**ФГБОУ ВО НИУ «МЭИ»**

Институт Автоматики и Вычислительной Техники

**Защита данных**

Лабораторная работа №2

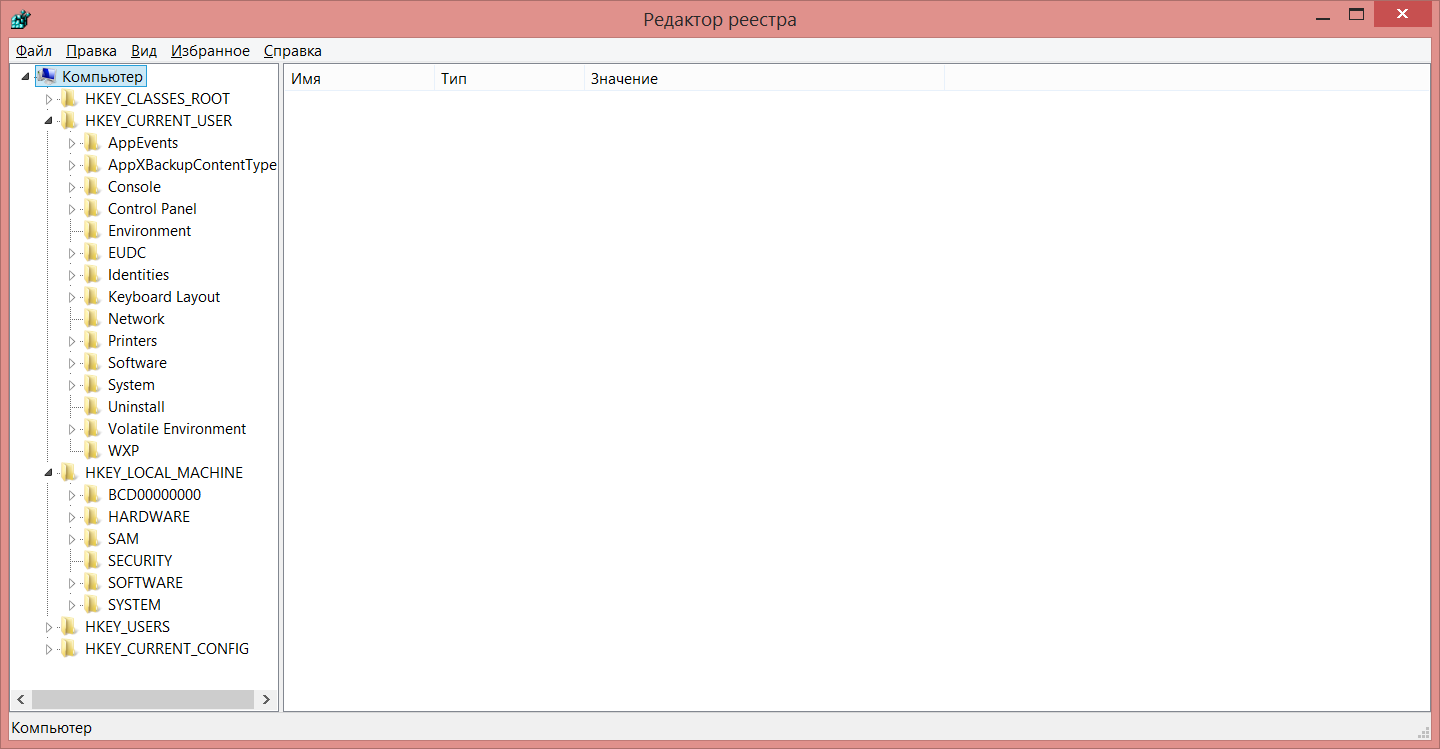
**Изучение программных средств защиты от несанкционированного доступа и разграничения прав пользователей**

**Выполнил:** Зиятдинов А.Б.

**Студент группы:** А-05-15

Москва 2018

1. Этот пункт выполняется в виртуальной машине Windows XP (если работа выполняется в компьютерном классе кафедры) или с правами администратора (если работа выполняется на домашнем компьютере). Запустить программу Редактор реестра Windows regedit.exe. Ознакомиться со структурой реестра.
   1. Включить в отчет, воспользовавшись, например, Справкой редактора реестра, краткие сведения о содержании основных разделов реестра (HKEY\_CURRENT\_USER и HKEY\_LOCAL\_MACHINE).
   2. Включить в электронную версию отчета копии экранных форм, иллюстрирующих использование редактора реестра (рисунок с изображением активной формы помещается в буфер обмена с помощью комбинации клавиш Alt+Print Screen).



1. Пункт выполняются в виртуальной машине Windows XP или с правами администратора. Запустить программу Редактор локальной групповой политики gpedit.msc, позволяющую ограничить возможности пользователей ОС Windows.
   1. Включить в отчет сведения о назначении и основных функциях программы.

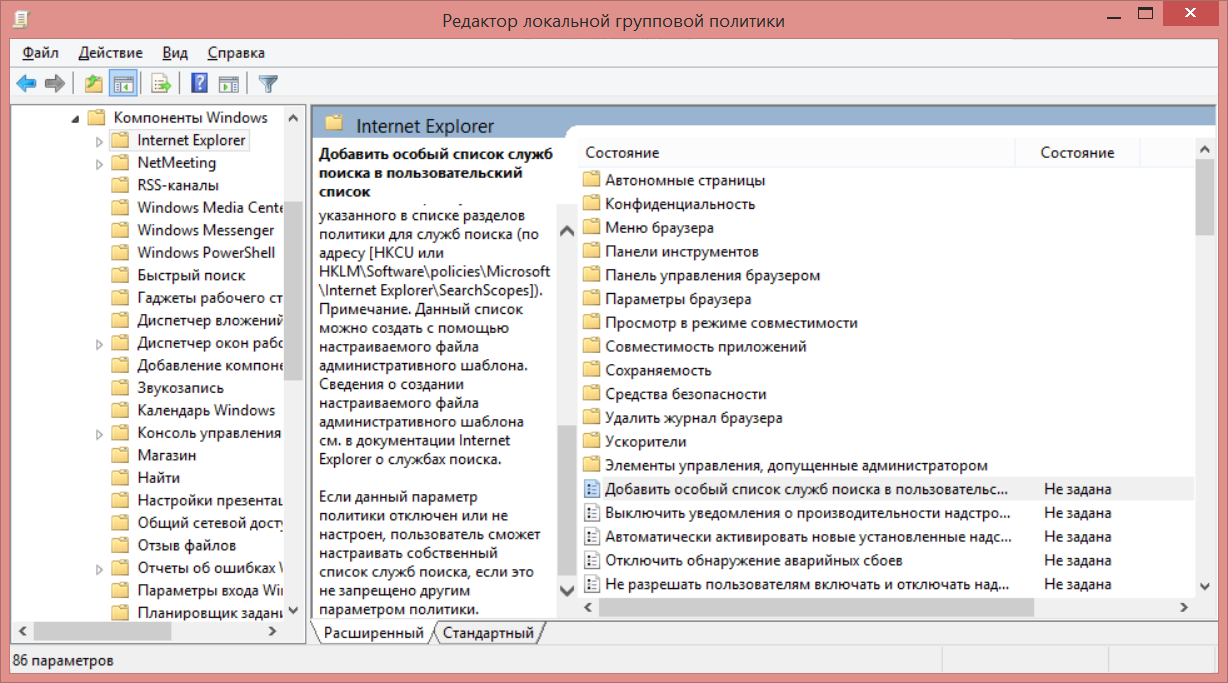
Редактор локальной групповой политики является специальной встроенной утилитой, которая позволяет управлять системой, администрировать и настраивать её, исходя из своих задач и потребностей.

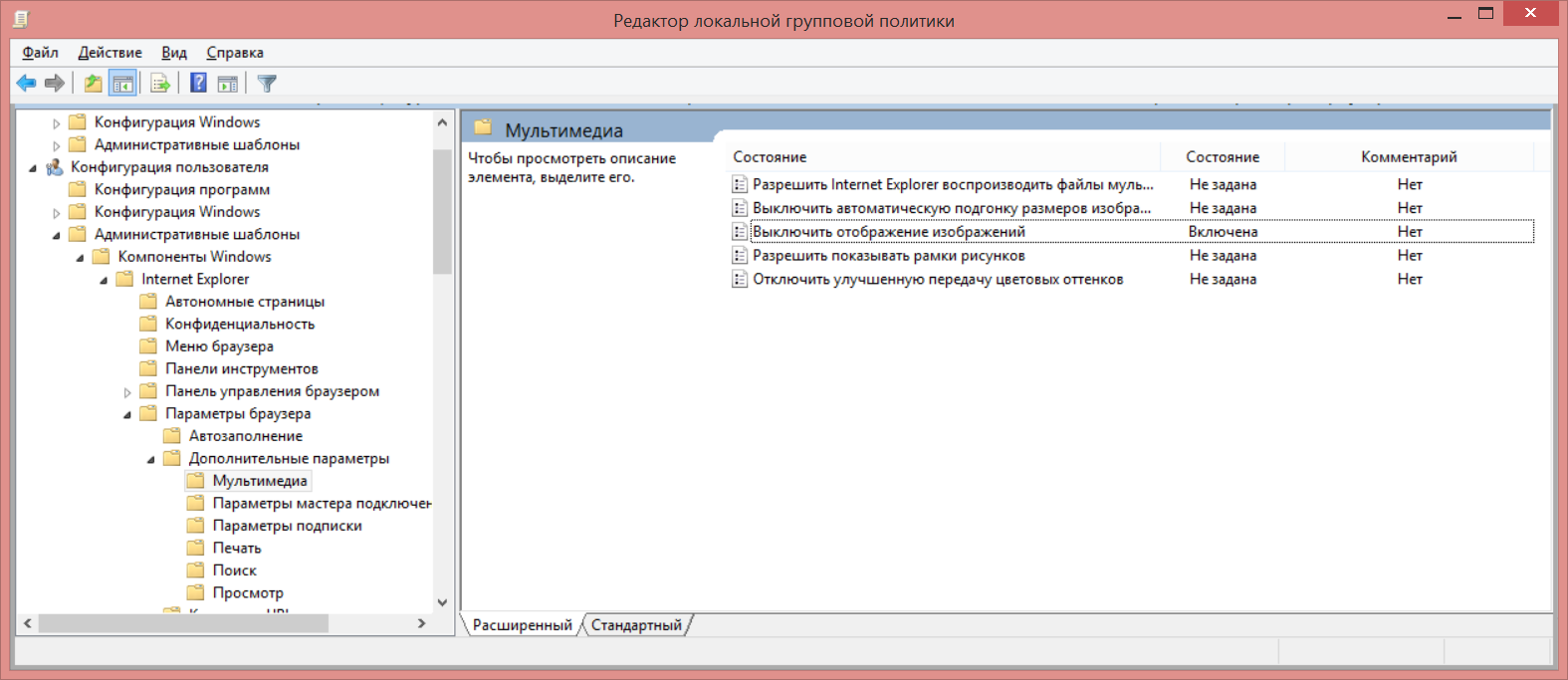
К основным функциям можно отнести:

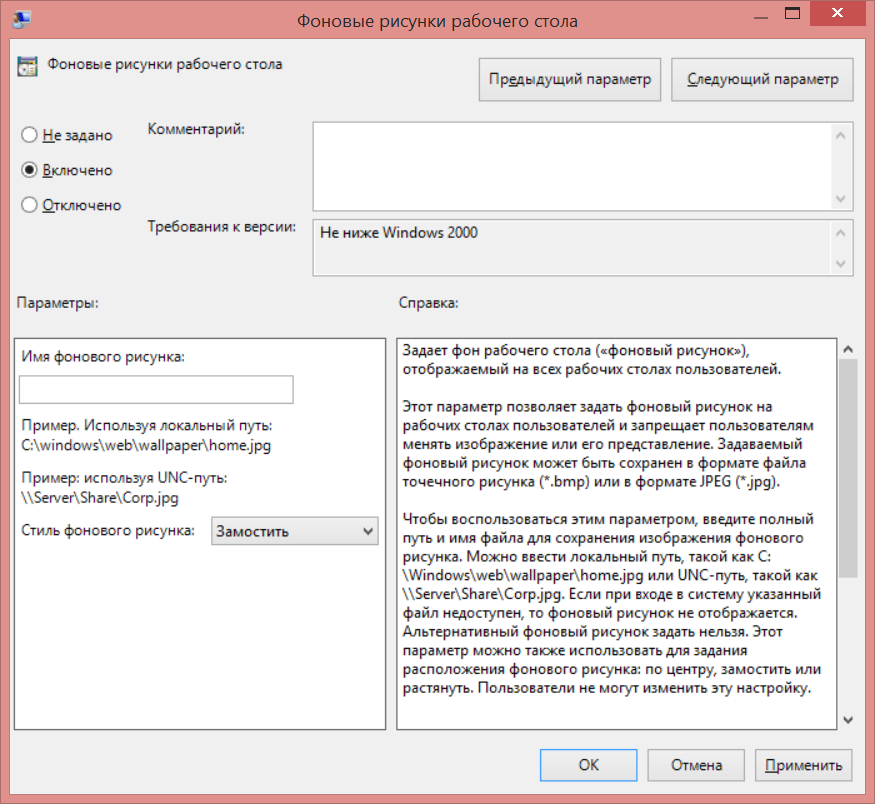
* заблокировать (или, наоборот, разрешить) пользователям доступ к определенным приложениям, к их настройкам;
* блокировать доступ к панели управления, скрыть некоторые её элементы; запретить доступ к устройствам (например, к картам памяти, внешним накопителям);
* изменить назначение комбинациям клавиш и др.  
  1. Освоить управление настройками обозревателя Internet Explorer для пользователя (узел Политика «Локальный компьютер» | Конфигурация пользователя | Административные шаблоны | Компоненты Windows | Internet Explorer).
  2. Освоить установку ограничений возможностей пользователя (узлы группы Политика «Локальный компьютер» | Конфигурация пользователя | Административные шаблоны) по изменению структуры Рабочего стола и Главного меню, использованию функций Панели управления и компонент Windows (Проводника, консоли управления Microsoft, планировщика задач, проигрывателя Windows Media и др.), работе с локальной сетью, использованию общих папок, использованию различных системных функций.
  3. Включить в отчет, воспользовавшись, например, Справкой Редактора локальной групповой политики, ответ на вопрос, чем отличаются значения параметров «отключен» и «не задан».

