Network
PROFI

LanAgent

Владея информацией,
владеешь миром

Руководство пользователя

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 авторизированным 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 пользователя LanAgent предоставляет информацию об использовании программы LanAgent для контроля активности на компьютерах в локальной сети. Данное руководство включает следующие главы:

- **О продукте LanAgent**, общая информация о программном продукте LanAgent.
- **Регистрация LanAgent**, содержит информацию о лицензионном соглашении, а также описание процедуры активации программы.
- **Быстрый запуск**, краткое описание процесса установки и настройки LanAgent, достаточное для начала работы с ним.
- **Работа с LanAgent Server**, содержит описание серверной части программы и инструкцию по реализации ее функциональных возможностей.
- **Работа с LanAgent Admin**, содержит описание административной части программы и инструкцию по реализации ее функциональных возможностей.
- **Работа с LanAgent View**, содержит описание модуля специалиста безопасности и инструкцию по реализации его функциональных возможностей.
- **Работа с LanAgent Sheduler**, содержит описание планировщика отчетов и инструкцию по реализации его функциональных возможностей.
- **Удаление программы**, содержит описание процедуры деинсталляции компонентов программы.
- **Техническая поддержка**, координаты службы технической поддержки.
- **Типичные действия**, описание реализации наиболее типичных действий пользователей.

Содержание

1 О продукте LanAgent 6
1.1 Описание программы LanAgent 6
1.2 Для кого предназначена программа 7
1.3 Как работает программа LanAgent 7
1.4 Системные требования 9
2 Регистрация LanAgent 10
2.1 Активация программы 10
3 Быстрый запуск 12
3.1 Установка сервера LanAgent 12
3.1.1 Установка СУБД (системы управления базой данных) 12
3.1.2 Установка сервисов LanAgent 12
3.2 Установка модуля администратора LanAgent Admin 12
3.3 Заполнение списка пользователей для мониторинга 14
3.4 Импорт пользователей из других доменов 16
3.5 Добавление «новых» пользователей 17
3.6 Создание групп пользователей 18
3.7 Установка LanAgent View 19
4 Работа с LanAgent Server 22
5 Работа с LanAgent Admin 23
5.1 Панель инструментов 23
5.2 Закладка «Основные» 25
5.3 Закладка «Агенты» 26
5.3.1 Общие настройки 27
5.3.2 Настройки безопасности 35
5.4 Закладка «Контроль» 40
6 Работа с LanAgent View 44
6.1 Список пользователей для мониторинга 45
6.2 Окно просмотра истории активности контролируемых компьютеров 46
6.2.1 Клавиатура 47
6.2.2 Скриншоты 48
6.2.3 Программы 51
6.2.4 Буфер обмена 52
6.2.5 Файлы 53
6.2.6 Принтер 54
6.2.7 Установленные программы 56
6.2.8 Посещённые сайты 57
6.2.9 Компьютер 58
6.2.10 ICQ 59
6.2.11 Mail.ru Agent 60
6.2.12 Почта 61
6.2.13 Web почта 63
6.2.14 Выгрузка файлов 64
6.3 Панель инструментов 65
6.4 Поиск по логам 66
6.5 Активное оповещение 66
6.6 «Светофор» безопасности 68

6.7 Настройка LanAgent View 69
6.8 Формирование задач 70
6.9 Составление отчетов 71
6.9.1 Отчеты - выборки 71
6.9.2 Вычисляемые отчёты 75
7 Работа с LanAgent Sheduler (планировщиком отчетов) 80
8 Удаление программы 84
8.1 Удаление Серверной части, Admin, View, Sheduler 84
8.2 Удаление учетных записей из списка мониторинга 84
9 Техническая поддержка 85
9.1 Типичные действия 85
9.2 Часто задаваемые вопросы 86

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

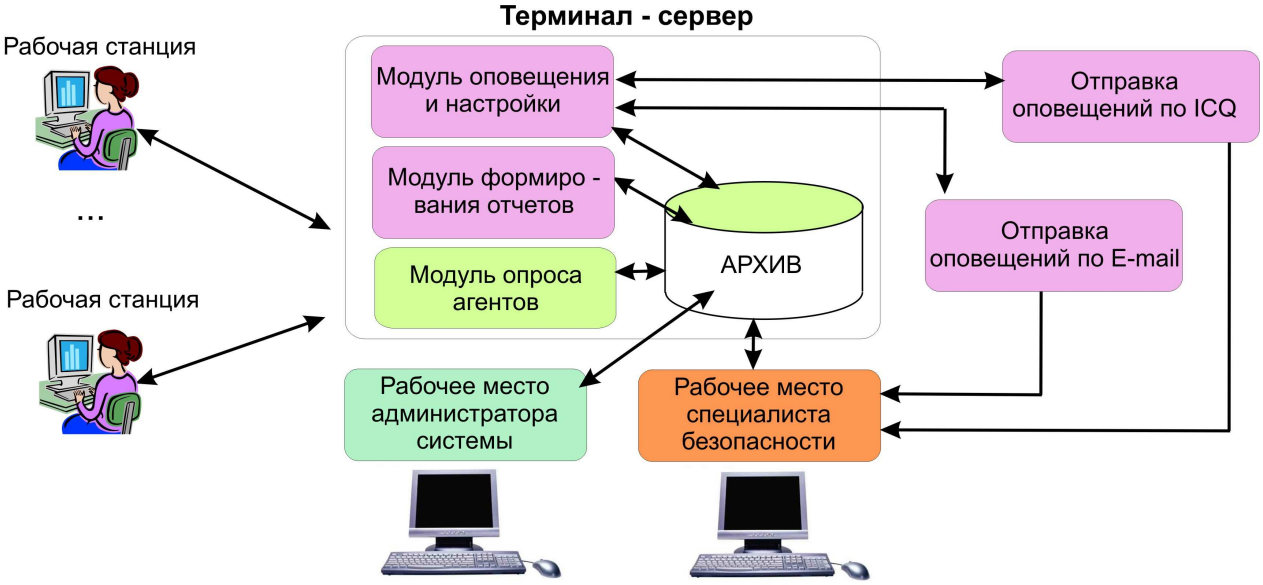


Рис. 1.1 – Структура LanAgent

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.

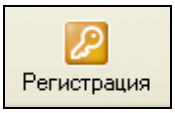
2 Регистрация LanAgent

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.

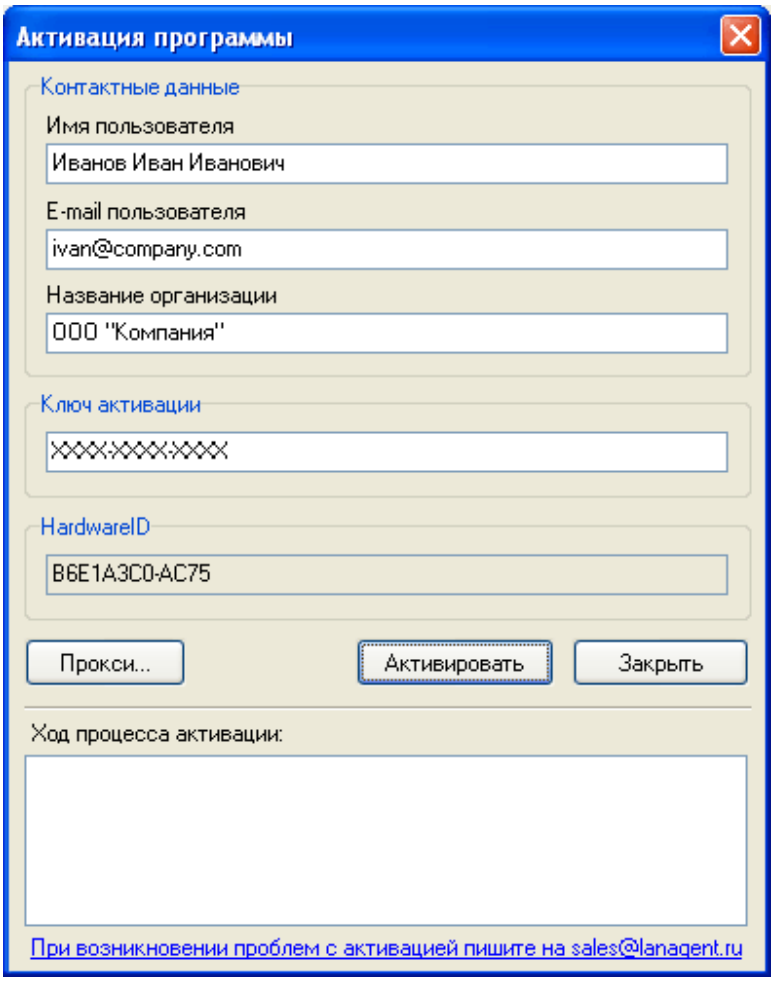


Рис. 2.1 - Активация программы

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 подключения к базе данных:

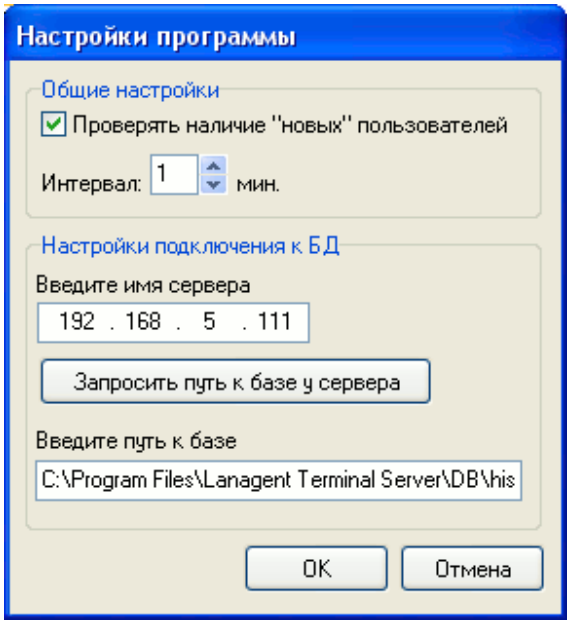


Рисунок 4 – Диалог соединения с базой

В этом диалоге требуется указать имя сервера, на котором установлена база, а также путь к файлу Hist.gdb
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.

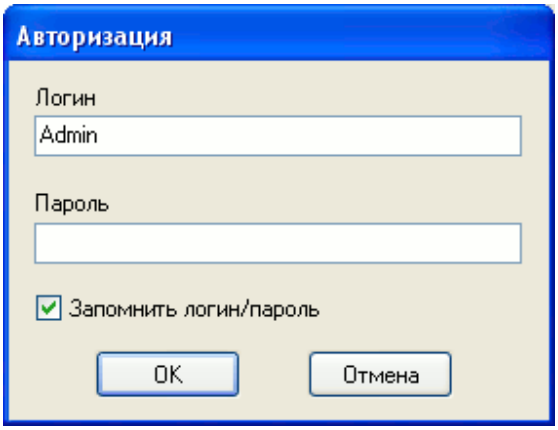


Рисунок 5 – Диалог авторизации

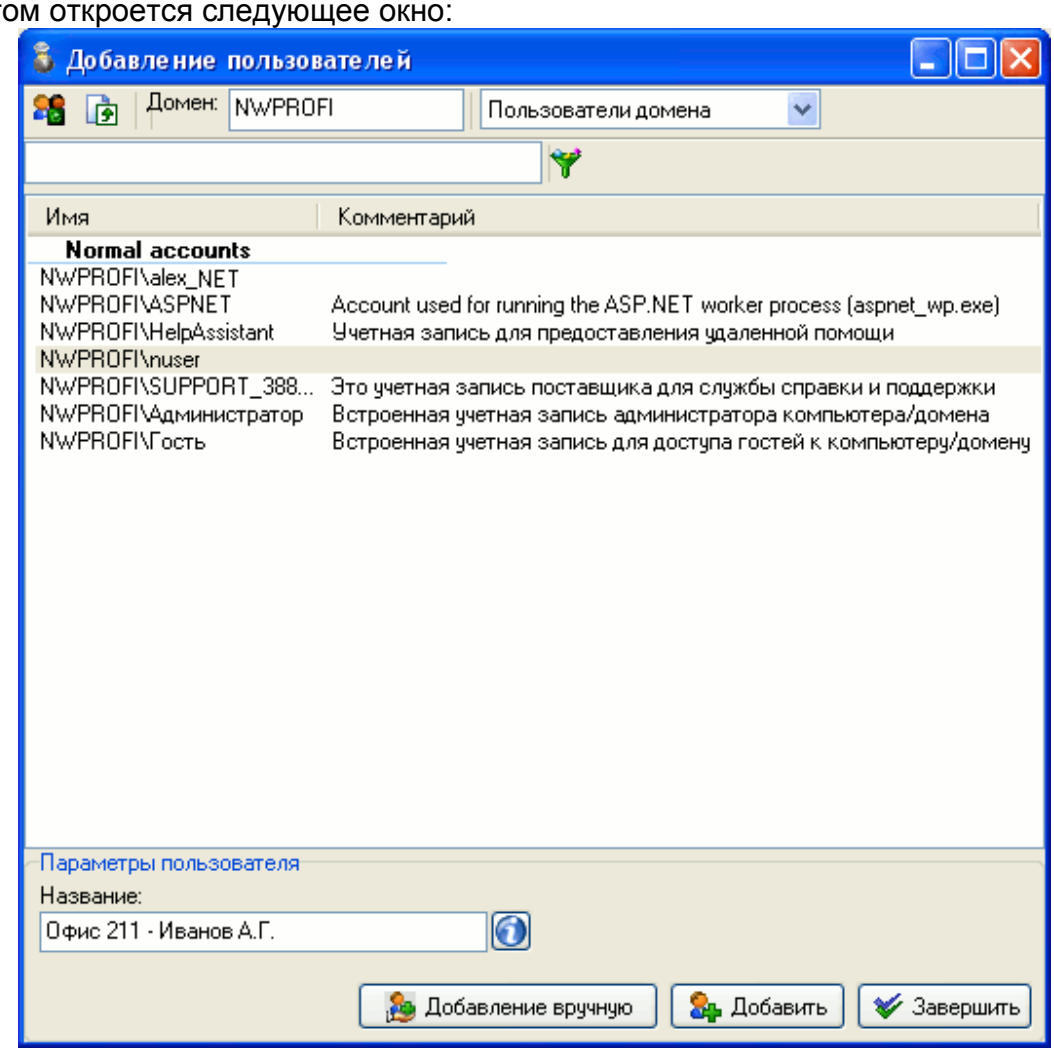
Внимание! Работать с LanAgent Admin может только пользователь с правами администратора!

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 пользователей 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...".

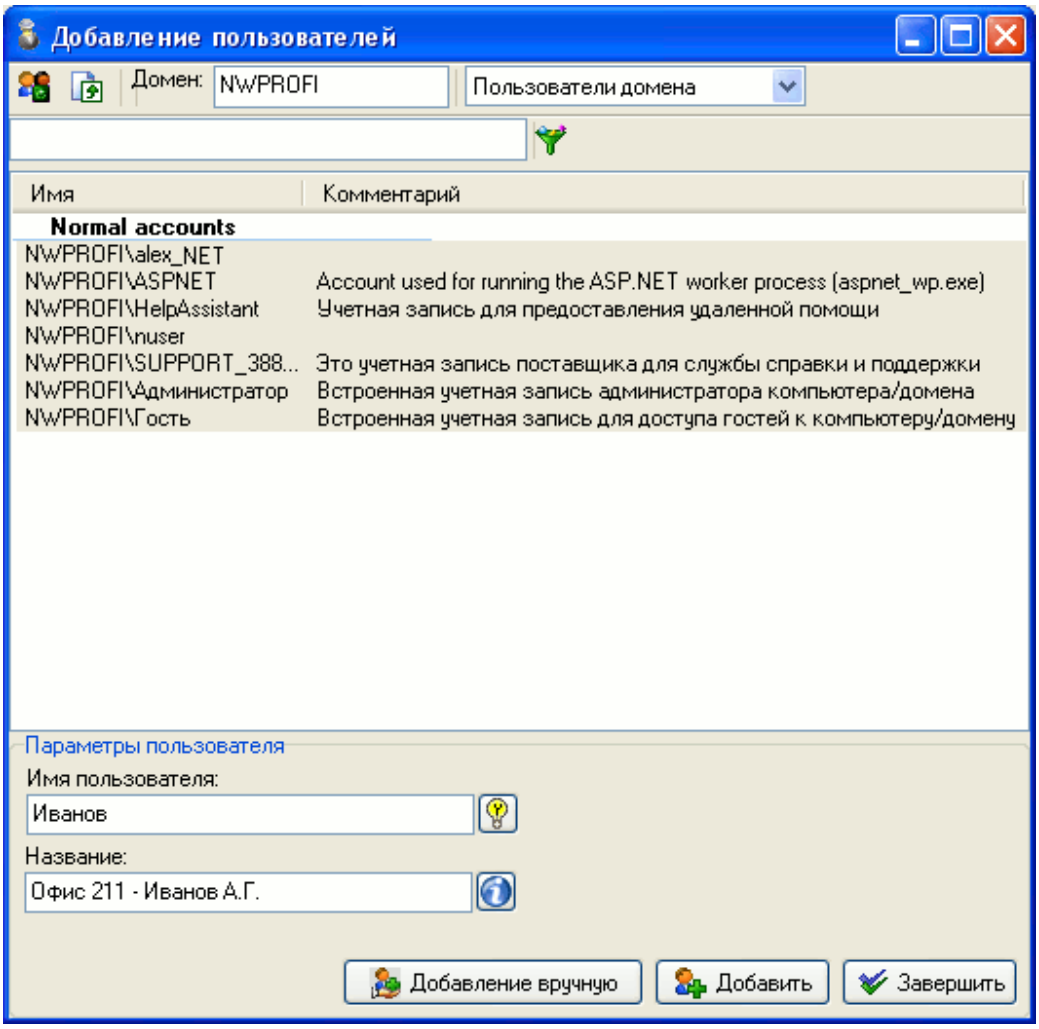
При этом откроется следующее окно:



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.

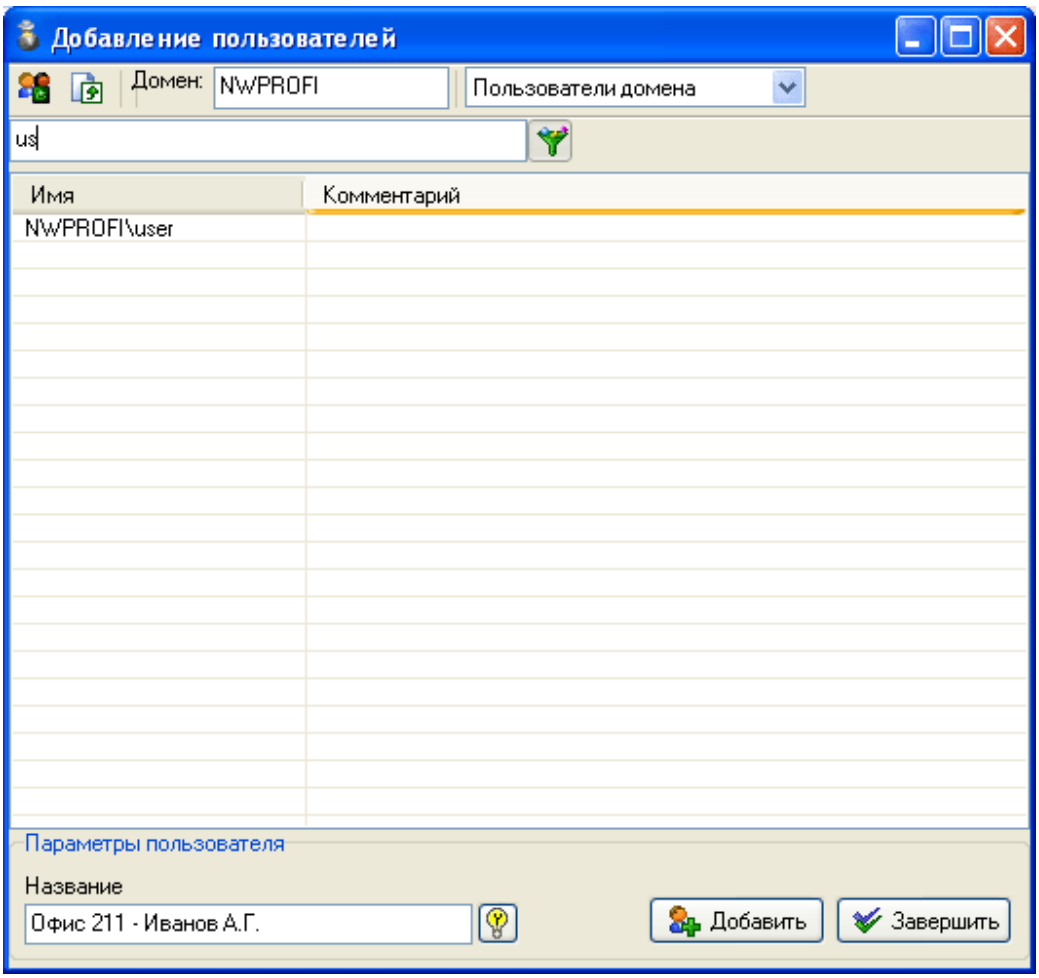
При необходимости самостоятельно задать имя пользователя, нажмите кнопку «Добавление вручную».



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».

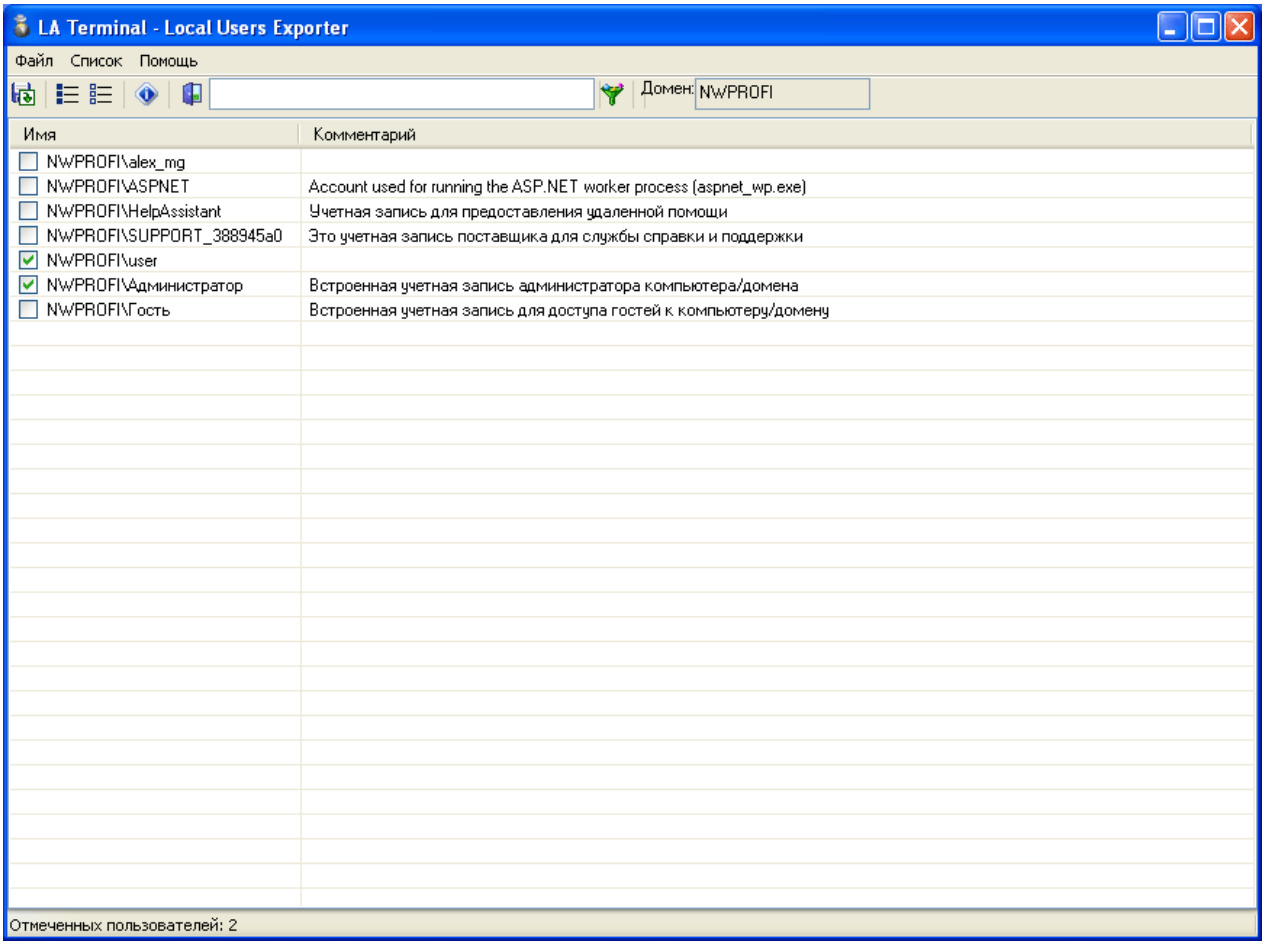
Для удобства поиска нужных учетных записей в списке, имеется возможность отфильтровать записи. Например так, как показано на рисунке ниже:



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

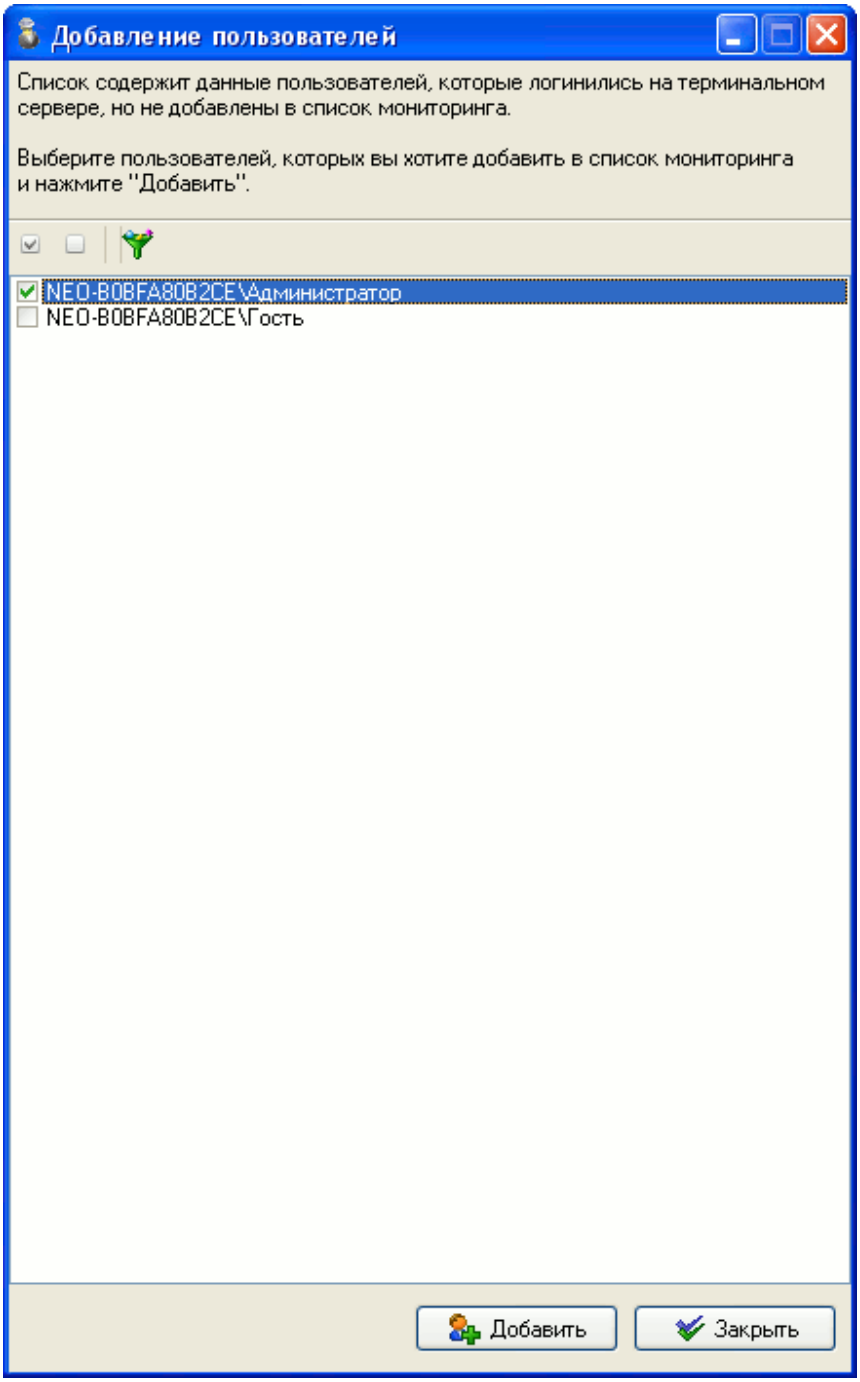
При помощи способа, описанного в пункте 3.3, можно произвести добавление в список мониторинга пользователей домена, в который включен компьютер, с которого запущена программа Terminal Admin. При необходимости внести в список пользователей других доменов, воспользуйтесь утилитой UsersExporter.exe, входящей 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:

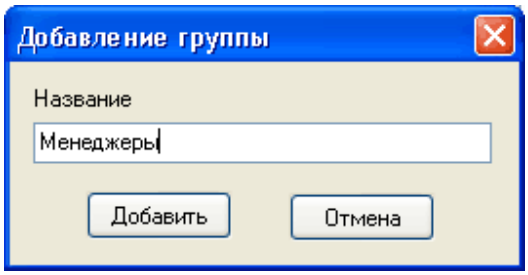
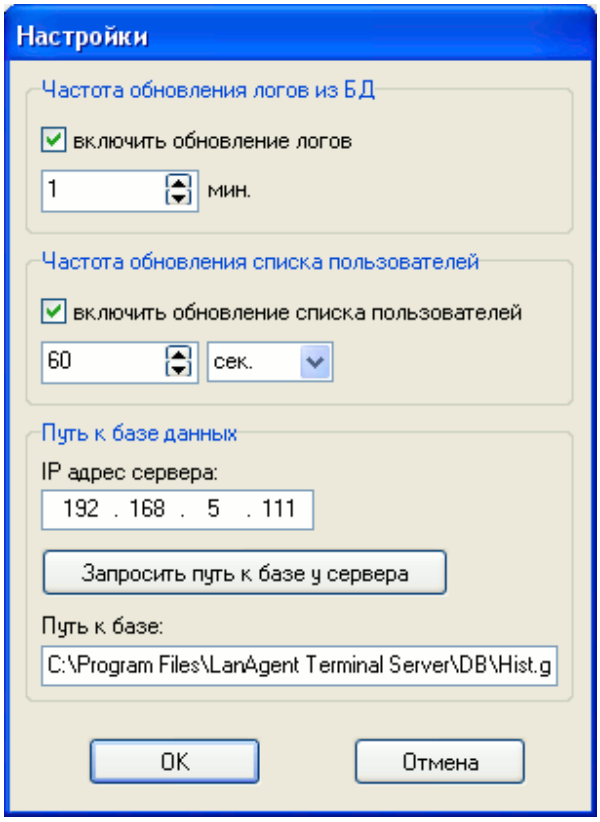


Рис. 3.5 – Добавление группы пользователей

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

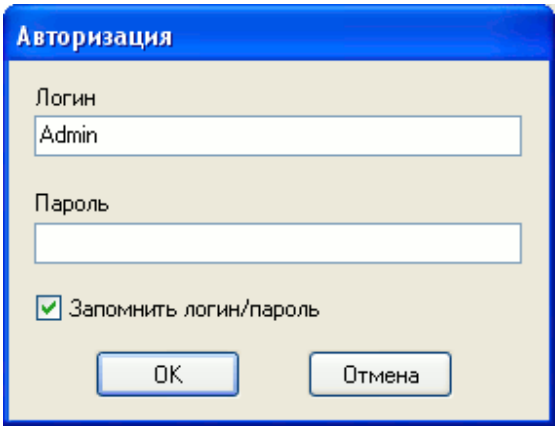
Данная программа устанавливается на рабочее место специалиста безопасности и позволяет просматривать собранные с контролируемых компьютеров данные, а также получать уведомления о нарушении политик безопасности.
Для начала процесса установки LanAgent View достаточно запустить установочный файл «**LanAgent 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 пункте 5.4 – «Закладка Контроль»)

4 Работа с LanAgent Server

Для управления сервисами **LanAgent Terminal** предусмотрена специальная утилита – Менеджер сервисов (**ServiceManager**):

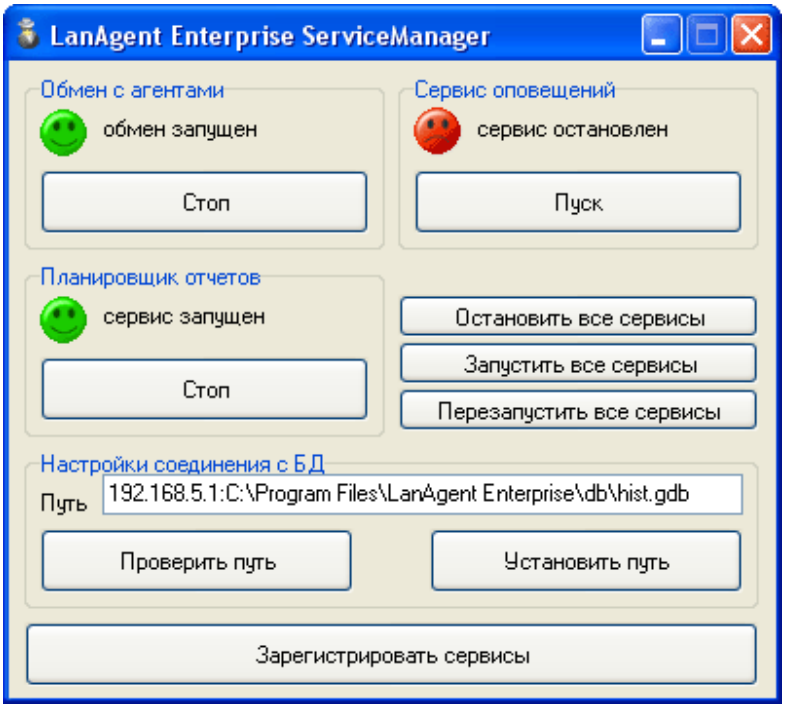
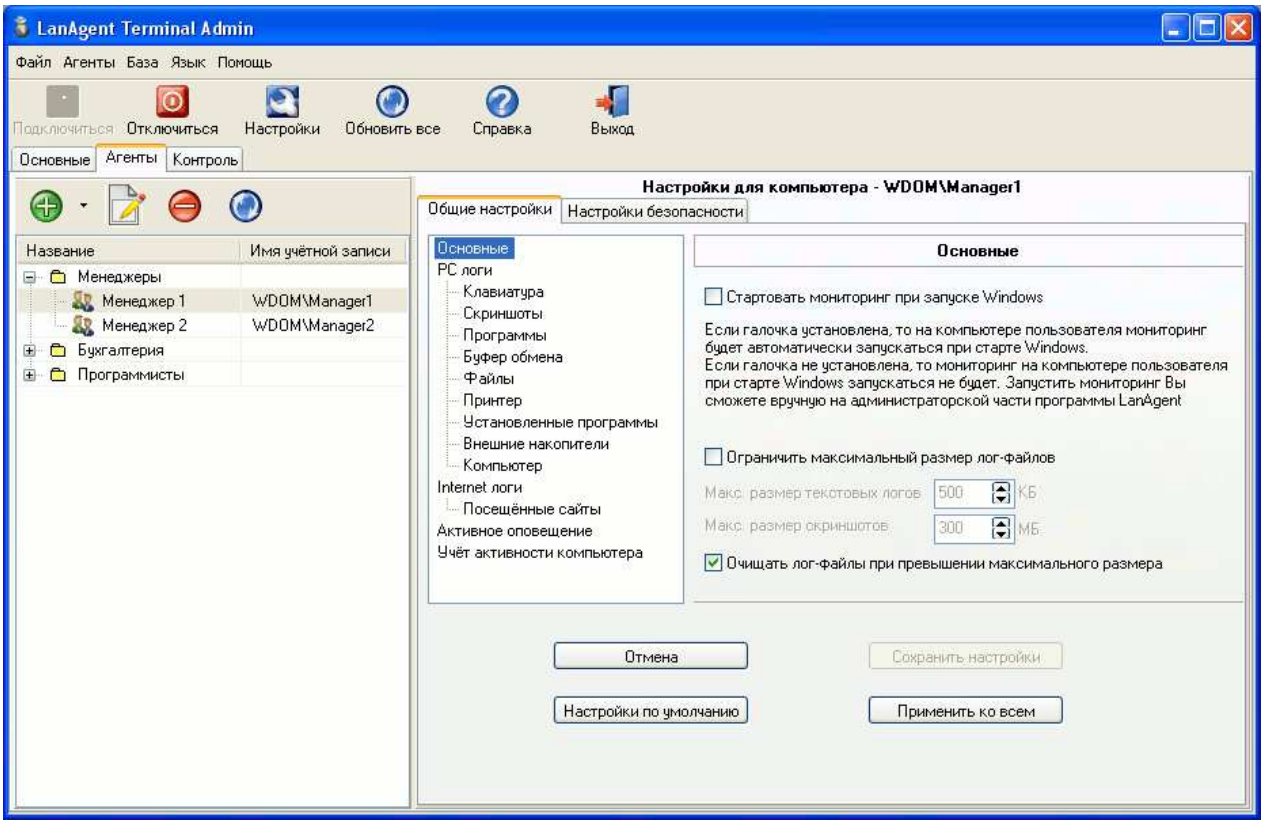


Рисунок 4.1 – Менеджер сервисов

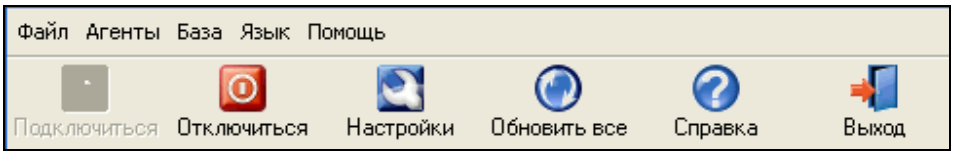
Ее первый запуск происходит сразу же после установки **LanAgent Server**.
Как видно из рисунка, для каждого установленного сервиса LanAgent отображается его статус («**сервис запущен**», «**сервис остановлен**») и имеется возможность остановить или запустить как какой-то конкретный сервис, так и все сервисы вместе.
Кнопка «**Перезапустить все сервисы**» производит соответственно перезапуск всех сервисов.
В нижней части окна имеется поле ввода пути к базе данных в формате «сервер:путь\к\базе\на\сервере». Если возникла необходимость в его изменении, то по окончанию корректировки нажмите кнопку «**Установить путь**». Для проверки правильности пути воспользуйтесь кнопкой «**Проверить путь**».
Кнопка «**Зарегистрировать сервисы**» используется для регистрации сервисов, после того как была проведена процедура регистрации и получен ключ активации в программе **LanAgent Admin**.

5 Работа с LanAgent Admin

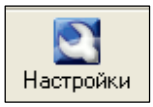


Как видно из рисунка, программа состоит из трех закладок («**Основные**», «**Агенты**», «**Контроль**»), на которых расположены соответствующие настройки и панели инструментов.

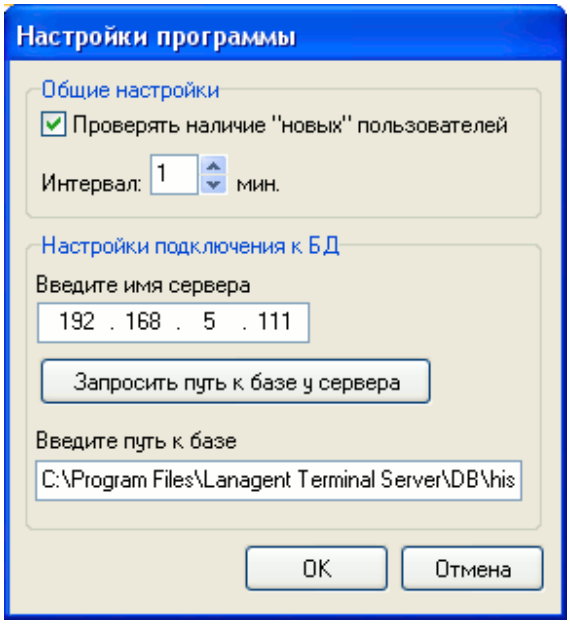
5.1 Панель инструментов



Назначение кнопок панели инструментов:



– вызывает диалог настройки подключения к базе данных:

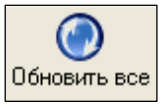


В этом диалоге требуется указать имя сервера, на котором установлена база, а также путь к файлу HIST.gdb

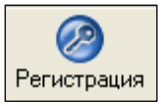
Внимание! Не надо открывать общего доступа к указанному файлу, путь указывается исключительно для сервера!

– если **LanAgent Admin** не подключена к базе данных, то при помощи данной кнопки будет произведено подключение.

– отсоединяет **LanAgent Admin** от базы данных.



– производит обновление всех списков.



– вызывает диалог регистрации программы. (подробней см. главу 2)

– запускает файл помощи. Также данный файл можно открыть через меню «Пуск»: «**Пуск->Программы->LanAgent->Справка по LanAgent**».

– закрывает программу.

Названные выше действия также продублированы в выпадающем меню.

5.2 Закладка «Основные»

Содержит системные и общесистемные настройки.

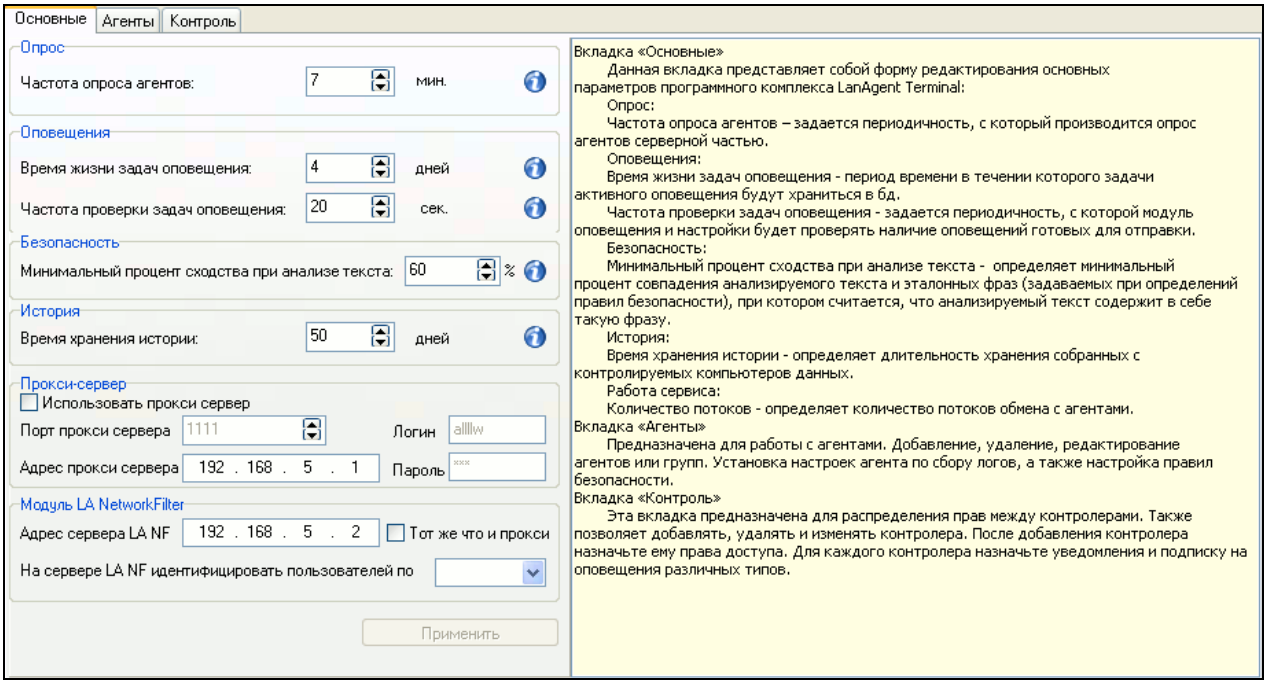


Рисунок 5.1 – Закладка «Основные» LanAgent Admin

Опрос:

Частота опроса агентов – задается периодичность, с который производится опрос агентов серверной частью.

Оповещения:

Время жизни задач оповещения – период времени в течении которого задачи активного оповещения будут храниться в базе данных.

Частота проверки задач оповещения – задается периодичность, с которой модуль оповещения и настройки LanAgent будет проверять наличие активных оповещений готовых для отправки специалисту безопасности.

Безопасность:

Минимальный процент сходства при анализе текста – определяет минимальный процент совпадения анализируемого текста и эталонных фраз (задаваемых при

определений правил безопасности), при котором считается, что анализируемый текст содержит в себе такую фразу.

История:

Время хранения истории – определяет длительность хранения собранных с контролируемых компьютеров данных.
Основное назначение такого ограничения – предотвратить излишнее разрастание базы данных из-за переизбытка устаревших данных.

Прокси-сервер:

Если выход в Интернет осуществляется через прокси сервер, то установите галочку «Использовать прокси сервер». Также необходимо задать IP адрес прокси, порт, логин и пароль для подключения.

Модуль LA NetworkFilter:

Данный пункт настроек становится активным в том случае, если дополнительно к LanAgent Terminal установлен модуль NetworkFilter, обеспечивающий контроль сетевого трафика. Необходимо указать IP адрес компьютера, на который установлена серверная часть NetworkFilter.

5.3 Закладка «Агенты»

На данной закладке имеется возможность добавления/удаления агентов в список мониторинга, а также возможность настройки агентов и безопасности.

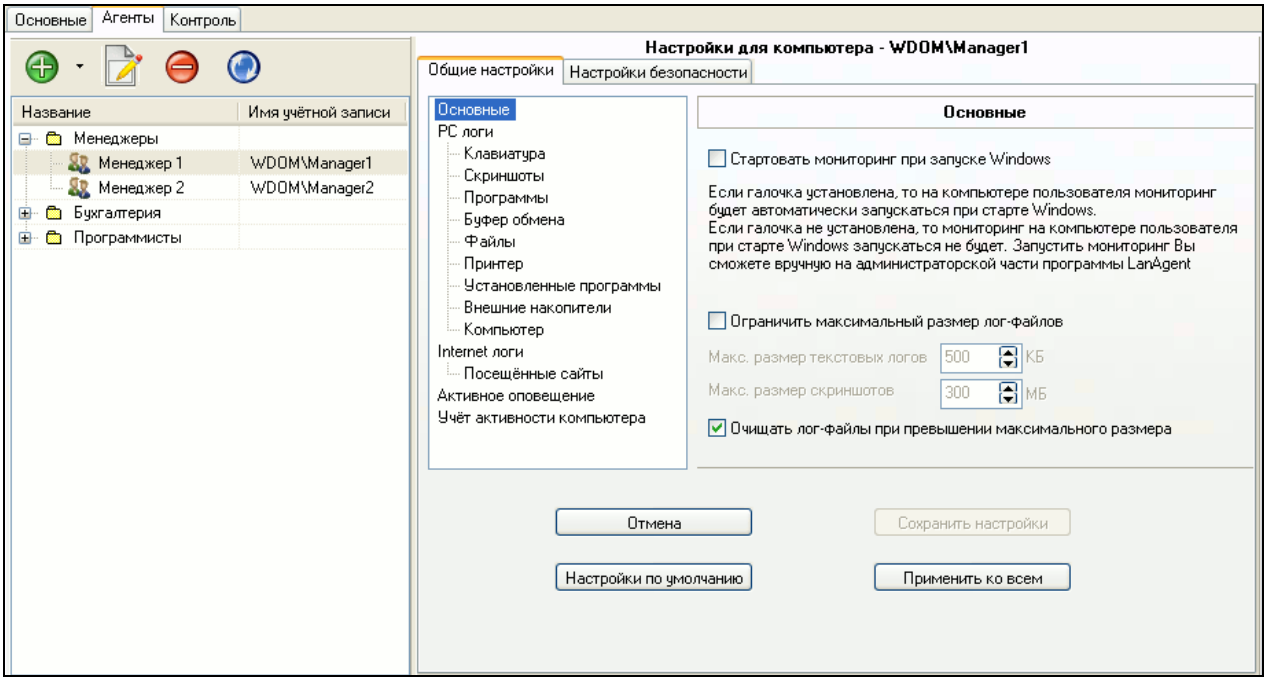


Рисунок 5.2 – Закладка «Агенты» LanAgent Admin

В левой части окна расположен список мониторинга.
Для добавления нового компьютера или группы в список, необходимо нажать кнопку Процесс добавления компьютеров подробно описан в пункте 3.3

5.3.1 Общие настройки

Настройки агента в целом, состоят из двух видов настроек: Общие настройки и Настройки безопасности.
Настройка агентов программы LanAgent производится удаленно из административной части программы. Для этого достаточно выбрать двойным кликом нужный компьютер из списка для мониторинга. Также имеется возможность групповой настройки агентов.

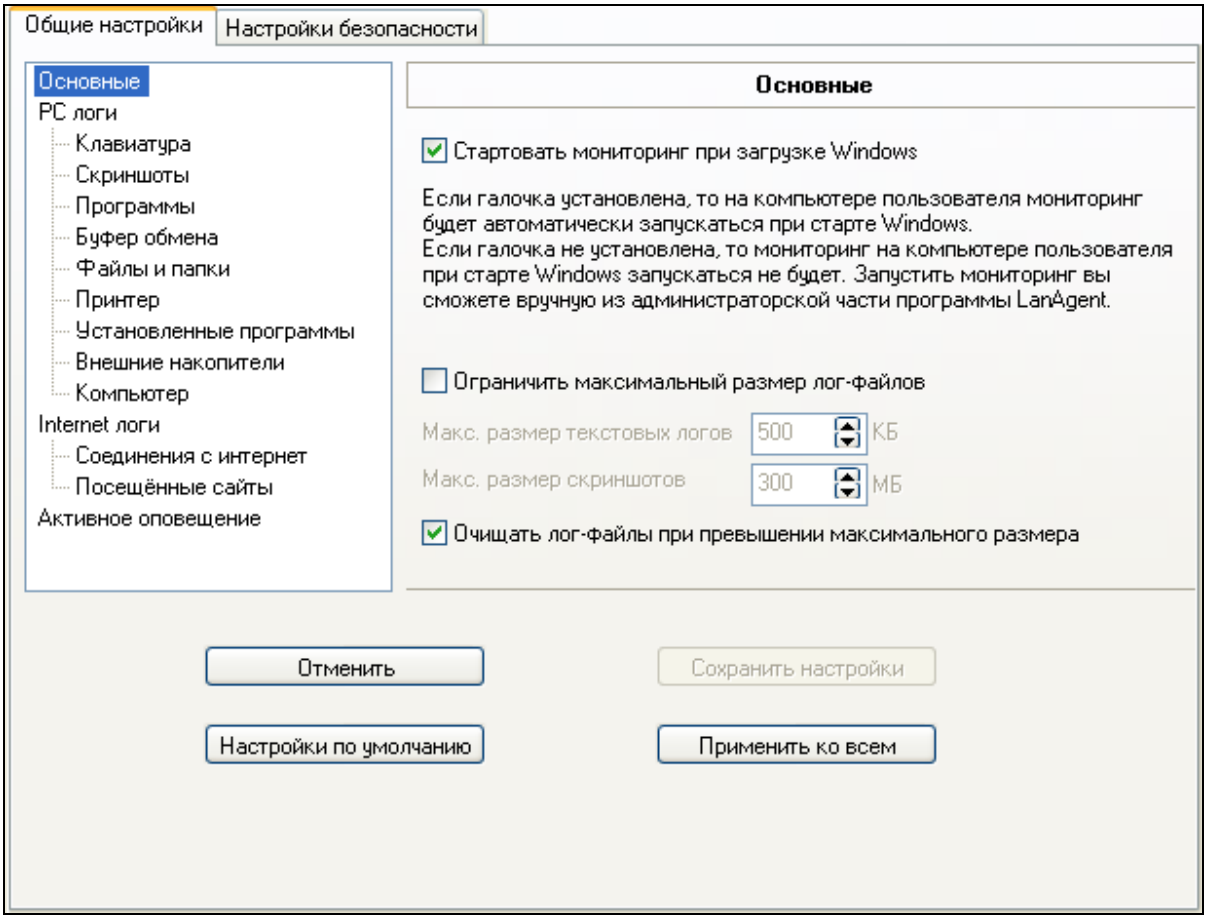


Рис. 5.3 – Главное окно настроек агентов

Можно изменять настройки для каждого пользователя отдельно или для всех сразу.

Чтобы изменить настройки для всех пользователей, нажмите кнопку "**Применить ко всем**".

Основные:

Стартовать мониторинг при загрузке Windows - установите эту галочку, если хотите чтобы на контролируемом компьютере мониторинг запускался автоматически при загрузке операционной системы.

Ограничивать максимальный размер лог-файлов - установите эту галочку, если хотите ввести ограничение на размер лог-файлов на компьютере пользователя.

PC логи - действия:

Запоминать нажатые клавиши - установите эту галочку, чтобы программа запоминала нажатия клавиш.

Делать скриншоты экрана - установите эту галочку, чтобы программа делала снимки экрана через определённый промежуток времени.

Запоминать запуск/закрытие программ - установите эту галочку, чтобы программа следила за запуском/закрытием программ.

Следить за буфером обмена - установите эту галочку, чтобы программа сохраняла содержимое буфера обмена, при условии, что в нём текстовая информация.

Запоминать изменения файлов и папок - установите эту галочку, чтобы программа отслеживала изменения в файловой системе.

Запоминать распечатанные документы - установите эту галочку, чтобы программа отслеживала отправленные на печать документы.

Запоминать установку/удаление программ - установите эту галочку, чтобы программа отслеживала установку и удаление программ.

Следить за подключением внешних носителей - установите эту галочку, чтобы программа отслеживала подключение и отключение внешних носителей информации.

Отслеживать включение/выключение компьютера - установите эту галочку, чтобы программа отслеживала включение/выключение компьютера.

Клавиатура:

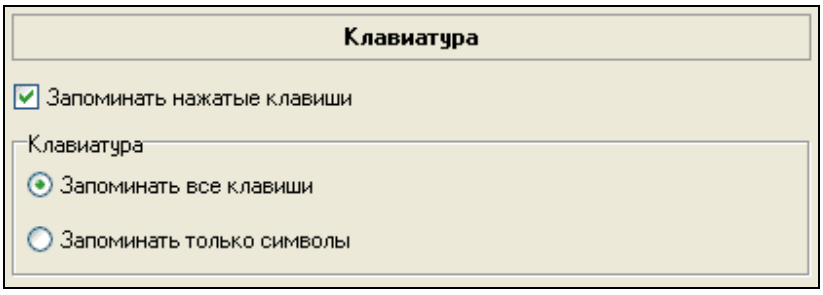


Рис. 5.4 – Настройки контроля клавиатуры агентов

Запоминать все клавиши - программа будет сохранять все нажатые клавиши, в том числе системные (такие как [Ctrl], [Shift] и т.д.).

Запоминать только символы - программа будет сохранять только символы, цифры и знаки препинания.

Скриншоты:

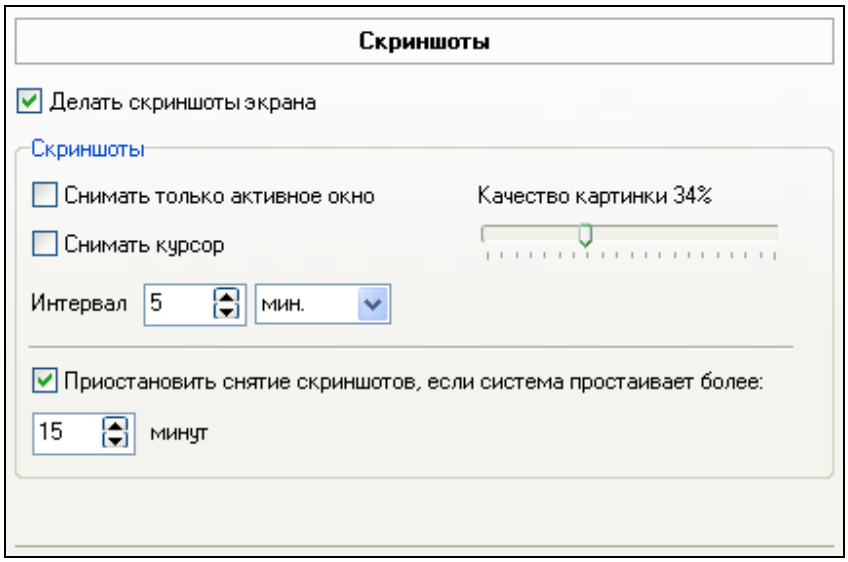


Рис. 5.5 – Настройки контроля снимков экранов

Снимать только активное окно - установите это галочку, если хотите, чтобы программа делала скриншот только активного в данный момент окна, иначе будет сделан скриншот всего экрана.

Снимать курсор - установите эту галочку, чтобы программа делала скриншот экрана вместе с курсором. Если галочка не установлена, то курсора на скриншоте не будет.

Качество картинки - с помощью указателя установите нужное вам качество скриншота. Чем выше качество, тем лучше будет скриншот и тем больше места он будет занимать на диске. Не рекомендуем устанавливать слишком высокое качество, так как скриншоты будут занимать очень много места на диске.

Интервал - установите интервал в минутах, через который будет делаться снимок экрана. Не рекомендуем устанавливать интервал слишком маленьким, так как скриншоты будут занимать очень много места на диске.

Приостановить снятие скриншотов, если система простаивает более - установите интервал в минутах. Если система простаивает более заданного времени, то скриншоты перестанут сниматься. Вследствие чего экономится дисковое пространство, и также скриншоты сделанные во время простоя системы не несут никакой полезной информации.

Программы:

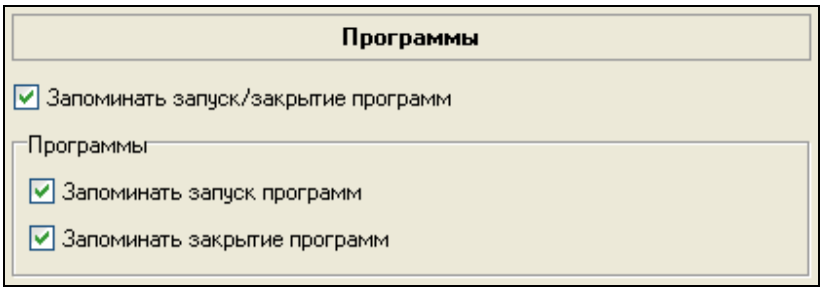


Рис. 5.6 – Настройки контроля запуска/закрытия программ

Запоминать запуск программ - установите эту галочку, чтобы программа следила за запуском программ.

