

## Настройка учётных записей для мониторинга в защищенной сети МИАЦ

БУЗ ВО «МИАЦ»

Центр Обработки Данных

Брянцев Егор Валериевич

В целях облегчения мониторинга объектов защищенной сети было решено опробовать давно витавшую в воздухе идею и использовать встроенные средства VipNet для удаленного просмотра компьютеров в защищенной сети. Дело в том, что в VipNet Coordinator изначально встроена возможность прямого доступа к компьютерам защищенной сети через протокол RDP. Если объяснять максимально просто – можно подключиться к другому компьютеру в защищенной сети всего за несколько щелчков мышью... если эта возможность на этом компьютере включена, разумеется. Поэтому сейчас стоит задача собрать учетные данные компьютеров защищенной сети, дабы в будущем при возникновении каких-то проблем, например, при выгрузке дампов МИС, не нужно было бы долго выпрашивать параметры подключения и ждать, пока будет включен, например, Teamviewer... достаточно было бы просто подключиться к компьютеру через координатор и определить, в чем причина проблем...

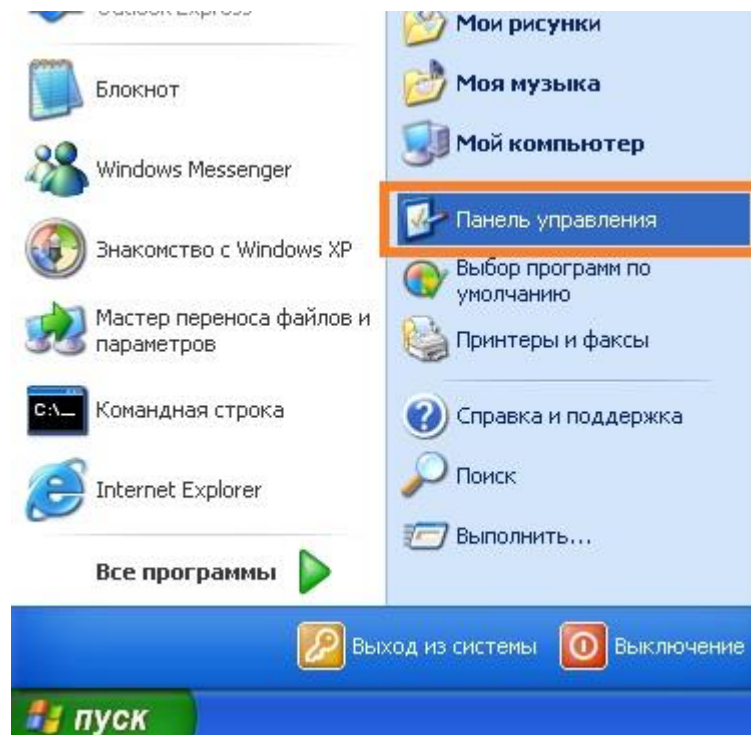
Сразу оговорю следующее. Это **исключительно добровольное дело**, никто никого не заставляет выдавать все логины-пароли от ваших сетей по первому запросу... Просто это поможет в случае возникновения неожиданных проблем... не всегда возможно быстро определить причины по телефону, а тут будет способ оперативно подключиться и посмотреть настройки, например...

Итак, если вы решите предоставить доступ на компьютеры в защищенной сети, тогда от вас потребуется просто создать новые учетные записи на компьютерах с координатором и МИС, а потом добавить их в список учетных записей, которые могут подключаться к этим компьютерам удаленно и передать в МИАЦ логин и пароль этих учетных записей...

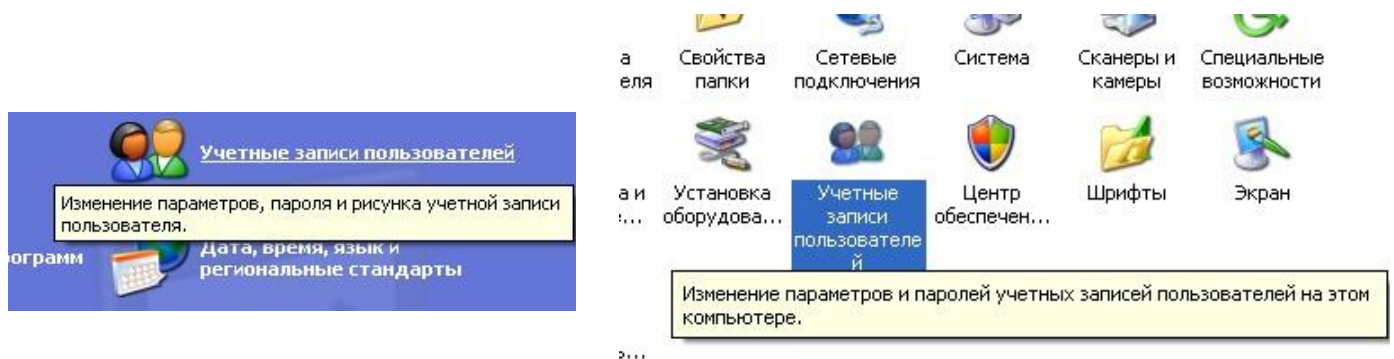
Для людей, в принципе не понимающих, о чём идёт речь, рассмотрю процесс максимально подробно, в примерах и картинках, на примере Windows XP и Windows 7...

# Windows XP

Создадим нового пользователя. Для этого откроем **Панель управления**:

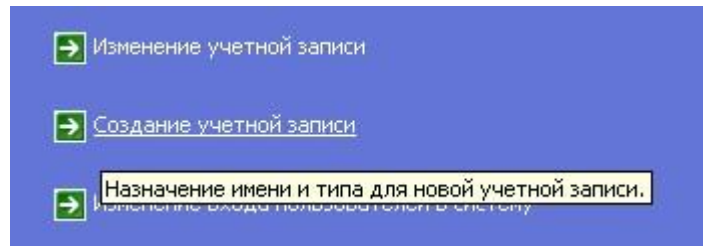


Там находим **Учетные записи пользователей**:



*Может выглядеть по-разному ...*

Теперь выберем **Создание учетной записи**:



Зададим имя. Имя может быть любым, я в качестве примера задал имя **zabbix**:

Введите имя для новой учетной записи:

Это имя отображается в окне приветствия и в меню "Пуск".

Укажем тип учетной записи. Можете выбрать админскую или пользовательскую... особо без разницы:

☒ Администратор компьютера    ☐ Ограниченная запись

---

С учетной записью администратора вы можете:

- Создавать, изменять и удалять учетные записи
- Вносить изменения, затрагивающие других пользователей
- Устанавливать программы и получать доступ к любым файлам

---

< Назад    **Создать учетную запись**    Отмена

Нажимаем **Создать учетную запись** и возвращаемся к экрану настройки учетных записей. Там выбираем созданную учетную запись:



Жмём **Создание пароля**:

## Что вы хотите изменить в своей учетной записи?

→ Изменение имени

→ **Создание пароля**

→ Изменение изображения

→ Изменение типа учетной записи

→ Использовать паспорт .NET



**zabbix**

Администратор компьютера

Задаем любой подходящий пароль, вводим его дважды, как показано на рисунке, и жмем **Создать пароль**:

### Создание пароля для вашей учетной записи

Введите новый пароль:  
.....

Введите пароль для подтверждения:  
.....

Если пароль содержит заглавные буквы, нужно вводить пароль точно таким же образом, как при задании пароля.

Введите слово или фразу, служащую подсказкой о пароле:

Подсказка о пароле будет видна всем пользователям этого компьютера.

**Создать пароль**

Отмена

Применение нового пароля для вашей учетной записи.

