**Дисциплина «Защита в операционных системах»**

# Лабораторная работа № 1

**Тема:** Управление пользователями и группами в операционных системах семейства Windows, локальная политика безопасности.

**Цель:**

- изучить способы создания локальных учетных записей пользователей и групп и настройки их свойств;
- изучить возможности настройки локальных политик безопасности для установки требований к паролям и учётным записям, блокировки нежелательных программ и сетевых соединений.

**Время выполнения лабораторной работы (аудиторные часы)** – 4 часа.

**Порядок выполнения лабораторной работы:** работа выполняется самостоятельно под руководством преподавателя.

**Оборудование и программное обеспечение:** работа выполняется на ПЭВМ типа IBM PC с использованием стандартных функций ОС.

## 1. Теоретические сведения

### 1.1 Управление пользователями и группами

В операционной системе Windows на одном и том же компьютере могут работать разные пользователи, каждый под своим именем. При входе в ОС запрашиваются имя и пароль, на основе которых происходит аутентификация пользователя.

Компьютер может работать автономно, а может быть рабочей станцией в сети. Если компьютер загружается для автономной работы или для работы в одноранговой сети, то пользователь регистрируется, используя внутренний (локальный) список имен пользователей системы.

Если компьютер загружается для работы в сети с выделенным сервером, то пользователь регистрируется, используя имя, которое ему выдал администратор сети. Список с этими именами хранится на сервере.

Данные о пользователе находятся в специальной базе данных на локальных компьютерах и на сервере. На каждого пользователя заводится отдельная учетная карточка, которая носит название учетная запись.

В ОС Windows используются следующие типы учетных записей пользователей:

1. Локальные учетные записи для регистрации пользователей локального компьютера. База локальных учетных записей хранится на каждом компьютере

своя, и содержит информацию о пользователях только данного компьютера. Создаются учетные записи администратором этого компьютера.

2. Встроенные учетные записи пользователей создаются автоматически при установке ОС Windows. Встроенных учетных записей две — ***Администратор*** и ***Гость***. Встроенные учетные записи хранятся в той же базе, что и локальные учетные записи.

3. Учетные записи пользователей домена хранятся на выделенном сервере и содержат данные о пользователях локальной сети.

*Локальная учетная запись* — это учетная запись, которой могут быть предоставлены разрешения и права на вашем компьютере. Для удобства управления локальными пользователями, их можно объединять в группы и управлять группами, чтобы не устанавливать одни и те же настройки для каждого пользователя в отдельности. Ограничения, установленные для группы, распространяются на всех пользователей этой группы.

Пользователи и группы важны для безопасности ОС Windows поскольку позволяют ограничить возможность пользователей и групп выполнять определенные действия путем назначения им прав и разрешений. Право дает возможность пользователю выполнять на компьютере определенные действия, такие как архивирование файлов и папок или завершение работы компьютера. Разрешение представляет собой правило, связанное с объектом (например, файлом, папкой или принтером), которое определяет, каким пользователям и какого типа доступ к объекту разрешен.

Операционная система содержит несколько встроенных учетных записей пользователей и групп, которые не могут быть удалены:

Учетная запись пользователя с именем ***«Администратор»*** используется при первой установке рабочей станции или рядового сервера. Эта учетная запись позволяет выполнять необходимые действия до того, как пользователь создаст свою собственную учетную запись. Администратор является членом группы администраторов на рабочей станции или рядовом сервере.

- Учетную запись ***Administrator (Администратор)*** нельзя удалить, отключить или вывести из группы администраторов, что исключает возможность случайной потери доступа к компьютеру после уничтожения всех учетных записей администраторов. Это свойство отличает пользователя «Администратор» от остальных членов локальной группы «Администраторы».
- Учетная запись ***«Guest» (Гость)*** предназначена для тех, кто не имеет реальной учетной записи на компьютере. Учетную запись «Гость» нельзя удалить, но можно переименовать или отключить. Учетной записи пользователя «Гость», как и любой другой учетной записи, можно предоставлять права и разрешения на доступ к объектам. Учетная запись «Гость» по умолчанию входит во встроенную группу «Гости», что позволяет пользователю войти в систему с рабочей станции или сервера. Дополнительные права, как любые разрешения, могут быть присвоены группе «Гости» членом группы «Администраторы».

Далее перечислены 15 встроенных групп в операционных системах семейства Windows, начиная с Windows 7 (см. рис. 1). Права пользователей, входящих в ту или иную группы 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 учетная 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;

- ***Power Users (Опытные пользователи).*** По умолчанию, члены этой группы имеют те же права пользователя и разрешения, что и учетные 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. Начиная с ОС версии Windows Vista учетные 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.

- ***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 учетная запись пользователя, созданная в домене, становится членом этой группы.

- ***Guests (Гости).*** Пользователи, входящие в эту группу, получают временный профиль, который создается при входе пользователя в систему и удаляется при выходе из нее. Учетная запись «Гость» (отключенная по умолчанию) также является членом данной встроенной группы.

- ***IIS_IUSRS.*** Это встроенная группа, используемая службами IIS.

- ***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 (Криптографические операторы).*** Членам этой группы разрешено выполнение криптографических операций.

- ***Debugger Users (Группа удаленных помощников).*** Члены этой группы могут предлагать удаленную помощь пользователям данного компьютера.

- ***Distributed COM Users (Пользователи DCOM).*** Членам этой группы разрешено запускать, активировать и использовать объекты DCOM[1] на компьютере.

- ***Event Log Readers (Читатели журнала событий).*** Членам этой группы разрешается запускать журнал событий Windows.

- ***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 удаленном 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 удаленном компьютере, не являясь при этом участниками групп «Администраторы» или «Пользователи журналов производительности».

- ***Remote Desktop Users (Пользователи удаленного рабочего стола).*** Пользователи, входящие в эту группу, имеют право удаленного входа на компьютер.

- ***Replicator (Репликатор).*** Эта группа поддерживает функции репликации. Единственный член этой группы должен иметь учетную запись пользователя домена, которая используется для входа в систему службы репликации контроллера домена. Не добавляйте в эту группу учетные записи реальных пользователей.

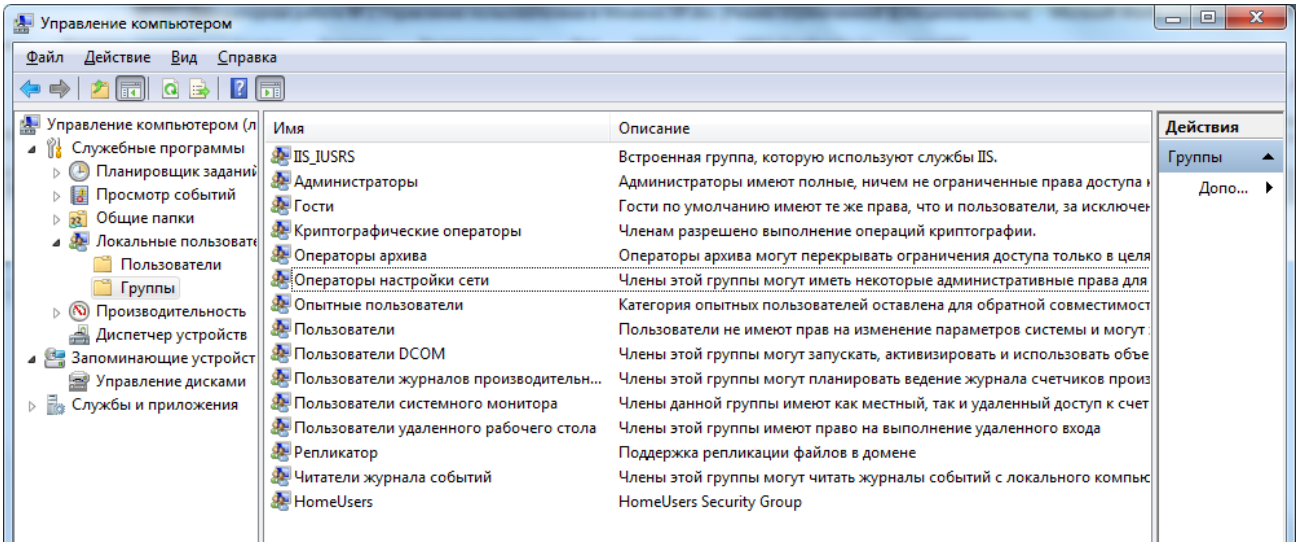


Рисунок 2 – Группы пользователей в ОС Windows 7

[1] **DCOM** (англ. *Distributed COM*) — расширение Component Object Model для поддержки связи между объектами на различных компьютерах по сети.

