



Network PROFI



LanAgent

Владея информацией,
владеешь миром

Руководство — «Быстрый
старт»

www.networkprofi.ru

Примечания

Copyright © 2005-2011 ООО «Нетворк Профи». Все права защищены.

Данное руководство включает следующие ограничения и условия:

- Руководство включает в себя информацию, принадлежащую ООО «Нетворк Профи». Она предоставлена исключительно в целях содействия авторизованным пользователям продукта LanAgent.
- Ни одна из частей документа не может быть использована в каких-либо других целях, предоставлена третьим лицам или компаниям, либо воспроизведена любыми средствами, электронными или механическими, без специального разрешения ООО «Нетворк Профи».
- Текст и изображения предназначены только для иллюстрации процесса работы. Компания оставляет за собой право изменения спецификации без предупреждения.
- Программное обеспечение, описанное в данном документе, лицензировано. Оно может быть использовано только в соответствии с лицензионным соглашением.
- Содержание руководства может быть изменено без предварительного предупреждения.

Данный документ создан ООО «Нетворк Профи». (<http://www.networkprofi.ru>)

Наименования других компаний, а также выпускаемых ими продуктов и оказываемых услуг, являются зарегистрированными торговыми марками соответствующих владельцев.

Информация об обновлении и сопроводительная информация находится на <http://www.lanagent.ru>

Если у вас возникли какие-либо вопросы или предложения, пишите на support@lanagent.ru.

Предисловие

Руководство Быстрый Старт предоставляет информацию о минимальном наборе настроек, необходимом для установки и быстрого запуска программы LanAgent Enterprise и включает Главы с 1 по 3 Руководства пользователя.

Содержание

1	О продукте LanAgent	5
1.1	Описание программы LanAgent	5
1.2	Для кого предназначена программа	6
1.3	Как работает программа LanAgent	7
1.4	Системные требования	9
2	Регистрация LanAgent	11
3	Быстрый запуск.....	13
3.1	Установка сервера LanAgent.....	13
3.1.1	Установка СУБД (системы управления базой данных)	13
3.1.2	Установка сервисов LanAgent	14
3.2	Установка модуля администратора LanAgent Admin	14
3.3	Установка агентов	16
3.3.1	Локальная установка агентов	16
3.3.2	Удаленная установка агентов	16
3.3.3	Устранение возможных проблем при удаленной установке агентов	18
3.3.4	Установка агентов через групповые политики Active Directory	20
3.4	Создание списка компьютеров для мониторинга	22
3.5	Создание групп пользователей	28
3.6	Установка LanAgent View.....	28

1 О продукте LanAgent

1.1 Описание программы LanAgent

LanAgent - ваш верный агент и помощник, позволяющий контролировать деятельность сотрудников вашей организации, работающих за компьютером, а также вести статистику использования компьютерного времени. Это дает возможность оптимизировать рабочий график. **LanAgent** позволяет наблюдать за деятельностью на любом из компьютеров, подключенных к локальной сети вашей организации и выполняет следующие действия: перехватывает все нажатия клавиш, делает снимки экрана, отслеживает установку и удаление программ, подключение и отключение носителей информации (таких как флэш, SD, жесткие диски), запоминает запуск и закрытие программ, следит за содержимым буфера обмена, следит за файлами и папками, отслеживает соединения с интернет и посещенные сайты, ведёт учет распечатанных на принтере документов. Ведение лога запускаемых программ, отслеживание содержимого буфера обмена, а также соединений с интернет и посещенных сайтов, позволит вам выявлять деятельность пользователей, не имеющую отношения к работе, а также те действия, которые могут быть опасными для вашей организации (копирование важных файлов, установка вредоносных программ). Снимки экранов компьютеров (скриншоты) дадут вам возможность визуального контроля.

Возможности программы LanAgent:

- Запоминает запуск и закрытие программ.
- Определяет подключение и отключение носителей информации.
- Делает снимки экранов мониторов.
- Перехватывает сообщения ICQ, Mail.ru Agent, MSN и Jabber.
- Запоминает набираемый на клавиатуре текст.
- Следит за содержимым буфера обмена.
- Перехватывает посещенные сайты.
- Ведет мониторинг входящей и исходящей почты.
- Производит теневое копирование файлов, копируемых на съемные usb носители или редактируемых на них.
- Перехватывает письма, отправляемые через web интерфейс, и выгрузку файлов в Интернет (при помощи модуля LA NetworkFilter).
- Запоминает установку и удаление программ.
- Ведет статистику создания и удаления файлов.
- Ведет учет документов, отправленных на печать на принтер.
- Отслеживает включение/выключение компьютера.
- Логирует работу с общими ресурсами компьютера.
- Расширенная система отчетов.
- Вся информация хранится централизованно в базе.
- Автоматическое получение статистики от контролируемых компьютеров.
- Информация передается по сети в зашифрованном виде.
- Возможность отправки текстовых сообщений на компьютер пользователя.

Уникальные особенности программы LanAgent:

- Скрытый режим работы агентов программы.
- Не видны в автозагрузке.
- "Активное оповещение" о нарушениях политик безопасности.
- Гибкий механизм назначения прав на просмотр информации специалистам безопасности.
- Оповещение о нарушениях политик безопасности на icq и e-mail.
- Встроенный планировщик отчетов с возможностью отправки отчетов на e-mail.
- При запоминании нажатых клавиш программа различает регистр, а также может запоминать русские буквы.
- При просмотре нажатых клавиш может показывать только символы и не показывать нажатия системных клавиш, что намного удобнее. Например, если были нажаты следующие клавиши:

"[Shift]Это[Space]программа[Space][Ctrl][Shift][Shift]Lan[Shift]Agent[Ctrl][Shift]."

- То установив галочку "Показывать только символы" вы увидите следующий текст:

"Это программа LanAgent."

- Поиск по логам с учётом или без учёта регистра.
- Установка ограничений при запоминании содержимого буфера обмена. Если в буфер обмена будут копироваться очень большие объёмы информации, то запоминаться будет только та часть, которую вы указали.

1.2 Для кого предназначена программа

LanAgent незаменимый помощник:

Для руководителя

Тактично и объективно предоставляет сведения о действиях, производимых Вашими сотрудниками за компьютером. Экономит Ваши средства, повышает эффективность использования рабочего времени.

Для специалиста информационной безопасности

LanAgent – Ваш инструмент для выявления утечек важной информации, а также фактов ведения переговоров с конкурентами.

Для системного администратора

Программа **LanAgent** поможет Вам узнать, что именно происходило в системе. Вы всегда будете знать обо всех действиях, производящихся на компьютерах вашей локальной сети, таких как установка вредоносных программ, удаление системных файлов и т.д.

