Network
PROFI

LanAgent

Владея информацией,
владеешь миром

www.networkprofi.ru

Примечания

Информация об обновлении и сопроводительная информация находится на http://www.lanagent.ru
Если у вас возникли какие-либо вопросы или предложения, пишите на support@lanagent.ru.

Предисловие

Руководство 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 программой LanAgent**, содержит описание основных составных частей программы и инструкцию по реализации ее функциональных возможностей.
- **Техническая поддержка**, координаты службы технической поддержки.
- **Типичные действия**, описание реализации наиболее типичных действий пользователей.

Содержание

1 О продукте LanAgent

1.1 Описание программы LanAgent

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

Возможности программы LanAgent:

- Запоминает запуск и закрытие программ.
- Определяет подключение и отключение носителей информации.
- Делает снимки экранов мониторов.
- Запоминает набираемый на клавиатуре текст.
- Следит за содержимым буфера обмена.
- Перехватывает посещённые сайты.
- Ведет учет соединений с интернет.
- Запоминает установку и удаление программ.
- Ведет статистику создания и удаления файлов.
- Ведет учет документов, отправленных на печать на принтер.
- Отслеживает включение/выключение компьютера.
- Формирует отчёт в html-формате.
- Вся информация хранится централизованно в базе.
- Автоматическое получение статистики от контролируемых компьютеров.
- Информация передаются по сети в зашифрованном виде.
- Возможность отправки текстовых сообщений на компьютер пользователя.

Уникальные особенности программы LanAgent:

- Агенты программы **LanAgent** абсолютно невидимы во всех операционных системах (даже в процессах Windows NT/2000/XP).
- Не видны в автозагрузке.
- При запоминании нажатых клавиш программа различает регистр, а также может запоминать русские буквы.
- При просмотре нажатых клавиш может показывать только символы и не показывать нажатия системных клавиш, что намного удобнее. Например, если были нажаты следующие клавиши:

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

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

  "Это программа LanAgent."

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

1.2 Для кого предназначена программа

LanAgent незаменимый помощник:

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

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

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

1.3 Как работает программа LanAgent

Программа состоит из 2-х частей – пользовательская часть (агент) и администраторская часть. Администраторская часть ставится на компьютер сотрудника, который будет производить контроль, а агенты – соответственно на те компьютеры, которые необходимо контролировать. Агенты осуществляют мониторинг всех действий пользователей, а администраторская часть производит централизованный сбор информации по сети (опрос агентов), чтобы затем администратор программы смог все эти данные просмотреть на своём компьютере и сделать отчёт.

Кроме того, имеется возможность активного оповещения администратора программы о таких опасных действиях пользователей как подключение и отключение носителей информации и установка/удаление программ. Для получения таких оповещений, необходимо чтобы администраторская часть была запущена.

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

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

Обмен информацией производится по протоколу TCP/IP. Вам необходимо знать только ip-адрес компьютера, на котором установлен агент, или сетевое имя компьютера, чтобы администраторская часть программы смогла к нему подключиться. Обмен информацией производится через порт: 7654. Если у вас на компьютере установлен firewall, то вам необходимо открыть этот порт.

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

1.4 Системные требования

Ввиду клиент-серверной архитектуры программы LanAgent требования к аппаратному обеспечению формулируются для каждого компонента отдельно.

Администраторская часть.

Минимальные требования:

- Операционная система: Windows 98/Me/2000/XP.
- Процессор Pentium 3 и выше.
- 128 MB оперативной памяти.
- 30 MB свободного места на диске.

Рекомендуемые требования:

- Операционная система: Windows 98/Me/2000/XP.
- Процессор Pentium 4 с частотой не менее 2 GHz.
- 512 MB оперативной памяти.
- 15 GB свободного места на диске (зависит от количества компьютеров и настроек программы).

Пользовательская часть (агент).

Минимальные требования:

- Операционная система: Windows 98/Me/2000/XP.
- Процессор Pentium 2 и выше.
- 32 MB оперативной памяти.
- 5 MB свободного места на диске.

Рекомендуемые требования:

- Операционная система: Windows 98/Me/2000/XP.
- Процессор Pentium 3 и выше.
- 128 MB оперативной памяти.
- 100 MB свободного места на диске.

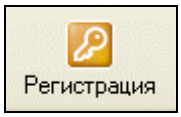
2 Регистрация LanAgent

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.

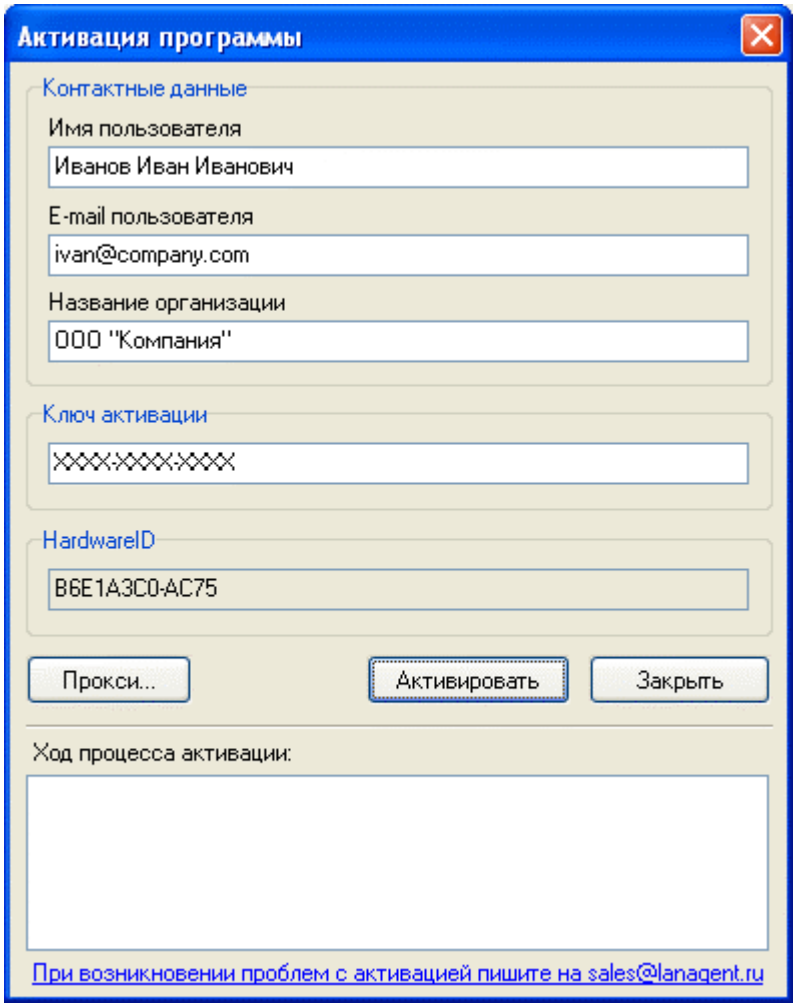


Рис. 1 - Активация программы

4. Нажмите кнопку "Активировать" и подождите некоторое время.
5. Если активация прошла успешно, то программа выдаст соответствующее сообщение.
6. Перезапустите программу.

3 Быстрый запуск

3.1 Установка администраторской части программы

Для установки администраторской (базовой) части программы достаточно запустить файл "admin.exe" на том компьютере, с которого вы собираетесь в дальнейшем производить администрирование, а также просматривать логи, и далее следовать указаниям мастера установки. Следует помнить, что возможности администрирования, а также просмотра логов будут доступны только на том компьютере, на котором установлена базовая часть программы.

3.2 Установка агентов

3.2.1 Локальная установка агентов

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

3.2.2 Удаленная установка агентов

На данный момент реализована для сетей с доменами.

Назначение установки программы

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

Создание распределительного пункта (distribution point)

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

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

Создания объекта групповой политики (GPO)

1. Запустите оснастку **Active Directory – пользователи и компьютеры** (Active Directory Users and Computers).
   *Примечание: Оснастку **Active Directory – пользователи и компьютеры** можно запустить так: Пуск, Программы, Администрирование, Active Directory – пользователи и компьютеры.*

2. В дереве консоли кликните правой клавишей мышки на вашем домене и выберите свойства.
3. Перейдите на вкладку **Групповая политика** и нажмите **Создать**.
4. Напишите желаемое имя вашей политики (например ***LanAgent distribution***) и нажмите **Enter**.
5. Нажмите **Свойства** и перейдите на вкладку **Безопасность**.
6. Отметьте **Применение групповой политики** для необходимой группы, затем нажмите **OK**.

Назначение пакета

1. Запустите оснастку **Active Directory – пользователи и компьютеры** (Active Directory Users and Computers).
2. Кликните правой клавишей мыши на имени вашего домена и выберите **Свойства**.
3. Перейдите на вкладку **Групповая политика** и выбрав нужную политику нажмите **Изменить**.
4. Разверните ветвь **Конфигурация компьютера**, **Конфигурация программ**
5. Кликните правой клавишей мыши на **Установка программ** и выберите **Создать** потом **Пакет**.
6. В открывшемся диалоговом окне введите полный UNC путь к общедоступной папке содержащей нужный Вам MSI пакет. Например ***\\file server\share\user.msi***. Важно что бы имя было в формате UNC.