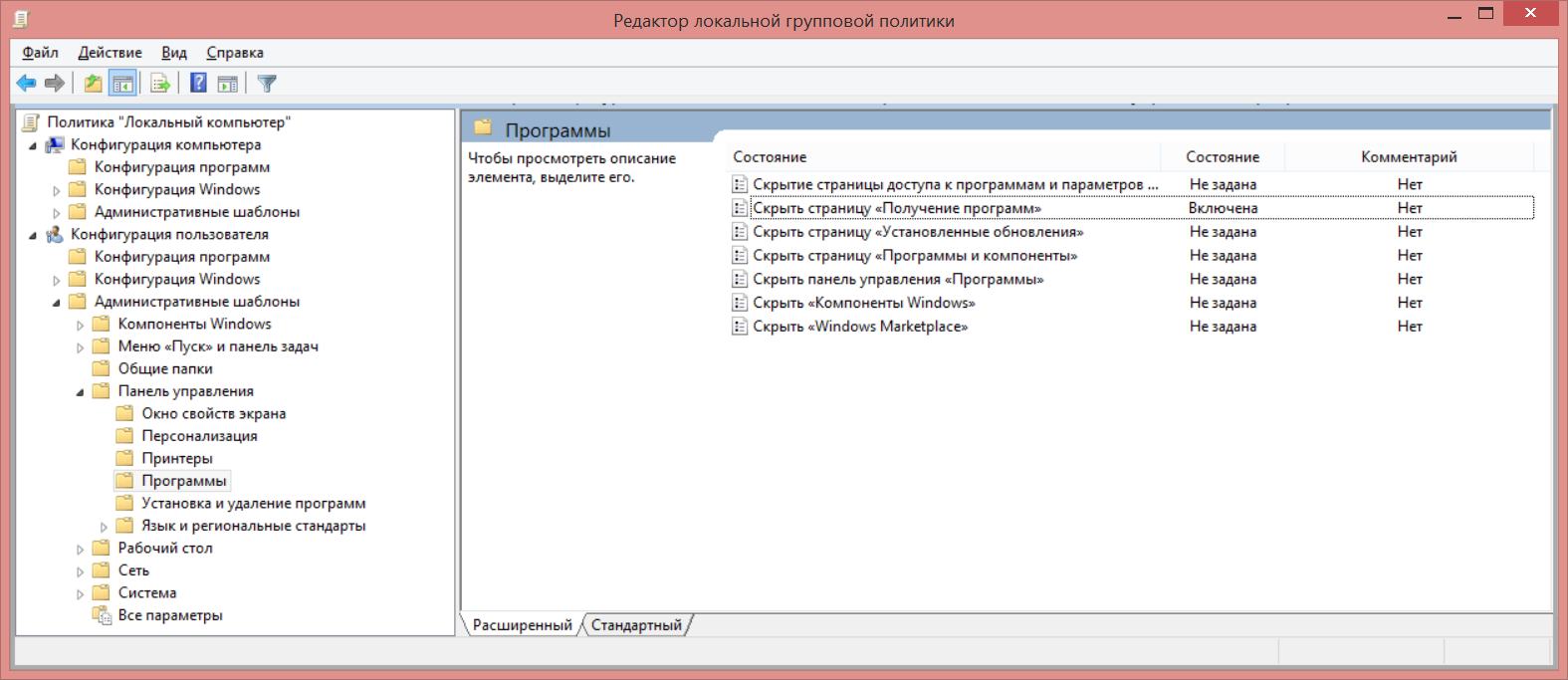
У всех параметров политики административных шаблонов может быть только одно из трех возможных состояний: «Не задано», «Включить» и «Отключить».

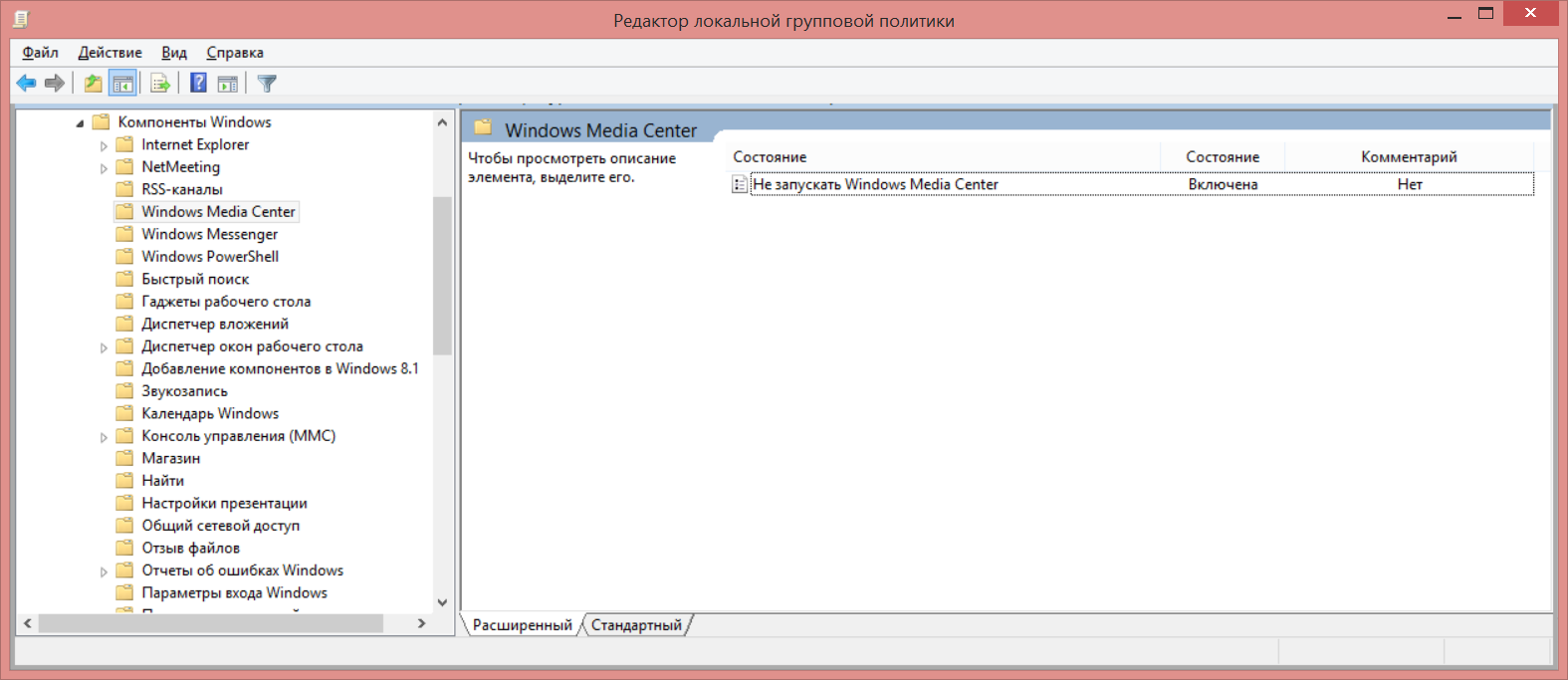
* «Не задано» - это состояние, которое применяется по умолчанию для всех параметров политики. Параметры политики в состоянии «Не задано» не влияют на пользователей или компьютеры. Включение параметра политики административных шаблонов задействует параметр политики;
* «Включить» - это состояние, которое указывает на то, что действие, применяемое в данном параметре политики должно применяться к компьютеру или пользователю;
* «Отключить» - это состояние, которое указывает на то, что действие, применяемое в данном параметре политики не должно применяться к компьютеру или пользователю.
  1. Включить в электронную версию отчета копии экранных форм, используемых при работе с программой gpedit.msc. Завершить работу с программой gpedit.msc.

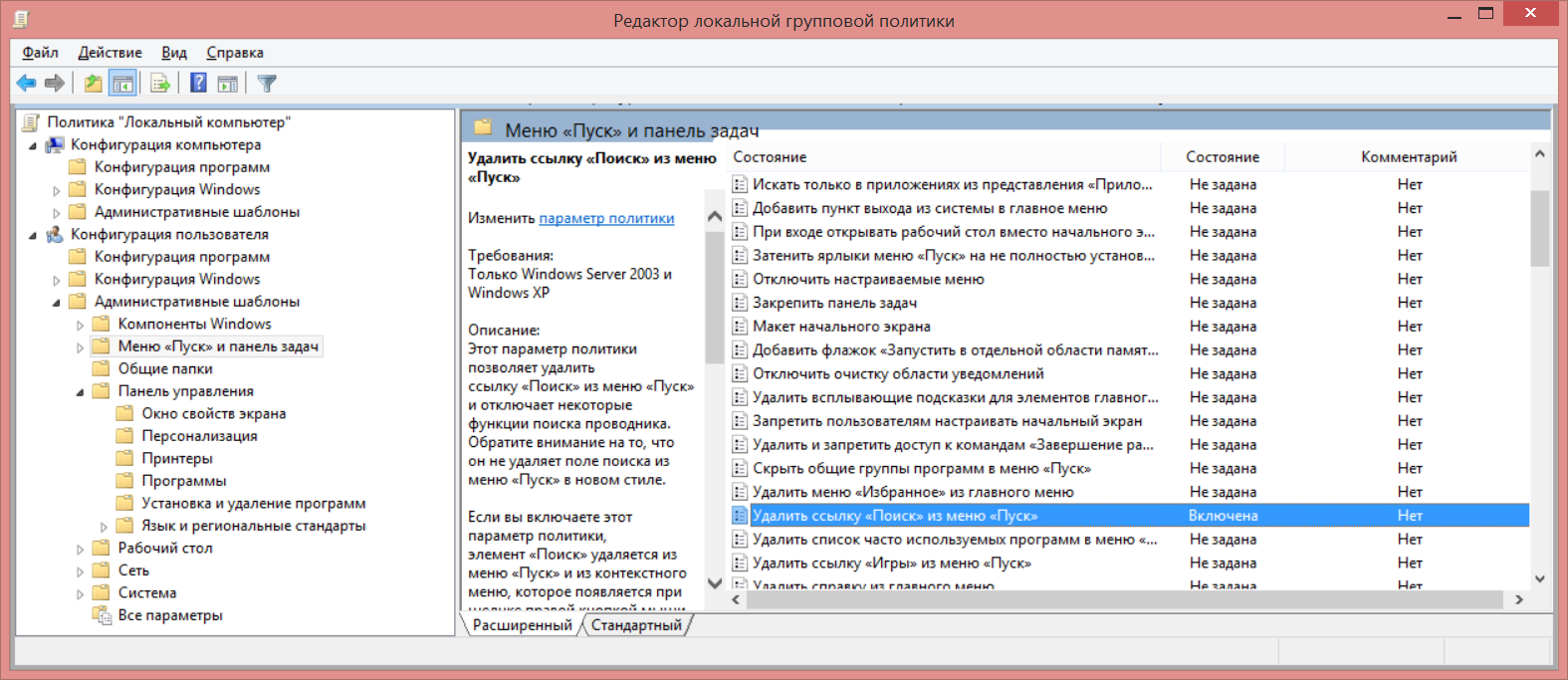












1. Пункт выполняется на компьютере с профессиональной версией Windows. С помощью процесса входа Winlogon, активизируемого комбинацией клавиш Ctrl+Alt+Del, заблокировать работу с используемой рабочей станцией на период временного отсутствия пользователя (если эта возможность не запрещена администратором). Разблокировать работу рабочей станции.
   1. Включить в отчет сведения о порядке защиты рабочей станции на период временного отсутствия пользователя и о других функциях Процесса входа, доступных при этом наряду с блокировкой.

На период временного отсутствия пользователя необходимо блокировать рабочую станцию с целью обеспечения защиты от несанкционированного доступа к информации. Данное действие может выполнять пользователь комбинацией клавиш Ctrl+Alt+Del. Так же можно настроить блокировку консолей рабочих станций пользователей при наступлении некоторого периода бездействия. Например, в качестве обязательного требования для большинства категорий пользователей может выставляться блокировка рабочего стола компьютера при отсутствии пользовательской активности более 10 минут.