1.3 Как работает программа LanAgent

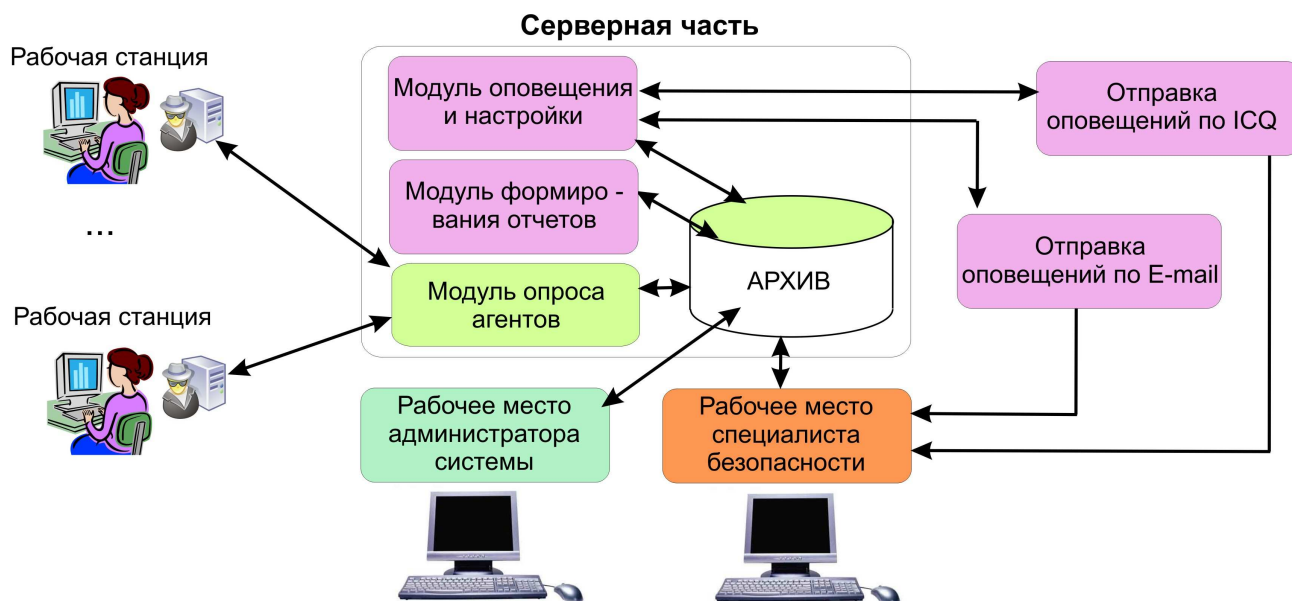


Рис. 1.1 – Структура LanAgent

Программа состоит из 4-х частей – пользовательская часть (агент), сервер, рабочее место специалиста безопасности и рабочее место администратора системы.

Агенты:

Устанавливаются непосредственно на те компьютеры, которые необходимо контролировать. Осуществляют мониторинг всех действий пользователей.

Серверная часть:

Устанавливается на специально выделенный под цели контроля компьютер. Она включает в себя модуль опроса агентов, который производит централизованный сбор информации по сети (опрос агентов); модуль оповещения и настройки; модуль формирования отчетов и базу данных, выполняющую роль архива. Модуль оповещения и настройки обеспечивает своевременную передачу событий активного оповещения (по ICQ и по E-mail) специалисту безопасности в случае нарушения политик безопасности. Модуль формирования отчетов предназначен соответственно для выполнения запланированных отчетов по – расписанию и отправки их, в случае необходимости, на указанный в настройках отчета e-mail. Для удобства управления серверными модулями, имеется специальная программа LanAgent ServiceManager.

Рабочее место специалиста безопасности:

Программный комплекс, позволяющий производить просмотр собранных от агентов данных, а также в совокупности с модулем оповещения и настройки, оперативно оповещать специалиста безопасности о произошедших нарушениях. Обеспечивает следующий функционал:

1. оперативное оповещение о нарушениях политики безопасности;
2. обеспечение доступа к архивам собранных от агентов данных;
3. планирование формирования отчетов;
4. доступ к данным производится только после обязательной аутентификации.

Данный комплекс включает в себя следующие программы:

1. LanAgent View - позволяет непосредственно производить просмотр собранных от агентов данных, получать активные оповещения, а также составлять отчеты в реальном времени;
2. LanAgent Sheduler (планировщик отчетов) – позволяет запланировать выполнение требуемых отчетов по - расписанию.

Рабочее место администратора системы:

Программный комплекс, позволяющий производить настройку системы: настройку агентов (какие виды событий (логов) и на каких компьютерах фиксировать), настройку правил безопасности по конкретным группам событий, настройку рабочих мест специалистов безопасности (раздача прав на просмотр собранных данных, подписка на оповещения и т.д.).

Обеспечивает следующий функционал:

1. управление настройками агентов;
2. настройка политик безопасности;
3. управление настройками рабочих мест специалистов безопасности (в т.ч. механизм подписки специалистов на определенные группы событий);
4. доступ к данным производится только после обязательной аутентификации.

Данный функционал реализован в программе LanAgent Admin.

Архитектура программы построена так, что агент может работать автономно, независимо от остальной части системы. То есть, если компьютер с серверной частью программы по какой-то причине выключен или с ним нет связи по локальной сети, то агент будет сохранять информацию в зашифрованных файлах на своем компьютере. И будет хранить эту информацию до тех пор, пока от серверной части не поступит запрос на получение логов. После отправки, лог-файлы на компьютере агента будут очищены.

Логи на компьютере пользователя могут храниться сколь угодно долго. Теоретически их размер ограничен только размером свободного дискового пространства. Тем не менее имеется возможность ввести ограничение на их размер, тогда при его превышении лог-файлы на компьютере пользователя будут очищены. Обратите внимание, что чем больше логов у пользователей, тем дольше будет производиться процесс получения логов модулем опроса агентов.

Обмен информацией производится по протоколу TCP/IP. Вам необходимо знать только ip-адрес компьютера, на котором установлен агент, или сетевое имя компьютера, чтобы серверная часть программы смогла к нему подключиться. Обмен информацией производится через порт: 47658. Если у вас на компьютере установлен firewall, то вам необходимо открыть этот порт.

Агенты запускаются при каждом старте Windows. Также по-умолчанию при каждом старте Windows автоматически запускается мониторинг. По желанию вы можете отключить автоматический старт мониторинга. Для этого в администраторской части выберите нужный компьютер в списке, нажмите правую кнопку мыши и в выпавшем меню выберите пункт "Настройки пользователя". Увидите галочку - "Стартовать мониторинг при загрузке Windows". Можете убрать эту галочку, тогда агент будет запускаться при загрузке Windows, но мониторинг вести не будет, а будет просто ждать команд от серверной части.

1.4 Системные требования

Ввиду клиент-серверной архитектуры программы LanAgent требования к аппаратному обеспечению формулируются для каждого компонента отдельно и будут различаться, в зависимости от количества контролируемых компьютеров.

Серверная часть.

Минимальные требования:

- Операционная система: Windows 2000/XP/2003/Vista/2008/7.
- Процессор Pentium 4 с частотой не менее 1,4 GHz.
- 512 МВ оперативной памяти.
- 100 МВ свободного места на диске.
- Открытые порты 47658, 7657, 3050 и 6587 TCP/IP на компьютере с сервером LanAgent (если используется фаервол, то надо в нем их открыть).

Рекомендуемые требования:

- Операционная система: Windows 2000/XP/2003/Vista/2008/7.
- Процессор Pentium 4 с частотой 3 GHz и выше.
- 1 GB оперативной памяти.
- 15 GB свободного места на диске (зависит от количества компьютеров и настроек программы).
- Открытые порты 47658, 7657, 3050 и 6587 TCP/IP на компьютере с сервером LanAgent (если используется фаервол, то надо в нем их открыть).

Пользовательская часть (агент).

Минимальные требования:

- Операционная система: Windows 2000/XP/2003/2008/Vista/7.
- Процессор Pentium 3 и выше.
- 128 МВ оперативной памяти.
- 15 МВ свободного места на диске.
- Открытые порты 47658 и 7657 TCP/IP на компьютере с агентом (если используется фаервол, то надо в нем их открыть).

Рекомендуемые требования:

- Операционная система: Windows 2000/XP/2003/2008/Vista/7.
- Процессор Pentium 3 и выше.
- 512 МВ оперативной памяти.
- 100 МВ свободного места на диске.
- Открытые порты 47658 и 7657 TCP/IP на компьютере с агентом (если используется фаервол, то надо в нем их открыть).