7. Нажмите **Открыть**.
8. Выберите **Назначенный** и нажмите **OK**. Пакет отобразится на правой панели окна групповых политик.
9. Закройте оснастку групповые политики и нажмите **OK** и выйдете из оснастки **Active Directory – пользователи и компьютеры**. Когда компьютер запустится указанная программа будет установлена.

Переустановка пакета

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

1. Запустите оснастку **Active Directory – пользователи и компьютеры** (Active Directory Users and Computers).
2. Кликните правой клавишей мыши на имени вашего домена и выберете **Свойства**.
3. Перейдите на вкладку **Групповая политика** и выбрав нужную политику нажмите **Изменить**.
4. Разверните ветвь **Конфигурация компьютера**, **Конфигурация программ**
5. Выберите ту программу, которую вы желаете обновить и кликнете на ней правой клавишей мыши в появившемся окне выберите **Все задачи**, **Развернуть приложение заново**.
6. Нажмите **Да**.

Ссылки

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

302430 - HOW TO: Assign Software to a Specific Group By Using a Group Policy
(http://support.microsoft.com/default.aspx/kb/302430/)
314934 - HOW TO: Use Group Policy to Remotely Install Software in Windows 2000
(http://support.microsoft.com/default.aspx/kb/314934/)
816102 - How to use Group Policy to remotely install software in Windows Server 2003
(http://support.microsoft.com/default.aspx/kb/816102/)

3.3 Создание списка компьютеров для мониторинга

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

При этом откроется следующее диалоговое окно:

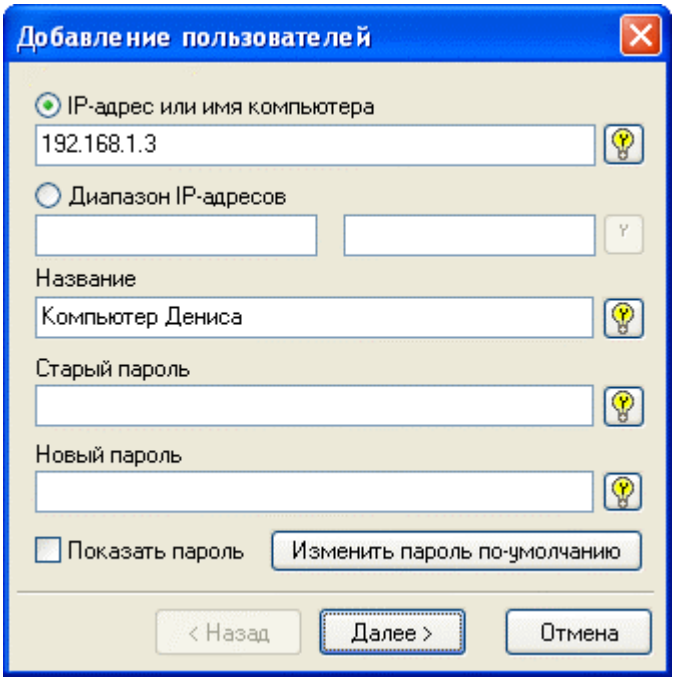


Рис. 3 - Добавление компьютера в список мониторинга

Добавить компьютеры в список можно 2-мя способами:

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

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

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

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

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

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

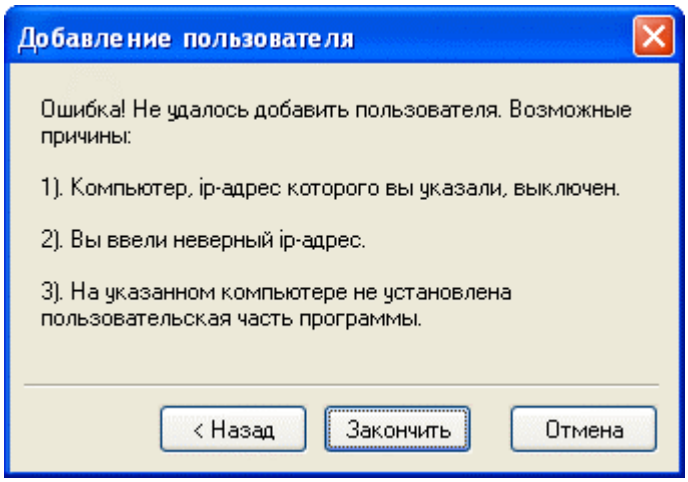


Рис. 4 – Ошибка добавления в список

Чтобы изменить параметры подключения, нажмите кнопку "Назад".

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

3.4 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:

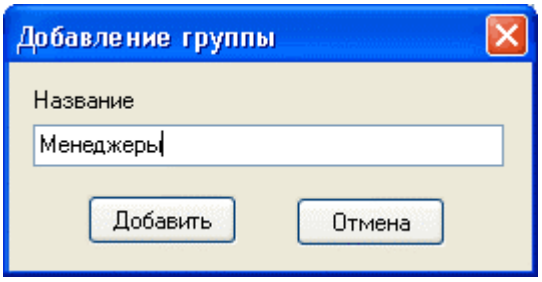


Рис. 5 – Добавление группы пользователей

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.

4 Работа с программой

Интерфейс программы LanAgent включает в себя следующие элементы:

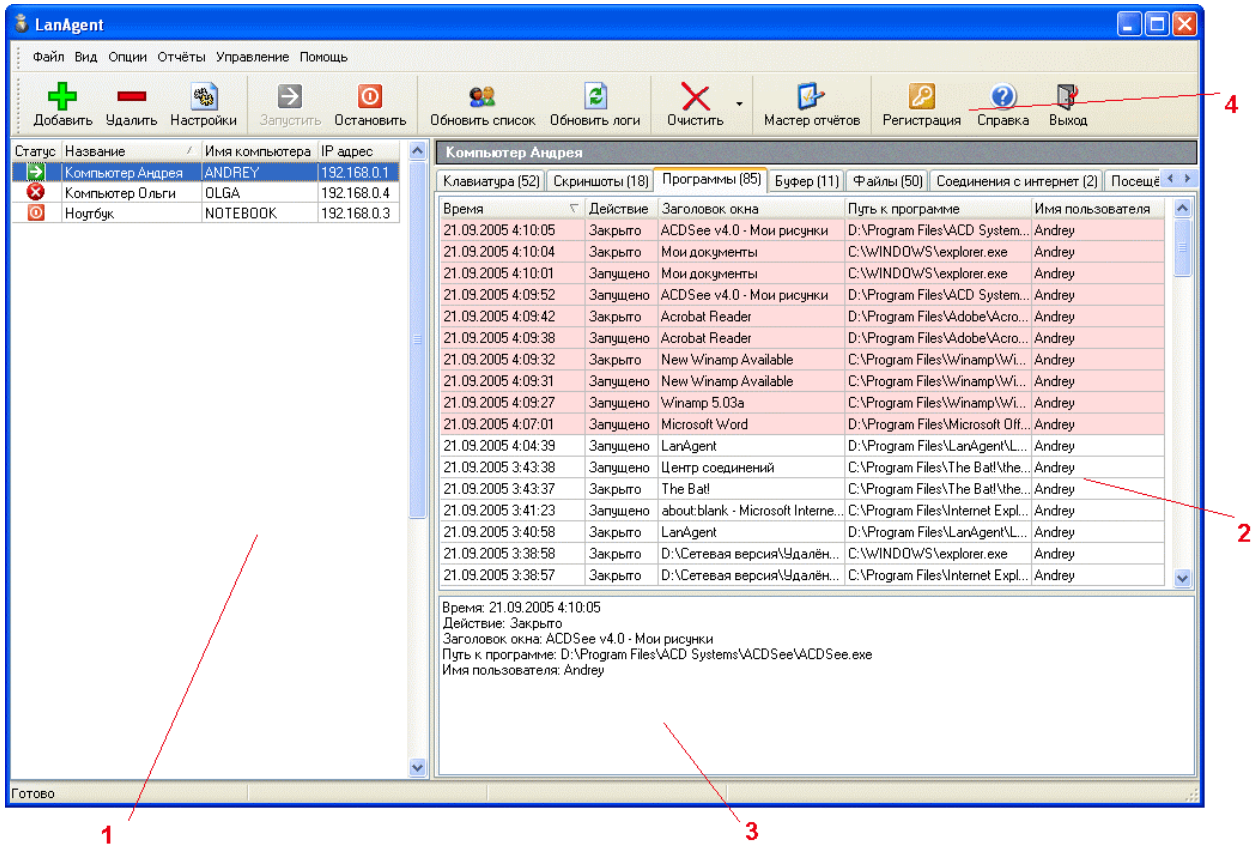


Рис. 6 – Главное окно программы

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

4.1 Список компьютеров для мониторинга

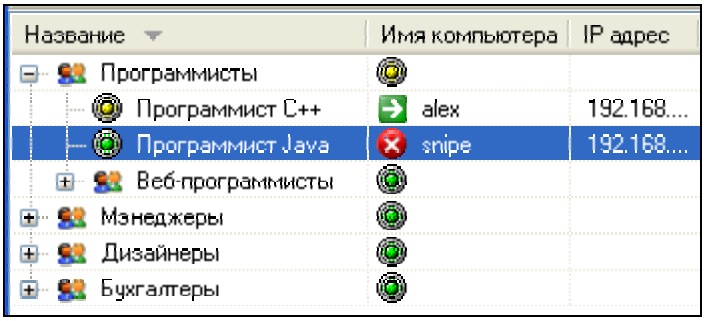


Рис. 7 – Окно списка мониторинга

Здесь отображаются рабочие станции вашей сети, за которыми ведётся наблюдение (на которых установлена пользовательская часть программы). 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. Вы можете добавлять компьютеры и группы в список мониторинга и удалять их.