Помимо блокировки компьютера можно воспользоваться следующими функциями:

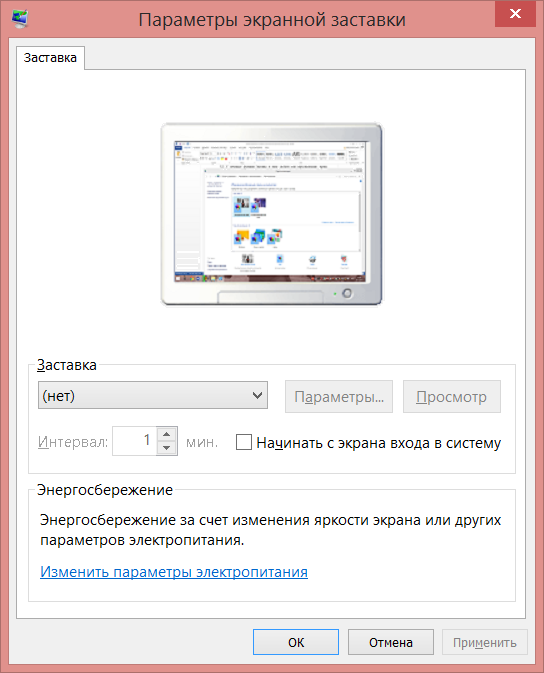
 **Сменить пользователя** – с помощью данного пункта вы сможете быстро сменить пользователя (учётную запись пользователя в Windows);

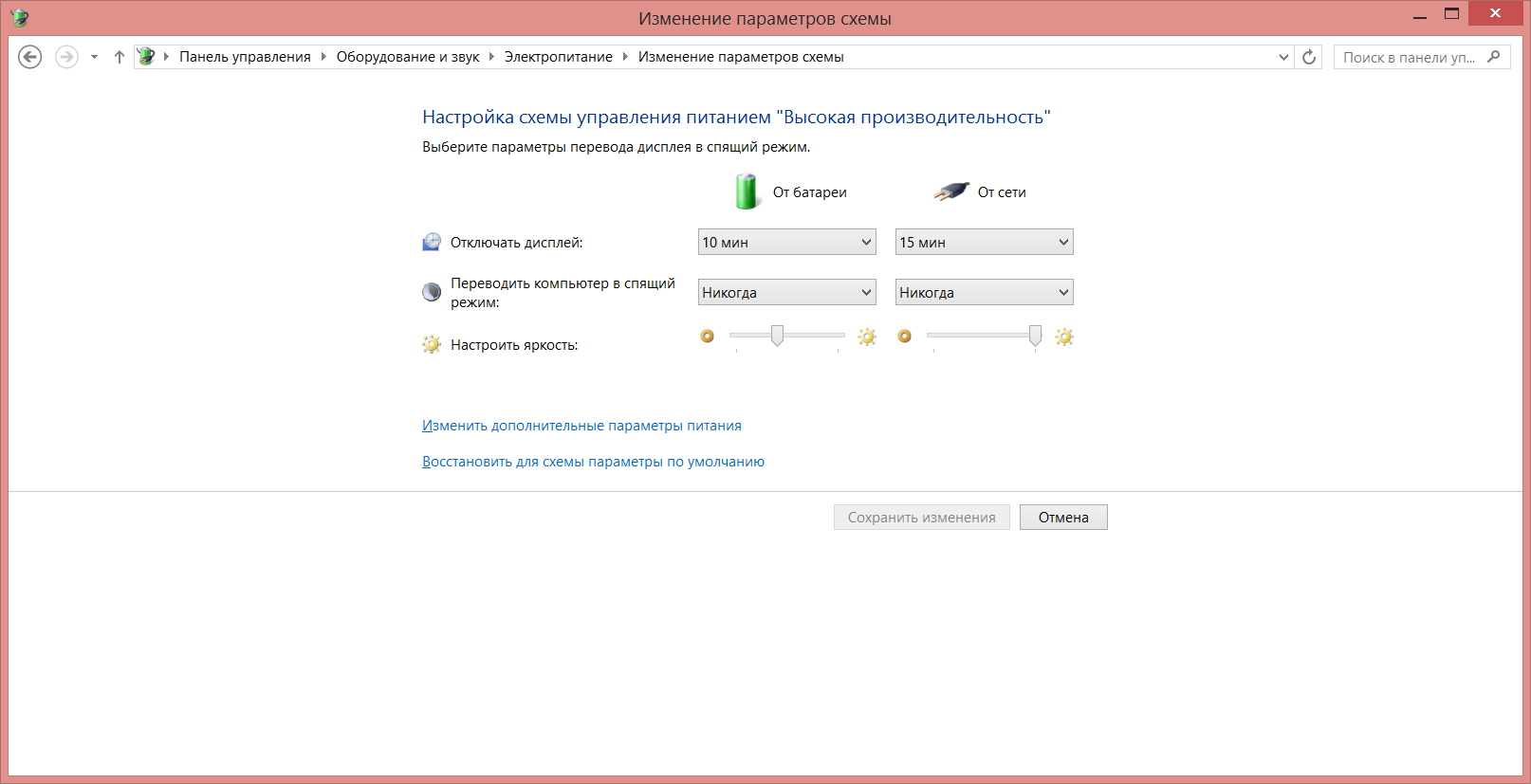
 **Выйти** – этот пункт позволяет быстро осуществить выход текущего пользователя из системы (из текущей загруженной учётной записи Windows с сохранением всех параметров работы);

 **Изменить пароль** – этот пункт позволяет быстро изменить ранее установленный пароль у текущего пользователя;

 **Диспетчер задач** – этот пункт позволяет быстро открыть диспетчер задач.

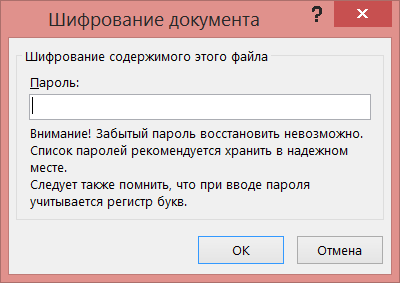
* 1. С помощью функции Заставка в окне свойств или персонализации экрана, вызываемого из его контекстного меню, ознакомиться с другой возможностью блокировки компьютера на период временного отсутствия пользователя. Отразить полученные сведения в отчете. Включить в электронную версию отчета копии экранных форм, полученных при выполнении этого пункта.

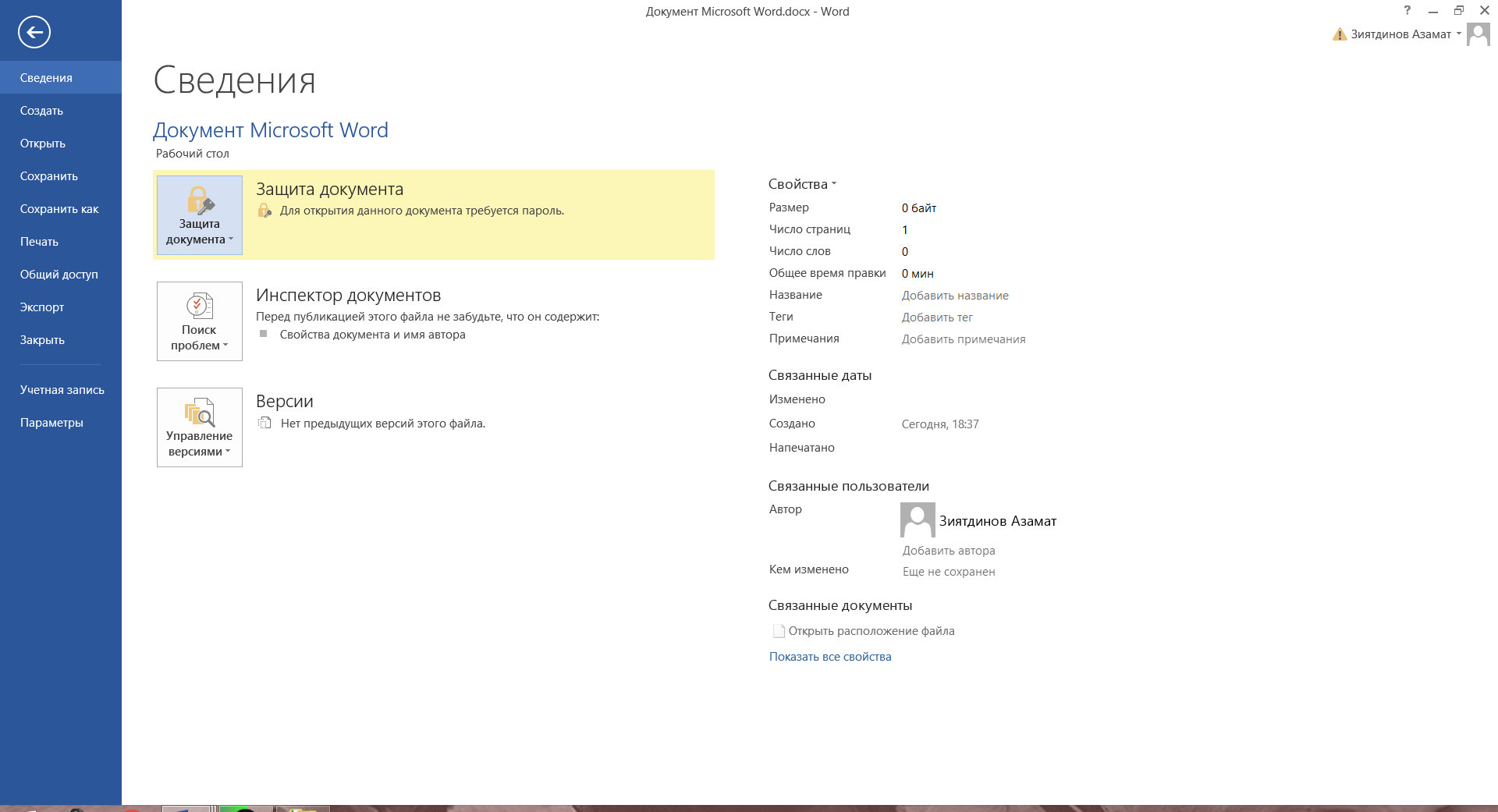


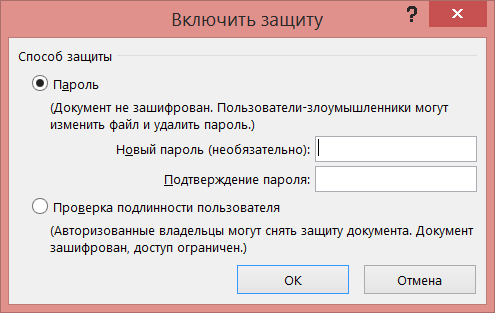


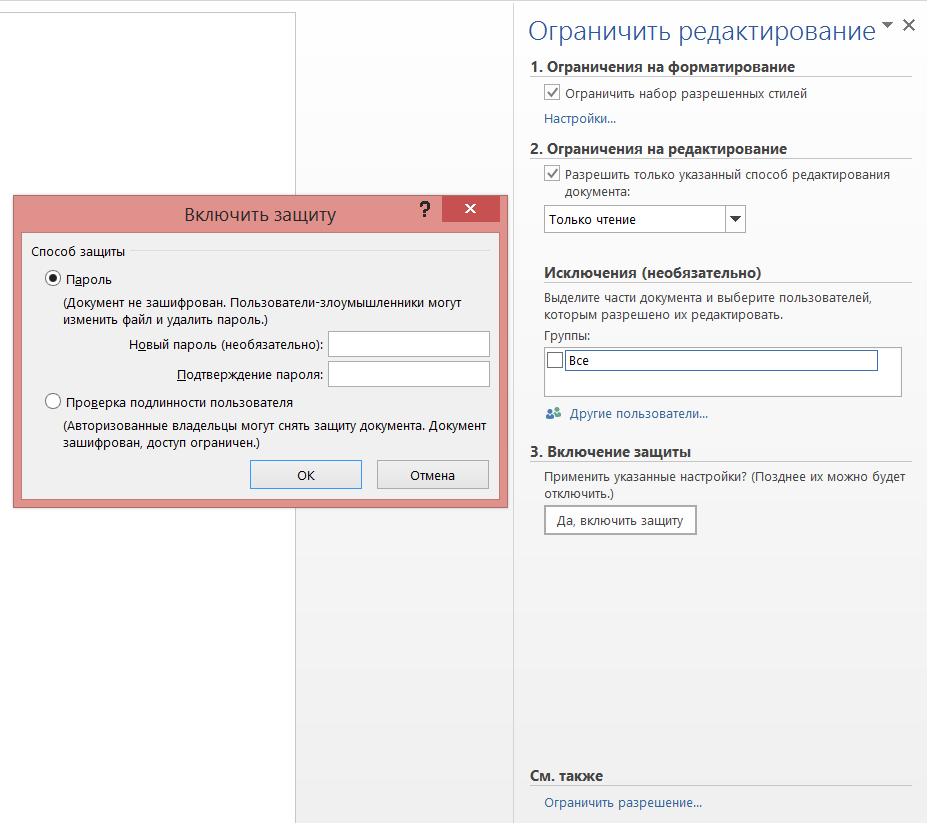
Здесь можно задать интервал неактивности, через который компьютер автоматически переходит в спящий режим. А когда он переходит в спящий режим – он блокируется.

1. Открыть (или создать) произвольный документ в текстовом процессоре Word.
   1. Изучить порядок использования паролей для защиты документов в Microsoft Word от чтения и записи (два разных типа паролей) и включить в отчет соответствующие сведения (в Office 2013 использовать команду Файл | Сведения | Защита документа, в Office 2010 использовать команду Файл | Сведения | Защитить документ, в Office 2007 – Кнопка Microsoft Office | Подготовить и Рецензирование | Защитить документ, в Office 2003 – Сервис | Параметры | Безопасность).
   2. Включить в электронную версию отчета копии экранных форм, использованных при выполнении данного пункта. Завершить работу с Word.





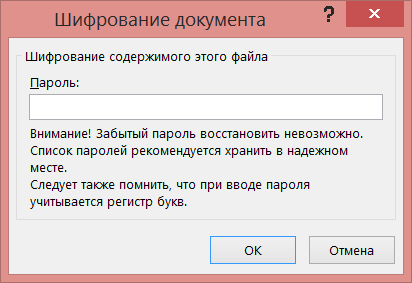




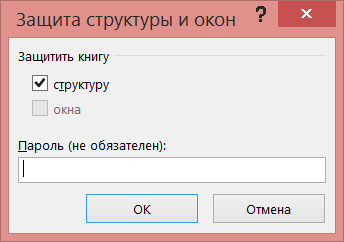
1. Открыть (или создать) произвольную таблицу Excel.
   1. Изучить порядок использования паролей для защиты документов или их частей в табличном процессоре Microsoft Excel от чтения и записи и включить в отчет соответствующие сведения.

