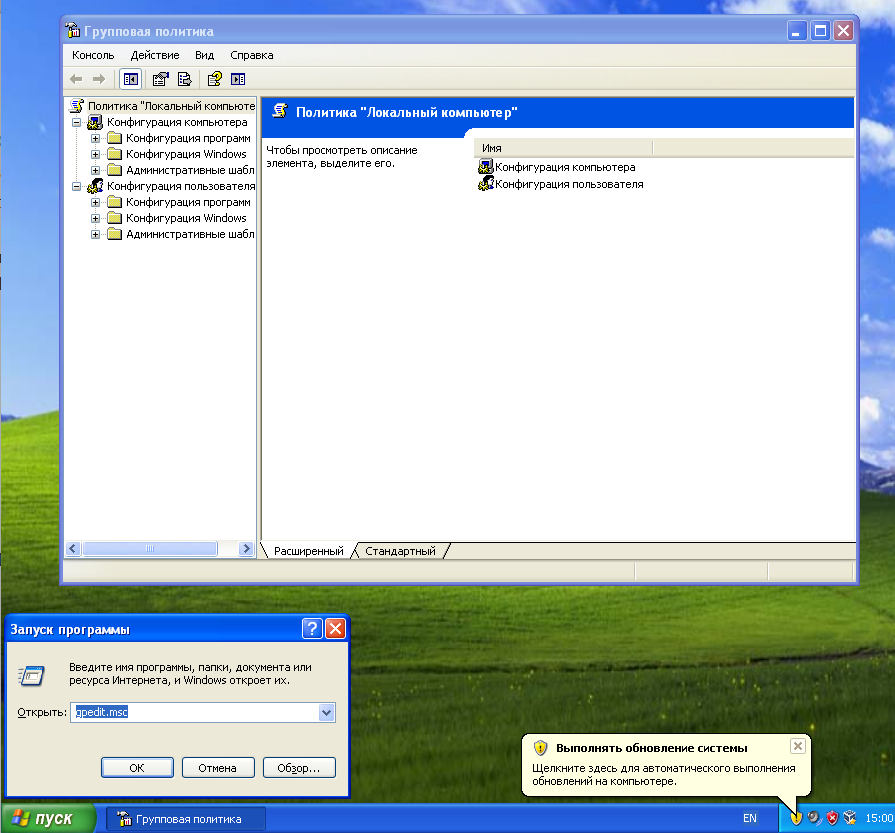
## **Изучение оснастки локальных политик Windows XP**

Работу выполнил студент 431гр. Никитин А.В.

Запустить оснастку управления локальными политками.

Для того, чтобы открыть консоль управления политиками, ввел gpedit.msc:



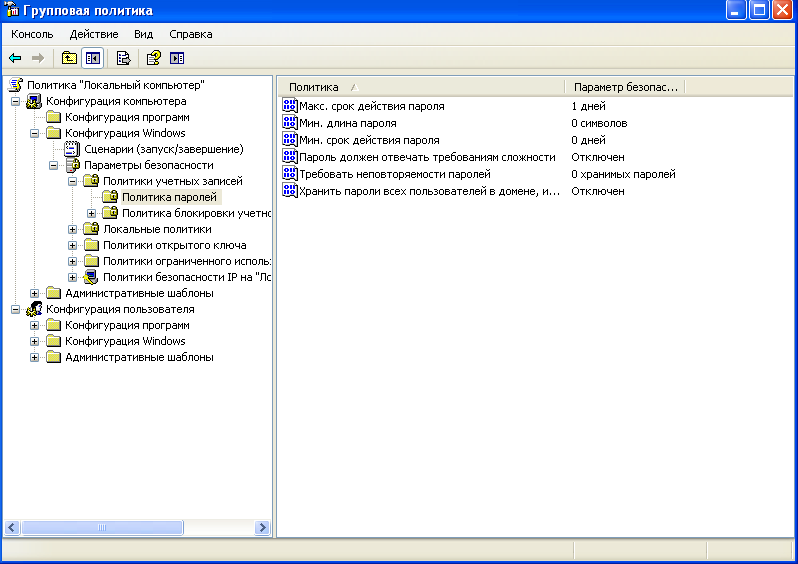
Выписать смысл следующих политик:

1. Политика учётных записей
   1. Политика паролей
      1. **Макс. Срок действия пароля**

Этот параметр безопасности определяет период времени (в днях), в течение которого пароль можно использовать, пока система не потребует от пользователя сменить пароль. Срок действия пароля может составлять от 1 до 999 дней; значение 0 соответствует неограниченному сроку действия пароля. Если значение максимального срока действия пароля составляет от 1 до 999 дней, то значение минимального срока действия пароля должно быть меньше максимального. Если значение максимального срока действия пароля равно 0, то значением минимального срока действия пароля может быть любое количество дней от 0 до 998. По умолчанию максимальный срок действия пароля составляет 42 дня.

Попробуем изменить максимальный срок действия пароля на 1 день и отмотаем время в нашей машине на сутки.

Далее политика, почему-то не предложила сменить пароль, даже после перезагрузки системы.



