МИНОБРНАУКИ РОССИИ
Федеральное государственное бюджетное образовательное учреждение
Высшего профессионального образования
Пензенский государственный технологический университет
Кафедра «Информационные компьютерные технологии»

Методические рекомендации к лабораторной работе

Тема:
«Управление правами пользователей в ОС Windows 7.
Локальная политика безопасности»

Пенза, 2014

Лабораторная работа на тему «Управление правами пользователей в ОС Windows 7. Локальная политика безопасности»

Цель работы: ознакомиться с процедурами создания учётных записей пользователей и управления их правами.

Задание: изучить процедуру создания учётных записей пользователей и научиться управлять их правами.

Учётные записи пользователей

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

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

Учётная запись может содержать следующие дополнительные анкетные данные о пользователе:

- имя;
- фамилию;
- отчество;
- псевдоним (ник);
- пол;
- национальность;
- расовую принадлежность;
- вероисповедание
- группу крови;
- резус-фактор;
- возраст;
- дату рождения;
- адрес электронной почты;
- домашний адрес;
- рабочий адрес;
- нетмейловый адрес;
- номер домашнего телефона;
- номер рабочего телефона;
- номер мобильного телефона;
- номер ICQ;

- идентификатор Skype, ник в IRC;
- другие контактные данные систем обмена мгновенными сообщениями;
- адрес домашней страницы и/или блога в Интернете или интранете;
- сведения о хобби;
- сведения о круге интересов;
- сведения о семье;
- сведения о перенесённых болезнях;
- сведения о политических предпочтениях;
- и многое другое.

Конкретные категории данных, которые могут быть внесены в такую анкету, определяются администраторами системы.

Учётная запись может также содержать одну или несколько фотографий или аватар пользователя. Учётная запись пользователя также может учитывать различные статистические характеристики поведения пользователя в системе: давность последнего входа в систему, продолжительность последнего пребывания в системе, адрес использованного при подключении компьютера, интенсивность использования системы, суммарное и (или) удельное количество определённых операций, произведённых в системе, и так далее.

Создание учётных записей пользователей

В операционной системе Windows 7 можно создавать несколькими способами как учётные записи пользователей для компьютеров, состоящих в рабочих группах, так и учётные записи пользователей для компьютеров, которые входят в состав домена. Домены, рабочие группы и домашние группы представляют разные методы организации компьютеров в сети. Основное их различие состоит в том, как осуществляется управление компьютерами и другими ресурсами.

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

Домен – это группа компьютеров одной сети, имеющих единый центр, использующий единую базу пользователей, единую групповую и локальную политики, единые параметры безопасности, ограничение времени работы учётной записи и прочие параметры, значительно упрощающие работу системного администратора организации, если в ней эксплуатируется большое число компьютеров.

Создание учётных записей пользователей для компьютеров, состоящих в рабочей группе

В операционной системе Windows 7 для компьютеров, которые состоят в рабочей или домашней группе, учётные записи можно создавать следующими способами:

Создание учётной записи при помощи диалога «Управление учётными записями пользователей»

Практическое задание №1

Для того чтобы создать учётную запись при помощи диалога «Управление учётными записями пользователей», нужно сделать следующее:

1. Нажать на кнопку «Пуск» для открытия меню, открыть «Панель управления» и из списка компонентов панели управления выбрать «Учётные записи пользователей».
2. В диалоге «Учётные записи пользователей» перейти по ссылке «Управление другой учётной записью», а затем нажать на «Создание учётной записи».
3. Здесь нужно будет ввести имя для учётной записи, выбрать тип учётной записи и нажать на кнопку «Создание учётной записи».

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

В этом диалоге, можно выбрать одну из двух типов учётных записей: «обычные учётные записи пользователей», которые предназначены для повседневной работы или «учётные записи администратора», которые предоставляют полный контроль над компьютером и применяются только в необходимых случаях.

Создание учётной записи при помощи диалога «Учётные записи пользователей»

Доступный через панель управления диалог «Управление учётными записями пользователей» имеет очень серьезное ограничение: оно предлагает на выбор только учётные записи типа «*Обычный доступ*» или «*Администратор*». Для того чтобы при создании нового пользователя его можно было поместить в какую-либо определённую группу, нужно сделать следующее:

1. Воспользоваться комбинацией клавиш +R для открытия диалога «Выполнить»;
2. В диалоговом окне «Выполнить», в поле «Открыть» ввести «*control userpasswords2*» и нажать на кнопку «ОК».
3. В диалоговом окне «Учётные записи пользователей» нажать на кнопку «Добавить» для запуска мастера добавления нового пользователя.

4. В появившемся диалоговом окне «Добавление нового пользователя» ввести имя пользователя. Поля «Полное имя» и «Описание» не являются обязательными, то есть их можно заполнять при желании. Нажать на кнопку «Далее».

5. В диалоге «Введите и подтвердите пароль этого пользователя» ввести пароль для данной учётной записи, а затем продублировать его в поле «Подтверждение», после чего нажать на кнопку «Далее».

6. Это последний диалог мастера добавления нового пользователя. Здесь необходимо установить переключатель, определяющий группу безопасности, к которой должна относиться данная учётная запись пользователя. Можно выбрать одну из следующих групп: «Обычный доступ», «Администратор» или «Другой». Последний переключатель стоит использовать в том случае, если нужно отнести пользователя к какой-то другой группе, созданной по умолчанию в операционной системе Windows 7.

В следующем списке перечислены 15 встроенных групп операционной системы Windows 7. Эти права назначаются в рамках локальных политик безопасности:

- **Administrators (Администраторы)**. Пользователи, входящие в эту группу, имеют полный доступ на управление компьютером и могут при необходимости назначать пользователям права пользователей и разрешения на управление доступом. По умолчанию членом этой группы является учётная запись администратора. Если компьютер подключен к домену, группа «Администраторы домена» автоматически добавляется в группу «Администраторы». Эта группа имеет полный доступ к управлению компьютером, поэтому необходимо проявлять осторожность при добавлении пользователей в данную группу;
- **Backup Operators (Операторы архива)**. Пользователи, входящие в эту группу, могут архивировать и восстанавливать файлы на компьютере независимо от любых разрешений, которыми защищены эти файлы. Это обусловлено тем, что право выполнения архивации получает приоритет над всеми разрешениями. Члены этой группы не могут изменять параметры безопасности.
- **Cryptographic Operators (Операторы криптографии)**. Членам этой группы разрешено выполнение операций криптографии.
- **Debugger Users (Группа удалённых помощников)**. Члены этой группы могут предлагать удалённую помощь пользователям данного компьютера.
- **Distributed COM Users (Пользователи DCOM)**. Членам этой группы разрешено запускать, активировать и использовать объекты DCOM на компьютере.
- **Event Log Readers (Читатели журнала событий)**. Членам этой группы разрешается запускать журнал событий Windows.
- **Guests (Гости)**. Пользователи, входящие в эту группу, получают временный профиль, который создаётся при входе пользователя в систему и

удаляется при выходе из неё. Учётная запись **«Гость»** (отключенная по умолчанию) также является членом данной встроенной группы.

- **IIS_IUSRS**. Это встроенная группа, используемая службами IIS.
- **Network Configuration Operators (Операторы настройки сети)**. Пользователи, входящие в эту группу, могут изменять параметры TCP/IP, а также обновлять и освобождать адреса TCP/IP. Эта группа не имеет членов по умолчанию.
- **Performance Log Users (Пользователи журналов производительности)**. Пользователи, входящие в эту группу, могут управлять счетчиками производительности, журналами и оповещениями на локальном или удалённом компьютере, не являясь при этом членами группы «Администраторы».
- **Performance Monitor Users (Пользователи системного монитора)**. Пользователи, входящие в эту группу, могут наблюдать за счетчиками производительности на локальном или удалённом компьютере, не являясь при этом участниками групп «Администраторы» или «Пользователи журналов производительности».
- **Power Users (Опытные пользователи)**. По умолчанию, члены этой группы имеют те же права пользователя и разрешения, что и учётные записи обычных пользователей. В предыдущих версиях операционной системы Windows эта группа была создана для того, чтобы назначать пользователям особые административные права и разрешения для выполнения распространенных системных задач. В этой версии операционной системы Windows учётные записи обычных пользователей предусматривают возможность выполнения большинства типовых задач настройки, таких как смена часовых поясов. Для старых приложений, требующих тех же прав опытных пользователей, которые имелись в предыдущих версиях операционной системы Windows, администраторы могут применять шаблон безопасности, который позволяет группе «Опытные пользователи» присваивать эти права и разрешения, как это было в предыдущих версиях операционной системы Windows.
- **Remote Desktop Users (Пользователи удалённого рабочего стола)**. Пользователи, входящие в эту группу, имеют право удалённого входа на компьютер.
- **Replicator (Репликатор)**. Эта группа поддерживает функции репликации. Единственный член этой группы должен иметь учётную запись пользователя домена, которая используется для входа в систему службы репликации контроллера домена. Не добавляйте в эту группу учётные записи реальных пользователей.
- **Users (Пользователи)**. Пользователи, входящие в эту группу, могут выполнять типовые задачи, такие как запуск приложений, использование локальных и сетевых принтеров и блокировку компьютера. Члены этой группы не могут предоставлять общий доступ к папкам или создавать локальные принтеры. По умолчанию членами этой группы являются группы

«Пользователи домена», «Проверенные пользователи» и «Интерактивные». Таким образом, любая учётная запись пользователя, созданная в домене, становится членом этой группы.

Создание учётной записи при помощи оснастки «Локальные пользователи и группы»

Оснастка «Локальные пользователи и группы» расположена в компоненте «Управление компьютером», представляющем собой набор средств администрирования, с помощью которых можно управлять одним компьютером, локальным или удалённым. Оснастка «Локальные пользователи и группы» служит для защиты и управления учётными записями пользователей и групп, размещенных локально на компьютере. Можно назначать разрешения и права для учётной записи локального пользователя или группы на определённом компьютере (и только на этом компьютере).

Использование оснастки «Локальные пользователи и группы» позволяет ограничить возможные действия пользователей и групп при помощи назначения им прав и разрешений. Право дает возможность пользователю выполнять на компьютере определённые действия, такие как архивирование файлов и папок или завершение работы компьютера. Разрешение представляет собой правило, связанное с объектом (обычно с файлом, папкой или принтером), которое определяет, каким пользователям, и какой доступ к объекту разрешен.

Для того чтобы создать локальную учётную запись пользователя при помощи оснастки «Локальные пользователи и группы», нужно сделать следующее:

1. Открыть оснастку «Локальные пользователи и группы» одним из следующих способов:

- нажать на кнопку «Пуск» для открытия меню, открыть «Панель управления» и из списка компонентов панели управления выбрать «Администрирование», затем открыть компонент «Управление компьютером». В «Управлении компьютером» открыть «Локальные пользователи и группы»**;**
- открыть «Консоль управления ММС». Для этого нажать на кнопку «Пуск», в поле поиска ввести *mmc*, а затем нажать на кнопку «Enter». Откроется пустая консоль ММС. В меню «Консоль» выбрать команду «Добавить или удалить оснастку» или воспользоваться комбинацией клавиш Ctrl+M. В диалоге «Добавление и удаление оснасток» выбрать оснастку «Локальные пользователи и группы» и нажать на кнопку «Добавить». Затем нажать на кнопку «Готово», а после этого – кнопку «ОК». В дереве консоли открыть узел «Локальные пользователи и группы (локально)»;
- воспользоваться комбинацией клавиш  +R для открытия диалога «Выполнить». В диалоговом окне «Выполнить», в поле «Открыть» ввести *lusrmgr.msc* и нажать на кнопку «ОК».

2. Открыть узел «Пользователи» и либо в меню «Действие», либо из контекстного меню выбрать команду «Новый пользователь».

3. В диалоговом окне «Новый пользователь» ввести соответствующие сведения. Помимо указанных данных, можно воспользоваться следующими флажками: «*Требовать смену пароля при следующем входе в систему»*, *«Запретить смену пароля пользователем»*, *«Срок действия пароля не ограничен»*, *«Отключить учётную запись»* и нажать на кнопку «Создать», а затем «Закрыть».

Для того чтобы добавить пользователя в группу, дважды щёлкнуть имя пользователя для получения доступа к странице свойств пользователя. На вкладке «Членство в группах» нажать на кнопку «Добавить».

В диалоге «Выбор группы» можно выбрать группу для пользователя двумя способами:

1. В поле «Введите имена выбираемых объектов» ввести имя группы и нажать на кнопку «Проверить имена».

2. В диалоге «Выбор группы» нажать на кнопку «Дополнительно», чтобы открыть диалоговое окно «Выбор группы». В этом окне нажать на кнопку «Поиск», чтобы отобразить список всех доступных групп, выбрать подходящую группу и нажать два раза на кнопку «ОК».

Создание учётной записи при помощи командной строки

Помимо вышеперечисленных способов, учётные записи пользователей можно создавать, изменять и удалять при помощи командной строки. Для этого нужно выполнить следующие действия:

1. Запустить командную строку от имени администратора.

2. Для создания учётной записи при помощи командной строки использовать команду *net user*.

Команда net user используется для добавления пользователей, установки паролей, отключения учётных записей, установки параметров и удаления учётных записей. При выполнении команды без параметров командной строки отображается список учётных записей пользователей, присутствующих на компьютере. Информация об учётных записях пользователей хранится в базе данных учётных записей пользователей.

Пример команды:

net user User /add /passwordreq:yes /times:monday-friday,9am-6pm/fullname:»New user»

Используемые параметры:

/add – этот параметр указывает, что необходимо создать новую учётную запись;

/passwordreq – этот параметр отвечает за то, чтобы при первом входе в систему пользователь сменил свой пароль;

/times – этот параметр определяет, сколько раз пользователю разрешено входить в систему. Здесь можно указывать как единичные дни, так и целые диапазоны (например Sa или M-F). Для указания времени допускается как 24-часовой формат, так и 12-часовой формат;

/fullname – этот параметр идентичен полю «Полное имя» при создании пользователя предыдущими способами.

Управление учётными записями при помощи диалога «Управление учётными записями пользователей»

При помощи диалогового окна **«Учётные записи пользователей»** можно не только создавать учётные записи, но и выполнять с ними простейшие действия, такие как:

- изменение имени;
- создание пароля;
- изменение пароля;
- удаление пароля;
- изменение рисунка;
- установка родительского контроля;
- изменение типа учётной записи;
- удаление учётной записи;
- включение и отключение гостевой учётной записи.

В этом разделе будет подробно рассмотрено каждое из перечисленных действий.

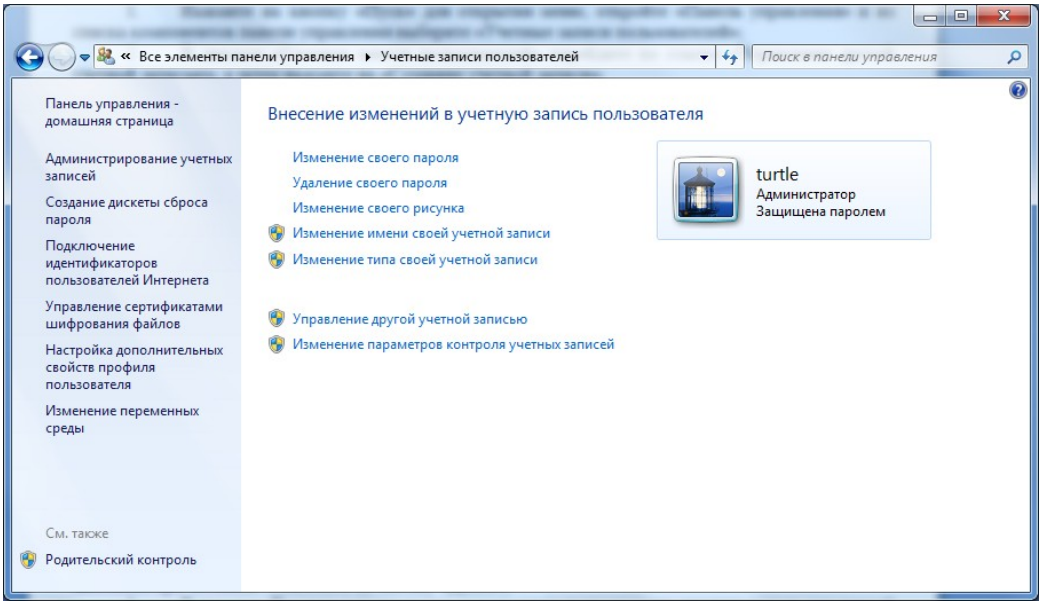

Рисунок 1 – Диалоговое окно «Учётные записи пользователей»

Изменение имени

Практическое задание №2

Для того чтобы изменить имя учётной записи необходимо выполнить следующие действия:

1. Нажать на кнопку «Пуск» для открытия меню, открыть «Панель управления» и из списка компонентов панели управления выбрать «Учётные записи пользователей».
2. Выбрать нужную учётную запись и перейти по ссылке «Изменение имени своей учётной записи».
3. В поле «Новое имя учётной записи» ввести новое имя пользователя и нажать на кнопку «Переименовать».

Создание пароля

Практическое задание №3

Для того чтобы создать пароль для учётной записи пользователя необходимо:

1. Нажать на кнопку «Пуск» для открытия меню, открыть «Панель управления» и из списка компонентов панели управления выбрать «Учётные записи пользователей».
2. Выбрать учётную запись, для которой нужно создать пароль и перейти по ссылке «Создание пароля своей учётной записи». Эта ссылка будет отображаться только в том случае, если у пользователя этой текущей записи нет пароля.
3. В диалоге «Создание пароля своей учётной записи» ввести пароль для данной учётной записи, а затем повторить его в поле «Подтверждение пароля» и ввести подсказку в поле «Введите подсказку для пароля». Подсказка – это текст, который операционная система отображает на экране приветствия. В связи с тем, что подсказку может увидеть любой пользователь, который попытается войти в систему, она должна быть менее очевидной, но при этом понятной для того, кто её создал в том случае, если он забудет пароль. После ввода пароля, подтверждения пароля и подсказки для создания пароля учётной записи необходимо нажать на кнопку «Создать».

Изменение пароля

Если у учётной записи пользователя уже имеется пароль, но его нужно сменить, нужно сделать следующее:

1. Нажать на кнопку «Пуск» для открытия меню, открыть «Панель управления» и из списка компонентов панели управления выбрать «Учётные записи пользователей».
2. Выбрать свою учётную запись и перейти по ссылке «Изменение своего пароля».

3. Находясь в диалоге «Изменение своего пароля», в поле «Текущий пароль» ввести пароль, который установлен для учётной записи в данный момент. В поля «Новый пароль» и «Подтверждение пароля» ввести и подтвердить новый пароль для учётной записи. В поле «Введите подсказку для пароля» ввести подсказку.

Для создания надежных паролей и парольных фраз также можно использовать расширенный набор знаков ASCII – системы, присваивающей числовые значения буквам, цифрам и другим символам. Используя расширенный набор знаков ASCII, можно повысить надежность паролей и парольных фраз. Перед использованием знаков из расширенного набора ASCII для создания паролей и парольных фраз следует убедиться, что пароли и фразы с такими знаками совместимы с приложениями, используемыми вами.

Удаление пароля

Практическое задание №4

В том случае, если у пользователя есть пароль и этот пароль для работы за компьютером ему не нужен, необходимо выполнить следующие действия:

1. Нажать на кнопку «Пуск» для открытия меню, открыть «Панель управления» и из списка компонентов панели управления выбрать «Учётные записи пользователей».
2. Выбрать свою учётную запись и нажать на ссылку «Удаление своего пароля».
3. В диалоге «Удаление своего пароля» в поле «Текущий пароль» ввести пароль текущей учётной записи и нажать на кнопку «Удалить пароль».

