Network PROFI

LanAgent

Владея информацией,
владеешь миром

Руководство – «Быстрый старт»

www.networkprofi.ru

Примечания

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

1.1 Описание программы LanAgent

LanAgent Terminal – Легко масштабируемый инструмент для слежения за действиями пользователей терминальных клиентов. Осуществляет контроль и мониторинг активности пользователей и выполняет следующие действия: перехватывает все нажатия клавиш, делает снимки экрана, отслеживает установку и удаление программ, запоминает запуск и закрытие программ, следит за содержимым буфера обмена, следит за файлами и папками, посещёнными сайтами, ведёт учет распечатанных на принтере документов. Ведение лога запускаемых программ, отслеживание содержимого буфера обмена, а также 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.

LanAgent позволит выявить деятельность, не имеющую отношения к работе, покажет, насколько рационально ваши сотрудники используют рабочее время. Решает одну из основных задач информационной безопасности - борьба с инсайдерами в организации. LanAgent – Ваш инструмент для выявления утечек важной информации, а также фактов ведения переговоров с конкурентами.

Возможности программы LanAgent:

- Запоминает запуск и закрытие программ.
- Делает снимки экранов мониторов.
- Запоминает набираемый на клавиатуре текст.
- Следит за содержимым буфера обмена.
- Перехватывает посещённые сайты.
- Запоминает установку и удаление программ.
- Ведет статистику создания и удаления файлов.
- Ведет учет документов, отправленных на печать на принтер.
- Отслеживает подключение и отключение пользователя к терминальному серверу.
- Перехватывает сообщения ICQ, Mail.ru Agent, MSN и Jabber.
- Ведет мониторинг входящей и исходящей почты, в т.ч. отправляемой через web-интерфейс и выгрузку файлов в Интернет (при помощи модуля LA NetworkFilter).
- Расширенная система отчетов.
- Вся информация хранится централизованно в базе.
- Автоматическое получение статистики с контролируемых пользователей.
- Возможность отправки текстовых сообщений на компьютер пользователя.

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

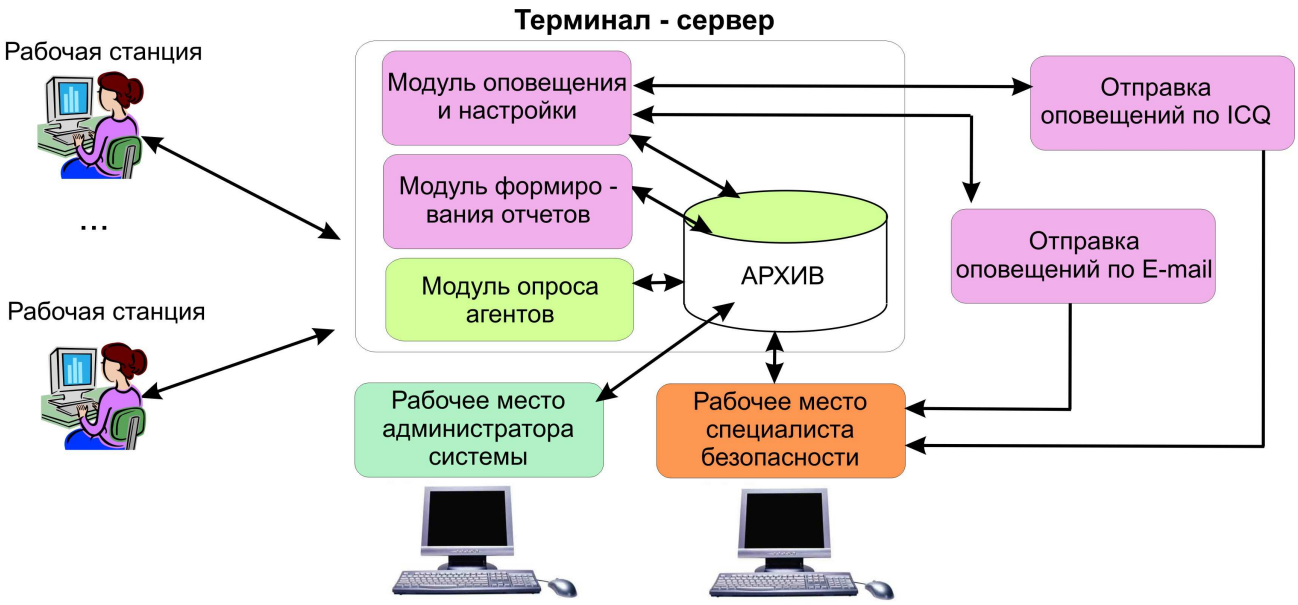


Рис. 1.1 – Структура LanAgent

Программа состоит из 3-х частей – сервер LanAgent, рабочее место специалиста безопасности и рабочее место администратора системы.