В более поздних версия ОС семейства Windows (Windows 8, 8.1, 10) добавлены дополнительные встроенные группы, перечень и назначение которых можно изучить, перейдя в соответствующий раздел оснастки ***compmgmt.msc*** «Управление компьютером».

## 1.2 Локальная политика безопасности

Безопасность операционной системы основана на правилах, регулирующих разные аспекты ее работы. Вместе эти правила составляют единую политику безопасности. Начиная с Windows 2000 и более поздних ОС семейства Windows NT политика безопасности представляет собой часть групповой политики. В свою очередь, она состоит из набора правил, объединенных в следующие группы:

— ***Политики учетных записей.*** Регулируют работу с политикой парольной безопасности, требования к паролям, условия блокировок учетной записи.

— ***Локальные политики.*** Включают правила аудита событий, назначения привилегий пользователям и группам и некоторые возможности защиты.

— ***Брандмауэр Windows в режиме повышенной безопасности***. Определяет политику использования брандмауэра Windows в режиме повышенной безопасности, при работе в котором брандмауэр отслеживает состояния, который позволяет задать, прохождение какого сетевого трафика разрешается между компьютером и сетью. Он также содержит правила безопасности подключения, которые используют протокол IPsec для защиты трафика при передаче его по сети.

— ***Политики диспетчера списка сетей.*** В данной политике определяется имя сети, значок и расположение групповых политик.

— ***Политики открытого ключа.*** Позволяют настроить, в частности, правила использования файловой системы с шифрованием (EFS, Encrypted File System). Эти политики и все последующие являются дополнительными, они не используются в шаблонах безопасности и не анализируются и не настраиваются оснасткой Анализ и настройка безопасности.

— ***Политики ограниченного использования программ.*** Разрешают/запрещают запуск программ пользователям.

— ***Политики управления приложениями.*** Политика использования функции AppLocker, включенной в ОС семейства Windows, начиная с Windows 7 и Windows Server 2008 R2, которая заменяет компонент «Политики ограниченного использования программ». AppLocker содержит новые возможности и расширения, которые сокращают затраты на администрирование и помогают администраторам определять, какие пользователи могут получать доступ и работать с такими файлами, как исполняемые файлы, сценарии, файлы установщика Windows и библиотеки DLL.

— ***Политики IP-безопасности.*** Используются для администрирования безопасности протокола IP (IP-Sec). Определяют настройки фильтров IP, а также использование шифрования пакетов.

— ***Конфигурация расширенной политики аудита.*** Позволяет настраивать параметры дополнительной конфигурации политик аудита.

Перечень локальных политик безопасности на примере ОС Windows 10 Pro приведен на рисунке 2.

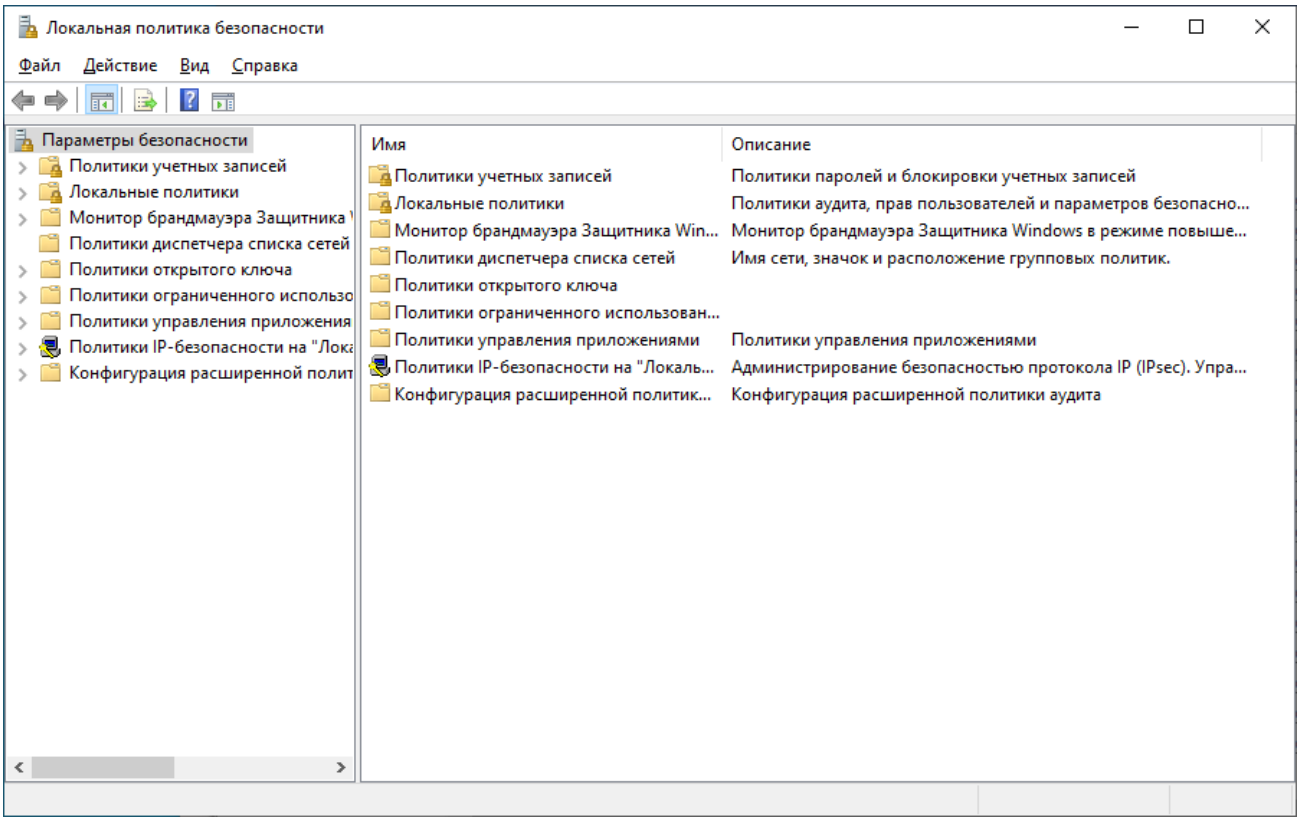


Рисунок 2 – Перечень локальных политик безопасности

### 1.2.1 Политики учетных записей

Данные правила подразделяются на две группы: *политика паролей* и *политика блокировки учетной записи*.

Правила паролей задают требования, предъявляемые к паролям пользователей системы.