Изменение рисунка учётной записи

В операционных системах Windows есть возможность выбора изображения, соответствующего учётной записи пользователя, которое отображается на всех окнах и меню, на которых должно отображаться имя пользователя. Для того чтобы изменить рисунок для учётной записи пользователя, необходимо сделать следующее:

1. Нажать на кнопку «Пуск» для открытия меню, открыть «Панель управления» и из списка компонентов панели управления выбрать «Учётные записи пользователей».
2. Выбрать свою учётную запись и нажать на ссылку «Изменение своего рисунка».
3. В диалоговом окне «Выберите новый рисунок для своей учётной записи» можно:

– выбрать понравившийся рисунок и нажать на кнопку «Изменение рисунка»;

– выбрать рисунок на своем компьютере. Для этого нужно нажать на ссылку «Поиск других рисунков». В диалоговом окне «Открыть», передвигаясь по дереву каталогов, следует открыть папку, содержащую нужный файл. По умолчанию в диалоговом окне будут выведены файлы с расширениями ***.bmp**, ***.gif**, ***.jpeg** и ***.png**. После того, как нужный документ будет найден, нужно его выделить, щёлкнув на нем левой кнопкой мыши, что поместит его имя в строку для ввода имени файла и нажать на кнопку «Открыть».

Установка родительского контроля

В том случае, если дети имеют доступ к компьютеру, нужно постараться ограничить им доступ для использования содержимого компьютера, а так же приложений, установленных на компьютере. Можно назначить интервалы времени, в течение которых дети могут пользоваться компьютером, а также определить, какими играми и программами они могут пользоваться.

При блокировании родительским контролем доступа к игре или программе появляется уведомление, что программа была заблокирована. Ребенок может щёлкнуть ссылку в уведомлении, чтобы запросить разрешение на доступ к игре или программе. Вы можете разрешить доступ, введя данные своей учётной записи.

Для настройки родительского контроля необходимо выполнить следующие действия:

1. Нажать на кнопку «Пуск» для открытия меню, открыть «Панель управления» и из списка компонентов панели управления выбрать «Учётные записи пользователей».
2. Создать для ребенка учётную запись, к которой будет применяться родительский контроль.
3. Перейти по ссылке «Управление другой учётной записью» и в диалоге «Выберите учётную запись для изменения» нажать на ссылку «Установить родительский контроль».
4. Далее выбрать ту учётную запись, к которой будет применяться родительский контроль.
5. Применить необходимые настройки для выбранной учётной записи.

Изменение типа учётной записи

После установки операционной системы, созданная учётная запись по умолчанию наделена административными правами. Эта учётная запись позволяет настраивать компьютер и устанавливать любые программы. После окончания настройки компьютера для повседневной работы компания Майкрософт настоятельно рекомендует использовать учётную запись без административных привилегий. Новые учётные записи пользователя следует создавать как обычные учётные записи. Использование обычных учётных записей более безопасно для компьютера. Для изменения типа учётной записи необходимо:

1. Нажать на кнопку «Пуск» для открытия меню, открыть «Панель управления» и из списка компонентов панели управления выбрать «Учётные записи пользователей».

2. Создать учётную запись с правами администратора, а затем выбрать свою учётную запись и перейти по ссылке «Изменение типа своей учётной записи».

3. Выбрать нужный тип учётной записи и нажать на кнопку «Изменение типа учётной записи».

Удаление учётной записи

Практическое задание №5

Если возникает необходимость в удалении учётной записи пользователя, то можно выполнить следующие действия:

1. Нажать на кнопку «Пуск» для открытия меню, открыть «Панель управления» и из списка компонентов панели управления выбрать «Учётные записи пользователей».

2. Выбрать учётную запись, которую нужно удалить.

3. В диалоге «Внесение изменений в учётную запись Имя_Пользователя» нажать на ссылку «Удаление учётной записи».

4. В появившемся диалоговом окне нажать на кнопку «Удалить файлы» или на кнопку «Сохранение файлов», если необходимо сохранить информацию удаляемого пользователя.

Включение и отключение гостевой учётной записи

Пользователи, которые заходят на компьютер под учётной записью гостя, получают временный профиль, который создаётся при входе пользователя в систему и удаляется при выходе из неё. Для того чтобы включить эту учётную запись необходимо:

1. Нажать на кнопку «Пуск» для открытия меню, откройте «Панель управления» и из списка компонентов панели управления выбрать «Учётные записи пользователей».

2. Нажать на ссылку «Управление другой учётной записью».

3. В диалоге «Выберите учётную запись для изменения» нажать левой кнопкой мыши на учётной записи «Гость».

4. В диалоговом окне «Включить учётную запись гостя?» нажать на кнопку «Включить».

Операции с учётными записями при помощи оснастки «Локальные пользователи и группы»

Как говорилось в первой части, использование оснастки «Локальные пользователи и группы» позволяет ограничить возможные действия пользователей и групп при помощи назначения им прав и разрешений. При помощи этой оснастки можно выполнять такие действия, как:

- сброс пароля пользователя;
- отключение учётной записи пользователя;
- удаление учётной записи;
- изменение имени;
- назначение сценариев входа;
- назначение домашней папки.

Далее подробно рассмотрена каждая из перечисленных операций.

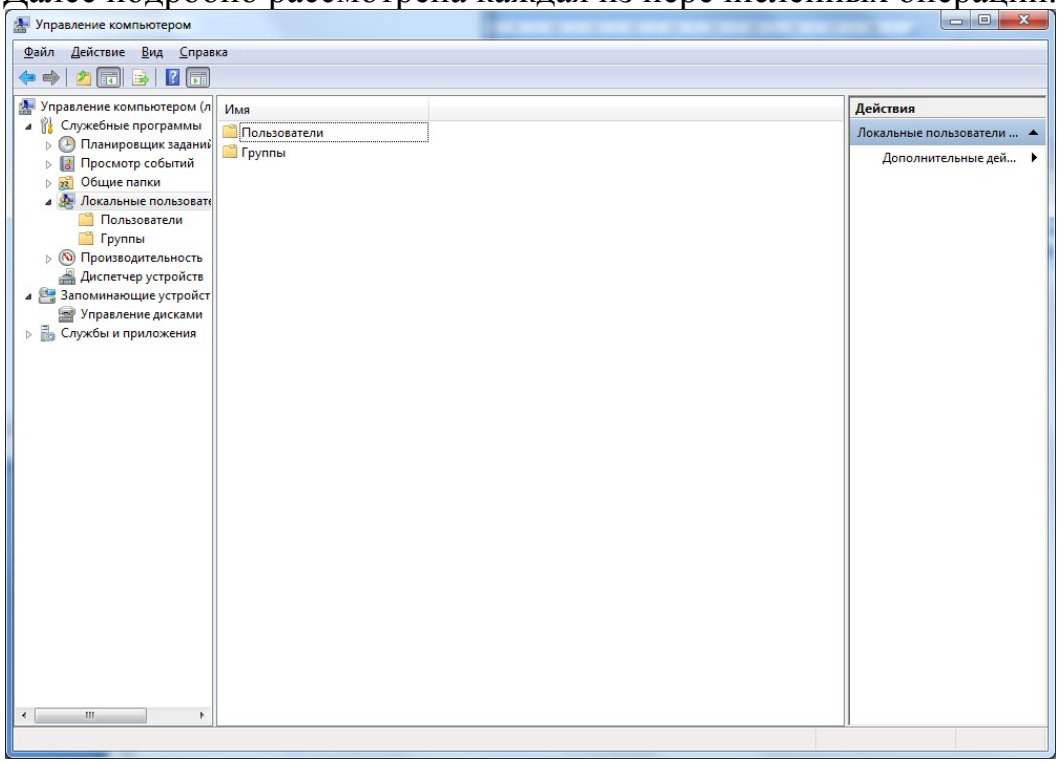

Рисунок 2 – Оснастка «Локальные пользователи и группы»

Сброс пароля пользователя

Прежде всего, не стоит забывать, что сброс пароля для локальной учётной записи пользователя может привести к частичной потере данных этого пользователя в случае, если у него имелись зашифрованные данные или альтернативные пароли Интернета. Для того чтобы сбросить пароль пользователя, необходимо сделать следующее:

1. Открыть оснастку «Локальные пользователи и группы».
2. Открыть узел «Пользователи».

3. Нажать правой кнопкой мыши на учётной записи пользователя, для которого нужно сменить пароль, а потом выбрать из контекстного меню команду «Задать пароль».

4. В появившемся диалоге «Установка пароля для Имя_пользователя» прочитать сообщение, предупреждающее о последствиях сброса пароля и нажать на кнопку «Продолжить».

5. Далее, в диалоговом окне «Установка пароля для Имя_пользователя» ввести пароль для данной учётной записи, а затем продублировать его в поле «Подтверждение», после чего нажать на кнопку «ОК».

Отключение или активация

При отключении учётной записи, пользователю запрещается вход в систему. В области сведений оснастки «Локальные пользователи и группы» значок отключенной учётной записи отображается со значком стрелочки. При активации учётной записи, пользователь снова получает возможность обычного входа в систему. Для того чтобы отключить учётную запись пользователя необходимо выполнить следующие действия:

1. Открыть оснастку «Локальные пользователи и группы»;
2. Открыть узел «Пользователи»;
3. Нажать правой кнопкой мыши на учётной записи пользователя, которую нужно отключить, а потом выбрать из контекстного меню команду «Свойства»;
4. Для того чтобы отключить выбранную учётную запись пользователя, установить флажок на опции «Отключить учётную запись».

Для того чтобы заново активировать учётную запись, нужно снять флажок «Отключить учётную запись».

Удаление учётной записи

Если возникает необходимость в удалении учётной записи пользователя, то компания Майкрософт рекомендует сначала отключить эту учётную запись. В том случае, если при отключении не возникло никаких ошибок, то её можно безопасно удалять. После удаления учётную запись восстановить невозможно. Для того чтобы удалить учётную запись необходимо:

1. Открыть оснастку «Локальные пользователи и группы».
2. Открыть узел «Пользователи».
3. Нажать правой кнопкой мыши на учётной записи пользователя, которую нужно удалить, а потом выбрать из контекстного меню команду «Удалить».

Изменение имени

Можно не волноваться за целостность данных при изменении имени пользователя. Поскольку идентификаторы безопасности (SID) учётных записей сохраняются, переименованная учётная запись сохраняет все остальные свойства, в том числе описание, пароль, принадлежность к группам, профиль пользователя, данные учётной записи, а также все разрешения и права пользователя. Для того чтобы переименовать учётную запись пользователя нужно сделать следующее:

1. Открыть оснастку «Локальные пользователи и группы».
2. Открыть узел «Пользователи».
3. Нажать правой кнопкой мыши на учётной записи пользователя, которую нужно переименовать, а потом выбрать из контекстного меню команду «Переименовать».

Назначение сценария входа

Системные администраторы могут использовать сценарии входа для назначения задач, которые будут автоматически выполнены при входе пользователя на определённый компьютер в системе. Эти сценарии используют системные переменные среды и могут также вызывать другие сценарии или исполняемые программы. Сценарии входа часто используются для подключения системных дисков, запуска процессов в фоновом режиме и задания пользовательских переменных среды.

Сценарий входа исполняется автоматически при входе пользователя на компьютер, работающий под управлением операционной системы семейства Windows. Сценарий может содержать команды операционной системы, например команды подключения сетевых дисков или запуска программ. Сценарии входа также содержат переменные среды для указания сведений, таких как путь для поиска файлов и расположение каталога для временных файлов. Как правило, сценарий входа в систему представляет собой пакетный файл (с расширением .bat или .cmd), но допускается использование и любой исполняемой программы.

Сценарии входа являются необязательными. Их можно использовать для настройки рабочей среды посредством создания сетевых подключений и запуска программ. Сценарии входа применяются тогда, когда требуется повлиять на некоторые параметры рабочей среды пользователя, не управляя всеми её аспектами.

Сценарии входа, размещенные на локальном компьютере, применяются только к пользователям, входящим в систему с данного локального компьютера. Локальные сценарии входа должны размещаться в общей папке или в подпапке общей папки с именем Netlogon. Если этой папки по умолчанию не существует, необходимо её создать. Чтобы указать сценарий входа, размещенный в подпапке папки Netlogon, перед именем файла укажите относительный путь к этой папке. Например, чтобы назначить сценарий входа Start.bat, сохраненный в папке \\ИмяКомпьютера\Netlogon\ИмяПапки локального пользователя, в поле «Сценарий входа» введите ИмяПапки\ Start.bat. Для того чтобы назначить сценарий входа для учётной записи пользователя, необходимо:

1. Открыть оснастку «Локальные пользователи и группы».
2. Открыть узел «Пользователи».
3. Нажать правой кнопкой мыши на учётной записи пользователя, которой нужно назначить сценарий входа, а потом выбрать из контекстного меню команду «Свойства».
4. Перейти на вкладку «Профиль» и там, в поле «Сценарий входа» нужно указать имя и относительный путь файла сценария.

Назначение домашней папки

Если домашняя папка не назначена, система назначает учётной записи пользователя локальную домашнюю папку по умолчанию (в корневой папке, где установлены файлы операционной системы). Чтобы указать для домашней папки сетевой путь, необходимо предварительно создать общий ресурс и задать разрешения позволяющие открыть доступ пользователям. Папка **«Документы»** представляет собой удобную альтернативу домашним папкам, но не заменяет их. На загрузочном томе создаются папки «Документы» для каждого пользователя. Для того чтобы указать домашнюю папку на локальном или сетевом ресурсе, нужно выполнить следующие действия:

1. Открыть оснастку «Локальные пользователи и группы».
2. Открыть узел «Пользователи».
3. Нажать правой кнопкой мыши на учётной записи пользователя, домашнюю папку которой нужно переназначить, а потом выбрать из контекстного меню команду «Свойства».
4. Перейти на вкладку «Профиль».
5. Указать домашнюю папку для пользователя:

- для того чтобы указать локальную домашнюю папку, в поле «Путь» ввести путь к папке на локальном компьютере;
- для того чтобы указать домашнюю папку на сетевом ресурсе, установить переключатель на опции «Подключить», указать букву диска и выбрать сетевой ресурс.

Локальные политики

Оснастка «Локальная политика безопасности» (рисунок 3) используется для изменения политики учётных записей и локальной политики на локальном компьютере, а политики учётных записей, привязанных к домену Active Directory можно настраивать при помощи оснастки «Редактор управления групповыми политиками».

Практическое задание №6

Запустить консоль можно несколькими способами:

1. Нажать на кнопку «Пуск» для открытия меню, в поле поиска ввести «Локальная политика безопасности» и открыть приложение в найденных результатах.
2. Воспользоваться комбинацией клавиш +R для открытия диалога «Выполнить». В диалоговом окне «Выполнить», в поле «Открыть» ввести secpol.msc и нажать на кнопку «ОК».
3. Открыть «Консоль управления ММС». Для этого нажать на кнопку «Пуск», в поле поиска ввести «mmc», а затем нажать на кнопку «Enter». Откроется пустая консоль ММС. В меню «Консоль» выбрать команду «Добавить или удалить оснастку» или воспользоваться комбинацией клавиш Ctrl+M. В диалоге «Добавление и удаление оснасток» выбрать оснастку «Редактор локальной групповой политики» и нажать на кнопку «Добавить». В появившемся диалоге «Выбор объекта групповой политики» нажать на кнопку «Обзор» для выбора компьютера или нажать на кнопку «Готово» (по умолчанию установлен объект «Локальный компьютер»). В диалоге «Добавление или удаление оснасток» нажать на кнопку «ОК». В оснастке «Редактор локальной групповой политики» перейти в узел «Конфигурация компьютера», а затем открыть узел «Параметры безопасности».

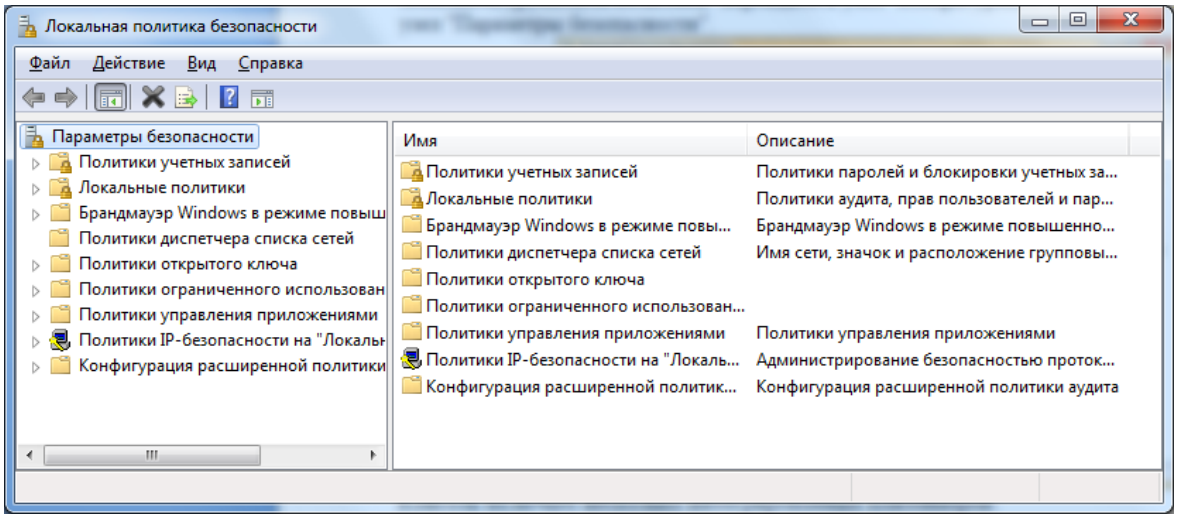

Рисунок 3 – Консоль «локальная политика безопасности»

Консоль включает несколько интегрированных контейнеров:

- «Политики учётных записей»;

- «Локальные политики»;
- «Брандмауэр Windows в режиме повышенной безопасности»;
- «Политики диспетчера списка сетей»;
- «Политики открытого ключа»;
- «Политики ограниченного использования программ»;
- «Политики управления приложениями»;
- «Политики безопасности IP на «Локальный компьютер»;
- «Конфигурация расширенной политики аудита».

Каждый контейнер включает свои интегрированные компоненты.

Политики учётных записей. Политика паролей

При помощи этого узла возможно изменение настроек паролей учётных записей пользователей, которые состоят как в домене, так и в рабочих группах. В организациях можно применять одинаковые политики паролей для всех пользователей, входящих в домен или только для отдельных групп при помощи оснастки **«Консоль управления групповыми политиками»**.

В узле **«Политика паролей»** доступно использование до шести политик безопасности, при помощи которых можно указать наиболее важные параметры безопасности, применяемые для управления паролями учётных записей. Если правильно настроить все шесть политик безопасности, расположенных в этом узле, безопасность паролей пользователей организации значительно повысится. Применив все политики, пользователям действительно придется создавать безопасные пароли, в отличие от тех, которые они считают «сложными». Доступны следующие политики безопасности:

Вести журнал паролей. Насколько не был бы ваш пароль безопасным, злоумышленник рано или поздно сможет его подобрать. Поэтому необходимо периодически изменять пароли учётных записей. При помощи этой политики можно указать количество новых паролей, которые назначаются для учётных записей до повторного использования старого пароля. После того как эта политика будет настроена, контроллер домена будет проверять кэш предыдущих хэш-кодов пользователей, чтобы в качестве нового пароля пользователи не могли использовать старый. Число паролей может варьироваться от 0 до 24. Т.е., если в качестве параметра указано число 24, то пользователь сможет использовать старый пароль с 25-ого раза.