Серверная часть:
Устанавливается на терминал-сервер, к которому будут подключаться рабочие станции (тонкие клиенты). Она включает в себя модуль опроса агентов, который производит централизованный сбор информации (логов) с контролируемых рабочих станций; 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 для каких учетных записей 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.

Мониторинг действий пользователей по-умолчанию запускается автоматически при каждом старте Windows. 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 мониторинг вестись не будет до тех пор, пока от программы LanAgent View не поступит команда на его запуск.

1.4 Системные требования

Минимальные требования:

- Операционная система: Windows 2003/2008 Server.
- Процессор Pentium 4 с частотой не менее 1,7 GHz.
- 256 MB оперативной памяти.
- 100 MB свободного места на диске.

Рекомендуемые требования:

- Операционная система: Windows 2003/2008 Server.
- Процессор Pentium 4 с частотой 3 GHz и выше.
- 1 GB оперативной памяти.
- 15 GB свободного места на диске (зависит от количества пользователей и настроек программы).

Для работы консолей администрирования и просмотра данных необходимо, чтобы были открыты порты 3050 и 6589 TCP/IP на компьютерах, на которых данные консоли установлены.

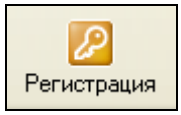
2 Регистрация LanAgent

2.1 Активация программы

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.

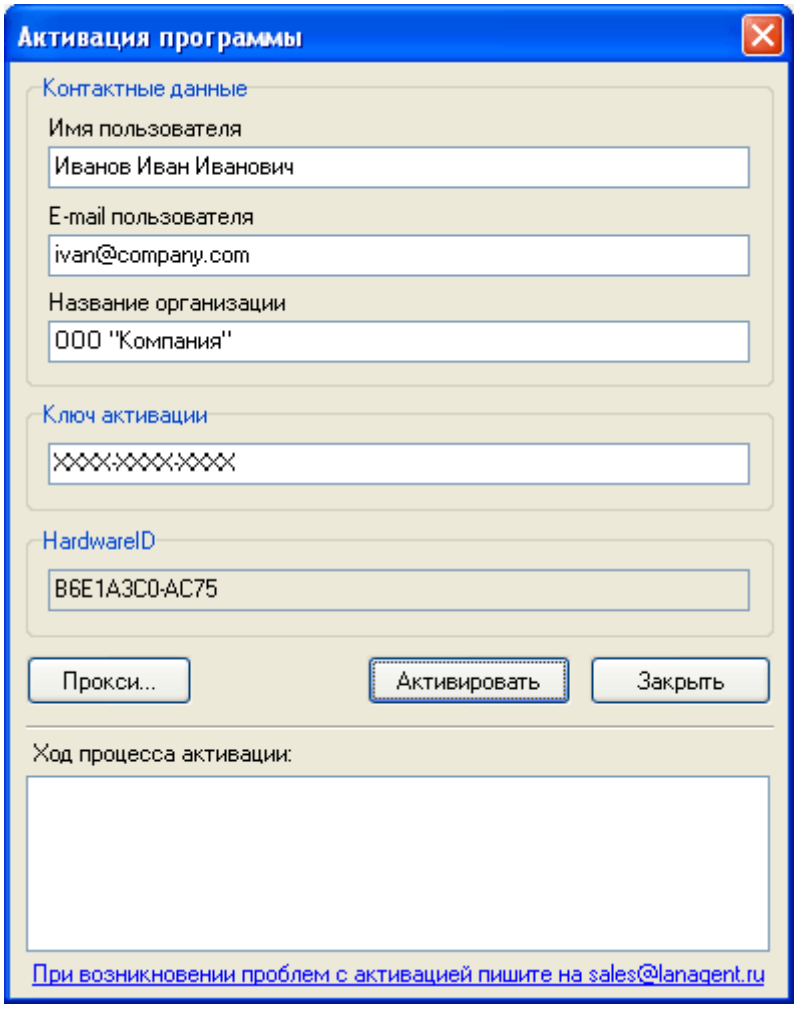


Рис. 2.1 - Активация программы

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**», а для перезапуска воспользуйтесь соответствующей кнопкой «**Перезапустить сервисы**» (подробней о «Менеджере сервисов» см. главу 4).