Если увидите следующее окно, то в нем можно выбрать **Да...** или **Нет...** тут уж сами решайте ☺

## Хотите сделать свои файлы и папки личными?

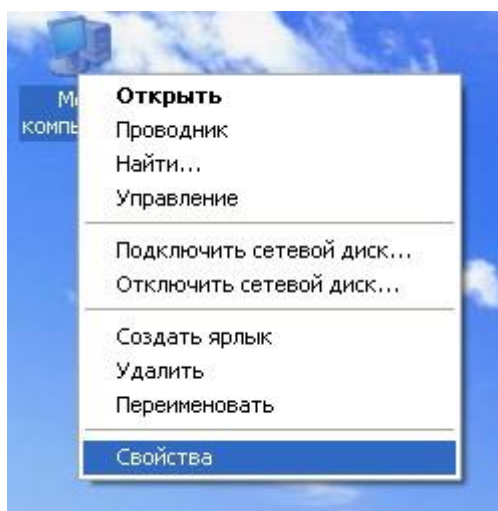
Даже при использовании пароля для вашей учетной записи другие пользователи на этом компьютере могут увидеть ваши документы. Чтобы предотвратить это, Windows может сделать ваши файлы и папки личными. Это не позволит другим пользователям с ограниченными правами получить доступ к вашим файлам и папкам.

Да, сделать их личными

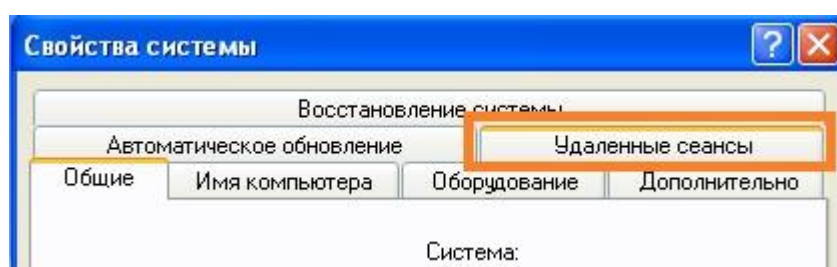
Нет

Сделать ваши файлы и папки личными (недоступными другим пользователям).

С настройкой учетной записи всё... Теперь добавим нового пользователя в список тех, кто может подключаться к компьютеру удаленно. Для этого щелкаем правой кнопкой мыши по **Мой компьютер** и выбираем **Свойства**:



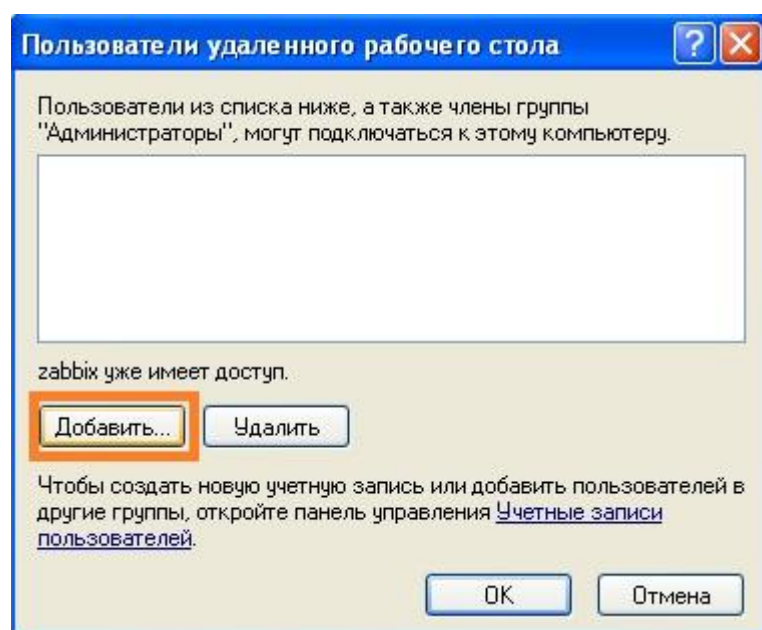
В открывшемся окне переходим на вкладку **Удаленные сеансы**:



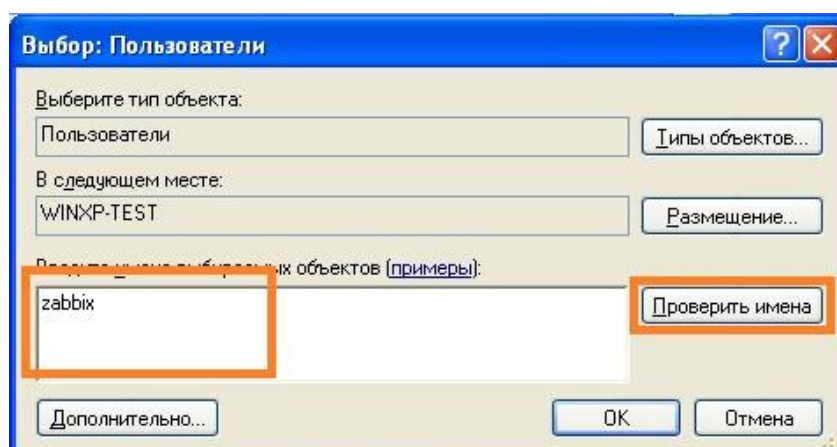
Включаем **Разрешить удаленный доступ к этому компьютеру** и жмем кнопку **Выбрать удаленных пользователей...**