Внимание! Начиная с версии LanAgent 3.4, для работы на операционной системе Windows 2000 выделен специальный вариант агента. Имя его инсталляционного файла userXX_win2000.msi. Удаленная установка агента на win 2000, средствами административной части LanAgent, возможна тоже только при использовании специального установочного файла. Для его получения, а также по всем возникающим вопросам пишите пожалуйста на support@lanagent.ru

Для работы консолей администрирования и просмотра данных необходимо, чтобы были открыты порты 3050 и 6587 TCP/IP на компьютерах, на которых данные консоли установлены.

2 Регистрация LanAgent

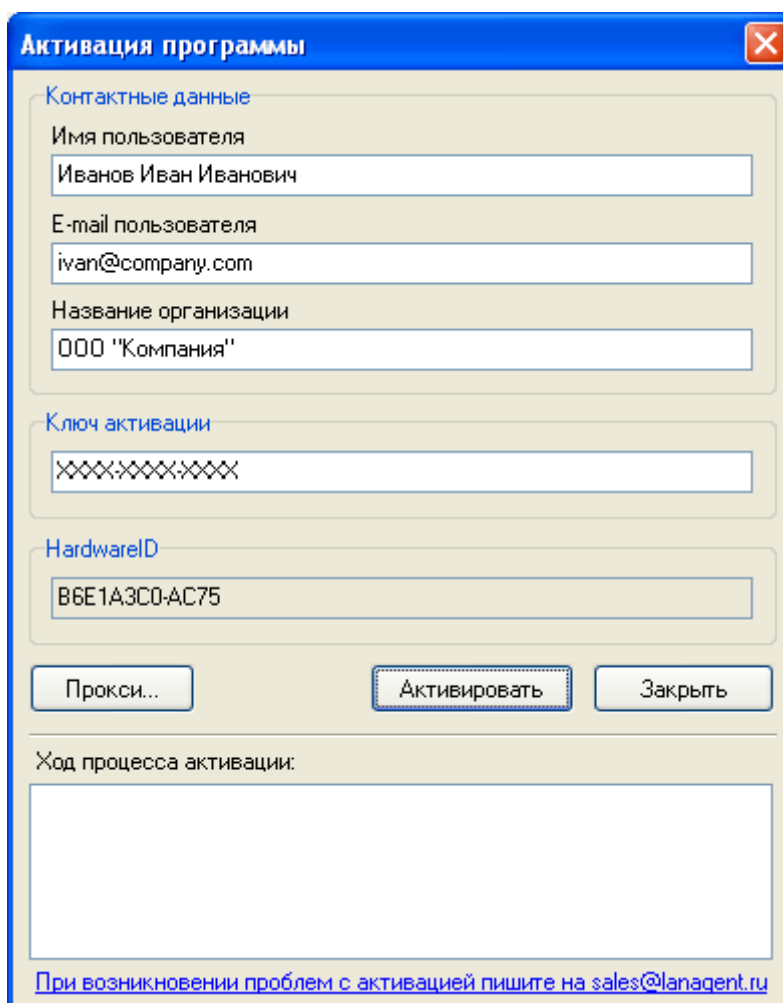
После установки программы LanAgent, необходимо произвести ее активацию.

Для активации вам необходимо:

1. Запустить программу **LanAgent**.
2. Нажать на кнопку "Регистрация".



3. В открывшемся окне введите ваши данные: Фамилию, Имя, Отчество, E-mail и Название организации (если есть), а также ключ активации. (Чтобы скопировать ключ активации, выделите его в письме и нажмите Ctrl+C; чтобы вставить в открывшееся окно нажмите Ctrl+V). Если необходимо, то введите данные прокси-сервера.

Скриншот окна "Активация программы". В окне есть три группы полей для ввода: "Контактные данные" (Имя пользователя: Иванов Иван Иванович, E-mail пользователя: ivan@company.com, Название организации: ООО "Компания"), "Ключ активации" (маска XXXXXXXXXX) и "HardwareID" (B6E1A3C0-AC75). Внизу расположены кнопки "Прокси...", "Активировать" и "Закреть". В самом низу есть поле "Ход процесса активации:" и ссылка "При возникновении проблем с активацией пишите на sales@lanagent.ru".

Активация программы

Контактные данные

Имя пользователя
Иванов Иван Иванович

E-mail пользователя
ivan@company.com

Название организации
ООО "Компания"

Ключ активации
XXXXXXXXXXXX

HardwareID
B6E1A3C0-AC75

Прокси... Активировать Закреть

Ход процесса активации:

При возникновении проблем с активацией пишите на sales@lanagent.ru

Рис. 2.1 - Активация программы

4. Нажмите кнопку "Активировать" и подождите некоторое время.
5. Если активация прошла успешно, то программа выдаст соответствующее сообщение.
6. Зарегистрируйте и перезапустите сервисы, при помощи «**Менеджера сервисов**»: регистрация сервисов производится нажатием кнопки «**Зарегистрировать сервисы**». В процессе регистрации сервисов будет выдан запрос на перезапуск сервисов LanAgent.

3 Быстрый запуск

Внимание! В процессе установки будут производиться необходимые изменения и дополнения в конфигурацию системы, поэтому важно следовать указанной ниже очередности установки программ.

3.1 Установка сервера LanAgent

Производится путем запуска установочного файла **LanAgent Server.msi**. Процесс установки включает в себя две ступени: установка СУБД (системы управления базой данных) и установка сервисов **LanAgent**.

3.1.1 Установка СУБД (системы управления базой данных)

В качестве СУБД для **LanAgent** выбрана FireBird 1.5.3. Ее установочный файл уже включен в состав инсталляционного пакета «**LanAgent Server.msi**» и запускается автоматически. Для установки запустите названный выше файл и следуйте инструкциям инсталлятора. В диалоге выбора варианта установки FireBird (**Classic** или **Superserver**) выберите вариант **Superserver**.

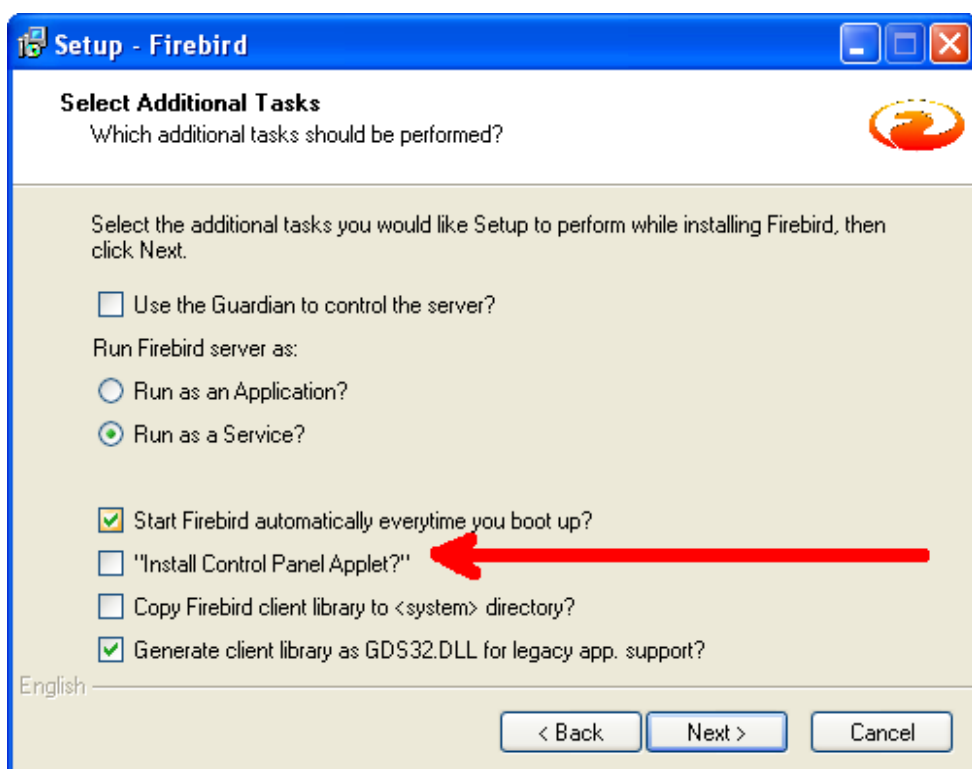
Отдельно саму СУБД можно скачать по адресу:

http://sourceforge.net/project/showfiles.php?group_id=9028

Важное замечание! При установке серверной части программы LanAgent (и СУБД FireBird в том числе) на компьютеры с ОС Windows Vista/7, при установке FireBird рекомендуем снять галочку с пункта «Установка апплета в панель управления» (**Install Control Panel Applet**).