Запоминать закрытие программ - установите эту галочку, чтобы программа следила за закрытием программ.

Буфер обмена:

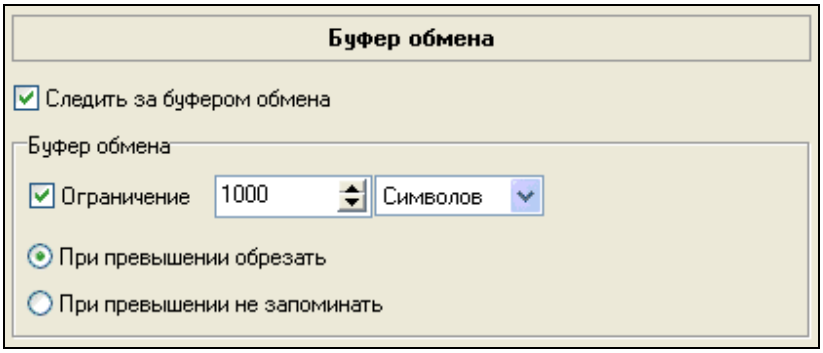


Рис. 5.7 – Настройки контроля буфера обмена

Ограничение - установите эту галочку, если хотите ограничить запоминаемый объём из буфера обмена. Установите максимальный объём (в Килобайтах или символах).

При превышении обрезать - при превышении установленного ограничения, будет сохранена только часть содержимого буфера обмена равная установленному ограничению, а остальная часть отброшена.

При превышении не запоминать - при превышении установленного ограничения, содержимое буфера обмена не будет сохранено.

Файлы и папки:

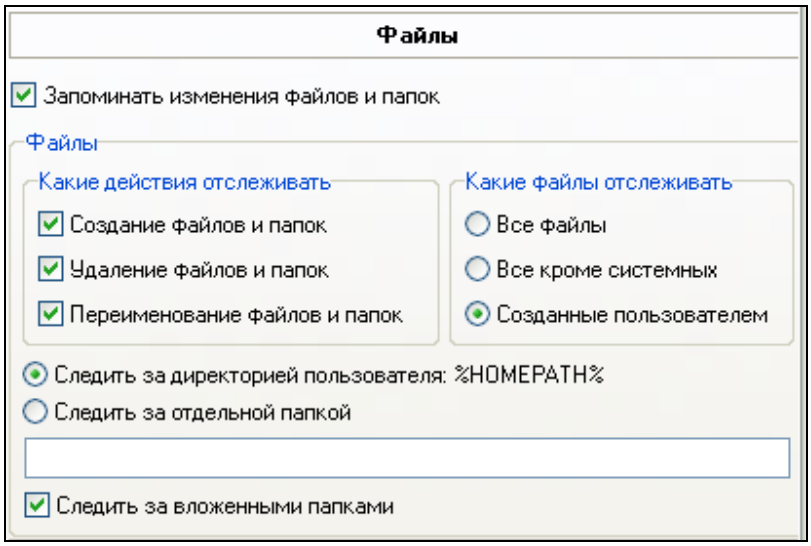


Рис. 5.8 – Настройки ведения мониторинга файловой системы

Создание файлов и папок - установите эту галочку, если хотите отслеживать создание файлов и папок.

Удаление файлов и папок - установите эту галочку, если хотите отслеживать удаление файлов и папок.

Переименование файлов и папок - установите эту галочку, если хотите отслеживать переименование файлов и папок.

Все файлы - будет отслеживаться создание, удаление и переименование абсолютно всех файлов: системных, скрытых. Не рекомендуется устанавливать эту опцию, так как операционная система постоянно создаёт и удалят временные файлы, которые не несут для вас никакой информации.

Все кроме системных - будет отслеживаться создание, удаление и переименование всех файлов кроме тех, которые создаются системой. То есть будут отслеживаться файлы, которые создал пользователь, а также файлы, создаваемые различными программами для своих нужд.

Созданные пользователем - будет отслеживаться создание, удаление и переименование только тех файлов и папок, которыми манипулирует пользователь. (Рекомендуется).

Следить за директорией пользователя: - наблюдение будет производится за файлами, которые находятся в «домашней» директории пользователя. Т.е. в рамках одного пользователя.

Следить за отдельной папкой - наблюдение будет производится только за теми файлами, которые расположены в указанной папке.

Следить за вложенными папками - установите эту галочку, если хотите отслеживать изменения во вложенных папках.

Компьютер:

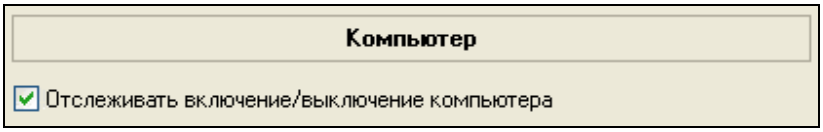


Рис. 5.9 – Настройки статистики включения/выключения компьютера

Отслеживать включение/выключение компьютера - установите эту галочку, чтобы программа отслеживала включение/выключение компьютера.

Internet логи - действия:

Запоминать посещённые сайты - установите эту галочку, чтобы программа запоминала посещённые веб-сайты.

Посещённые сайты:

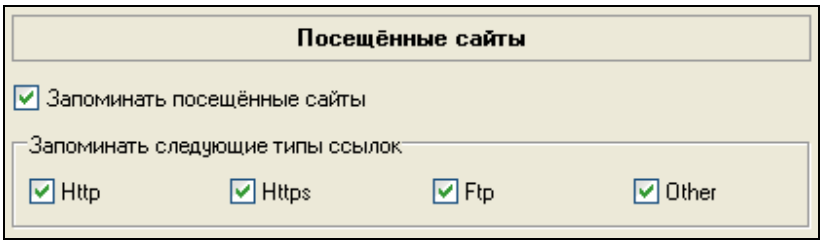


Рис. 5.11 – Настройки контроля посещенных сайтов

Запоминать следующие типы ссылок - выберите типы протоколов для которых нужно запоминать ссылки.

Принтер:

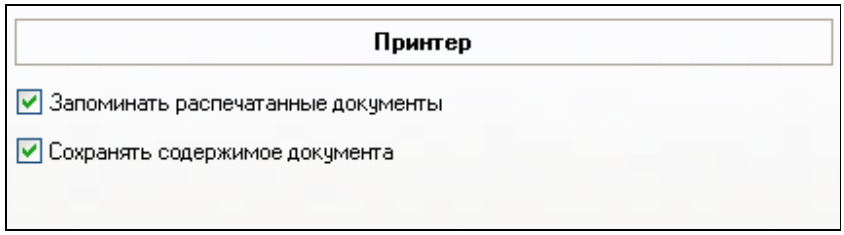


Рис. 5.12 – Настройки контроля принтеров

Запоминать распечатанные документы - установите эту галочку, чтобы программа отслеживала отправленные на печать документы.

Сохранять содержимое документа - установите эту галочку, чтобы программа сохраняла содержимое отправленного на печать документа.

Установленные программы:

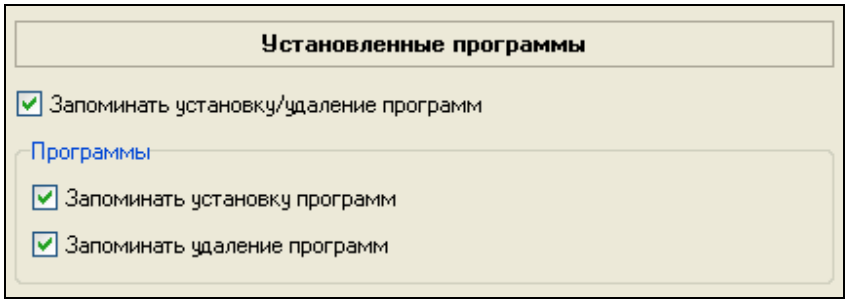


Рис. 5.13 – Настройки контроля установленных программ

Запоминать установку программ - установите эту галочку, чтобы программа следила за установкой новых программ на компьютер пользователя.

Запоминать удаление программ - установите эту галочку, чтобы программа следила за удалением программ с компьютера пользователя.

Внешние накопители:

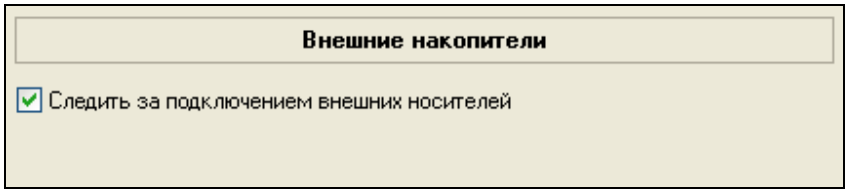


Рис. 5.14 – Настройки контроля подключения носителей

Следить за подключением внешних носителей - установите эту галочку, чтобы программа отслеживала подключение и отключение внешних носителей информации.

Активное оповещение:

Данные настройки определяют обратную связь от агента. В случае если активное оповещение включено, агент будет информировать о возникновении

соответствующих событий (подкл/откл носителя информации и установка/удаление программ) сразу после их возникновения, не дожидаясь команды обновления логов.

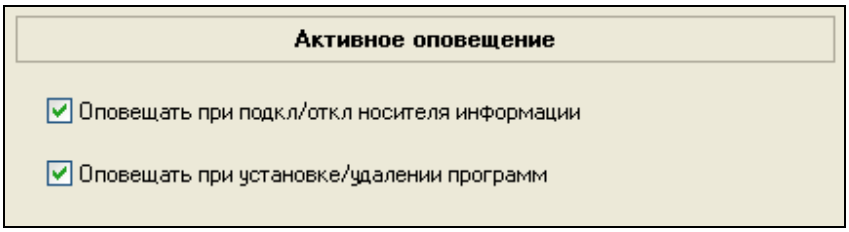


Рис. 5.15 – Настройки активного оповещения

Оповещать при подкл/откл носителя информации - если данный пункт включен, то при подключении или отключении носителя информации на контролируемом компьютере, агент выдаст административной части соответствующее сообщение, которое отобразится в окне активных оповещений.

Оповещать при установке/удалении программ - если данный пункт включен, то при установке или удалении программ на контролируемом компьютере, агент выдаст административной части соответствующее сообщение, которое отобразится в окне активных оповещений.

После изменения настроек нажмите кнопку **"Сохранить настройки",** если хотите сохранить сделанные изменения, или нажмите кнопку **"Отменить"**, если хотите вернуть старые настройки. Чтобы установить стандартные настройки нажмите кнопку "Настройки по умолчанию".

5.3.2 Настройки безопасности

На данной закладке имеется возможность редактирования списка правил безопасности. Этот список призван облегчить процедуру контроля за соблюдением политик безопасности и использования компьютерной техники работниками организации.

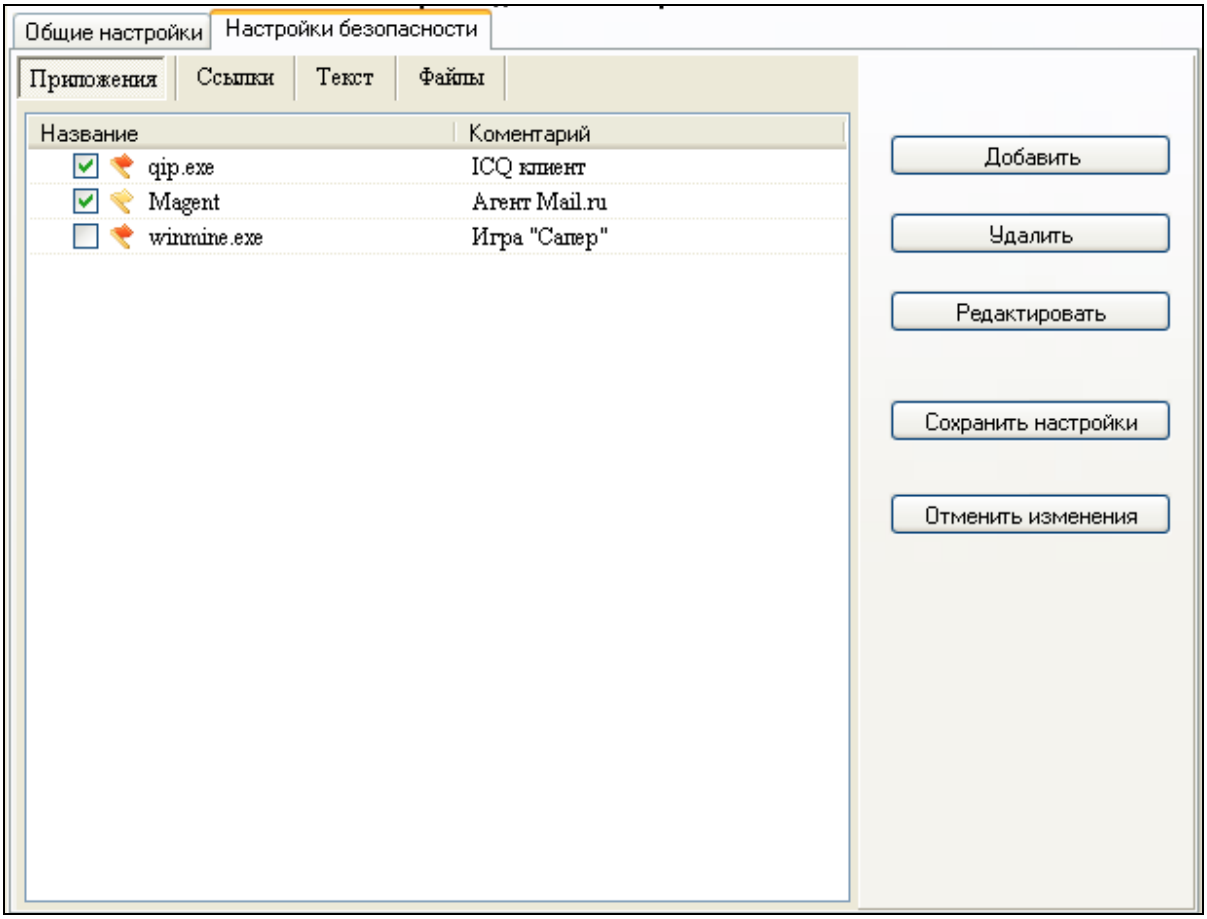


Рис. 5.16 – Список правил безопасности

Настройки агента в целом, состоят из двух видов настроек: Общие настройки и Настройки безопасности. Настройки безопасности, в свою очередь, разбиты на 4 категории: Приложения, Ссылки, Текст, Файлы.

На закладке **«Приложения»**, заполняется список программ, запуск которых будет считаться нарушением правил безопасности (программы идентифицируются по имени запускающего файла).

На закладке **«Ссылки»** определяются все web-адреса, посещение которых считается нарушением безопасности (идентификация производится простым поиском указанных слов в строке адреса).

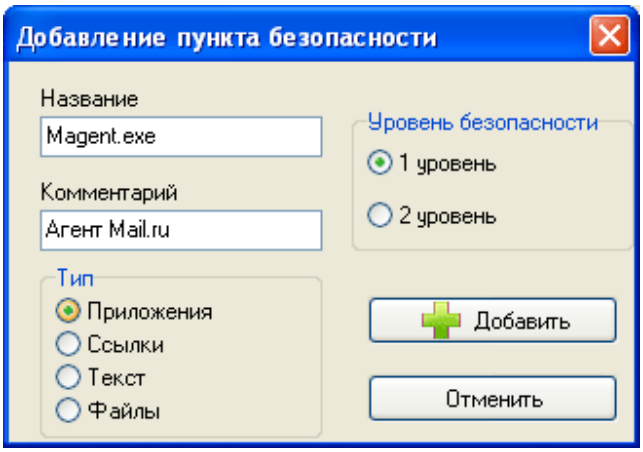
На закладке **«Файлы»** указываются непосредственно имена файлов, открытие/закрытие которых будет считаться нарушением правил.

Закладка **«Текст»**: здесь вводятся слова или фразы, которые будут искаться в набираемом пользователем на клавиатуре тексте, в содержимом буфера обмена, а также в заголовках окон программ и web-страниц.

Для каждого конкретного компьютера список применяемых именно для него правил помечается галочкой. Для добавления/удаления применяемых для компьютера правил, необходимо установить/снять соответствующие галочки и нажать кнопку **"Сохранить настройки"**. Для отмены изменений - нажать кнопку **"Отменить изменения"**.

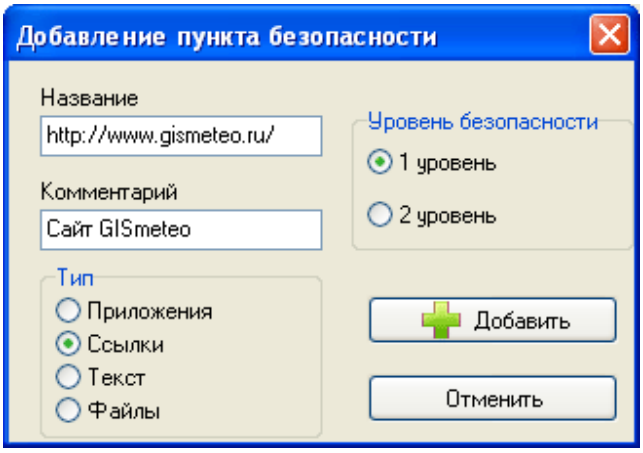
Рассмотрим заполнение правил на конкретных примерах:

1. Допустим, мы хотим, чтобы программа MailAgent подсвечивалась в логах запуска программ, как запрещенная. Для это в окне настроек безопасности, переходим на закладку приложения и нажимаем кнопку **«Добавить»** (в правой части окна). При этом откроется окно добавления пункта безопасности. В поле **«Название»** записываем имя exe файла (в нашем случае это Magent.exe). Выбираем уровень безопасности (1-ый соответствует желтому цвету светофора, 2-ой - красному). При желании можно указать комментарии, например, как на рисунке.

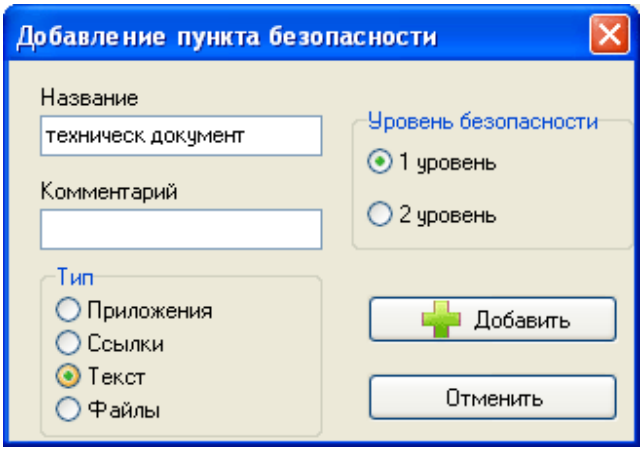


После нажатия кнопки **«Добавить»**, данное правило будет сохранено.

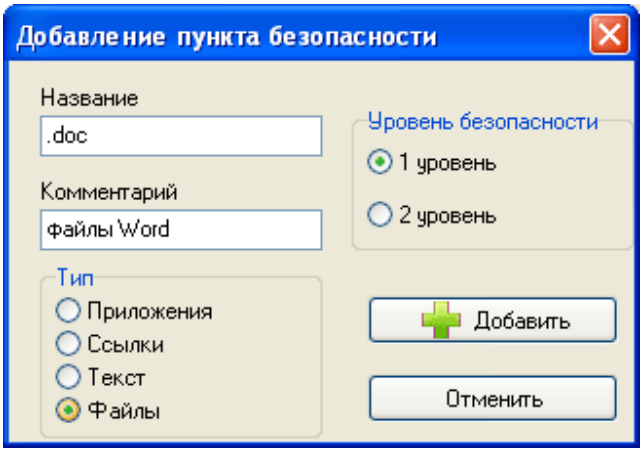
2. Установка правил для Web-ссылок. Начальные действия теже, что и в первом примере, только вызываем диалог добавления пункта безопасности с закладки **«Ссылки»** или выбираем эту категорию в самом диалоге добавления. Если мы хотим выделять только какую-то конкретную ссылку, то ее необходимо заполнить в поле **«Название»**, например «http://www.gismeteo.ru/». Но необходимо иметь в виду, что ссылка при анализе будет распознана только в том случае, когда в строке адреса будет полностью содержаться заданный фрагмент. Т.е. например, «http://www.gismeteo.ru/towns/34172.htm». Если необходимо отлавливать еще и ссылки типа «http://www.forum.gismeteo.ru», то необходимо в качестве названия задать более короткую строку, например просто «gismeteo».



3. Теперь что касается настроек для закладки **«Текст»**. В версии 2.0 поиск производится без учета падежа, рода и числа слова (т.е. для «узнавания» необходимо полное совпадение эталона со словом или частью слова в исследуемом тексте). Поэтому при задании текста пункта безопасности, желательно убрать у слов окончания (например «техническ документ»). Если в качестве строки для поиска задано не одно слово, а целая фраза, то во время анализа она будет разобрана на отдельные слова и поиск произведется для каждого слова. Далее будет произведен подсчет % совпадения и если он окажется больше заданного (указанного в настройках программы), то LanAgent будет считать, что анализируемый текст содержит запрещенные слова.



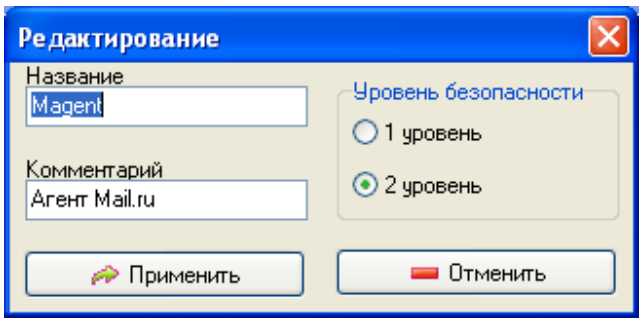
4. Закладка **«Файлы»**. Допустим мы хотим запретить работу с любыми текстовыми документами с расширением .doc. Тогда в поле **«Название»** мы соответственно внесем всё расширение.



Если надо особо отмечать работу с конкретным файлом, то соответственно добавляем в список только его.

Редактирование правил:

Для того чтобы отредактировать уже созданное правило, необходимо выделить его в таблице и нажать кнопку **"Редактировать"**, расположенную в правой части окна.



Удаление правил:

Для того чтобы удалить правило, необходимо выделить его в таблице и нажать кнопку "**Удалить**", расположенную в правой части окна.

5.4 Закладка «Контроль»

Позволяет определять круг пользователей, имеющих право на работу с программами **LanAgent Admin** (администраторы) и **LanAgent View** (специалисты безопасности), определять для них права доступа, а также производить подписку на оповещения по различным группам событий.

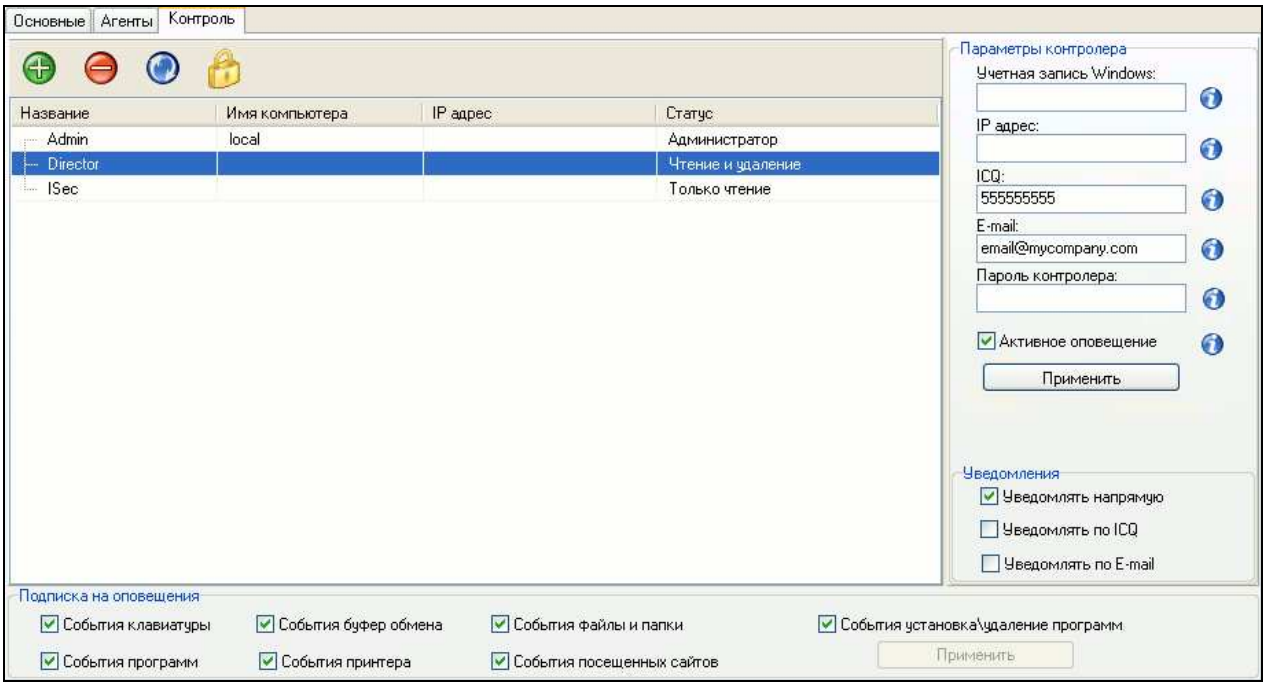


Рисунок 5.17 – Закладка «Контроль» LanAgent Admin

В левой части окна расположен сам список пользователей, имеющих право на работу с **LanAgent**.

Внимание! Пользователи, внесенные в данный список (после ввода соответствующих им логина и пароля), будут иметь доступ к программе **LanAgent View** в определенном для них объеме (кнопка «**Настройка доступа**»). Доступ к **LanAgent Admin** имеют только пользователи 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.

Для добавления нового пользователя в список, нажмите кнопку, при этом откроется следующее окно:

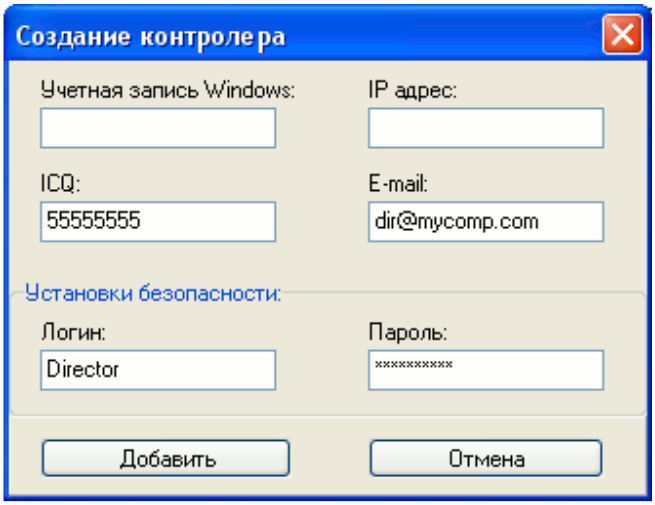


Рисунок 36 - Диалог добавления контролера

Поля «**Учетная запись Windows**» и «**IP адрес**» используются для «привязки» контролера к конкретной учетке windows и IP адресу соответственно. Если они заданы, то войти в программу LA View можно будет только из-под указанной учетки и с компьютера, имеющего данный IP адрес. **Поэтому если нет необходимости в такой привязке, то оставьте данные поля пустыми!**
«**ICQ**» и «**E-mail**» будут использоваться для адресации оповещений, на которые данный пользователь будет подписан. Они не являются обязательными.
Значения, введенные в поля «**Логин**» и «**Пароль**», данный пользователь будет вводить в диалоге авторизации в качестве логина и пароля соответственно при запуске программ **LanAgent View** или **LanAgent Admin.**
По окончанию заполнения, нажмите кнопку «**Добавить**», для внесения пользователя в список.

Для удаления уже существующего пользователя, нажмите кнопку.

При нажатии кнопки список пользователей будет загружен заново из базы. Данной опцией имеет смысл пользоваться, если список кроме вас может редактироваться еще кем-то. Это позволит увидеть все сделанные изменения.

При выборе конкретного пользователя из списка, в правой части окна для него становятся доступными «**Параметры контролера**» (используются для адресации оповещений) и «**Настройка доступа**» (логин и пароль пользователя).

Для определения прав пользователя, воспользуйтесь кнопкой «**Настройка доступа**».