Так как среди злоумышленников популярностью пользуются атаки, заключающиеся в подборе пароля по заранее составленному файлу с набором типичных паролей («словарная атака») и просто грубому перебору всех возможных комбинаций символов («brute force»), то необходимо принять меры, страхующие систему от подобных методов взлома. Именно эти задачи и решает политика блокировки учетной записи. В рамках рассматриваемой политики имеется возможность: установки количества ошибочных попыток набора пароля, блокировки учетной записи, срока этой блокировки и периода сброса счетчика неудачных попыток ввода пароля. Это мощное средство, однако им нужно пользоваться с осторожностью, так как возможен обратный эффект от его действия — взломщик может просто заблокировать аккаунт администратора, перешагнув порог блокировки учетной записи своими попытками подобрать пароль. Именно для этого существует правило, задающее срок этой блокировки.

Одним из источников нормативных требований по настройке различных локальных и групповых политик безопасности информационных систем общего назначения, в которых обрабатывается информация ограниченного доступа, является РД ФСТЭК РФ «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации».

На рисунке 3 приведен фрагмент обязательных и рекомендуемых требований политики учетных записей для различного класса ОС.

| Параметр | Классы защищенности АС | | |
|---|---|---|---|
| | 1Б, 1В, 1Г, 1Д | 2А, 2Б | 3А, 3Б |
| **Группа "Вход в систему"** | | | |
| **Максимальный период неактивности до блокировки экрана** | все: Не более 10 (реком.) | все: Не более 10 (реком.) | все: Не более 10 (реком.) |
| **Запрет вторичного входа в систему** | все: Да (реком.) | все: Да (реком.) | все: Да (реком.) |
| **Режим идентификации пользователя** | все: Смешанный (реком.) | все: Смешанный (реком.) | все: Смешанный (реком.) |
| **Режим аутентификации пользователя** | все: Усиленная по паролю (обяз.) | все: Усиленная по паролю (обяз.) | все: Усиленная по паролю (обяз.) |
| **Режим аутентификации пользователя: Регистрировать неверные аутентификационные данные** | 1Б,1В,1Г: Да (обяз.)<br>1Д: – | все: Да (обяз.) | 3А: Да (обяз.)<br>3Б: – |
| **Парольная политика** | все: Заданы значения (обяз.) | все: Заданы значения (обяз.) | все: Заданы значения (обяз.) |
| **Минимальная длина пароля** | 1Б: Не менее 8 символов (обяз.)<br>1В,1Г,1Д: Не менее 6 символов (обяз.) | все: Не менее 6 символов (обяз.) | все: Не менее 6 символов (обяз.) |
| **Срок действия пароля** | 1Б: Не более 90 дней (обяз.)<br>1В,1Г,1Д: Не более 180 дней (обяз.) | все: Не более 180 дней (обяз.) | все: Не более 180 дней (обяз.) |

Рисунок 3 - Обязательные и рекомендуемые требования политики учетных записей

### 1.2.2 Локальные политики

Локальные политики определяют правила безопасности локального компьютера. Они делятся на три группы: политики аудита, назначение прав пользователя и параметры безопасности.

Политика аудита предписывает заносить в журнал Безопасность те или иные события (удачные и/или неудачные). После указания событий, требующих регистрации, можно указать конкретные объекты, за которыми будет вестись слежение (например, после разрешения аудита доступа к объектам можно в

свойствах папки указать ведение аудита доступа для конкретных пользователей и/или групп).

### 1.2.3 Политики открытого ключа

Используя политики открытого ключа, администратор может автоматически выдавать сертификаты компьютерам, управлять агентами восстановления шифрованных данных, создавать списки доверия сертификатов и автоматически устанавливать доверительные отношения с центрами сертификации.

### 1.2.4 Политики ограниченного использования программ

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

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, что еще хуже, содержать вирусы или «троянские» программы для несанкционированного удаленного доступа.

При интенсивном использовании сетей, Интернета и электронной почты 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.

## 2. Задание

### 2.1 Задание «Управление пользователями и группами»

Для управления учетными записями используется компонент ***«Управление компьютером»***. Чтобы его открыть выберите ***Пуск → Настройка → Панель управления***. Дважды щелкните значок ***«Администрирование»*** затем дважды щелкните значок ***«Управление компьютером»***. Второй способ открыть ***«Управление компьютером»*** нажать правой кнопкой на значке ***«Мой компьютер»*** и в появившемся контекстном меню выбрать ***«Управление»***.

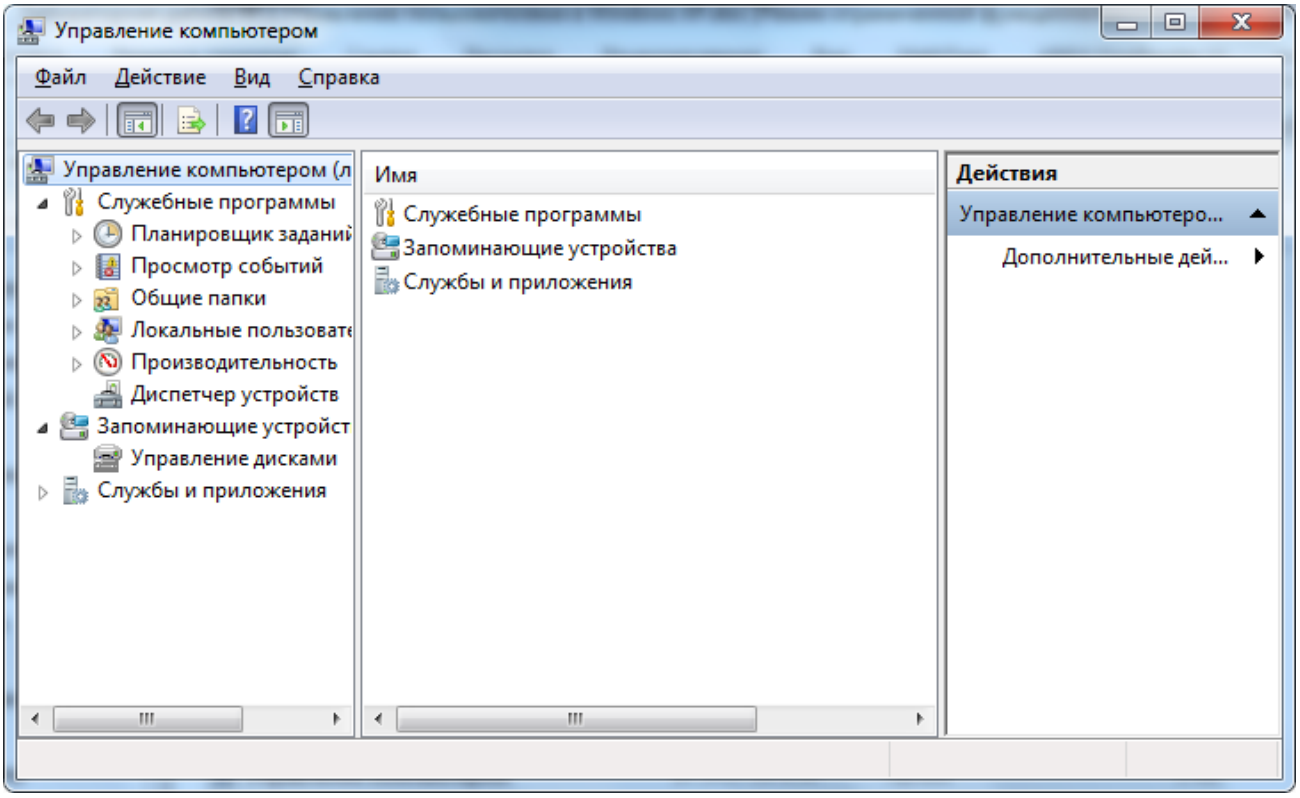


*Рис. 2.2 Оснастка «Управление компьютером»*

#### 2.1.1 Создание новой учетной записи пользователя

Откройте компонент ***«Управление компьютером»*** одним из описанных выше способов.