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

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 Server.msi». 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 Terminal Admin.exe**» и следовать инструкциям мастера установки.
При первом запуске **LanAgent Admin** предложит заполнить параметры к базе данных:

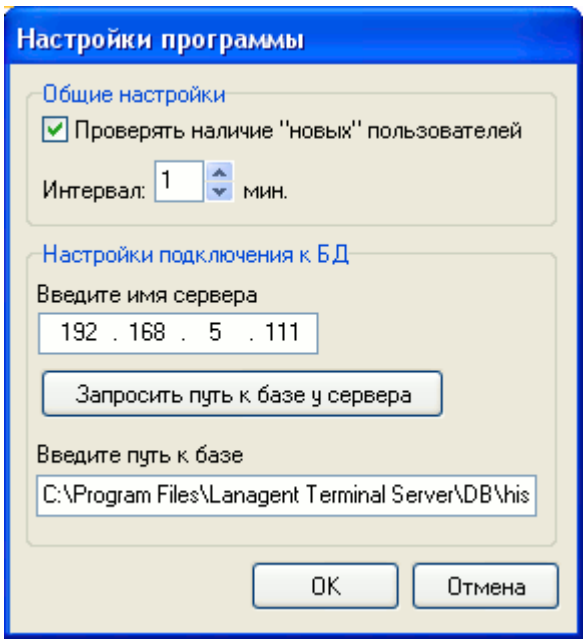


Рисунок 4 – Диалог соединения с базой

В этом диалоге требуется указать имя сервера, на котором установлена база, а также путь к файлу Hist.gdb
Внимание! Не надо открывать общего доступа к указанному файлу, путь указывается исключительно для сервера!

Для упрощения процедуры ввода пути к файлу базы, имеется кнопка «**Запросить путь к базе у сервера**». При ее нажатии путь будет получен автоматически. Для этого необходимо только чтобы на сервере был запущен сервис обмена с агентами.

Опция **Проверять наличие «новых» пользователей** позволяет на всех ОС кроме Win 2003 x64 при подключении к терминальному серверу пользователя, еще не добавленного в список мониторинга, выдавать в программе LA Admin уведомление об этом. Через окно такого уведомления есть возможность добавить пользователя в список.