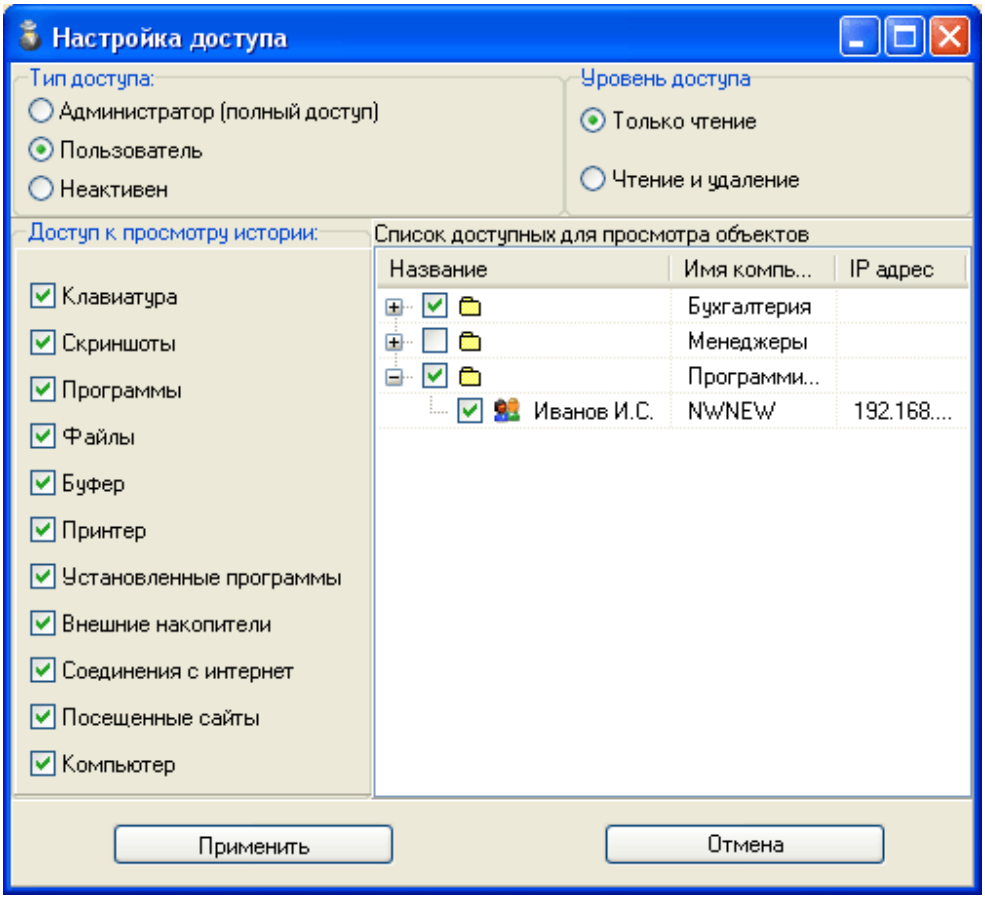


Рисунок 5.18 – Окно настройки доступа

Возможны три типа пользователей: Администратор (обладает неограниченными правами) Пользователь (для него возможны 2 уровня доступа к данным: «Только чтение» и «Чтение и удаление») и Неактивен (учетные записи с данным типом соответственно не имеют никаких прав доступа).
Обычный пользователь не имеет доступа к **LanAgent Admin**, а в **LanAgent View** для него недоступна системная история (Log).
Его права на просмотр данных по другим категориям определяются ниже, в окне «Доступ к просмотру истории». По-умолчанию у вновь созданного пользователя уже есть право на просмотр всех типов истории. Для запрещения доступа к определенной категории, достаточно убрать галочку рядом с ней и, затем, нажать кнопку «**Применить**».
Также, для каждого пользователя необходимо указывать список компьютеров, собранную информацию с которых он имеет право просматривать. Для пользователя с правами администратора по-умолчанию доступны для просмотра все контролируемые компьютеры.

Подписка на оповещения:

Здесь определяется по каким типам событий выбранный специалист безопасности будет получать уведомления.

Уведомления:

В разделе «**Уведомления**» определяется каким способом выбранный специалист безопасности будет получать уведомления о происшедших событиях:

- **Уведомлять напрямую** – требует запущенной у специалиста безопасности программы **LanAgent View.** При возникновении события, **LanAgent View** выдаст соответствующее сообщение на экран и, при необходимости, перейдет на соответствующую строку истории событий. (необходимо заполнение параметров «**Имя компьютера**» и «**IP адрес**»)
- **Уведомлять по ICQ** – при возникновении события, специалисту безопасности придет сообщение ICQ, в котором будет содержаться тип события, время его возникновения, на каком компьютере оно произошло (необходимо заполнение параметра «**ICQ**»)
- **Уведомлять по E-mail** – при возникновении события, специалисту безопасности придет письмо, на указанный в соответствующем поле настройки электронный ящик, в котором будет содержаться тип события, время его возникновения, на каком компьютере оно произошло (необходимо заполнение параметра «**E-mail**»)

Активное оповещение:

Если данная опция включена, то выбранный специалист будет получать также события активного оповещения (сообщения о подключении к контролируемому компьютеру съемного носителя информации, установке/удалении программы).

Для изменения указанных выше настроек достаточно установить галочки рядом с нужными пунктами и нажать кнопку «**Применить**».

6 Работа с LanAgent View

Интерфейс программы LanAgent View включает в себя следующие элементы:

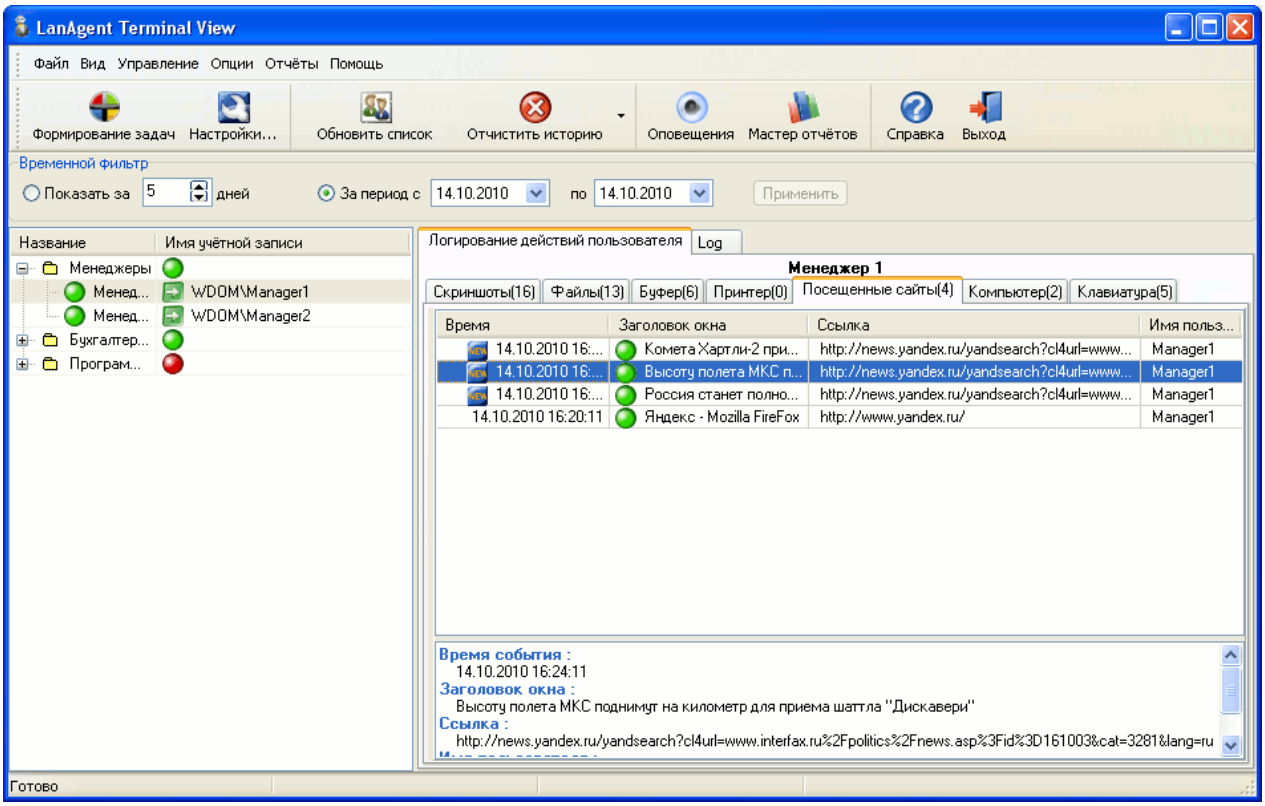


Рис. 6.1 – Главное окно программы

1 – список компьютеров для мониторинга
2 – окно просмотра истории активности контролируемых компьютеров
3 – окно просмотра подробной информации по конкретной записи истории
4 – панель инструментов.

Одной из отличительных особенностей версии Enterprise по сравнению со стандартной версией LanAgent, является то, что передача заданий агентам производится не напрямую, а через дополнительное звено – модуль обмена. Поэтому такие задачи как старт/стоп мониторинга, получение скриншота в текущий момент, внеочередной сбор логов и передача сообщений на контролируемый компьютер, применяются не сразу, а через промежуток времени, необходимый для их отработки модулем обмена.
Поставить задачи, а также проследить стадии их выполнение можно при помощи специального диалога формирования задач (подробней смотрите пункт 6.8).

6.1 Список пользователей для мониторинга

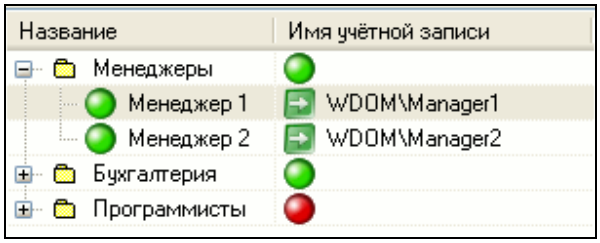


Рис. 6.2 – Окно списка мониторинга

Здесь отображаются терминальные пользователи, за которыми ведётся наблюдение. Для удобства работы со списком компьютеров для мониторинга, имеется возможность объединять пользователей в группы, например в соответствии с тем как они распределены по отделам структуры предприятия. Вы можете добавлять пользователей и группы в список мониторинга и удалять их (это производится при помощи программы LanAgent Terminal Admin).

Для удобства контроля за соблюдением политик безопасности и политик использования компьютерной техники, для каждого компьютера отображается статус опасности действий, производимых на нем (**"Светофор" безопасности**). Статус опасности группы равен наибольшему статусу опасности из входящих в нее компьютеров.

Внимание! В данном списке будут отображены только те пользователи и группы, на просмотр данных по которым имеет право данный специалист безопасности (логин и пароль которого были введены при входе в программу). Задание прав на просмотр данных и выбор доступных для просмотра данных производятся в программе LanAgent Admin (подробней см. пункт 5.4)

Таблица состоит из следующих столбцов:

- **Имя учетной записи** - имя учетной записи контролируемого пользователя.
- **Название** - название для данной учетной записи в списке мониторинга. Вы указываете его самостоятельно при ее добавлении. Также в любой момент вы можете изменить его.
- Рядом с названием каждого компьютера имеется специальный значок - **статус**, который информирует, в каком состоянии находится пользовательская часть программы на указанном компьютере. Может принимать следующие значения:

- мониторинг запущен;

- мониторинг остановлен;

- нет связи с агентом (возможно пользователь не подключен к терминальному серверу или на нём не запущена пользовательская часть программы).

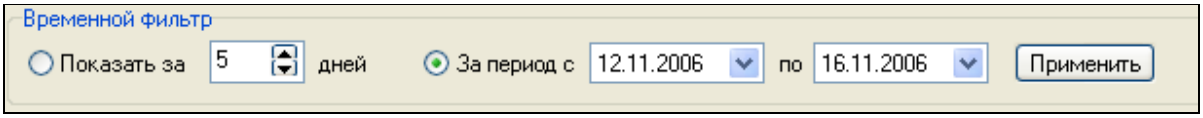
- Рядом с названием каждого компьютера и в колонке имени каждой группы имеется значок **"светофора" безопасности**, который может принимать три значения: зеленый, желтый и красный.

6.2 Окно просмотра истории активности контролируемых компьютеров

Для удобства работы, информация по различным видам активности (логи) контролируемых компьютеров размещена на различных закладках:

- Клавиатура (хранит текст, набираемый пользователем на клавиатуре);
- Скриншоты (содержит список произведенных снимков экранов мониторов);
- Программы (история запуска и закрытия программ);
- Буфер (хранит текст, копируемый пользователями в буфер обмена);
- Файлы (содержит статистику создания, удаления и переименовывания файлов);
- Принтер (перечень документов, отправленных на печать на принтер);
- Установленные программы (история установки и удаления программ);
- Внешние накопители (хранит события подключения и отключения носителей информации);
- Посещенные сайты (перечень посещенных пользователями сайтов);
- Компьютер (лог подключения и отключения пользователей к терминальному серверу).

Для того чтобы просмотреть интересующую категорию информации, выберите соответствующую закладку. Для выбора интервала времени, за который требуется выдать информацию, воспользуйтесь **Временным фильтром**.



6.2.1 Клавиатура

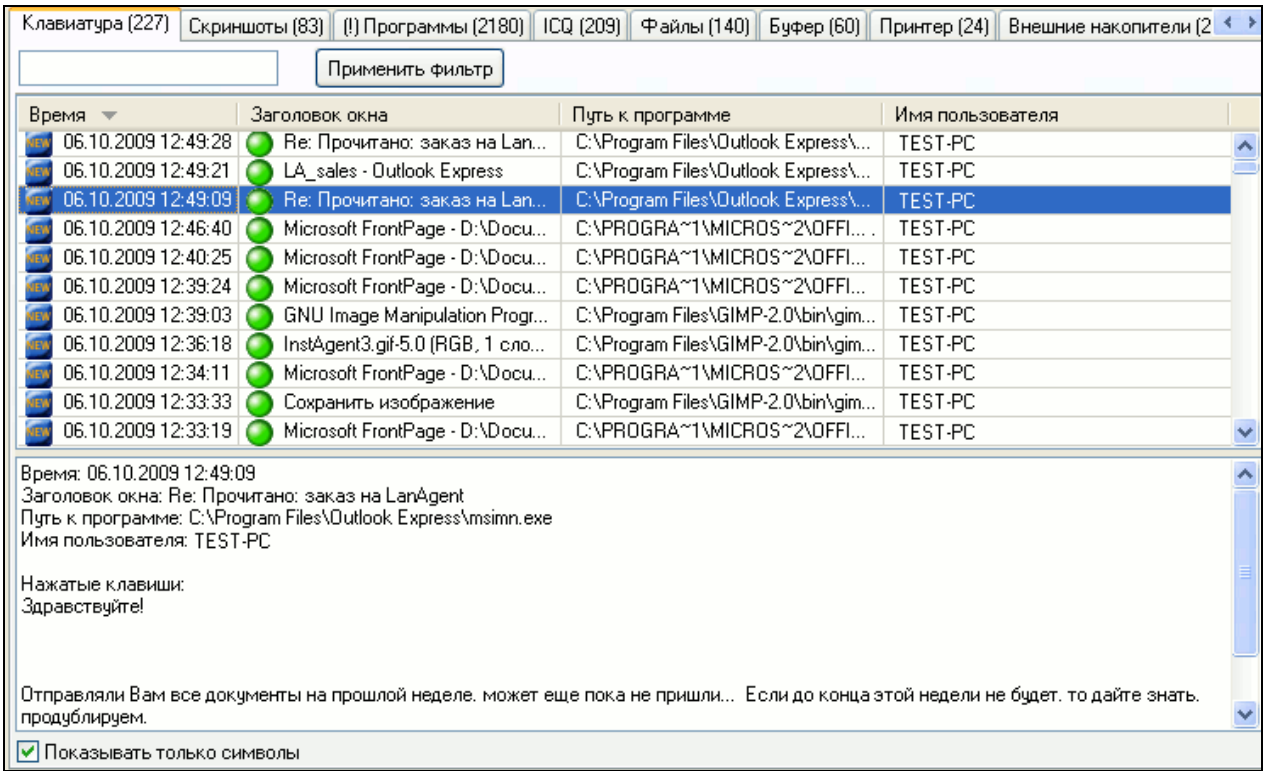


Рис. 6.3 – Окно логов клавиатуры

На этой странице находится информация по нажатым на клавиатуре клавишам, что позволяет, например, просмотреть текст, набранный пользователем. В заголовке закладки в скобках указано количество записей в таблице. Данные в таблице могут быть отсортированы по любому из столбцов, например по убыванию времени (то есть последняя информация содержится вверху таблицы). В таблице содержится следующая информация: дата и время нажатия клавиш, заголовок окна и полный путь к программе, где набиралась информация, а также имя пользователя. Для перемещения по таблице можно пользоваться как мышкой, так и стрелками курсора. В текстовом поле под таблицей отображается вся информация из таблицы по данной записи для более удобного просмотра, а также нажатые клавиши. Соотношение высоты таблицы и текстового поля можно изменять. Для этого надо поместить курсор мыши на границе таблицы и текстового поля (при этом курсор изменит вид), прижать левую кнопку мыши и потянуть вверх или вниз.

Программа **LanAgent** регистрирует все нажатия клавиш, различает регистр и русскую раскладку. Может запоминать только символы и цифры, без запоминания системных клавиш (таких как Ctrl, Shift и т.д.). При просмотре нажатых клавиш можно просматривать только символы, чтобы не отображались нажатия системных клавиш, что намного удобнее. Например, если были нажаты следующие клавиши:

"[Shift]Регистрирует[Space]все[Space]нажатия[Space]клавиш"

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

"Регистрирует все нажатия клавиш"

Также имеется возможность установить фильтр по времени возникновения событий. Тогда будут отображаться только те записи, которые соответствуют указанному условию. Возможны два варианта: указать период в днях от текущего, за который показывать логи или задать период конкретными датами, началом суток которых будет ограничиваться выбираемый диапазон логов.

6.2.2 Скриншоты

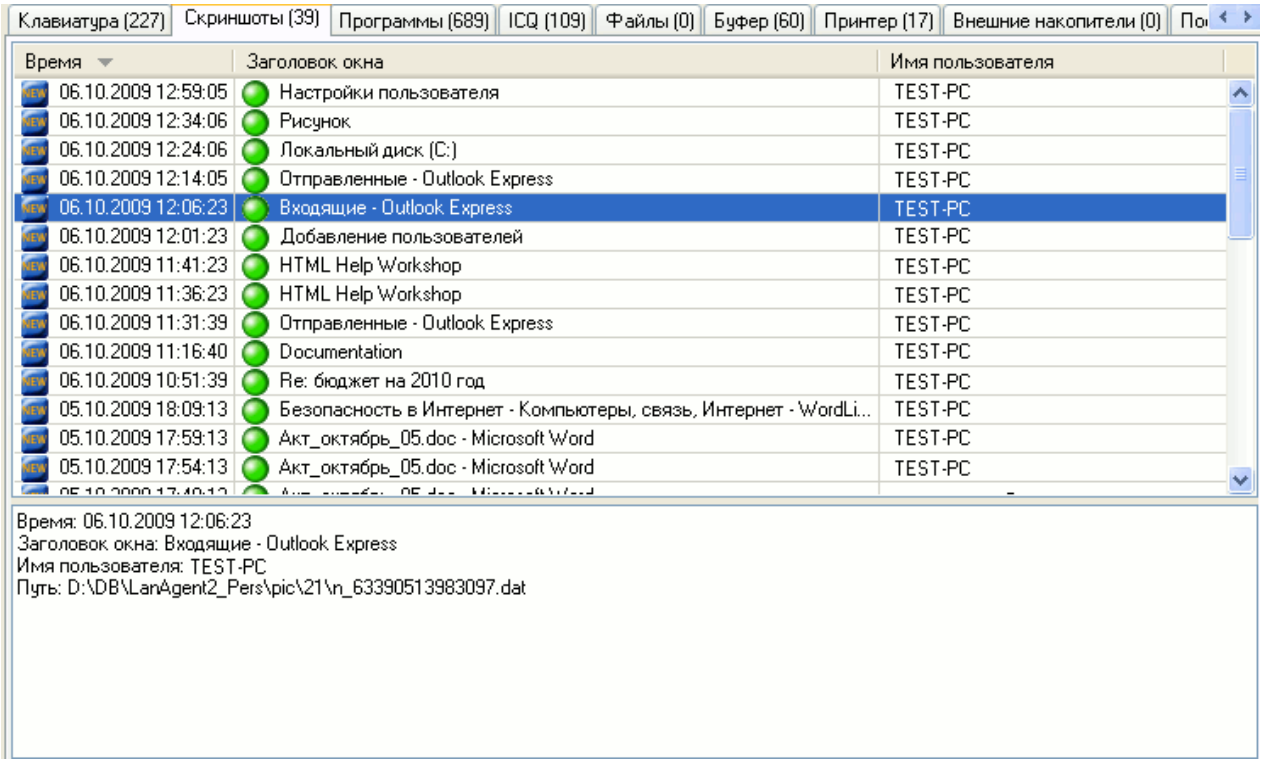


Рис. 6.4 – Окно логов снимков экранов (скриншотов)

На этой странице находится информация по произведенным снимкам экранов мониторов пользователей (скришотам). В заголовке закладки в скобках указано количество записей в таблице. Данные в таблице могут быть отсортированы по любому из столбцов, например по убыванию времени (то есть последняя информация содержится вверху таблицы). В таблице содержится следующая информация: дата и время, когда был сделан скриншот, заголовок активного окна, а также имя пользователя. Для перемещения по таблице можно пользоваться как мышкой, так и стрелками курсора. В текстовом поле под таблицей отображается вся информация из таблицы по данной записи для более удобного просмотра, а также путь к скриншоту на диске. Соотношение высоты таблицы и текстового поля можно изменять. Для этого надо поместить курсор мыши на границе таблицы и текстового

поля (при этом курсор изменит вид), прижать левую кнопку мыши и потянуть вверх или вниз.

Для просмотра скриншотов, кликните дважды в таблице по той записи, для которой хотите просмотреть скриншот (или нажмите клавишу "Enter" на клавиатуре). Появится окно для просмотра скриншотов.

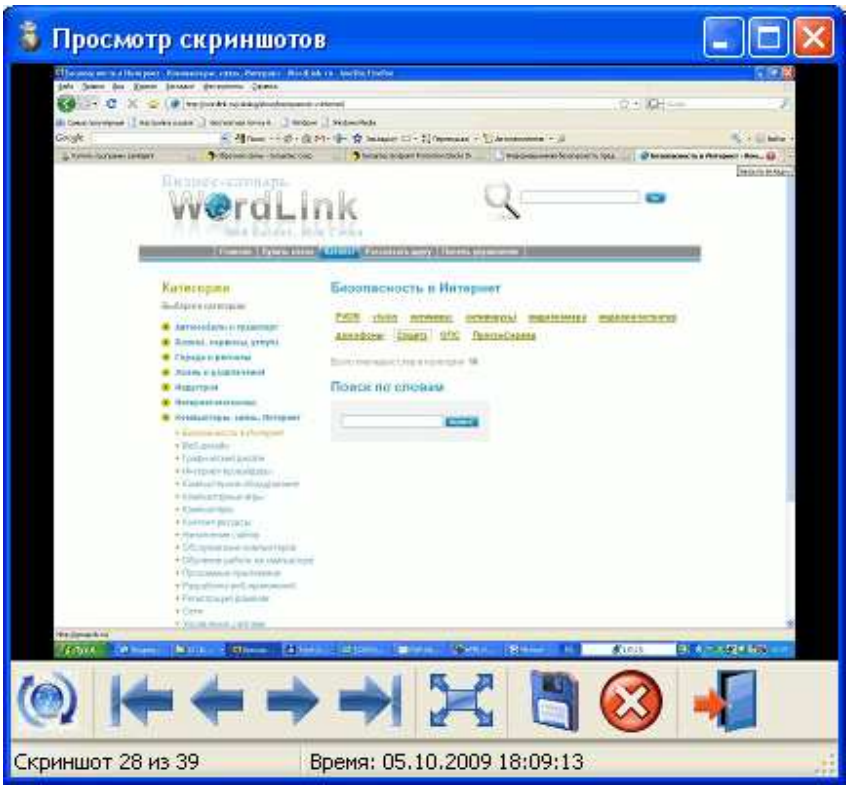


Рис. 6.5 – Окно просмотра скриншотов

В строке состояния отображается общее количество скриншотов и номер скриншота, который просматривается в данный момент, а также дата и время, в которое был сделан этот скриншот.

Назначение кнопок панели инструментов:

- переместиться к первому скриншоту (в начало).

- показать предыдущий скриншот.

- показать следующий скриншот.

- переместиться к последнем скриншоту (в конец).

- показать скриншот во весь экран (также для этого можно дважды кликнуть на самом скриншоте).

- сохранить скриншот на диск (появится диалоговое окно, в котором вы должны выбрать место, куда сохранить картинку).

- удалить скриншот.

- удалить все скриншоты.

- закрыть окно просмотра скриншотов.

6.2.3 Программы

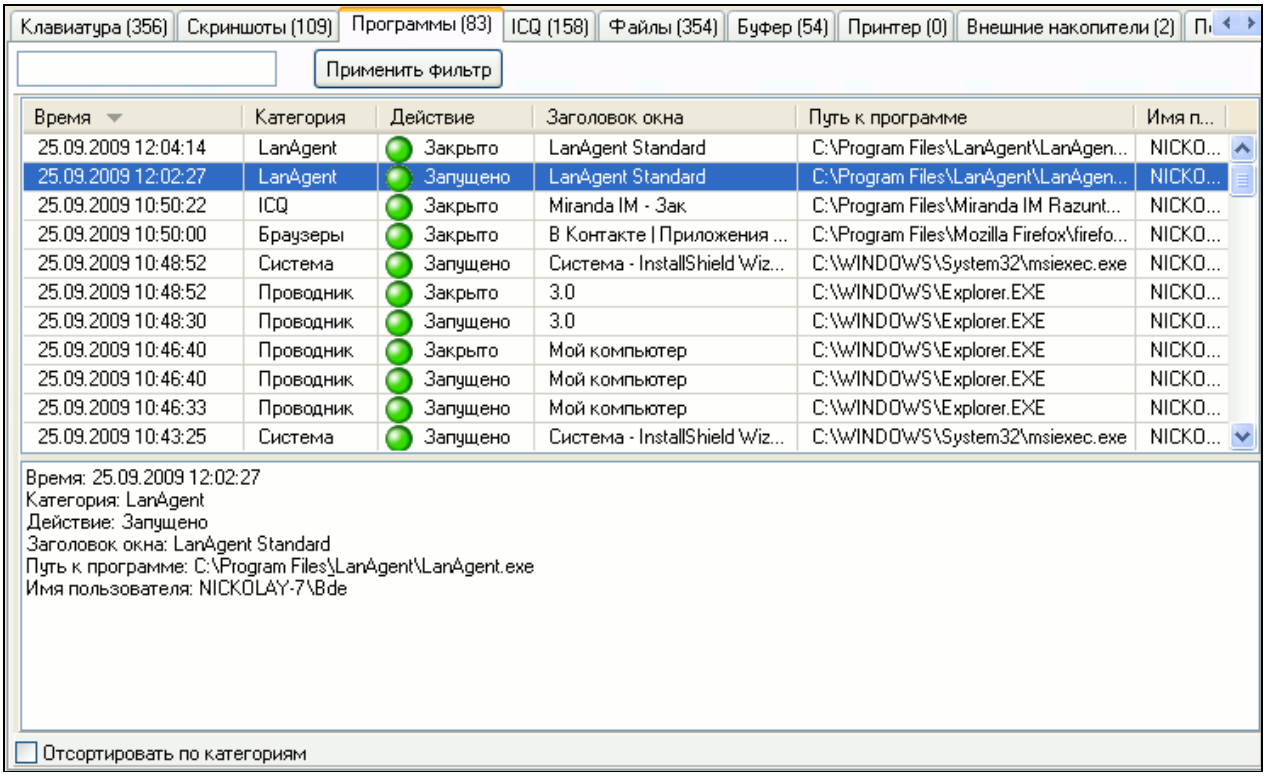


Рис. 6.6 – Окно логов программ

На этой странице находится история запуска/закрытия программ. В заголовке закладки в скобках указано количество записей в таблице. Данные в таблице могут быть отсортированы по любому из столбцов, например по убыванию времени (то есть последняя информация содержится вверху таблицы). В таблице содержится следующая информация: дата и время запуска или закрытия программы, какое действие было произведено (запущена или закрыта программа), заголовок окна и полный путь к программе, а также имя пользователя. Для перемещения по таблице можно пользоваться как мышкой, так и стрелками курсора. В текстовом поле под таблицей отображается вся информация из таблицы по данной записи для более удобного просмотра. Соотношение высоты таблицы и текстового поля можно изменять. Для этого надо поместить курсор мыши на границе таблицы и текстового поля (при этом курсор изменит вид), прижать левую кнопку мыши и потянуть вверх или вниз.

Также имеется возможность установить фильтр по времени возникновения событий. Тогда будут отображаться только те записи, которые соответствуют указанному условию. Возможны два варианта: указать период в днях от текущего, за который показывать логи или задать период конкретными датами, началом суток которых будет ограничиваться выбираемый диапазон логов.