В открывшемся окне жмем кнопку **Добавить:**

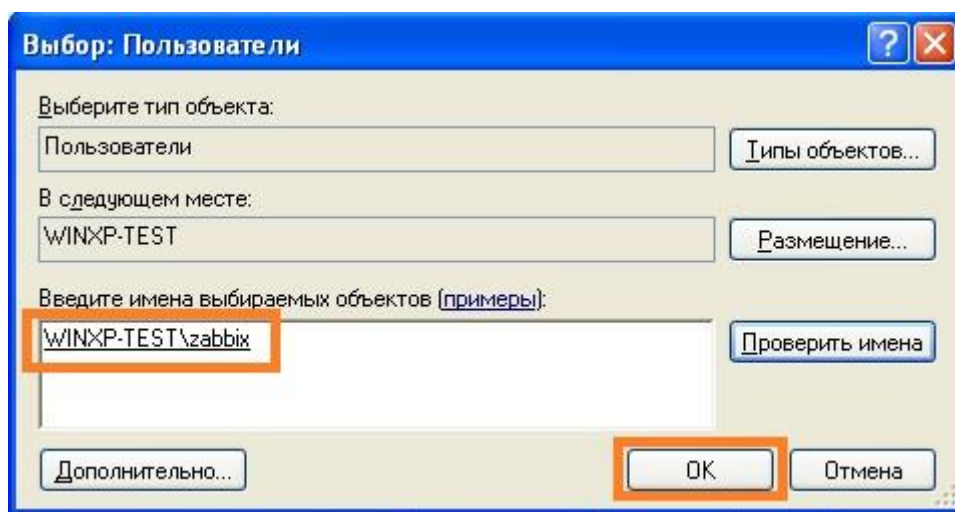


Пишем имя пользователя, которого создали и нажимаем кнопку **Проверить имена:**

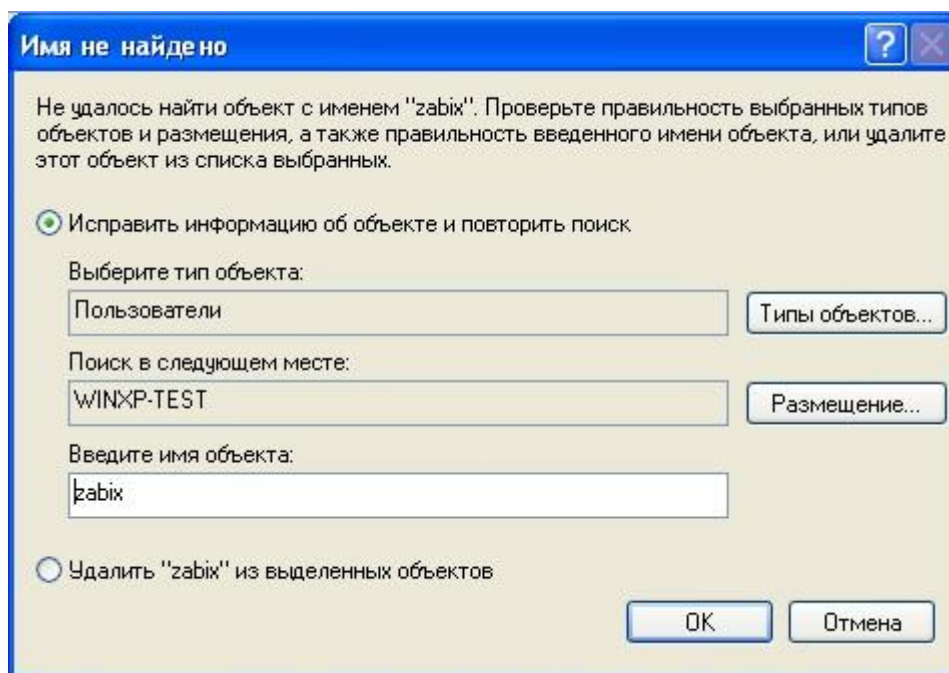




Если имя написано правильно, то никаких сообщений об ошибках выдано не будет и можно жать **ОК**:

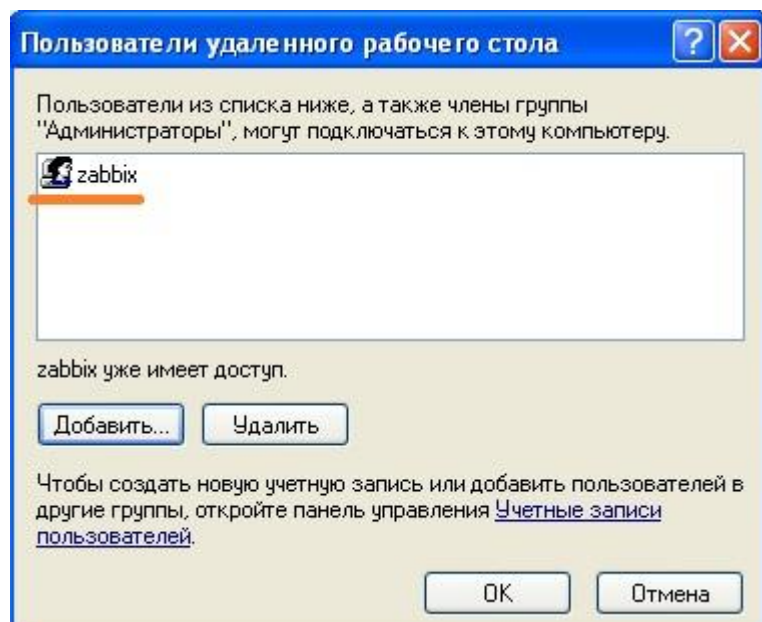


Если же вы видите следующее:



Значит, ошибка в написании имени... жмём **Отмена** и вводим имя учетной записи еще раз...

Если все сделано верно, то в списке пользователей появится тот, которого вы только что создали...



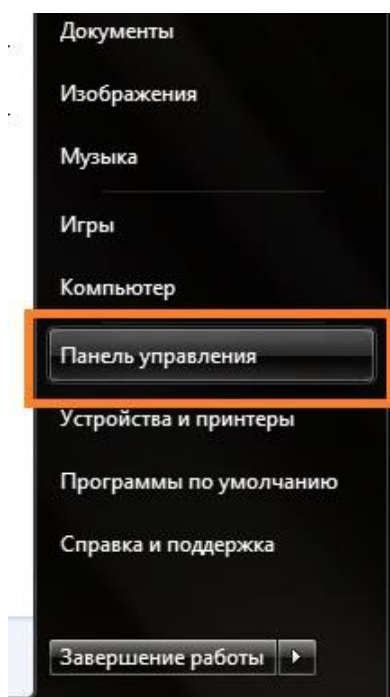
Просто жмем **ОК** и еще раз **ОК**, чтобы закрыть окно свойств системы...

Теперь можно отправить логин и пароль созданной учетной записи в МИАЦ...

## Windows 7

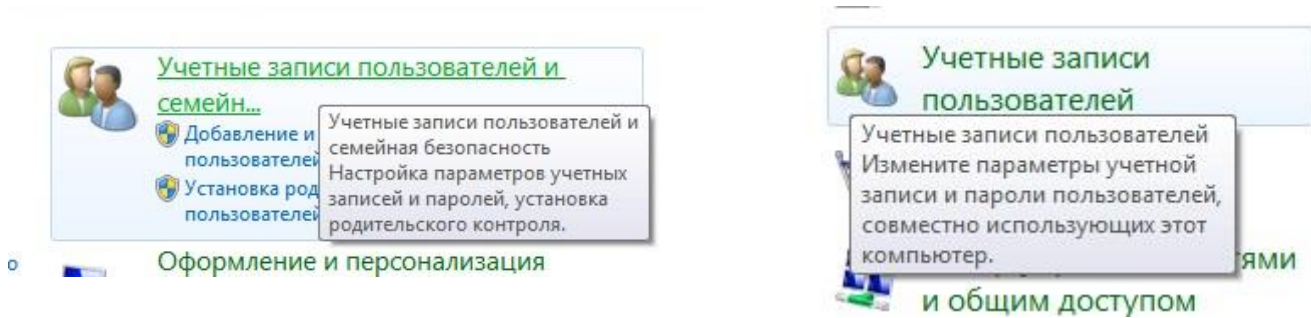
В принципе, создание новой учетной записи идентично таковому в WinXP...

Вначале **Панель управления**:





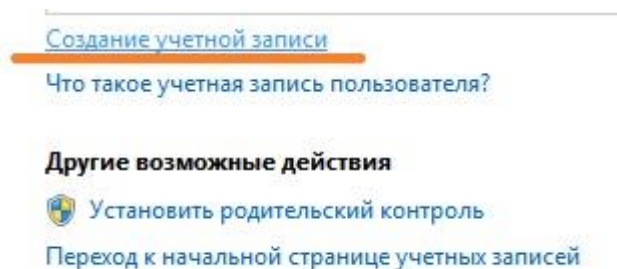
Теперь **Учетные записи пользователей:**



Теперь **Управление другой учетной записью:**



Выбираем **Создание учетной записи:**



Вводим имя учетной записи (я по-прежнему использую zabbix), указываем тип (обычная или администратор; тут уж сами решайте) и жмём **Создание учетной записи:**

### Укажите имя учетной записи и ее тип

Это имя будет отображаться на экране приветствия и в меню "Пуск".

☒ Обычный доступ

Стандартные учетные записи пользователей позволяют использовать большинство программ и изменять параметры системы, которые не влияют на настройки других пользователей и безопасность компьютера.

☐ Администратор

Администраторы имеют полный доступ к компьютеру и могут выполнять любые изменения. В зависимости от параметров уведомлений администраторы могут получать запрос на ввод пароля для применения изменений, влияющих на настройки других пользователей.

Рекомендуется защищать все учетные записи надежными паролями.