Максимальные срок действия пароля. Эта политика указывает период времени, в течение которого пользователь может использовать свой пароль до последующего изменения. По окончанию установленного срока пользователь обязан изменить свой пароль, так как без изменения пароля войти в систему ему не удастся. Доступные значения могут быть установлены в промежутке от 0 до 999 дней. Если установлено значения равное 0, срок действия пароля неограничен. В связи с мерами безопасности желательно отказаться от такого выбора. Если значения максимального срока действия пароля варьируется от 1 до 999 дней, значение минимального срока должно быть меньше максимального. Лучше всего использовать значения от 30 до 45 дней.

Минимальная длина пароля. При помощи этой политики можно указать минимальное количество знаков, которое должно содержаться в пароле. Если активировать этот параметр, то при вводе нового пароля количество знаков будет сравниваться с тем, которое установлено в этой политике. Если количество знаков будет меньше указанного, то придется изменить пароль в соответствии с политикой безопасности. Можно указать значение политики от 1 до 14 знаков. Оптимальным значением для количества знаков для пароля пользователей является 8, а для серверов от 10 до 12.

Минимальные срок действия пароля. Многие пользователи не захотят утруждать себя запоминанием нового сложного пароля и могут попробовать сразу при вводе изменить такое количество новых паролей, чтобы использовать свой хорошо известный первоначальный пароль. Для предотвращения подобных действий была разработана текущая политика безопасности. Можно указать минимальное количество дней, в течение которого пользователь должен использовать свой новый пароль. Доступные значения этой политики устанавливаются в промежутке от 0 до 998 дней. Установив значение равное 0 дней, пользователь сможет изменить пароль сразу после создания нового. Необходимо обратить внимание на то, что минимальный срок действия нового пароля не должен превышать значение максимального срока действия.

Пароль должен отвечать требованиям сложности. Это одна из самых важных политик паролей, которая отвечает за то, должен ли пароль соответствовать требованиям сложности при создании или изменении пароля. В связи с этими требованиями, пароли должны:

- содержать буквы верхнего и нижнего регистра одновременно;
- содержать цифры от 0 до 9;
- содержать символы, которые отличаются от букв и цифр (например, !, @, #, $, *);
- не содержать имени учётной записи пользователя или частей полного имени пользователя длиной более двух рядом стоящих знаков.

В том случае, если пользователь создал или изменил пароль, который соответствует требованиям, то пароль пропускается через математический алгоритм, преобразовывающий его в хэш-код (также называемый односторонней функцией), о котором шла речь в политике **«Вести журнал паролей».**

Хранить пароли, используя обратимое шифрование. Для того чтобы пароли невозможно было перехватить при помощи приложений, Active Directory хранит только хэш-код. Но если перед вами встанет необходимость поддержки приложений, использующих протоколы, требующие знание пароля пользователя для проверки подлинности, можно использовать текущую политику. Обратимое шифрование по умолчанию отключено, так как, используя эту политику, уровень безопасности паролей и всего домена в частности значительно понижается. Использование этой функции аналогично хранению пароля в открытом виде.

Политика блокировки учётной записи

Даже после создания сложного пароля и правильной настройки политик безопасности, учётные записи пользователей могут быть подвергнуты атакам недоброжелателей. Например, если установлен минимальный срок действия пароля в 20 дней, у хакера достаточно времени для подбора пароля к учётной записи. Узнать имя учётной записи не является проблемой для хакеров, так как, зачастую имена учётных записей пользователей совпадает с именем адреса почтового ящика. А если будет известно имя, то для подбора пароля понадобится две-три недели.

Групповые политики безопасности Windows могут противостоять таким действиям, используя набор политик узла «Политика блокировки учётной записи». При помощи данного набора политик возможно ограничение количества некорректных попыток входа пользователя в систему. Для этого узла доступны только три политики, которые рассматриваются ниже.

Время до сброса счетчиков блокировки. Active Directory и групповые политики позволяют автоматически разблокировать учётную запись, количество попыток входа в которую превышает установленное вами пороговое значение. При помощи этой политики устанавливается количество минут, которые должны пройти после неудачной попытки для автоматической разблокировки. Разрешается устанавливать значение от одной минуты до 99999. Это значение должно быть меньше значения политики **«Продолжительность блокировки учётной записи»**.

Пороговое значение блокировки. Используя эту политику, можно указать количество некорректных попыток входа, после чего учётная запись будет заблокирована. Окончание периода блокировки учётной записи задается политикой **«Продолжительность блокировки учётной записи»** или администратор может разблокировать учётную запись вручную. Количество неудачных попыток входа может варьироваться от 0 до 999. Рекомендуется устанавливать допустимое количество от трех до семи попыток.

Продолжительность блокировки учётной записи. При помощи этого параметра можно указать время, в течение которого учётная запись будет заблокирована до её автоматической разблокировки. Можно установить значение от 0 до 99999 минут. В том случае, если значение этой политики будет равно 0, учётная запись будет заблокирована до тех пор, пока администратор не разблокирует её вручную.

Политика Kerberos

В доменах Active Directory для проверки подлинности учётных записей пользователей и компьютеров домена используется протокол Kerberos. Сразу после аутентификации пользователя или компьютера, этот протокол проверяет подлинность указанных реквизитов, а затем выдает особый пакет данных, который называется **«Билет предоставления билета (TGT – Ticket Granting Ticket)»**. Перед подключением пользователя к серверу для запроса документа на контроллер домена пересылается запрос вместе с билетом TGT, который идентифицирует пользователя, прошедшего проверку подлинности Kerberos. После этого контроллер домена передает пользователю другой пакет данных, называемый билетом доступа к службе. Пользователь предоставляет билет на доступ службе на сервере, который принимает его как подтверждение прохождения проверки подлинности.

Данный узел можно обнаружить только на контроллерах домена. Доступны следующие пять политик безопасности:

Максимальная погрешность синхронизации часов компьютера. Для предотвращения «атак повторной передачи пакетов» существует текущая политика безопасности, которая определяет максимальную разность времени, допускающую Kerberos между временем клиента и временем на контроллере домена для обеспечения проверки подлинности. В случае установки данной политики, на обоих часах должны быть установлены одинаковые дата и время. Подлинной считается та отметка времени, которая используется на обоих компьютерах, если разница между часами клиентского компьютера и контроллера домена меньше максимальной разницы времени, определённой этой политикой.

Максимальный срок жизни билета пользователя. При помощи текущей политики можно указать максимальный интервал времени, в течение которого может быть использован билет представления билета (TGT). По истечении срока действия билета TGT необходимо возобновить существующий билет или запросить новый.

Максимальный срок жизни билета службы. Используя эту политику безопасности, сервер будет выдавать сообщение об ошибке в том случае, если клиент, запрашивающий подключение к серверу, предъявляет просроченный билет сеанса. Можно определить максимальное количество минут, в течение которого полученный билет сеанса разрешается использовать для доступа к конкретной службе. Билеты сеансов применяются только для проверки подлинности на новых подключениях к серверам. После того как подключение пройдет проверку подлинности, срок действия билета теряет смысл.

Максимальный срок жизни для возобновления билета пользователя. С помощью данной политики можно установить количество дней, в течение которых может быть восстановлен билет предоставления билета.

Принудительные ограничения входа пользователей. Эта политика позволяет определить, должен ли центр распределения ключей Kerberos проверять каждый запрос билета сеанса на соответствие политике прав, действующей для учётных записей пользователей.

Практическое задание №7

1. Запустить консоль «Локальные политика безопасности», перейти к настройке «Политике учётных записей».
2. Перейти к пункту «Пороговое значение блокировки» в «Политике блокировки учётной записи», установить параметр равный 3 попыткам.
3. Перейти к пункту «Минимальная длина пароля» в «Политике паролей», установить значение 10.
4. Перейти к пункту «Пароль должен отвечать требованиям сложности», поставить галочку.

Длина пароля может достигать 128 знаков. Маленький отрывок из поэмы А.С.Пушкина «Руслан и Людмила» со всеми знаками препинания, набранный русскими буквами в латинской раскладке и установленный в качестве пароля, может привести в замешательство любого взломщика: E kerjvjhmz le, ptktysq, Pkfnfz wtgm yf le,t njv, B lytv b yjxm. Rjn extysq, Dct [jlbn gj wtgb rheujv/. Этот пароль надежный, а запомнить его очень просто: «У лукоморья дуб зеленый, златая цепь на дубе том, и днём и ночью кот учёный, всё ходит по цепи кругом».

Кроме того, специалистами были разработаны рекомендации по созданию усиленных паролей, использование которых уменьшает вероятность успешной атаки взломщика:

– пароль должен содержать не менее 6 символов, и среди них должны быть символы по крайней мере трех типов из следующих четырех: заглавные буквы, строчные буквы, цифры и специальные символы (то есть ,%,*,&,!)

– пароль не может включать учётное имя пользователя;

– если пользователь создаёт пароль, который не отвечает перечисленным требованиям, операционная система выдает сообщение об ошибке и не принимает пароль.

5. Проверить действие установленных настроек.

Политика аудита

В процессе аудита используются три средства управления: политика аудита, параметры аудита в объектах, а также журнал «Безопасность», куда заносятся события, связанные с безопасностью, такие как вход/выход из системы, использование привилегий и обращение к ресурсам.

Политика аудита настраивает в системе определённого пользователя и группы аудит активности. Для того чтобы отконфигурировать политики аудита, в редакторе управления групповыми политиками необходимо открыть узел «Конфигурация компьютера/Конфигурация Windows/Параметры безопасности/Локальные политики /Политика аудита». Необходимо помнить, что по умолчанию параметр политики аудита, для рабочих станций установлен на «Не определено». В общей сложности, возможна настройка девяти политик аудита.

Так же, как и с остальными политиками безопасности, для настройки аудита нужно определить параметр политики. После двойного нажатия левой кнопкой мыши на любом из параметров, установите флажок на опции «Определить следующие параметры политики» и укажите параметры ведения аудита успеха, отказа или обоих типов событий.

После настройки политики аудита события будут заноситься в журнал безопасности. Просмотреть эти события можно в журнале безопасности.

Аудит входа в систему. Текущая политика определяет, будет ли операционная система пользователя, для компьютера которого применяется данная политика аудита, выполнять аудит каждой попытки входа пользователя в систему или выхода из неё. Например, при удачном входе пользователя на компьютер генерируется событие входа учётной записи. События выхода из системы создаются каждый раз, когда завершается сеанс вошедшей в систему учётной записи пользователя. Аудит успехов означает создание записи аудита для каждой успешной попытки входа в систему. Аудит отказов означает создание записи аудита для каждой неудачной попытки входа в систему.

Аудит доступа к объектам. Данная политика безопасности выполняет аудит попыток доступа пользователей к объектам, которые не имеют отношения к Active Directory. К таким объектам можно отнести файлы, папки, принтеры, разделы системного реестра, которые задаются собственными списками в системном списке управления доступом (SACL). Аудит создаётся только для объектов, для которых указаны списки управления доступом, при условии, что запрашиваемый тип доступа и учётная запись, выполняющая запрос, соответствуют параметрам в данных списках.

Аудит доступа к службе каталогов. При помощи этой политики безопасности можно определить, будет ли выполняться аудит событий, указанных в системном списке контроля доступа (SACL), который можно редактировать в диалоговом окне «Дополнительные параметры безопасности» свойств объекта Active Directory. Аудит создаётся только для объектов, для которых указан системный список управления доступом, при условии, что запрашиваемый тип доступа и учётная запись, выполняющая запрос, соответствуют параметрам в данном списке. Данная политика в какой-то степени похожа на политику **«Аудит доступа к объектам»**. Аудит успехов означает создание записи аудита при каждом успешном доступе пользователя к объекту Active Directory, для которого определена таблица SACL. Аудит отказов означает создание записи аудита при каждой неудачной попытке доступа пользователя к объекту Active Directory, для которого определена таблица SACL.

Аудит изменения политики. Эта политика аудита указывает, будет ли операционная система выполнять аудит каждой попытки изменения политики назначения прав пользователям, аудита, учётной записи или доверия. Аудит успехов означает создание записи аудита при каждом успешном изменении политик назначения прав пользователей, политик аудита или политик доверительных отношений. Аудит отказов означает создание записи аудита при каждой неудачной попытке изменения политик назначения прав пользователей, политик аудита или политик доверительных отношений.

Аудит изменения привилегий. Используя эту политику безопасности, можно определить, будет ли выполняться аудит использования привилегий и прав пользователей. Аудит успехов означает создание записи аудита для каждого успешного применения права пользователя. Аудит отказов означает создание записи аудита для каждого неудачного применения права пользователя.

Аудит отслеживания процессов. Текущая политика аудита определяет, будет ли операционная система выполнять аудит событий, связанных с процессами, такими как создание и завершение процессов, а также активация программ и непрямой доступ к объектам. Аудит успехов означает создание записи аудита для каждого успешного события, связанного с отслеживаемым процессом. Аудит отказов означает создание записи аудита для каждого неудачного события, связанного с отслеживаемым процессом.

Аудит системных событий. Данная политика безопасности имеет особую ценность, так как именно при помощи этой политики можно узнать, перегружался ли у пользователя компьютер, превысил ли размер журнала безопасности пороговое значение предупреждений, была ли потеря отслеженных событий из-за сбоя системы аудита и даже вносились ли изменения, которые могли повлиять на безопасность системы или журнала безопасности вплоть до изменения системного времени. Аудит успехов означает создание записи аудита для каждого успешного системного события. Аудит отказов означает создание записи аудита для каждого неудачного завершения системного события.

Аудит событий входа в систему. При помощи этой политики аудита можно указать, будет ли операционная система выполнять аудит каждый раз при проверке данным компьютером учётных данных. При использовании этой политики создаётся событие для локального и удаленного входа пользователя в систему. Члены домена и компьютеры, не входящие в домен, являются доверенными для своих локальных учётных записей. Когда пользователь пытается подключиться к общей папке на сервере, в журнал безопасности записывается событие удалённого входа (события выхода из системы не записываются). Аудит успехов означает создание записи аудита для каждой успешной попытки входа в систему. Аудит отказов означает создание записи аудита для каждой неудачной попытки входа в систему.

Аудит управления учётными записями. Эта последняя политика тоже считается очень важной, так как именно при помощи неё можно определить, необходимо ли выполнять аудит каждого события управления учётными записями на компьютере. В журнал безопасности будут записываться такие действия как создание, перемещение и отключение учётных записей, а также изменение паролей и групп. Аудит успехов означает создание записи аудита для каждого успешного события управления учётными записями. Аудит отказов означает создание записи аудита для каждого неудачного события управления учётными записями

Политики назначения прав пользователей

Как говорилось выше, для назначения прав пользователей существует 44 политики безопасности. Далее можно ознакомиться с восемнадцатью политиками безопасности, которые отвечают за назначение различных прав для пользователей или групп вашей организации.

1. **Архивация файлов и каталогов**. При помощи данной политики можно указать пользователей или группы, предназначенные для выполнения операций резервного копирования файлов, каталогов, разделов реестра и других объектов, которые подлежат архивации. Данная политика предоставляет доступ для следующих разрешений:

- обзор папок/выполнение файлов;
- содержимое папки/чтение данных;
- чтение атрибутов;
- чтение расширенных атрибутов;
- чтение разрешений.

На рабочих станциях и серверах данные привилегии предоставляются группам «Администраторы» и «Операторы архивации», а на контроллерах домена – «Операторы архивации» и «Операторы сервера».

2. **Блокировка страниц в памяти**. Используя эту политику безопасности, можно указать конкретных пользователей или группы, которым разрешается использовать процессы для сохранения данных в физической памяти для предотвращения сброса данных в виртуальную память на диске.

По умолчанию, как на рабочих станциях, так и на серверах, ни у одной группы нет на это разрешений.

3. **Восстановление файлов и каталогов**. Эта политика позволяет указывать пользователей и группы, которые могут выполнять восстановление файлов и каталогов, в обход блокировке файлов, каталогов, разделов реестра и прочих объектов, расположенных в архивных версиях файлов.

На рабочих станциях и серверах данные привилегии предоставляются группам «Администраторы» и «Операторы архивации», а на контроллерах домена – «Операторы архивации» и «Операторы сервера».

4. **Вход в качестве пакетного задания**. При создании задания, используя планировщик заданий, операционная система регистрирует пользователя в системе как пользователя с пакетным входом. Данная политика разрешает группе или определённому пользователю входить в систему при помощи такого метода.

По умолчанию, как на рабочих станциях, так и на контроллерах домена, данные привилегии предоставляются группам «Администраторы» и «Операторы архивации».

5. **Вход в качестве службы**. Некоторые системные службы осуществляют вход в операционную систему под разными учётными записями. Например, служба «Windows Audio» запускается под учётной записью «Локальная служба», служба «Телефония» использует учётную запись «Сетевая служба». Данная политика безопасности определяет, какие учётные записи служб могут зарегистрировать процесс в качестве службы.

По умолчанию, как на рабочих станциях, так и на серверах, ни у одной группы нет на это разрешений.

6. **Выполнение задач по обслуживанию томов**. Используя эту политику, можно указать пользователей или группы, участники которых могут выполнять операции, предназначенные для обслуживания томов. У пользователей, обладающих такими привилегиями, есть права на чтение и изменение запрошенных данных после открытия дополнительных файлов, они также могут просматривать диски и добавлять файлы в память, занятую другими данными.

По умолчанию, такими правами обладают только администраторы рабочих станций и контроллеров домена.

7. **Добавление рабочих станций к домену**. Эта политика отвечает за разрешение пользователям или группам добавлять компьютеры в домен Active Directory. Пользователь, обладающий данными привилегиями, может добавить в домен до десяти компьютеров.

По умолчанию, все пользователи, прошедшие проверку подлинности, на контроллерах домена могут добавлять до десяти компьютеров.

8. **Доступ к диспетчеру учётных данных от имени доверенного вызывающего**. Диспетчер учётных данных – это компонент, который предназначен для хранения учётных данных, таких как имена пользователей и пароли, используемых для входа на веб-сайты или другие компьютеры в сети. Эта политика используется диспетчером учётных данных в ходе архивации и восстановления, и её не желательно предоставлять пользователям.

По умолчанию, как на рабочих станциях, так и на серверах, ни у одной группы нет на это разрешений.

9. **Доступ к компьютеру из сети**. Данная политика безопасности отвечает за разрешение подключения к компьютеру по сети указанным пользователям или группам.

На рабочих станциях и серверах данные привилегии предоставляются группам «Администраторы» и «Операторы архивации», «Пользователи» и «Все». На контроллерах домена – «Администраторы», «Проверенные пользователи», «Контроллеры домена предприятия» и «Все».

10. **Завершение работы системы**. Используя этот параметр политики, можно составить список пользователей, которые имеют право на использование команды «Завершение работы» после удачного входа в систему.

На рабочих станциях и серверах данные привилегии предоставляются группам «Администраторы», «Операторы архивации» и «Пользователи» (только на рабочих станциях), а на контроллерах домена – «Администраторы», «Операторы архивации», «Операторы сервера» и «Операторы печати».

11. **Загрузка и выгрузка драйверов устройств**. При помощи текущей политики можно указать пользователей, которым будут предоставлены права на динамическую загрузку и выгрузку драйверов устройств в режиме ядра.

Эта политика не распространяется на PnP-устройства. **Plug and Play** – технология, предназначенная для быстрого определения и конфигурирования устройств в компьютере и других технических устройствах. Разработана фирмой Microsoft при содействии других компаний. Технология PnP основана на использовании объектно-ориентированной архитектуры, ее объектами являются внешние устройства и программы. Операционная система автоматически распознает объекты и вносит изменения в конфигурацию абонентской системы.).

На рабочих станциях и серверах данные привилегии предоставляются группам «Администраторы», а на контроллерах домена – «Администраторы» и «Операторы печати».

12. **Замена маркера уровня процесса**. Используя данную политику безопасности, можно ограничить пользователей или группу от использования API-функции CreateProcessAsUser для того, чтобы одна служба могла запускать другую функцию, процесс или службу. Стоит обратить внимание на то, что такое приложение как «Планировщик заданий» для своей работы использует данные привилегии.