6.2.4 Буфер обмена

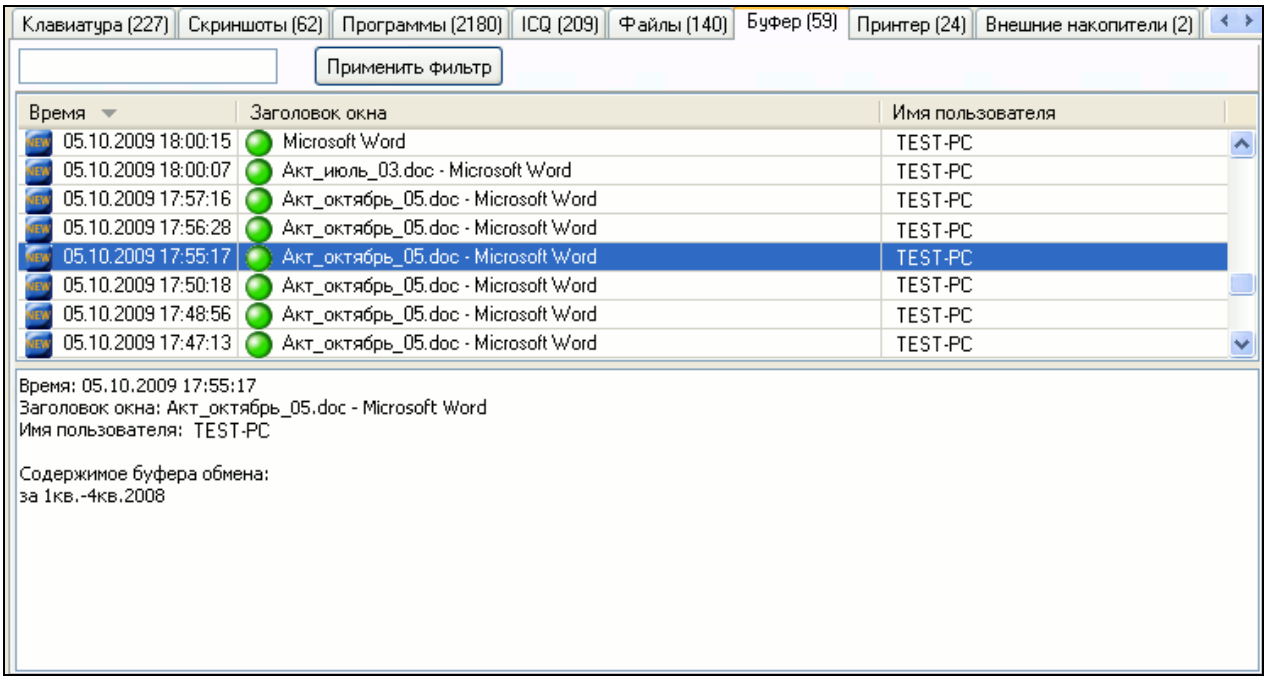


Рис. 6.7 – Окно логов буфера обмена

На этой странице находится информация, копируемая пользователями в буфер обмена. В заголовке закладки в скобках указано количество записей в таблице. Данные в таблице могут быть отсортированы по любому из столбцов, например по убыванию времени (то есть последняя информация содержится вверху таблицы). В таблице содержится следующая информация: дата и время изменения буфера обмена, заголовок окна, из которого была скопирована информация, а также имя пользователя. Для перемещения по таблице можно пользоваться как мышкой, так и стрелками курсора. В текстовом поле под таблицей отображается вся информация из таблицы по данной записи для более удобного просмотра, а также содержимое буфера обмена. Соотношение высоты таблицы и текстового поля можно изменять. Для этого надо поместить курсор мыши на границе таблицы и текстового поля (при этом курсор изменит вид), прижать левую кнопку мыши и потянуть вверх или вниз.

Также имеется возможность установить фильтр по времени возникновения событий. Тогда будут отображаться только те записи, которые соответствуют указанному условию. Возможны два варианта: указать период в днях от текущего, за который показывать логи или задать период конкретными датами, началом суток которых будет ограничиваться выбираемый диапазон логов.

6.2.5 Файлы

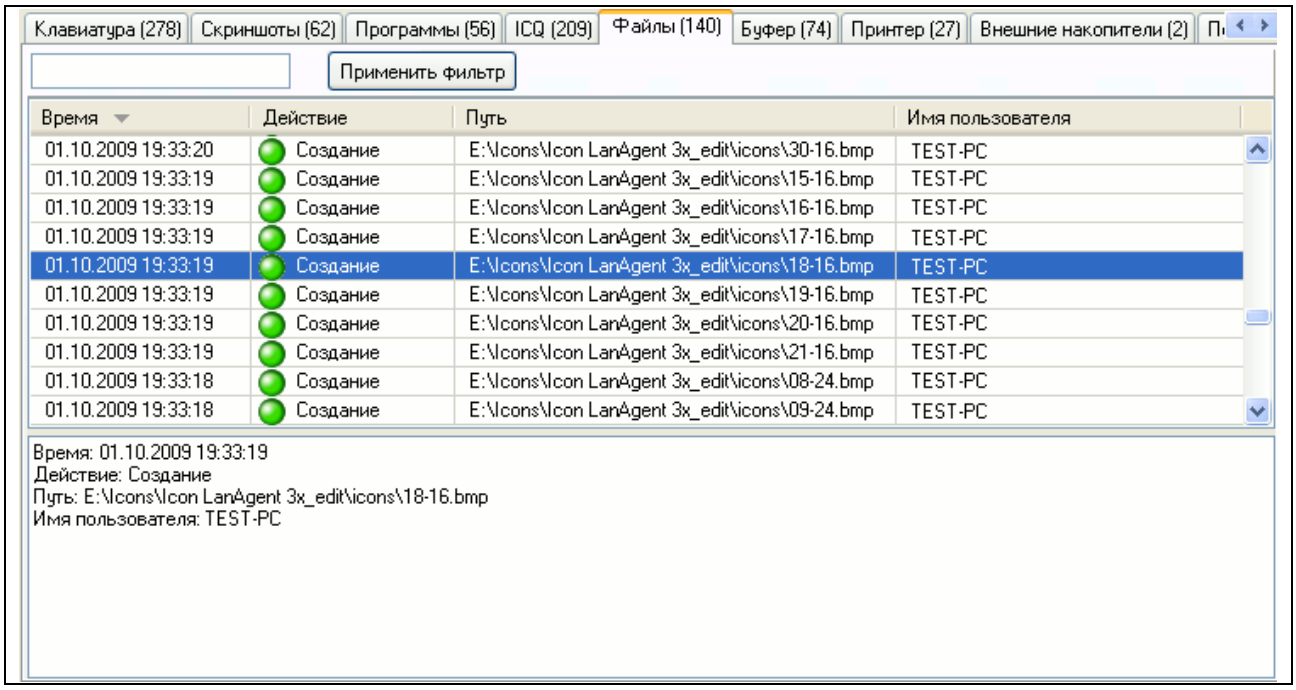


Рис. 6.8 – Окно статистики создания/удаления файлов

На этой странице находится статистика изменений в файловой системе пользователей (создание, удаление, переименование файлов). В заголовке закладки в скобках указано количество записей в таблице. Данные в таблице могут быть отсортированы по любому из столбцов, например по убыванию времени (то есть последняя информация содержится вверху таблицы). В таблице содержится следующая информация: дата и время события, какое действие было произведено (создан, удалён или переименован файл или папка), путь к этому файлу или папке, а также имя пользователя. Для перемещения по таблице можно пользоваться как мышкой, так и стрелками курсора. В текстовом поле под таблицей отображается вся информация из таблицы по данной записи для более удобного просмотра. Соотношение высоты таблицы и текстового поля можно изменять. Для этого надо поместить курсор мыши на границе таблицы и текстового поля (при этом курсор изменит вид), прижать левую кнопку мыши и потянуть вверх или вниз.

Также имеется возможность установить фильтр по времени возникновения событий. Тогда будут отображаться только те записи, которые соответствуют указанному условию. Возможны два варианта: указать период в днях от текущего, за который показывать логи или задать период конкретными датами, началом суток которых будет ограничиваться выбираемый диапазон логов.

6.2.6 Принтер

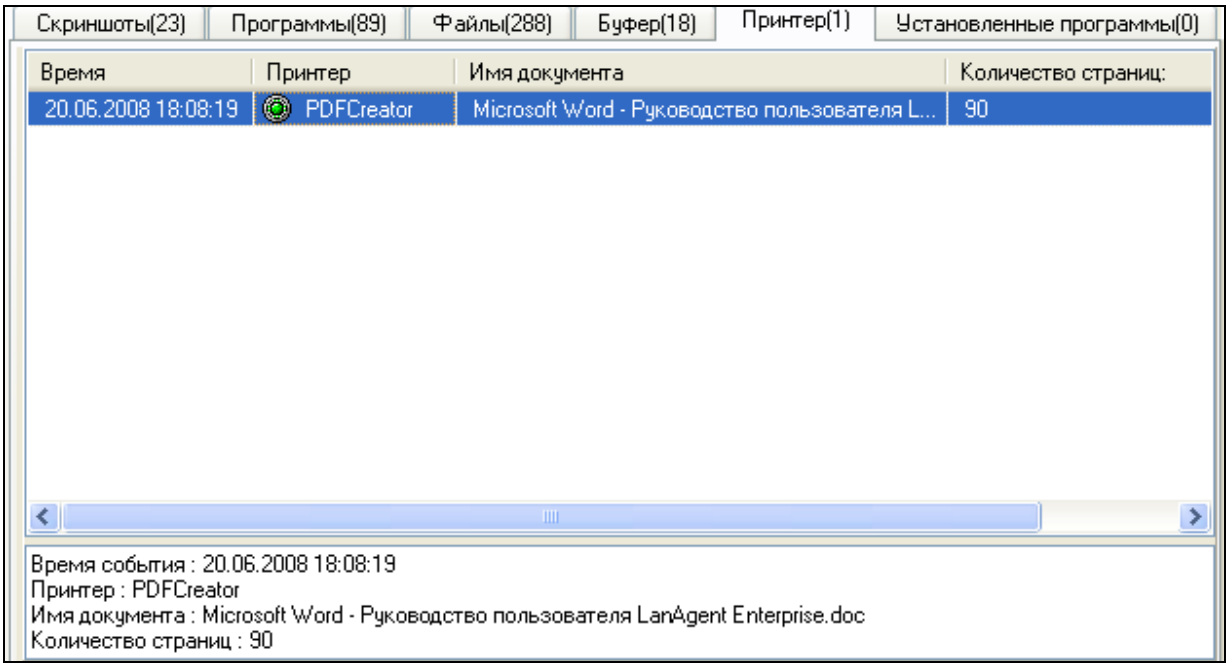
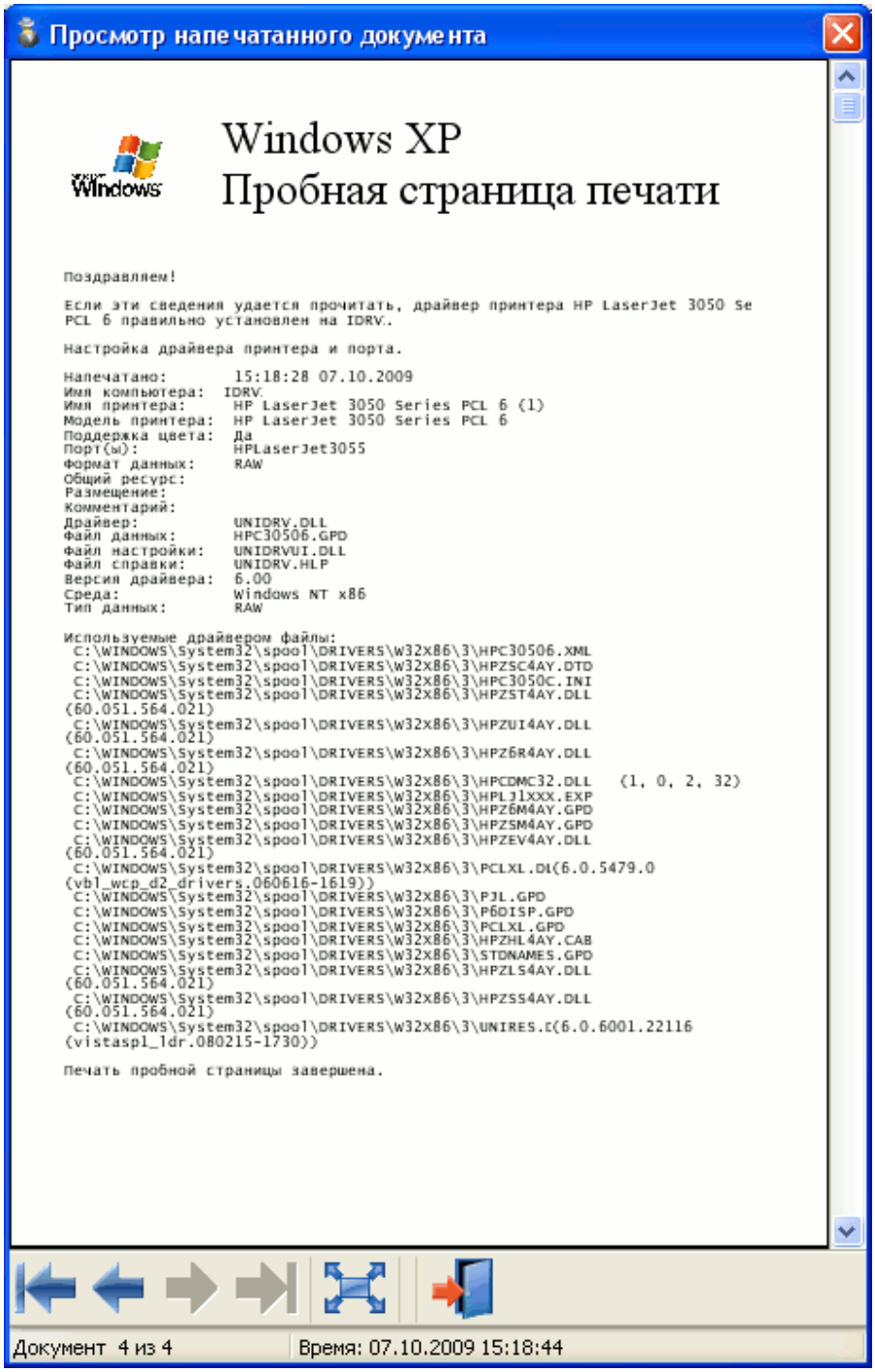


Рис. 6.9 – Окно логов принтеров

На этой странице находится информация по документам, распечатанным пользователями на принтере. В заголовке закладки в скобках указано количество записей в таблице. Данные в таблице могут быть отсортированы по любому из столбцов, например по убыванию времени (то есть последняя информация содержится вверху таблицы). В таблице содержится следующая информация: дата и время печати документа, название принтера, на котором был напечатан документ, имя самого документа, количество распечатанных страниц, а также имя пользователя. Для перемещения по таблице можно пользоваться как мышкой, так и стрелками курсора. В текстовом поле под таблицей отображается вся информация из таблицы по данной записи для более удобного просмотра. Соотношение высоты таблицы и текстового поля можно изменять. Для этого надо поместить курсор мыши на границе таблицы и текстового поля (при этом курсор изменит вид), прижать левую кнопку мыши и потянуть вверх или вниз.

Для просмотра самого содержимого напечатанного документа, кликните дважды в таблице по той записи, для которой хотите просмотреть содержимое. При этом появится окно для просмотра:



В строке состояния отображается общее количество скриншотов и номер скриншота, который просматривается в данный момент, а также дата и время, в которое был сделан этот скриншот.

Назначение кнопок панели инструментов:

- переместиться к первому скриншоту (в начало).

- показать предыдущий скриншот.

- показать следующий скриншот.

- переместиться к последнем скриншоту (в конец).

- показать во весь экран (также для этого можно дважды кликнуть на самом изображении).

- закрыть окно просмотра.

6.2.7 Установленные программы

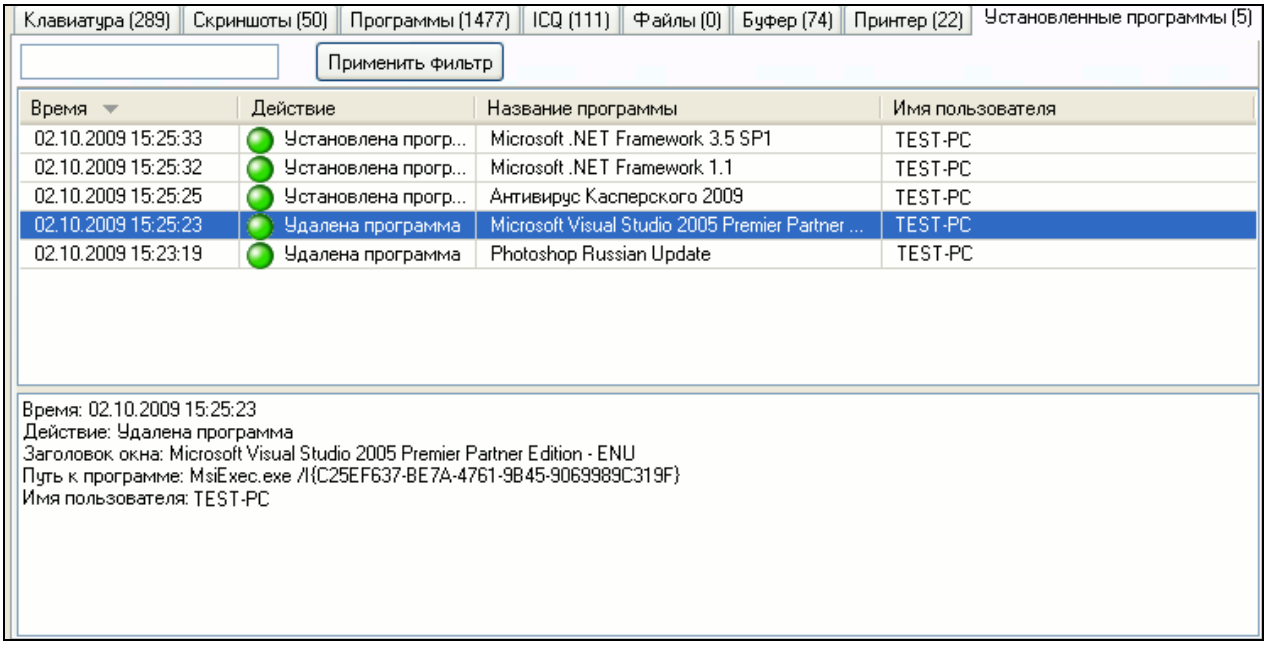


Рис. 6.10 – Окно логов установки/удаления программ

На этой странице находится история установки/удаления программ на контролируемых компьютерах. В заголовке закладки в скобках указано количество записей в таблице. Данные в таблице могут быть отсортированы по любому из

столбцов, например по убыванию времени (то есть последняя информация содержится вверху таблицы). В таблице содержится следующая информация: дата и время установки или удаления программы, какое действие было произведено (установлена или удалена программа), название программы, а также имя пользователя. Для перемещения по таблице можно пользоваться как мышкой, так и стрелками курсора. В текстовом поле под таблицей отображается вся информация из таблицы по данной записи для более удобного просмотра. Соотношение высоты таблицы и текстового поля можно изменять. Для этого надо поместить курсор мыши на границе таблицы и текстового поля (при этом курсор изменит вид), прижать левую кнопку мыши и потянуть вверх или вниз.

Также имеется возможность установить фильтр по времени возникновения событий. Тогда будут отображаться только те записи, которые соответствуют указанному условию. Возможны два варианта: указать период в днях от текущего, за который показывать логи или задать период конкретными датами, началом суток которых будет ограничиваться выбираемый диапазон логов.

6.2.8 Посещённые сайты

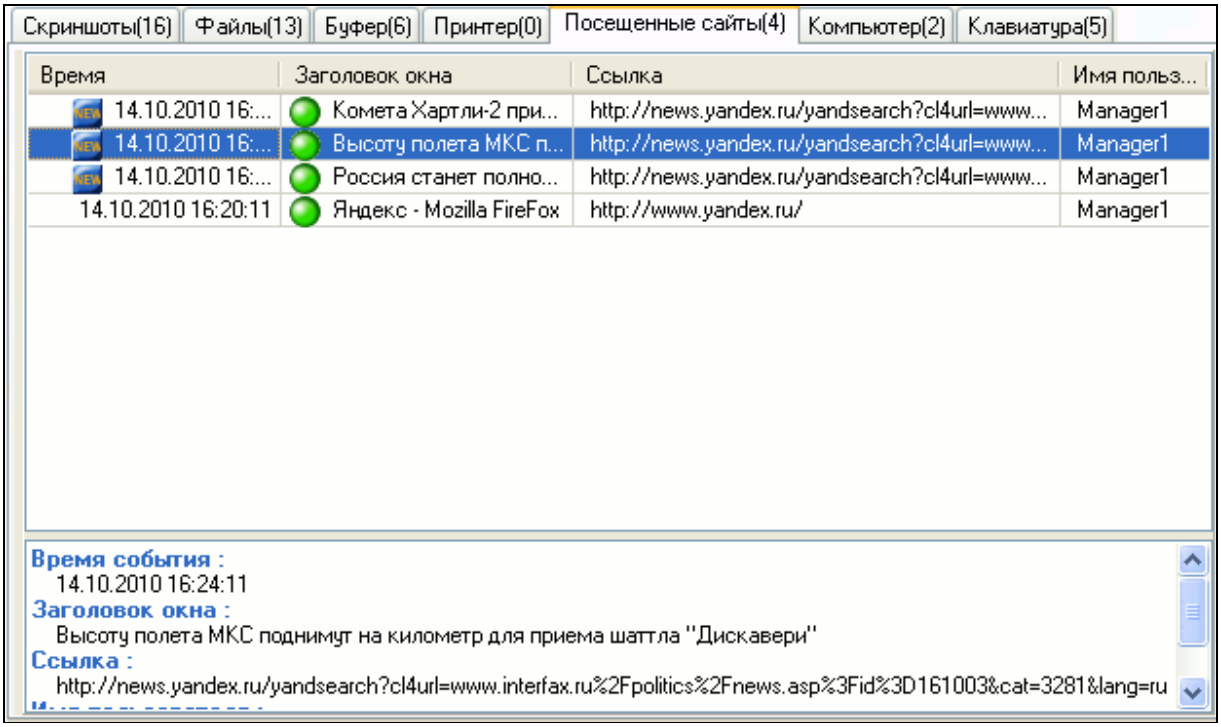


Рис. 6.13 – Окно логов посещенных сайтов

На этой странице находится информация о посещённых веб-сайтах. В заголовке закладки в скобках указано количество записей в таблице. Данные в таблице могут быть отсортированы по любому из столбцов, например по убыванию времени (то есть последняя информация содержится вверху таблицы). В таблице содержится

следующая информация: дата и время посещения сайта, название сайта (заголовок окна браузера), адрес сайта, а также имя пользователя. Для перемещения по таблице можно пользоваться как мышкой, так и стрелками курсора. В текстовом поле под таблицей отображается вся информация из таблицы по данной записи для более удобного просмотра. Соотношение высоты таблицы и текстового поля можно изменять. Для этого надо поместить курсор мыши на границе таблицы и текстового поля (при этом курсор изменит вид), прижать левую кнопку мыши и потянуть вверх или вниз.

Также имеется возможность установить фильтр по времени возникновения событий. Тогда будут отображаться только те записи, которые соответствуют указанному условию. Возможны два варианта: указать период в днях от текущего, за который показывать логи или задать период конкретными датами, началом суток которых будет ограничиваться выбираемый диапазон логов.

Для перехода на какой-либо из посещённых сайтов, кликните дважды в таблице по нужной записи - сайт откроется в браузере.

6.2.9 Компьютер

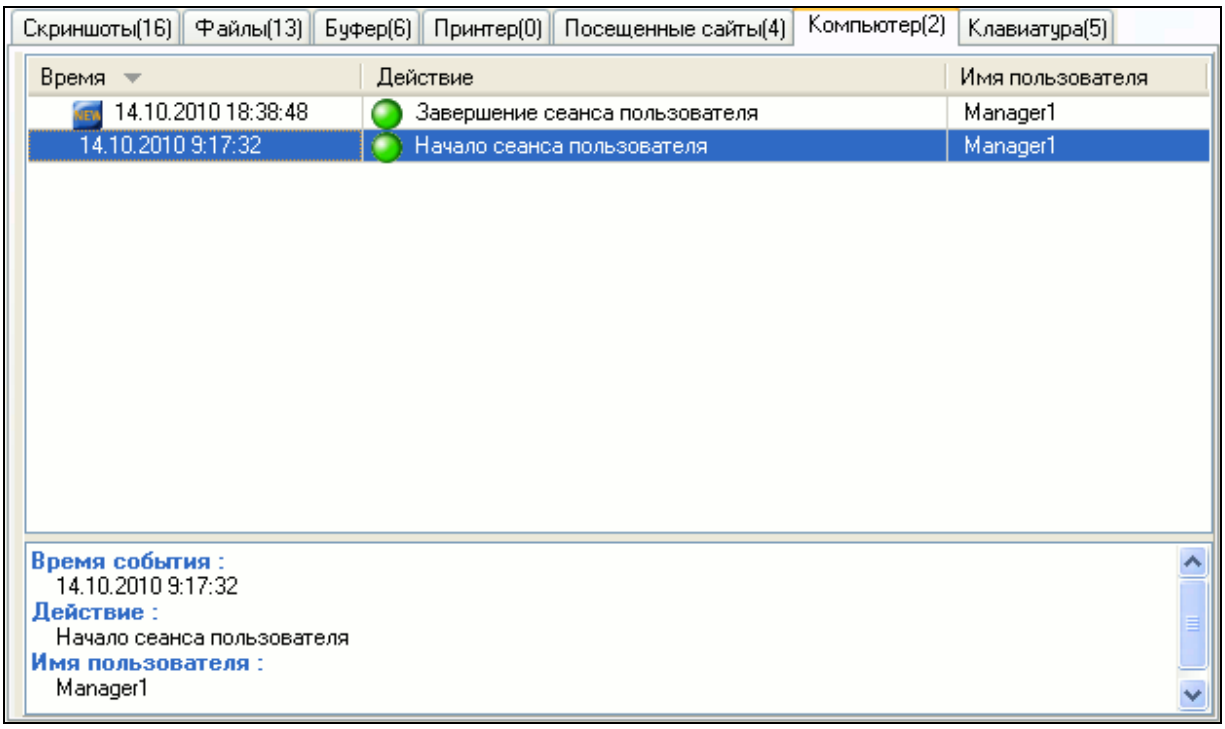


Рис. 6.14 – Окно статистики подключений/отключений терминального пользователя

На этой странице находится история подключений/отключений контролируемых терминальных пользователей. В заголовке закладки в скобках указано количество записей в таблице. Данные в таблице могут быть отсортированы по любому из

столбцов, например по убыванию времени (то есть последняя информация содержится вверху таблицы). В таблице содержится следующая информация: дата и время подключения или отключения пользователя, какое конкретно действие было произведено, а также имя пользователя. Для перемещения по таблице можно пользоваться как мышкой, так и стрелками курсора. В текстовом поле под таблицей отображается вся информация из таблицы по данной записи для более удобного просмотра. Соотношение высоты таблицы и текстового поля можно изменять. Для этого надо поместить курсор мыши на границе таблицы и текстового поля (при этом курсор изменит вид), прижать левую кнопку мыши и потянуть вверх или вниз.

Также имеется возможность установить фильтр по времени возникновения событий. Тогда будут отображаться только те записи, которые соответствуют указанному условию. Возможны два варианта: указать период в днях от текущего, за который показывать логи или задать период конкретными датами, началом суток которых будет ограничиваться выбираемый диапазон логов.

6.2.10 ICQ

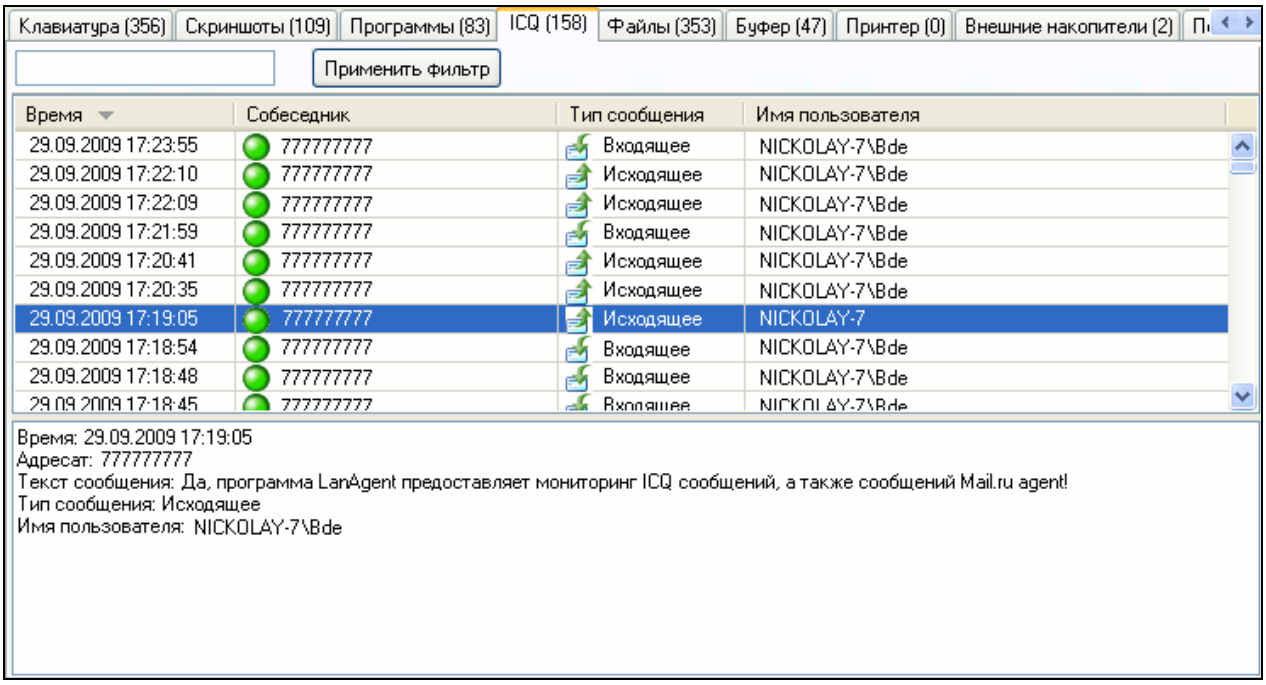


Рис. 6.15 – Окно статистики ICQ

Данная закладка становится доступной для просмотра в том случае, если кроме сервера LanAgent Terminal установлен также модуль LanAgent NetworkFilter.