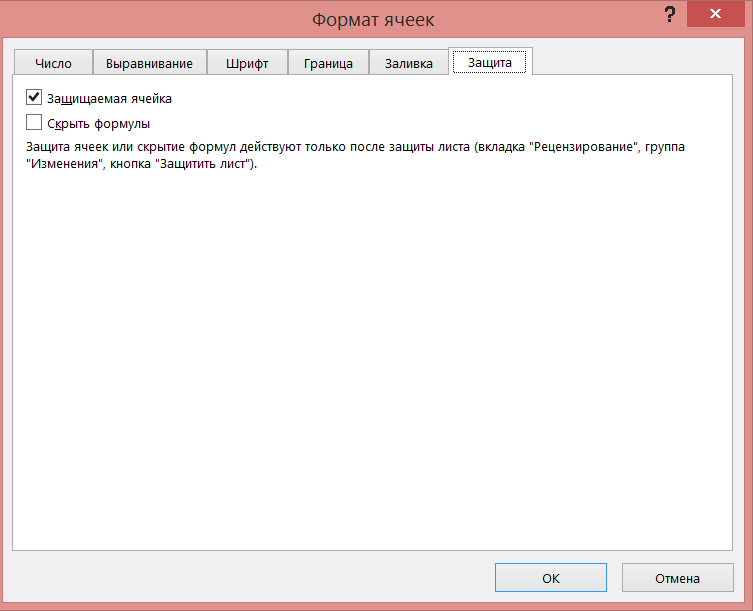
В Microsoft Excel предусмотрено несколько уровней защиты, позволяющих управлять доступом к данным Microsoft Excel и их изменением. Можно ограничить доступ к книге (файлу), например, несанкционированное открытие. Можно применить защиту к элементам книги, ограничив просмотр отдельных листов и/или изменение данных на листе. Можно защитить элементы листа, например, ячейки с формулами, запретив доступ к ним всем пользователям.

* 1. Включить в электронную версию отчета копии экранных форм, использованных при выполнении данного пункта. Завершить работу с Excel.







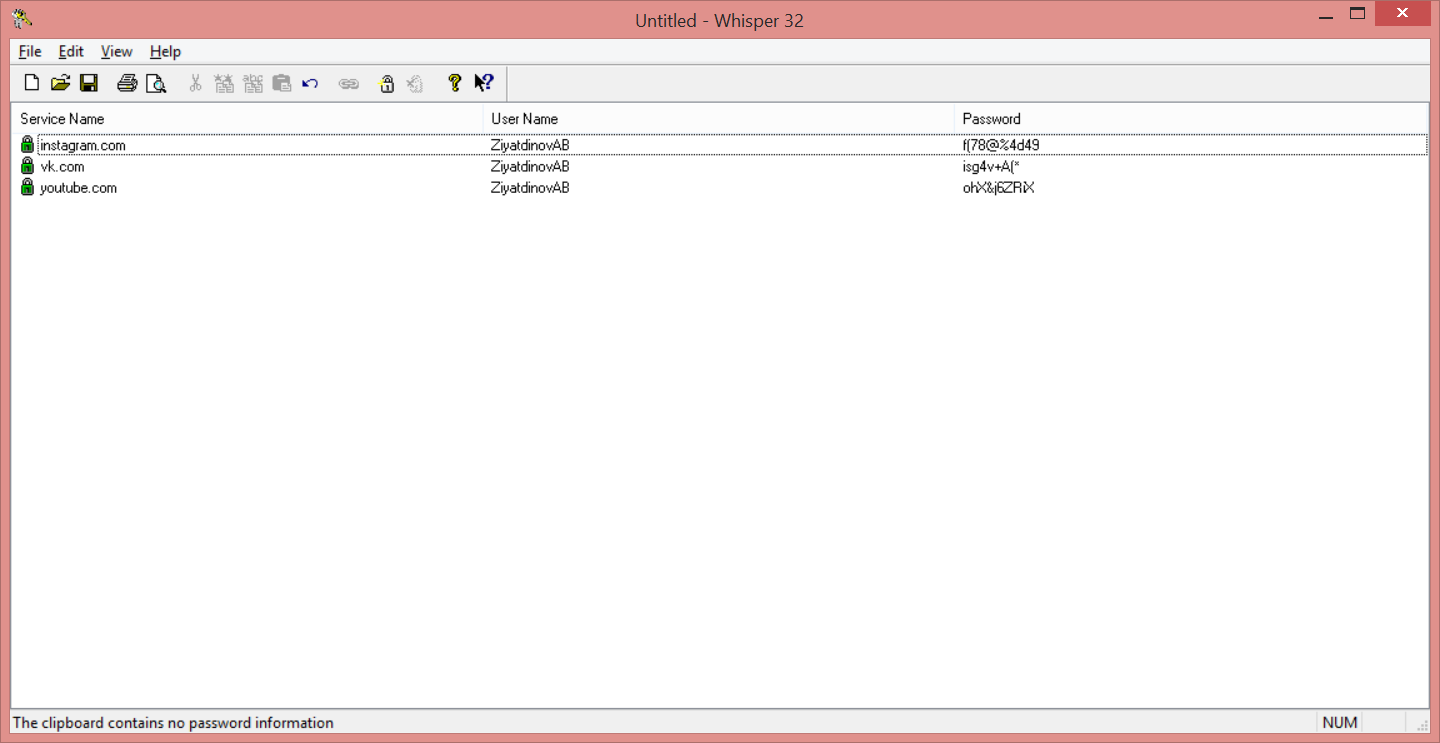


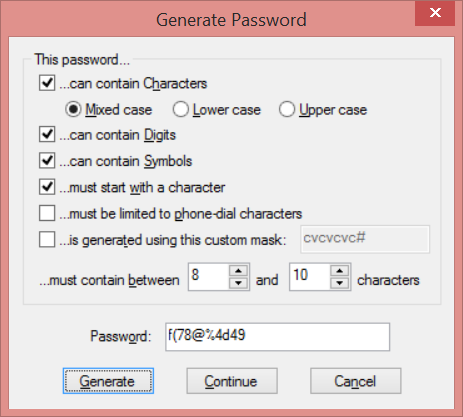
1. Пункты 6-8 выполняются в виртуальной машине Windows XP или с правами администратора. Скопировать в личную папку на локальном жестком диске файл whisper.msi.
2. Если программа Whisper 32 не установлена (соответствующий пункт отсутствует в главном меню), то установить ее с помощью файла whisper.msi.
3. Запустить программу whisper.exe, предназначенную для создания и ведения базы данных паролей пользователя.
   1. Изучить назначение и основные функции программы и включить в отчет соответствующие сведения.

Whisper 32 - программа, предназначенная для создания и ведения базы данных паролей пользователя. Хранит все имена пользователей и пароли в одном защищенном паролем файле. Вы можете распечатать список или скопировать его в буфер обмена.

Есть возможность программного генерирования паролей. В форме генератора паролей нужно указать используемые символы и длину пароля. Так же есть возможность указания срока действия пароля. По истечении этого периода программа выдаст сообщение об изменения пароля. Данная возможность обеспечивает дополнительную безопасность от несанкционированного доступа к личному кабинету на сайтах.

* 1. Создать 2-3 записи о паролях к различным ресурсам (записи обязательно должны содержать фамилию и инициалы студента в полях имени учетной записи или комментария).
  2. Включить в электронную версию отчета копии экранных форм, использованных при выполнении данного пункта. Завершить работу с программой whisper.exe.





1. Ознакомиться (на примере папок c: \ Пользователи \ *Имя пользователя* \ Мои документы \ *Папка с фамилией студента* и c: \ Пользователи \ Общие\ Общие документы или, при работе в Windows XP Professional, c:\ Documents and Settings \ *Имя пользователя* \ Документы \ *Папка с фамилией студента* и c:\ Documents and Settings \ All Users \ Документы) с порядком разграничения доступа к ресурсам воперационной системе Windows (с помощью команды Свойства | Безопасность контекстного меню объекта и элементов управления соответствующих диалоговых окон). Если команда Безопасность недоступна (при работе в ОС Windows XP Professional), то выключить режим «Использовать простой общий доступ к файлам» на вкладке «Вид» окна свойств папки.
   1. Включить в отчет сведения об особенностях управления доступом к папкам и файлам (родовых (generic, общих) правах доступа, полном наборе специальных и стандартных прав доступа, владельце объекта, действующих разрешениях на доступ к объекту для конкретного субъекта). Для выполнения этого задания обязательно открыть все вкладки окна дополнительных параметров безопасности папки.

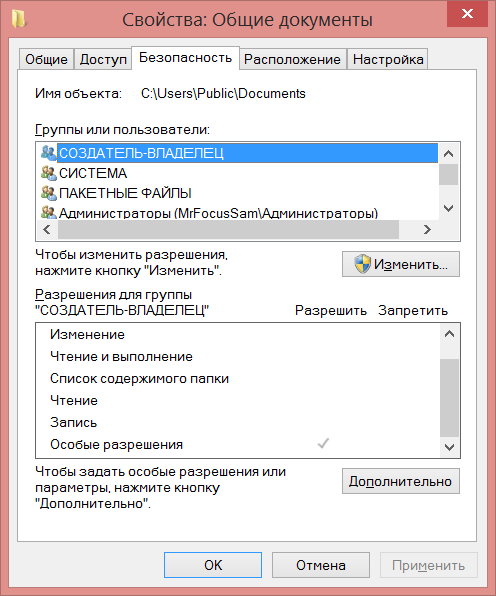
Различаются специальные, стандартные и общие (generic) права доступа к объектам.

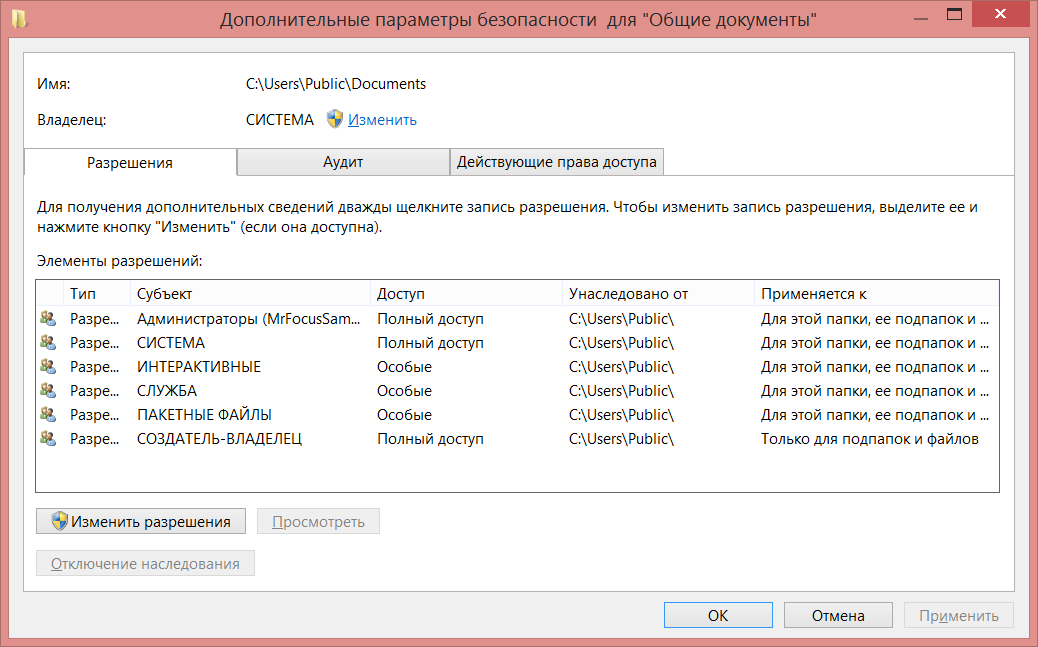
* Специальные права определяют возможность обращения к объекту по свойственному только данной категории объектов методу – обзор папок/выполнение файлов, содержание папки/чтение данных, чтение атрибутов, чтение дополнительных атрибутов, создание файлов/запись данных, создание папок/добавление данных, запись атрибутов, запись дополнительных атрибутов, удаление подпапок и файлов.
* Стандартные права определяют возможность доступа к объекту по методу, применимому к любому объекту – удалить, чтение разрешений, смена разрешений, смена владельца
* Общие права представляют собой комбинацию специальных и стандартных прав, и предоставляет возможность обращения к объекту с помощью некоторого набора методов доступа. Примеры общих прав доступа:
* Чтение (чтение DACL, чтение данных, чтение атрибутов и расширенных атрибутов, использование объекта для синхронизации);
* Запись (чтение DACL, запись и добавление данных, запись атрибутов и расширенных атрибутов, использование объекта для синхронизации).