[Почему рекомендуется использовать обычную учетную запись?](#)

Создание учетной записи

Отмена

Вернувшись к списку учетных записей, выбираем только что созданную:



zabbix  
Обычный доступ

Здесь выбираем **Создание пароля**:

### Внесение изменений в учетную запись zabbix

[Изменение имени учетной записи](#)

[Создание пароля](#)

[Изменение рисунка](#)

[Установить родительский контроль](#)

[Изменение типа учетной записи](#)

[Удаление учетной записи](#)

[Управление другой учетной записью](#)



zabbix  
Обычный доступ

Вводим пароль дважды, как показано на рисунке, потом жмём кнопку **Создать пароль**:

## Создайте пароль учетной записи zabbix



zabbix  
Обычный доступ

Вы создаете пароль zabbix.

**В этом случае zabbix потеряет все EFS-шифрованные файлы, личные сертификаты и сохраненные пароли для веб-сайтов и сетевых ресурсов.**

Чтобы избежать потерь данных в будущем, попросите zabbix сделать дискету сброса пароля.



При вводе пароля учитываются различия между строчными и заглавными буквами.

[Как создать надежный пароль](#)

Введите подсказку для пароля

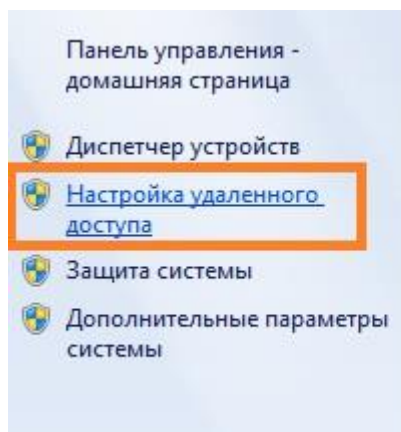
Подсказка для пароля будет видна всем, кто использует этот компьютер.

[Что такое подсказка для паролей?](#)

Создать пароль

Отмена

Теперь закрываем Панель управления и заходим в свойства системы (щелчок правой кнопкой мыши на значке **Компьютер - Свойства**), там выбираем **Настройка удаленного доступа**:



### Просмотр основ

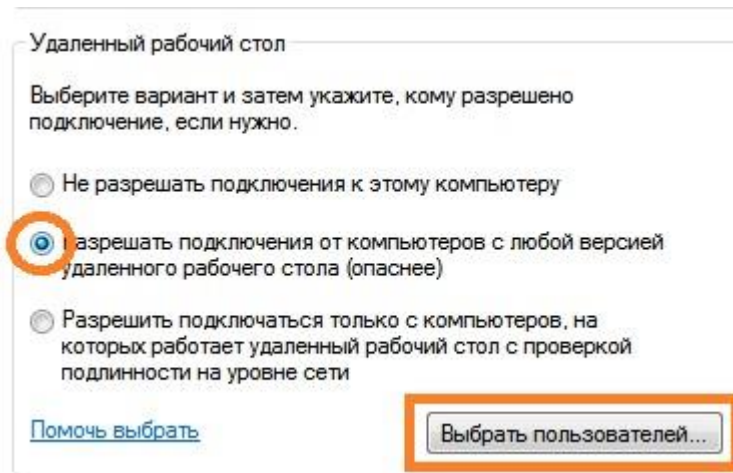
Издание Windows —

Windows 7 Макси

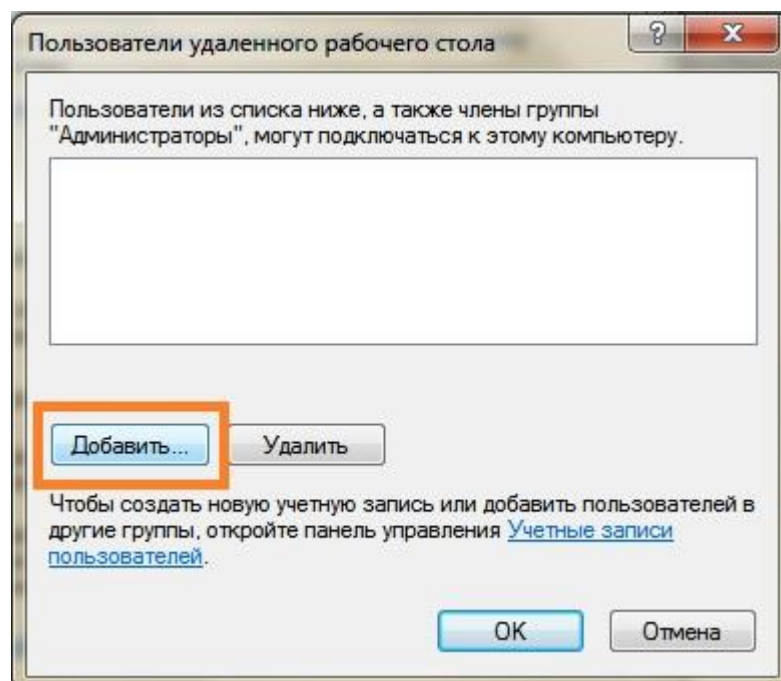
© Корпорация Ма

Service Pack 1

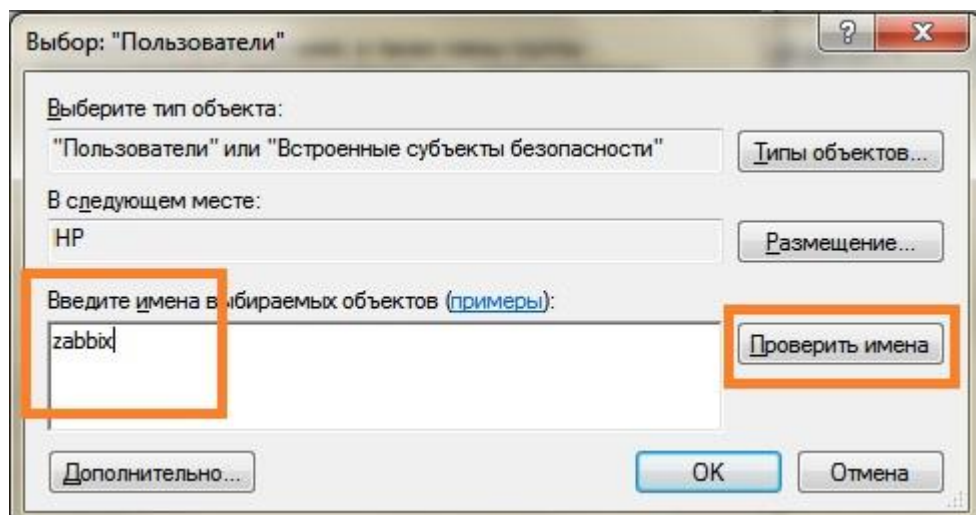
В открывшемся окне выбираем пункт **Разрешать подключения от компьютеров с любой версией удаленного рабочего стола**, потом жмём кнопку **Выбрать пользователей**:



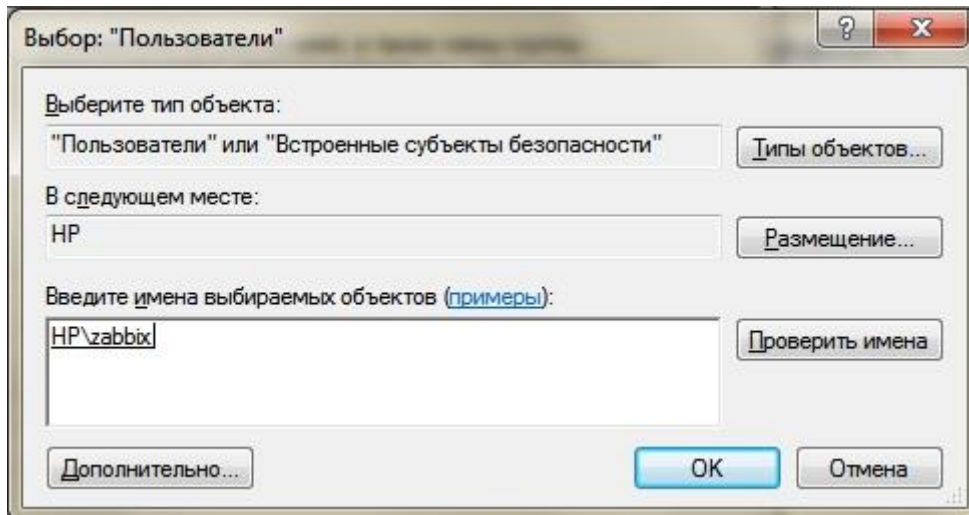
Жмём кнопку **Добавить**:



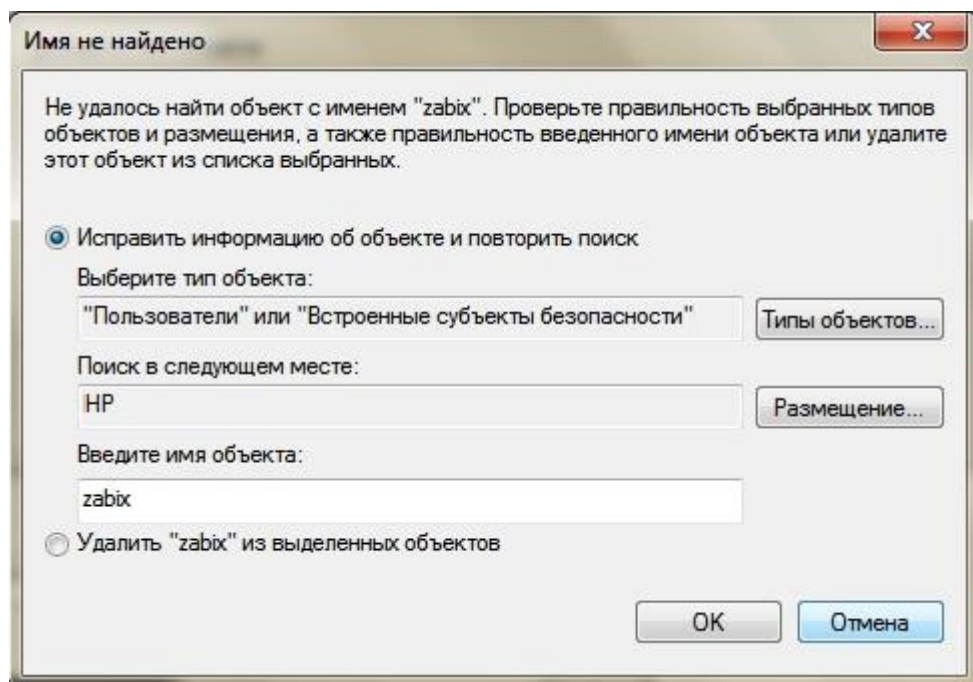
Вводим имя созданной учётной записи и жмем кнопку **Проверить имена**:



Если всё в порядке, и имя введено верно, то можно нажать кнопку **ОК**:

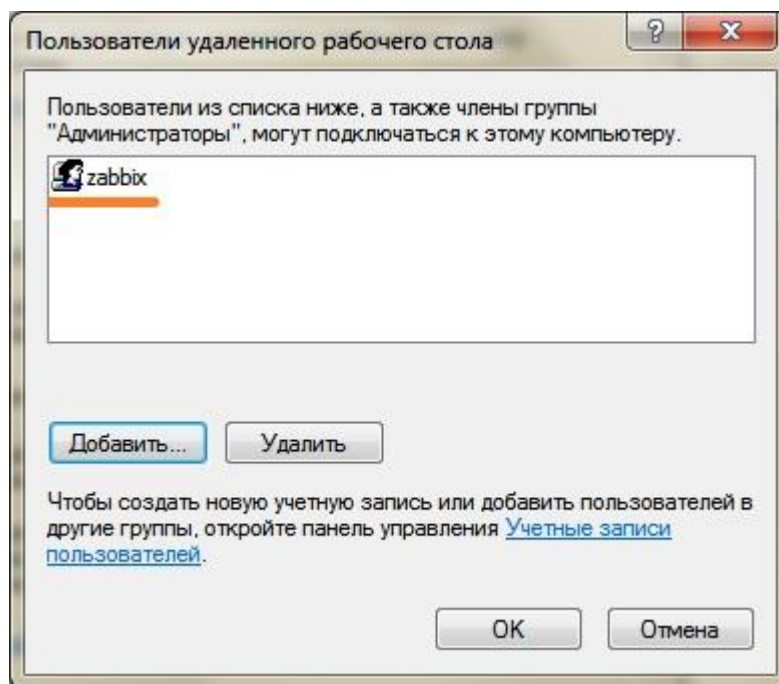


Иначе, если имя введено неверно, выдается сообщение об ошибке, и надо нажать **Отмена** и ввести имя еще раз...



В итоге, попадаем назад в окно выбора пользователей. Теперь там появился недавно созданный и добавленный пользователь...





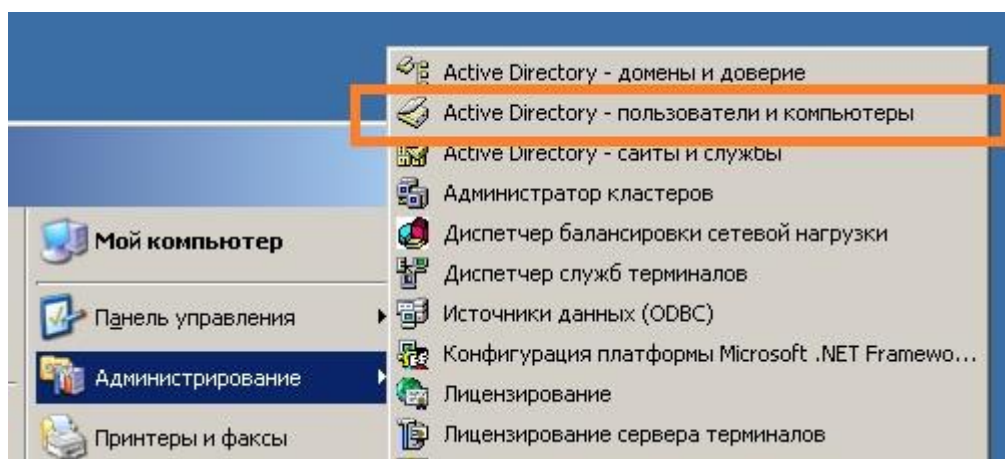
Жмём **ОК** и отправляем логин и пароль нового пользователя в МИАЦ...

Отмечу, что если у вас координатор и сервер МИС находятся на двух разных машинах, то вышеописанные операции нужно провести на них обеих...