В дереве консоли (слева) выберите *компонент* ***«Локальные пользователи и группы»*** и щелкните в нем узел ***«Пользователи»***.

Нажмите правой кнопкой мыши в окне со списком пользователей и в появившемся меню выберите команду ***«Новый пользователь»*** (см. рис.2.3).

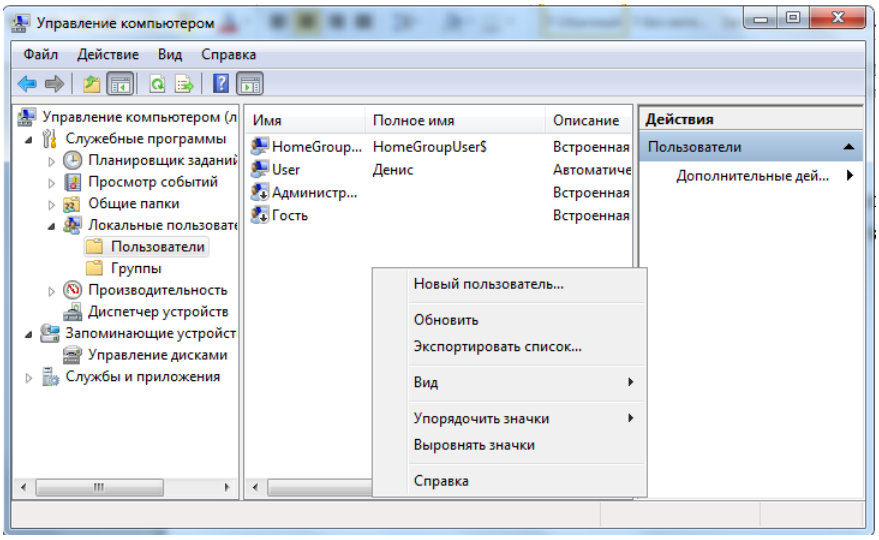


*Рис. 2.3 Создание нового пользователя из оснастки «Управление компьютером»*

В появившемся окне заполните поля **«Пользователь»**, содержащее имя, под которым пользователь будет входить в систему, а также **«Пароль»** и **«Подтверждение»**.

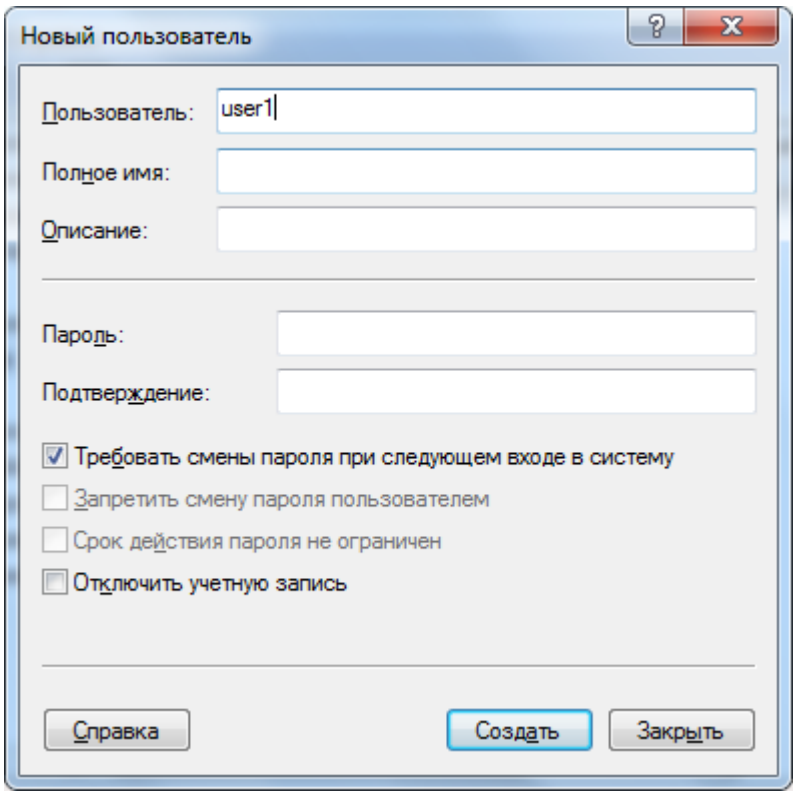


*Рис. 2.4 Создание нового пользователя*

По умолчанию в данном окне стоит опция **«Потребовать смену пароля при следующем входе в систему»**. То есть система при первом входе пользователя в ОС потребует от него сменить пароль. Если убрать галочку с этого пункта, появится возможность выбрать следующие опции:

— *запретить смену пароля пользователем*. Пользователь будет использовать пароль, заданный при создании учетной записи;

— *срок действия пароля не ограничен*.

Опция **«Отключить учетную запись»** делает вход в систему данного пользователя невозможным.

Чтобы завершить работу, нажмите кнопку **«Создать»**, а затем **«Закрыть».**

Если есть необходимость в создании сразу нескольких пользователей нужно нажать на кнопку **«Создать»** и повторить все предыдущие шаги.

Помимо вышеперечисленного способа, учетные 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 учетной записи при помощи командной строки используйте команду net user[2](см. рис. 2.5).

Информация об учетных записях пользователей хранится в базе данных учетных записей пользователей.

**Пример команды:**

net user User2 /add /times:monday-friday,9am-6pm /fullname:"New user"

Используемые параметры:

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

/times – Время для входа в систему. Параметр время указывается в формате день[-день][,день[-день]],час [-час][,час [-час]], причем приращение равняется 1 часу. Название дней недели могут указываться полностью или в сокращенном виде. Часы могут указываться в 12- или 24-часовом представлении. Для 12-часового представления используются обозначения am, pm, a.m. или p.m. Значение all соответствует отсутствию ограничений на время входа в систему, а пустое значение обозначает полный запрет на вход в систему. Значения дней недели и времени разделяются запятой; несколько записей для значений дней недели и времени разделяются точкой с запятой;

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

/active:{yes|no} - Активирует или деактивирует учетную запись. Если учетная запись не активирована, пользователь не может получить доступ к серверу. По умолчанию учетная запись активирована.

/delete - Удаление учетной записи пользователя.

/expires:{дата|never} - Дата истечения срока действия учетной записи. Значение never соответствует неограниченному сроку действия. Дата указывается в формате мм/дд/гг или дд/мм/гг в зависимости от кода страны. Месяц может указываться цифрами, полностью или в сокращенном виде (тремя буквами). Год может указываться двумя ли четырьмя цифрами. Элементы даты разделяются слэшем (/) без пробелов.

---

[2] *Команда **net user** используется для добавления пользователей, установки паролей, отключения учетных записей, установки параметров и удаления учетных записей. При выполнении команды без параметров командной строки отображается список учетных записей пользователей, присутствующих на компьютере.*

/passwordchg:{yes|no} - Указывает, может ли пользователь изменять свой пароль (по умолчанию может).