* + 1. **Пароль должен отвечать требованиям сложности**

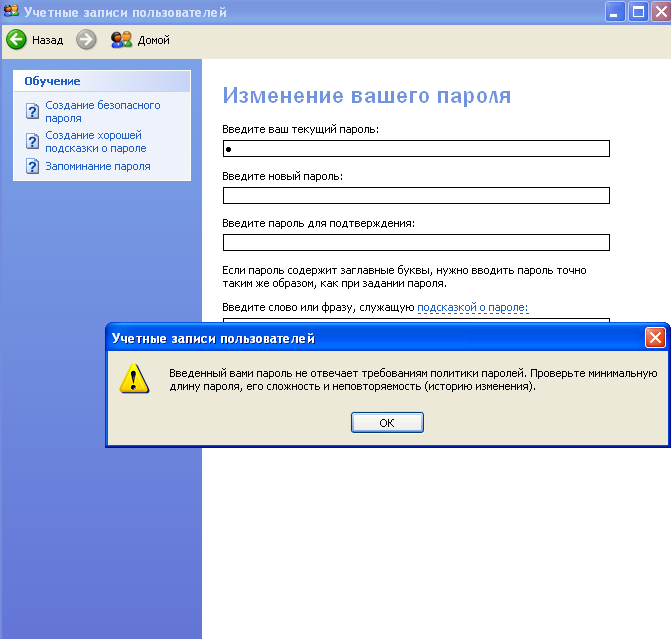
Если эта политика включена, пароли должны удовлетворять следующим минимальным требованиям:

1. Пароль не должен содержать имя учетной записи пользователя или фрагменты имени пользователя длиной больше двух символов.
2. Пароль должен состоять не менее чем из шести символов.
3. Пароль должен содержать символы, относящиеся к трем из следующих четырех категорий:
4. латинские заглавные буквы (A - Z);
5. латинские строчные буквы (a - z);
6. цифры (0 - 9);
7. отличные от букв и цифр символы (например, !, $, #, %).

Проверка соблюдения этих требований выполняется при изменении или создании паролей.

Изначально поставил пароль «1».

Попробуем включить политику и попытаемся изменить исходный пароль, не попадающий под требования, например, пусть это будет пароль «1234»:

Как видно из скриншота, пароль со включенной политикой поменять не получилось.

* + 1. **Требовать неповторяемость паролей**

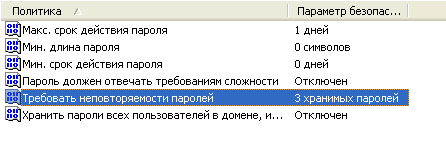
Этот параметр безопасности определяет количество новых паролей, которые необходимо связать с учетной записью пользователя перед повторным использованием старого пароля. Значение должно быть в диапазоне от 0 до 24.

Эта политика позволяет администраторам повысить уровень безопасности, предотвращая постоянное использование старых паролей.

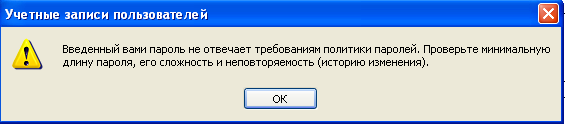
По умолчанию:

1. 24 - на контроллерах домена.
2. 0 - на автономных серверах.

На рисунке ниже показан один из вариантов действия политики.



Изменил исходный пароль на новый, а потом попытался изменить пароль на старый:



* + 1. Хранить пароли всех пользователей в домене, используя обратимое шифрование

Этот параметр безопасности определяет, используется ли в операционной системе обратимое шифрование для хранения паролей.

* 1. Политика блокировки учетных записей

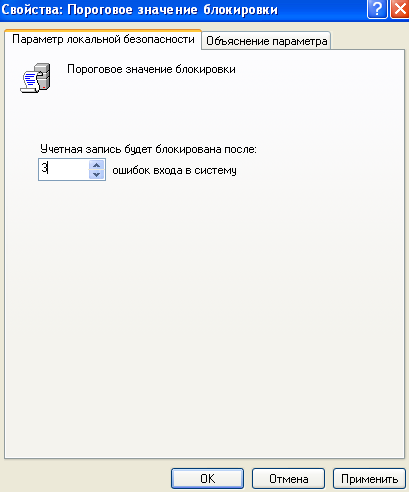
Этот параметр безопасности определяет количество неудачных попыток входа в систему, приводящее к блокировке учетной записи пользователя. Заблокированная учетная запись не может использоваться до тех пор, пока не будет восстановлена администратором, либо пока не истечет период блокировки этой учетной записи.

* + 1. Блокировка учетной записи на …

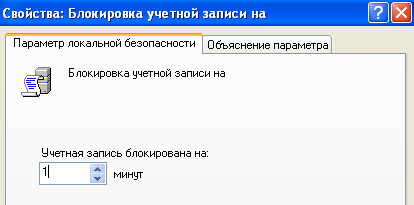
Этот параметр безопасности определяет число минут, в течение которых учетная запись остается заблокированной, прежде чем будет автоматически разблокирована. Этот параметр может принимать значения от 0 до 99 999 минут.

* + 1. **Пороговое значение блокировки**

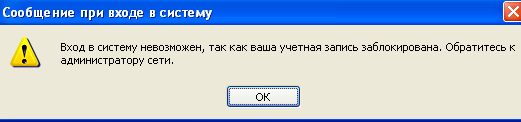
Этот параметр безопасности определяет количество неудачных попыток входа в систему, приводящее к блокировке учетной записи пользователя. Заблокированная учетная запись не может использоваться до тех пор, пока не будет восстановлена администратором, либо пока не истечет период блокировки этой учетной записи.