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.

Таблица состоит из следующих столбцов:

- **IP-адрес** - IP-адрес компьютера, на котором установлена пользовательская часть программы.

- **Имя компьютера** - имя компьютера, на котором установлена пользовательская часть программы (администраторская часть получает его автоматически).

- **Название** - название для данной рабочей станции в списке мониторинга. Вы указываете его самостоятельно при добавлении компьютера. 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 компьютер выключен или на нём не установлена 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.

4.2 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);
- Соединения с Интернет (статистика подключения и отключения соединений с интернет);
- Посещенные сайты (перечень посещенных пользователями сайтов);
- Компьютер (история включения и выключения компьютеров пользователей).

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

4.2.1 Клавиатура

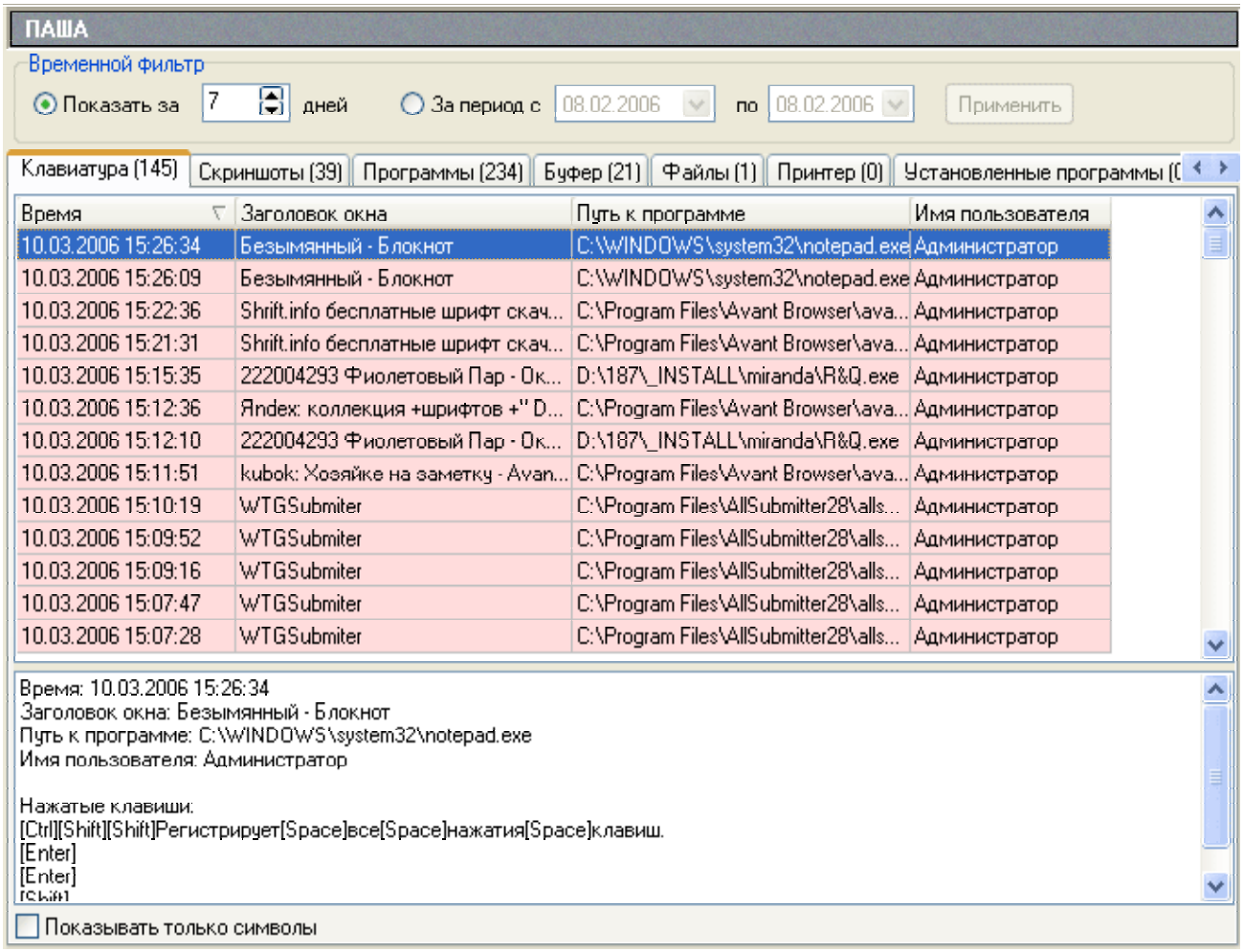


Рис. 8 – Окно логов клавиатуры

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.

4.2.2 Скриншоты

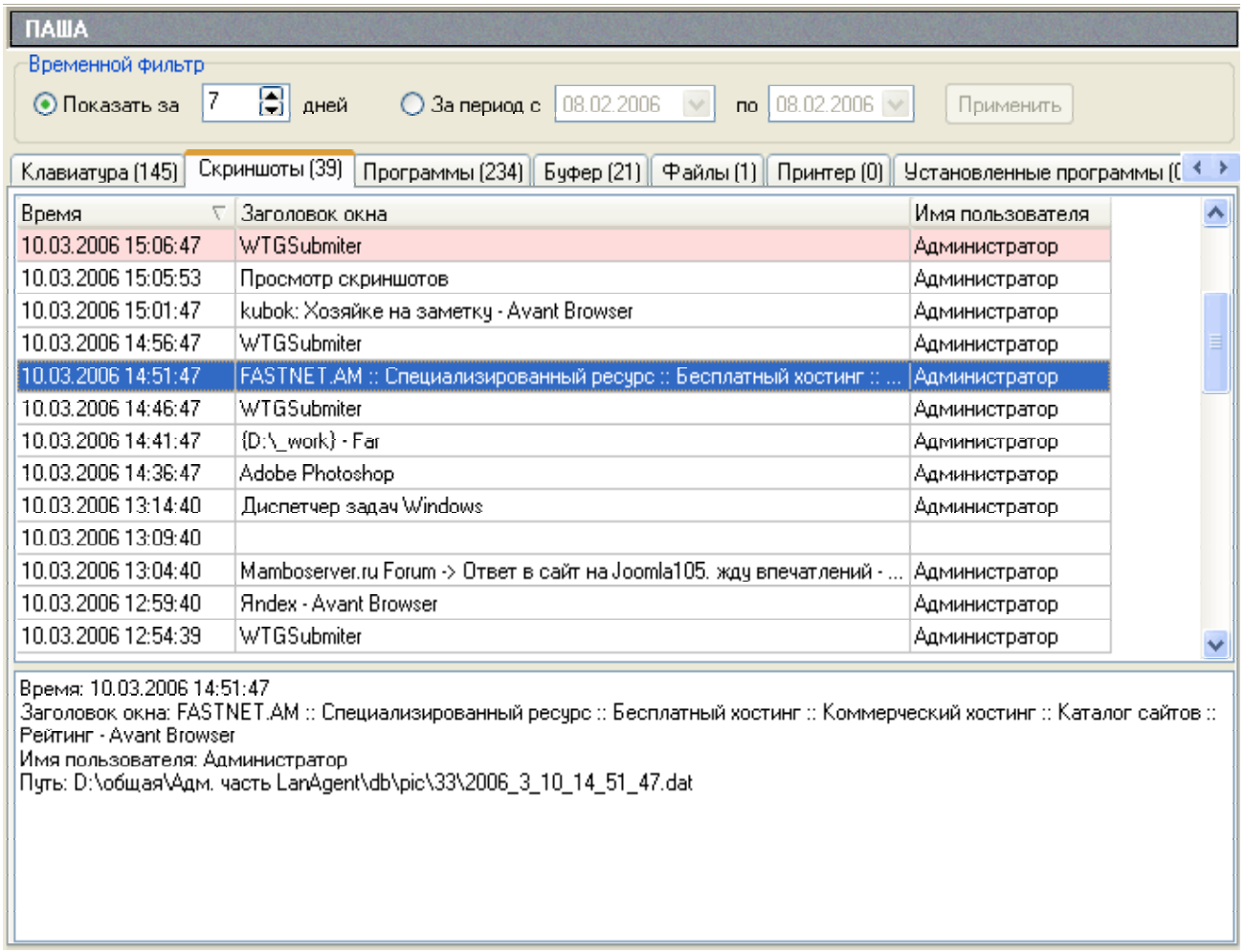


Рис. 9 – Окно логов снимков экранов (скриншотов)

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.