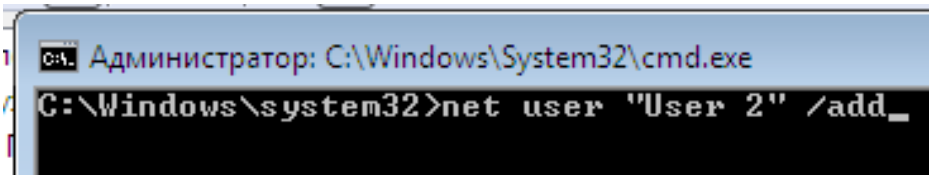


*Рис. 2.5 Создание нового пользователя с использованием командной строки*

Создайте пользователей User 1 (создается через оснастку «Управление компьютером») и User 2 (создается с использованием командной строки). После создания пользователи должны появится в списке выбора пользователей на начальном экране загрузки. Сделайте скриншот полученного результата.

Войдите от имени созданного пользователя User 2. Далее смените пользователя на пользователя User 1. Для этого нажмите ***«Пуск» → «Выход из системы» → «Смена пользователя»***.

На появившемся экране выберите созданного пользователя «User 1» и введите заданный для него при создании пароль.

Появится окно с сообщением о необходимости изменения пароля. Задайте новый пароль и сделайте скриншот окна в котором проводились изменения.

Вернитесь обратно к пользователю «User 2». Для этого нажмите ***«Пуск» → «Выход из системы» → «Выход».***

Разница между вариантами выхода из системы «Смена пользователя» и «Выход» заключается в том, что при смене пользователя все процессы, запущенные им, продолжают выполняться, а при выходе завершаются. Если завершить работу, используя учётную запись одного пользователя, пока второй остаётся в системе, это может привести к потере несохраненных данных приложений второго пользователя.

### 2.1.2 Изменение пароля пользователя

Выберите учетную запись, которую требуется изменить (например, учетная запись пользователя «User1»).

В контекстном меню выберите пункт «Задать пароль».

В появившемся окне введите новый пароль и сделайте скриншот результата.

Войдите в систему от имени пользователя «User1» используя новый пароль.

Аналогичным образом задайте пароль учётной записи «User 2».

### 2.1.3 Отключение и активизация учетной записи пользователя

Выберите учетную запись «User1».

В контекстном меню выберите Свойства.

Чтобы отключить выбранную учетную запись пользователя, установите флажок «Отключить учетную запись».

Отключение учетной записи также возможно с использованием команды net user с параметрами **net user имя пользователя /active:no**

Отключите учетную запись пользователя User 1 любым из приведенных способов, попробуйте войти от имени «User1». Сделайте скриншот результата.

### 2.1.4 Удаление учетной записи пользователя

Выберите учетную запись «user1».

В контекстном меню учетном записи выберите Удалить.

Появится окно, предупреждающее о последствиях удаления пользователя.

Выберите ДА. Сделайте скриншот полученного результата.

Удаление учетной записи также возможно с использованием команды net user с параметрами **net user имя пользователя /delete**

### 2.1.5 Управление группами пользователей

Пользователь, принадлежащий группе, имеет все права на разрешения, предоставленные этой Группе. Пользователь, являющийся членом нескольких групп, имеет все права и разрешения, предоставленные каждой из этих групп.

При удалении локальной группы удаляется учетная запись группы. Учетные записи пользователей, являющихся членами удаленной группы, при этом не удаляются.

Вновь созданные пользователи попадают в группу ***«Пользователи»***. Чтобы убедиться в этом откройте компонент ***«Управление компьютером»***, в дереве консоли выберите ***«Локальные пользователи и группы»*** и щелкните в нем узел ***«Группы»,*** после чего появится список существующих групп (см. рис. 2.1).

Управление группами пользователей (добавление, отображение и изменение локальных групп) также осуществляется с использованием командной строки, по средсвам команды **net localgroup**. Ввод команды **net localgroup** без параметров выводит имя сервера и имена локальных групп компьютера.

**Синтакис команды NET LOCALGROUP**

net localgroup [имя_группы [/comment:"текст"]] [/domain]

net localgroup [имя_группы {/add [/comment:"текст"] | /delete} [/domain]]

net localgroup [имя_группы имя [ ...] {/add | /delete} [/domain]],

где:

- имя_группы - Имя локальной группы для добавления, удаления или раскрытия. При запуске команды net localgroup имя_группы без дополнительных параметров выводится список пользователей или глобальных групп, входящих в локальную группу.

- /comment:"текст" - Добавление комментария для новой или существующей группы. Длина комментария может составлять до 48 знаков. Текст следует заключать в кавычки.

- /domain - Выполнении операции на основном контроллере текущего домена. В противном случае операция осуществляется на локальном компьютере.

- имя [ ...] - Список из одного или нескольких имен пользователей или групп для добавления или удаления из локальной группы.

- /add - Добавление глобальной группы или пользователя в локальную группу. Для пользователей или глобальных групп группы, добавляемых в локальную группу, должны иметься учетные записи.

- /delete - Удаление группы или пользователя из локальной группы.

- net help localgroup - Отображение справки для указанной команды net.

Примеры команды NET LOCALGROUP:

1) Вывод списка всех локальных групп на локальном сервере: **net localgroup**;

2) Добавить локальную группу «Group1» в локальную базу учетных записей пользователей: **net localgroup Group1 /add**;

3) Добавить учетные записи существующих пользователей «User1», «User2» в группу «Group1»: **net localgroup Group1 User1 User2 /add**;

4) Вывести список пользователей локальной группы «Group1»: **net localgroup Group1**.

Нажмите дважды на группу ***«Пользователи»*** и посмотрите, какие учётные записи входят в эту группу. Сделайте скриншот данного окна.

Добавьте пользователя «User 1» в группу «Опытные пользователи» с помощью командной строки, сделайте скиншот результата.

Попробуйте от имени пользователя «User 2» создать файл на диске C:. Пользователи группы «Пользователи» не имеют данного права, поэтому будет выдано сообщение о невозможности выполнения данной операции. Сделайте его скриншот.

Выйдите из системы и зайдите от имени пользователя «Администратор».

Добавьте пользователя «User2» в группу «Администраторы», используя графический интерфейс. Для этого нажмите правой кнопкой на имени группы и выберите пункт меню «Добавить в группу…» (рис. 2.6).

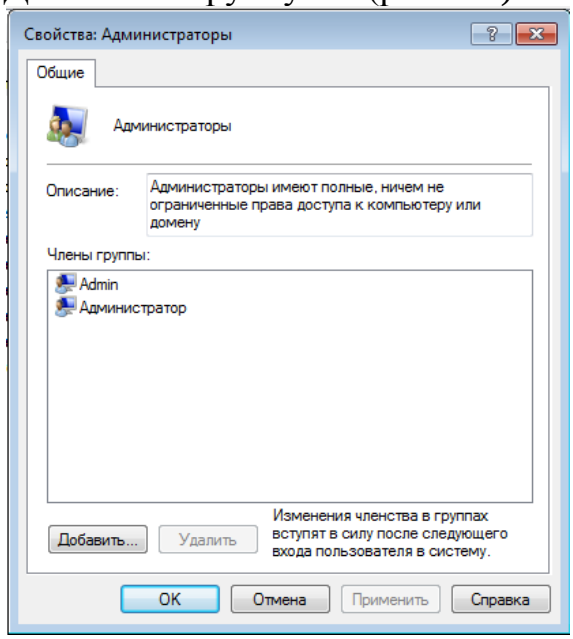


*Рис. 2.6 Добавление пользователя «User2» в группу «Администраторы»*

Появится окно выбора пользователя. Введите имя «User 2» и нажмите «OK».

