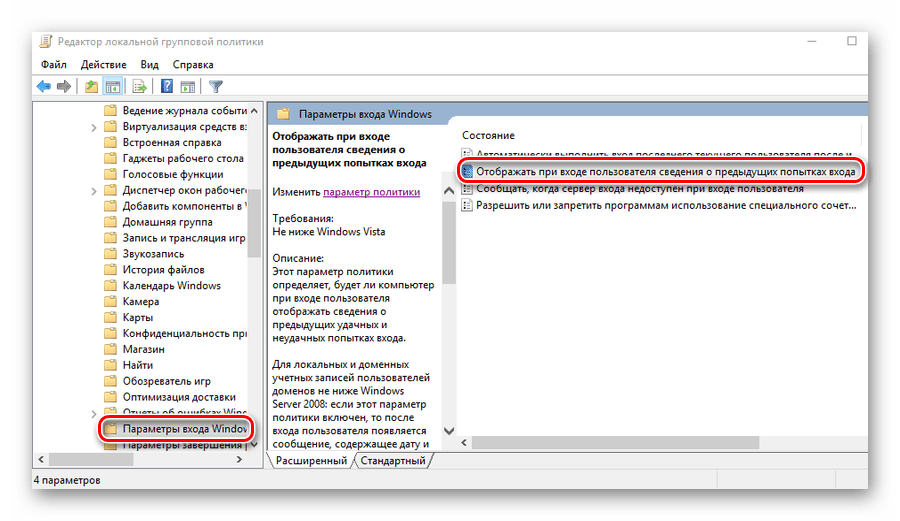
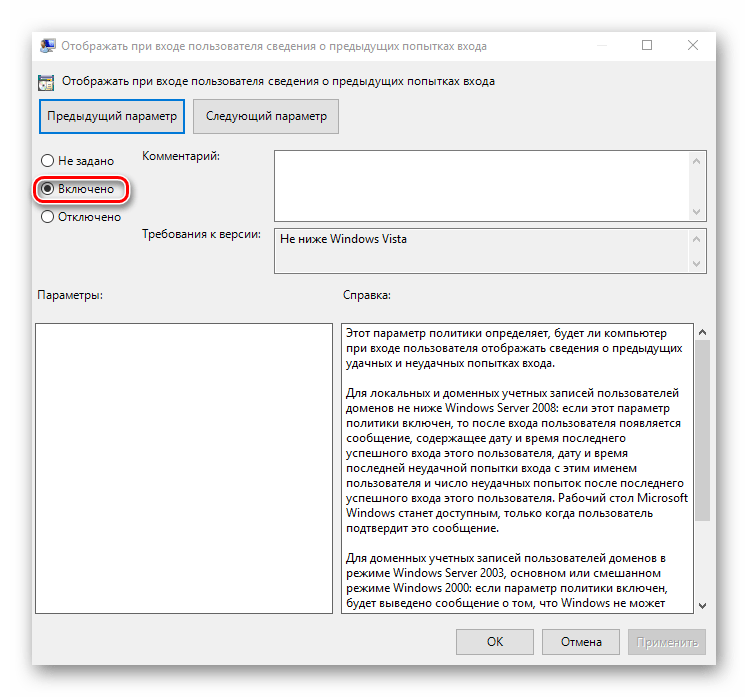
Узнать много интересного о том, что происходит в системе, можно из журнала событий, который ведется автоматически во всех версиях Windows. Чтобы попасть туда, необходимо сделать следующее:

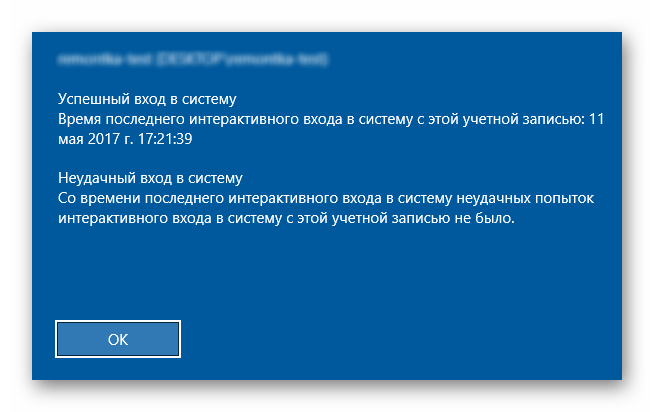
1. Правым кликом по иконке **«Мой компьютер»** открыть окно управления компьютером.  
     
   Тем пользователям, для кого способ появления на рабочем столе системных ярлыков остался тайной, или которые просто предпочитают чистый рабочий стол, можно воспользоваться строкой поиска Windows. Там нужно ввести фразу **«Просмотр событий»** и перейти по появившейся ссылке в результате поиска.  
   
2. В окне управления перейти к журналам Виндовс в **«Система»**.  
   
3. В окне справа перейти к настройкам фильтра, чтобы скрыть ненужную информацию.  
   