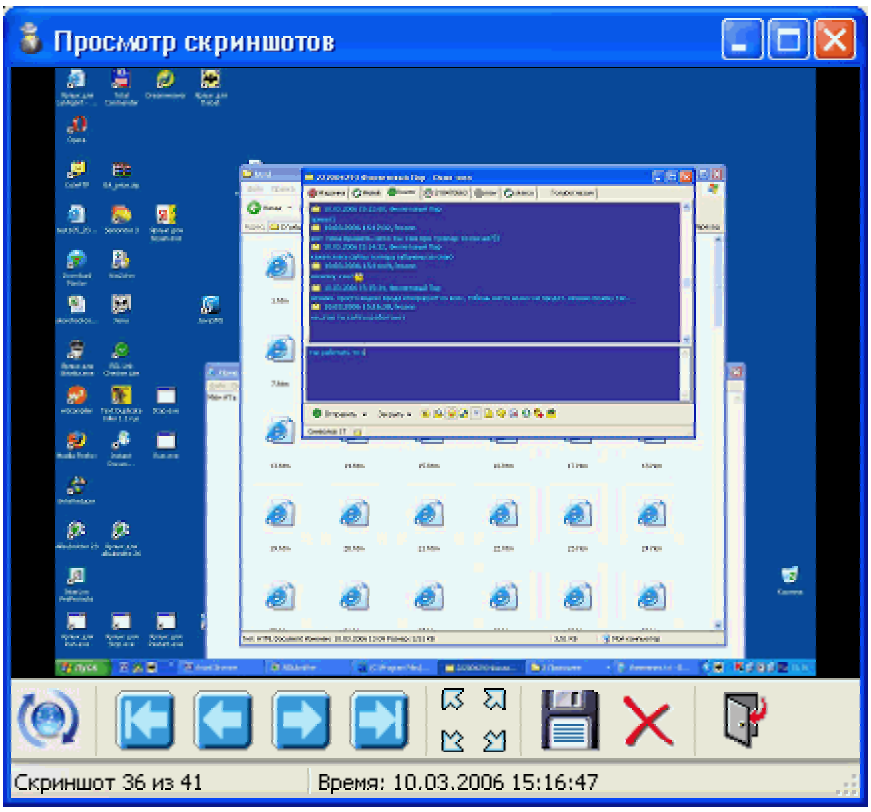


Рис. 10 – Окно просмотра скриншотов

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:

 - получить скриншот

 - 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.

4.2.3 Программы

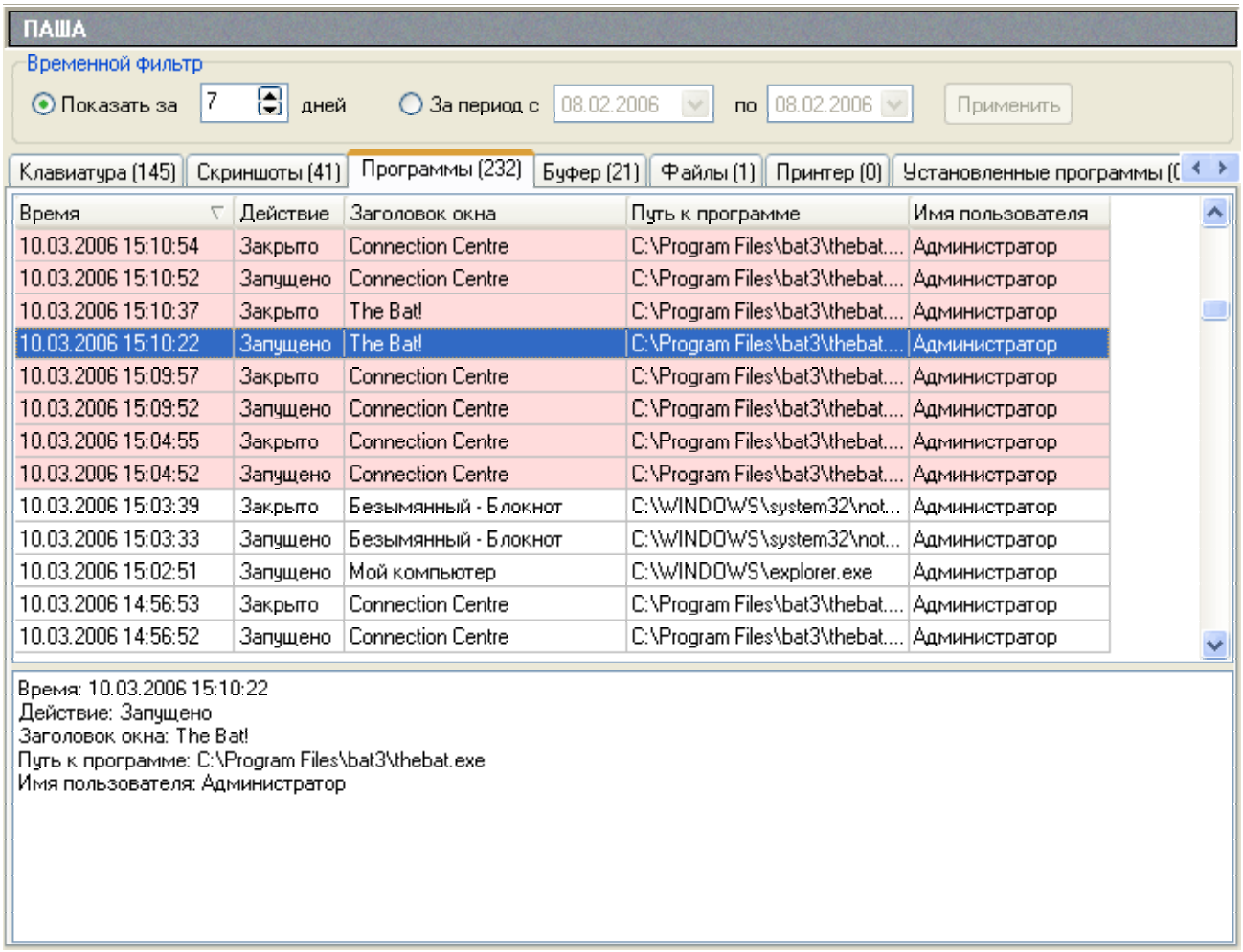


Рис. 11 – Окно логов программ

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.

4.2.4 Буфер обмена

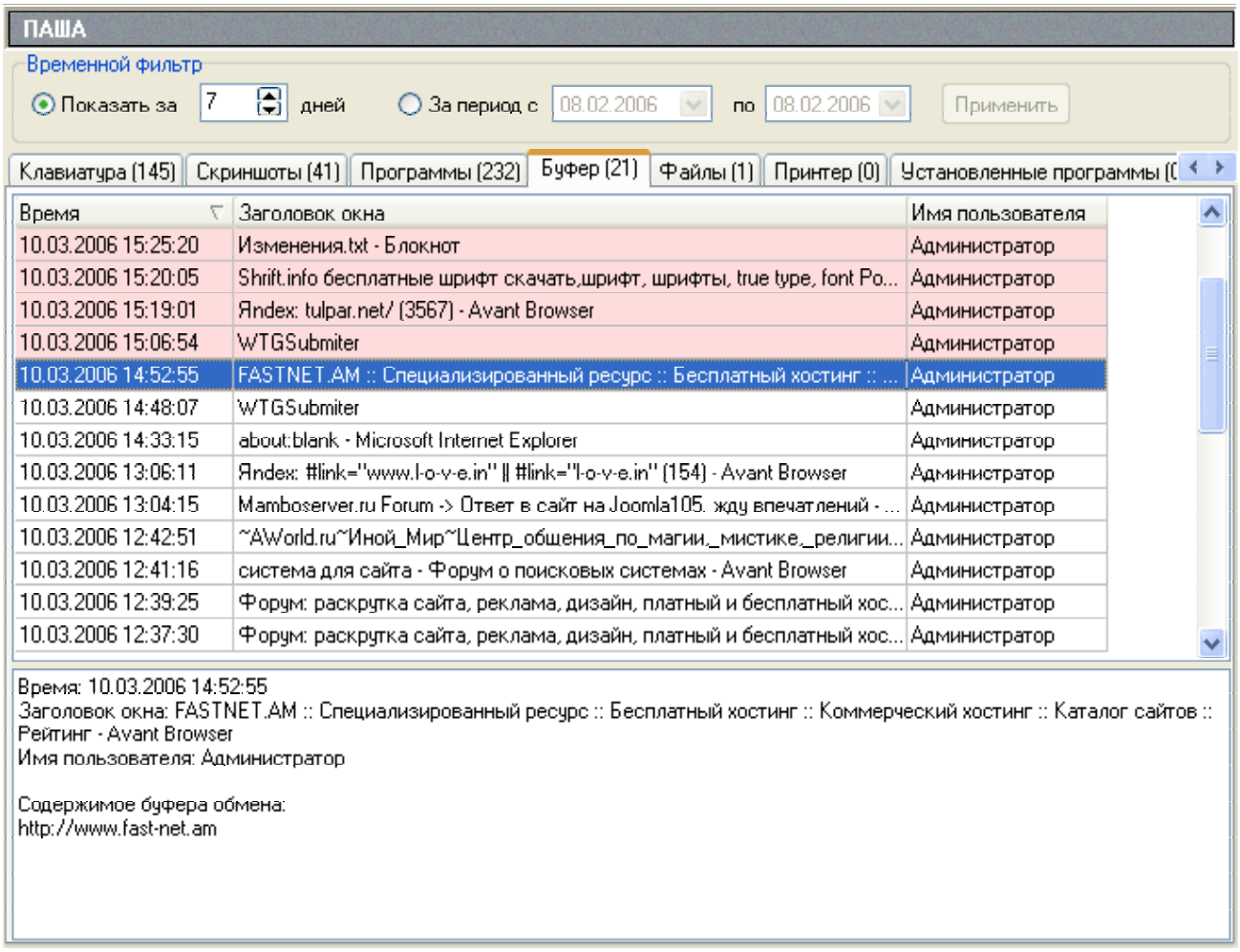


Рис. 12 – Окно логов буфера обмена

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.