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

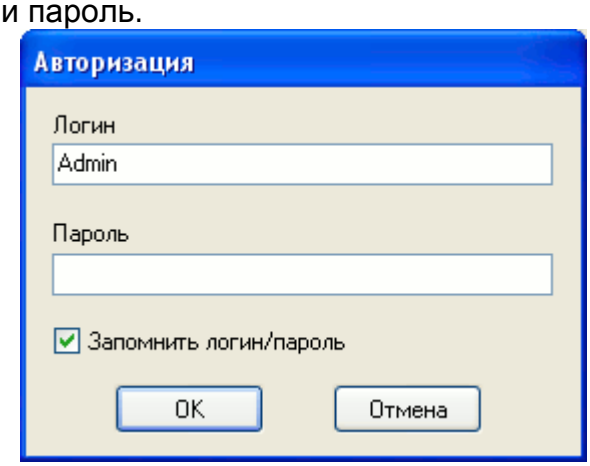


Рисунок 5 – Диалог авторизации

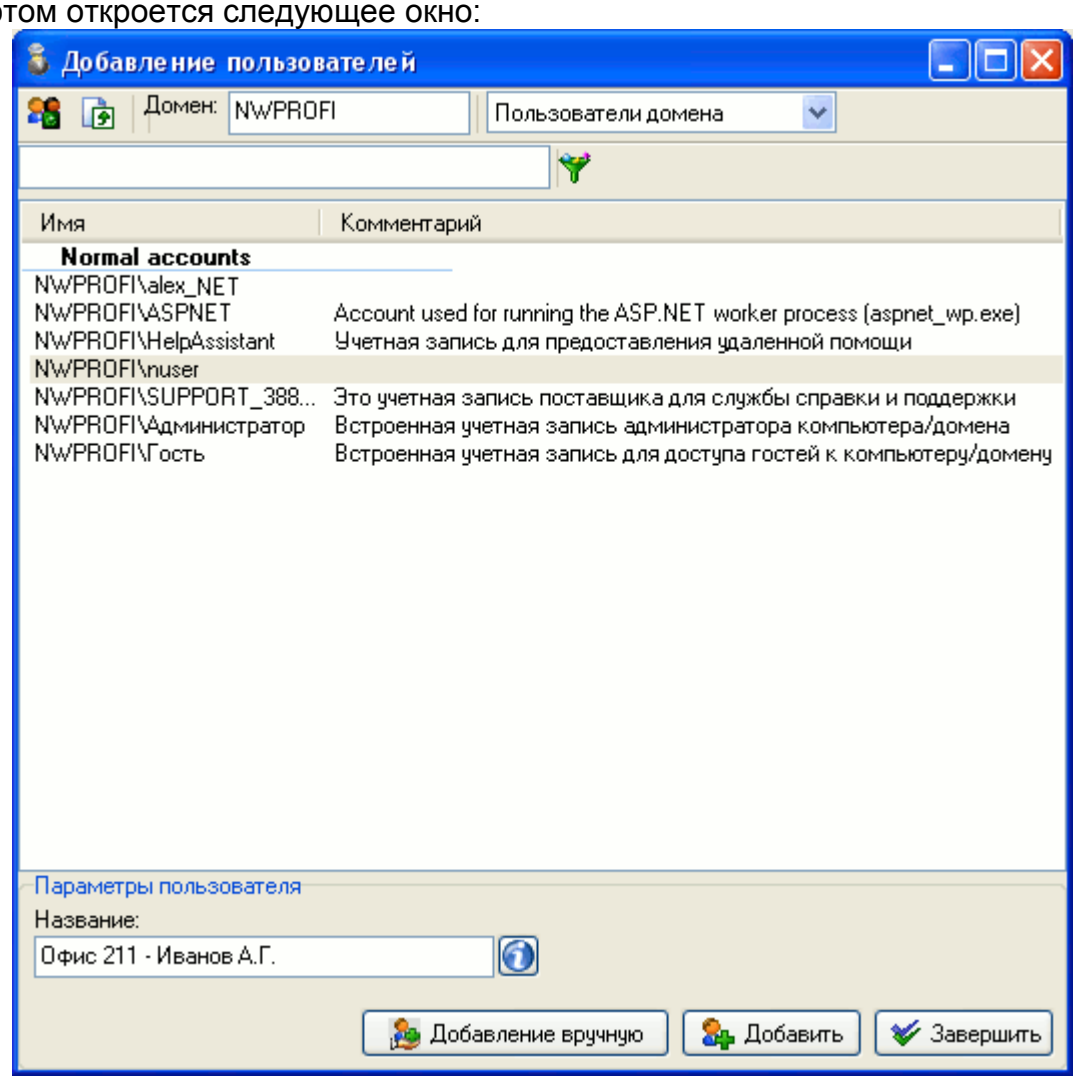
Внимание! Работать с LanAgent Admin может только пользователь с правами администратора!

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 Заполнение списка компьютеров для мониторинга

Для сбора данных с рабочих станций, подключаемых к терминал - серверу, необходимо внести учетные записи работающих на них пользователей 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...".

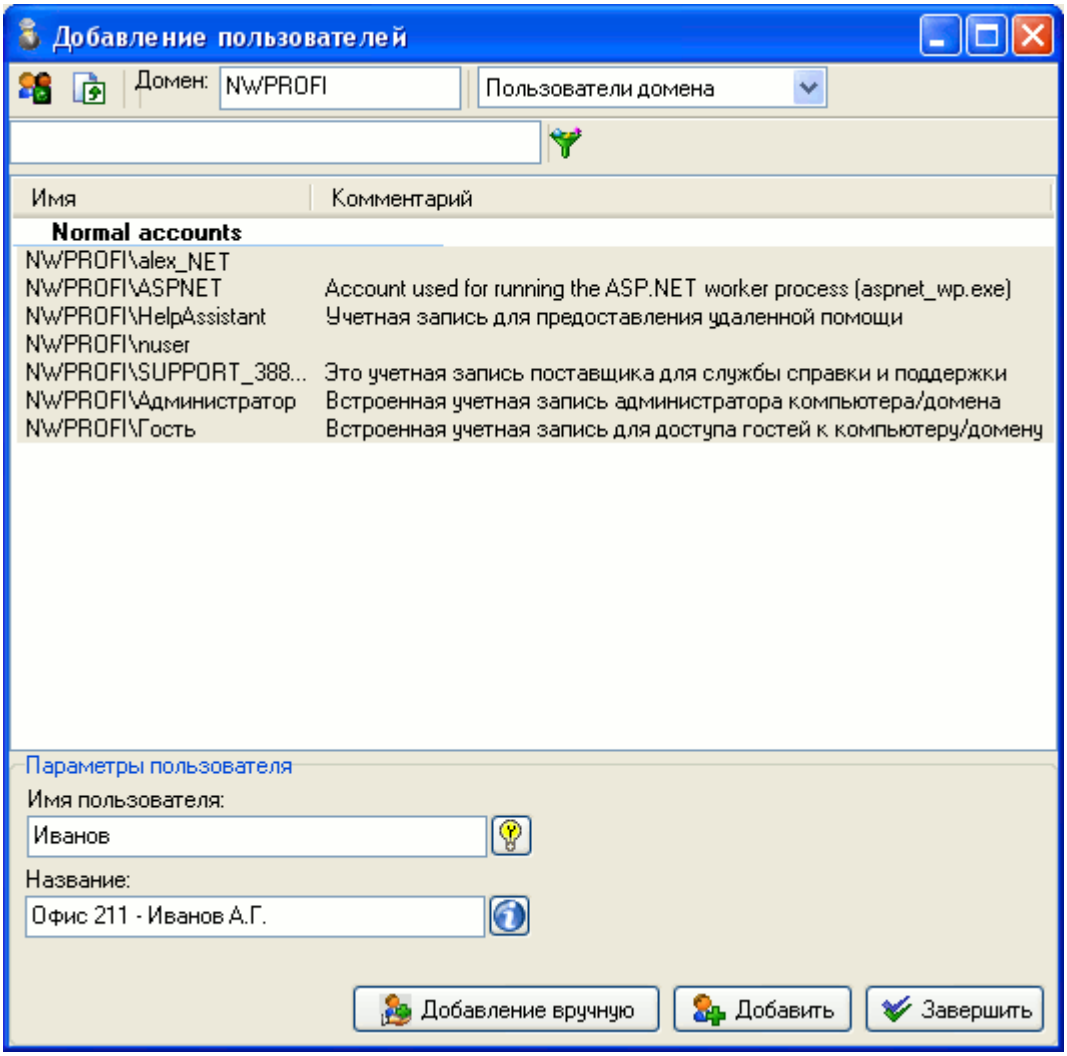
При этом откроется следующее окно:



В нем будут отображены все имеющиеся учетные записи пользователей. Выберите в списке нужную, заполните для нее поле «Название» и нажмите кнопку «Добавить».

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

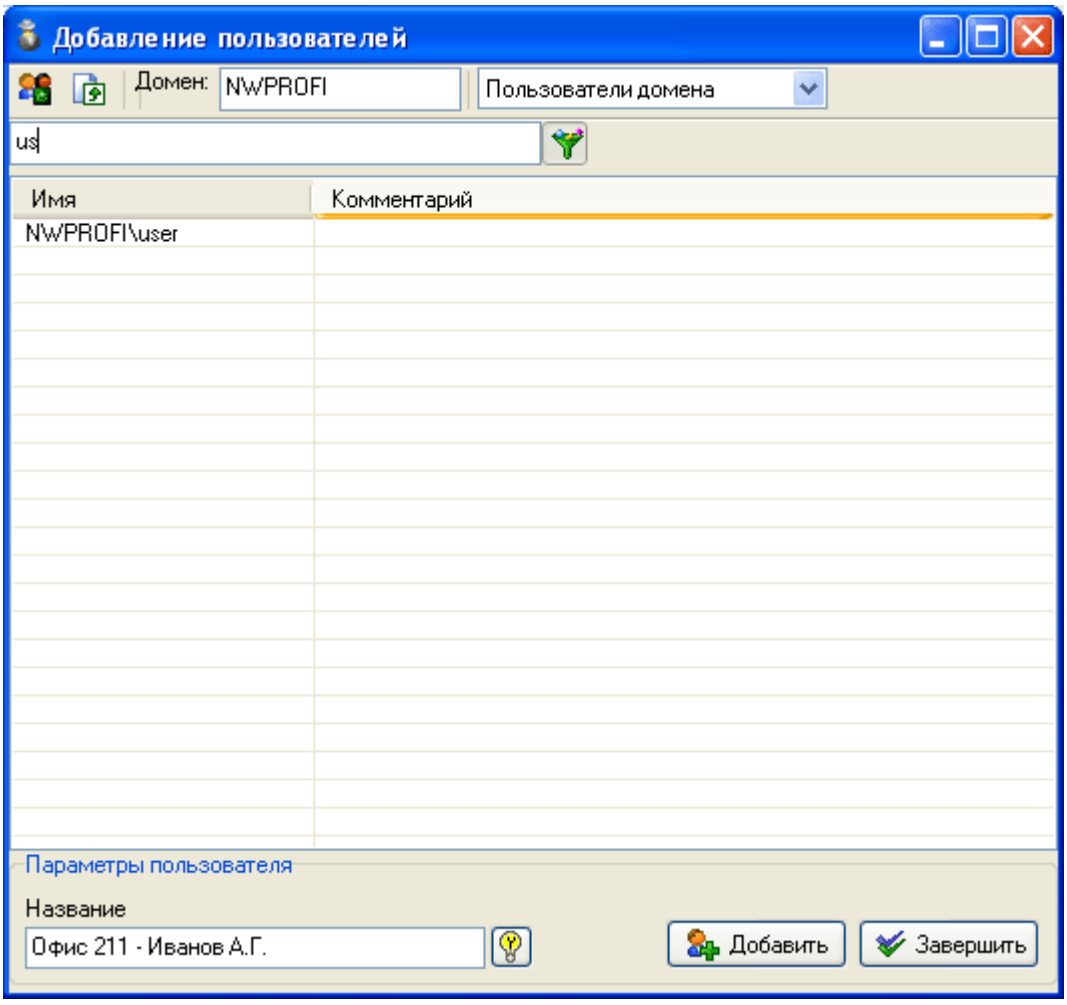
При необходимости самостоятельно задать имя пользователя, нажмите кнопку «Добавление вручную».