Поставим блокировку учетной записи, если пароль будет введен неверно 3 раза:

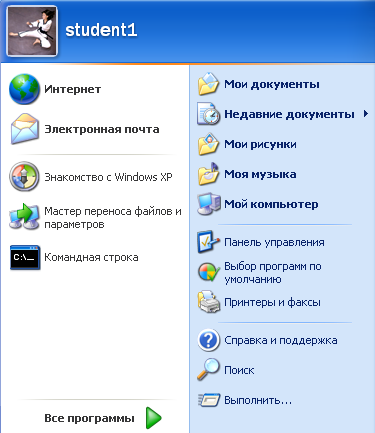
Также блокирование учетной записи на одну минуту:



И попытаемся ввести пароль неверно несколько раз. После неудачных попыток входа в систему появляется следующее сообщение:

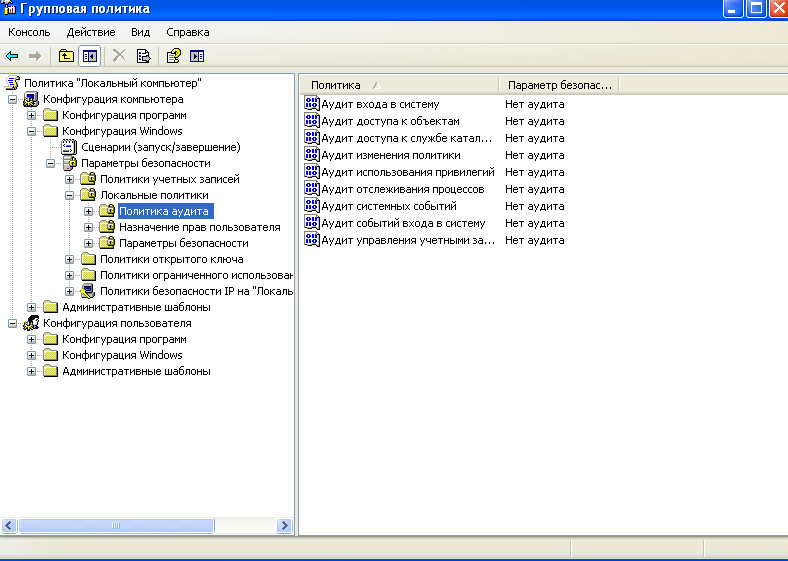


Спустя одну минуту в систему войти удалось:



1. Локальные политики
   1. Политика аудита

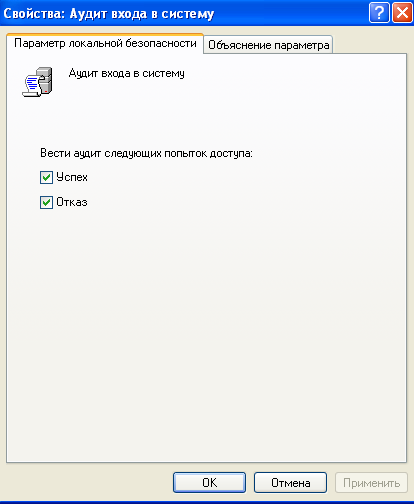
Окно политик аудита:



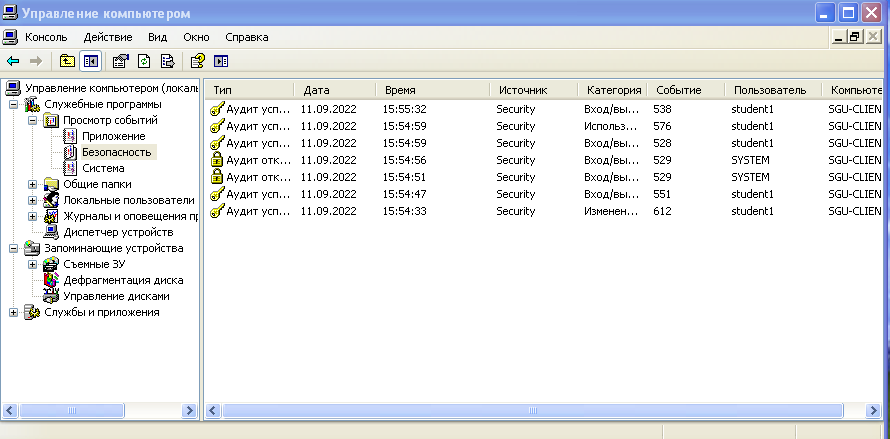
* + 1. **Аудит входа в систему**

Этот параметр безопасности определяет, подлежит ли аудиту каждая попытка пользователя войти в систему с компьютера или выйти из нее.