На данных ОС установка апплета FireBird может привести к «падению» проводника windows при попытках доступа к Панели управления. Подробное описание данного момента приведено тут: <http://www.firebirdfaq.org/faq360/>

Снимок окна инсталлятора, на котором отмечена опция установки апплета, приведен ниже.



3.1.2 Установка сервисов LanAgent

Сервер LanAgent включает в себя несколько компонент, каждая из которых выполняет свою функцию. Установка всех компонент производится через один инсталляционный файл «**LanAgent Enterprise Server.exe**». Для этого необходимо его запустить и далее следовать инструкциям программы установки. В процессе работы инсталлятора будет также произведена конфигурация сервера.

3.2 Установка модуля администратора LanAgent Admin

Данная программа устанавливается на рабочее место администратора системы, с ее помощью производится настройка системы.

Для начала процесса установки **LanAgent Admin** достаточно запустить установочный файл «**LanAgent Enterprise Admin.msi**» и следовать инструкциям мастера установки.

При первом запуске **LanAgent Admin** предложит заполнить параметры подключения к базе данных:

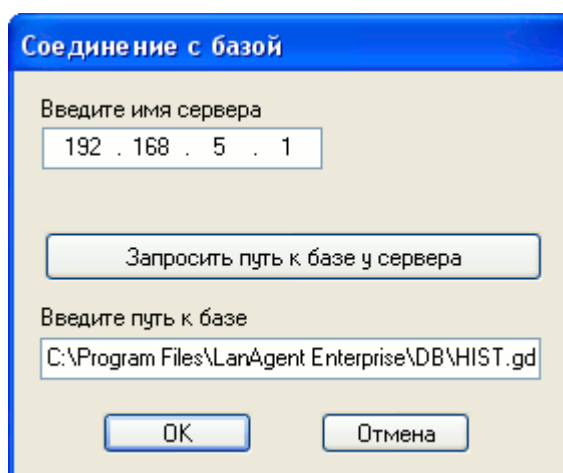


Рисунок 4 – Диалог соединения с базой

В этом диалоге требуется указать имя сервера, на котором установлена база, а также путь к файлу Hist.gdb. Сам путь можно получить от сервера LanAgent, нажав соответствующую кнопку (Запросить путь к базе у сервера). Если в ходе запроса пути к базе было выдано сообщение о невозможности подключения к серверу, то необходимо убедиться, что на сервере запущен сервис обмена LanAgent и обмен с сервером не блокируется фаерволом.

Внимание! Не надо открывать общего доступа к указанному файлу базы данных, путь указывается исключительно для сервера!

Далее программа попросит ввести имя пользователя, имеющего права на изменение настроек, и пароль.

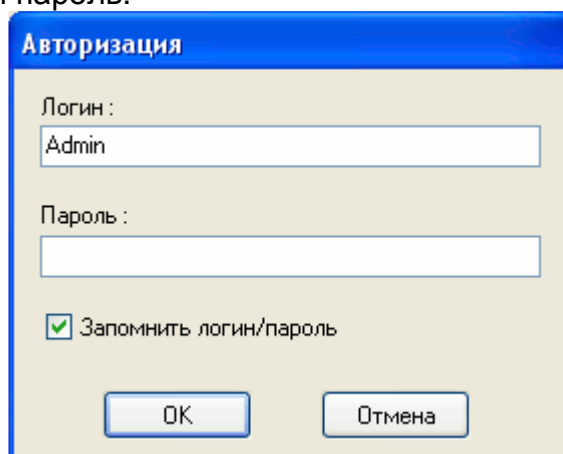


Рисунок 5 – Диалог авторизации

Внимание! Работать с LanAgent Admin может только пользователь с правами администратора!

По-умолчанию в базе уже имеется учетная запись с именем **Admin** и пустым паролем. Настоятельно рекомендуем в дальнейшем сменить для нее пароль, в целях повышения безопасности.

3.3 Установка агентов

3.3.1 Локальная установка агентов

Для установки агента необходимо скопировать файл "User.msi" на компьютер пользователя, запустить его и следовать инструкциям мастера установки. Внимание! Установку пользовательской части нужно производить из-под учётной записи с администраторскими правами.

3.3.2 Удаленная установка агентов

Для этого воспользуйтесь диалогом установки агентов, который вызывается в администраторской части LanAgent кнопкой **"Добавить"**.

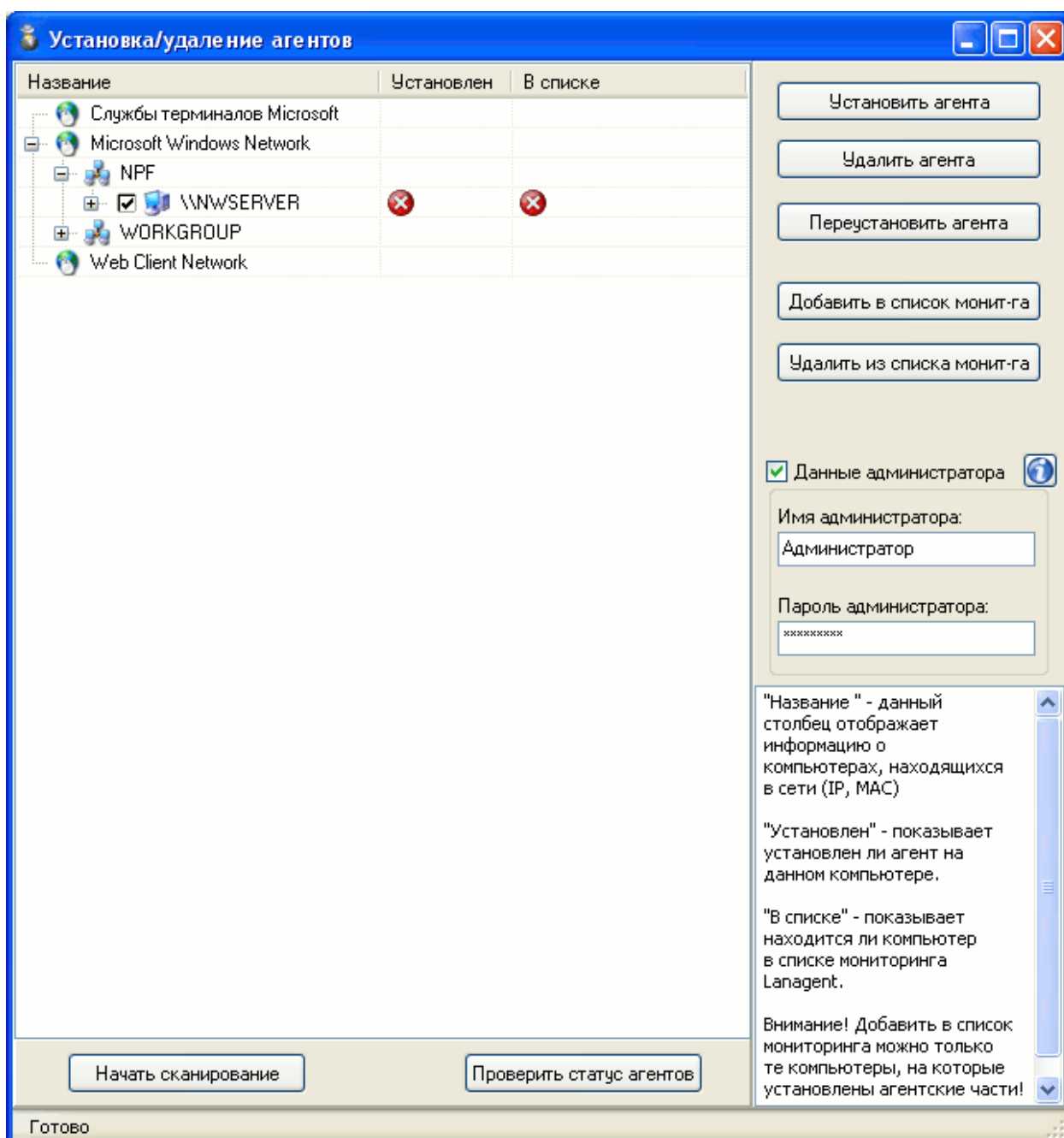
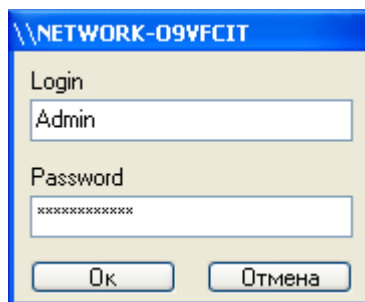