### Домен (Windows 2003\2008)

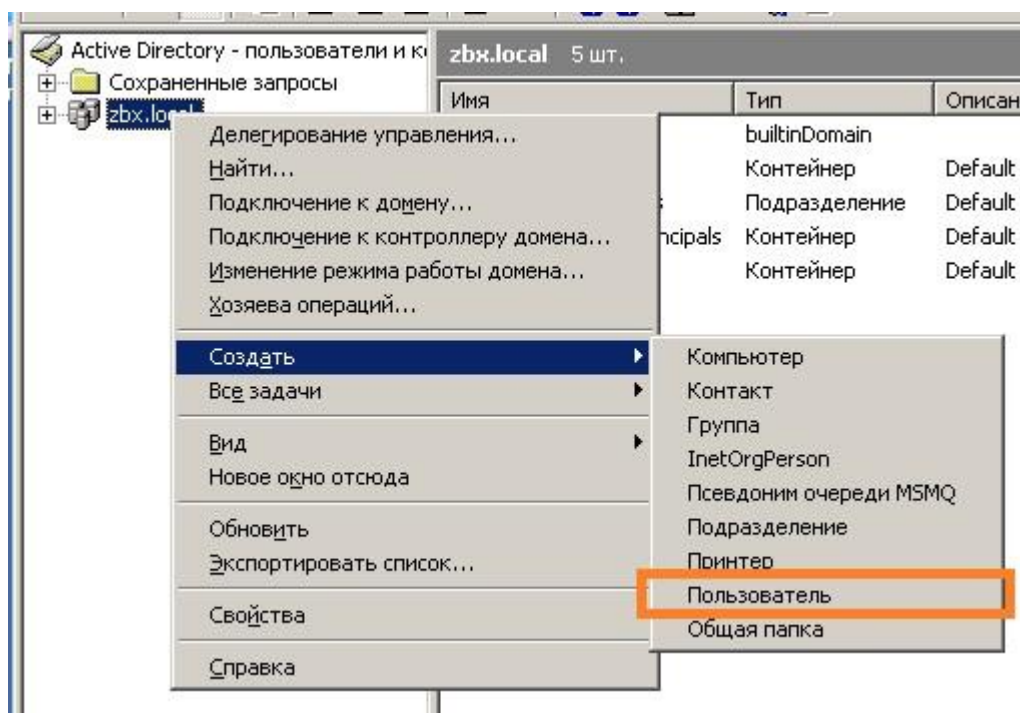
Если в ЛПУ внедрена доменная сеть (и компьютеры, для которых нужно открыть доступ, введены в домен), то для создания нового пользователя нужно воспользоваться оснасткой **Пользователи и компьютеры**. Покажу на примере Windows Server 2003. Все нижеперечисленное выполняется на контроллере домена.

Итак, в главном меню выбираем **Администрирование – Пользователи и компьютеры**:





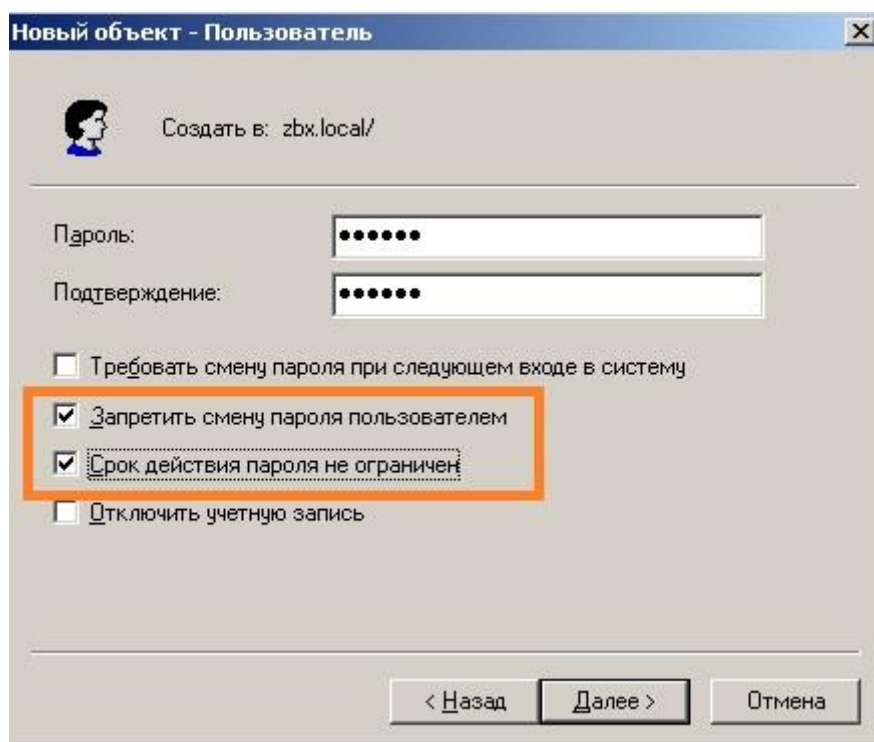
Щелкаем правой кнопкой мыши по названию своего домена и выбираем в меню **Создать – Пользователь**:



Заполняем все поля в появившемся окне... можно указать любые учетные данные, тут важно только **Имя входа пользователя**, это имя учетной записи, которое понадобится для удаленного подключения...

The image shows a screenshot of the 'Новый объект - Пользователь' (New Object - User) dialog box. The 'Создать в:' (Create in:) field is set to 'zbx.local/'. The 'Имя:' (Name) field is filled with 'z', and the 'Инициалы:' (Initials) field is filled with 'zbx'. The 'Фамилия:' (Surname) field is filled with 'bx'. The 'Полное имя:' (Full name) field is filled with 'z zbx. bx'. The 'Имя входа пользователя:' (User logon name) field is filled with 'zabbix' and '@zbx.local'. The 'Имя входа пользователя (пред-Windows 2000):' (User logon name (pre-Windows 2000)) field is filled with 'ZBX\'. The 'zabbix' field is also filled. The 'Назад' (Back) button is disabled, and the 'Далее' (Next) button is enabled. The 'Отмена' (Cancel) button is also present.

Нажимаем кнопку **Далее**, указываем пароль для учетной записи, включаем **Запретить смену пароля пользователем** и **Срок действия пароля не ограничен**:



Новый объект - Пользователь

Создать в: zbx.local/

Пароль: [password field]

Подтверждение: [password field]

☐ Требовать смену пароля при следующем входе в систему

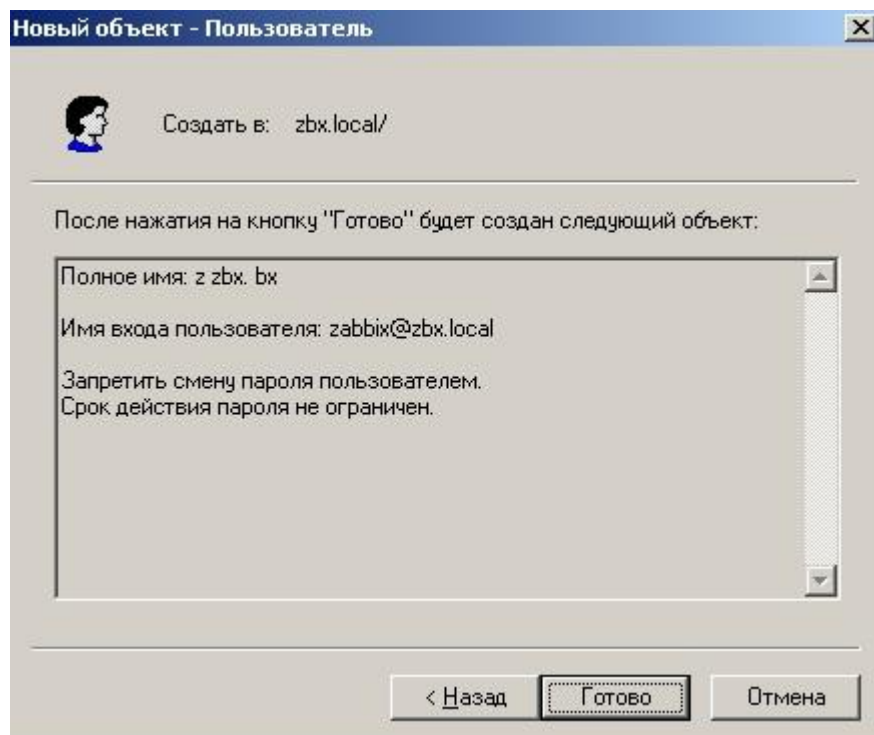
☒ **Запретить смену пароля пользователем**