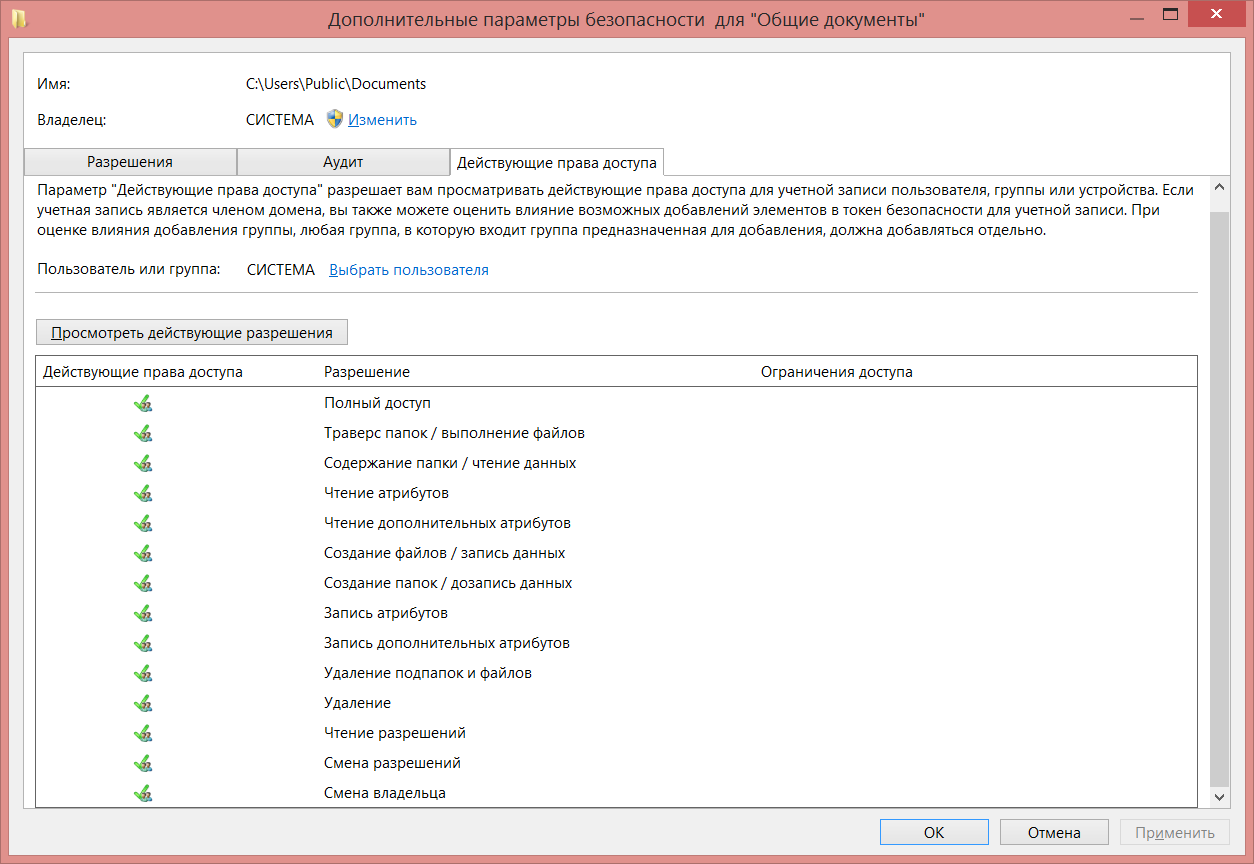
Владелец имеет право на чтение и изменение разрешений. И даже явно указанный запрет для учетной записи не имеет приоритета над правами владельца.

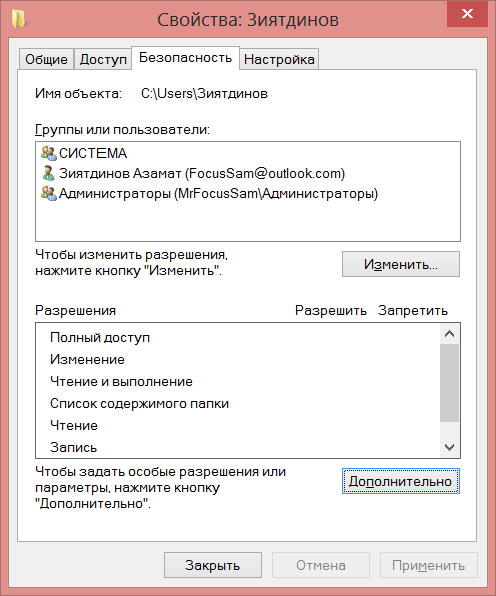
Каждый объект имеет набор связанных с ним действующих разрешений. Вкладка *Действующие разрешения* содержит список разрешений, которые будут даны выбранной группе или пользователю только на основании членства в группах.

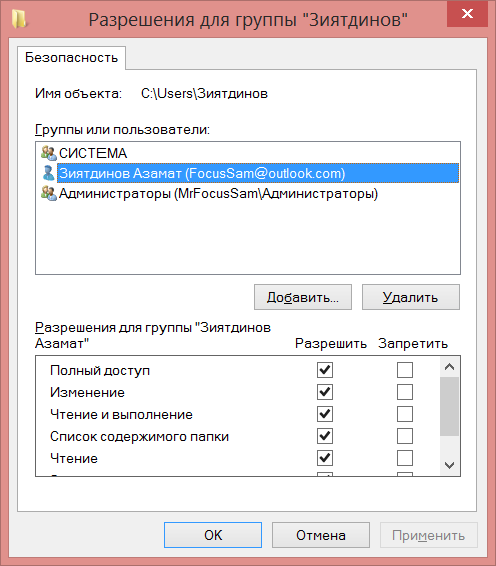
* 1. Включить в электронную версию отчета копии экранных форм, использованных при выполнении данного пункта.

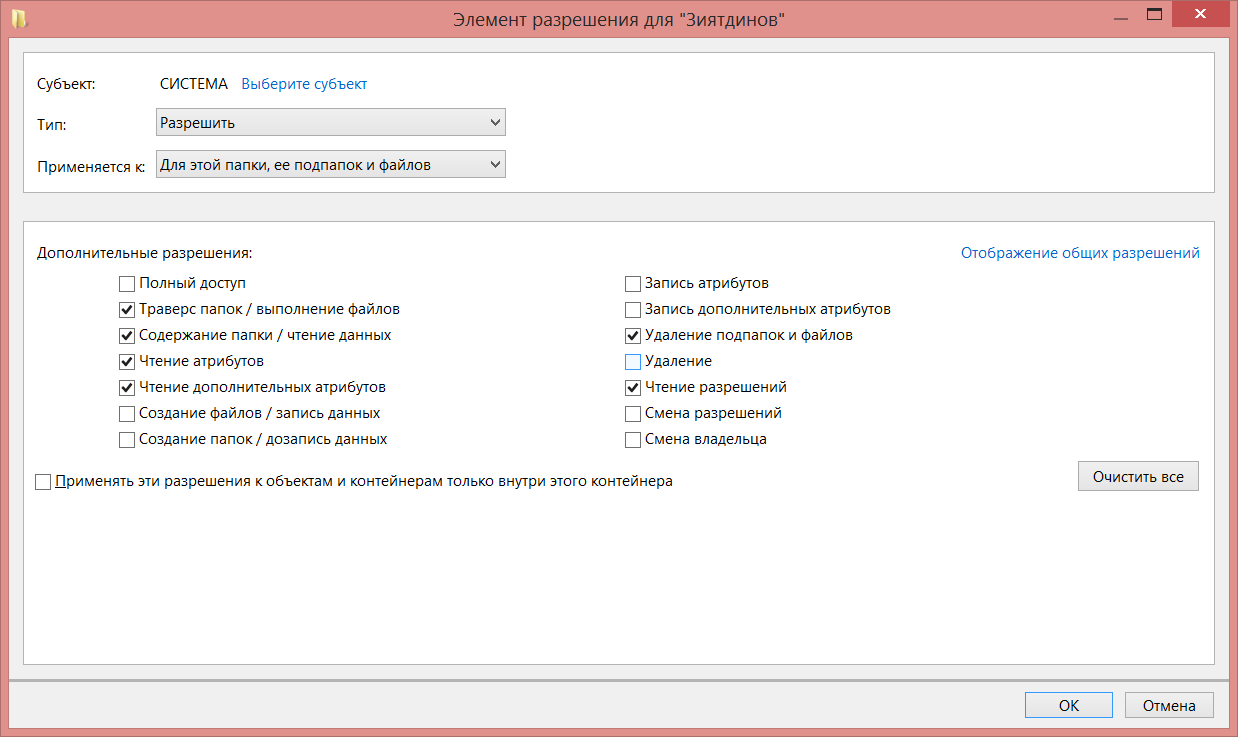












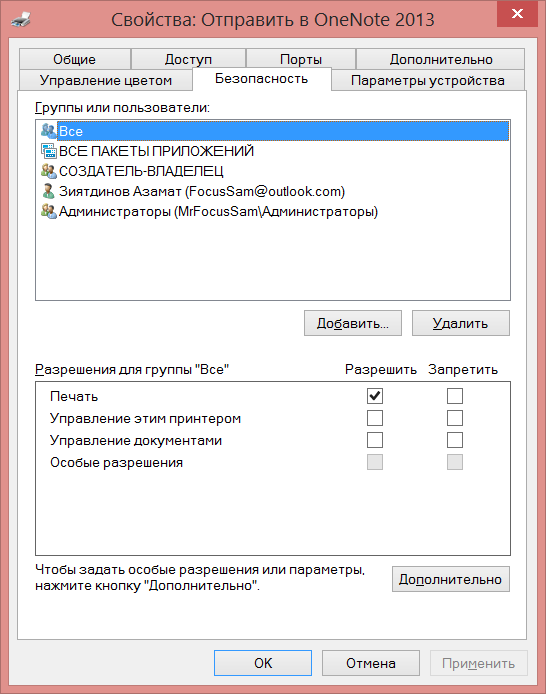
1. Ознакомиться с порядком разграничения доступа к принтерам (с помощью Панели управления Windows | Устройства и принтеры | Свойства принтера).
   1. Включить в отчет сведения об особенностях управления доступом к принтерам (родовых правах доступа, полном наборе специальных и стандартных прав доступа, владельце объекта, действующих разрешениях на доступ к объекту для конкретного субъекта). Для выполнения этого задания обязательно открыть все вкладки окна дополнительных параметров безопасности объекта.

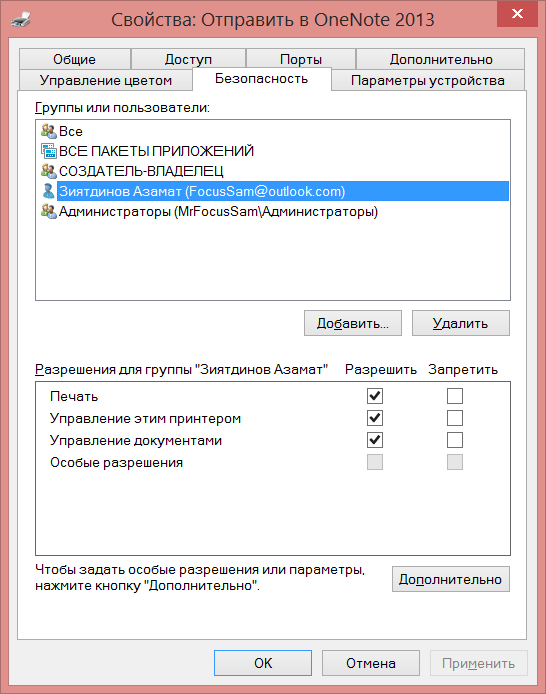
* Специальные права определяют возможность обращения к объекту по свойственному только данной категории объектов методу – печать, управление принтерами, управление документами.
* Стандартные права определяют возможность доступа к объекту по методу, применимому к любому объекту – чтение разрешений, смена разрешений, смена владельца
* Общие права представляют собой комбинацию специальных и стандартных прав, и предоставляет возможность обращения к объекту с помощью некоторого набора методов доступа. Пример общих прав доступа:
* Печать (возможность посылать задания на принтер, чтение DACL)

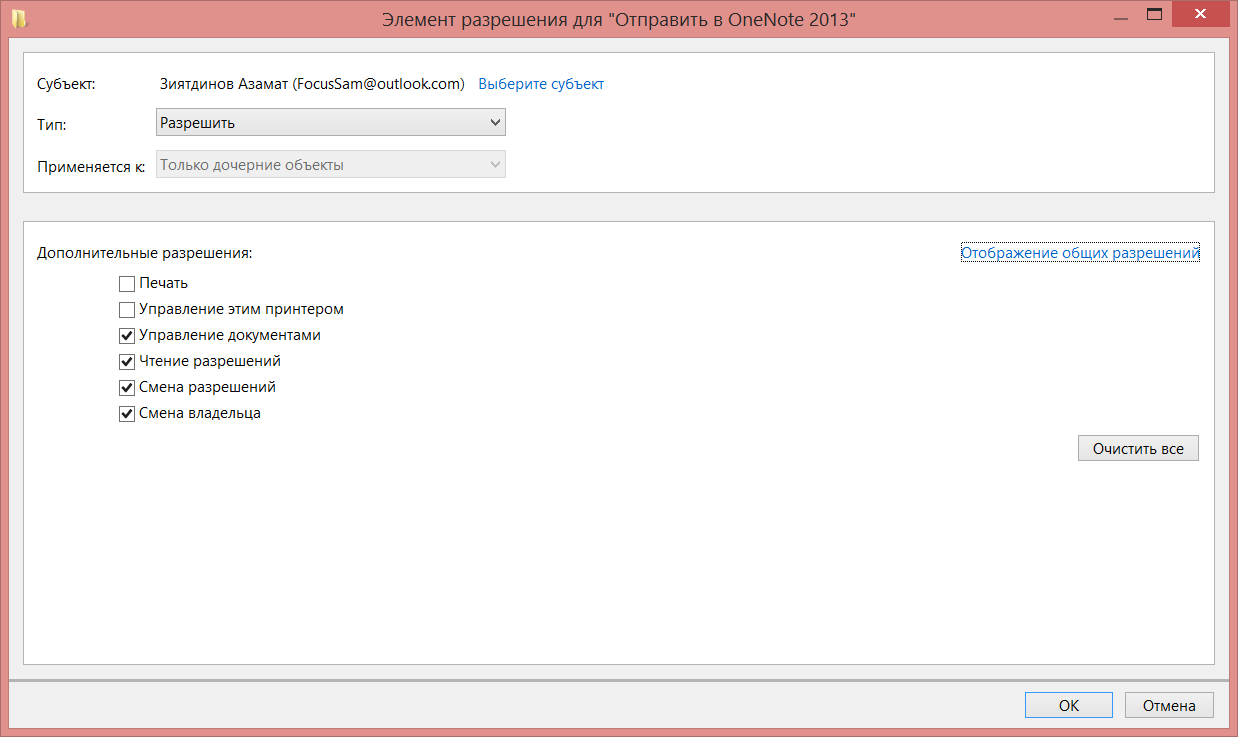
Владелец имеет право на чтение и изменение разрешений. И даже явно указанный запрет для учетной записи не имеет приоритета над правами владельца.