4.2.5 Файлы

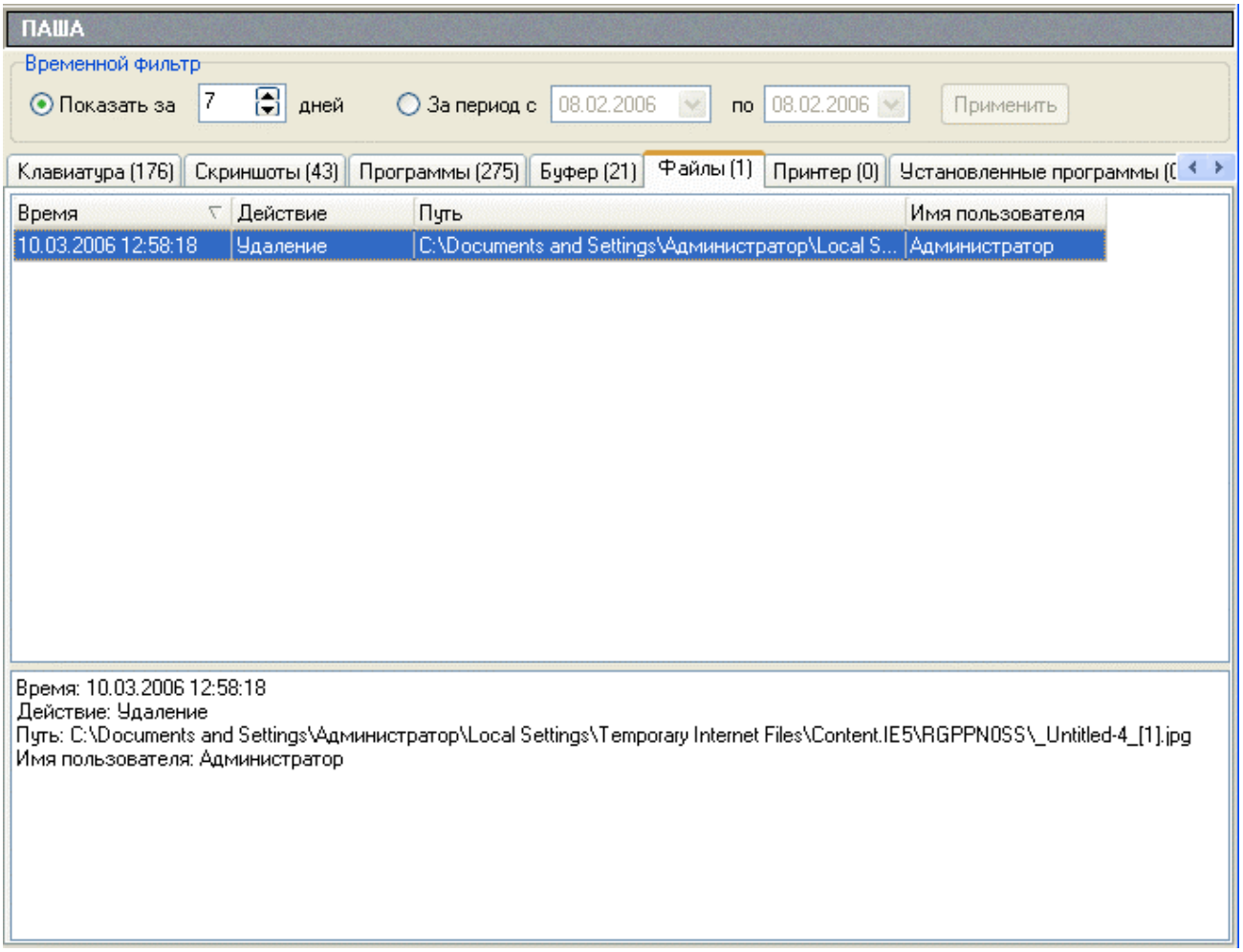


Рис. 13 – Окно статистики создания/удаления файлов

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.

4.2.6 Принтер

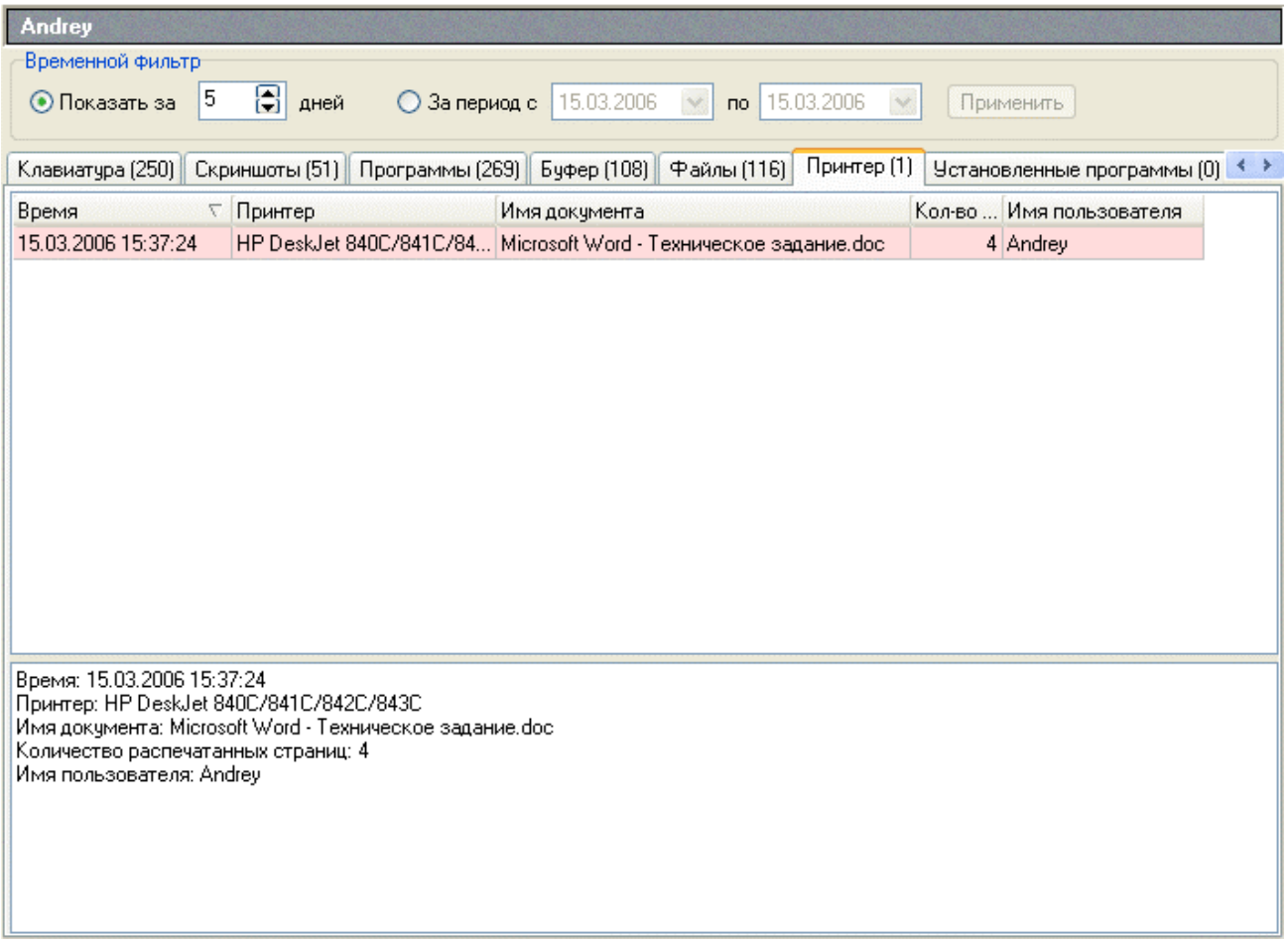


Рис. 14 – Окно логов принтеров

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.

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.