На этой странице находится информация по перехваченным сообщениям ICQ. В заголовке закладки в скобках указано количество записей в таблице. Данные в таблице могут быть отсортированы по любому из столбцов, например по убыванию времени (то есть последняя информация содержится вверху таблицы). В таблице

содержится следующая информация: дата и время сообщения, собеседник которому было отправлено или от которого было принято сообщение, тип сообщения (Входящее или Исходящее), а также имя пользователя. Для перемещения по таблице можно пользоваться как мышкой, так и стрелками курсора. В текстовом поле под таблицей отображается вся информация из таблицы по данной записи для более удобного просмотра. Соотношение высоты таблицы и текстового поля можно изменять. Для этого надо поместить курсор мыши на границе таблицы и текстового поля (при этом курсор изменит вид), прижать левую кнопку мыши и потянуть вверх или вниз.

Также имеется возможность установить фильтр по времени возникновения событий. Тогда будут отображаться только те записи, которые соответствуют указанному условию. Возможны два варианта: указать период в днях от текущего, за который показывать логи или задать период конкретными датами, началом суток которых будет ограничиваться выбираемый диаппазон логов.

6.2.11 Mail.ru Agent

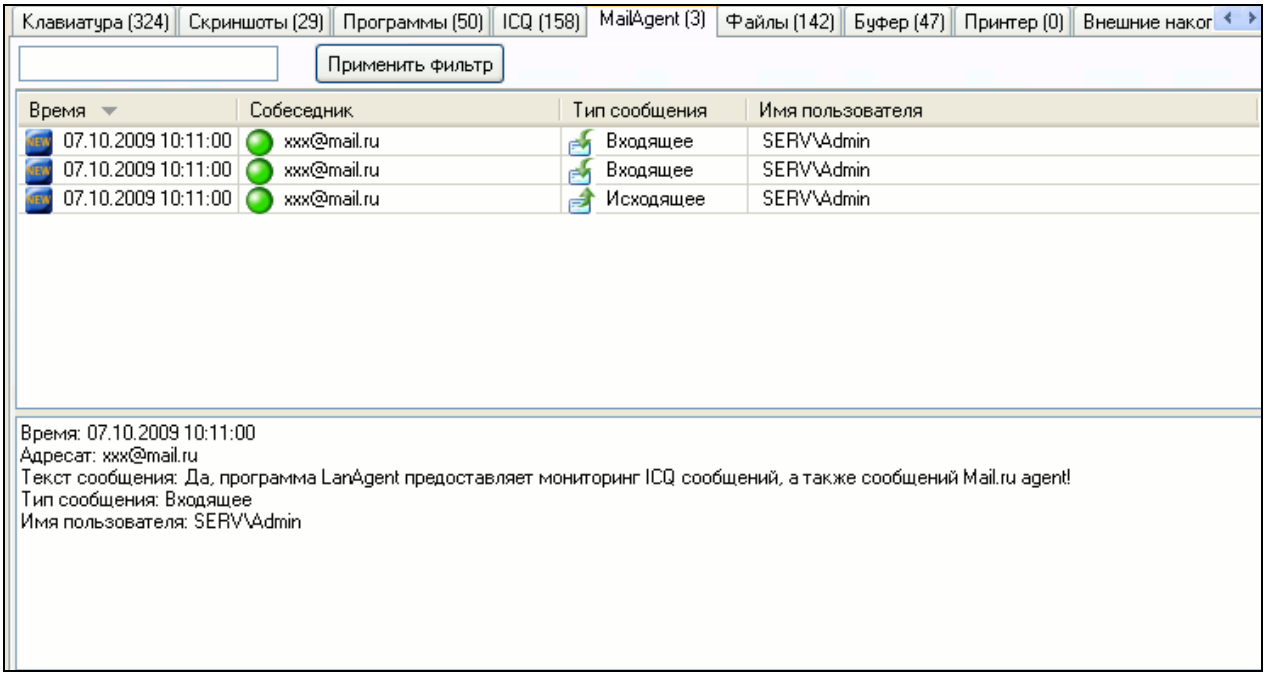


Рис. 6.16 – Окно статистики Mail.ru agent

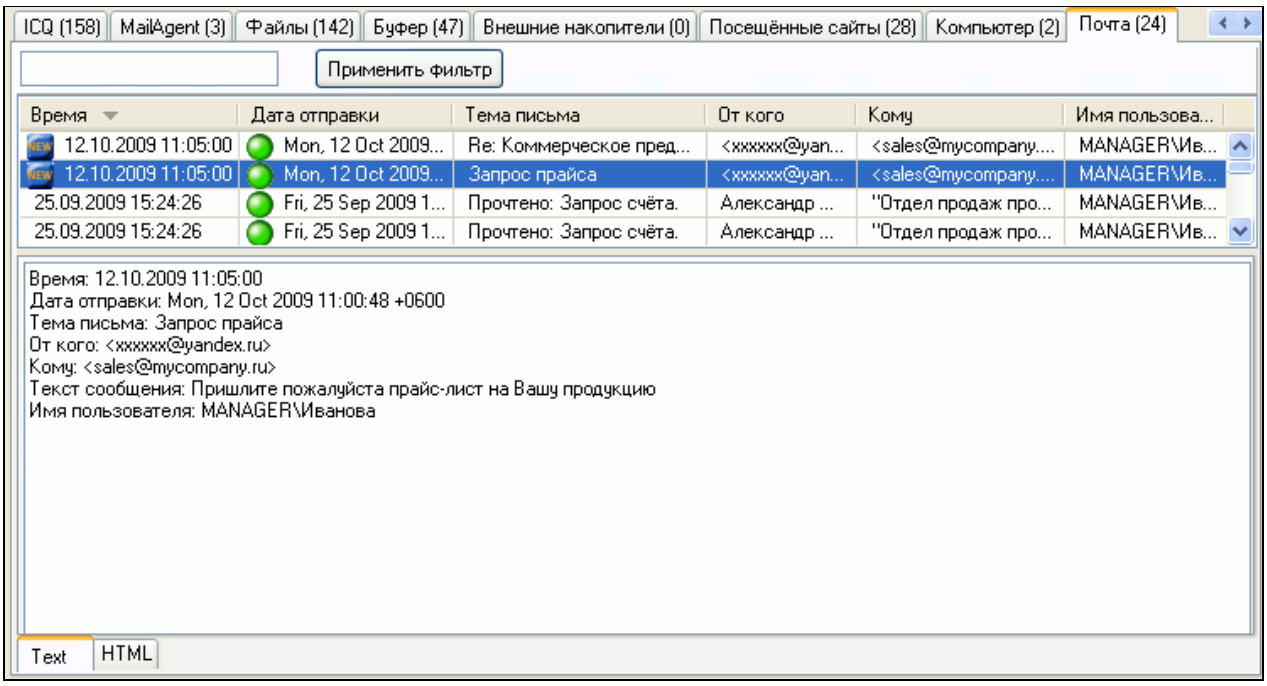
Данная закладка становится доступной для просмотра в том случае, если кроме сервера LanAgent Terminal установлен также модуль LanAgent NetworkFilter.

На этой странице находится информация по перехваченным сообщениям Mail.ru Agent. В заголовке закладки в скобках указано количество записей в таблице. Данные

в таблице могут быть отсортированы по любому из столбцов, например по убыванию времени (то есть последняя информация содержится вверху таблицы). В таблице содержится следующая информация: дата и время сообщения, собеседник которому было отправлено или от которого было принято сообщение, тип сообщения (Входящее или Исходящее), а также имя пользователя. Для перемещения по таблице можно пользоваться как мышкой, так и стрелками курсора. В текстовом поле под таблицей отображается вся информация из таблицы по данной записи для более удобного просмотра. Соотношение высоты таблицы и текстового поля можно изменять. Для этого надо поместить курсор мыши на границе таблицы и текстового поля (при этом курсор изменит вид), прижать левую кнопку мыши и потянуть вверх или вниз.

Также имеется возможность установить фильтр по времени возникновения событий. Тогда будут отображаться только те записи, которые соответствуют указанному условию. Возможны два варианта: указать период в днях от текущего, за который показывать логи или задать период конкретными датами, началом суток которых будет ограничиваться выбираемый диаппазон логов.

6.2.12 Почта



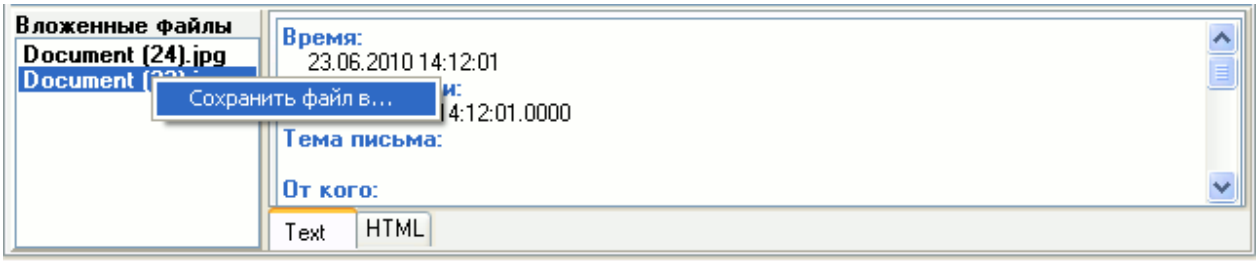
Данная закладка становится доступной для просмотра в том случае, если кроме сервера LanAgent Terminal установлен также модуль LanAgent NetworkFilter.

На этой странице находится информация по перехваченным электронным письмам. В заголовке закладки в скобках указано количество записей в таблице. Данные в таблице могут быть отсортированы по любому из столбцов, например по убыванию времени (то есть последняя информация содержится вверху таблицы). В таблице

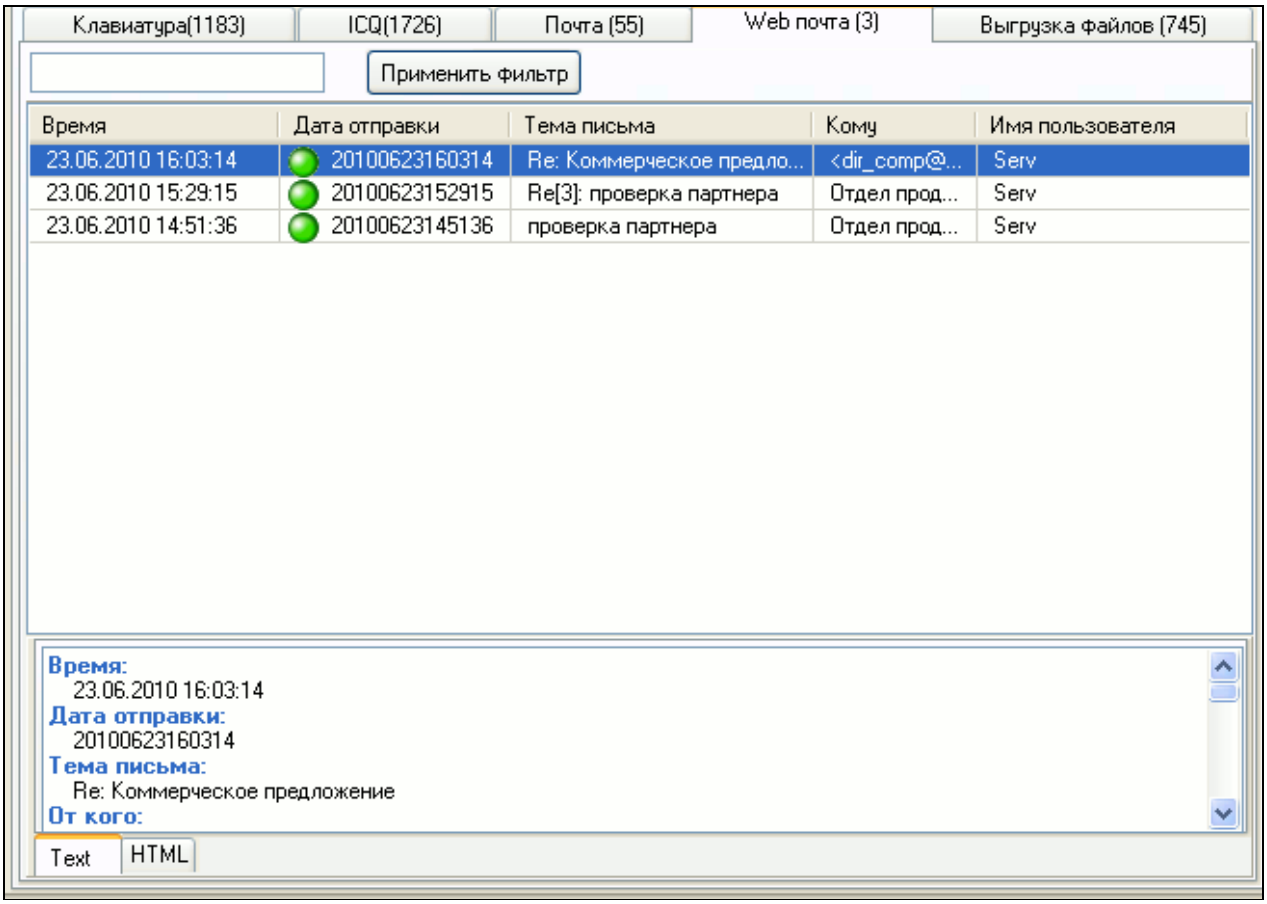
содержится следующая информация: дата и время перехвата письма, дата отправки письма, тема письма, от кого и кому оно отправлено, а также имя пользователя. Для перемещения по таблице можно пользоваться как мышкой, так и стрелками курсора. В текстовом поле под таблицей отображается вся информация из таблицы по данной записи для более удобного просмотра. Соотношение высоты таблицы и текстового поля можно изменять. Для этого надо поместить курсор мыши на границе таблицы и текстового поля (при этом курсор изменит вид), прижать левую кнопку мыши и потянуть вверх или вниз.

Также имеется возможность установить фильтр по времени возникновения событий. Тогда будут отображаться только те записи, которые соответствуют указанному условию. Возможны два варианта: указать период в днях от текущего, за который показывать логи или задать период конкретными датами, началом суток которых будет ограничиваться выбираемый диапазон логов.

Если письмо содержит вложенные файлы, то оно будет иметь значок "скрепки" и при выделении соответствующей строки лога, вложенные файлы будут показы в виде списка.



6.2.13 Web почта

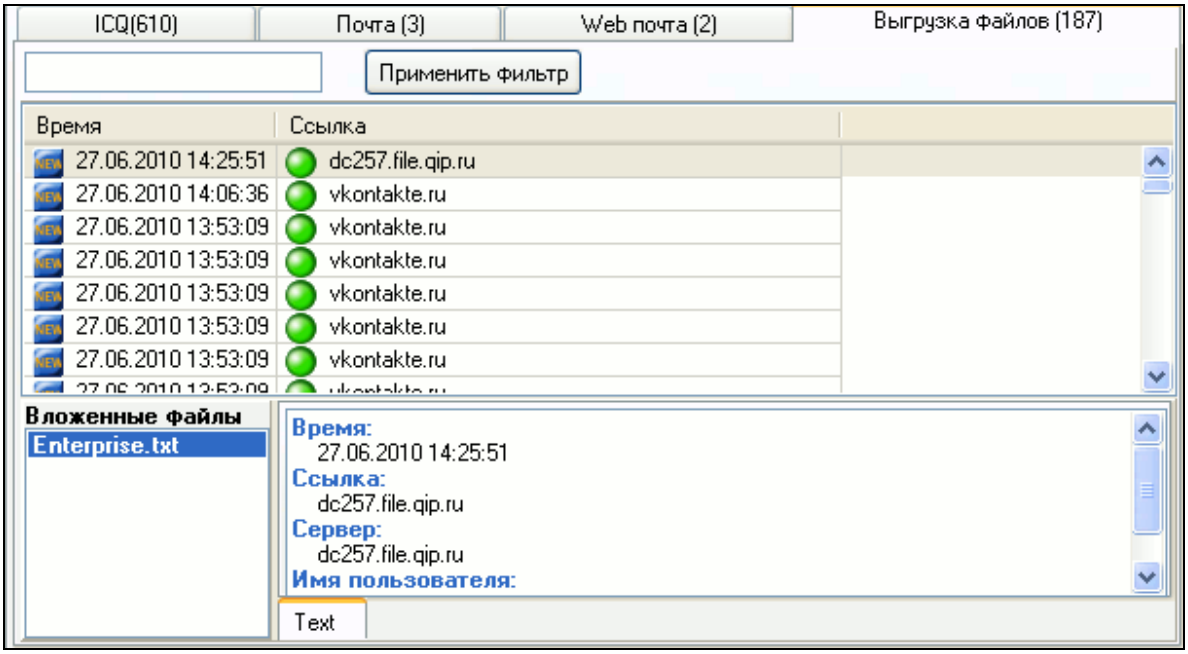


Данная закладка становится доступной для просмотра в том случае, если кроме сервера LanAgent Terminal установлен также модуль LanAgent NetworkFilter.

На этой странице находится информация по письмам, отправленным пользователем через web интерфейс. В заголовке закладки в скобках указано количество записей в таблице. Данные в таблице могут быть отсортированы по любому из столбцов, например по убыванию времени (то есть последняя информация содержится вверху таблицы). В таблице содержится следующая информация: дата и время перехвата отправки письма, дата отправки письма, тема письма, на какой e-mail оно было отправлено, Имя пользователя. Для перемещения по таблице можно пользоваться как мышкой, так и стрелками курсора. В текстовом поле под таблицей отображается вся информация из таблицы по данной записи для более удобного просмотра. Соотношение высоты таблицы и текстового поля можно изменять. Для этого надо поместить курсор мыши на границе таблицы и текстового поля (при этом курсор изменит вид), прижать левую кнопку мыши и потянуть вверх или вниз.

Также имеется возможность установить фильтр по времени возникновения событий. Тогда будут отображаться только те записи, которые соответствуют указанному условию. Возможны два варианта: указать период в днях от текущего, за который показывать логи или задать период конкретными датами, началом суток которых будет ограничиваться выбираемый диапазон логов.

6.2.14 Выгрузка файлов



Данная закладка становится доступной для просмотра в том случае, если кроме сервера LanAgent Terminal установлен также модуль LanAgent NetworkFilter.

На этой странице находится информация по файлам, выгруженным пользователем в Интернет. Также на данную вкладку могут попасть письма, отправленные через web интерфейс. Это произойдет в том случае, если web сервер, через который производится отправка письма, имеет нестандартный набор параметров авторизации. В таких случаях свяжитесь пожалуйста с нами и сообщите с какого web сервера была произведена отправка письма и сам набор параметров, чтобы мы смогли добавить разбор таких писем.

В заголовке закладки в скобках указано количество записей в таблице. Данные в таблице могут быть отсортированы по любому из столбцов, например по убыванию времени (то есть последняя информация содержится вверху таблицы). В таблице содержится следующая информация: дата и время отправки данных в интернет, Ссылка и Имя пользователя. Для перемещения по таблице можно пользоваться как мышкой, так и стрелками курсора. В текстовом поле под таблицей отображается вся информация из таблицы по данной записи для более удобного просмотра. Соотношение высоты таблицы и текстового поля можно изменять. Для этого надо поместить курсор мыши на границе таблицы и текстового поля (при этом курсор изменит вид), прижать левую кнопку мыши и потянуть вверх или вниз.

Также имеется возможность установить фильтр по времени возникновения событий. Тогда будут отображаться только те записи, которые соответствуют указанному условию. Возможны два варианта: указать период в днях от текущего, за который

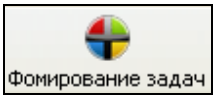
показывать логи или задать период конкретными датами, началом суток которых будет ограничиваться выбираемый диапазон логов.

6.3 Панель инструментов

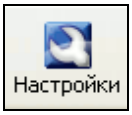
Ниже приведено описание кнопок панели управления программы LanAgent и выполняемых ими функций.

Рис. 6.15 – Панель инструментов

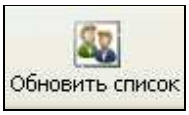
Назначение кнопок панели инструментов:



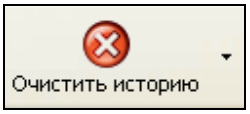
- открыть окно формирования задач для агентов.



- открыть окно настроек подключения к базе данных.

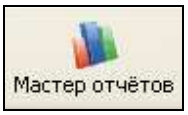


- обновить список компьютеров и их статус из базы данных.

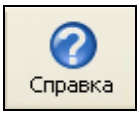


- очистка содержимого логов. Включает в себя следующие пункты:
  - удалить текущую запись,
  - очистить выбранную категорию,
  - очистить все логи пользователя.

- открыть окно истории активного оповещения.



- открыть окно мастера отчетов.



- вызов файла справки.

- выйти из программы.

6.4 Поиск по логам

Начиная с версии 2.0, в LanAgent имеется возможность поиска по содержимому логов. Для этого необходимо перейти на интересующую закладку (например закладку **"Программы"**) и щелкнуть мышкой на таблицу истории, далее нажать на клавиатуре **<Ctrl>+<F>**. Перед Вами появится окно поиска. Так, применимо к закладке **"Программы",** оно будет иметь следующий вид:

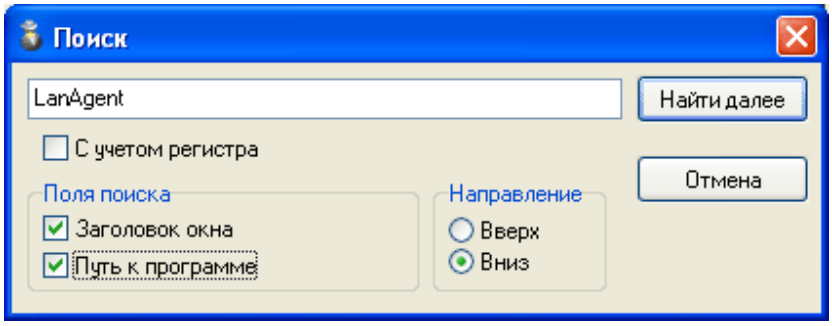


Рис. 6.16 – Диалог поиска по логам

В нем потребуется задать текст для поиска, а также указать поля для поиска (в данном случае это **"Заголовок окна"** и **"Путь к программе"**). Поиск может вестись в двух направлениях: вверх или вниз относительно выделенной строки истории. Кроме того, поиск может производиться с учетом или без учета регистра.

Для начала поиска, нажмите кнопку **"Найти далее"**. Если в истории есть строки, удовлетворяющие критериям поиска, то будет осуществлен переход на ближайшую найденную строку. Чтобы продолжить поиск с заданными критериями, нажмите клавишу **<F3>**. Если больше нет записей, соответствующих критериям поиска, то выдастся соответствующее сообщение: "Искомого текста не найдено".

6.5 Активное оповещение

Служит для оперативного оповещения специалиста службы безопасности о нарушениях заданных политик безопасности. Полученные события отображаются в специальном окне истории активного оповещения (см. рисунок ниже). Настроить активное оповещение (для каких событий его производить) можно индивидуально для каждого компьютера на закладке «Агенты» программы LanAgent Admin. Подробно о настройках можно посмотреть в разделе 5.3.2.

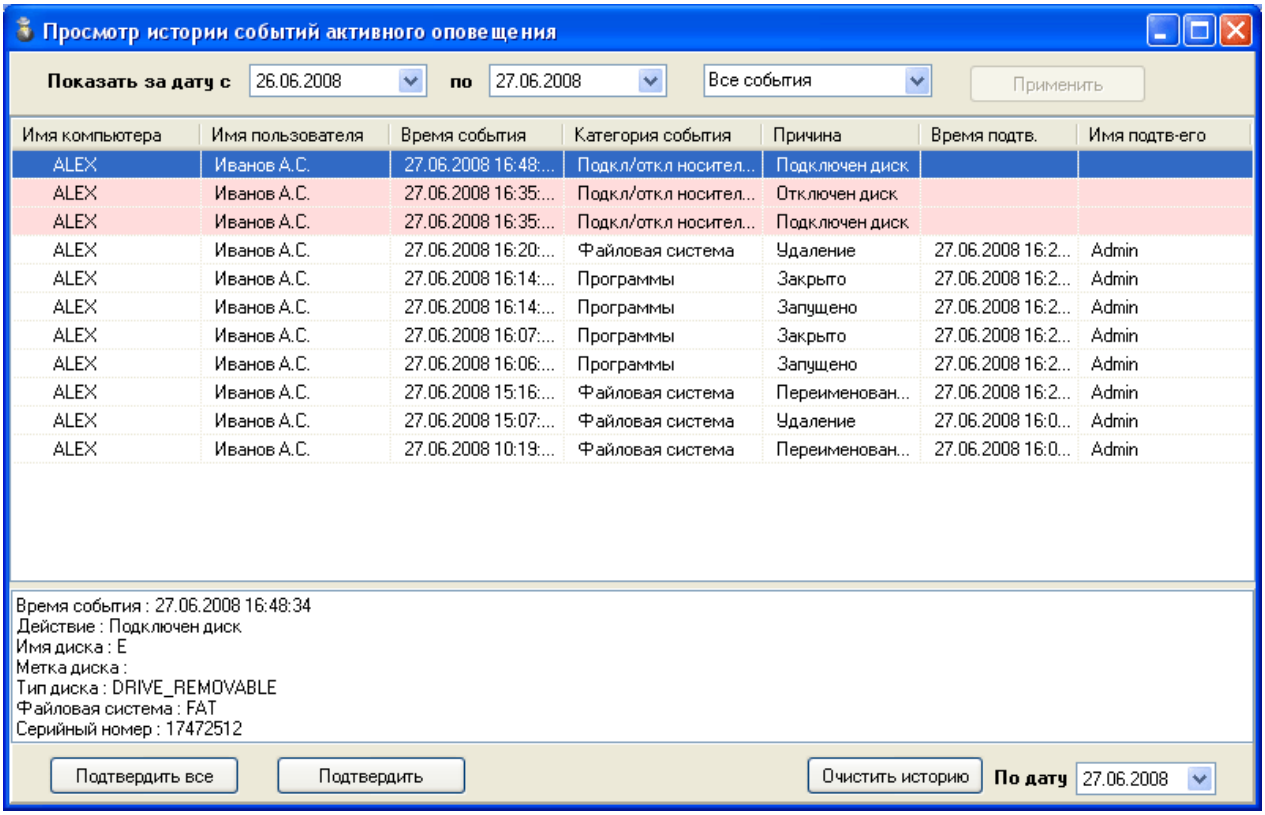


Рис. 6.17 – Окно истории активного оповещения

В верхней части окна расположена панель выбора периода просмотра истории и типа событий. По-умолчанию отображаются все события за текущий день. Возможные типы событий: Все события, Только подтвержденные, Не подтвержденные.

Для каждого пришедшего события, в таблице отображаются: имя компьютера, на котором оно произошло; Имя пользователя, который за данным компьютером работал в тот момент; Время возникновения события; Категория события (Установка/удаление программ, Подкл/откл носителей информации, Файловая система и т.д.); Причина события (т.е что непосредственно произошло: Подключение диска, Установка программы, Отключение диска, ...); Время подтверждения (здесь фиксируется момент времени, когда специалист безопасности просмотрел данное событие и подтвердил его (нажатием кнопки "Подтвердить")); Имя подтвердившего.

Просмотреть более подробную информацию по конкретной записи можно перейдя на нее в списке.

Любое пришедшее событие требует подтверждения (квитирования). Смысл данного действия в том, чтобы обеспечить гарантированную доставку информации непосредственно до специалиста безопасности, который легко сможет увидеть какие сообщения он уже просматривал, а какие еще нет. Кроме того, теперь он не сможет просто проигнорировать сообщение, т.к. кроме информации о самом событии также хранится информация и о времени его подтверждения.

В самой нижней части окна расположена панель управления, позволяющая производить подтверждение (квитирование) событий (кнопки "Подтвердить" и "Подтвердить все") и, при необходимости, очищать историю оповещения по указанную дату (кнопка "Очистить историю").

6.6 «Светофор» безопасности

Призван облегчить процедуру контроля за соблюдением политик безопасности и политик использования компьютерной техники. Смысл его сводится к следующему: для контролируемых компьютеров задаются наборы правил, позволяющих оценить степень опасности конкретных действий пользователей по трем градациям: "зеленый", "желтый", "красный". И далее, при совершении пользователем этих действий, в окне списка компьютеров рядом с названием компьютера отображается статус его безопасности. О самой процедуре назначения правил можно прочитать в разделе 4.8.