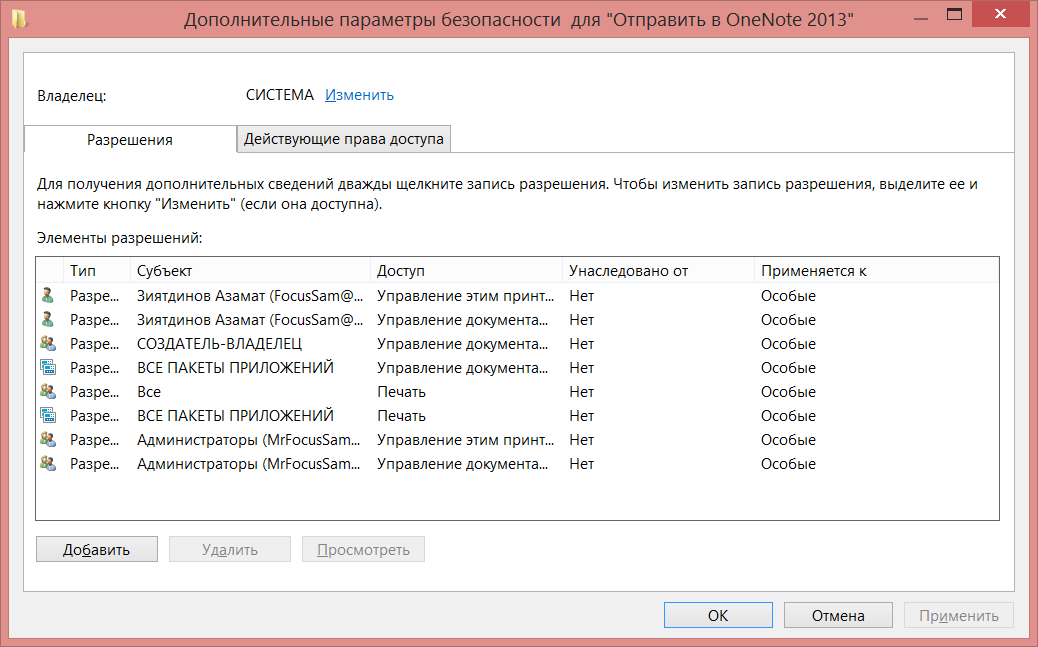
Каждый объект имеет набор связанных с ним действующих разрешений. Вкладка *Действующие разрешения* содержит список разрешений, которые будут даны выбранной группе или пользователю только на основании членства в группах.

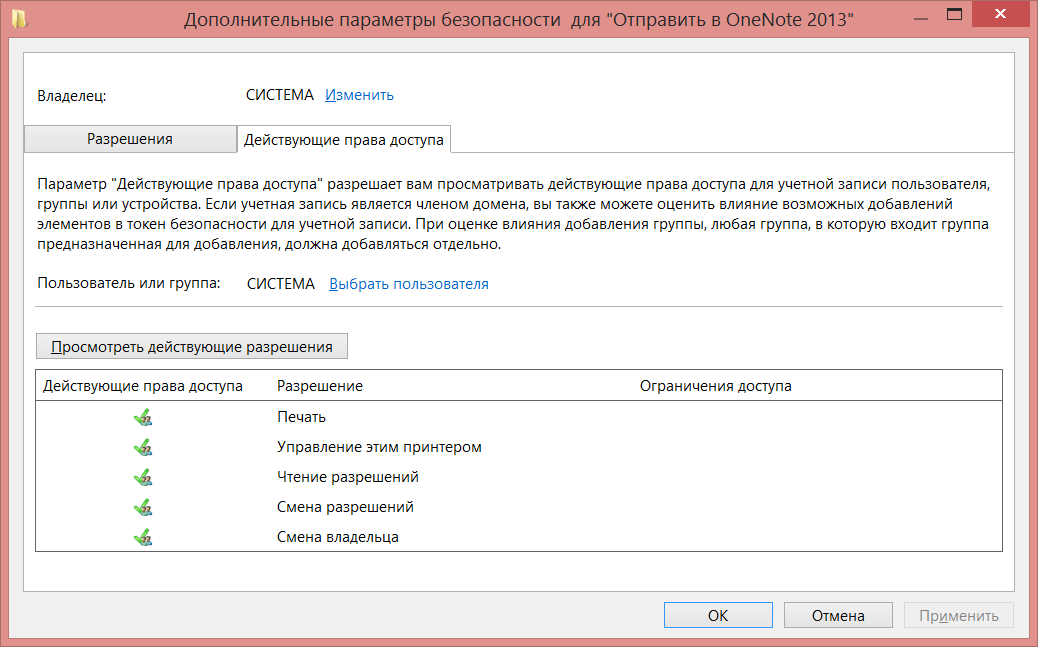
* 1. Включить в электронную версию отчета копии экранных форм, использованных при выполнении данного пункта.











1. Ознакомиться с порядком разграничения доступа к разделам реестра (с помощью команды меню редактора реестра Правка | Разрешения, пункт выполняется в виртуальной машине Windows XP или с правами администратора).
   1. Включить в отчет сведения об особенностях управления доступом к разделам реестра (родовых правах доступа, полном наборе специальных и стандартных прав доступа, владельце объекта, действующих разрешениях на доступ к объекту для конкретного субъекта). Для выполнения этого задания обязательно открыть все вкладки окна дополнительных параметров безопасности объекта.

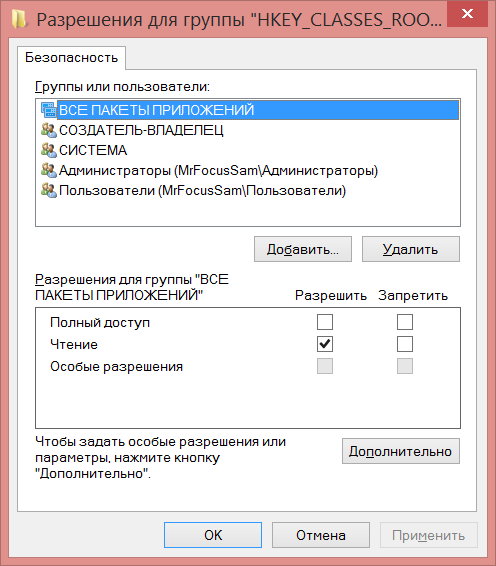
Для каждого раздела реестра можно настроить разрешения доступа на изменение, чтение, запись во вкладке «Безопасность». Настройки разделов реестра прав владельца и прав доступа работают по такому же принципу, как и аналогичные команды «Проводника» по установке прав доступа к файлам и каталогам.

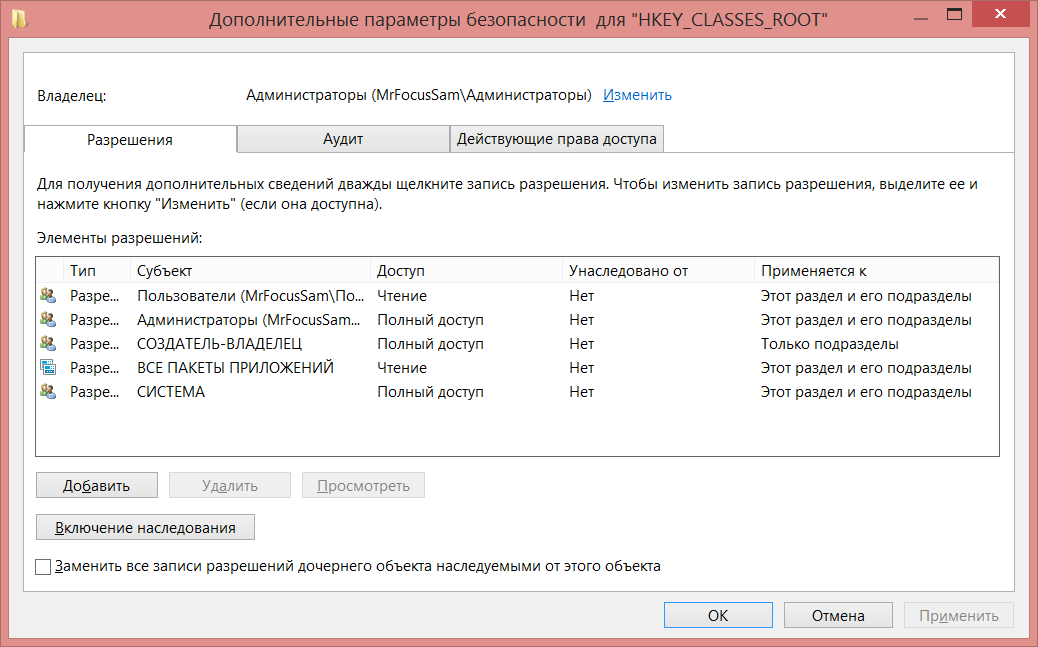
* Специальные права определяют возможность обращения к объекту по свойственному только данной категории объектов методу – запрос значения, задание значения, создание подраздела, перечисление подразделов, уведомление, создание связи.
* Стандартные права определяют возможность доступа к объекту по методу, применимому к любому объекту – удаление, чтение разрешений, запись DAC, смена владельца
* Общие права представляют собой комбинацию специальных и стандартных прав, и предоставляет возможность обращения к объекту с помощью некоторого набора методов доступа. Пример общих прав доступа:
* Чтение (запрос значения, перечисление подразделов, уведомление, чтение разрешений)

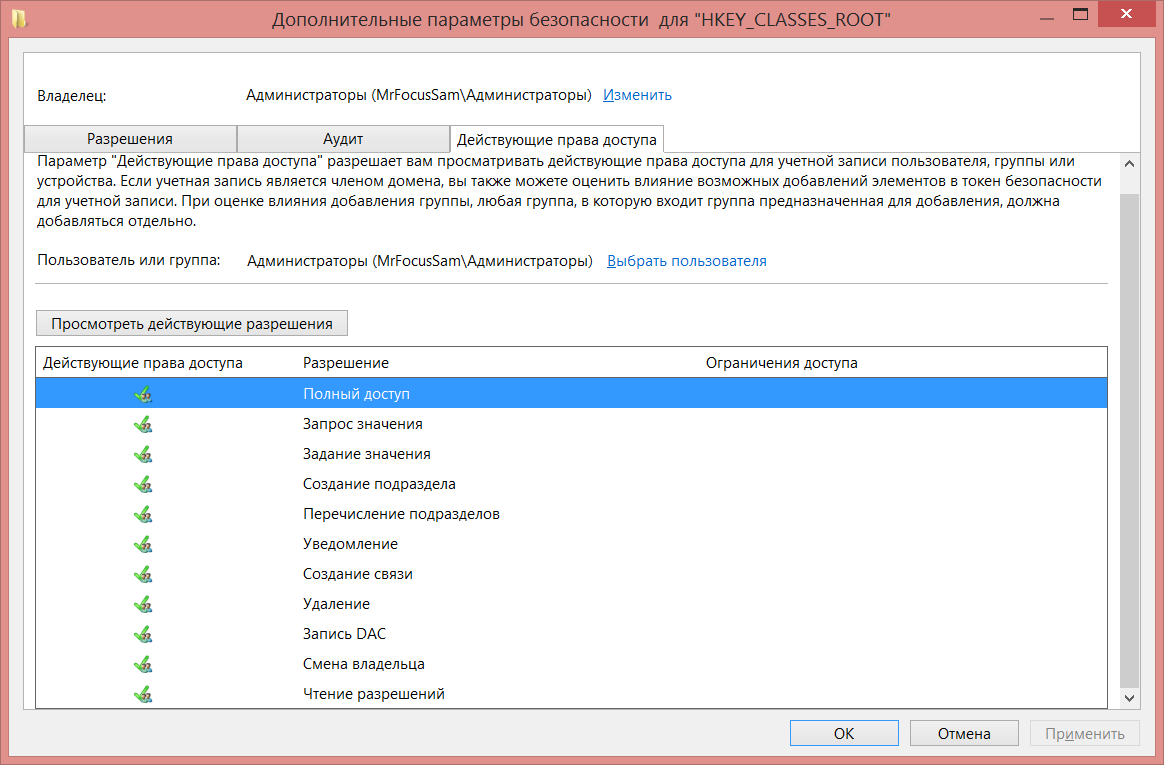
Владелец имеет право на чтение и изменение разрешений. И даже явно указанный запрет для учетной записи не имеет приоритета над правами владельца.

Каждый объект имеет набор связанных с ним действующих разрешений. Вкладка *Действующие разрешения* содержит список разрешений, которые будут даны выбранной группе или пользователю только на основании членства в группах.

* 1. Включить в электронную версию отчета копии экранных форм, использованных при выполнении данного пункта.







1. Пункты 12-15 выполняются в виртуальной машине Windows XP или с правами администратора. Ознакомиться (с помощью функции Панели управления Администрирование | Управление компьютером – административная оснастка compmgmt.msc, узел Локальные пользователи и группы) с порядком создания и изменения учетных записей пользователей и групп в защищенных версиях операционной системы Windows.
   1. Включить в отчет соответствующие сведения.