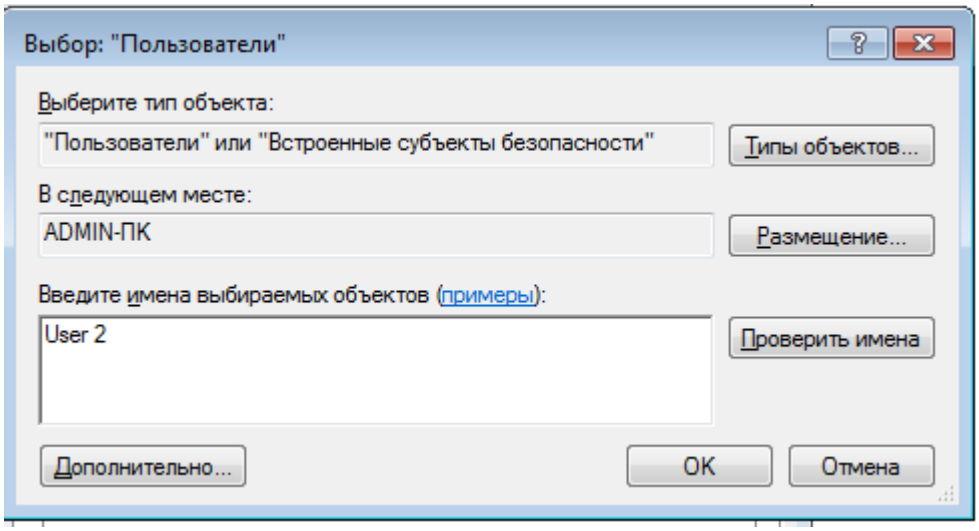


*Рис. 2.7 Окно добавления пользователя «User 2» в группу «Администраторы»*

Зайдите снова от имени «User 2» и создайте на диске C: любой файл. Сделайте скриншот результата.

## 2.2 Задание «Локальная политика безопасности»

Для выполнения задания 2.2 лабораторной работы используется консоль «Локальная политики безопасности». Чтобы открыть её нажмите ***Пуск → Панель управления → Администрирование → Локальная политики безопасности***.

### 2.2.1 Политика паролей

Откройте вкладку ***«Политики учётных записей» → «Политика паролей»***.

Установите минимальную длину пароля — 8 символов.

Смените пароль любому из существующих пользователей и проверьте невозможность задания пароля длиной меньше 8 символов. Сделайте скриншот соответствующего сообщения.

Включите требование ***«Пароль должен отвечать требованиям сложности»***.

Смените пароль любому пользователю. Приведите примеры паролей отвечающих требованиям сложности и не отвечающих данным требованиям.

### 2.2.2 Блокировка учётных записей

Откройте вкладку ***«Политики учётных записей» → «Политика блокировки учётной записи»***.

Измените параметр ***«Ошибок входа в систему»*** политики ***«Пороговое значение блокировки»*** на 3 (см. рис. 2.8).

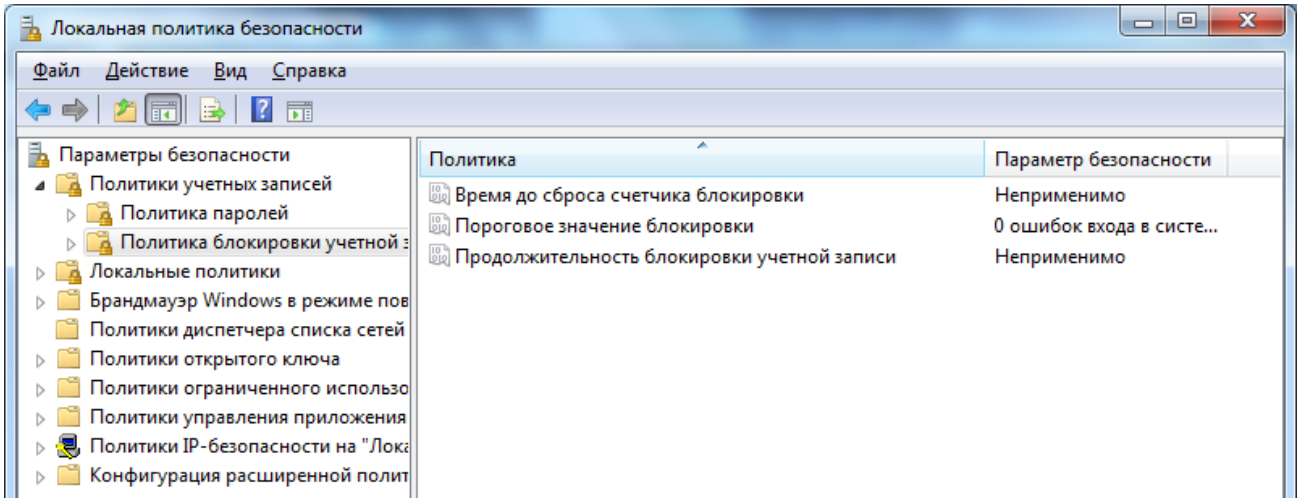


*Рис. 2.8 Окно настройки политики блокировки учетных записей пользователей*

Попытайтесь войти от имени любого пользователя, например: User 1, имеющего пароль, введя неправильный пароль 3 раза. Затем введите правильный пароль и снова попытайтесь выполнить вход.

Откройте консоль управления компьютером. Для этого нажмите на значке ***«Мой компьютер»*** правой кнопкой мыши и выберите пункт меню ***«Управление»***. Откройте папку ***«Локальные пользователи и группы» → «Пользователи»*** и дважды щелкните на пользователя от имени которого Вы пытались выполнить вход. Обратите внимание на установленный флажок ***«Заблокировать учётную запись»***, объясните причину блокировки пользователя, сделайте скриншот окна свойств пользователя.

### 2.2.3 Аудит

В консоли ***«Локальная политика безопасности»*** откройте папку ***«Локальные политики» → «Политики Аудита»*** и в окне свойств каждого параметра установите флажки ***«Вести аудит следующих попыток доступа»*** в пунктах «Успех» и «Отказ» (см. рис. 2.9).