Рис 3.1 – Диалог установки/удаления агентов

После открытия окна, потребуется немного подождать, пока будет просканирована локальная сеть на предмет наличия в ней компьютеров с уже установленными агентами. Это будет отображено в виде таблички (см рисунок), где в колонке "Установлен" - показан статус самого агента (установлен/не установлен), в колонке "В списке" - занесен ли данный компьютер в список мониторинга.

Далее, надо отметить галочками компьютеры, на которые необходимо установить агентов и нажать кнопку "**Установить агента**". Для каждого выбранного компьютера будет вызван диалог ввода логина и пароля администратора.



Процесс установки агента может занять некоторое время. Дождитесь его завершения, не закрывая диалог установки/удаления агентов.

Рекомендуем внести в исключение в антивирусе следующие пути: "Admin\$\installservice.exe" и "C:\Windows\installservice.exe" это необходимо, чтобы антивирус не блокировал сам файл установки агента. Каталог установки агента по умолчанию system32\lasys. Рекомендуем внести в исключение файлы агента (system.exe, svchost.exe, sys.dll, wssfcmai.exe) из данного каталога.

Если в процессе установки возникнут ошибки, то они будут выведены на экран в виде сообщений. Подробнее об устранении ошибок при инсталляции агентов см. пункт 3.2.3.

3.3.3 Устранение возможных проблем при удаленной установке агентов

Ниже будут приведены наиболее типичные причины, из-за которых не получается произвести удаленную установку, и методы их устранения. В самом низу раздела указаны моменты, специфичные для конкретных операционных систем.

Внимание! Прежде чем приступать к изменению настроек, проконсультируйтесь с Вашим системным администратором!

Возможные причины:

1. Указаны неверные логин и пароль администратора для доступа к компьютеру.

Проверьте еще раз их правильность. У введенной учетной записи должны быть права администратора на компьютере, на который производится установка агента.

2. Включен "Простой доступ к файлам" ("Simple file sharing") на удаленном компьютере.

Необходимо выключить данную опцию. Для этого откройте папку "Мой компьютер", в меню "Сервис" выберите пункт "Свойства папки...". Далее

перейдите на вкладку "Вид" и уберите галочку на строке "Использовать простой общий доступ к файлам". Подтвердите изменения кнопкой "ОК" или "Применить".

3.Сервис "Сервер" ("Server") не включен на удаленной машине.

Запустите его. Например так: "Панель управления"->"Администрирование"->"Службы". Далее выберите нужный сервис из списка и нажмите кнопку "Запустить".

4.Отсутствует служебный ресурс ADMIN\$ на удаленном компьютере.

Для того чтобы его включить, потребуется набрать в командной строке "net share admin\$". Если на компьютере в реестре присутствует такой ключ: "HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\lanmanserver\parameters"

Для Windows Server 2000/2003 - AutoShareServer типа REG_DWORD;

для Windows 2000/XP - AutoShareWks типа REG_DWORD

то установить его в "1".

5.Выключен сервис "Удаленный вызов процедур (RPC)" ("Remote Registry Service").

Включите его. "Панель управления"->"Администрирование"->"Службы". Далее выберите нужный сервис из списка и нажмите кнопку "Запустить".

6.Не настроен фаервол.

Обмен информацией с агентом производится по протоколу TCP/IP через порт: 47658. Если у вас на компьютере установлен firewall, то вам необходимо открыть этот порт.

7.Процесс установки блокируется антивирусом.

Рекомендуем внести в исключение в антивирусе следующие пути: "Admin\$\installservice.exe" и "C:\Windows\installservice.exe" это необходимо, чтобы антивирус не блокировал сам файл установки агента. Каталог установки агента по умолчанию system32\asys. Рекомендуем внести в исключение файлы агента (system.exe, svchost.exe, sys.dll, wssfcmai.exe) из данного каталога.

Установка агента на Windows 7/Vista.

На ОС Win 7 по умолчанию отсутствует служебный ресурс Admin\$. Добавить его можно так:

1). Зайти в панель управления (Control panel) -> выбрать пункт "Сеть и Интернет" (Network and Internet) -> Сеть и общий доступ (Network and Sharing Center).

2). В левой части нового открывшегося окна кликнуть на строке "Изменить дополнительные параметры общего доступа" (Change Advanced Sharing Settings). Далее, нажать на "Включить общий доступ к файлам и принтерам" ("Turn on file and printer sharing"). Сохранить настройки.

3). Открыть редактор реестра, зайти в ветку HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System и создать в ней ключ типа DWORD с именем LocalAccountTokenFilterPolicy. Выставить значение этого параметра в 1 и перезагрузить компьютер. Либо можно загрузить ключ реестра по ссылке www.lanagent.ru/localsp.reg

Кроме того, на время установки должен быть отключен UAC (User account control).

Установка агента на Windows 2000.

Для удаленной установки агентов средствами административной части LanAgent на данную ОС, необходимы специальные файлы установки. Для их получения напишите нам на e-mail support@lanagent.ru

3.3.4 Установка агентов через групповые политики Active Directory

Также, для сетей с доменной архитектурой, установку агентов можно произвести используя групповые политики.

Назначение установки программы

Вы можете назначить установку программы для указанного компьютера или группы компьютеров. Программа будет установлена при первом запуске компьютера.

Создание распределительного пункта (distribution point)

Для установки программы на другие компьютеры Вы должны создать распределительный пункт (distribution point) на публичном сервере, где будет храниться установочный файл пользовательской части программы LanAgent.

1. Зайдите на публичный сервер под администратором
2. Создайте папку с общим доступом (distribution point) и скопируйте туда Microsoft Software Installer (MSI) пакет пользовательской части программы LanAgent (**user.msi**).
3. Установите разрешения на доступ к папке с установочным пакетом

Создания объекта групповой политики (GPO)

1. Запустите оснастку **Active Directory – пользователи и компьютеры** (Active Directory Users and Computers).
*Примечание: Оснастку **Active Directory – пользователи и компьютеры** можно запустить так: Пуск, Программы, Администрирование, Active Directory – пользователи и компьютеры.*
2. В дереве консоли кликните правой клавишей мышки на вашем домене и выберите свойства.
3. Перейдите на вкладку **Групповая политика** и нажмите **Создать**.
4. Напишите желаемое имя вашей политики (например **LanAgent distribution**) и нажмите **Enter**.
5. Нажмите **Свойства** и перейдите на вкладку **Безопасность**.
6. Отметьте **Применение групповой политики** для необходимой группы, затем нажмите **ОК**.