Сбросить статус опасности компьютера до "зеленого" можно, выбрав соответствующий пункт выпадающего меню (вызываемого нажатием правой клавиши мыши) "**Сбросить уровень опасности до "зеленого"**", на строке с нужным компьютером.

Как видно из приведенного ниже рисунка, у одного или нескольких пользователей из группы "Программисты" имеются значительные нарушения, поэтому статус опасности группы "красный".

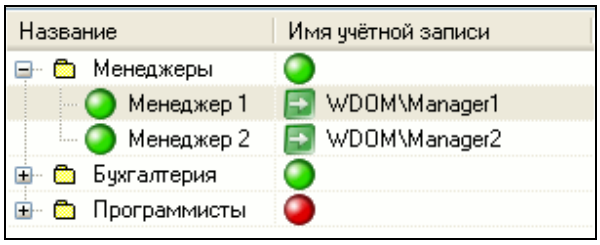


Рис. 6.18 – «Светофор» списка компьютеров

Также "светофор" отображается и для групп (подразделений). Статус группы равен наибольшему статусу опасности из входящих в нее компьютеров. Как видно из рисунка, для групп значок светофора размещается в колонке "Имя компьютера".

При просмотре логов компьютера с нарушением, строки событий, нарушающие правила, имеют соответствующий значок и подкраску (см рисунок). А перед именем закладки, содержащей записи с нарушением стоит восклицательный знак.

Время	Категория	Действие	Заголовок окна	Путь к программе	Имя пользователя
13.10.2009 18:12:59	Система	Закрыто	Мастер нового оборудова...	C:\WINDOWS\system32\r...	SYSTEM
13.10.2009 18:12:53	Система	Запущено	Мастер нового оборудова...	C:\WINDOWS\system32\r...	SYSTEM
13.10.2009 18:11:31	Проводник	Запущено	Мой компьютер	C:\WINDOWS\Explorer.EXE	SYSTEM
13.10.2009 18:09:51	Система	Запущено	Управление компьютером	C:\WINDOWS\system32\m...	SYSTEM
13.10.2009 18:07:48	Другое	Закрыто	Сапер	C:\WINDOWS\system32\w...	SYSTEM
13.10.2009 18:07:47	Другое	Запущено	Сапер	C:\WINDOWS\system32\w...	SYSTEM
13.10.2009 18:07:33	Другое	Закрыто	Калькулятор	C:\WINDOWS\system32\c...	SYSTEM
13.10.2009 18:07:31	Другое	Запущено	Калькулятор	C:\WINDOWS\system32\c...	SYSTEM

Рис. 6.19 – «Светофор» событий в логах

Таким образом, при правильно подобранном наборе правил, снижается необходимость просмотра логов каждого пользователя.

Внимание! "Светофор" отображает статус безопасности для компьютеров на момент последнего обновления логов!

6.7 Настройка LanAgent View

В данный раздел можно попасть, нажав кнопку "Настройки" в панели инструментов.

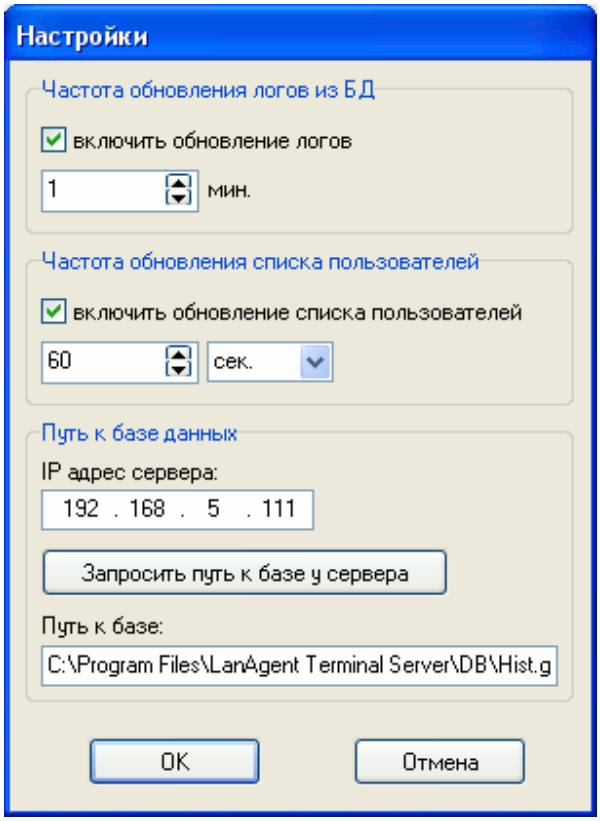


Рис. 6.20 – Настройки программы LanAgent View

Включить обновление логов - установите эту галочку, если хотите чтобы программа автоматически подгружала из базы данных новые собранные логи для выбранного компьютера. Ниже указывается периодичность подгрузки новых логов. Данная опция не является необходимой, т.к. при выборе компьютера для просмотра (двойном щелке левой клавиши мыши по нему в списке мониторинга) будет итак загружена для него полная информация из базы данных.

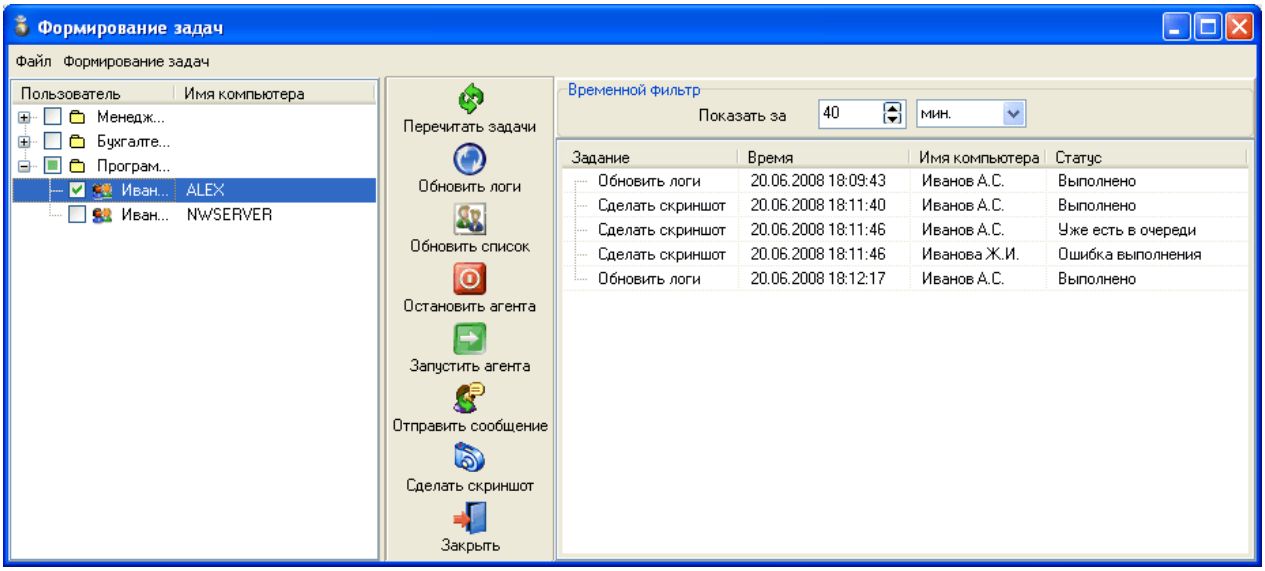
Включить обновление списка пользователей - установите эту галочку, если хотите чтобы программа автоматически производила обновление списка пользователей из базы данных. При этом будет происходить также и обновление статуса для компьютеров. Ниже указывается периодичность обновления списка.

Путь к базе данных - здесь задается путь по которому размещена база данных LanAgent. Он состоит из 2-х частей: ip адреса (или имени) компьютера, на котором расположена база и пути к каталогу, в котором она непосредственно расположена.

После изменения настроек нажмите кнопку "Применить", если хотите сохранить сделанные изменения, или нажмите кнопку "Отмена", если хотите вернуть старые настройки.

6.8 Формирование задач

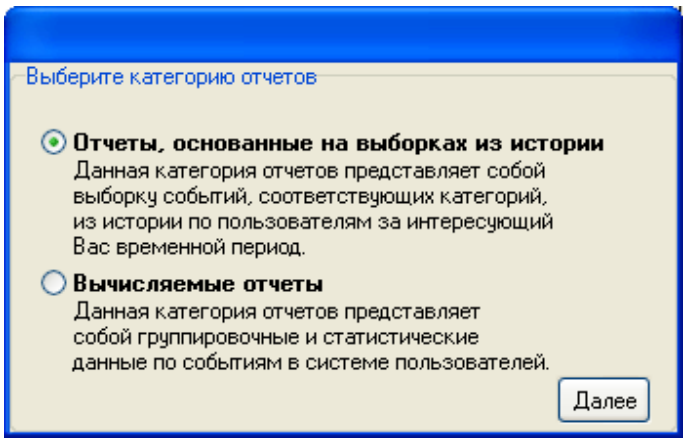
Окно формирования задач можно открыть, нажав кнопку "**Формирование задач**" в панели инструментов или выбрав соответствующий пункт в выпадающем меню «Управление».



В левой части окна расположен список контролируемых компьютеров, доступных для просмотра данным специалистом безопасности.
В правой части окна отображается ход выполнение задач.
Для постановки новой задачи, выберите из списка требуемый компьютер(ы) и нажмите кнопку с соответствующей задачей.

6.9 Составление отчетов

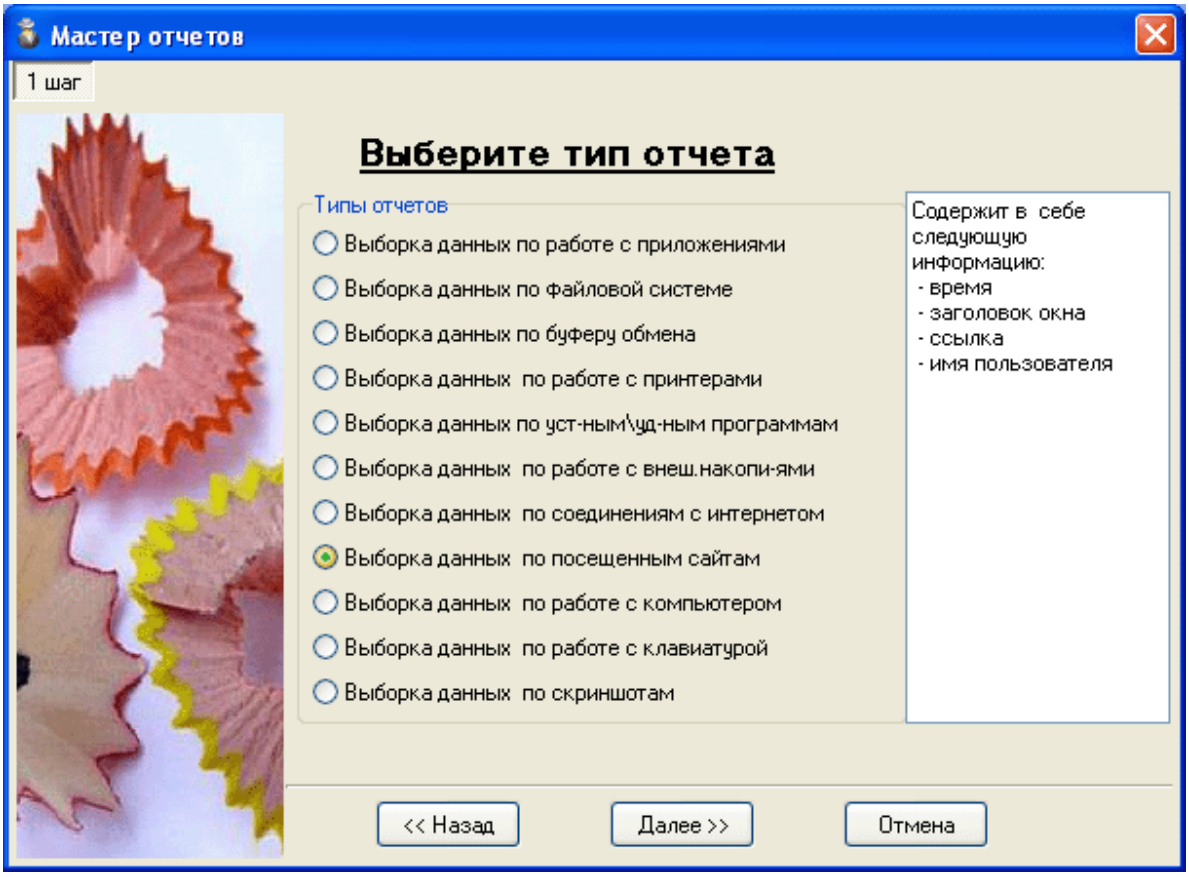
При вызове мастера отчетов откроется следующее окно:



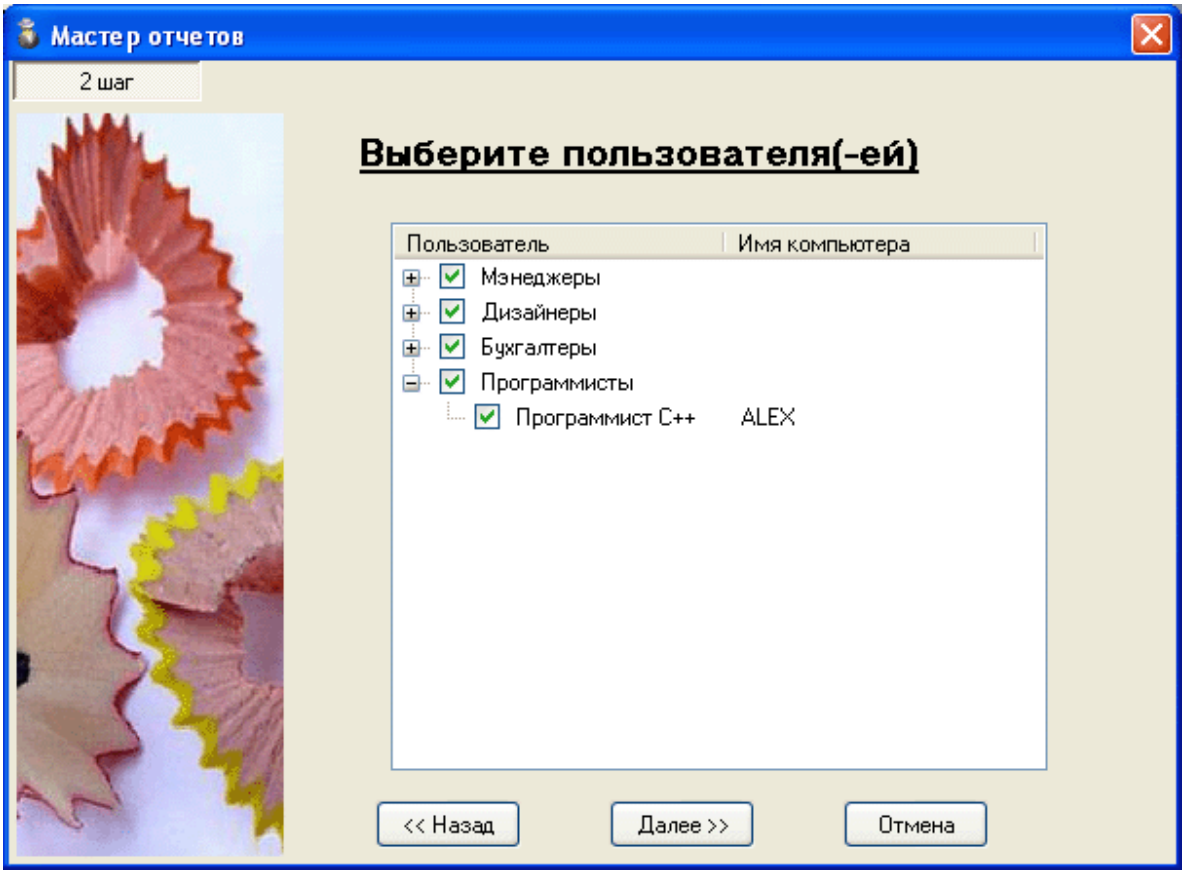
Как видно из рисунка, отчеты имеются 2-х категорий, каждая из которых содержит свой набор отчетов: это **«Вычисляемые отчеты»** (полученные на основе статистического анализа информации) и **«Отчеты, основанные на выборках из истории»**, которые по структуре повторяют выбираемые данные в окне просмотра логов.

6.9.1 Отчеты - выборки

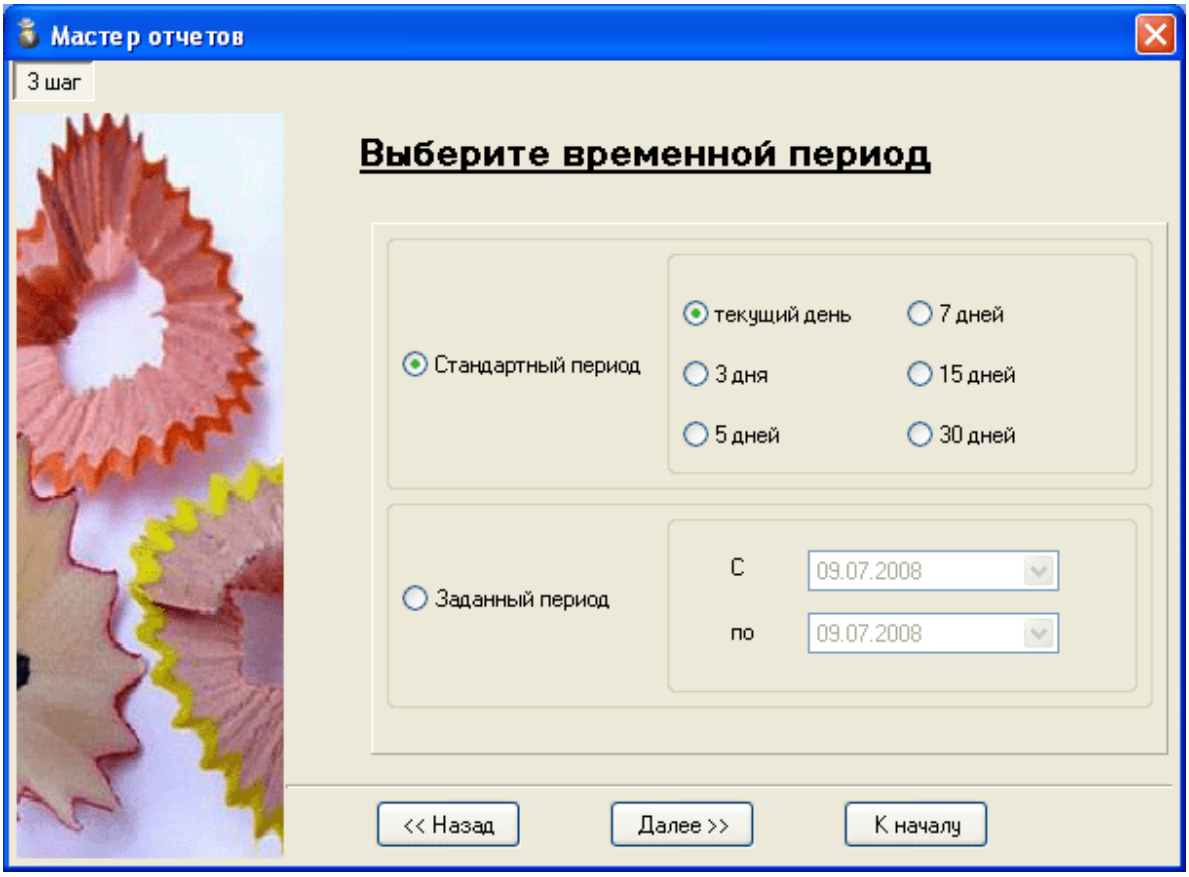
Набор отчетов-выборок имеет следующий вид:



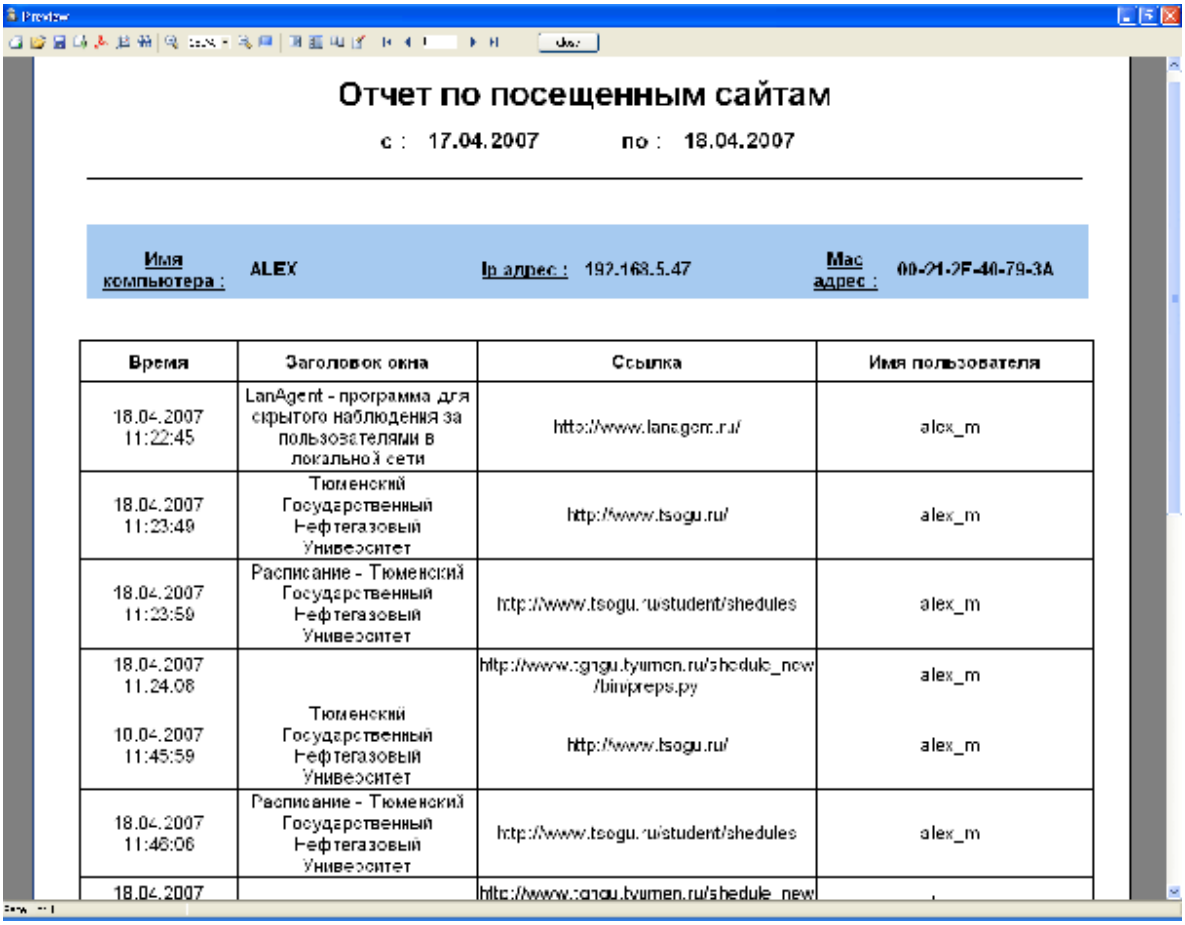
Выберите из списка нужный тип отчета и нажмите кнопку **"Далее"**. В открывшемся окне укажите компьютеры, для которых будет составляться отчет.



Далее выберите период отчета и нажмите кнопку **"Показать"** для создания отчета.



Ниже представлен пример отчета по посещенным сайтам.



Отчет по посещенным сайтам

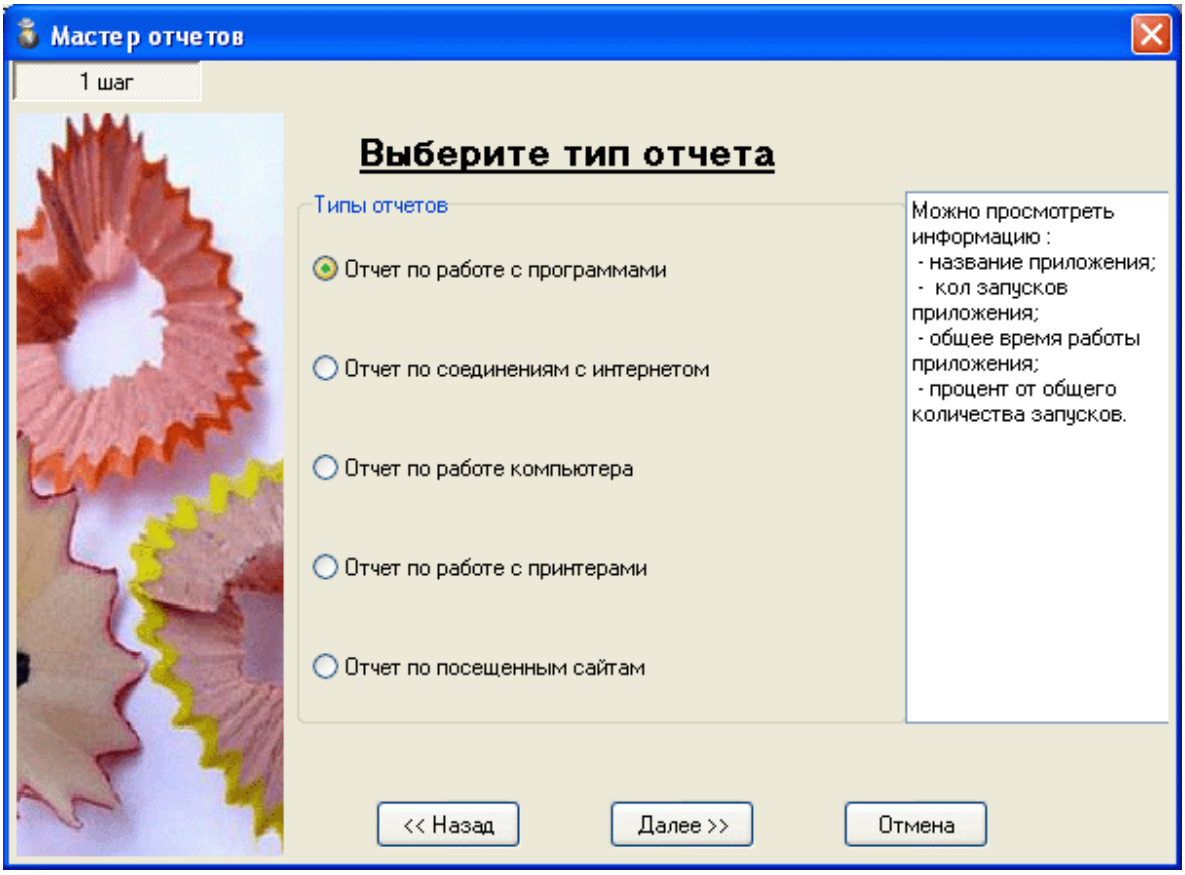
с : 17.04.2007 по : 18.04.2007

Имя компьютера : ALEX Ip адрес : 192.168.5.47 Mac адрес : 00-21-2F-40-79-3A

Время	Заголовок окна	Ссылка	Имя пользователя
18.04.2007 11:22:45	LanAgent - программа для скрытого наблюдения за пользователями в локальной сети	http://www.lanagent.ru/	alex_m
18.04.2007 11:23:49	Тюменский Государственный Нефтегазовый Университет	http://www.tsogu.ru/	alex_m
18.04.2007 11:23:59	Расписание - Тюменский Государственный Нефтегазовый Университет	http://www.tsogu.ru/student/shedules	alex_m
18.04.2007 11.24.08 10.04.2007 11:45:59	Тюменский Государственный Нефтегазовый Университет	http://www.sgngu.tyumen.ru/shedule_new/bin/preps.py http://www.tsogu.ru/	alex_m alex_m
18.04.2007 11:46:06	Расписание - Тюменский Государственный Нефтегазовый Университет	http://www.tsogu.ru/student/shedules	alex_m
18.04.2007		http://www.sgngu.tyumen.ru/shedule_new/	