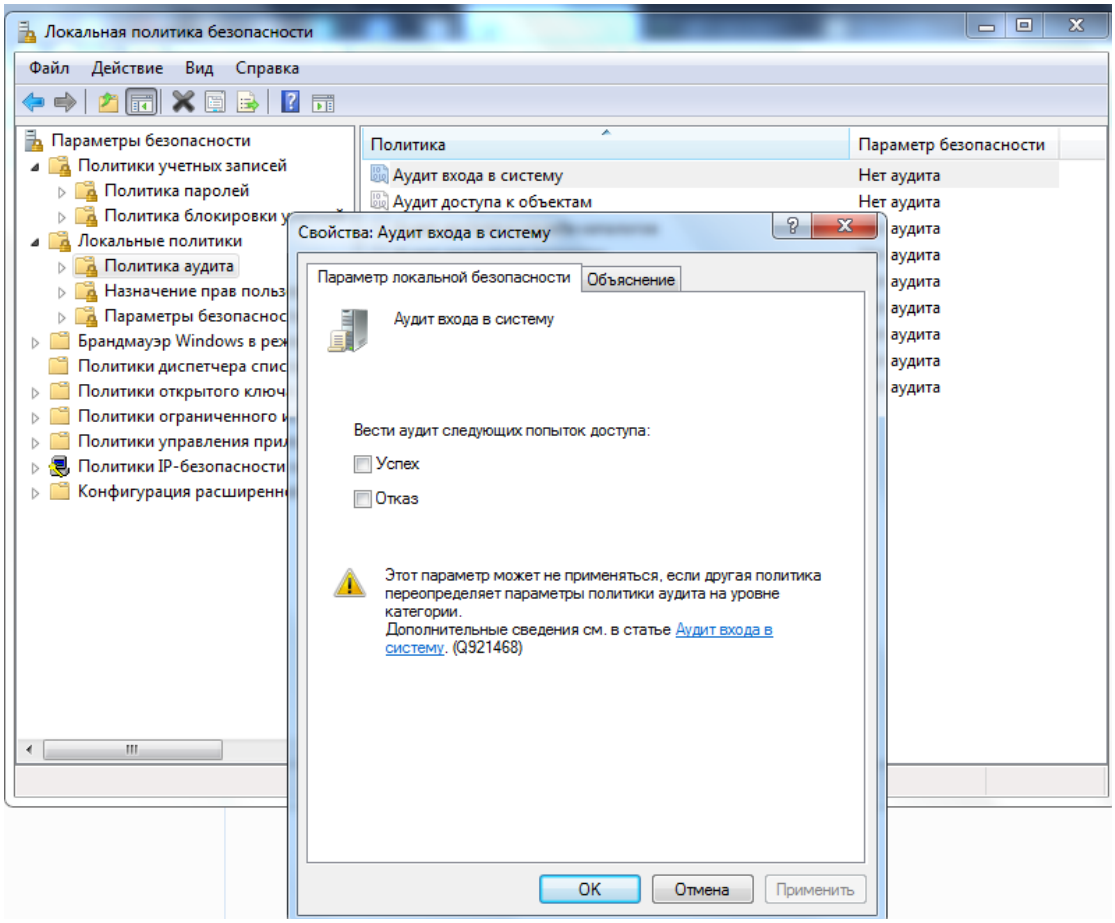


*Рис. 2.9 Окно настройки политики аудита для параметра локальной безопасности «Аудит входа в систему»*

Откройте консоль «Управление компьютером», выберите раздел ***«Служебные программы» → «Просмотр событий» → «Безопасность».***

Найдите последнюю по времени запись, относящуюся к категории «Изменение политики» откройте её и посмотрите описание события, в котором должны быть указаны новые настройки политик аудита, а ниже — пользователь, изменивший их. Текст описания события необходимо поместить в отчёт.

Попытайтесь войти под учетной записью, заблокированной в ходе выполнения предыдущего задания, и определите, какие записи в журнале аудита событий безопасности будут при этом созданы. Приведите в отчёте описание событий зарегистрированных в журнале.

Попытайтесь войти под учетной записью какого-либо пользователя, вводя неправильный пароль несколько раз до блокировки учётной записи. Найдите в журнале событий безопасности появившиеся при этом записи и приведите их в отчёте.

### 2.2.4 Политики прав пользователей и безопасности

В консоли «Локальная политика безопасности» откройте папку ***«Локальные политики» → «Назначение прав пользователя».***

Найдите параметр ***«Завершение работы системы»*** дважды щелкните на нём, чтобы открыть окно свойств и из перечисленных в нём групп удалите группу ***«Пользователи»***.

Зайдите от имени пользователя, входящего в эту группу, и попытайтесь завершить работу, сделайте скриншот результата.

Откройте ***«Локальные политики» → «Параметры безопасности»***.

Найдите параметр ***«Интерактивный вход в систему: Заголовок сообщения для пользователей при входе в систему»*** и в окне его свойств:

- в поле для ввода впишите любой заголовок сообщения (например: «Сообщение»);

- в поле для ввода впишите любой текст сообщения (например: «Привет»).

Зайдите от имени любого пользователя и сделайте скриншот с окном сообщения, появляющимся при входе.

### 2.2.5 Запрет запуска программ

Политики ограниченного использования программ, SRP (англ. Software Restriction Policies) – это основанная на групповых политиках функция, которая выявляет программы, работающие на компьютерах в домене, и управляет возможностью выполнения этих программ. Эти политики позволяют создать конфигурацию со строгими ограничениями для компьютеров, где разрешается запуск только определенных приложений. Политики интегрируются с доменными службами Active Directory и групповой политикой, но также могут настраиваться на изолированных компьютерах.

Политики ограниченного использования программ позволяют определить уровень безопасности по умолчанию и правила (исключения из уровня безопасности по умолчанию), указывающие, какие программы могут выполняться на компьютере. Политики ограниченного использования программ применяются при попытке выполнения программного обеспечения пользователем или процессом.

Начиная с Windows Server 2008 R2 и Windows 7, вместо политики SRP или вместе с ней в рамках стратегии управления приложениями можно использовать Windows AppLocker[3].

В ОС Windows предусмотрено три уровня безопасности при реализации Политики ограниченного использования программ:

1) «Запрещено» - программное обеспечение запускаться не будет вне зависимости от прав доступа пользователя;

2) «Обычный пользователь» - разрешает выполнение программ без прав администратора, но позволяет обращаться к ресурсам, доступным обычным пользователям;

---

[3] AppLocker - это новый компонент в Windows 7 и Windows Server 2008 R2, при помощи которого можно указать, какие пользователи и группы в организации могут запускать определенные приложения в зависимости от уникальных идентификаторов файлов. Используется Windows 7 Максимальная, Windows 7 Корпоративная и Windows Server 2008 R2

3) «Неограниченный» - доступ программ к ресурсам определяется правами пользователя.

В консоли ***«Локальная политика безопасности»*** выделите папку ***«Политики ограниченного использования программ»***. В основном окне появится надпись ***«Политики ограниченного использования программ не определены»*** (см. рис. 2.10).

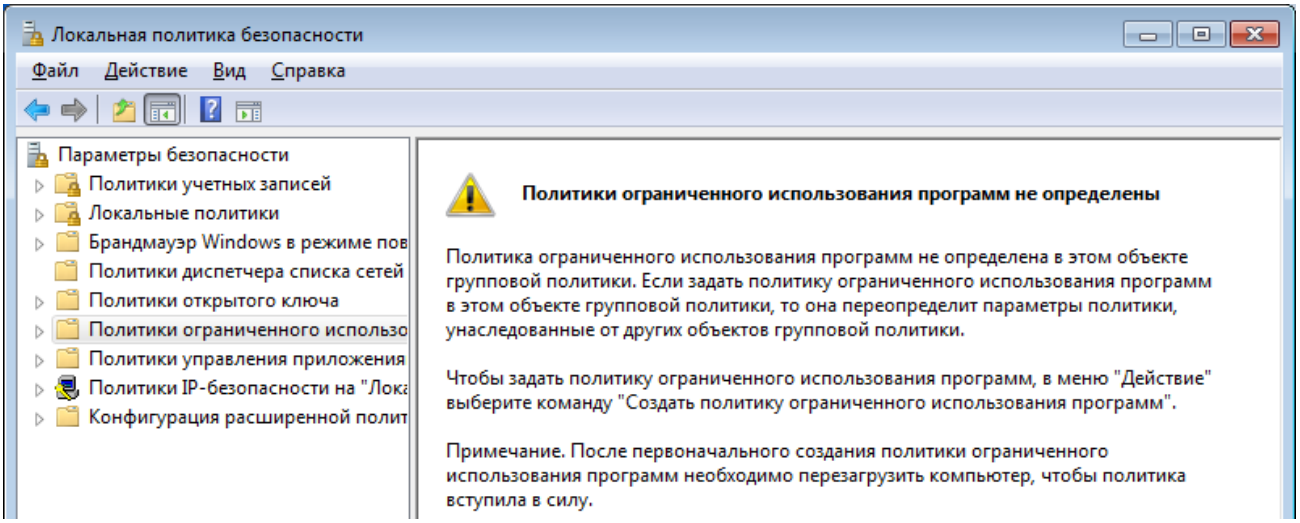


*Рис. 2.9 Окно начальной настройки политики ограниченного использования программ*

Нажмите правой кнопкой мыши на папке ***«Политики ограниченного использования программ»*** и выберите пункт контекстного меню ***«Создать политику ограниченного использования программ»*** (см. рис. 2.10).