Назначение пакета

1. Запустите оснастку **Active Directory – пользователи и компьютеры** (Active Directory Users and Computers).
2. Кликните правой клавишей мыши на имени вашего домена и выберите **Свойства**.
3. Перейдите на вкладку **Групповая политика** и выбрав нужную политику нажмите **Изменить**.
4. Разверните ветвь **Конфигурация компьютера, Конфигурация программ**
5. Кликните правой клавишей мыши на **Установка программ** и выберите **Создать** потом **Пакет**.
6. В открывшемся диалоговом окне введите полный UNC путь к общедоступной папке содержащей нужный Вам MSI пакет. Например **\\file server\share\user.msi**. Важно что бы имя было в формате UNC.
7. Нажмите **Открыть**.
8. Выберите **Назначенный** и нажмите **ОК**. Пакет отобразится на правой панели окна групповых политик.
9. Закройте оснастку групповые политики и нажмите **ОК** и выйдете из оснастки **Active Directory – пользователи и компьютеры**. Когда компьютер запустится указанная программа будет установлена.

Переустановка пакета

Иногда Вам необходимо обновить программу, для этого нужно воспользоваться функцией переустановки.

1. Запустите оснастку **Active Directory – пользователи и компьютеры** (Active Directory Users and Computers).
2. Кликните правой клавишей мыши на имени вашего домена и выберете **Свойства**.

3. Перейдите на вкладку **Групповая политика** и выбрав нужную политику нажмите **Изменить**.
4. Разверните ветвь **Конфигурация компьютера, Конфигурация программ**
5. Выберите ту программу, которую вы желаете обновить и кликнете на ней правой клавишей мыши в появившемся окне выберите **Все задачи, Развернуть приложение заново**.
6. Нажмите **Да**.

Ссылки

Для получения дополнительной информации по вопросу удаленной установки программного обеспечения в сети под управлением домена Windows обратитесь к базе знаний Microsoft:

[302430 - HOW TO: Assign Software to a Specific Group By Using a Group Policy](http://support.microsoft.com/default.aspx/kb/302430/)

(<http://support.microsoft.com/default.aspx/kb/302430/>)

[314934 - HOW TO: Use Group Policy to Remotely Install Software in Windows 2000](http://support.microsoft.com/default.aspx/kb/314934/)

(<http://support.microsoft.com/default.aspx/kb/314934/>)

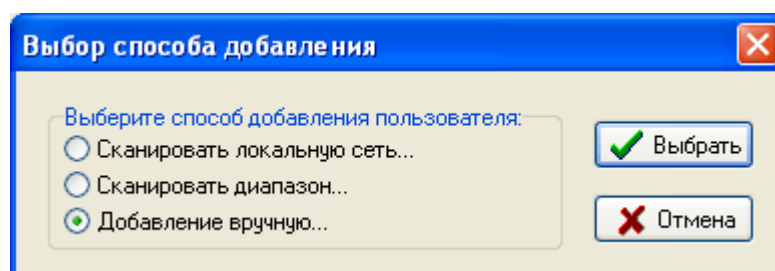
[816102 - How to use Group Policy to remotely install software in Windows Server 2003](http://support.microsoft.com/default.aspx/kb/816102/)

(<http://support.microsoft.com/default.aspx/kb/816102/>)

3.4 Создание списка компьютеров для мониторинга

Для сбора данных с компьютера, за которым требуется установить контроль, необходимо после установки пользовательской части программы LanAgent, добавить этот компьютер в список мониторинга. Для удобства работы с данным списком, имеется возможность распределить компьютеры по группам. Поэтому если вы хотите сразу добавить компьютер в группу, то выберите в списке группу, к которой будет относиться данный компьютер и нажмите кнопку "Добавить" на панели инструментов (в верхней части окна программы) и выберите подпункт "Добавить пользователя...".

При этом откроется окно выбора способа добавления:



При выборе варианта "Добавление вручную", откроется следующее диалоговое окно:

Рис. 3.2 - Добавление компьютера в список мониторинга

Добавить компьютеры в список можно 2-мя способами:

- конкретно указав ip-адрес или имя компьютера
- указав диапазон ip-адресов

В поле "IP-адрес или имя компьютера" впишите IP адрес или имя компьютера, которого добавляете в список.

Содержимое поля "Название" в дальнейшем будет отображаться в списке мониторинга. Поэтому заполните его **понятным вам** названием.

Если вы уже назначали пароль для агента, которого хотите добавить, то введите старый пароль. Если вы добавляете этого агента впервые, то оставьте поле "Старый пароль" пустым.

В поле "Новый пароль" впишите пароль на доступ к агенту, чтобы только вы могли получать логи. По-умолчанию это поле пустое. Вы можете изменить пароль по-умолчанию в настройках программы. Если у вас нет особой надобности защищать соединения паролем, то оставьте это поле пустым.

После нажатия кнопки "Далее", будет произведена проверка подключения к программе-агенту, установленной на контролируемом компьютере. Если подключение произведено успешно, то данный компьютер будет добавлен в список, в противном случае вы увидите следующее:

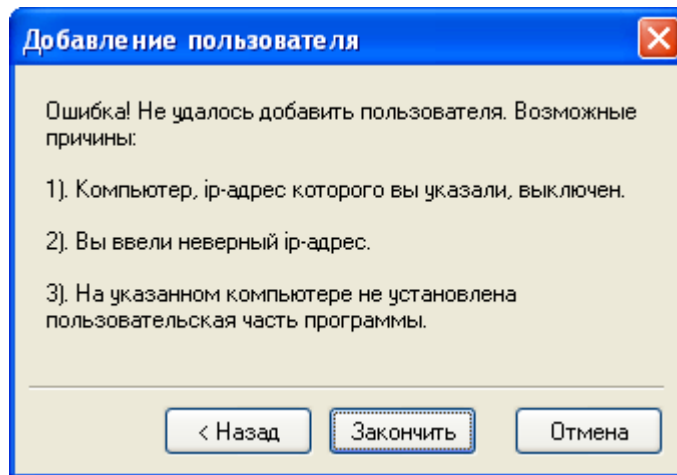


Рис. 3.3 – Ошибка добавления в список

Чтобы изменить параметры подключения, нажмите кнопку "Назад".