☒ **Срок действия пароля не ограничен**

☐ Отключить учетную запись

< Назад    Далее >    Отмена

Жмем **Готово**:



Новый объект - Пользователь

Создать в: zbx.local/

После нажатия на кнопку "Готово" будет создан следующий объект:

Полное имя: z zbx. bх

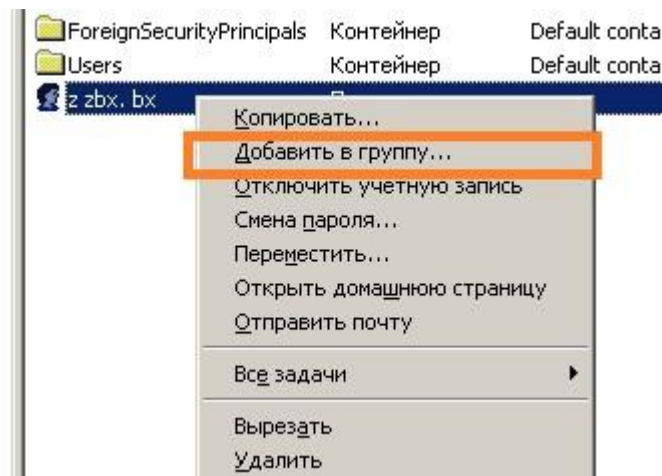
Имя входа пользователя: zabbix@zbx.local

Запретить смену пароля пользователем.

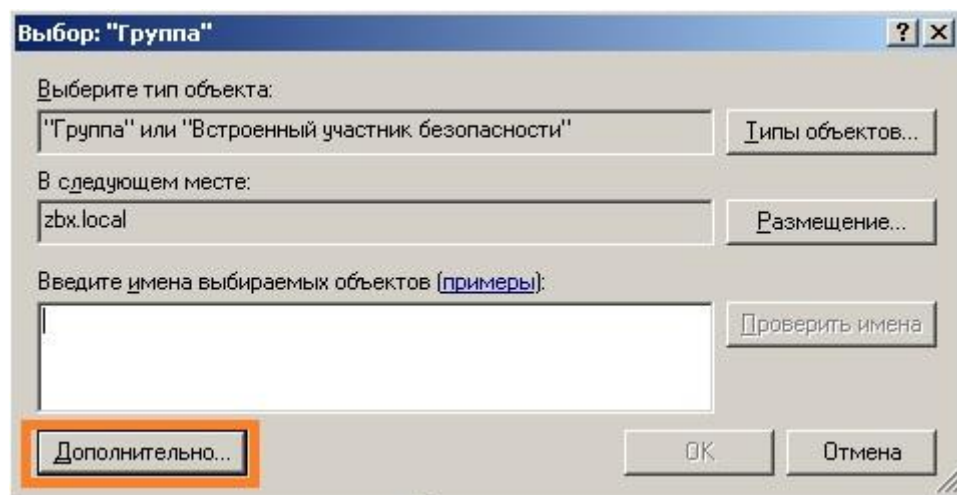
Срок действия пароля не ограничен.

< Назад    **Готово**    Отмена

Теперь добавим нового пользователя в группу пользователей удаленного рабочего стола. Для этого выбираем созданного пользователя все в той же оснастке **Пользователи и компьютеры**, щелкаем правой кнопкой мыши и выбираем пункт **Добавить в группу...**



Здесь проще всего нажать кнопку **Дополнительно**, потом **Поиск** и в появившемся списке найти **Пользователи удалённого рабочего стола**:



**Выбор: "Группа"**

Выберите тип объекта:

В следующем месте:

Общие запросы

Имя:

Описание:

☐ Отключенные учетные записи

☐ Пароли с неограниченным сроком действия

Число дней со времени последнего входа в систему:

Результаты поиска:

| Имя (RDN) | Описание | В папке |
|-----------|----------|---------|
|-----------|----------|---------|

**Выбор: "Группа"**

Выберите тип объекта:

В следующем месте:

Общие запросы

Имя:

Описание:

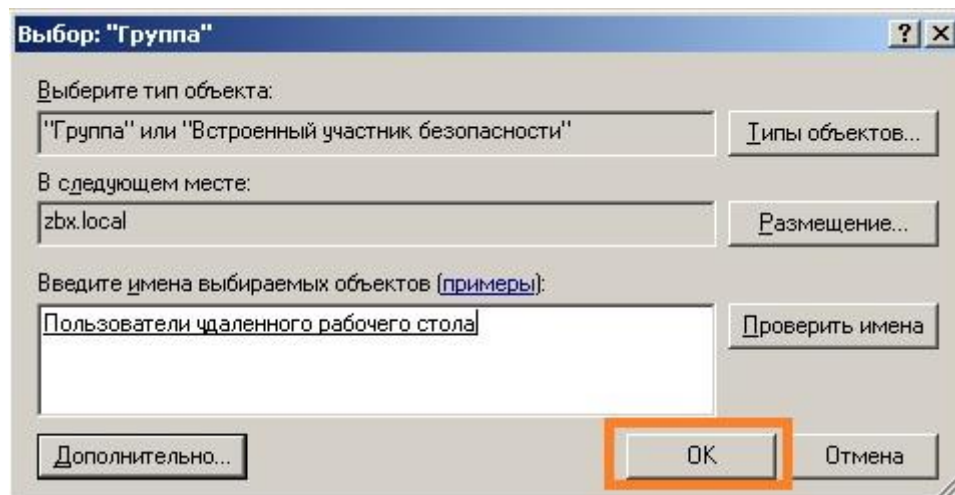
☐ Отключенные учетные записи

☐ Пароли с неограниченным сроком действия

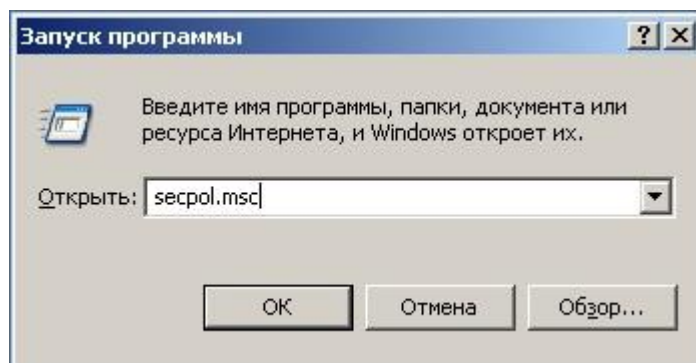
Число дней со времени последнего входа в систему:

Результаты поиска:

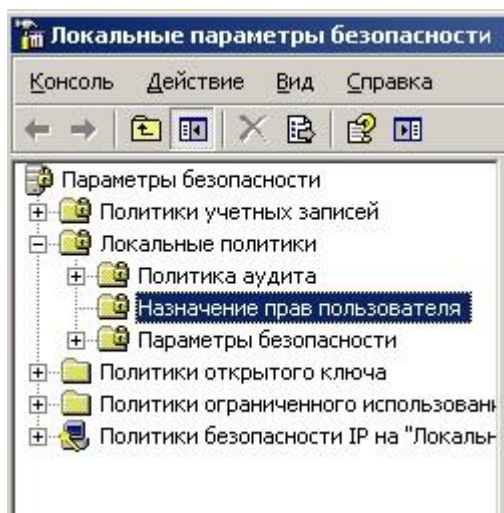
| Имя (RDN)                                | Описание         | В папке           |
|--|------------------|-------------------|
| Пользователи                             |                  | zbx.local/Builtin |
| Пользователи DCOM                        |                  | zbx.local/Builtin |
| Пользователи домена                      | Все пользоват... | zbx.local/Users   |
| Пользователи журналов производительности |                  | zbx.local/Builtin |
| Пользователи системного монитора         |                  | zbx.local/Builtin |
| Пользователи удаленного рабочего стола   |                  | zbx.local/Builtin |
| Пред-windows 2000 доступ                 |                  | zbx.local/Builtin |
| Репликатор                               |                  | zbx.local/Builtin |
| Серверы RAS и IAS                        | Серверы в это... | zbx.local/Users   |
| Серверы лицензий сервера терминалов      |                  | zbx.local/Builtin |