По умолчанию, как на рабочих станциях, так и на контроллерах домена, данные привилегии предоставляются учётным записям «Сетевая служба» и «Локальная служба».

13. **Запретить вход в систему через службу удалённых рабочих столов**. При помощи данной политики безопасности можно ограничить пользователей или группы от входа в систему в качестве клиента удалённых рабочих столов.

По умолчанию, как на рабочих станциях, так и на серверах, всем разрешено входить в систему как клиенту удалённых рабочих столов.

14. **Запретить локальный вход**. Данная политика запрещает отдельным пользователям или группам выполнять вход в систему.

По умолчанию всем пользователям разрешен вход в систему.

15. **Изменение метки объектов**. Благодаря данной политике назначения прав, можно предоставить возможность указанным пользователям или группам изменять метки целостности объектов других пользователей, таких как файлы, разделы реестра или процессы.

По умолчанию никому не разрешено изменять метки объектов.

16. **Изменение параметров среды изготовителя**. Используя эту политику безопасности, можно указать пользователей или группы, которым будет доступна возможность чтения переменных аппаратной среды. Переменные аппаратной среды – это параметры, сохраняемые в энергонезависимой памяти компьютеров, архитектура которых отлична от x86.

На рабочих станциях и контроллерах домена, по умолчанию данные привилегии предоставляются группам «Администраторы».

17. **Изменение системного времени**. Эта политика отвечает за изменение системного времени. Предоставив данное право пользователям или группам, тем самым кроме разрешения изменения даты и времени внутренних часов предоставляется возможность изменения соответствующего времени отслеживаемых событий в оснастке «Просмотр событий».

На рабочих станциях и серверах данные привилегии предоставляются группам «Администраторы» и «Локальная служба», а на контроллерах домена – «Администраторы», «Операторы сервера» и «Локальная служба».

18. **Изменение часового пояса**. При помощи текущей политики безопасности, можно указать пользователей или группы, которым разрешено изменять часовой пояс своего компьютера для отображения местного времени, которое представляет собой сумму системного времени компьютера и смещения часового пояса.

На рабочих станциях и контроллерах домена по умолчанию данные привилегии предоставляются группам «Администраторы» и «Пользователи».

Параметры безопасности

Узел «Параметры безопасности» позволяет администратору безопасности вручную настраивать уровни безопасности, назначенные политике локального компьютера. Чтобы изменить любое из значений шаблона, необходимо дважды щёлкнуть его. Появится диалоговое окно, позволяющее модифицировать значение.

Таким образом контролировать включение или отключение настроек безопасности, таких как цифровая подпись данных, имена учётных записей администратора и гостя, доступ к дисководам гибких и компакт-дисков, установка драйверов и приглашения на вход в систему и все остальные доступные параметры политики безопасности. Далее будут рассмотрены подробнее, какие параметры рекомендуется устанавливать для повышения защиты компьютера от различного рода атак по сети Интернет.

Первое – напоминать пользователям об истечении срока действия пароля – 14 дней (по умолчанию).

Рекомендуется включать политику «Не отображать последнего имени пользователя в диалоге входа» (по умолчанию – отключен). Особенно полезно в случае, когда рядовой пользователь имеет пароль аналогичный своему имени, и тогда без труда можно с нескольких переборов пароля хакеру проникнуть на этот компьютер.

Рекомендуется включать политику «Запретить пользователям установку драйвера принтера» (по умолчанию – отключен). А также рекомендуется включить политику «Очистка страничного файла виртуальной памяти» (по умолчанию – отключен). После этого система всегда при выключении компьютера будет удалять файл подкачки. Но здесь есть свой недостаток – система будет долго выключатся.

Следующая политика безопасности относится к состоянию окна CTRL+ALT+DEL при входе в систему. Эта политика по умолчанию не установлена. После перезагрузки при входе в систему на экране будет отображаться окно CTRL+ALT+DEL, которое по умолчанию не отображается.

Кроме этого, в целях безопасности полезно настраивать следующие параметры:

- «Автоматически отключать сеансы пользователей по истечении разрешённого времени» (Включить);
- «Длительность простоя перед отключением сеанса» (примерно 10 мин);
- «Дополнительные ограничения для анонимных подключений» (установить в значение «Нет доступа, без явного разрешения анонимного доступа»);
- «Использовать цифровую подпись со стороны клиента (Всегда)» (Включить);
- «Использовать цифровую подпись со стороны клиента (по возможности)» (Включить);
- «Использовать цифровую подпись со стороны сервера (Всегда)» (Включить);
- «Использовать цифровую подпись со стороны сервера (по возможности)» (Включить);
- «Разрешить доступ к дисководам компакт-дисков только локальным пользователям» (Включить);
- «Разрешить доступ к НГМД только локальным пользователям» (Включить).

Брандмауэр Windows в режиме повышенной безопасности

Брандмауэр Windows в режиме повышенной безопасности – это брандмауэр, регистрирующий состояние сети, для рабочих станций. В отличие от брандмауэров для маршрутизаторов, которые развёртывают на шлюзе между локальной сетью и Интернетом, брандмауэр Windows создан для работы на отдельных компьютерах. Он отслеживает только трафик рабочей станции: трафик, приходящий на IP-адрес данного компьютера, и исходящий трафик самого компьютера. Брандмауэр Windows в режиме повышенной безопасности выполняет следующие основные операции.

Входящий пакет проверяется и сравнивается со списком разрешённого трафика. Если пакет соответствует одному из значений списка, брандмауэр Windows передает пакет протоколу TCP/IP для дальнейшей обработки. Если пакет не соответствует ни одному из значений списка, брандмауэр Windows блокирует пакет, и в том случае, если включено протоколирование, создаёт запись в файле журнала.

Список разрешённого трафика формируется двумя путями:

– когда подключение, контролируемое брандмауэром Windows в режиме повышенной безопасности, отправляет пакет, брандмауэр создаёт значение в списке разрешающее прием ответного трафика. Для соответствующего входящего трафика потребуется дополнительное разрешение;

– когда создаётся разрешающее правило брандмауэра Windows в режиме повышенной безопасности. Трафик, для которого создано соответствующее правило, будет разрешён на компьютере с работающим брандмауэром Windows. Этот компьютер будет принимать явно разрешённый входящий трафик в режимах работы в качестве сервера, клиентского компьютера или узла одноранговой сети.

Первым шагом по решению проблем, связанных с Брандмауэром Windows, является проверка того, какой профиль является активным. Брандмауэр Windows в режиме повышенной безопасности является приложением, отслеживающим сетевое окружение. Профиль брандмауэра Windows меняется при изменении сетевого окружения. Профиль представляет собой набор настроек и правил, который применяется в зависимости от сетевого окружения и действующих сетевых подключений.

Основным нововведением в брандмауэре Windows 7 является одновременная работа нескольких сетевых профилей.

– «Общий» – публичные (общедоступные) сети, например, в кафе или аэропорт;

– «Частный» – домашние или рабочие сети;

– «Доменный» – доменная сеть в организации, определяемая автоматически.

В Windows Vista только один профиль мог быть активен в любой момент времени. Если было включено несколько профилей, наиболее безопасный из них становился активным. Например, при одновременном подключении к публичной и домашней сетям, активным становился общедоступный профиль, обеспечивающий более высокую безопасность. В Windows 7 все три профиля могут быть активны одновременно, обеспечивая соответствующий уровень безопасности для каждой сети.

Политики диспетчера списка сетей

Для того чтобы воспользоваться функционалом локальных политик безопасности, предназначенным для изменения политик списка сетей, необходимо открыть «Редактор управления групповыми политиками», в дереве консоли развернуть узел «Конфигурация компьютера\Политики\ Конфигурация Windows\Параметры безопасности\Политики диспетчера списка сетей».

В области сведений политик диспетчера списка сетей можно настраивать:

– сети, которые не удается идентифицировать из-за ошибок сети или отсутствия идентифицируемых признаков, называемых «Неопознанные сети»;

– временное состояние сетей, находящихся в процессе идентификации, которые называются «Идентификация сетей»;

– все сети, к которым подключен пользователь, называемое «Все сети»;

– а также текущее сетевое подключение (рабочая группа или домен).

Принудительное изменение названия сетей для пользователей, находящихся в домене

Как в рабочих группах, так и в доменах пользователи могут самостоятельно изменять имя сети. Для этого нужно выполнить следующие действия:

1. Открыть окно «Центр управления сетями и общим доступом»;
2. В группе «Просмотр активных сетей» щёлкнуть на значке сети, имя которой необходимо изменить;
3. В диалоговом окне «Настройка свойств сети», в текстовом поле «Сетевое имя» изменить имя сети.

Нужно сделать так, чтобы пользователи домена не могли изменить название сети в «Центре управления сетями и общим доступом». Для этого нужно выполнить следующие действия:

1. Так как действие этой групповой политики должно распространяться на все компьютеры этого домена, в оснастке «Управление групповой политикой», в дереве консоли, развернуть узел «Лес: имя домена\ Домены\имя домена» и выбрать объект групповой политики «Default Domain Policy»;
2. Нажать правой кнопкой мыши на этом объекте групповой политики и из контекстного меню выбрать команду «Изменить»;
3. В открывшейся оснастке «Редактор управления групповыми политиками» в дереве консоли развернуть узел «Конфигурация компьютера\ Политики\Конфигурация Windows\Параметры безопасности\Политики диспетчера списка сетей» и открыть политику «Все сети». В открывшемся окне политики безопасности, в группе «Имя сети» установить переключатель на опцию «Пользователь не может изменить имя» и нажать на «ОК»;
4. Открыть политику, именем которой назначено имя домена. На вкладке «Имя сети», в группе «Имя» установить переключатель на опцию «Имя» и указать название. В группе «Разрешёния пользователя» можно установить переключатель на опцию «Пользователь не может изменить имя», но в этом нет крайней необходимости, так как подобная операция была выполнена на предыдущем шаге для всех сетей компьютеров организации.
5. Закрыть «Редактор управления групповыми политиками» и, при необходимости, обновить политики конфигурации компьютера, используя команду ***GPUpdate /Target:Computer /force /boot*** в командной строке.

Принудительное изменение профиля брандмауэра Windows в неопознанных сетях

В последние годы всё больше пользователь используют мобильные компьютеры. Используя свои мобильные компьютеры, пользователи могут подключаться к сети Интернет даже находясь в кафе, аэропортах или просто сидя на скамейке в парке. Именно в таких случаях их компьютеры находятся под более существенным риском нападения злоумышленниками, нежели в корпоративной среде или у себя дома. Когда пользователь подключается к беспроводной сети, операционная система Windows автоматически определяет такую сеть как общедоступную. Для того чтобы настройки безопасности брандмауэра Windows применялись к компьютеру в зависимости от пользовательского места нахождения были разработаны профили брандмауэра. В том случае, если соединение проходит проверку подлинности на контроллере домена, то сеть классифицируется как тип доменного размещения сети. Если компьютер используется дома или в офисе – обычно применяется домашняя сеть с частным профилем брандмауэра. В местах общего пользования принято использовать общий профиль брандмауэра. Часто случается, что пользователи, находясь в общедоступных местах, пренебрегают этим средствам безопасности и для общедоступного профиля устанавливают частные профили брандмауэра.

Используя политики диспетчера списка сетей можно указать пользователю, какой профиль нужно использовать в случае неопознанных сетей, которые идентифицируются как «Общественная сеть». Для этого выполните следующие действия:

1. Открыть оснастку «Редактор локальной групповой политикой».
2. В открывшемся окне, в дереве оснастки, перейти в узел «Конфигурация компьютера\Конфигурация Windows\Параметры безопасности\Политики диспетчера списка сетей» и открыть политику «Неопознанные сети».
3. В диалоговом окне «Свойства: Неопознанные сети», в группе «Тип расположения», установив переключатель на нужную опцию, выбрать профиль брандмауэра, который будет сопоставлен с неопознанными сетями. В данном случае, устанавливается профиль «Общий». В группе «Разрешения пользователя» можно установить переключатель на опцию «Пользователь не может изменить расположение» для того чтобы пользователь вручную не мог изменить сетевое расположение.
4. Закрыть «Редактор локальной групповой политикой» и, при необходимости, обновить политики конфигурации компьютера, используя команду ***GPUpdate /Target:Computer /force /boot*** в командной строке.

Политики открытого ключа. Файловая система EFS

Дополнительные функции шифрованной файловой системы (Encrypting File System, EFS) обеспечили дополнительную гибкость для корпоративных пользователей при развертывании решений безопасности, основанных на шифровании файлов с данными.

Любой злоумышленник, имеющий физический доступ к компьютеру, может загрузить на нем другую ОС, обойти защиту основной ОС и получить доступ к конфиденциальным данным. Шифрование конфиденциальных файлов средствами EFS обеспечивает дополнительную защиту. Данные зашифрованного файла останутся недоступными, даже если атакующий получит полный доступ к среде хранения данных компьютера.

Только полномочные пользователи и назначенные агенты восстановления данных в состоянии расшифровывать файлы. Пользователи с другими учётными записями, обладающие разрешениями для файла – даже разрешением на передачу прав владения (Take Ownership), не в состоянии открыть его. Администратору доступ к содержимому файла также закрыт, если только он не назначен агентом восстановления данных. При попытке несанкционированного доступа к зашифрованному файлу система откажет в доступе.

Процесс шифрования в EFS

Две основные криптографические системы. Наиболее простая – шифрование с использованием секретного (симметричного) ключа, т.е. для шифровки и расшифровки данных используется один и тот же ключ. Преимущества: высокая скорость шифрования; недостатки: проблема передачи секретного ключа, а именно возможность его перехвата. Представители: DES, 3DES, DESX, AES. Отличие шифрования с открытым ключом (асимметричное шифрование) заключается в том, что данные шифруются одним ключом, а расшифровываются другим, с помощью одного и того же ключа нельзя осуществить обратное преобразование. Эта технология шифрования предполагает, что каждый пользователь имеет в своем распоряжении пару ключей – открытый ключ (public key) и личный или закрытый ключ (private key). Таким образом, свободно распространяя открытый ключ, один пользователь предоставляет другим пользователям возможность шифровать свои сообщения, направленные этому пользователю, которые сможет расшифровать только он. Если открытый ключ и попадет в «плохие руки», то он не даст возможности определить секретный ключ и расшифровать данные. Отсюда и основное преимущество систем с открытым ключом: не нужно передавать секретный ключ, однако есть и недостаток – низкая скорость шифрования. Представители: RSA, алгоритм Эль-Гамаля, алгоритм Диффи-Хелмана.

В EFS для шифрования используются все преимущества вышеперечисленных систем. Данные шифруются с помощью симметричного алгоритма с применением ключа шифрования файла (File Encryption Key, FEK). FEK – сгенерированный EFS случайным образом ключ. На следующем этапе FEK шифруется с помощью открытого ключа пользователя и сохраняется в пределах атрибута, называемого полем расшифровки данных (Data Decryption Field, DDF) непосредственно внутри самого файла. Кроме того, EFS шифрует FEK, используя открытый ключ агента восстановления, и помещает его в атрибут Data Recovery Field – DRF. DRF может содержать данные для множества агентов восстановления.

Агент восстановления данных (Data Recovery Agent, DRA) – пользователь, который имеет доступ ко всем зашифрованным данным других пользователей. Это актуально в случае утраты пользователями ключей или других непредвиденных ситуациях. Агентом восстановления данных назначается обычно администратор. Для создания агента восстановления нужно сначала создать сертификат восстановления данных и определить политику восстановления, а затем назначить одного из пользователей таким агентом. Политика восстановления играет важную роль в системе шифрования, она определяет агентов восстановления, а их отсутствие или удаление политики вообще запрещает использование пользователями шифрования.

EFS и NTFS

Шифрованная файловая система (EFS) защищает конфиденциальные данные в файлах на томах NTFS. EFS – основная технология шифрования и расшифровки файлов на томах NTFS. Открывать файл и работать с ним может только пользователь, его зашифровавший. Это чрезвычайно важно для пользователей переносных компьютеров: даже если взломщик получит доступ к потерянному или украденному компьютеру, он не сможет открыть зашифрованные файлы. В Windows XP шифрованная файловая система также поддерживает автономные файлы и папки (Offline Files and Folders).

Зашифрованный файл останется недоступным для просмотра в исходном виде, даже если атакующий обойдет системную защиту, например, загрузив другую ОС. EFS обеспечивает устойчивое шифрование по стандартным алгоритмам и тесно интегрирована с NTFS. EFS в Windows XP предоставляет новые возможности совместного использования зашифрованных файлов или отключения агентов восстановления данных, а также облегчает управление посредством групповой политики и служебных программ командной строки.

Как работает EFS

EFS позволяет сохранить конфиденциальность информации на компьютере в условиях, когда люди, имеющие физический доступ к компьютеру, могут преднамеренно или неумышленно скомпрометировать её. EFS чрезвычайно удобна для обеспечения конфиденциальности данных на мобильных компьютерах или на компьютерах, на которых работают несколько пользователей, т. е. таких системах, которые могут подвергаться атакам, предусматривающим обход ограничений списков ACL.

В совместно используемой системе атакующий обычно получает несанкционированный доступ, загружая другую ОС. Злоумышленник также может захватить компьютер, вынуть жесткий диск, поместить его на другой компьютер и получить доступ к файлам. Однако если у него нет ключа расшифровки, зашифрованный средствами EFS файл будет выглядеть как бессмысленный набор символов.

Поскольку EFS тесно интегрирована с NTFS, шифрование и расшифровка выполняются незаметно («прозрачно») для пользователя. При открытии файла EFS автоматически расшифровывает его по мере чтения данных с диска, а при записи – шифрует данные при записи на диск.

В стандартной конфигурации EFS позволяет зашифровать файл прямо из Проводника Windows без какого-либо вмешательства администратора. С точки зрения пользователя шифрование файла или папки – это просто назначение ему определённого атрибута.

Конфигурирование EFS

По умолчанию система поддерживает работу EFS. Разрешается шифровать файлы, для которых имеется разрешение на изменение. Поскольку в EFS для шифрования файлов применяется открытый ключ, нужно создать пару ключей открытый/закрытый и сертификат с открытым ключом шифрования. В EFS разрешены сертификаты, подписанные самим владельцем, поэтому вмешательство администратора для нормальной работы не требуется.

Если применение EFS не соответствует требованиям организации или если есть файлы, которые нельзя шифровать, существует много способов отключить EFS или нужным образом конфигурировать её.

Для работы с EFS всем пользователям требуются сертификаты EFS. Если в организации нет инфраструктуры открытого ключа (Public Key Infrastructure, PKI), применяются подписанные самим владельцем сертификаты, которые автоматически создаются ОС. При наличии центров сертификации сертификаты EFS обычно выпускают именно они. Если используется EFS, необходимо предусмотреть план восстановления данных при сбое системы.

Что разрешается шифровать?

На томах NTFS атрибут шифрования разрешается назначать отдельным файлам и папкам с файлами (или подпапками). Хотя папку с атрибутом шифрования и называют «зашифрованной», сама по себе она не шифруется, и для установки атрибута пары ключей не требуется. При установленном атрибуте шифрования папки EFS автоматически шифрует:

- все новые файлы, создаваемые в папке;
- все незашифрованные файлы, скопированные или перемещённые в папку;
- все вложенные файлы и подпапки (по особому требованию);
- автономные файлы.

Политики ограниченного использования программ

Политики ограниченного использования программ предоставляют механизм идентификации программ и управления возможностями их выполнения. Существует два варианта установки правил ограничения:

- на всё программное обеспечение устанавливается ограничение на запуск и создаются исключения, то есть список программ, разрешенных к выполнению;
- разрешается запуск любых программ и создаётся список исключений, запрещающий запуск некоторых программ, доступ к программам определяется правами пользователя.