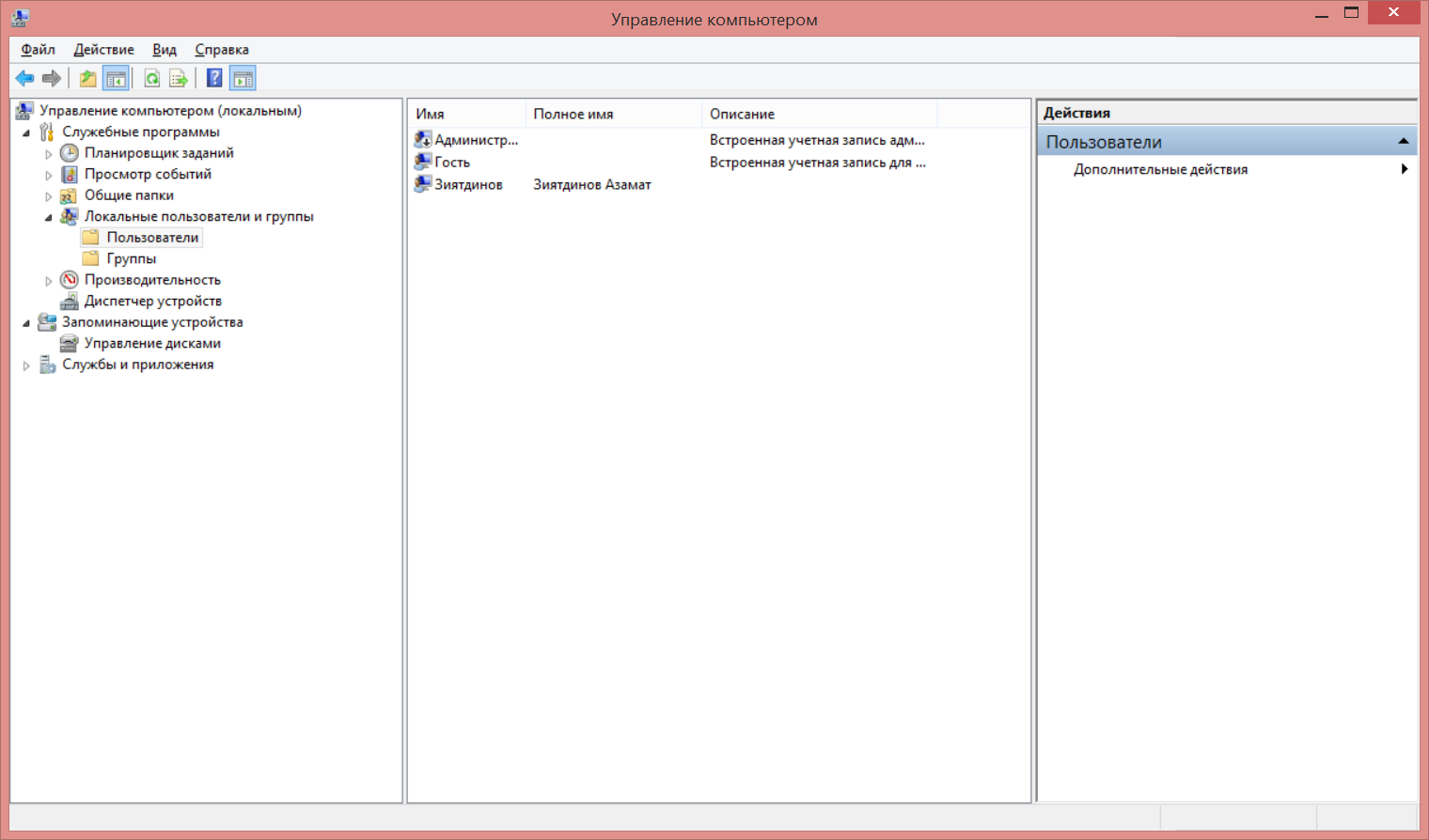
Оснастка "Локальные пользователи и группы" служит для создания пользователей и групп, хранимых локально на компьютере, и управления ими.

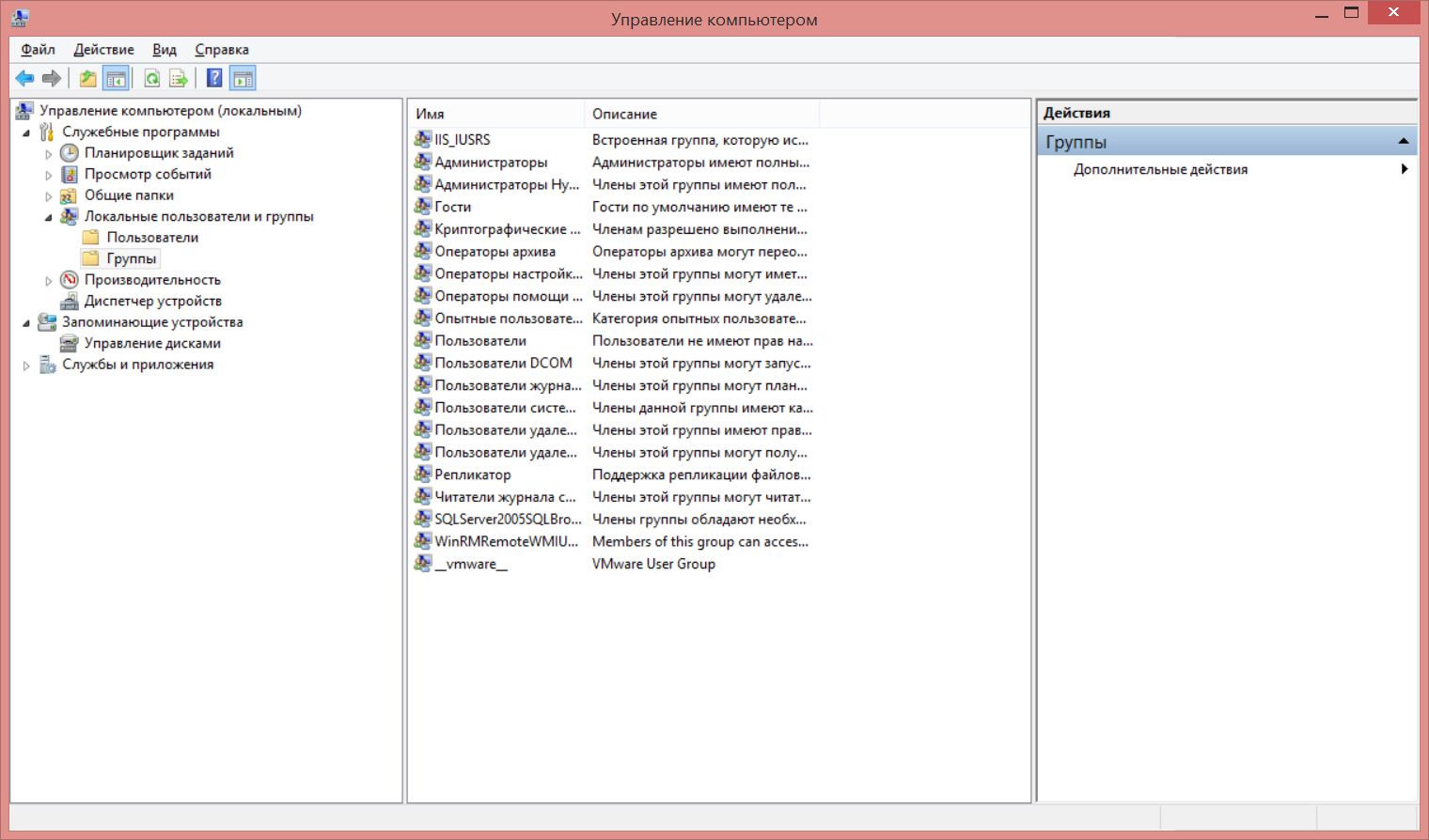
Основные действия по администрированию локальных пользователей:

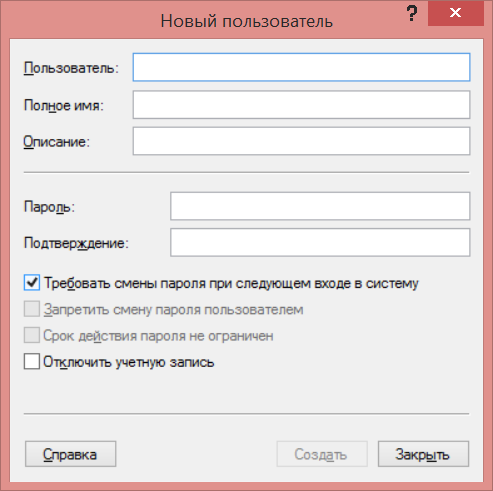
* Создание локальной учетной записи пользователя;
* Сброс пароля для локальной учетной записи пользователя;
* Отключение или активация локальной учетной записи пользователя;
* Удаление локальной учетной записи пользователя;
* Переименование локальной учетной записи пользователя;
* Назначение сценария входа для локальной учетной записи пользователя;
* Назначение домашней папки локальной учетной записи пользователя.

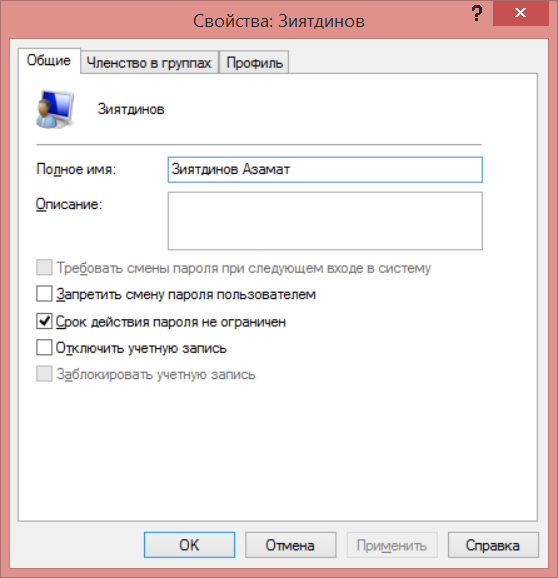
Основные действия по администрированию локальных групп:

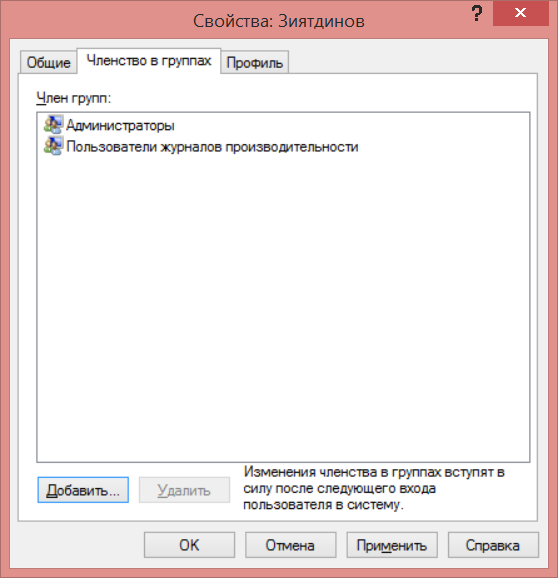
* Создание локальной группы;
* Добавление члена в локальную группу;
* Идентификация членов локальной группы;
* Удаление локальной группы.
  1. Включить в электронную версию отчета копии соответствующих экранных форм.