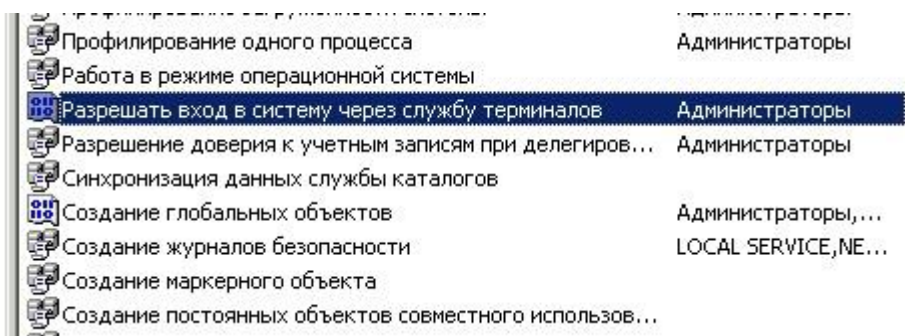


Теперь включим возможность подключаться к компьютерам удаленно. Для этого изменим локальные параметры безопасности. Откроем **Выполнить...** в главном меню, впишем туда **secpol.msc** и жмем OK:

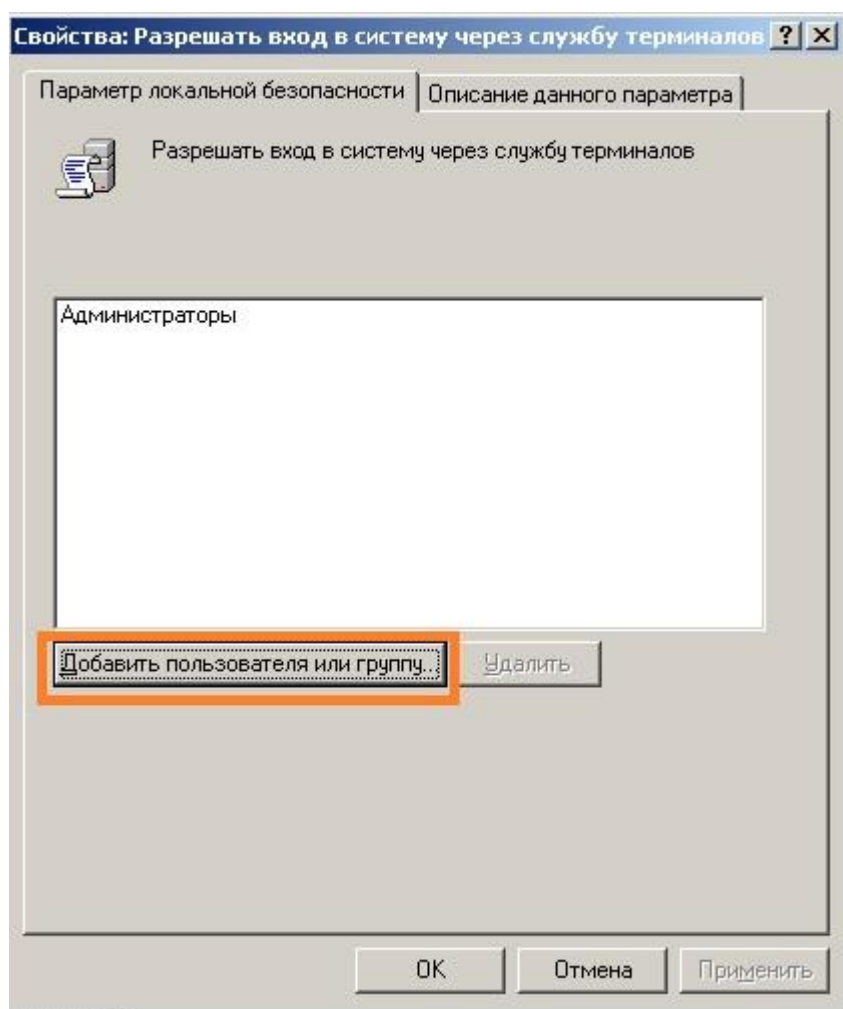


Выбираем **Локальные политики – Назначение прав пользователя**, там находим пункт **Разрешать вход в систему через службу терминалов**:

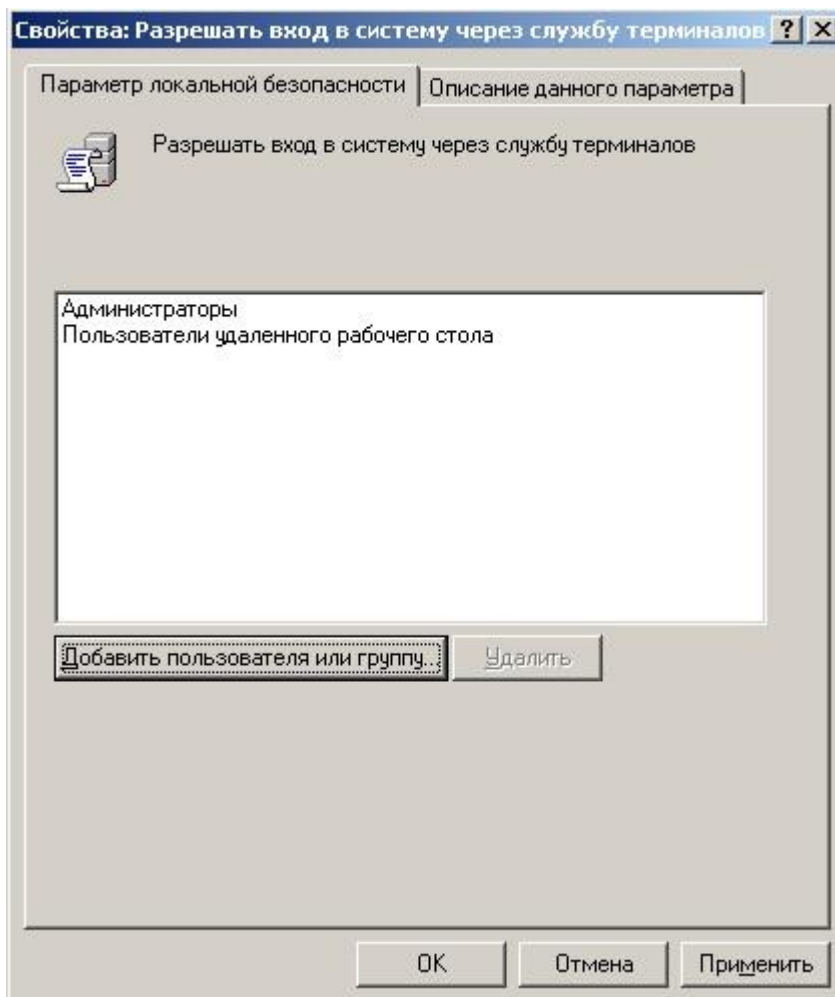




Теперь по аналогии добавляем в список группу **Пользователи удаленного рабочего стола**:







В принципе, всё... на Windows Server 2008 последовательность действий будет аналогичной...

После всего отправляем логин и пароль созданных учетных записей в МИАЦ через защищенную почту, на Администратора (**admin@vologdamed.local**)... Подробнее см. в инструкции **Защищенная почта**.

\*\*\*\*\*  
*See you next time. . . or never :->*

21.01.2015