Для того чтобы выбрать один из вариантов как вариант по умолчанию, необходимо открыть пункт «Уровни безопасности» и выбрать нужный уровень. По умолчанию установлен уровень безопасности «Неограниченный», то есть запуск любых программ разрешен и необходимо создать исключения для запрета запуска определённых программ.

Политики ограниченного использования программ распространяются только на исполняемые файлы, чтобы посмотреть список таких файлов, перейдите в пункт «Назначенные типы файлов». В этот список можно добавить новый тип файлов, соответственно на такие файлы будут распространяться все установленные правила, или удалить какой-то тип, исключив такие файлы из правил политик.

По умолчанию политики распространяются на всех пользователей компьютера. Но при создании некорректных правил (например, политик ограничивающих запуск системных файлов), система может работать неправильно, при этом существует риск невозможности возвращения системы в исходное состояние. Поэтому желательно распространять действие политик только на пользователей, исключив из области действия политик локальных администраторов. Для этого перейдите в пункт «Принудительный» и выполните соответствующие настройки.

Кроме того в пункте «Принудительный» существует возможность выбора, будут ли политики распространяться на файлы библиотек *.dll. Если политики будут распространяться и на файлы *.dll, то при установке уровня безопасности по умолчанию запрещающего выполнение программ, придется создавать дополнительные разрешения для каждой библиотеки которую использует программа, иначе программа будет работать некорректно.

С помощью политик ограниченного использования программ имеется возможность защищать компьютерное оборудование от программ неизвестного происхождения посредством определения программ, разрешенных для запуска. В данной политике приложения могут быть определены с помощью правила для хеша, правила для сертификата, правила для пути и правила для зоны Интернета. Программное обеспечение может выполняться на двух уровнях: неограниченном и запрещённом.

Политики ограниченного использования программ регулируют использование неизвестных программ и программ, к которым нет доверия. В организациях используется набор хорошо известных и проверенных приложений. Администраторы и служба поддержки обучены для поддержки этих программ. Однако, при запуске пользователем других программ, они могут конфликтовать с установленным программным обеспечением, изменять важные данные настройки или, содержать вирусы или «троянские» программы для несанкционированного удалённого доступа.

При интенсивном использовании сетей, Интернета и электронной почты в бизнесе пользователи повсеместно сталкиваются с различными программами. Пользователям постоянно приходится принимать решения о запуске неизвестных программ, поскольку документы и веб-страницы содержат программный код – сценарии. Вирусы и «троянские» программы зачастую умышленно замаскированы для введения пользователей в заблуждение при запуске. При таком большом количестве и разнообразии программ отдельным пользователям трудно определить, какое программное обеспечение следует запускать.

Пользователем необходим эффективный механизм идентификации и разделения программ на безопасные и не заслуживающие доверия. После идентификации программы к ним может быть применена политика для определения, могут ли они быть запущены. Политики ограниченного использования программ предоставляют различные способы идентификации программного обеспечения и средства определения, следует ли запускать данное приложение.

При применении политик ограниченного использования программ идентификация программного обеспечения производится посредством следующих правил:

- Правило для сертификата;

Политики ограниченного использования программ могут идентифицировать файл по его сертификату подписи. Правила для сертификатов не применяются к файлам с расширением .exe или .dll. Они используются для сценариев и пакетов установщика Windows. Имеется возможность создать правило для сертификата, идентифицирующее приложение и затем, в зависимости от уровня безопасности, позволяющее или не позволяющее его запустить. Например, администратор может использовать правила для сертификатов, чтобы автоматически доверять программам из проверенного источника в домене без запроса пользователя. Кроме того, правила для сертификатов могут использоваться в запрещённых областях операционной системы.

- Правило для пути;

Правило для пути идентифицирует программы по пути к файлу. Например, если имеется компьютер с политикой запрета по умолчанию, имеется возможность, предоставить неограниченный доступ к указанной папке для каждого пользователя. Для данного типа правил могут быть использованы некоторые общие пути: %userprofile%, %windir%, %appdata%, %programfiles% и %temp%.

Поскольку данные правила определяются с использованием пути, при перемещении программы правило для пути применяться не будет.

- Правило для хеша;

Хеш представляет собой серию байтов фиксированной длины, однозначно идентифицирующую программу или файл. Хеш рассчитывается с помощью алгоритма хеширования. Политики ограниченного использования программ могут идентифицировать файлы по их хешу с помощью алгоритмов хеширования SHA-1 (Secure Hash Algorithm) и MD5 hash algorithm.

Например, имеется возможность создать правило для хеша и задать уровень безопасности «Не разрешено», чтобы запретить запуск определённого файла. Хеш переименованного или перемещённого в другую папку файла не изменяется. Однако при любом изменении файла значение хеша изменяется, позволяя обойти ограничения.

Политики ограниченного использования программ распознают только хеши, рассчитанные с помощью политик ограниченного использования программ.

- Правило для зоны Интернета;

Правила для зоны влияют только на пакеты установщика Windows.

Правило для зоны идентифицирует программное обеспечение из зоны, указанной посредством Internet Explorer. Такими зонами являются Интернет, локальный компьютер, местная интрасеть, ограниченные узлы и надёжные сайты.

В политиках ограниченного использования программ используются следующие уровни безопасности:

– *«Неограниченный»*. Приложения запускается со всеми правами пользователя, вошедшего в систему.

– *«Не разрешено»*. Приложения не могут быть запущены.

Политики управления приложениями

AppLocker – управление правами на запуск приложений.

Одна из причин, по которой безопасность корпоративной сети организации может оказаться под угрозой, – несанкционированная установка и запуск приложений пользователями. Сотрудники могут запускать сомнительные приложения, утилиты, которые расходуют корпоративный трафик (например, Bittorent-клиенты), программы, которые вносят изменения в различные компоненты системы, что, в конечном итоге, приводит к ухудшению её производительности. Наконец, не исключена возможность запуска приложений, содержащих вредоносный код, что может стать причиной заражения компьютера вирусами.

В предыдущих версиях Windows была возможность решения этой задачи при помощи политик ограниченного использования программ (Software Restriction Policies), однако этот инструмент был неудобен и несовершенен. В Windows 7 функция политик ограниченного использования программ заменена средством AppLocker, которое представляет собой изменённую и доработанную версию Software Restriction Policies.

AppLocker значительно упрощает контроль за действиями пользователей, которые касаются установки приложений, а также запуска файлов EXE, использования библиотек DLL, файлов инсталляторов MSI и MSP, а также сценариев. Основные отличия AppLocker от политик ограниченного использования программ:

– применение правила к определённому пользователю или к группе, а не только ко всем пользователям;

– мастер автоматического создания правил;

– импорт и экспорт созданных правил;

– режим «Только аудит», в котором ведется аудит приложений, которые обрабатываются правилами, однако на самом деле правила не применяются;

– условие «Издатель», которое является расширенной версией условия «Сертификаты», существовавшего ранее;

– поддержка новой командной строки Windows Power Shell;

– коллекции правил для разных типов файлов, которые не зависят друг от друга.

Для доступа к настройкам AppLocker необходимо перейти в раздел «Администрирование» (Administrative Tools) панели управления выбрать пункт «Локальная политика безопасности» (Local Security Policy), после чего раскрыть список «Политики управления приложениями» (Application Control Policies).

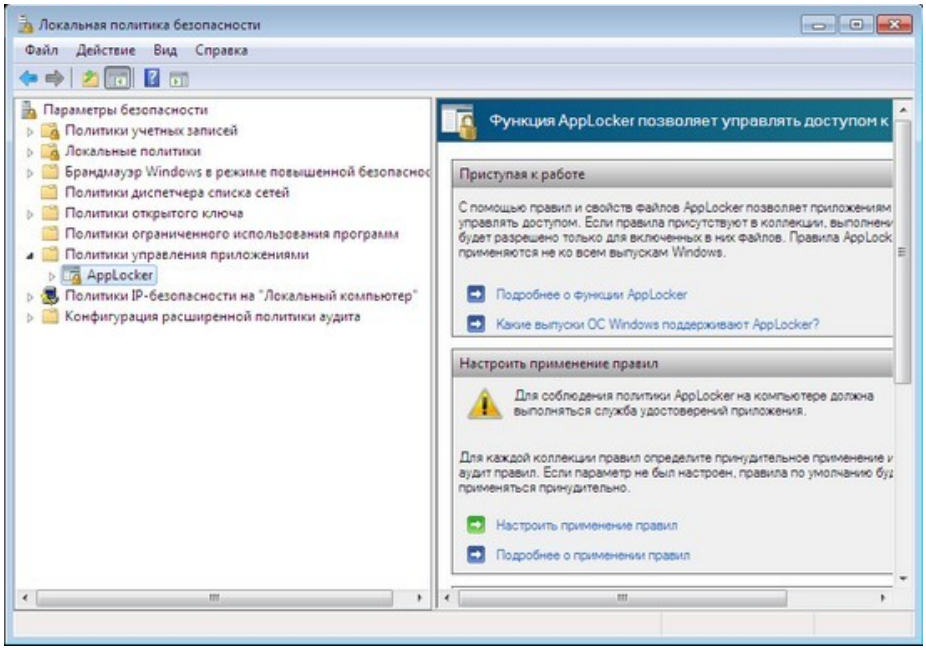

Рисунок 4 – Узел «Политики управления приложениями»

Одна из особенностей AppLocker состоит в том, что по умолчанию все правила, настроенные при помощи этого средства, применяются. Именно поэтому необходимо очень осторожно настраивать их, так как можно по неопытности заблокировать работу Windows. Во-первых, рекомендуется перед созданием правил перейти в окно их настройки, щёлкнув по ссылке «Настроить применение правил» (Configure Rule Enforcement), и для каждого типа правил (исполняемые файлы, установщик Windows и сценарии) выбрать вариант применения «Только аудит» (Audit Only). В этом случае правила с любыми настройками не смогут блокировать работу приложений или системы в целом, однако при помощи журнала событий администратор сможет просмотреть, как они применяются по отношению к файлам или приложениям. Если окажется, что правила блокируют приложения, к которым доступ должен быть разрешён, или, наоборот, не действуют на программы, к которым нужно ограничить доступ, правила можно будет отредактировать.

Второе решение, которое может помочь администраторам разобраться с новыми возможностями управления доступом, – создание и отладка правил на тестовом компьютере. AppLocker поддерживает импорт и экспорт правил, благодаря чему можно создать набор политик ограничений в безопасной среде, тщательно протестировать их работоспособность, после чего импортировать уже в рабочую среду.

Для применения правил, созданных при помощи AppLocker, необходимо, чтобы на компьютерах была запущена служба «Удостоверение приложения» (Application Identity). По умолчанию она отключена. Для её запуска откройте раздел «Администрирование» панели управления и выберите пункт «Службы», после чего найдите службу в списке, щёлкните по её названию правой кнопкой мыши и выберите команду «Запустить». В свойствах службы можно настроить её автоматический запуск.

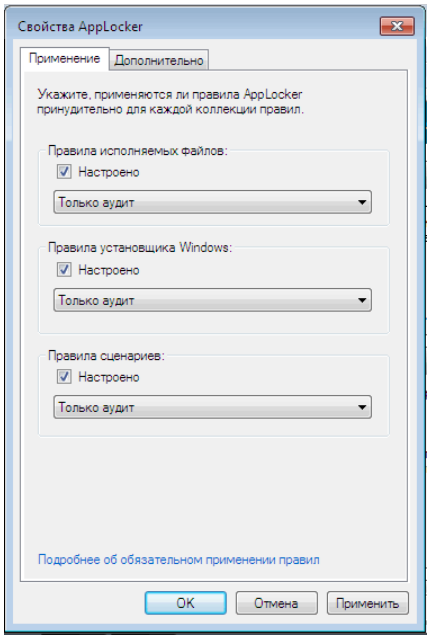

Рисунок 5 – Окно свойств AppLocker, вкладка «Примечание»

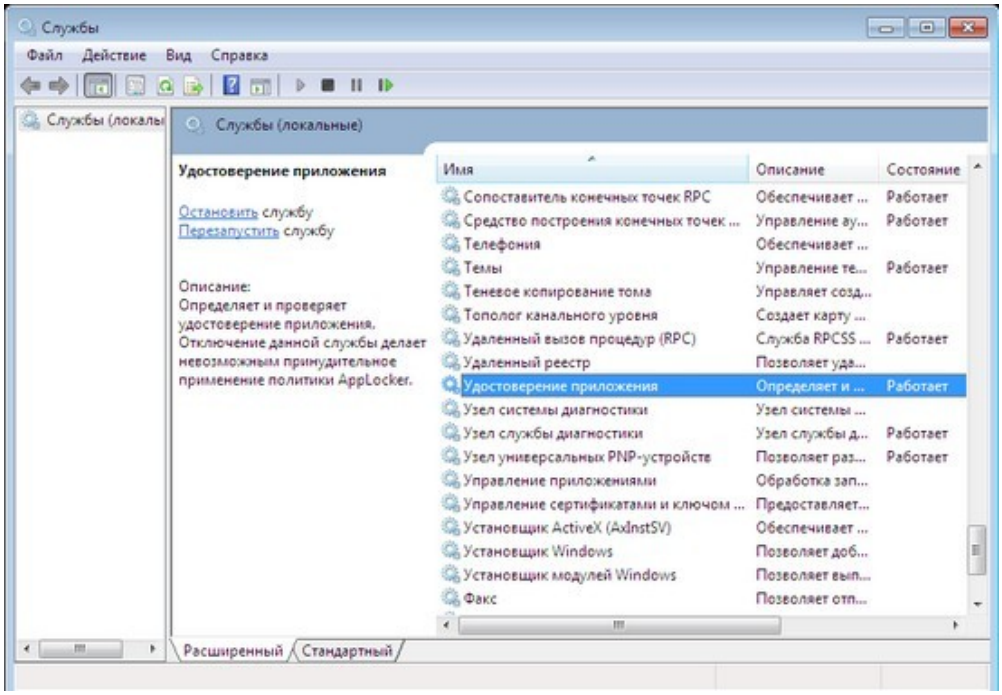

Рисунок 6 – Запуск службы «Удостоверение приложения»

По умолчанию в AppLocker используется три типа (коллекции) правил, которые настраиваются и используются независимо друг от друга: исполняемые файлы (EXE и COM), установщик Windows (MSI и MSP) и сценарии (PS1, BAT, CMD, VBS и JS), однако при необходимости можно также включить правила для файлов библиотек DLL (сюда входят и файлы с расширением OCX). Для этого нужно установить флажок «Включить коллекцию правил DLL» (Enable the DLL rule collection) на вкладке «Дополнительно» (Advanced) окна «Свойства AppLocker» (AppLocker Properties).

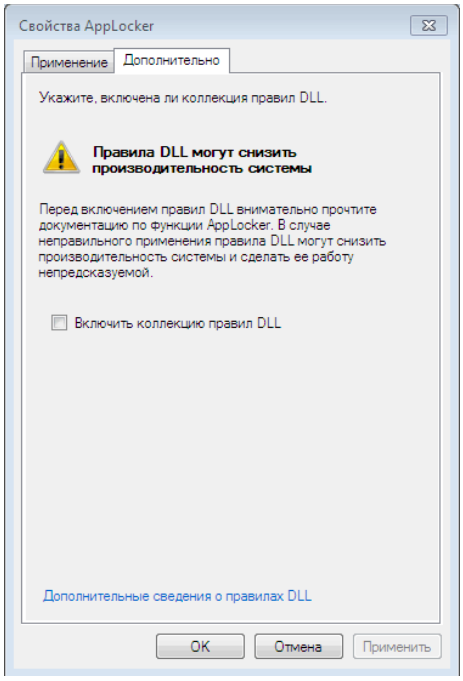

Рисунок 7 – Окно свойств AppLocker, вкладка «Дополнительно»

Стоит, однако, иметь в виду, что использование таких правил может существенно повлиять на производительность системы. Это связано с тем, что каждое приложение, как правило, использует для работы несколько файлов библиотек, поэтому на их проверку и соответствие правилам уходит гораздо больше времени, чем на проверку только приложений. Кроме этого, некоторые приложения загружают дополнительные файлы библиотек в процессе работы, поэтому проверка, которую Windows будет при этом выполнять, может замедлить работу пользователя с программой. При включении правил DLL их необходимо создавать для каждой библиотеки, которая используется всеми разрешёнными программами.

Необходимо отметить, что использование большого числа правил любого типа (это касается не только правил DLL) в любом случае будет снижать производительность системы, поскольку при попытке запуска каждого приложения Windows потребуется обрабатывать все правила, чтобы разрешить или запретить пользователю работу с программой.

Именно поэтому, создавая правила, имеет смысл строить их таким образом, чтобы общее их число было как можно меньшим. Все правила AppLocker работают по принципу разрешения («белый список»), запрета («черный список») и исключения. Иными словами, перед созданием правила стоит решить, что удобнее: 1) сделать правило, разрешающее определённое действие (при этом запуск всех приложений, которых нет в составленном администратором списке, будет запрещён), и сделать исключения для некоторых групп пользователей или приложений; или же 2) создать правило, разрешающее запускать все приложения, кроме указанных в списке, и также указать исключения.

Несмотря на то, что при помощи AppLocker можно создавать как разрешающие, так и запрещающие правила, в большинстве случаев рекомендуется использовать первый вариант. Это связано с тем, что для обеспечения безопасности любой организации гораздо логичнее составить фиксированный список разрешённых приложений, который можно по мере необходимости обновлять, нежели попытаться перечислить в правиле те программы, которые запрещено запускать. Любой новый вирус, который администратор не успел добавить в запрещающее правило, имеет все шансы проникнуть в корпоративную сеть. Также причиной, по которой рекомендуется использовать разрешающие правила, является то, что запрещающие действия во всех случаях переопределяют разрешающие.

Для создания нового правила раскройте список AppLocker в окне «Локальная политика безопасности», необходимо щёлкнуть правой кнопкой мыши по нужному типу правила и выбрать команду «Создать новое правило». Будет запущен мастер, на первом этапе работы которого нужно будет определиться с тем, будет ли это правило разрешать или запрещать определённые действия, а также, на какие категории пользователей оно будет распространяться.

Затем нужно будет выбрать тип основного условия: «Издатель» (Publisher), «Путь» (Path) и «Хэшируемый файл» (File Hash). Несмотря на то, что типы условий похожи на те, которые использовались в политиках ограниченного использования программ в предыдущих версиях Windows, работа с ними организована по-другому.

Наиболее интересным является условие «Издатель», прототипом которого в политиках ограниченного использования программ было условие «Сертификаты» (Certificate). Это условие дает возможность разрешить запуск приложений, для которых имеется цифровая подпись издателя. При создании правил с таким условием учитывается не только название производителя, как это было в Windows XP, но и другая информация, такая как название продукта, имя файла, номер версии.

При этом условие может распространяться в точности на указанный номер версии приложения или на все версии, номер которых выше или ниже заданного. Благодаря этому, можно гибко настроить правило, которое будет разрешать установку новых версий приложений, но при этом запрещать установку старых релизов, которые могут быть несовершенны с точки зрения безопасности. Для использования условия «Издатель» нужно указать путь к файлу приложения, который содержит цифровую подпись. Установив флажок «Пользовательские значения», можно вручную отредактировать значения всех полей. Стоит иметь в виду, что если приложение не имеет цифровой подписи, то использовать условие «Издатель» в его отношении невозможно.

Условие «Путь» позволяет определить приложения, которые разрешено запускать и устанавливать пользователю, на основе их расположения в файловой системе локального компьютера, в сети или на сменных носителях. Создавая такое условие, можно использовать подстановочные знаки и переменные окружения. Например, чтобы указать путь на CD/DVD-диске, нужно использовать переменную %REMOVABLE%, а для указания пути на USB-накопителе – %HOT%.