4.2.7 Установленные программы

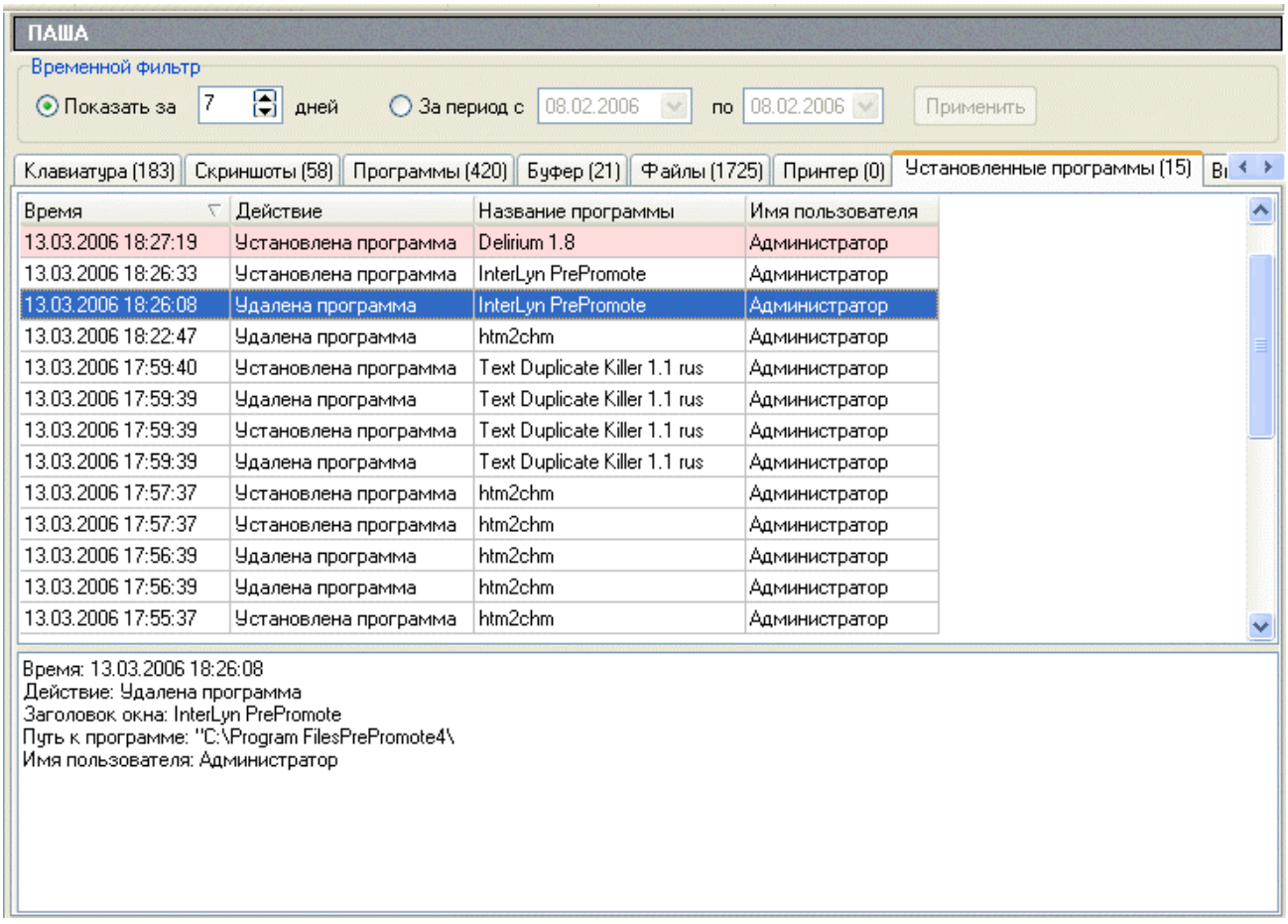


Рис. 15 – Окно логов установки/удаления программ

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.

4.2.8 Внешние накопители

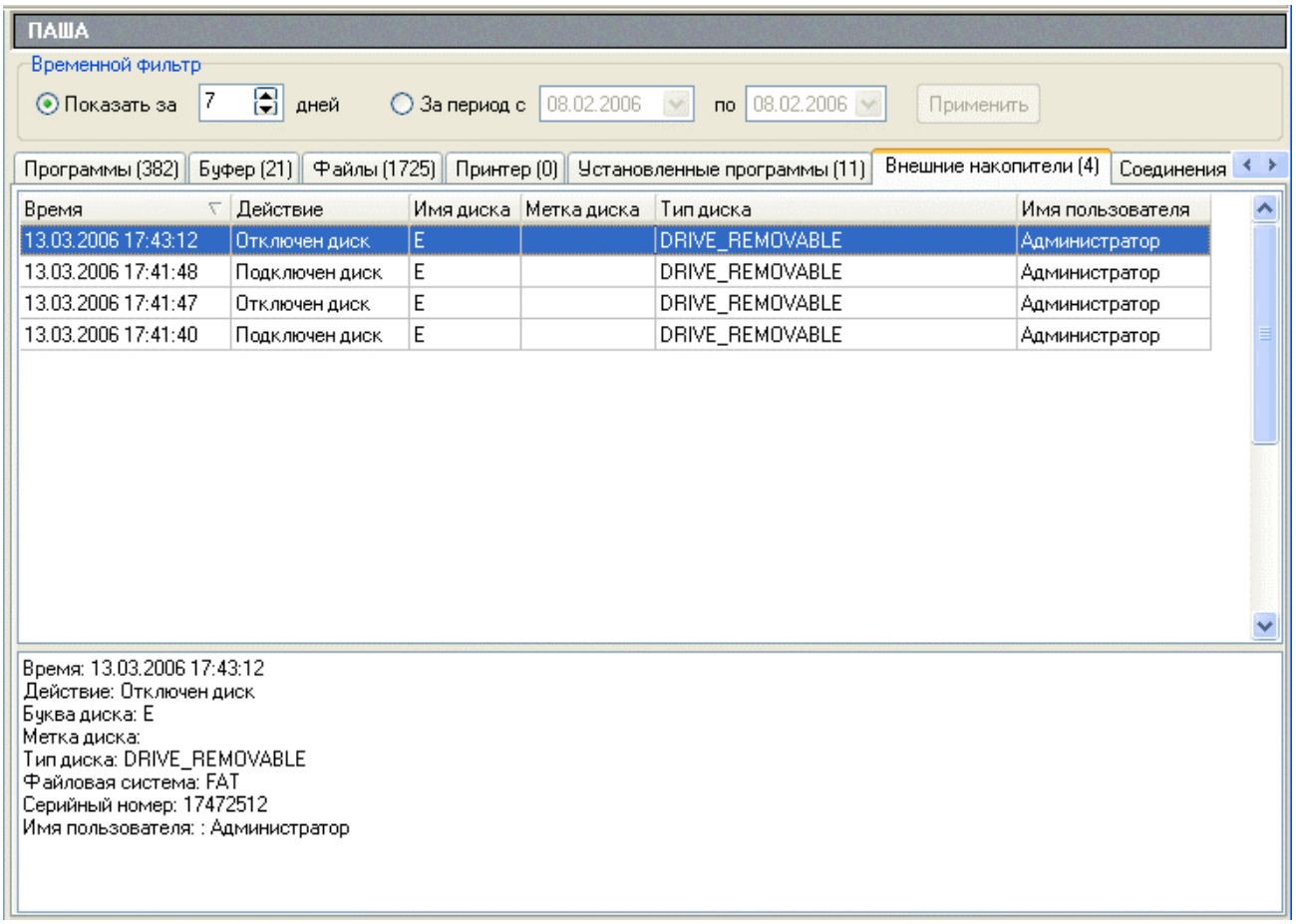


Рис. 16 – Окно логов подключения/отключения носителей информации

На этой странице находится информация по подключению/отключению внешних устройств, таких как флэш, SD, USB-диски, жесткие диски. 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 устройства, какое действие было произведено (подключено или отключено устройство), имя диска, метка диска, тип диска, 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, а также еще тип файловой

системы и серийный номер диска. И так по каждой выбранной 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.