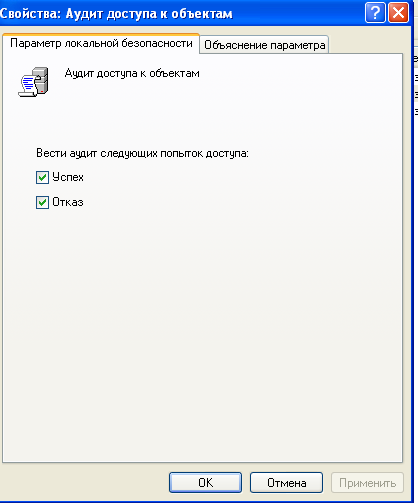
Включим контроль аудита входа в систему:



Просмотрим события политики аудита:



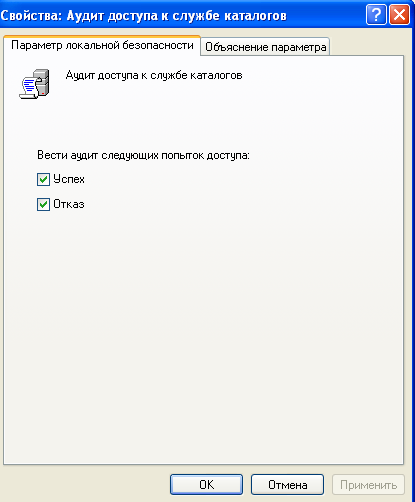
* + 1. **Аудит доступа к объектам**

Этот параметр безопасности определяет, подлежит ли аудиту событие доступа пользователя к объекту - например к файлу, папке, разделу реестра, принтеру и т.п., - для которого задана собственная системная таблица управления доступом (SACL).

Создал текстовый документ и попробовал открыть его со включенной политикой аудита доступа к объектам. Информация отобразилась в просмотре событий:

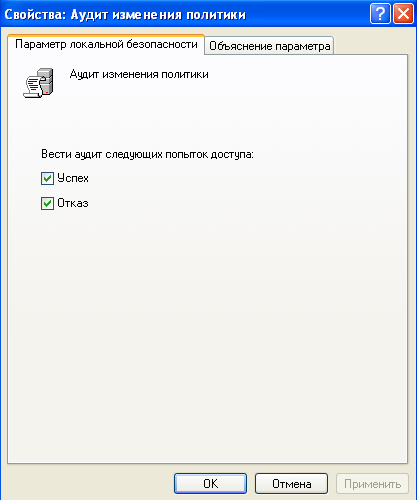


* + 1. Аудит доступа к службе каталогов

Этот параметр безопасности определяет, подлежит ли аудиту событие доступа пользователя к объекту каталога Active Directory, для которого задана собственная системная таблица управления доступом (SACL).

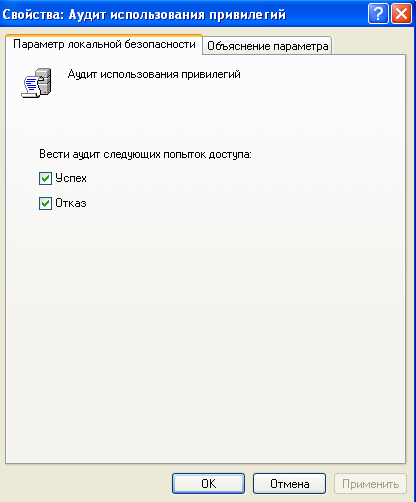
* + 1. **Аудит изменения политики**

Этот параметр безопасности определяет, подлежит ли аудиту каждый факт изменения политик назначения прав пользователей, политик аудита или политик доверительных отношений.



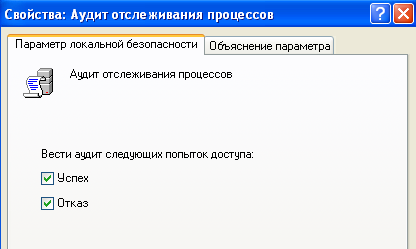
* + 1. Аудит использования привилегий

Этот параметр безопасности определяет, подлежит ли аудиту каждая попытка пользователя воспользоваться предоставленным ему правом.



* + 1. Аудит отслеживания процессов

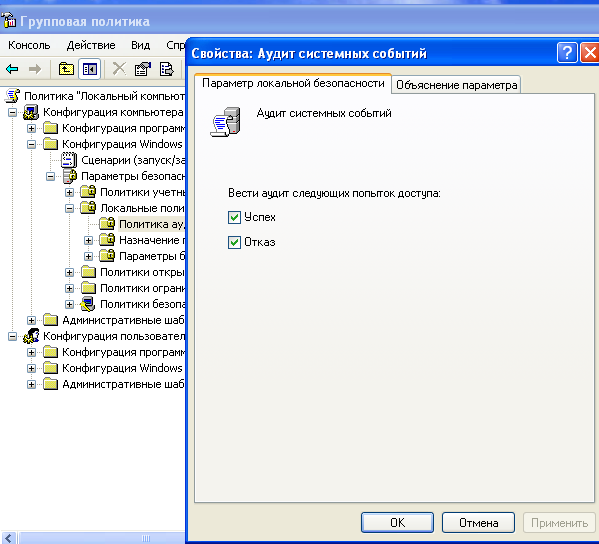
Этот параметр безопасности определяет, подлежат ли аудиту такие события, как активизация программы, завершение процесса, повторение дескрипторов и косвенный доступ к объекту.