Условие «Путь» необходимо использовать очень осторожно, так как при недостаточной продуманности оно может стать причиной того, что пользователи смогут с его помощью обходить некоторые запреты. Например, если создать разрешающее условие такого типа и включить в него расположение папки, в которую пользователь может выполнять запись, то пользователь сможет скопировать в такую папку запрещённый для запуска файл из другого расположения и запустить его.

Условие «Хэшируемый файл» в большинстве случаев является наименее эффективным, так как определение легитимности файла построено на вычислении его контрольной суммы. Нетрудно догадаться, что если выходит обновление приложения, то его контрольная сумма изменяется, и условие перестает работать. С другой стороны, такой способ позволяет защититься от возможности запуска известной программы, в которую был внедрен вредоносный код. Поскольку при этом контрольная сумма изменяется, модифицированное приложение запустить будет невозможно.

Как видно, каждое из условий несовершенно и имеет свои недостатки. Именно поэтому на следующем этапе работы мастера предлагается настроить исключения. Исключения можно использовать, если в качестве основного выбраны условия «Издатель» и «Путь».

Наконец, на последнем этапе работы мастера нужно дать правилу название, а также снабдить его описанием. Несмотря на то, что последнее необязательно, не стоит пренебрегать этой возможностью, так как описание может помочь в будущем вспомнить, за что отвечает то или иное правило.

Чтобы лучше понять, как работают правила, можно начать с создания правил по умолчанию. Они доступны для каждого из типов правил. Например, правила для исполняемых файлов включают такие: разрешение на запуск любых приложений членам группы «Администраторы», разрешение на запуск приложений, находящихся в директории Program Files и в папке Windows, для членов группы «Все». Для создания набора правил по умолчанию нужно раскрыть список AppLocker в окне «Локальная политика безопасности», щёлкнуть правой кнопкой мыши по нужному типу правила и выбрать команду «Создать правила по умолчанию».

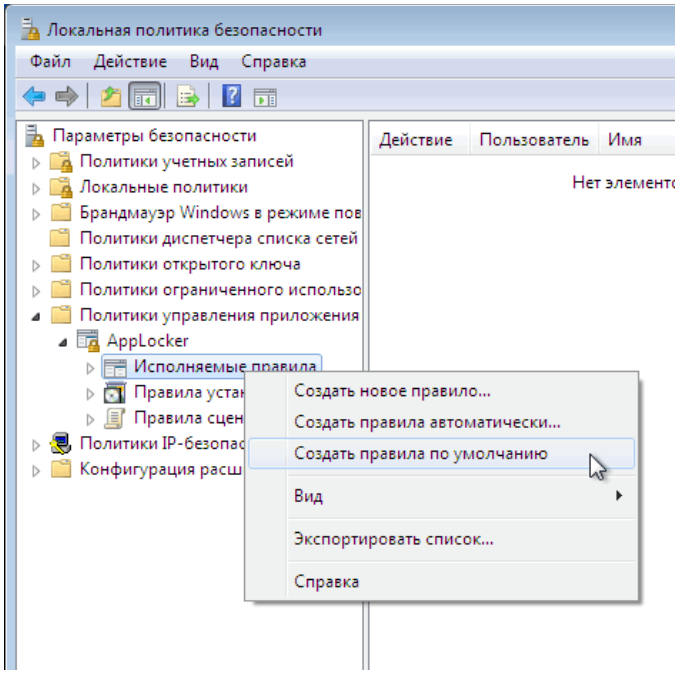

Рисунок 8 – Создание правила по умолчанию

Правила по умолчанию можно редактировать. Для этого нужно щёлкнуть по названию правила в списке и выбрать строку «Свойства». Редактировать можно все свойства правил, например, добавлять исключения, изменять пути, группы пользователей, на которые они распространяются, и т.д.

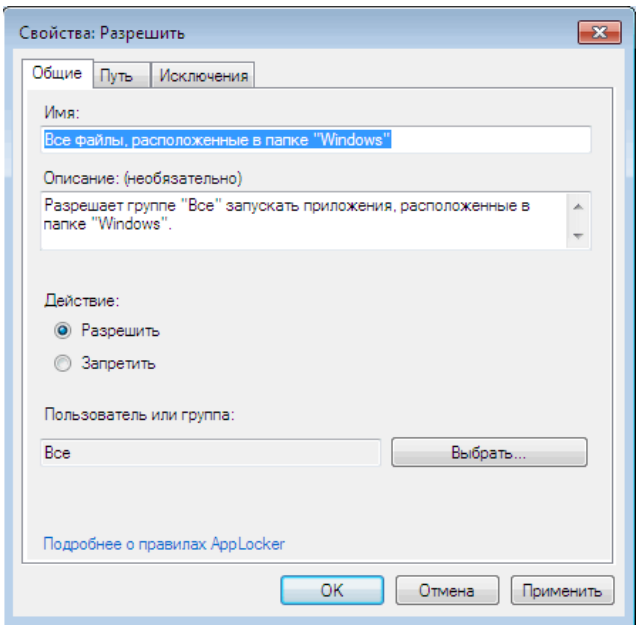

Рисунок 9 – Редактирование свойств

В AppLocker встроен автоматический механизм, упрощающий создание правил. Выберите команду «Создать правила автоматически» для определённого типа правил, укажите группы пользователей, к которым будут применяться создаваемые правила, а также папку, в которую установлены приложения.

При автоматическом создании правил мастер пытается максимально уменьшить их число. В таком режиме создаются только разрешающие правила. Если среди проанализированных приложений имеются такие, которые созданы одним разработчиком и у которых совпадает название продукта (согласно цифровой подписи), для них создаётся одно правило с условием «Издатель». Что касается условия «Хеш», то создаётся одно условие, которое содержит контрольные суммы всех файлов.

После завершения работы мастера автоматического создания правил AppLocker выдает отчет, в котором выводит общее количество файлов и число правил, которые будут созданы. Перед созданием правил есть возможность просмотреть как проанализированные файлы, так и составленные правила.

Используя AppLocker, нужно иметь в виду, что правила, созданные с его помощью, могут быть применены только на компьютерах, работающих под управлением Windows 7 Максимальная, Windows 7 Корпоративная и Windows Server 2008 R2.

Политики безопасности IP на «Локальный компьютер

После стандартной инсталляции в операционной системе предлагаются три варианта настройки для организации защищенного IP-канала – политики безопасности IPSec в рамках одного домена:

– «Сервер» – для всего трафика IP всегда запрашивает безопасность с помощью доверия Kerberos. Разрешает небезопасную связь с клиентами, которые не отвечают на запрос;

– «Безопасность сервера» – для всего IP-трафика всегда запрашивает безопасность с помощью доверия Kerberos. Не разрешает небезопасную связь с недоверенными клиентами;

– «Клиент» – обычная связь (небезопасная). Использует правило ответа по умолчанию для согласования с серверами, запрашивающими безопасность. Только запрошенный протокол и трафик с этим сервером будут безопасными.

После установки операционной системы ни одна из политик не назначена. Пользователь может активизировать (назначить) одну и только одну из существующих политик.

Ниже, в качестве справочной информации, приводятся настройки, которые используются Microsoft для трех стандартных вариантов политики безопасности IPSec.

При изучении вопросов, связанных с установлением защищенного соединения IPSec индивидуальные рекомендации необходимы для случая, если компьютер, который необходимо задействовать в схеме защищенного соединения, имеет несколько IP-адресов. Кроме того, для случая работы в домене локальная политика безопасности компьютера может перекрываться политикой безопасности, определяемой контроллером домена.

Таблица 1 – Настройки стандартных политик безопасности IP в ОС Windows 7

Политика безопасности IP *Правило безопасности IP*	***Клиент (только ответ)***	***Безопасность сервера (требовать безопасность)***			***Сервер (запрос безопасности)***		
	Динамический	*Динамический*	*Весь ICMP-трафик*	*Весь IP-трафик*	*Динамический*	*Весь ICMP-трафик*	*Весь IP-трафик*
Методы проверки подлинности	Kerberos V5	Kerberos V5	Kerberos V5	Kerberos V5	Kerberos V5	Kerberos V5	Kerberos V5
Тип подключения	Все сетевые подключения	Все сетевые подключения	Все сетевые подключения	Все сетевые подключения	Все сетевые подключения	Все сетевые подключения	Все сетевые подключения
Методы безопасности (Действия фильтра/ Методы безопасности)	Использование протокола ESP (3DES или DES) и (SHA1	Использование протокола ESP (3DES или DES) и (SHA1	Разрешить (Блокирование согласования безопасности IP	Согласовывать - использование протокола ESP (3DES или	Использование протокола ESP (3DES или DES) и (SHA1	Разрешить (Блокирование согласования безопасности IP	**Разрешать связь с компьютером, не поддерживающим IPSec** Согласован

	или MD5) Использование протокола AH (SHA1 или MD5)	или MD5) Использование протокола AH (SHA1 или MD5)	- поток данных защищать не требуется)	DES) и (SHA1 или MD5), Принимать небезопасную связь, но отвечать с помощью IPSec	или MD5) Использование протокола AH (SHA1 или MD5)	- поток данных защищать не требуется)	ие - использование протокола ESP (3DES или DES) и (SHA1 или MD5), принимать небезопасную связь, но отвечать с помощью IPSec
Список фильтров	–	–	ICMP (Мой IP <-> Любой IP)	Любой протокол (Мой IP <-> Любой IP)	–	ICMP (Мой IP <-> Любой IP)	Любой протокол (Мой IP <-> Любой IP)

Назначение и отключение IPSec-соединения с использованием стандартных настроек Windows

Для организации аутентифицированного и закрытого обмена данными между двумя компьютерами по протоколу IPSec необходимо активизировать на одной стороне политику «Безопасность сервера», на другой – «Клиент» в разделе «Политики безопасности IP на Локальный компьютер». Это можно сделать, выбрав пункт локального меню (вызываемого по правой кнопке «мыши») «Назначить», предварительно выбрав строку с нужной политикой.

Стандартные политики предназначены для использования в рамках одного домена. В противном случае защищённое соединение не будет установлено.

Связывающиеся стороны должны быть уверены, что настройки используемых политик остались неизменными с момента установки операционной системы. Вместе с тем теоретически существует ненулевая вероятность, что после выполнения согласования поддерживаемых криптографических алгоритмов и ключевых данных, соединение будет организовано только с использованием протокола аутентификации, которое предполагает активизацию механизмов только авторства и целостности передаваемых пакетов, в то время как само содержимое пакетов будет передаваться по сети в открытом виде. Это создаёт предпосылки к тому, что все данные, которыми обмениваются компьютеры, организовавшие «защищенный» канал, будут перехвачены.

Чтобы удалить назначение политики IPSec, нужно щёлкнуть на активной политике правой кнопкой «мыши» и выбрать команду «Снять». Кроме того, можно отключить на компьютере службу «Агент политики IPSEC». Это позволит обеспечить гарантированное отключение использования политики безопасности IPSec, которая может управляться на уровне контроллера домена.

Редактирование общих настроек политики безопасности IP

Необходимо выберать закладку «Общие» в окне «Свойства».

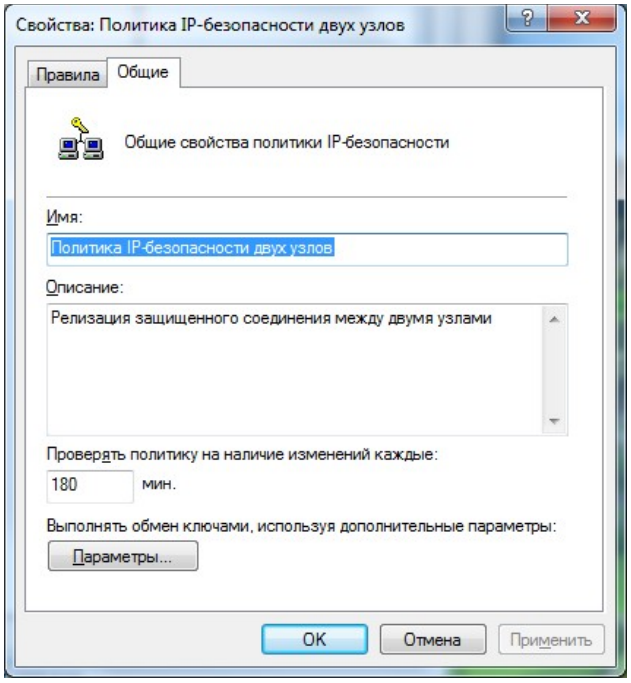

Рисунок 10 – Окно свойств политики безопасности IP двух узлов

В поле «Проверять политику на наличие изменений каждые: « должно быть записано значение 180 мин., щёлкнуть кнопку «Дополнительно...». При этом открывается окно «Параметры обмена ключами».

Установитьпараметры, как показано на рисунке 11, и щёлкнуть «Методы».

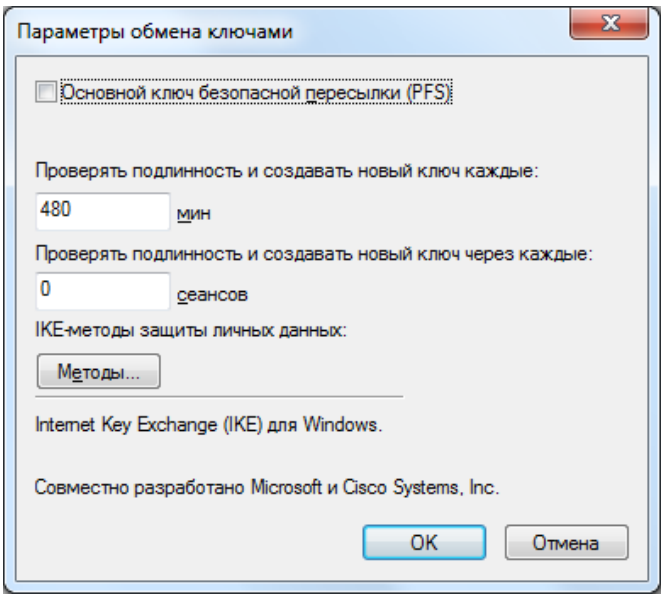

Рисунок 11 – Окно параметров обмена ключами

При этом откроется окно «Методы безопасности при обмене ключами», в котором нужно удалить все строки, кроме одной с параметрами:

- «Тип (Type)» – IKE;
- «Шифрование (Encryption)» – 3DES;
- «Целостность (Integrity)» – SHA1;
- «Группа Диффи-Хелмана (Diffie-Hellman ...)» – Средняя (2).

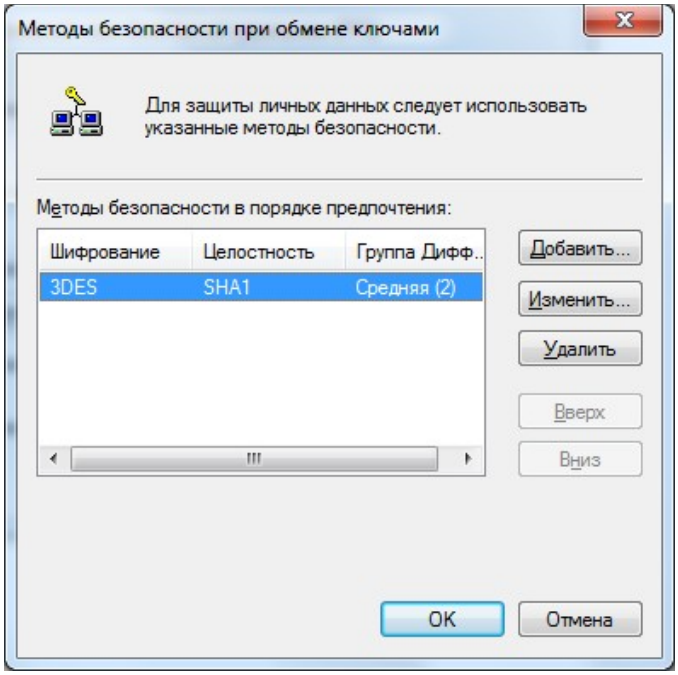

Рисунок 12 – Окно методов безопасности при обмене ключами

Настройки новой политики безопасности IP

Для настройки новой политики ниже будет подробно описана последовательность действий, определяемая следующими шагами:

1. Создание новой политики безопасности IP.
2. Определение нового правила:

– списка IP-фильтров (назначение используемых сетевых протоколов и адресов взаимодействующих хостов);

– действия фильтра (выбор используемых криптографических алгоритмов);

– методов проверки подлинности (назначение способа установления доверительных отношений между компьютерами);

– типа подключения (удалённый доступ, локальная сеть);

– параметров туннеля (использовать или нет туннельный вариант протокола IPSec).

Практическое задание №8

1. Создание новой политики

В левой части окна «Локальные параметры безопасности» выбрать пункт «Политики безопасности IP на Локальный компьютер» и создать новую политику либо «кликнув» на значке меню, либо выбрав пункт контекстного меню (вызываемого при нажатии правой кнопки «мыши» в правой части окна) «Создать политику безопасности». При этом открывается окно «Мастер политики IP-безопасности». Щёлкнуть «Далее» для перехода к следующему окну диалога.

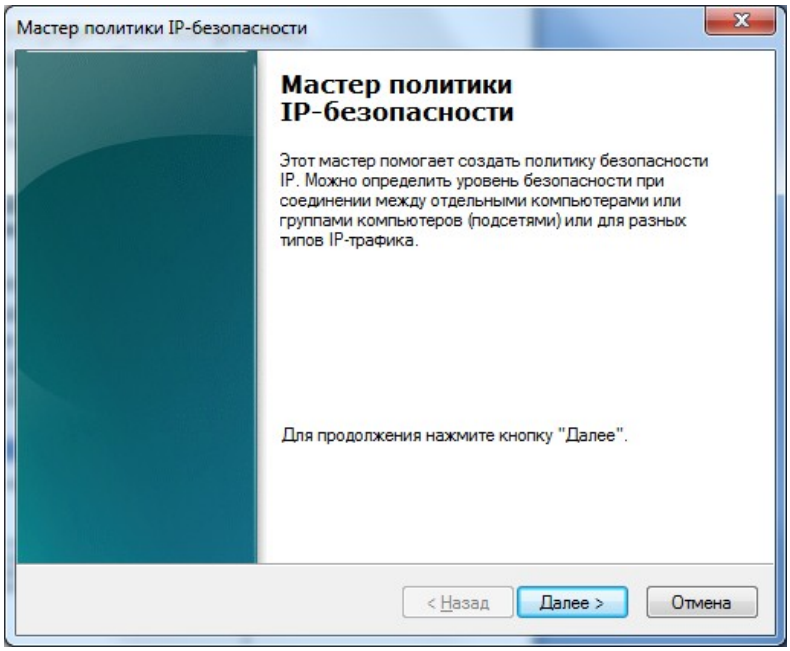

Рисунок 13 – Начальное окно мастера политики IP-безопасности

Ввести любое имя новой политики и, если это необходимо, её описание. Щёлкнуть «Далее» для перехода к следующему окну диалога.