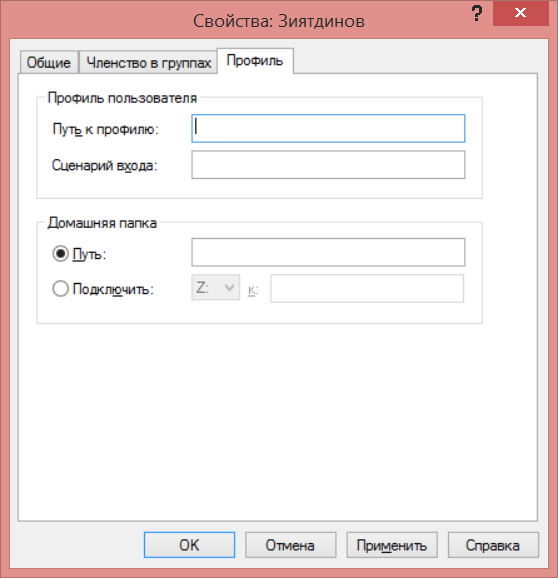


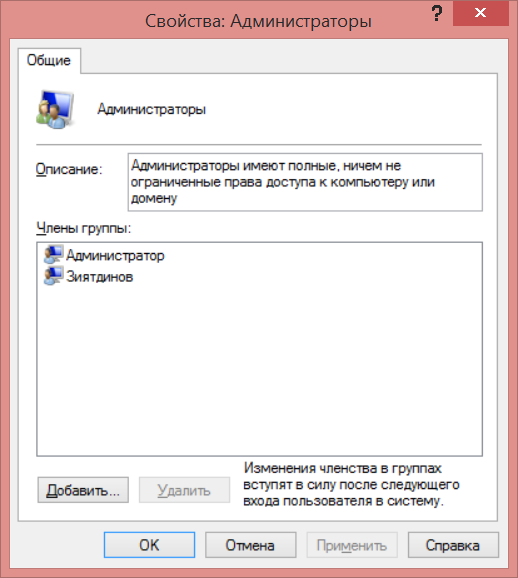








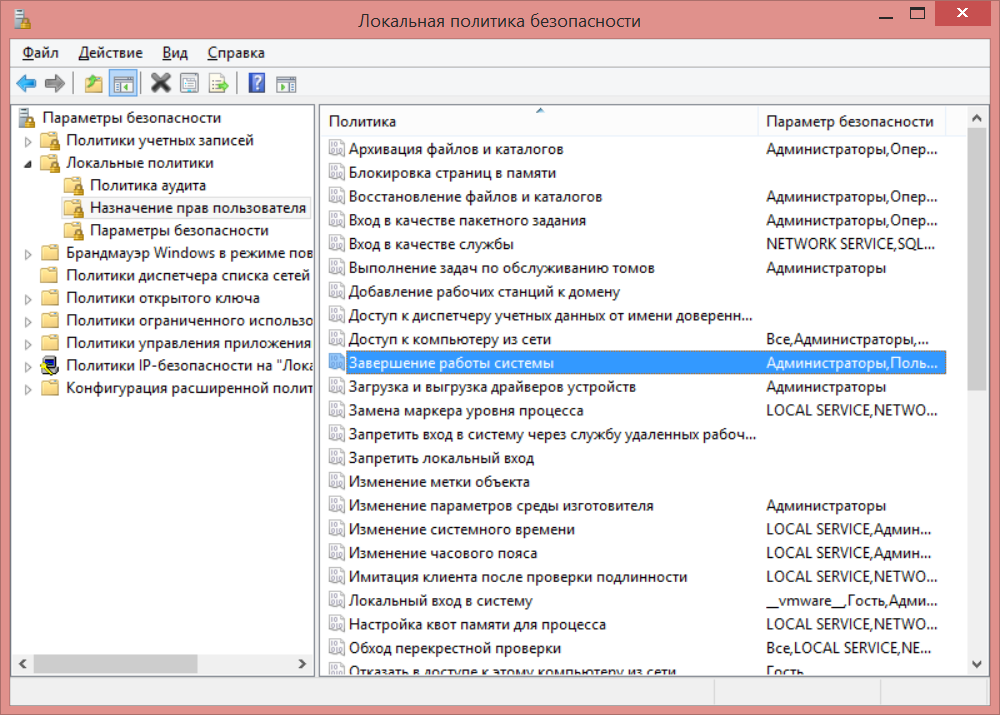


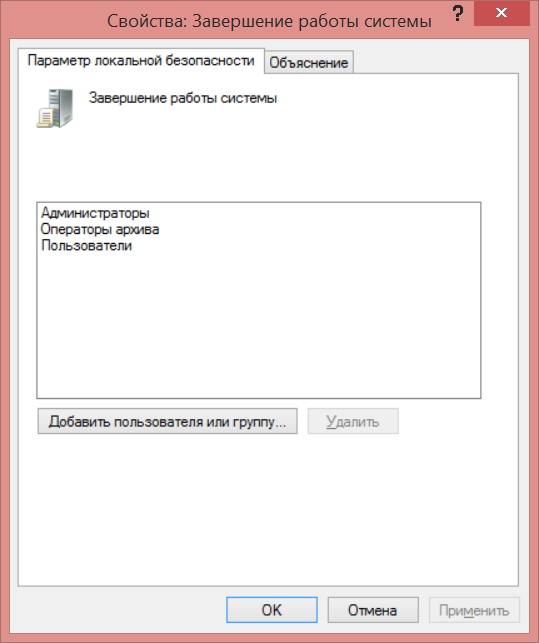


1. Ознакомиться (с помощью функции Панели управления Администрирование | Локальная политика безопасности | Локальные политики | Назначение прав пользователя – административная оснастка secpol.msc, узел Локальные политики | Назначение прав пользователя) с порядком назначения прав пользователям и группам.
   1. Включить в отчет соответствующие сведения.

Основные параметры настройки локальной политики безопасности:

* Запретить вход в систему через службы удаленных рабочих столов. Этот параметр безопасности определяет, каким пользователям и группам будет запрещено входить в систему как клиенту служб удаленных рабочих столов.
* Запретить локальный вход. Этот параметр безопасности определяет, каким пользователям будет отказано во входе в систему. Этот параметр политики заменяет параметр "Разрешить локальный вход в систему", если к учетной записи применяются обе политики. Если этот параметр безопасности применяется к группе "Все", никто не сможет войти в систему локально.
* Отказать в доступе к этому компьютеру из сети. Этот параметр безопасности определяет, каким пользователям будет отказано в доступе к компьютеру из сети. Этот параметр заменяет параметр политики "Разрешить доступ к компьютеру из сети", если к учетной записи пользователя применяются об политики.
* Разрешать вход в систему через службы удаленных рабочих столов. Этот параметр безопасности определяет, какие пользователи или группы имеют право входа в систему в качестве клиента служб удаленных рабочих столов.
  1. Включить в электронную версию отчета копии соответствующих экранных форм.

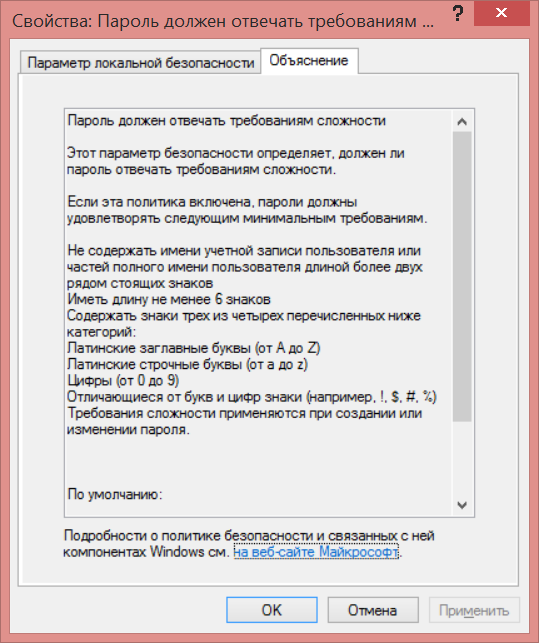


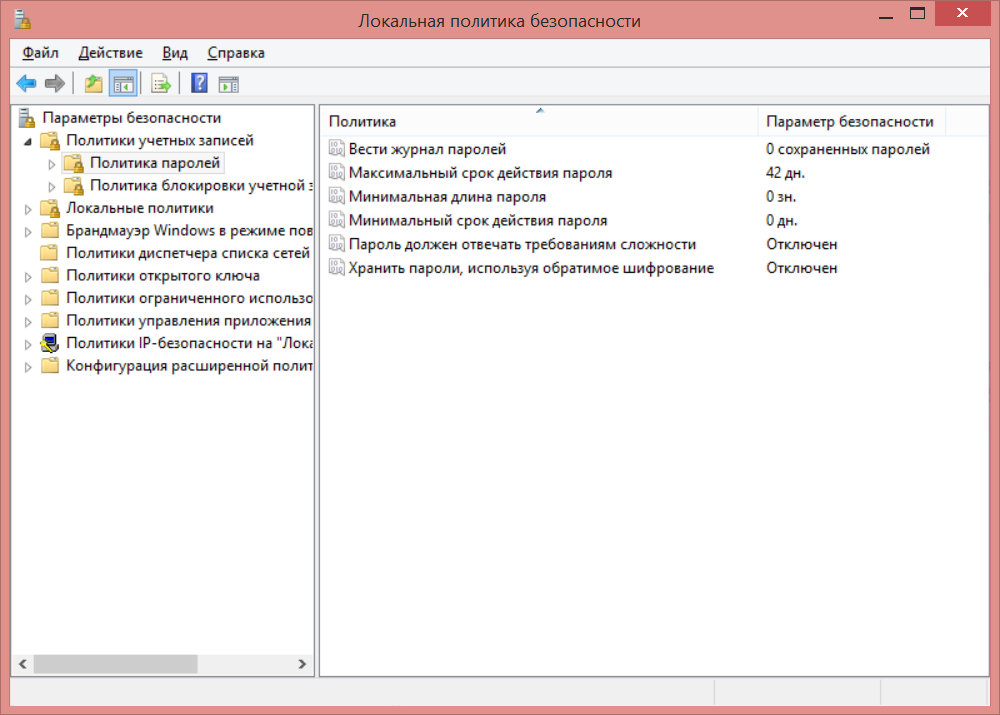


1. Ознакомиться (с помощью функции Панели управления Администрирование | Локальная политика безопасности | Политики учетных записей | Политика паролей – административная оснастка secpol.msc, узел Политики учетных записей | Политика паролей) с порядком определения параметров безопасности для парольной аутентификации.
   1. Включить в отчет соответствующие сведения.

Политики паролей операционной системы Windows позволяют довольно гибко настроить ограничения по выбору паролей для пользователей Windows. Политики паролей позволяют настроить минимальную длину паролей, их сложность и многие другие параметры.

* 1. Включить в электронную версию отчета копии соответствующих экранных форм.

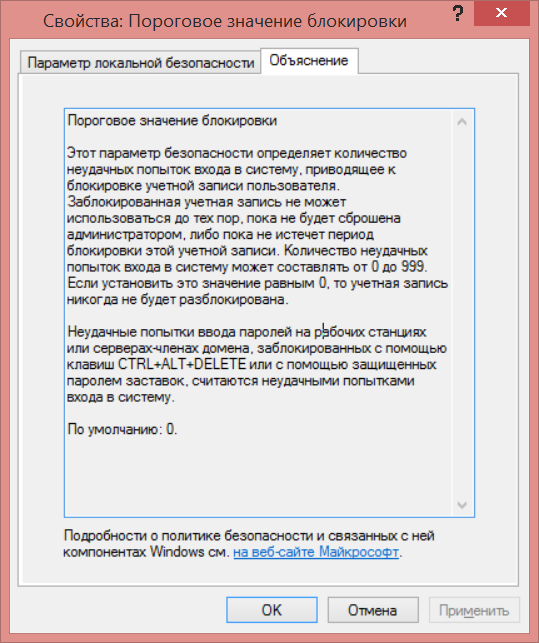




1. Ознакомиться (с помощью функции Панели управления Администрирование | Локальная политика безопасности | Политики учетных записей | Политика блокировки учетных записей – административная оснастка secpol.msc, узел Политики учетных записей | Политика блокировки учетных записей) с порядком определения параметров безопасности для политики блокировки учетных записей.
   1. Включить в отчет соответствующие сведения.

Политики блокировки учетных записей операционной системы Windows позволяют настроить параметры блокировки учетных записей.

* 1. Включить в электронную версию отчета копии соответствующих экранных форм.





19. Включить в отчет ответы на контрольные вопросы, номера которых выбираются в соответствии с номером варианта и прилагаемой ниже таблицей.

7. В чем недостаточность средств ограничения прав пользователей, предоставляемых редактором объектов групповой политики и оснасткой «Локальная политика безопасности» Windows?

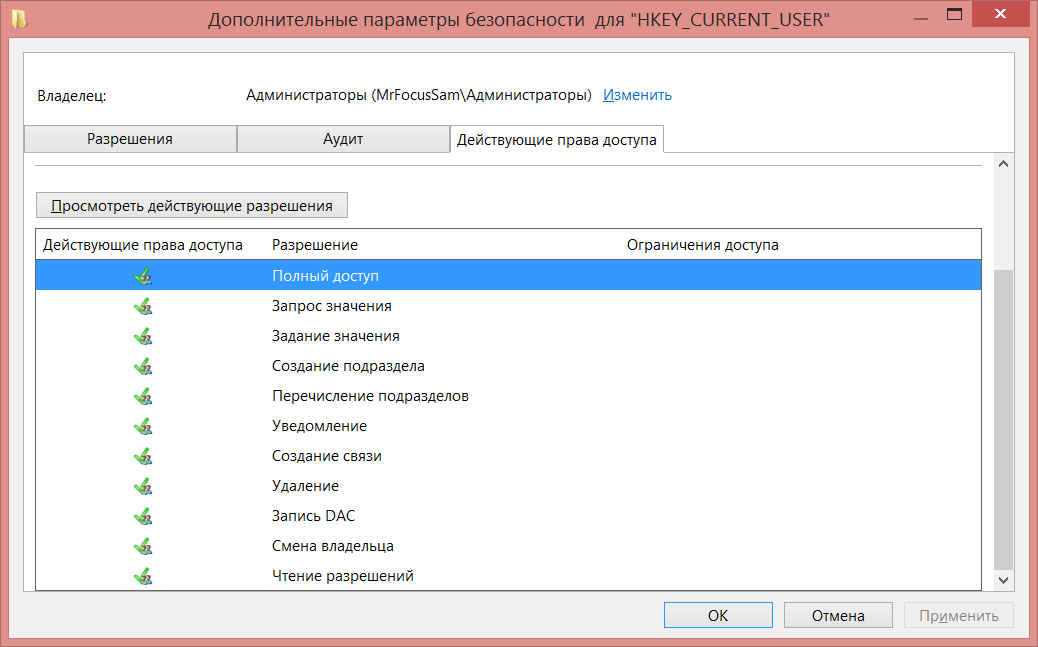
15. Насколько надежна защита документов Microsoft Office от изменения с помощью паролей (может ли она быть «вскрыта»)?

Защита не идеальная и она может быть взломана с помощью программ-взломщиков. Например, с помощью «полного перебора», «атаки по словарю».

24. Кто может управлять разрешениями на доступ к объекту в системах с дискреционным разграничением доступа?

Правом редактирования дискреционного списка контроля доступа обычно обладают владелец объекта и администратор безопасности.

29. Какие специфические права доступа могут быть определены для раздела реестра?



40. Какие требования по сложности могут предъявляться к паролям в операционной системе Windows?

* Не содержать имени учетной записи пользователя или частей полного имени пользователя длиной более двух рядом стоящих знаков
* Иметь длину не менее 6 знаков
* Содержать знаки трех из четырех перечисленных ниже категорий:

1. Латинские заглавные буквы (от A до Z)
2. Латинские строчные буквы (от a до z)
3. Цифры (от 0 до 9)
4. Отличающиеся от букв и цифр знаки (например, !, $, #, %)

46. Какой может быть реакция системы на попытку подбора паролей?

Реакцией системы на неудачную попытку входа пользователя могут быть:

• блокировка учетной записи, под которой осуществляется по­пытка входа, при превышении максимально возможного числа попыток (на заданное время или до ручного снятия блокировки администратором);

• нарастающее увеличение временной задержки перед предо­ставлением пользователю следующей попытки входа.