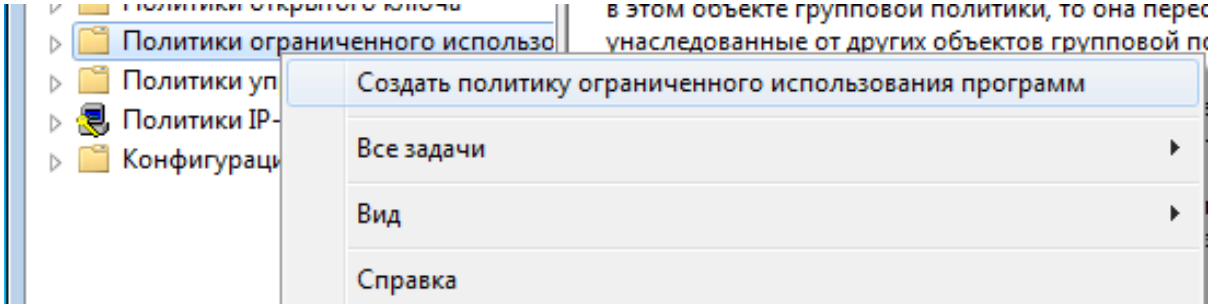


*Рис. 2.10 Создание новой политики ограниченного использования программ*

Зайдите в папку ***«Дополнительные правила»***. Нажмите правой кнопкой мыши и выберите пункт контекстного меню «***Создать правило для хеша…»***.

В появившемся окне нажмите кнопку «Обзор…» и выберите хешируемый файл. Это может быть любой исполняемый файл какого-либо приложения (например калькулятор Windows — C:\Windows\system32\calc.exe) (см. рис. 2.11).

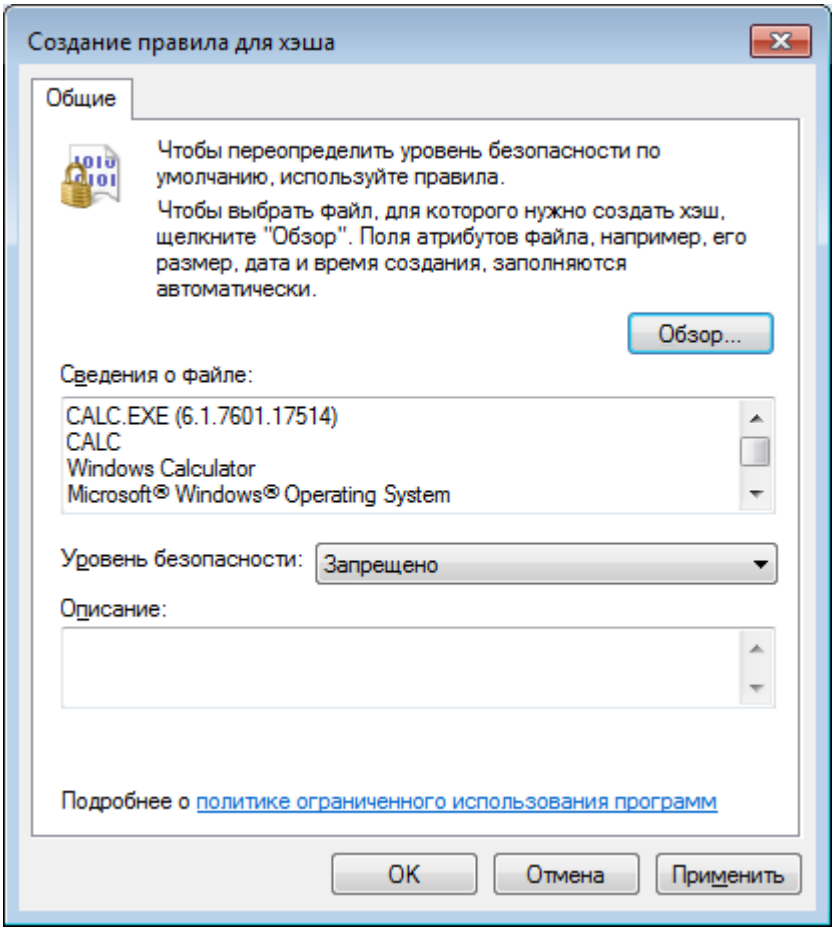


*Рис. 2.11 Создание правила для хеша исполняемого файла calc.exe политики ограниченного использования программ*

В выпадающем меню «Безопасность» оставьте значение «Запрещено» и нажмите «ОК».

Попытайтесь запустить калькулятор и сделайте скриншот результата. Правило, созданное для хеша применяется к файлу независимо от того где он находится. Можно переместить файл calc.exe в любую другую папку, и он по-прежнему не будет запускаться.

**Создайте правило для пути.** Для этого нажмите правой кнопкой на папке ***«Дополнительные правила»*** и выберите пункт ***«Создать правило для пути…»***.

В появившемся окне нажмите кнопку ***«Обзор…»*** и укажите путь к папке, для которой требуется создать правило (например: папка «Мои документы» текущего пользователя).

В выпадающем меню «Безопасность» оставьте значение «Запрещено» и нажмите «ОК».

Поместите в папку «Мои документы» любой исполняемый файл какой-либо программы (можно скопировать туда например файл regedit.exe из папки C:\Windows).

Попытайтесь запустить скопированный файл и сделайте скриншот результата.

Скопируйте еще один исполняемый файл в папку «Мои документы» (пусть теперь это будет блокнот C:\Windows\notepad.exe) и попытайтесь запустить его.

## 3. Контрольные вопросы

1. Какой компонент используется для управления учётными записями пользователей и как получить к нему доступ?
2. Кто может осуществлять управление учётными записями?
3. В чём разница между выходом из системы и сменой пользователя?
4. Как сменить пароль учётной записи?
5. Что такое отключение учётной записи? Чем оно отличается от удаления? Как отключить учётную запись?
6. Для чего предназначены группы пользователей?
7. Как добавить пользователя в группу?
8. Каким требованиям должен отвечать пароль при включении параметра «Пароль должен отвечать требованиям сложности»?
9. Что такое пороговое значение блокировки в политике учётных записей?
10. Что такое «Политики аудита»?
11. Что такое политики ограниченного использования программ?
12. Какие уровни безопасности могут использоваться в правилах политик ограниченного использования программ?
13. Чем отличается правило для хеша и правило для пути в политиках ограниченного использования программ?

## 4. Требования к отчёту

Отчёт выполняется каждым студентом индивидуально. Работа должна быть оформлена в электронном виде в формате .doc и распечатана на листах формата А4. На титульном листе указываются: наименование учебного учреждения, наименование дисциплины, название и номер работы, вариант, выполнил: фамилия, имя, отчество, группа, проверил: преподаватель ФИО (приложение 1).

Отчёт по лабораторной работе должен содержать:

— титульный лист,
— цель работы,
— описание хода выполнения работы со скриншотами;
— вывод.

**Приложение 1**

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ

**ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ «ДОНСКОЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ» (ДГТУ)**

Факультет «Информатика и вычислительная техника»

Кафедра «Кибербезопасность информационных систем»

**Лабораторная работа № ____**
на тему «_____»

Выполнил обучающийся гр._____

_____
(Фамилия, Имя, Отчество)

Проверил:

_____
(должность, Фамилия, Имя, Отчество)

Ростов-на-Дону
20__