4.2.9 Соединения с интернет

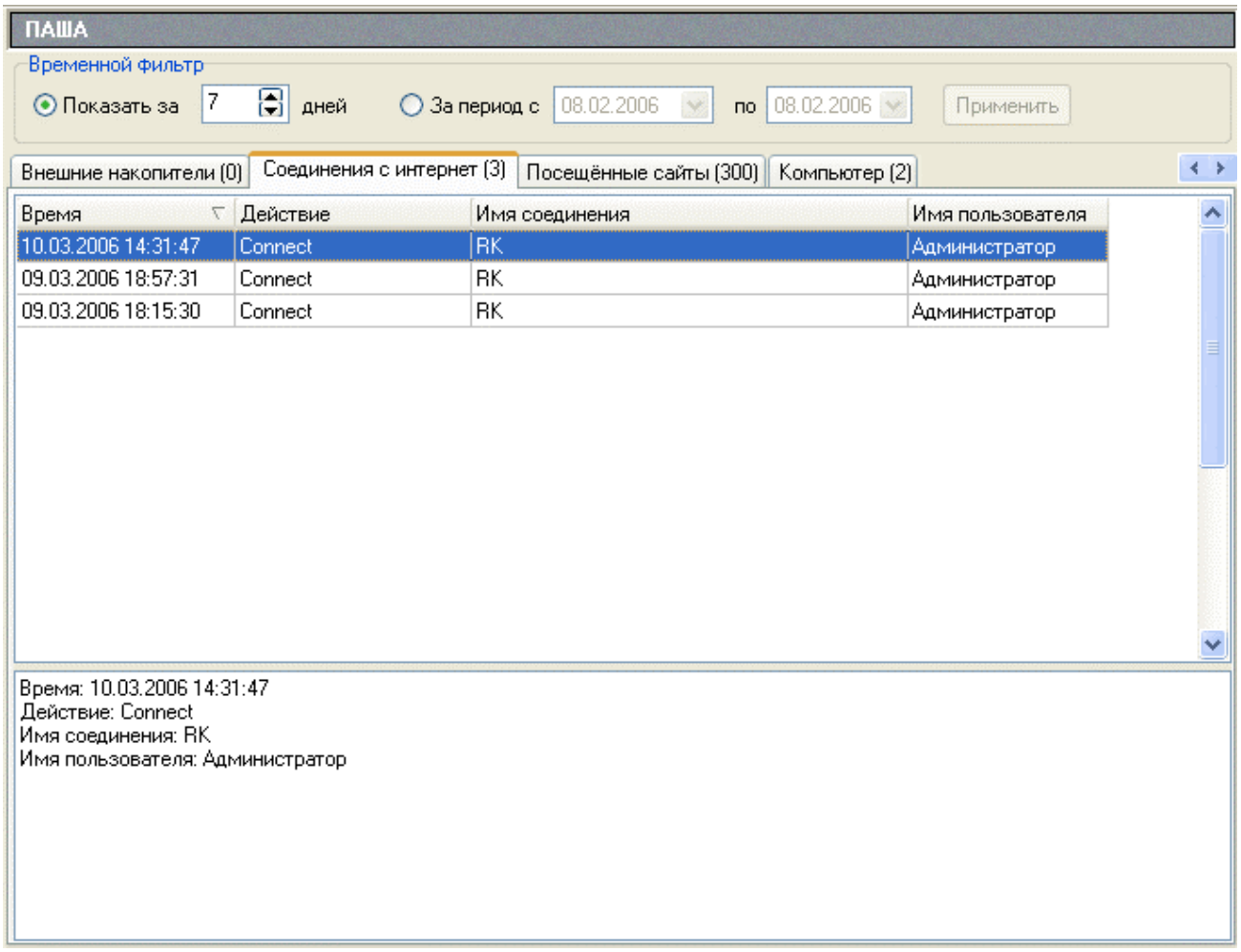


Рис. 17 – Окно логов соединений с Интернет

На этой странице находится информация о подключении и отключении соединений с Интернет 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 входа или выхода из интернет, какое действие было произведено (connect или disconnect), имя соединения, по которому вышли в интернет, 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.

4.2.10 Посещённые сайты

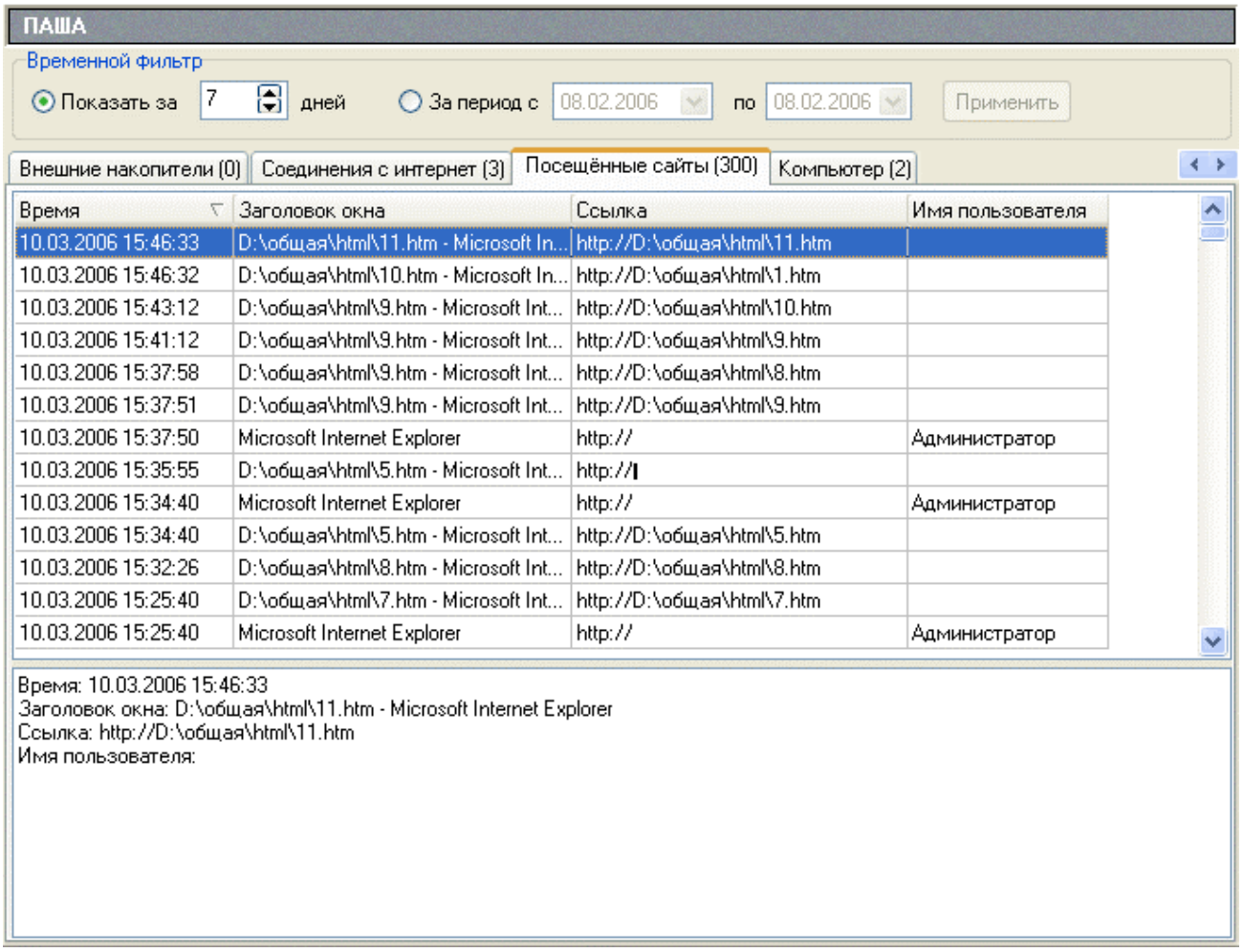


Рис. 18 – Окно логов посещенных сайтов

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.