При выборе в первом диалоге варианта "Сканировать локальную сеть", откроется общий диалог установки/удаления агентов и добавления их в список:

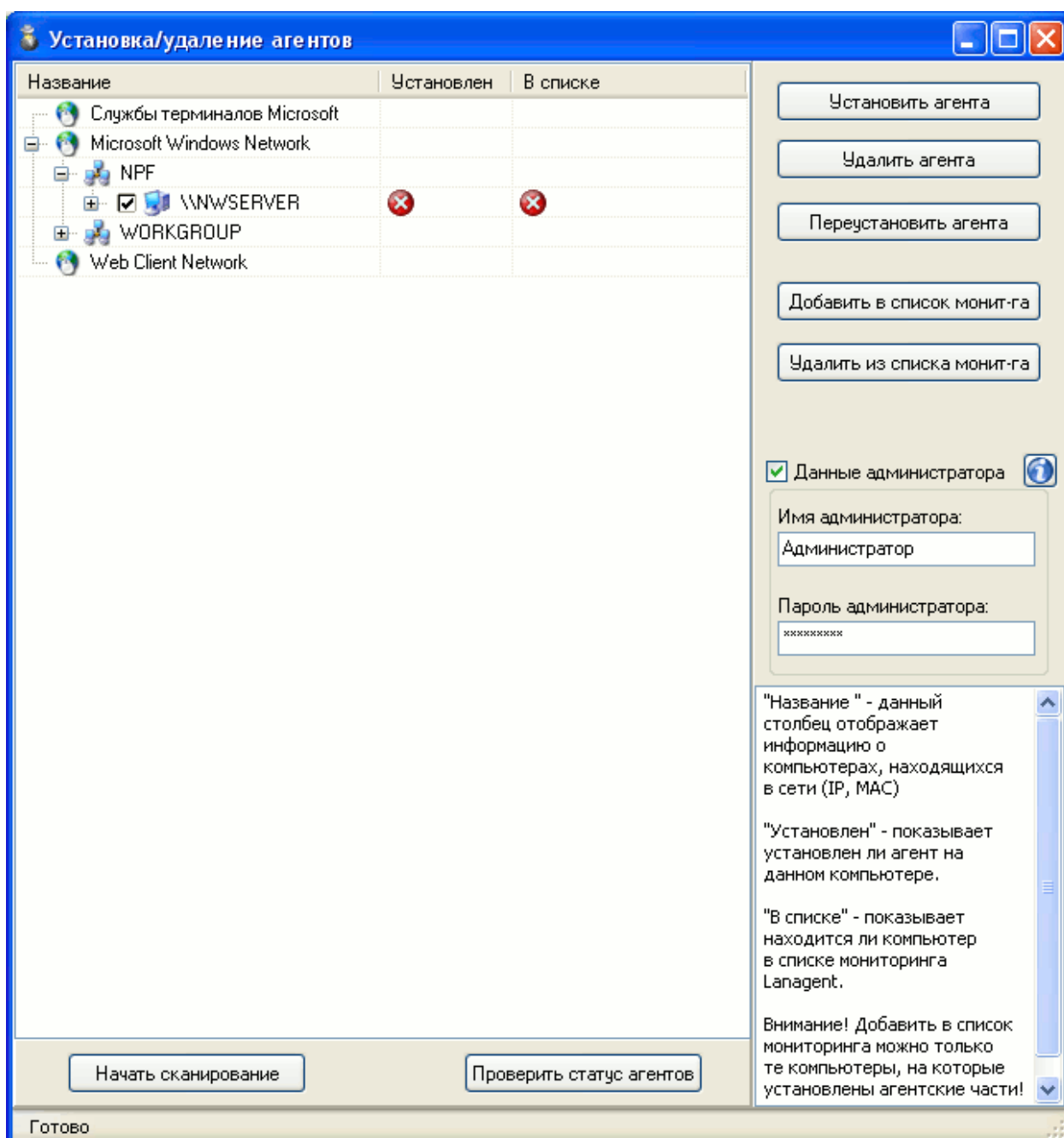


Рис. 3.4 – Диалог установки/удаления агентов

После открытия окна, потребуется немного подождать, пока будет просканирована локальная сеть на предмет наличия в ней компьютеров с уже установленными агентами. Это будет отображено в виде таблички (см рисунок), где в колонке "Установлен" - показан статус самого агента (установлен/не установлен), в колонке "В списке" - занесен ли данный компьютер в список мониторинга.

Для добавления компьютеров в список мониторинга, надо отметить их галочками и нажать кнопку **"Добавить в список монит-га"**. (разумеется, добавить в список мониторинга можно только те компьютеры, на которых установлены агенты)

При этом откроется следующее диалоговое окно:

Добавление пользователей

Название
Программист

Старый пароль

Новый пароль

Показать пароль

Изменить пароль по-умолчанию

< Назад Далее > Отмена

Если в предыдущем окне был выбран только один компьютер для добавления в список, то поле "Название" будет доступно для заполнения. Его содержимое в дальнейшем будет отображаться в списке мониторинга. Поэтому заполните его **понятным вам** названием. В случае добавления сразу нескольких компьютеров, данное поле будет заполнено автоматически.

Если вы уже назначали пароль для агента, которого хотите добавить, то введите старый пароль. Если вы добавляете этого агента впервые, то оставьте поле "Старый пароль" пустым.

В поле "Новый пароль" впишите пароль на доступ к агенту, чтобы только вы могли получать логи. По-умолчанию это поле пустое. Вы можете изменить пароль по-умолчанию в настройках программы. Если у вас нет особой надобности защищать соединения паролем, то оставьте это поле пустым.

После нажатия кнопки "Далее", будет произведена проверка подключения к программе-агенту, установленной на контролируемом компьютере. Если подключение произведено успешно, то данный компьютер будет добавлен в список, иначе будет сообщено об ошибке.

Добавление пользователей

Кол-во добавленных пользователей: 1

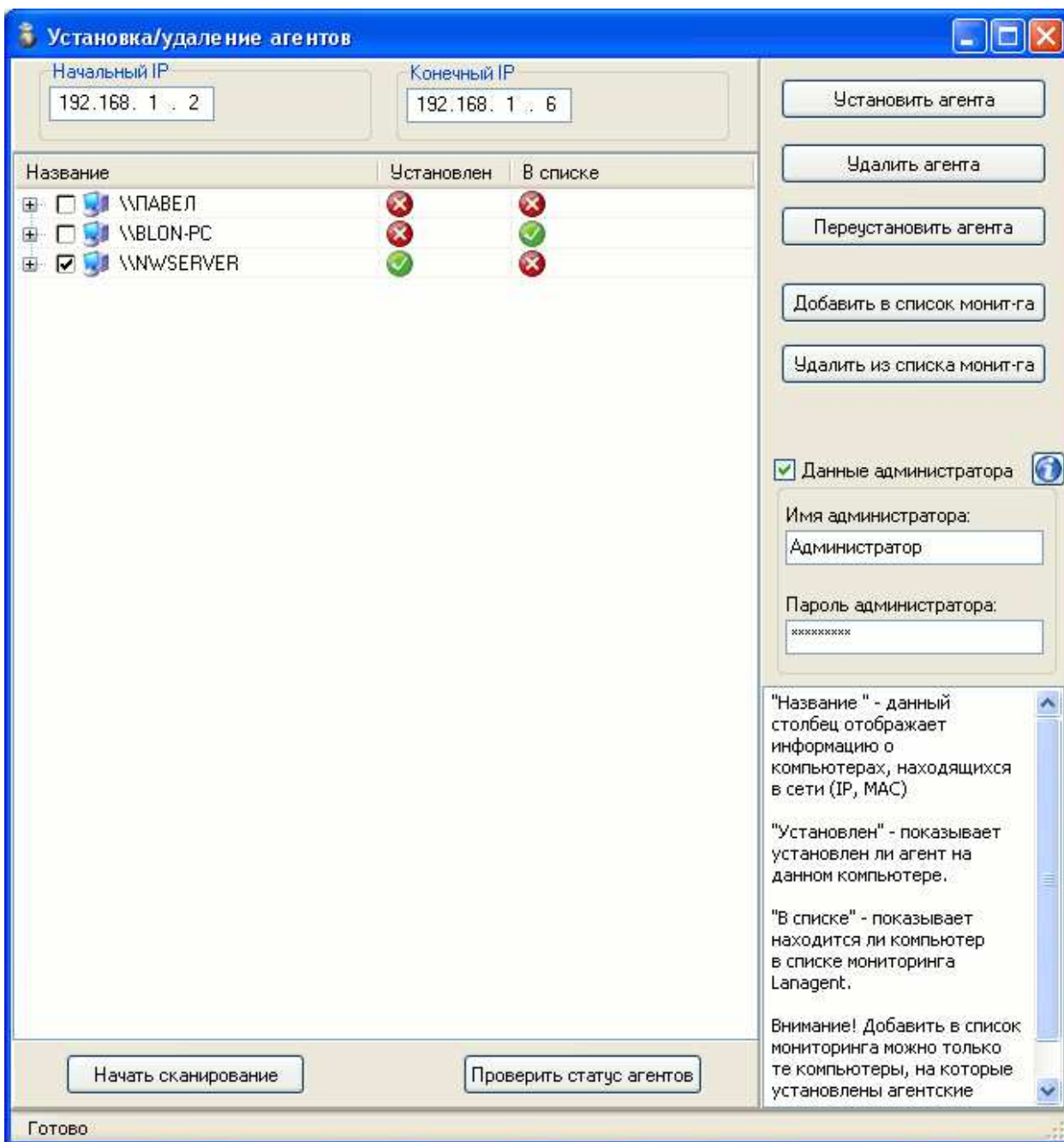
Пользователь 192.168.7.4 (ALEX) успешно добавлен