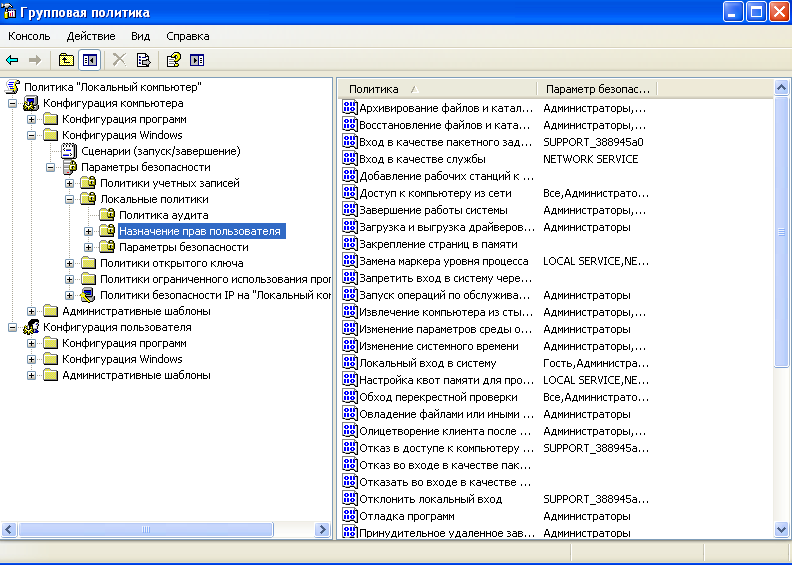
* + 1. **Аудит системных событий**

Этот параметр безопасности определяет, подлежат ли аудиту события перезагрузки или отключения компьютера, а также события, влияющие на системную безопасность или на журнал безопасности.

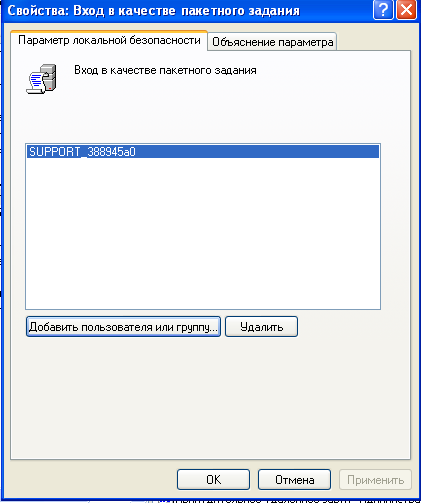
Если этот параметр политики определен, можно задать аудит успехов или отказов либо вообще отключить аудит событий данного типа. Аудит успехов означает создание записи аудита для каждого успешного системного события. Аудит отказов означает создание записи аудита для каждого неудачного завершения системного события.



* 1. Назначение прав пользователя

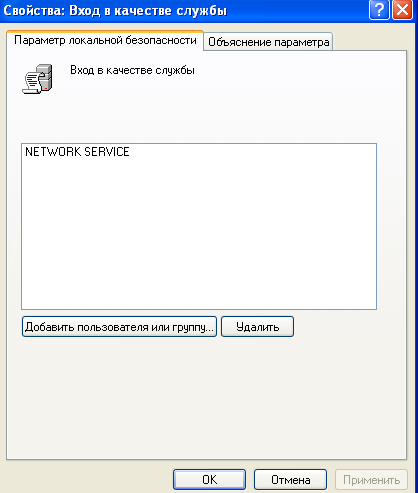


* + 1. Вход в качестве пакетного задания

Эта настройка безопасности позволяет пользователю входить в систему с помощью средства обработки пакетных заданий. Пользователь обеспечивается входом в систему в качестве пакетного пользователя а не интерактивного.

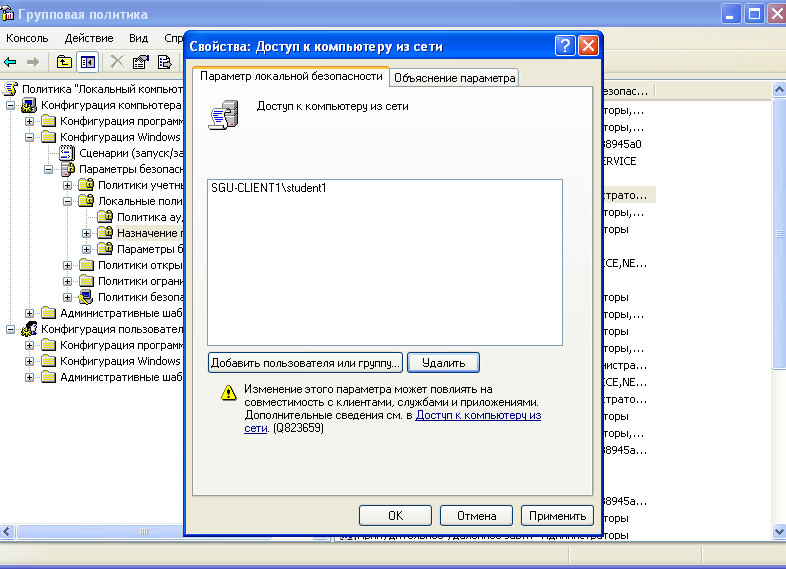
* + 1. Вход в качестве службы

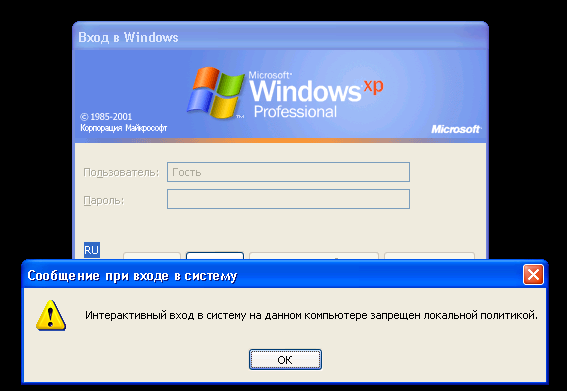
Этот параметр безопасности определяет, какие учетные записи служб могут регистрировать процесс как службу.