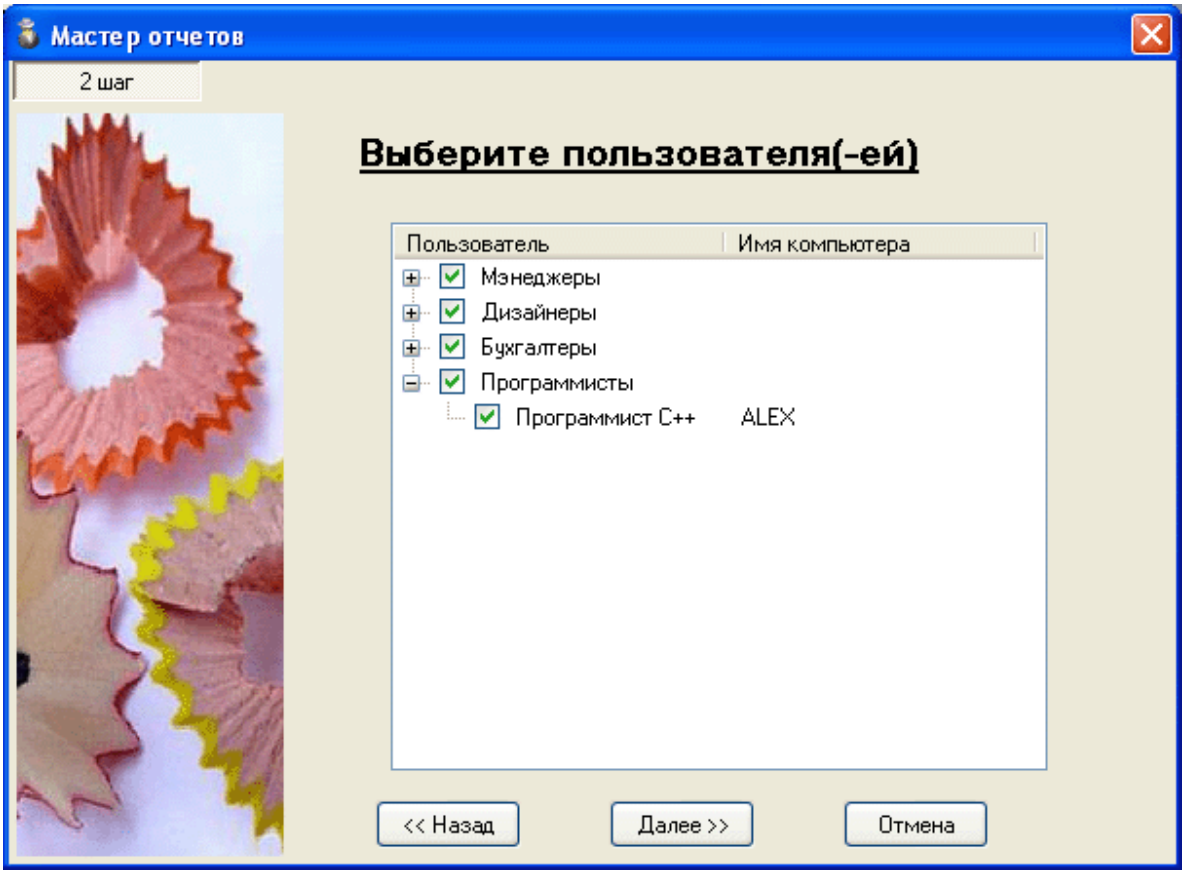
6.9.2 Вычисляемые отчёты

Набор вычисляемых отчетов имеет следующий вид:

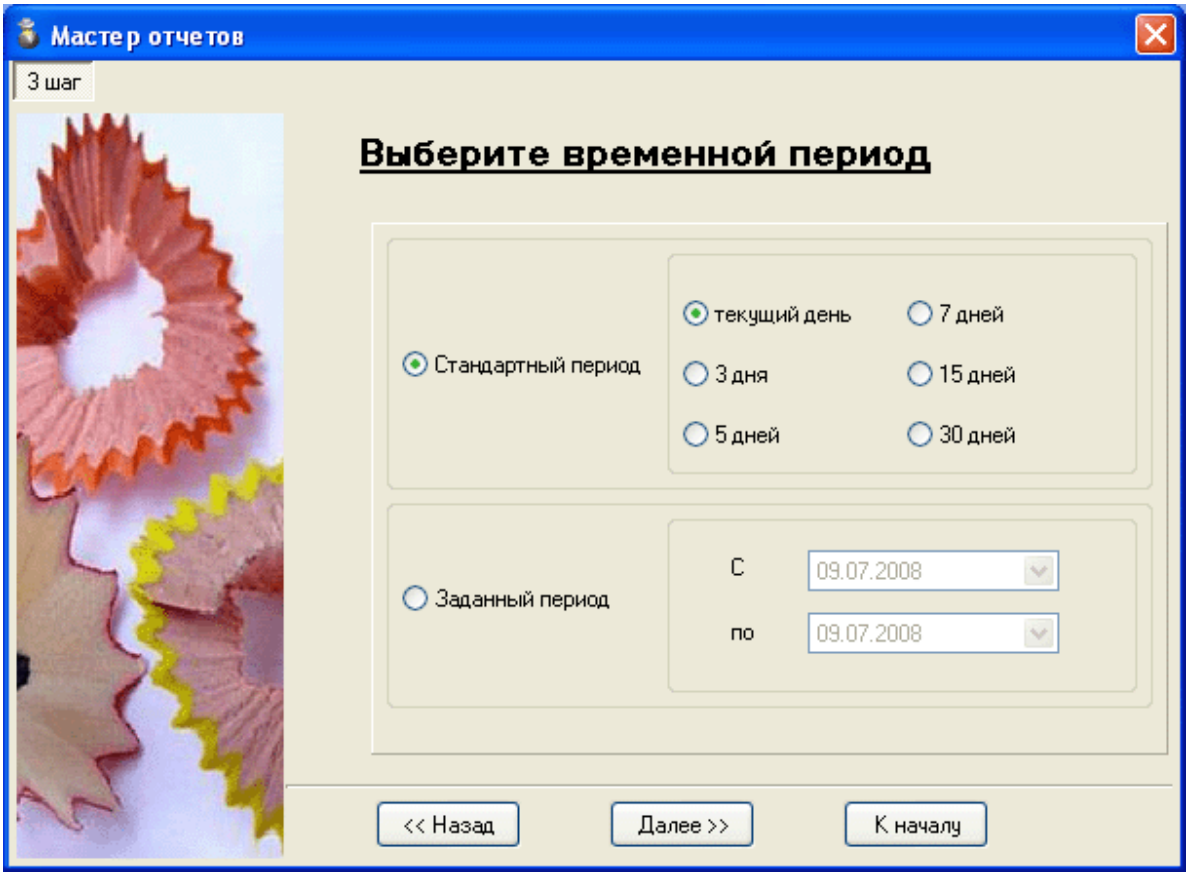


Это статистика по работе программ (содержит следующие данные: названия, количество запусков, общее время работы, процент от общего числа запусков); Статистика соединений с Интернет; Статистика работы с компьютером (время работы, время простоя, количество вкл/выкл); Статистика использования принтеров (на каком принтере сколько раз печатали, какое количество страниц); и статистика посещения web-сайтов (какой адрес сколько раз посещался, процент от общего числа посещений).

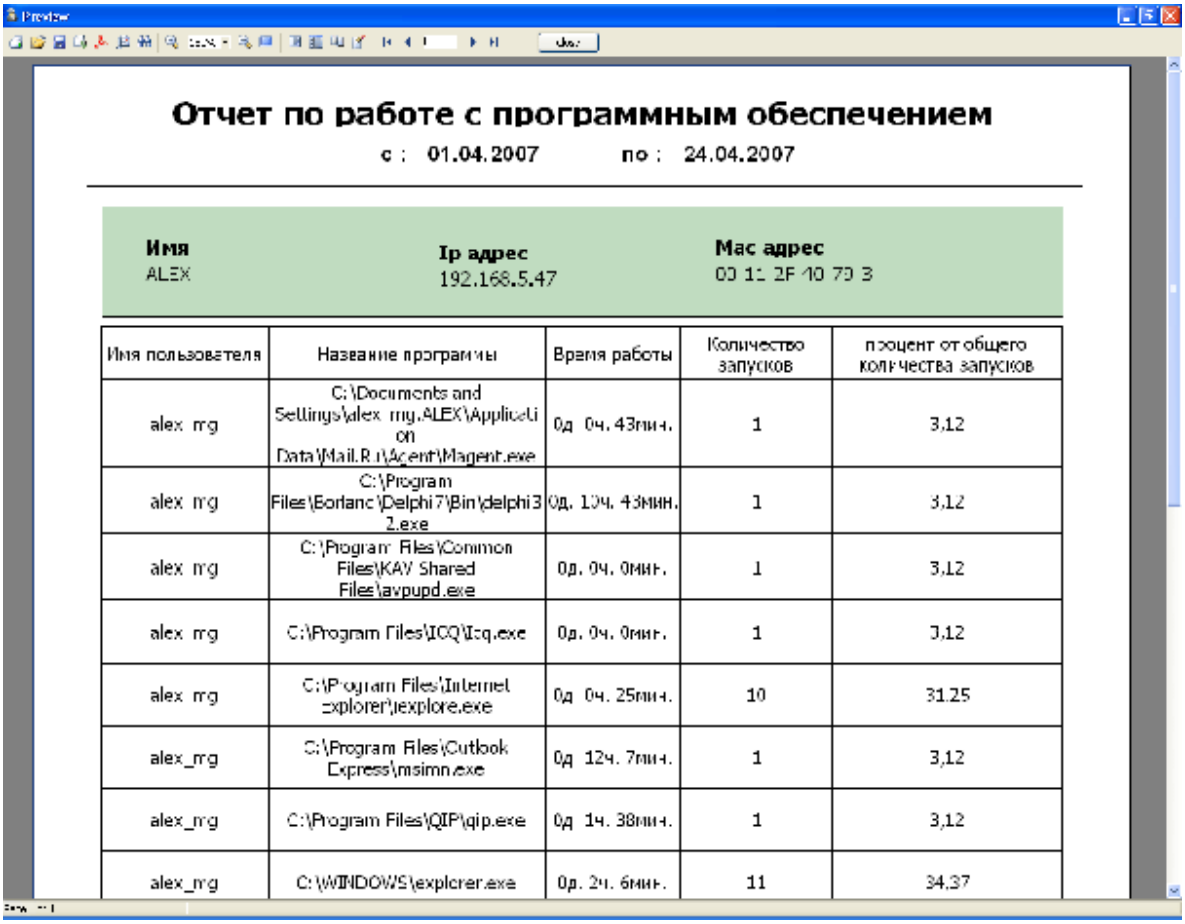
Выберите из списка нужный тип отчета и нажмите кнопку **"Далее"**. В открывшемся окне укажите компьютеры, для которых будет составляться отчет.



Далее выберите период отчета и нажмите кнопку **"Показать"** для создания отчета.



Ниже представлен пример вычисляемого отчета по программам.



Отчет по работе с программным обеспечением

с : 01.04.2007 по : 24.04.2007

Имя	Ip адрес	Mac адрес
ALEX	192.168.5.47	00 11 2F 40 7D 3

Имя пользователя	Название программы	Время работы	Количество запусков	процент от общего количества запусков
alex_mg	C:\Documents and Settings\alex_mg.ALEX\Application Data\Mail.Ru\Agent\Magent.exe	0д. 0ч. 43мин.	1	3,12
alex_mg	C:\Program Files\Borland\Delphi7\Bin\delphi32.exe	0д. 10ч. 43мин.	1	3,12
alex_mg	C:\Program Files\Common Files\KAV Shared Files\avpupd.exe	0д. 0ч. 0мин.	1	3,12
alex_mg	C:\Program Files\ICQ\Icq.exe	0д. 0ч. 0мин.	1	3,12
alex_mg	C:\Program Files\Internet explorer\iexplore.exe	0д. 0ч. 25мин.	10	31,25
alex_mg	C:\Program Files\Outlook Express\msimn.exe	0д. 12ч. 7мин.	1	3,12
alex_mg	C:\Program Files\QIP\qip.exe	0д. 1ч. 38мин.	1	3,12
alex_mg	C:\WINDOWS\explorer.exe	0д. 2ч. 6мин.	11	34,37

7 Работа с LanAgent Sheduler (планировщиком отчетов)

Интерфейс программы LanAgent Sheduler имеет следующий вид:

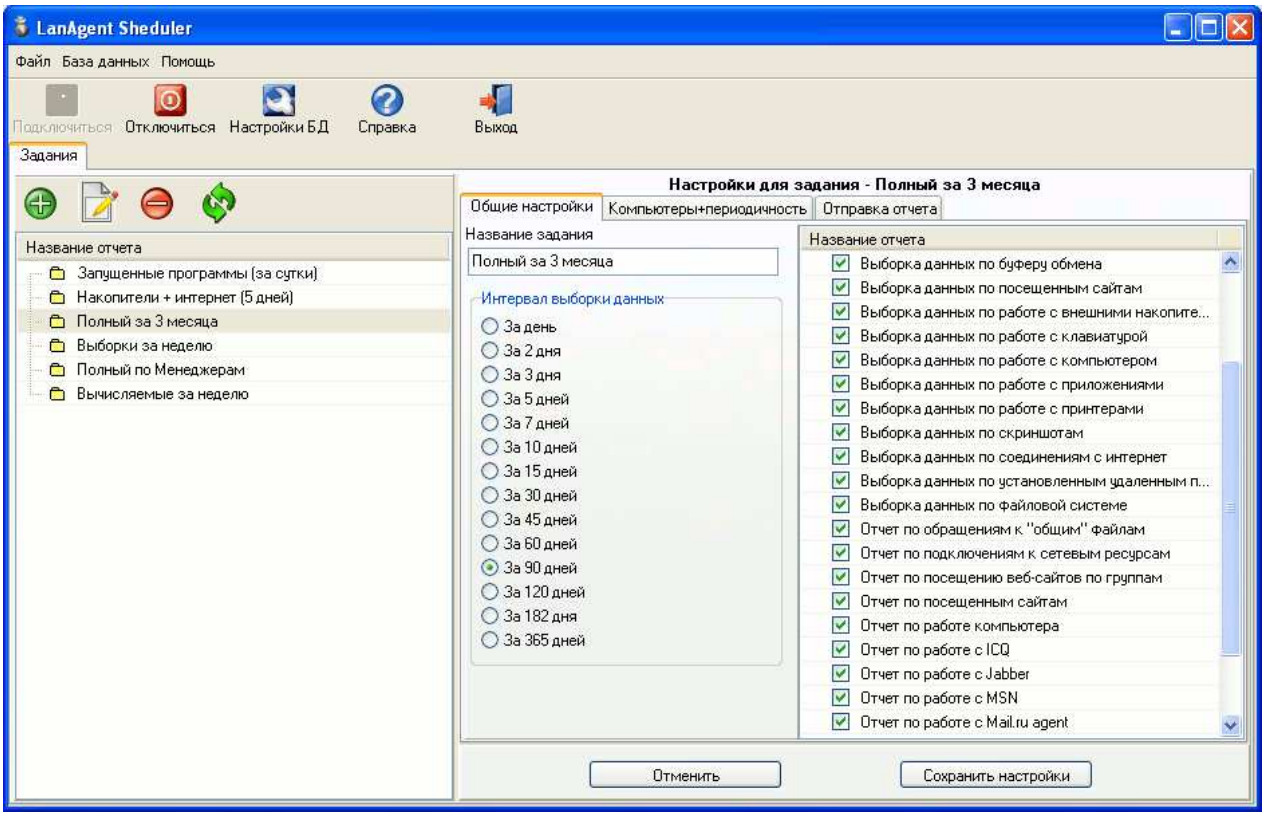
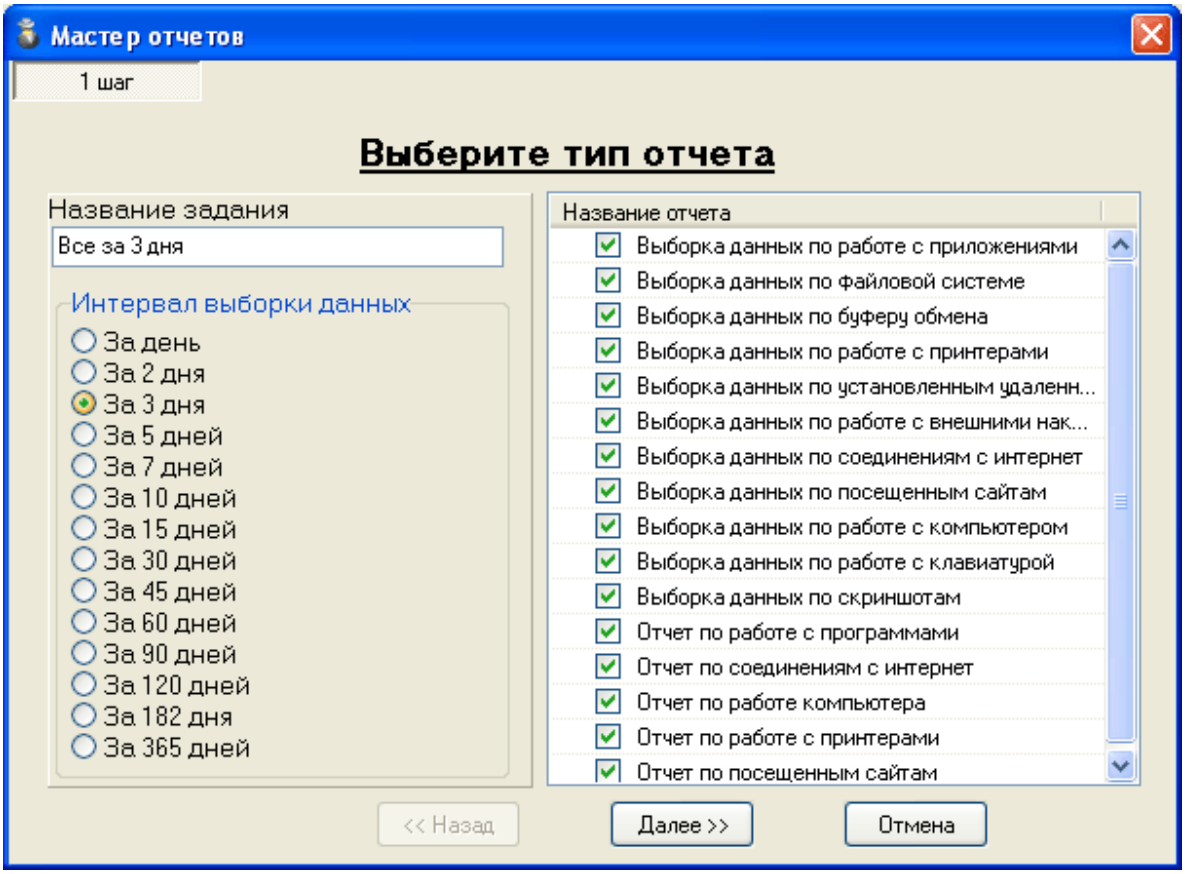


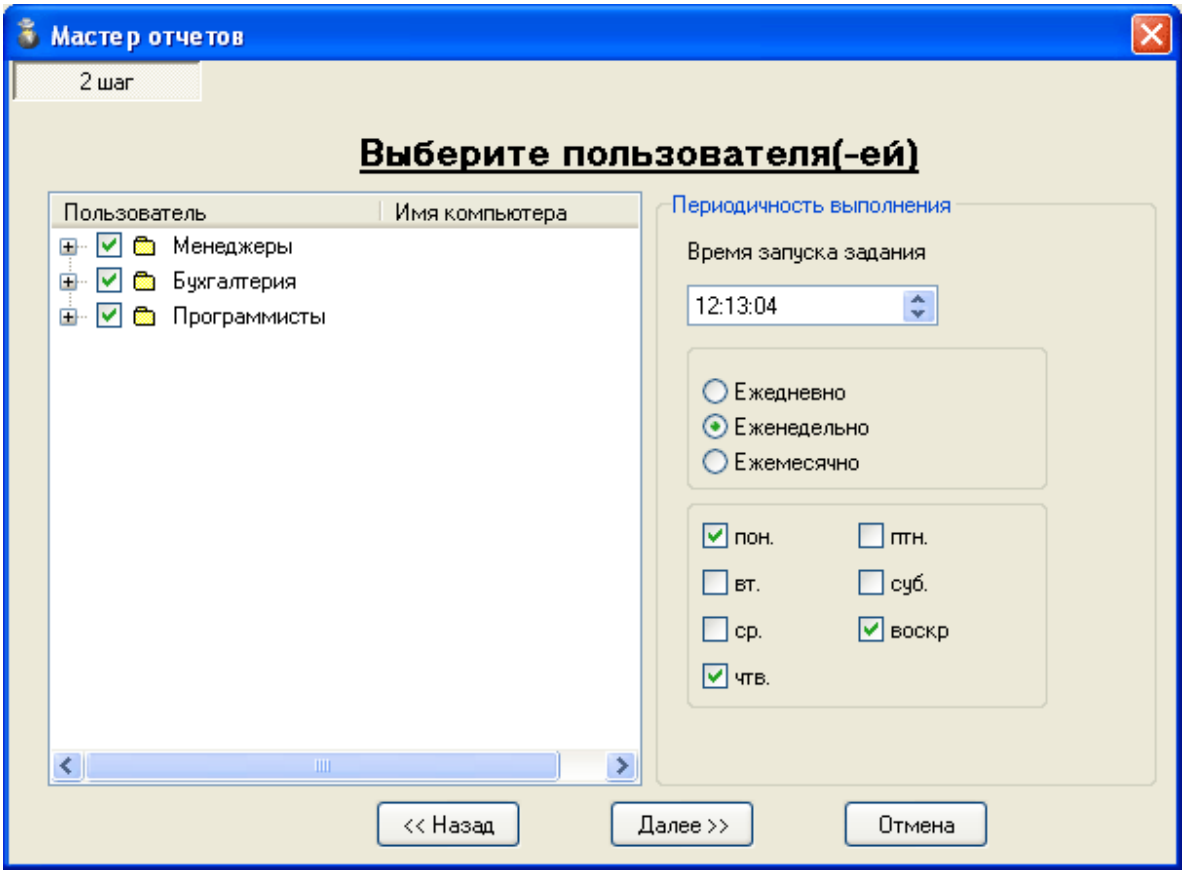
Рис. 7.1 – Главное окно программы

В левой части окна расположен список запланированных отчетов. Для редактирования уже созданного заданий, необходимо выбрать его в данном списке двойным нажатием левой клавиши мыши.

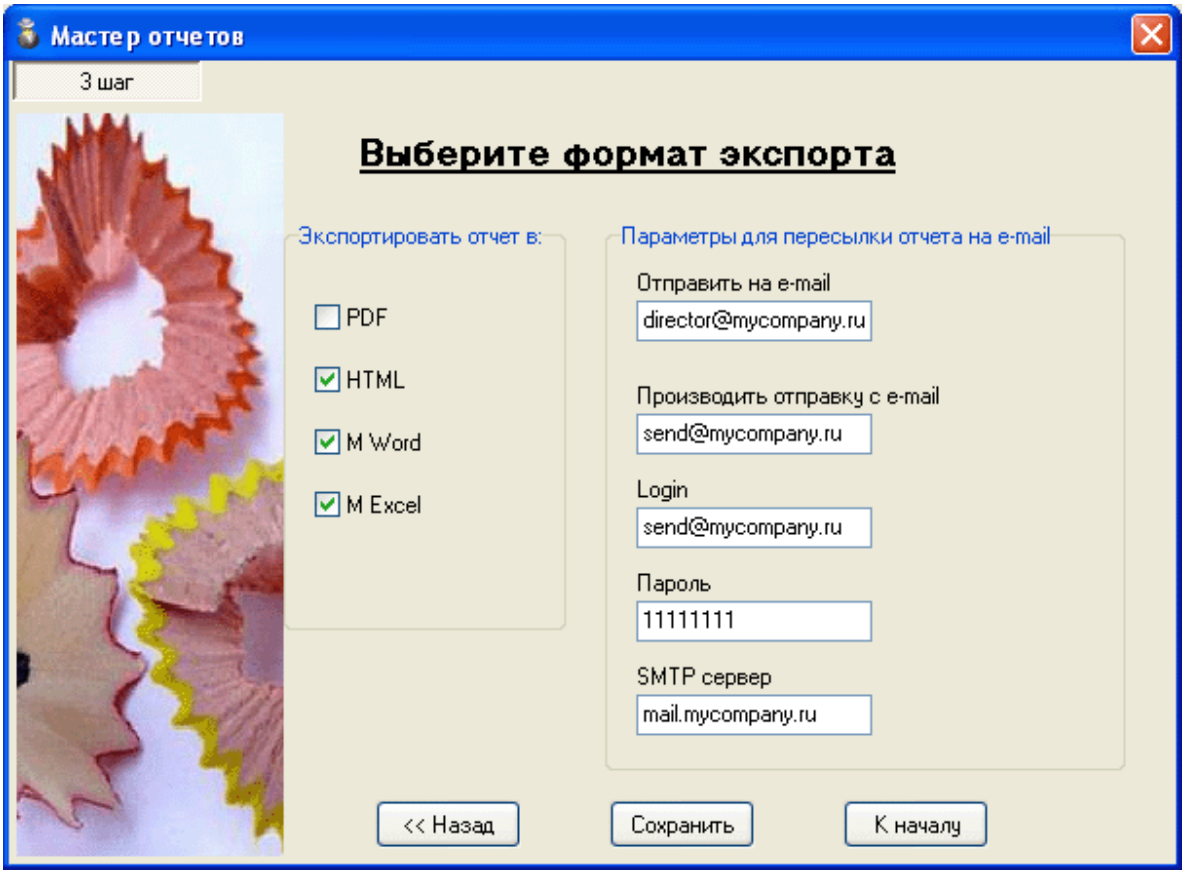
Для создания нового – воспользуйтесь кнопкой панели инструментов. При этом откроется следующий диалог добавления:



Заполните в нем название задания, выберите интервал, за который будут выбираться данные из базы данных, а также укажите какие именно отчеты требуется сформировать. По завершению выбора, нажмите кнопку «Далее»



На 2-ом шаге, необходимо выбрать компьютеры, данные по которым будут внесены в отчет, время запуска задания и периодичность его выполнения.



И, наконец, завершающим этапом является указание в какие форматы конвертировать созданный отчет и на какой e-mail произвести его отправку. Если нет необходимости в отправке отчета, то оставьте параметры e-mail пустыми.

8 Удаление программы

Если возникла необходимость произвести удаление программы, например при переходе на следующую версию программы, то это производится отдельно для серверной части, программ Admin, Viewer, Sheduler.

8.1 Удаление Серверной части, Admin, View, Sheduler

Для удаления любой из перечисленных в заголовке программ, можно использовать стандартные средства Windows, также как и для любого другого приложения. Для этого в "Панели управления" ("Control Panel") выбрать пункт "Установка и удаление программ" ("Add and remove programs"), выберите в списке соответствующую программу и нажмите кнопку "Удалить" ("Remove").

8.2 Удаление учетных записей из списка мониторинга

Для удаления учетной записи пользователя из списка мониторинга, запустите программу LanAgent Admin, выберите на закладке «Агенты» из списка нужную строку и нажмите в панели инструментов кнопку «Удалить» .

9 Техническая поддержка

Получить полную техническую поддержку можно у нашего представителя, через которого была приобретена программа LanAgent. Посмотреть список наших представителей можно на сайте www.lanagent.ru в разделе «Контакты».

Ниже представлены варианты реализации наиболее типичных действий в программе LanAgent, а также ответы на часто задаваемые вопросы.

9.1 Типичные действия

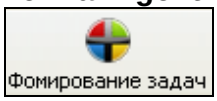
1 Добавление учетной записи пользователя в список мониторинга

Данная возможность реализуется в программе **LanAgent Admin**. Для добавления нового пользователя в список мониторинга, необходимо нажать кнопку "Добавить" панели инструментов LanAgent или выбрать соответствующий пункт "Добавить пользователя" из меню "Файл".

2. Удаление пользователя из списка мониторинга

Данная возможность реализуется в программе **LanAgent Admin**. Для удаления определенного компьютера из списка мониторинга, необходимо встать на строку, соответствующую данному пользователю в списке и нажать кнопку "Удалить" панели инструментов LanAgent Admin или выбрать соответствующий пункт "Удалить пользователя" из меню "Файл".

3. Запуск или остановка мониторинга на нужном компьютере

Данная возможность реализуется через интерфейс формирования задач в программе **LanAgent View**. Для вызова диалога формирования задач, нажмите кнопку 

панели инструментов. В открывшемся окне выберите требуемые компьютеры и щелкните на кнопке "Запустить" (если хотите запустить мониторинг) или "Остановить" (если хотите его остановить). Процесс отработки задания будет отображаться в правой части окна.

4. Обновление логов

Данное действие, также как и запуск/останов мониторинга осуществляются через диалог формирования задач программы LanAgent View. Запустите его, выберите требуемые компьютеры, а затем нажмите кнопку "Обновить логи". Процесс отработки задания будет отображаться в правой части окна.

5. Очистка логов

В программе LanAgent имеется возможность очистки выбранной категории логов (например "Программы") для выбранного пользователя; очистки всех логов для выбранного пользователя; очистка всех логов для всех пользователей. Для выбора любого из этих вариантов можно воспользоваться кнопкой "Очистить", а можно выбрать соответствующий пункт в меню "Управление". **Внимание!** Производить очистку логов могут только пользователи, имеющие соответствующие права.

6. Сбросить статус опасности компьютера до "зеленого"

Сбросить статус опасности компьютера до "зеленого" можно, выбрав в окне списка компьютеров соответствующий пункт выпадающего меню (вызываемого нажатием правой клавиши мыши) "**Сбросить уровень опасности до "зеленого""**, на строке с нужным компьютером.

9.2 Часто задаваемые вопросы

1. Как просмотреть снимки экранов мониторов (скриншоты)?

Выберите интересующего вас пользователя из списка мониторинга двойным щелчком левой клавиши мыши. Откройте закладку «Скриншоты» в окне просмотра статистики активности и щелкните дважды в таблице по той записи, для которой хотите просмотреть скриншот. Появится окно для просмотра скриншотов.

2. В каких операционных системах может работать программа?

Программа работает на серверных операционных системах семейства Windows:

- Windows 2003 Server
- Windows 2008 Server

3. Каковы системные требования программы LanAgent?

Минимальные требования:

- Операционная система: Windows 2003 Server/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 Server/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).

4. Как установить срок хранения логов в базе?

Это можно сделать на закладке «Основные» программы LanAgent Admin. Подробнее смотрите пункт 5.2.