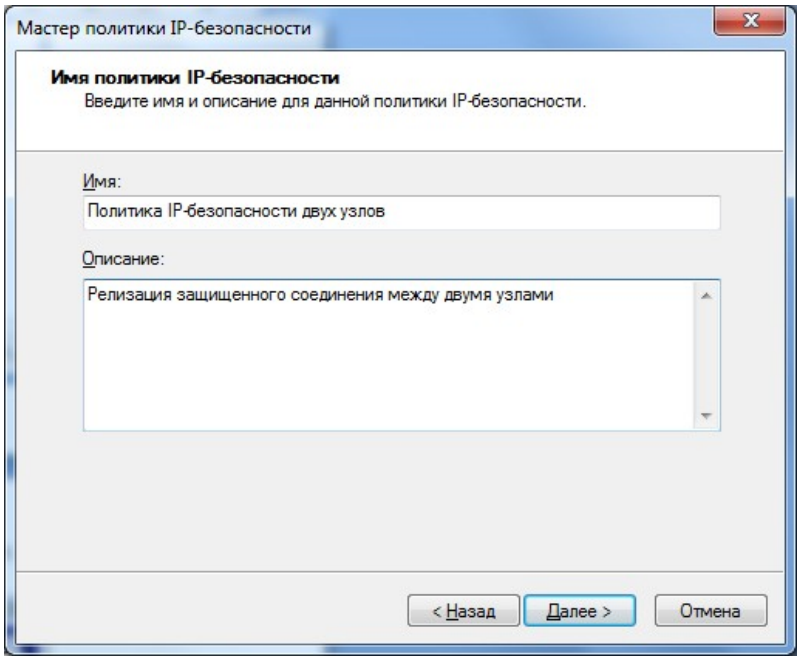

Рисунок 14 – Определение названия политики безопасности

Отменить установку флажка «Использовать правило по умолчанию», в результате чего для данной политики можно будет определить пользовательское правило. Щёлкнуть «Далее» для перехода к следующему окну диалога.

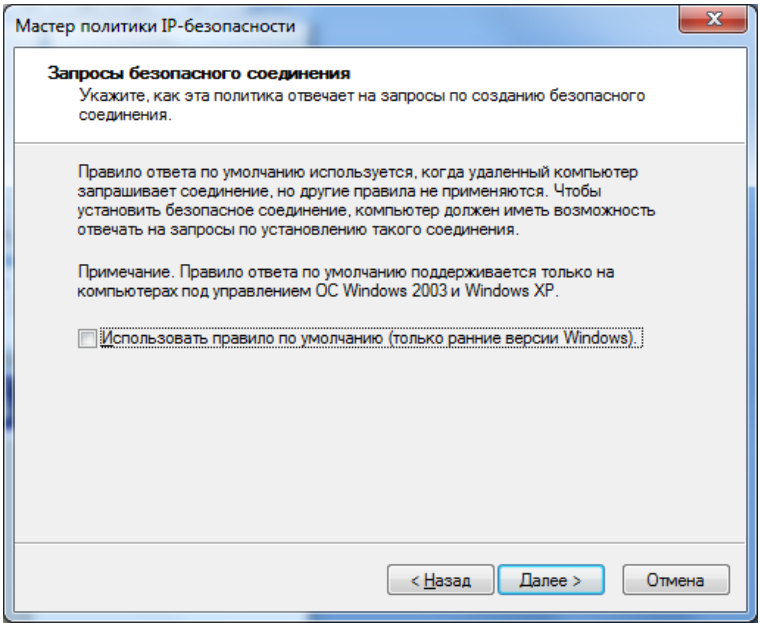

Рисунок 15 – Окно определения активизации политики

после задания параметров

Удостовериться, что флажок «Изменить свойства» установлен, и щёлкнуть «Готово».

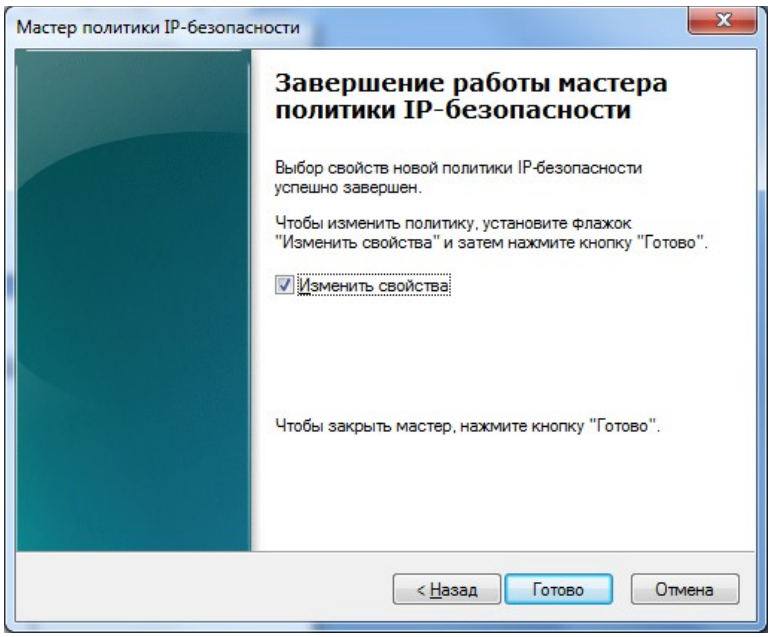

Рисунок 16 – Окно завершения назначения новой политики IP-безопасности

2. Редактирование свойств политики безопасности IP;

При этом создание новой политики заканчивается и открывается окно «Свойства».

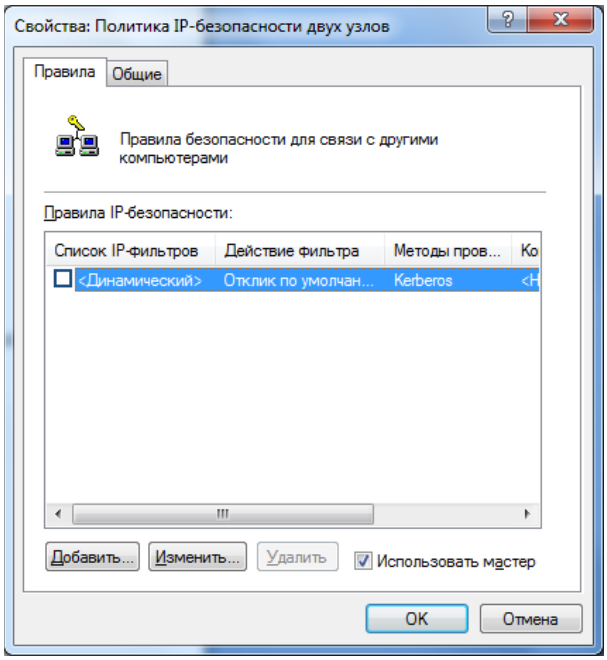

Рисунок 17 – Окно правил для вновь созданной политики

Необходимо отменить установку флажка «Использовать мастер» и щёлкнуть «Добавить». При этом открывается окно «Свойства: Новое правило».

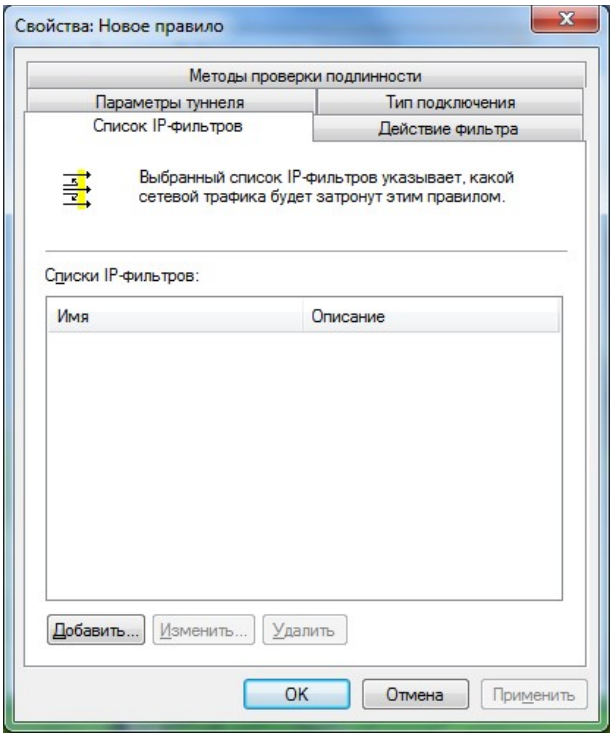

Рисунок 18 – Окно создания нового правила

3. Создание нового фильтра;

На закладке «Список фильтров» щёлкнуть «Добавить», при этом открывается окно «Список фильтров IP».

Ввести любое имя фильтра и, если это необходимо, его описание. Отмените флажок «Использовать мастер» и щёлкнуть «Добавить». При этом открывается окно «Свойства: Фильтр».

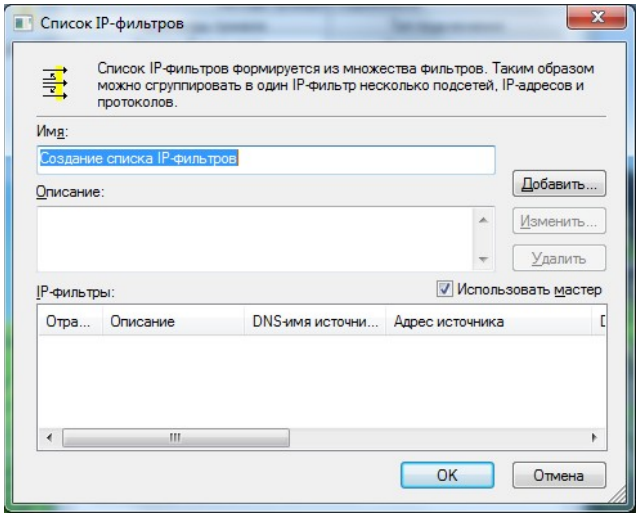

Рисунок 19 – Определение названия фильтра IP

Выбрать закладку «Адресация» и установить следующие параметры:

- адрес источника пакетов – Определённый IP-адрес»;
- IP-адрес – IP-адрес вашего компьютера;
- адрес назначения пакетов – Определённый IP-адрес;
- IP-адрес – адрес компьютера, с которым устанавливается защищенное соединение;
- проверить установку флажка «Отраженный».

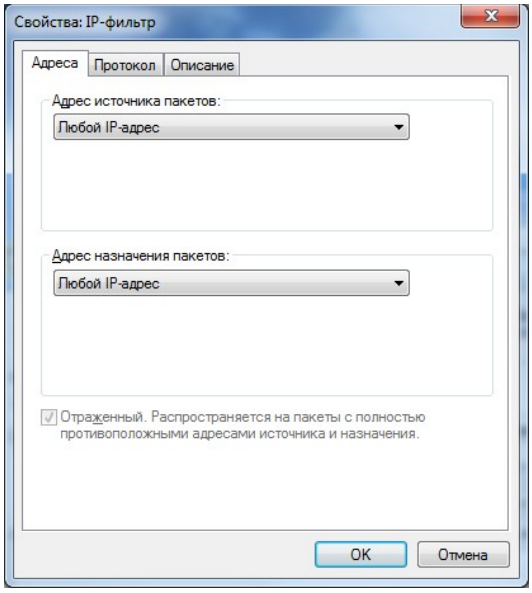

Рисунок 20 – Назначение адресов и источника IP-пакетов для фильтра

Выбрать закладку «Протокол» и установить «Тип протокола» – «Любой».

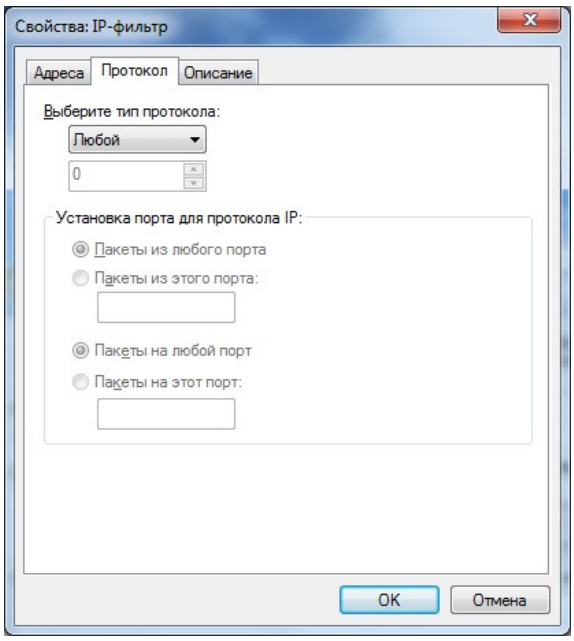

Рисунок 21 – Выбор типа протокола, который должен обрабатываться фильтром

Закончить описание свойств фильтра, щёлкнув «OK» в окне «Свойства: Фильтр».

Щёлкнуть «Закрыть (OK)» в окне «Список фильтров IP».

На закладке «Список фильтров IP» в окне «Свойства: Новое правило» поставить точку в строке, отображающей только что созданный новый фильтр.

4. Создание нового действия;

Выбрать закладку «Действие фильтра» в окне «Свойства: Новое правило».

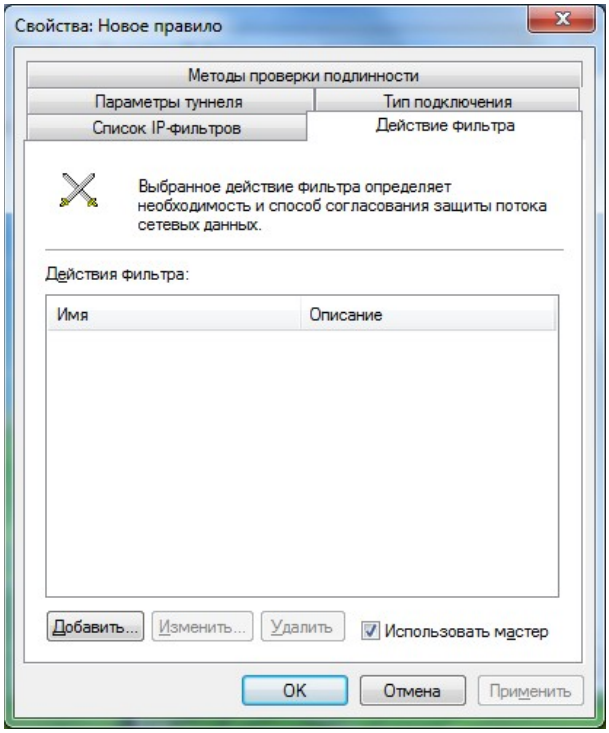

Рисунок 22 – Закладка «Действие фильтра»

Отменить установку флажка «Использовать мастер» и щёлкнуть «Добавить». При этом открывается окно «Свойства: Создание действия фильтра».

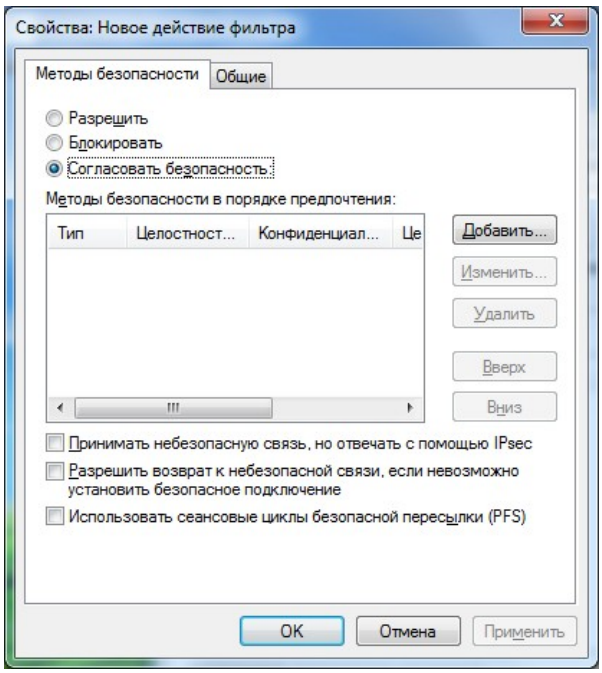

Рисунок 23 – Определение методов безопасности, используемых для фильтра

На закладке «Методы безопасности» выбрать пункт «Согласовать безопасность» и щёлкнуть «Добавить», при этом открывается окно «Создать метод безопасности».

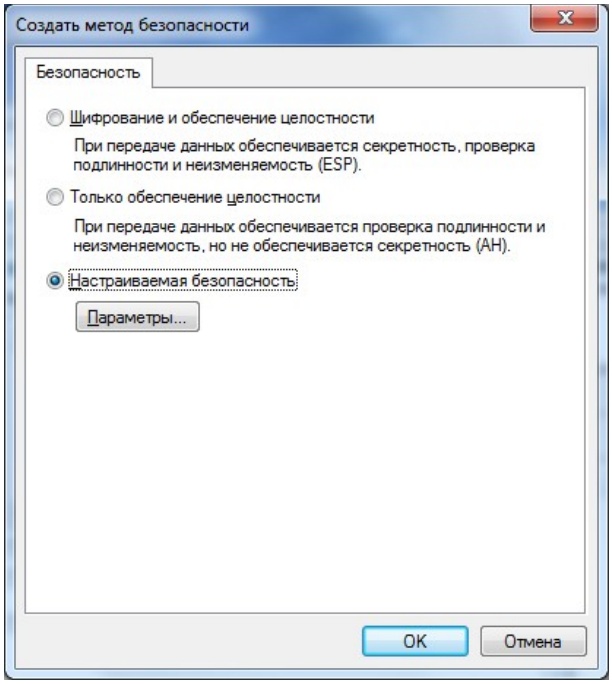

Рисунок 24 – Создание метода безопасности

Выбрать пункт «Настраиваемая безопасность» и щёлкнуть «Параметры...». При этом открывается окно «Параметры особого метода безопасности», в котором необходимо установить значения.

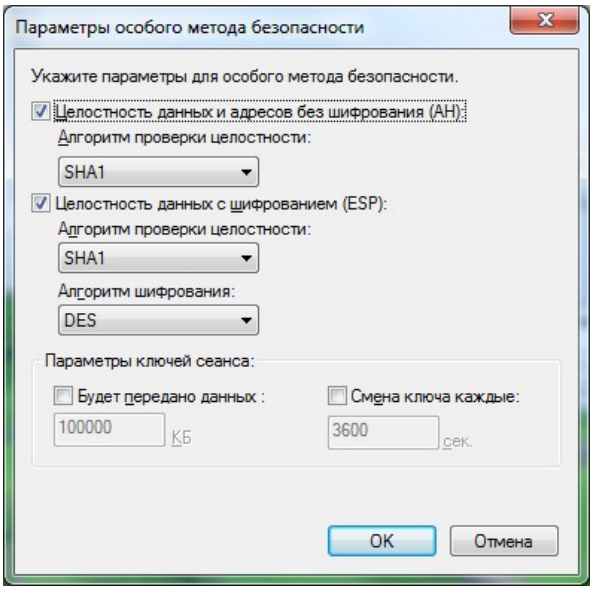

Рисунок 25 – Определение криптографических настроек IPSec-протокола

Щёлкнуть «OK» в этом окне и окне «Создать метод безопасности».

В окне «Свойства: Создание действия фильтра» флажок должен быть установлен только на пункте «Принимать небезопасную связь, но отвечать с помощью IPSec». На закладке «Общие» заполнить имя и, если это необходимо, описание.

Щёлкнуть «OK».

На закладке «Действие фильтра» в окне «Свойства: Новое правило» поставить точку в строке, отображающей только что созданное новое действие фильтра.

5. Установка параметров туннеля и типа подключения;

Выбрать закладку «Параметры туннеля» в окне «Свойства: Новое правило» и сохранить заданную по умолчанию настройку «Правило не определяет туннель».