* + 1. **Доступ к компьютеру из сети**

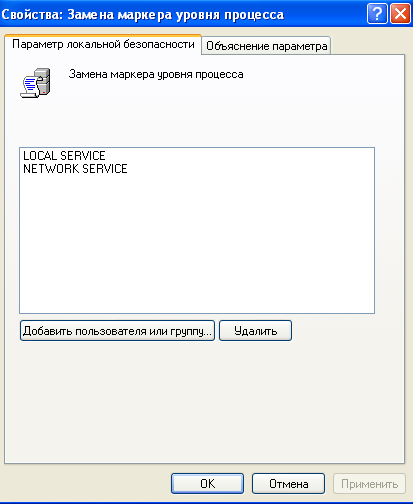
Это право определяет, каким пользователям и группам разрешается подключаться к компьютеру через сеть. Это право не влияет на службы терминалов.

Попробуем подключиться к удаленному рабочему столу с помощью второй машины. В качестве логина пользователя будем использовать неразрешенный. При попытке подключения через пользователя student1, подключиться удается:

****

* + 1. Замена маркера уровня процесса

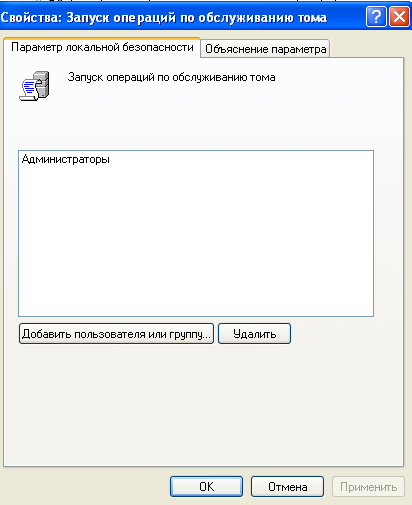
Этот параметр безопасности определяет, какие учетные записи пользователей могут вызывать функцию CreateProcessAsUser() интерфейса API, позволяющую службе запускать другую службу. Примером процесса, использующего это право пользователя, является планировщик заданий.



* + 1. Запуск операций по обслуживанию томов

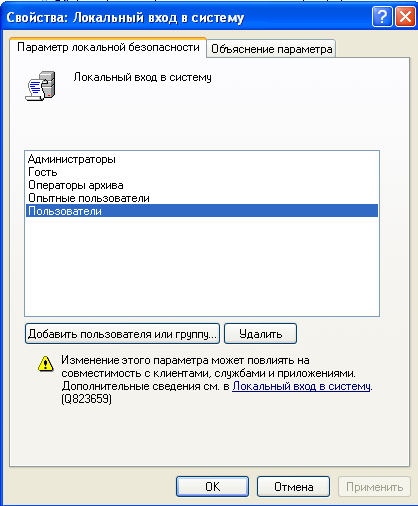
Этот параметр безопасности определяет, какие пользователи и группы могут запускать процедуры обслуживания томов, такие, например, как удаленная дефрагментация.

При текущих настройках, процедуру обслуживания томов может запускать только администратор:



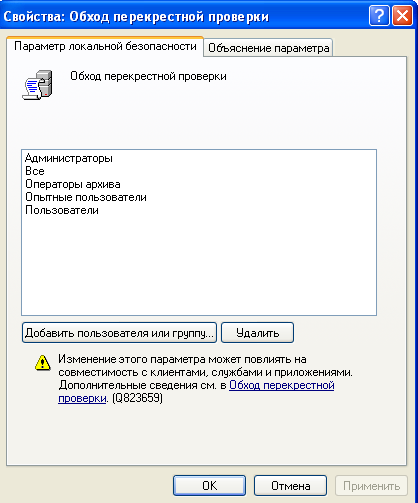
* + 1. Локальный вход в систему

Это право определяет, каким пользователям разрешается интерактивно входить в систему. Данное право необходимо для входа пользователя в систему после одновременного нажатия клавиш CTRL+ALT+DEL на клавиатуре компьютера.



* + 1. Обход перекрестной проверки

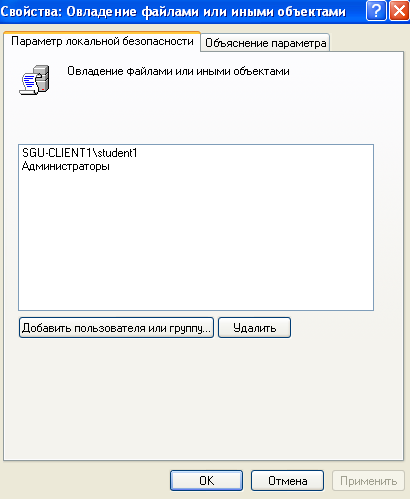
Это право пользователя определяет, какие пользователи могут перемещаться по деревьям каталогов независимо от того, имеются ли у них разрешения на доступ к соответствующему каталогу. Эта привилегия не позволяет пользователю выводить список содержимого каталога, а только перемещаться по его структуре.