В появившемся дополнительном поле укажите имя нужной учетной записи (без имени домена или рабочей группы). При этом при нажатии кнопки «Добавить», имя учетной записи будет сформировано из имени домена, указанного в верхней части окна и имени пользователя. Т.е. для данного примера: NWPROFI\Иванов.

Для закрытия окна, нажмите кнопку «Завершить».

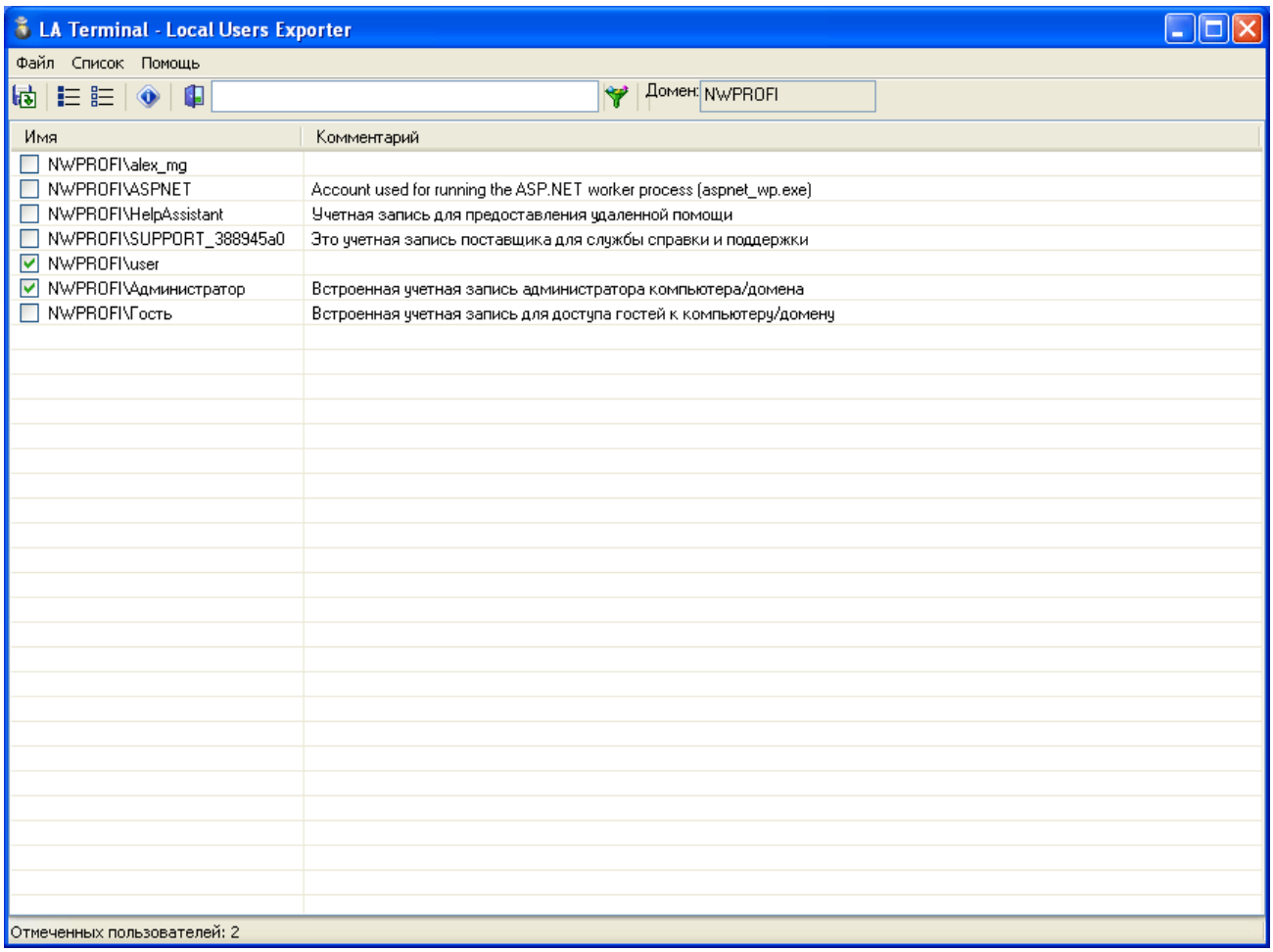
Для удобства поиска нужных учетных записей в списке, имеется возможность отфильтровать записи. Например так, как показано на рисунке ниже:



После успешного завершения, учетная запись будет добавлен в список мониторинга в указанную группу. В процессе работы вы сможете переместить ее 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.