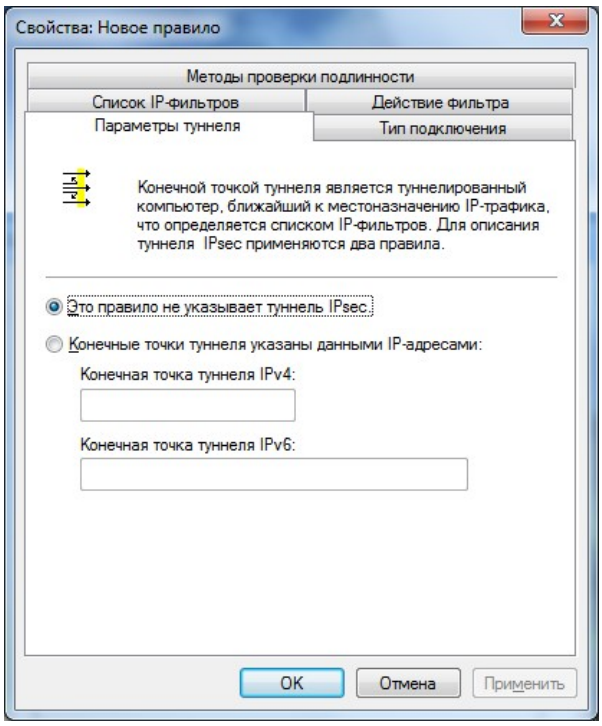

Рисунок 26 – Выбор использования туннелирования при соединении

Выберать закладку «Тип подключения» в окне «Свойства: Новое правило». Можно выбрать пункт «Все сетевые подключения», но лучше выбрать конкретный тип: либо «Локальное сетевое подключение (LAN)», либо «Удалённый доступ».

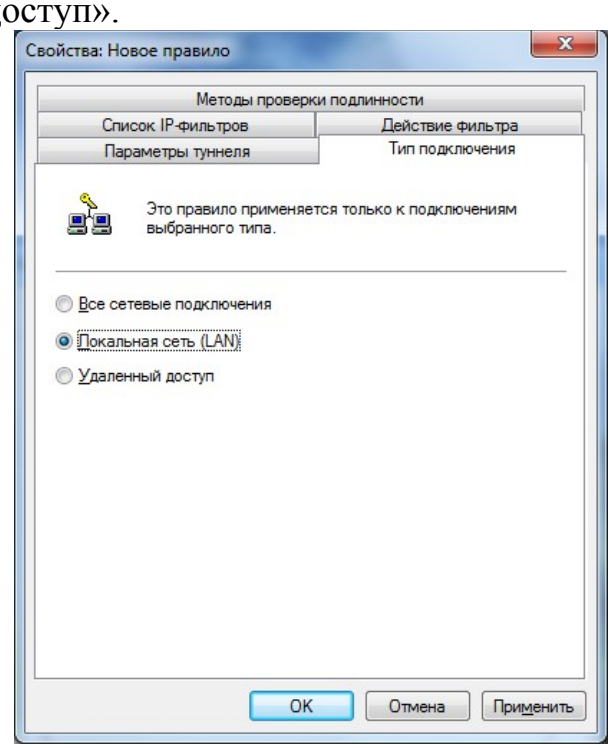

Рисунок 27 – Определение типа подключения для правила

6. Установка метода проверки подлинности;

Выбрать закладку «Методы проверки подлинности» в окне «Свойства: Новое правило». По умолчанию Kerberos устанавливается в качестве метода проверки подлинности.

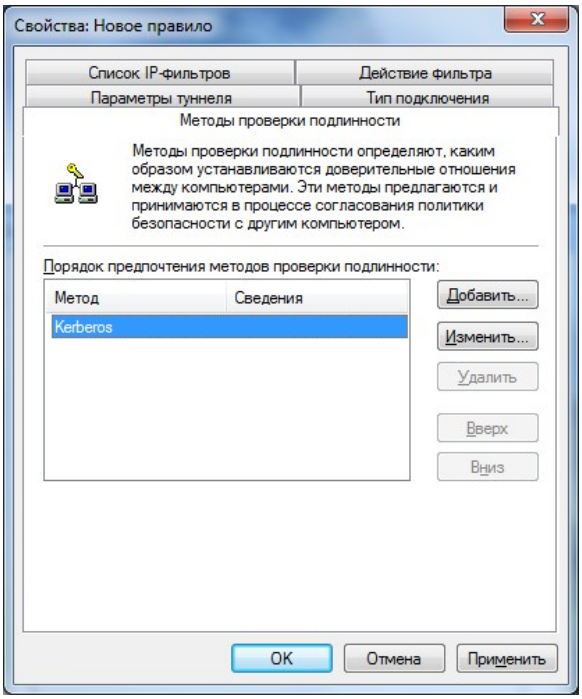

Рисунок 28 – Определение методов проверки подлинности

Щёлкнуть «Добавить», при этом откроется окно «Свойства: Изменить способ проверки подлинности».

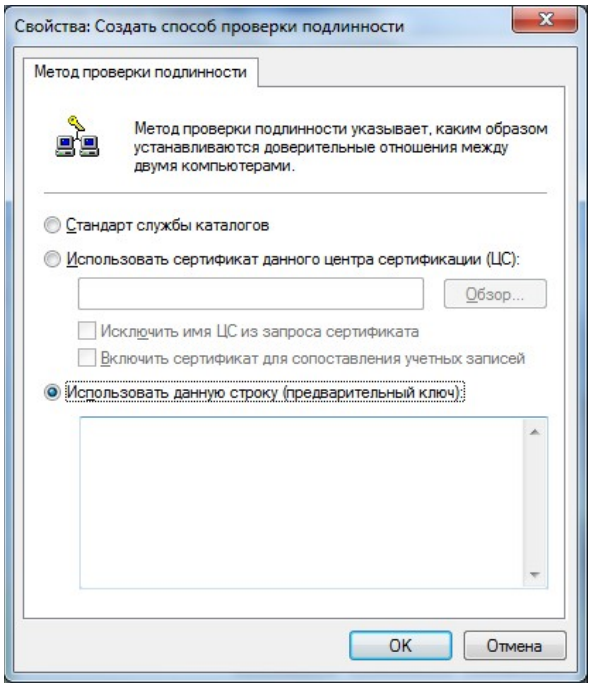

Рисунок 29 – Задание методов проверки подлинности для фильтра

Выбрать пункт «Использовать данную строку для защиты обмена ключами» и внести в окно пароль, который будет использоваться для установления защищенной связи между компьютерами.

Щёлкнуть «ОК».

Удалить из списка методов все, кроме созданного вами.

Щёлкнуть в окне «Свойства: Новое правило –> ОК».

На этом создание нового правила закончено.

Некоторые пояснения для возможных методов установления доверительных отношений:

«Стандарт Windows 2000 Kerberos V5» – протокол Kerberos задан по умолчанию, и если все участники находятся в одном домене, это будет лучшим вариантом, поскольку облегчает конфигурирование.

«Использовать сертификат данного Центра сертификации» – безопасность, основанная на применении сертификатов. Можно использовать сертификаты для инициализации защищенного соединения. Они совместимы со многими системами сертификации.

«Использовать данную строку для защиты обмена ключами» – использование предварительно совместно используемых строк является наиболее нежелательным методом обеспечения безопасности, если строка будет сфальсифицирована, невозможно гарантировать конфиденциальность. Однако подобный метод можно использовать в том случае, если поддерживаются внешние операционные системы или устройства.

Конфигурация расширенной политики аудита

Предоставляет дополнительные локальные политики, отвечающие за аудит.

Варианты заданий

1	1, 10, 20
2	2, 9, 21
3	3, 8, 19
4	4, 7, 18
5	5, 11, 17
6	6, 12, 22
7	7, 13, 16
8	1, 8, 14
9	6, 15, 21
10	1, 6, 16

Задание 1. Создать учётную запись при помощи диалога «Управление учётными записями пользователей» (п.1.2.1).

Задание 2. Создать учётную запись при помощи диалога «Учётные записи пользователей» (п.1.2.2).

Задание 3. Создать учётную запись при помощи оснастки «Локальные пользователи и группы» (п.1.2.3).

Задание 4. Создать учётную запись с помощью командной строки (п.1.2.4).

Задание 5. Изменить имя учётной записи при помощи диалогового окна «Управление учётными записями пользователей» (п.2.1).

Задание 6. Создать пароль учётной записи при помощи диалогового окна «Управление учётными записями пользователей» (п.2.2).

Задание 7. Создать пароль учётной записи и изменить его (п.2.3).

Задание 8. Создать и удалить пароль учётной записи (п.2.4).

Задание 9. Изменить рисунок учётной записи (п. 2.5).

Задание 10. Изменить тип учётной записи (п.2.7).

Задание 11. Включить (отключить) учётную запись «Гость» (п.2.9).

Задание 12. Отключить (активизировать) учётную запись пользователя с помощью оснастки «Локальные пользователи и группы» (п.3.2).

Задание 13.Установить максимальный срок действия пароля 30 дней и минимальный срок действия 10 дней.

Задание 14. Установить требование к сложности и длине пароля (не менее 10 символов).

Задание 15. Установить требование к неповторямости паролей (не менее 3 хранимых паролей).

Задание 16. Использовать шифрование для хранения паролей.

Задание 17. Установите блокировку учётной записи на 5 минут после 3 неудачных попыток входа.

Задание 18. Установите аудит для каждой успешной попытки входа в систему учётной записи пользователя.

Задание 19. Установите аудит каждой попытки изменения политики назначения прав пользователям, аудита, учётной записи или доверия.

Задание 20. Установите аудит событий управления учётными записями на компьютере (создание, перемещение и отключение учётных записей, изменение их паролей и групп).

Задание 21. Предоставьте определённому пользователю право изменения системного времени.

Задание 22. Создайте новую политику безопасности (без последующего изменения её свойств).

Контрольные вопросы:

1. Что такое учётная запись пользователя и какие сведения она может содержать?
2. Какими способами создаётся учётная запись для компьютеров, состоящих в рабочей группе?
3. Какие ограничения накладываются на имя пользователя?
4. Перечислите группы пользователей, встроенные в ОС Windows 7.
5. Как создать учётную запись при помощи оснастки «Локальные пользователи и группы»?
6. Как создать учётную запись при помощи командной строки?
7. Какие действия можно выполнять при помощи окна «Управление учётными записями пользователей»?
8. Какие действия с учётными записями можно производить при помощи оснастки «Локальные пользователи и группы»?
9. Каким образом можно открыть оснастку «Локальная политика безопасности»?
10. Какие интегрированные контейнеры включает консоль «Локальная политика безопасности»?
11. В каком узле политики можно установить требования к длине, сложности пароля?
12. Какие политики можно настраивать в разделе «Политика аудита»?
13. В каком узле можно определить какие пользователи могут управлять аудитом и журналом безопасности?
14. Что такое «Брандмауэр Windows в режиме повышенной безопасности»?
15. Что можно настраивать в области сведений политик диспетчера списка сетей?
16. Как происходит процесс шифрования в EFS?
17. Посредством каких правил производится идентификация ПО при применении политик ограниченного использования программ?
18. Какие уровни используются в политиках ограниченного использования программ?
19. Какие существует 3 варианта настройки для организации защищённого IP-канала – политики безопасности IPSec в рамках одного домена?
20. Опишите последовательность действий при создании и настройке новой политики безопасности IP?

Тестовые задания:

1. Сопоставьте понятия и определения:
    1. Рабочая группа;
    2. Домен;
    3. Учётная запись пользователя.
    a. Это группа компьютеров, подключенных к сети, которые совместно используют ресурсы;
    b. Это запись, которая содержит сведения, необходимые для идентификации пользователя при подключении к системе, а также информацию для авторизации и учёта;
    c. Это группа компьютеров одной сети, имеющих единый центр, использующий единую базу пользователей, единую групповую и локальную политики, единые параметры безопасности, ограничение времени работы учётной записи и прочие параметры, значительно упрощающие работу системного администратора организации, если в ней эксплуатируется большое число компьютеров.
2. Каким образом создать учётную запись при помощи диалога «Управление учётными записями пользователей»?

    a. «Выполнить»→в поле «Открыть» введите *control userpasswords2*→»Учётные записи пользователей»→»Добавить»;

    b. «Пуск»→»Панель управления»→»Учётные записи пользователей»→»Управление другой учётной записью»→»Создание учётной записи»;

    c. «Пуск»→»Панель управления»→»Учётные записи пользователей»→»Добавить учётную запись».
3. Сопоставьте группы пользователей и их определения.
    1. Администраторы;
    2. Операторы архива;
    3. Операторы криптографии;
    4. Группа удалённых помощников;
    5. Читатели журнала событий;
    6. Гости.
    a. Члены этой группы могут предлагать удалённую помощь пользователям данного компьютера;
    b. Пользователи, входящие в эту группу, могут архивировать и восстанавливать файлы на компьютере независимо от любых разрешений, которыми защищены эти файлы. Члены этой группы не могут изменять параметры безопасности;
    c. Членам этой группы разрешается запускать журнал событий Windows;
    d. Членам этой группы разрешено выполнение операций криптографии;

e. Пользователи, входящие в эту группу, имеют полный доступ на управление компьютером и могут при необходимости назначать пользователям права пользователей и разрешения на управление доступом;
f. Пользователи, входящие в эту группу, получают временный профиль, который создаётся при входе пользователя в систему и удаляется при выходе из неё.

4. Сопоставьте группы пользователей и их определения.
   1. Операторы настройки сети;
   2. Пользователи журналов производительности;
   3. Пользователи системного монитора;
   4. Опытные пользователи;
   5. Пользователи удалённого рабочего стола;
   6. Пользователи.

   a. Пользователи, входящие в эту группу, могут управлять счетчиками производительности, журналами и оповещениями на локальном или удалённом компьютере;
   b. Пользователи, входящие в эту группу, могут наблюдать за счетчиками производительности на локальном или удалённом компьютере;
   c. Пользователи, входящие в эту группу, могут выполнять типовые задачи, такие как запуск приложений, использование локальных и сетевых принтеров и блокировку компьютера;
   d. Пользователи, входящие в эту группу, могут изменять параметры TCP/IP, а также обновлять и освобождать адреса TCP/IP. Эта группа не имеет членов по умолчанию;
   e. По умолчанию, члены этой группы имеют те же права пользователя и разрешения, что и учётные записи обычных пользователей;
   f. Пользователи, входящие в эту группу, имеют право удалённого входа на компьютер.

5. Каким образом изменить уже имеющийся пароль учётной записи?

a. «Пуск» → «Панель управления» → «Учётные записи пользователей» → «Изменение своего пароля»;

b. «Пуск» → «Панель управления» → «Учётные записи пользователей» → «Создать новый пароль»;

c. «Пуск» → «Панель управления» → «Учётные записи пользователей» → «Изменить существующий пароль».

6. Как настроить родительский контроль учётной записи?

a. «Пуск» → «Панель управления» → «Администрирование» → «Управление компьютером» → «Локальные пользователи и группы» → «Пользователи» → «Действие» → «Установить родительский контроль»;

b. «Пуск» → «Панель управления» → «Учётные записи пользователей» → «Установить родительский контроль»;

c. «Пуск» → «Панель управления» → «Учётные записи пользователей» → «Управление другой учётной записью» → «Выберите учётную запись для изменения» → «Установить родительский контроль».

7. Каким образом можно создать локальную учётную запись пользователя при помощи оснастки «Локальные пользователи и группы»?

a. «Пуск» → «Панель управления» → «Администрирование» → «Управление компьютером» → «Локальные пользователи и группы» → «Пользователи» → «Действие» → «Добавить»;

b. «Пуск» → «Панель управления» → «Администрирование» → «Управление компьютером» → «Локальные пользователи и группы» → «Пользователи» → «Действие» → «Новый пользователь»;

c. «Пуск» → «Выполнить» → «Открыть» введите *lusrmgr.msc* → «Локальные пользователи и группы» → «Создать учётную запись».

8. С помощью, какой команды можно создать новую учётную запись в командной строке?
   a. net user;
   b. new user;
   c. net new user.
9. Какие действия можно выполнять при помощи диалогового окна «Управление учётными записями пользователей»?
   a. Изменение имени;
   b. Назначение сценариев входа;
   c. Создание пароля; Изменение пароля; Удаление пароля;
   d. Изменение рисунка;
   e. Назначение домашней папки.
10. Какой командой можно вызвать редактор локальной политики безопасности?
    a. sekpol.msc;
    b. secpol.msc;
    c. secpol.mck.
11. На каких пользователей распространяются настройки в узле «Политика паролей»?
    a. Только на администратора;

b. На всех пользователей, за исключением тех, для которых установлены личные настройки в разделе «Пуск»→»Панель управления»→»Администрирование»→»Управление компьютером» → «Пользователи и группы»→»Пользователи»;

c. На всех пользователей.

12. Каким требованиям сложности должен отвечать пароль при установке соответствующей настройки?

a. Содержать буквы верхнего и нижнего регистра одновременно; содержать цифры от 0 до 9; не содержать имени учётной записи пользователя или частей полного имени пользователя длиной более двух рядом стоящих знаков, длина пароля должна быть не менее 8 -10 символов;

b. Содержать буквы верхнего и нижнего регистра одновременно; содержать цифры от 0 до 9; не содержать имени учётной записи пользователя или частей полного имени пользователя длиной более двух рядом стоящих знаков;

c. Содержать буквы верхнего и нижнего регистра одновременно; содержать цифры от 0 до 9; содержать символы, которые отличаются от букв и цифр (например, !, @, #, $, *); не содержать имени учётной записи пользователя или частей полного имени пользователя длиной более двух рядом стоящих знаков.

13. Для чего предназначен протокол Kerberos?

a. Для проверки подлинности учётных записей пользователей и компьютеров домена используется протокол Kerberos;

b. Для идентификации пользователя;

c. Протокол Kerberos используется при передаче данных между компьютерами в домене.

14. В каком узле локальной политики безопасности можно настроить очистку страничного файла виртуальной памяти при выключении компьютера?

a. Назначение прав пользователей;

b. Параметры безопасности;

c. Политики управления приложениями.

15. Какая технология шифрования лежит в основе EFS?

a. Шифрование с использованием секретного (симметричного) ключа, т.е. для шифровки и расшифровки данных используется один и тот же ключ;

b. Шифрования с открытым ключом (асимметричное шифрование) заключается в том, что данные шифруются одним ключом, а расшифровываются другим, с помощью одного и того же ключа нельзя осуществить обратное преобразование;

c. В EFS для шифрования используются все преимущества вышеперечисленных систем.

16. Выберите возможные варианты установки правил ограничения «Политики ограниченного использования программ».

a. На все программное обеспечение устанавливается ограничение на запуск и создаются исключения, то есть список программ, разрешённых к выполнению;

b. На все программное обеспечение устанавливается ограничение на запуск;

c. Разрешается запуск любых программ и создаётся список исключений, запрещающий запуск некоторых программ, доступ к программам определяется правами пользователя.

17. Политика безопасности «Сервер» IP на «Локальный компьютер» предполагает:

a. Для всего IP-трафика всегда запрашивает безопасность с помощью доверия Kerberos. Не разрешает небезопасную связь с недоверенными клиентами;

b. Для всего трафика IP всегда запрашивает безопасность с помощью доверия Kerberos. Разрешает небезопасную связь с клиентами, которые не отвечают на запрос;

c. Использует правило ответа по умолчанию для согласования с серверами, запрашивающими безопасность. Только запрошенный протокол и трафик с этим сервером будут безопасными.

18. Политика безопасности «Безопасность сервера» IP на «Локальный компьютер» предполагает:

a. Для всего IP-трафика всегда запрашивает безопасность с помощью доверия Kerberos. Не разрешает небезопасную связь с недоверенными клиентами;

b. Для всего трафика IP всегда запрашивает безопасность с помощью доверия Kerberos. Разрешает небезопасную связь с клиентами, которые не отвечают на запрос;

c. Использует правило ответа по умолчанию для согласования с серверами, запрашивающими безопасность. Только запрошенный протокол и трафик с этим сервером будут безопасными.

19. Политика безопасности «Клиент» IP на «Локальный компьютер» предполагает:

a. Для всего IP-трафика всегда запрашивает безопасность с помощью доверия Kerberos. Не разрешает небезопасную связь с недоверенными клиентами;

b. Для всего трафика IP всегда запрашивает безопасность с помощью доверия Kerberos. Разрешает небезопасную связь с клиентами, которые не отвечают на запрос;

c. Использует правило ответа по умолчанию для согласования с серверами, запрашивающими безопасность. Только запрошенный протокол и трафик с этим сервером будут безопасными.