4. В настройках фильтра журнала событий в параметре **«Источник событий»** установить значение **«Winlogon»**.  
   

В результате произведенных действий в центральной части окна журнала событий появятся данные о времени всех входов и выходов из системы.  
  
Проанализировав эти данные, можно легко установить, включал ли компьютер кто-нибудь посторонний.

Способ 3: Локальные групповые политики

Возможность вывода сообщения о времени последнего включения компьютера предусмотрена в настройках групповых политик. Но по умолчанию этот параметр отключен. Чтобы задействовать его, нужно сделать следующее:

1. В строке запуска программ набрать команду gpedit.msc.  
   
2. После того как откроется редактор, последовательно открыть разделы так, как показано на скриншоте:  
   
3. Перейти к **«Отображать при входе пользователя сведения о предыдущих попытках входа»** и открыть двойным щелчком.  
   
4. Установить значение параметра в позицию **«Включено»**.  
   

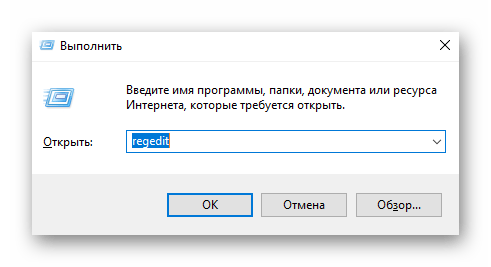
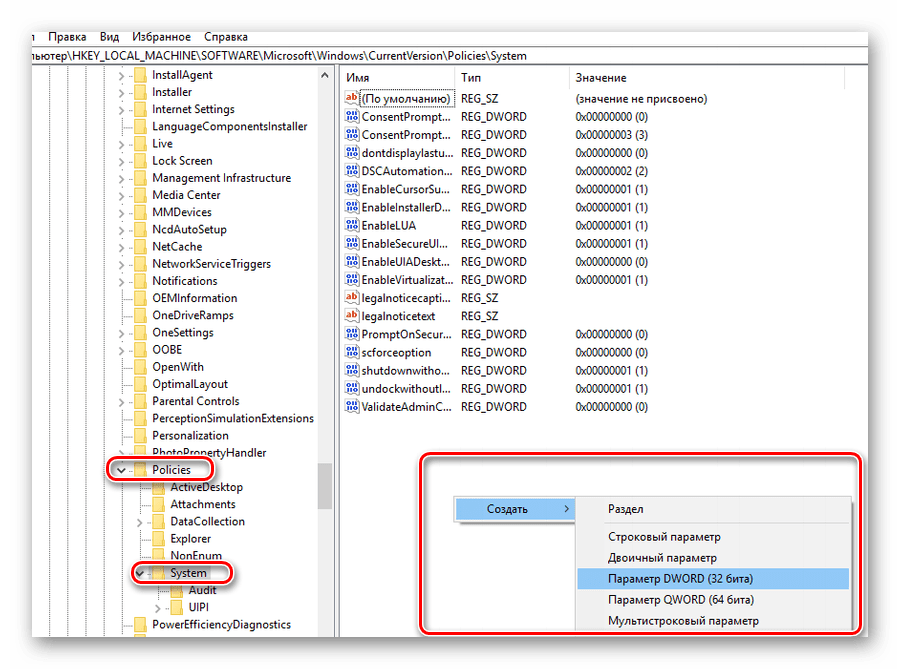
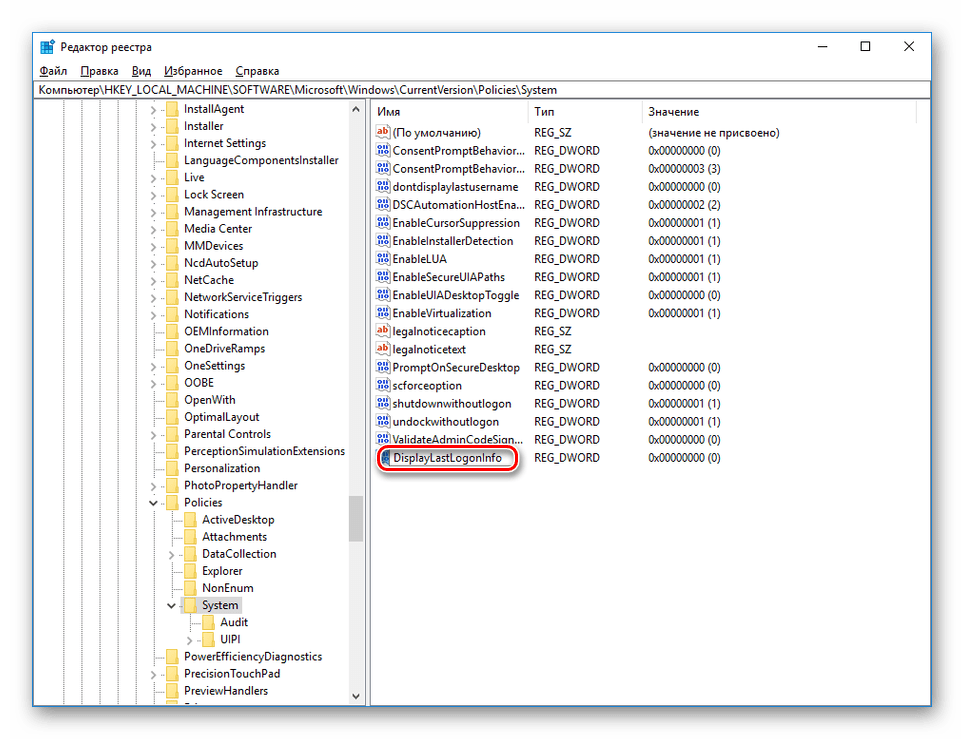
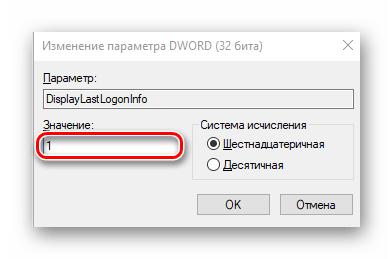
В результате произведенных настроек, при каждом включении компьютера будет отображаться сообщение такого типа:  
  