3.4 Импорт пользователей из других доменов

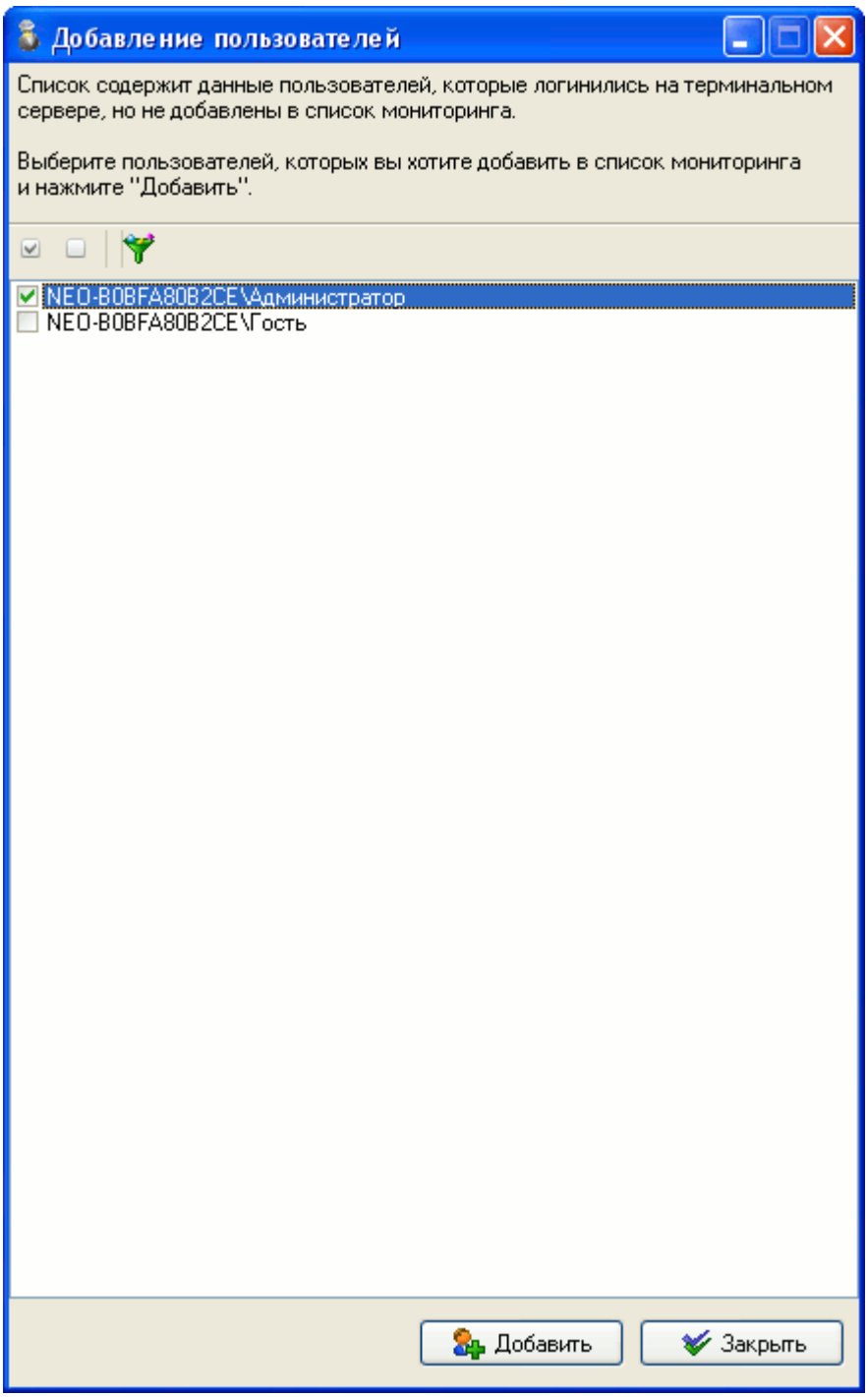
При помощи способа, описанного в пункте 3.3, можно произвести добавление в список мониторинга пользователей домена, в который включен компьютер, с которого запущена программа Terminal Admin. При необходимости внести в список пользователей других доменов, воспользуйтесь утилитой UsersExporter.exe, входящей в состав инсталляции Admin. Ее необходимо скопировать и запустить на сервере, входящем в домен, пользователей которого необходимо добавить.
Внешний вид данной утилиты представлен ниже:



Выберите из списка пользователей, которых хотите экспортировать, и нажмите кнопку «Экспортировать список в файл» (либо комбинацию клавиш Ctrl + S). Далее сохранить файл в любое место на диске, перенесите его на сервер, на котором установлена LanAgent Terminal Admin и произведите импорт пользователей.