* + 1. **Овладение файлами и иными объектами**

Этот параметр безопасности определяет, какие пользователи могут стать владельцами любого объекта системы, контролируемого средствами безопасности, в том числе объектов Active Directory, файлов и папок, принтеров, разделов реестра, процессов и потоков.

Назначим контроль за действиями пользователю student1:



* + 1. Принудительное удаленное завершение

Этот параметр безопасности определяет, каким пользователям разрешено завершать работу компьютера с удаленного узла сети. Неправильное использование этого права может привести к атаке на службу.

* + 1. Создание маркерного объекта

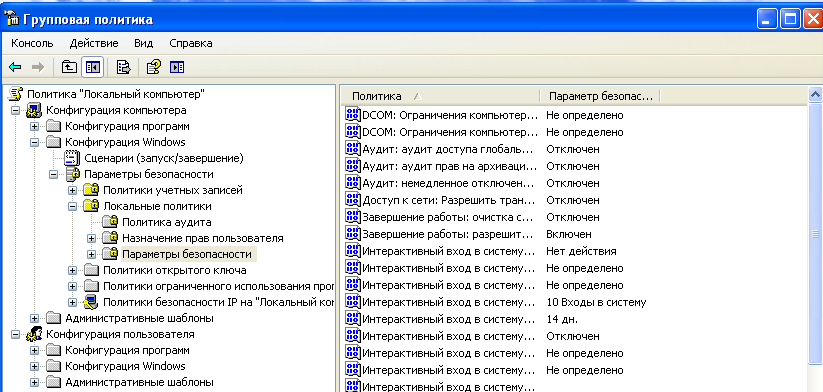
Этот параметр безопасности определяет, какие учетные записи могут использоваться процессами для создания маркера, позволяющего получать доступ к любым локальным ресурсам, если маркер доступа создается с помощью встроенного интерфейса API.

* + 1. Управление аудитом и журналом безопасности

Этот параметр безопасности определяет, кто из пользователей может указывать параметры аудита доступа к объектам для отдельных ресурсов, таких как файлы, объекты Active Directory и разделы реестра.

* 1. Параметры безопасности

Окно параметров безопасности:



* + 1. **Завершение работы: очистка страничного файла виртуальной памяти**

Этот параметр безопасности определяет, следует ли очищать файл подкачки виртуальной памяти при завершении работы системы.

* + 1. Интерактивный вход в систему: требовать смарт-карту

Этот параметр безопасности требует использования смарт-карты для входа пользователя на компьютер. Если параметр включен, то вход в систему будет происходить только с использованием смарт-карты. Если выключен, пользователи смогут войти на компьютер с использованием любого метода.

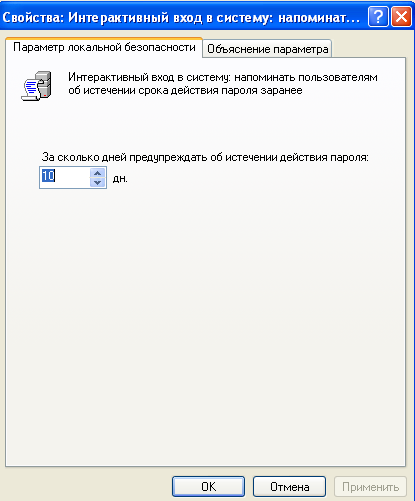
* + 1. Интерактивный вход в систему: количество предыдущих подключений к КЭШу

Сведения о предыдущих входах пользователей в систему кэшируются локально, чтобы обеспечить последующий вход в систему в случае отсутствия доступа к контроллеру домена.

* + 1. **Интерактивный вход в систему: напоминать пользователям об истечении срока действия пароля заранее**

Определяет, за сколько дней до истечения срока действия пароля следует предупреждать об этом пользователей. Если пользователя заблаговременно предупредить, он успеет подготовить новый достаточно надежный пароль. По умолчанию 14 дней.

Поставим напоминание за 10 дней до окончания срока действия:



Затем вышел из системы и зашел обратно под той же учетной записью, но, к сожалению, никакого сообщения об истечении срока действия пароля не получил. В ранее установленной политике максимального срока действия пароля также попытался задать 1 день и попробовал зайти заново в систему, но политика также не работала.

* + 1. Клиент сети Microsoft: использовать цифровую подпись

Этот параметр безопасности определяет, является ли обязательным использование подписи пакетов для SMB-компоненты клиента.

Протокол SMB обеспечивает основу для используемого в сетевых продуктах корпорации Майкрософт совместного доступа к файлам и печати, а также для многих других сетевых операций, таких как удаленное администрирование в Windows. Чтобы предотвратить атаки злоумышленников, искажающие SMB-пакеты при передаче, протокол SMB поддерживает использование цифровой подписи для SMB-пакетов. Этот параметр политики определяет, должны ли проводиться переговоры относительно использования подписи для SMB-пакетов перед выдачей разрешения на дальнейшую связь с SMB-сервером.