Плюсом данного метода является то, что кроме мониторинга успешного старта, будет выводиться информация о тех действиях по входу, которые закончились неудачей, что позволит узнать о том, что кто-то пытается подобрать пароль к учетной записи.

Редактор групповых политик присутствует только в полных версиях Windows 7, 8 (8.1), 10. В домашних базовых и Pro версиях настроить вывод сообщений о времени включения компьютера с помощью данного способа нельзя.

Способ 4: Реестр

В отличие от предыдущего, данный способ работает во всех редакциях операционных систем. Но при его использовании следует быть предельно внимательным, чтобы не допустить ошибку и случайно не испортить что-нибудь в системе.

Для того чтобы при запуске компьютера выводилось сообщение о его предыдущих включениях, необходимо:

1. Открыть реестр, введя в строке запуска программ команду regedit.  
   
2. Перейти к разделу  
   HKEY\_LOCAL\_MACHINE\ SOFTWARE\ Microsoft\ Windows\ CurrentVersion\ Policies\ System
3. С помощью правого клика мышкой по свободной области справа, создать новый 32-битный параметр DWORD.  
     
   Создавать нужно именно 32-битный параметр, даже если установлена 64-битная Windows.
4. Присвоить созданному элементу название **DisplayLastLogonInfo**.  
   
5. Открыть вновь созданный элемент и установить его значение равным единице.  
   

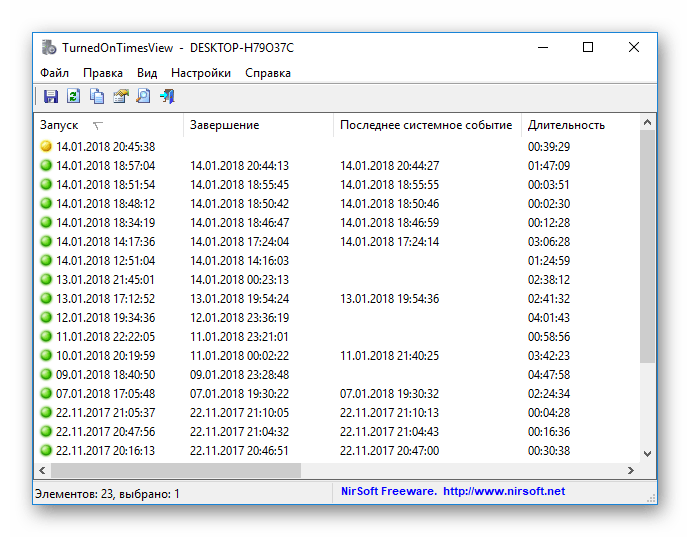
Теперь при каждом старте система будет выводить точно такое же сообщение о времени предыдущего включения компьютера, как и описанное в предыдущем способе.

Способ 5: TurnedOnTimesView

Пользователи, которые не хотят копаться в запутанных системных настройках с риском повредить систему, для получения информации о времени последнего включения компьютера могут воспользоваться утилитой стороннего разработчика TurnedOnTimesView. По своей сути она представляет собой очень упрощенный журнал событий, где отображаются только те из них, которые касаются включения/выключения и перезагрузки компьютера.

Утилита у вас в папке с заданием, установить на виртуальную машину.

(TurnedOnTimesView)

Утилита очень проста в использовании. Достаточно только распаковать скачанный архив и запустить исполняемый файл, как на экран будет выведена вся необходимая информация.  
  
По умолчанию русскоязычный интерфейс в утилите отсутствует, но на сайте производителя можно дополнительно скачать нужный языковой пакет. Программа распространяется абсолютно бесплатно.

Вот и все основные способы, с помощью которых можно узнать, когда компьютер включали в последний раз. Какой из них предпочтительнее — решать самому пользователю.