< Назад Закончить Отмена

Чтобы изменить параметры подключения, нажмите кнопку "Назад".

После успешного завершения, компьютер будет добавлен в список мониторинга в указанную группу. В процессе работы вы сможете переместить компьютер в другую группу. Для этого просто щелкните мышкой на строке с перемещаемым объектом и, удерживая клавишу нажатой, перетащите его на строку с требуемой группой. Чтобы отвязать объект (переместить его на самый верх иерархии) достаточно перетащить его на заголовок списка или просто на любое незаполненное место списка.

Ну и наконец, при выборе в первом диалоге варианта "Сканировать диапазон...", откроется диалог установки/удаления агентов с ограничением диапазона сканирования:



После открытия окна, необходимо задать диапазон IP адресов и нажать кнопку **"Начать сканировать"**. Потребуется немного подождать, пока будет просканирована локальная сеть на предмет наличия в ней компьютеров с уже установленными агентами. Это будет отображено в виде таблички (см рисунок), где в колонке "Установлен" - показан статус самого агента (установлен/не установлен), в колонке "В списке" - занесен ли данный компьютер в список мониторинга. Все остальные действия с данным диалогом подобны описанным для варианта **"Сканировать локальную сеть"**.

3.5 Создание групп пользователей

Для удобства работы со списком компьютеров для мониторинга, имеется возможность объединять компьютеры в группы, например в соответствии с тем как они распределены по отделам структуры предприятия. Для создания новой группы нажмите кнопку "Добавить" на панели инструментов (в верхней части окна программы) и выберите подпункт "Добавить группу...".

При этом откроется следующее диалоговое окно:

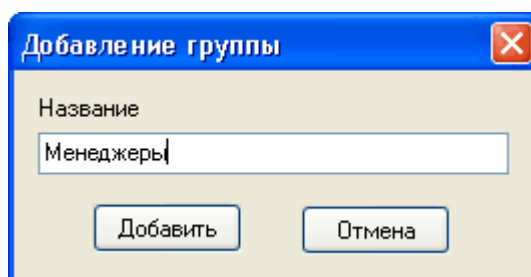


Рис. 3.5 – Добавление группы пользователей

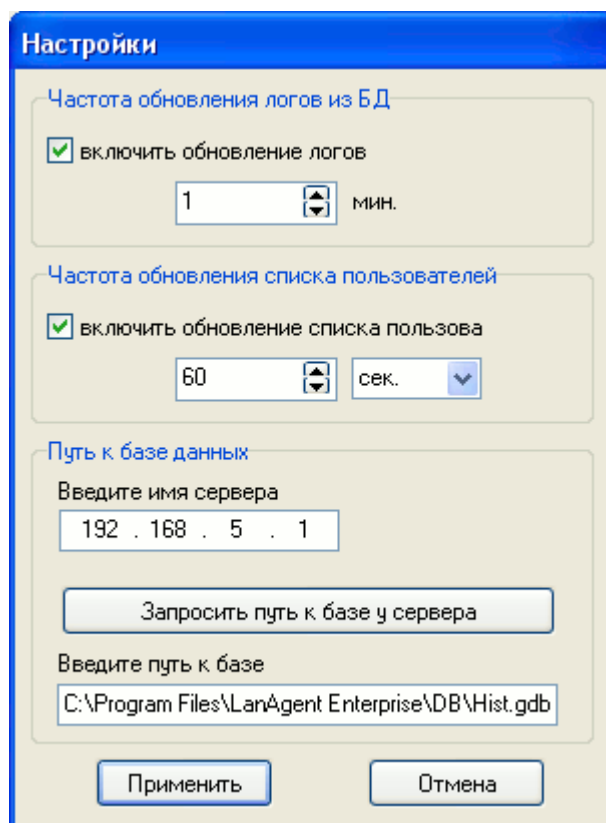
После нажатия кнопки "Добавить", группа будет добавлена в список мониторинга. Также имеется возможность создания вложенных подгрупп. Для этого выберите из списка группу, в которой хотите добавить подгруппу и нажмите кнопку "Добавить"->"Добавить группу...". (смотри выше). В процессе работы вы можете перемещать как компьютеры из одной группы в другую, так и целые группы. Для этого просто щелкните мышкой на строке с перемещаемым объектом и, удерживая клавишу нажатой, перетащите его на строку с требуемой группой. Чтобы отвязать объект (переместить его на самый верх иерархии) достаточно перетащить его на заголовок списка или просто на любое незаполненное место списка.

3.6 Установка LanAgent View

Данная программа устанавливается на рабочее место специалиста безопасности и позволяет просматривать собранные с контролируемых компьютеров данные, а также получать уведомления о нарушении политик безопасности.

Для начала процесса установки LanAgent View достаточно запустить установочный файл «**LanAgent Enterprise View.msi**» и следовать инструкциям мастера установки.

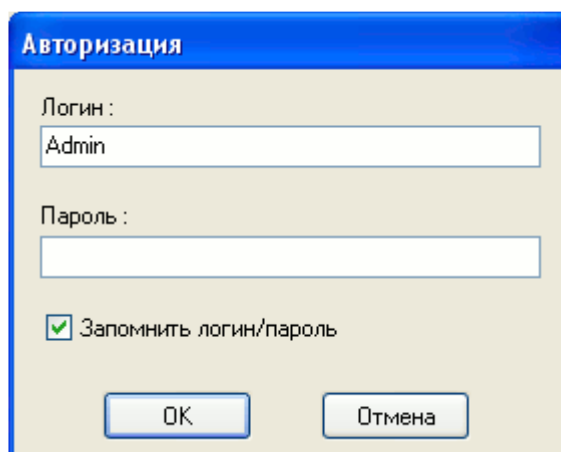
При первом запуске LanAgent View предложит заполнить параметры подключения к базе данных.



В этом диалоге требуется указать имя сервера, на котором установлена база, а также путь к файлу HIST.gdb. Сам путь можно получить от сервера LanAgent, нажав соответствующую кнопку (Запросить путь к базе у сервера). Если в ходе запроса пути к базе было выдано сообщение о невозможности подключения к серверу, то необходимо убедиться, что на сервере запущен сервис обмена LanAgent и обмен с сервером не блокируется фаерволом.

Внимание! Не надо открывать общего доступа к указанному файлу, путь указывается исключительно для сервера!

Далее программа попросит ввести имя пользователя, имеющего право доступа, и пароль.



В зависимости от прав доступа, для пользователя будут доступны соответствующие категории информации. Администратор имеет полный доступ. (подробнее о правах доступа, их назначении и изменении смотрите в Руководстве пользователя).