Если этот параметр включен, клиент сети Microsoft не установит связь с сервером сети Microsoft при его отказе от использования подписи SMB-пакетов. Если этот параметр отключен, использование подписи SMB-пакетов согласовывается между клиентом и сервером.

* + 1. Консоль восстановления: разрешить копирование дискет и доступ ко всем дискам и папкам

При включении данного параметра становится доступной команда консоли восстановления SET, которая позволяет настраивать следующие переменные среды консоли восстановления:

AllowWildCards: "Включен"ие поддержки подстановочных знаков для некоторых команд (таких как DEL).

AllowAllPaths: разрешение доступа ко всем файлам и папкам на данном компьютере.

AllowRemovableMedia: разрешение копирования файлов на съемные носители, такие как дискета.

NoCopyPrompt: отмена запроса подтверждения при записи поверх существующего файла.

* + 1. Сервер сети Microsoft: отключить клиентов по истечении разрешенных часов входа

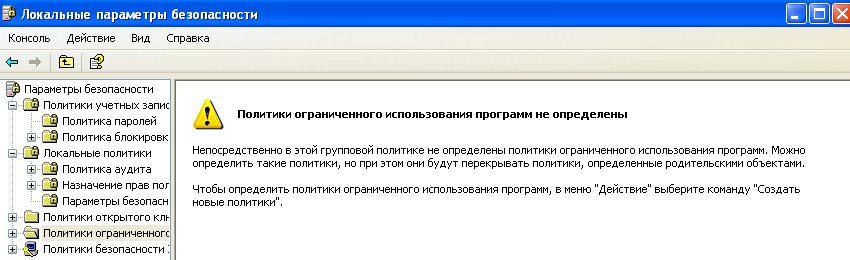
Этот параметр безопасности определяет, требуется ли отсоединять пользователей, подключенных к локальному компьютеру по истечении разрешенного времени входа. Этот параметр затрагивает компонент блоков сообщений сервера (SMB).

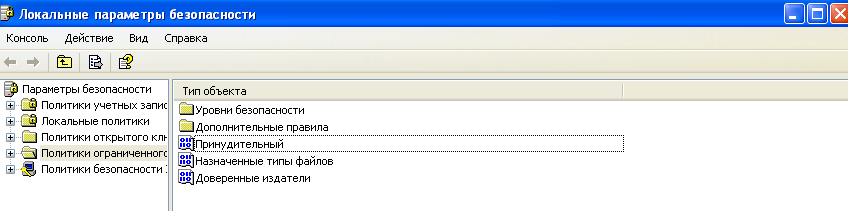
Если этот параметр включен, клиентские сеансы связи со SMB-службой принудительно прерываются по истечении времени входа.

Если этот параметр отключен, установленный сеанс связи разрешено поддерживать после истечения времени входа клиента.

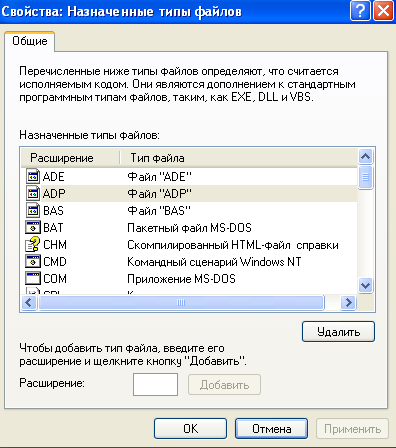
1. Политики ограниченного использования программ (создать политику и изучить все ее параметры)

Создадим политику:

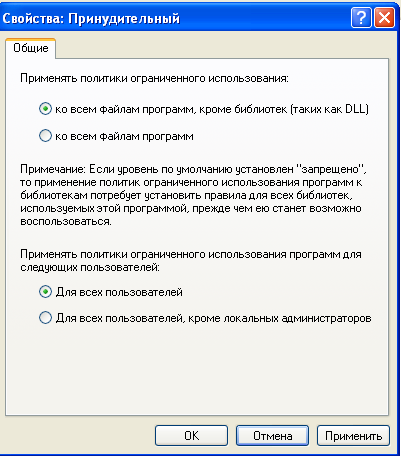
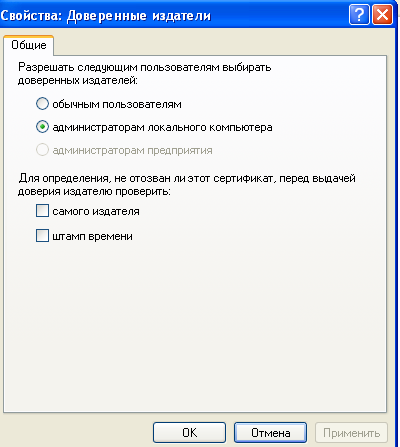




Назначенные типы файлов для политики:



Только администратор может принимать решения о доверии издателю исполняемого файла:



Проверить фактическую работу политик (отмечено **жирным**) устанавливая их по очереди и выполняя контролируемые ими действия. Законспектируйте результаты вашей работы по каждой политике. При необходимости устанавливайте и меняйте субъектов (пользователей), системное время, подключайте другую виртуальную машину в сеть и т.д.