3.5 Добавление «новых» пользователей

Данная опция позволяет внести в список мониторинга тех пользователей, которые подключались к терминальному серверу. Окно диалога имеет следующий вид:



Кнопка фильтра в панели инструментов, позволяет отображать/скрывать пользователей, которые уже были просмотрены.

3.6 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:

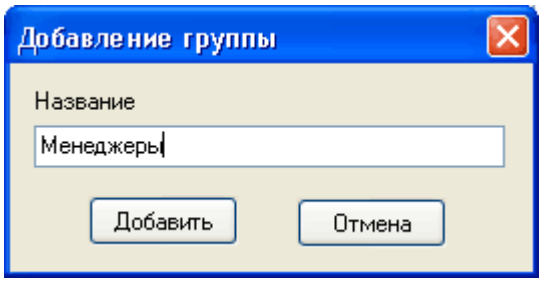
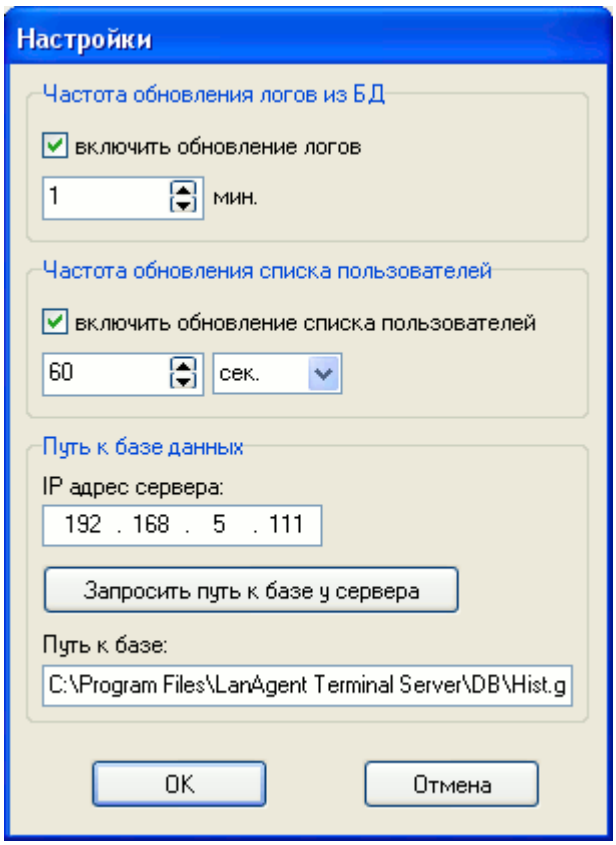


Рис. 3.5 – Добавление группы пользователей

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.

3.7 Установка LanAgent View

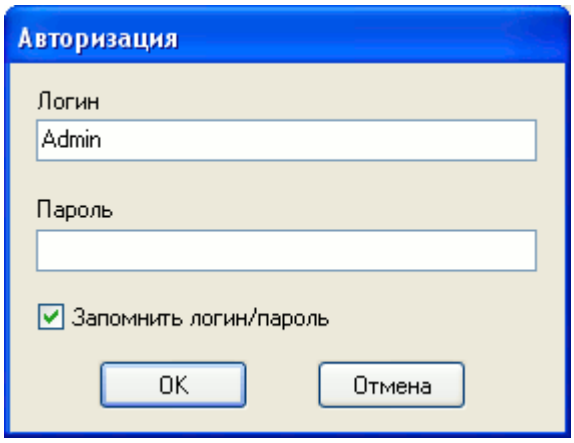
Данная программа устанавливается на рабочее место специалиста безопасности и позволяет просматривать собранные с контролируемых компьютеров данные, а также получать уведомления о нарушении политик безопасности.
Для начала процесса установки LanAgent View достаточно запустить установочный файл «**LanAgent Terminal Viewer.exe**» и следовать инструкциям мастера установки.
При первом запуске LanAgent View предложит заполнить параметры подключения к базе данных.



В этом диалоге требуется указать IP адрес сервера, на котором установлена база, а также путь к файлу HIST.gdb на сервере.
Внимание! Не надо открывать общего доступа к указанному файлу, путь указывается исключительно для сервера!

Для упрощения процедуры ввода пути к файлу базы, имеется кнопка «**Запросить путь к базе у сервера**». При ее нажатии путь будет получен автоматически. Для этого необходимо только чтобы на сервере был запущен сервис обмена с агентами.

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.