4.2.11 Компьютер

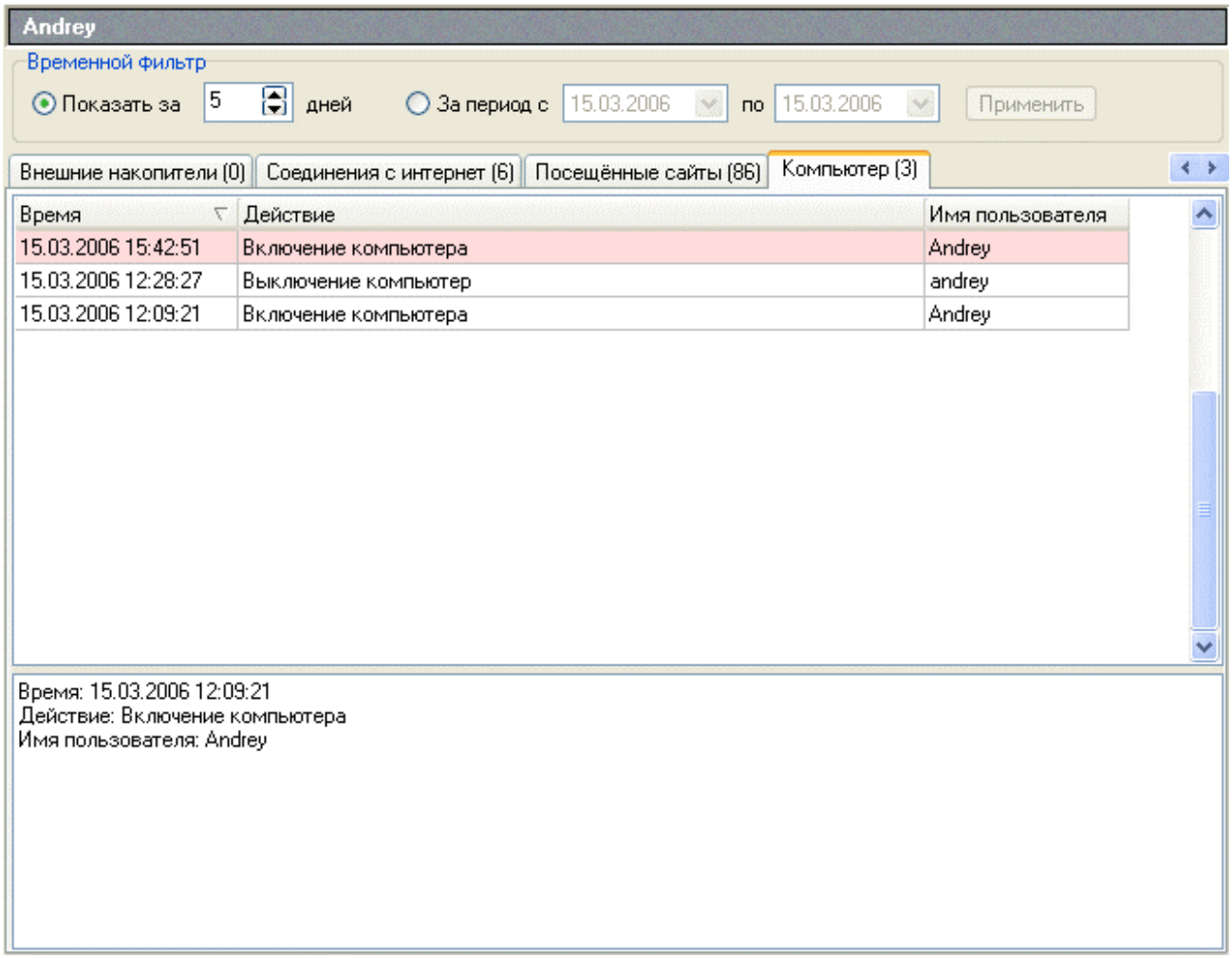


Рис. 19 – Окно статистики включения/выключения компьютера

На этой странице находится история включений/выключений контролируемых компьютеров. 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 включения или выключения компьютера, какое конкретно действие было произведено (включён компьютер или выключен), 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.

4.3 Панель инструментов

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

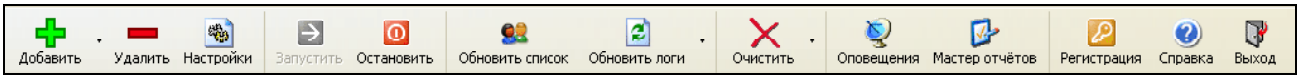
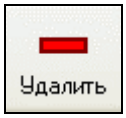


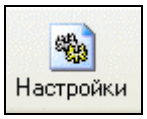
Рис. 20 – Панель инструментов

Назначение кнопок панели инструментов:

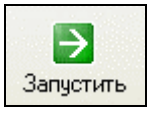
- добавить группу или компьютер в список мониторинга.



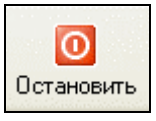
- удалить компьютер из списка мониторинга.



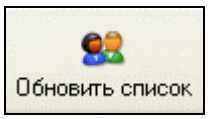
- открыть окно настроек пользовательской части программы.



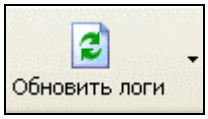
- запустить мониторинг на выбранном компьютере.



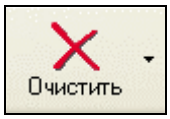
- остановить мониторинг на выбранном компьютере.



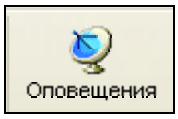
- обновить список компьютеров и состояний мониторинга.



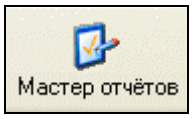
- обновить содержимое логов для всех пользователей.



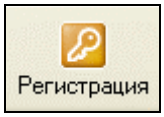
- очистка содержимого логов. Включает в себя следующие пункты:
  - очистить выбранную категорию,
  - очистить все логи пользователя,
  - очистить все логи для всех пользователей.



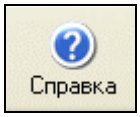
- открыть окно истории активного оповещения.



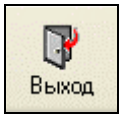
- открыть окно мастера отчетов.



- ввести регистрационный код.



- вызов файла справки.

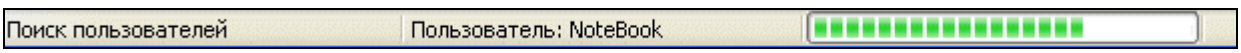


- выйти из программы.

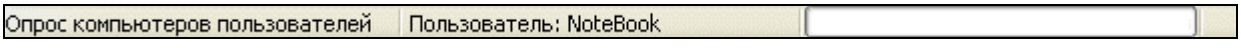
4.4 Информация о состоянии процесса

В строке состояния отображаются 2 события:

1). Поиск пользователей - компьютеры из списка проверяются на доступность.



2). Опрос пользователей - происходит загрузка логов с компьютеров пользователей.



4.5 Активное оповещение

Служит для оперативного оповещения специалиста службы безопасности о таких опасных действиях пользователей, как подключение носителей информации, установка программ. При осуществлении пользователем указанных выше действий, агентская часть программы LanAgent передаст эту информацию на базовый компьютер, не дожидаясь команды обновления логов. 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 в специальном диалоге настройки, вызвать который можно нажав кнопку "Настройки" панели управления основного окна программы, или воспользовавшись кнопкой "Настройки" панели управления самого окна истории активного оповещения. Подробно о настройках можно посмотреть в разделе 4.9.

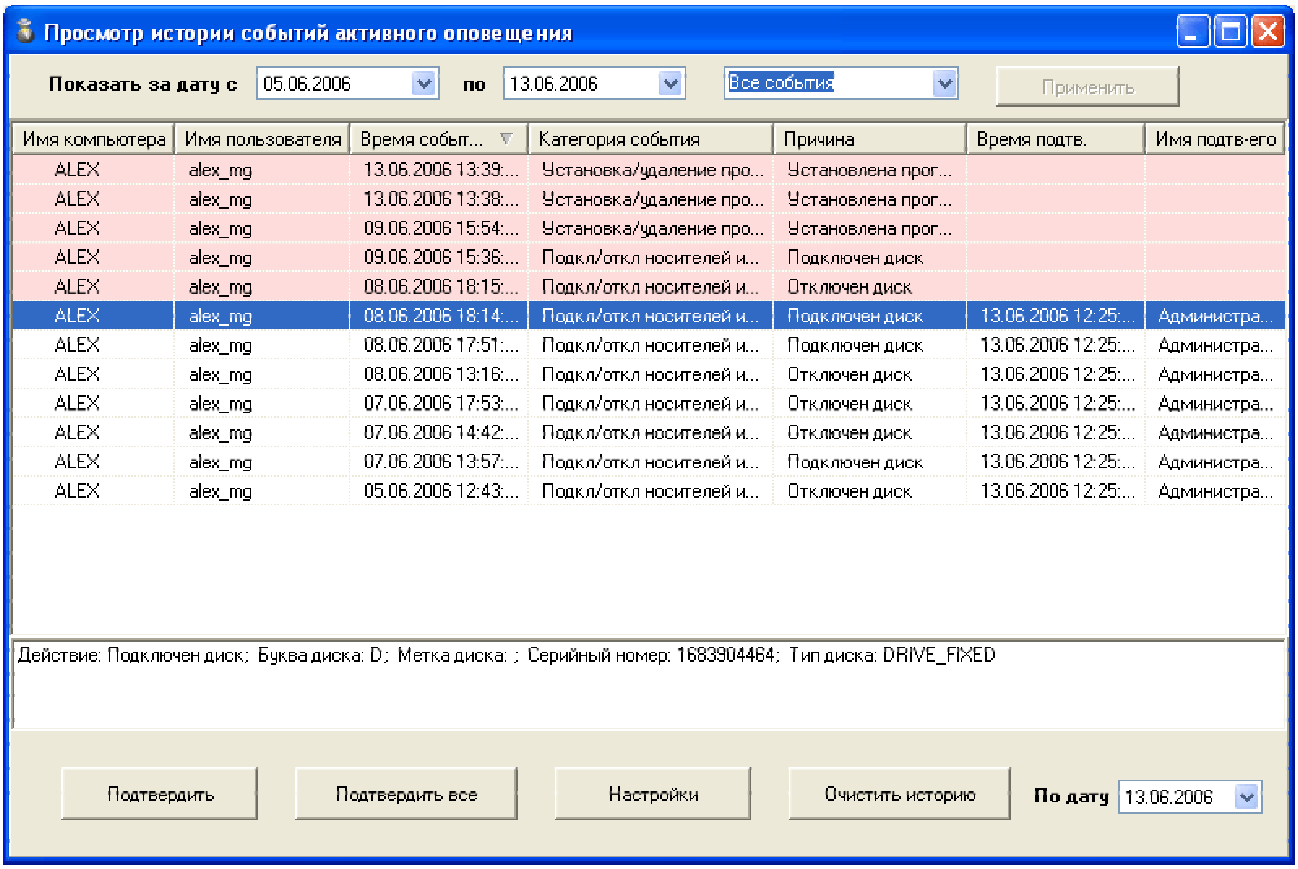


Рис. 21 – Окно истории активного оповещения

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 или Подкл/откл носителей информации); Причина события (т.е что непосредственно произошло: Подключение диска, Установка программы, Отключение диска, ...); Время подтверждения (здесь фиксируется момент времени, когда администратор программы просмотрел данное событие и подтвердил его (нажатием кнопки "Подтвердить")); Имя подтвердившего.

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.

Более подробную информацию о пришедшем сообщении можно просмотреть в специальном поле, расположенном под таблицей.

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

4.6 «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 4.7.

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 пользователя "Программист" имеются незначительные нарушения, поэтому статус его опасности "желтый".

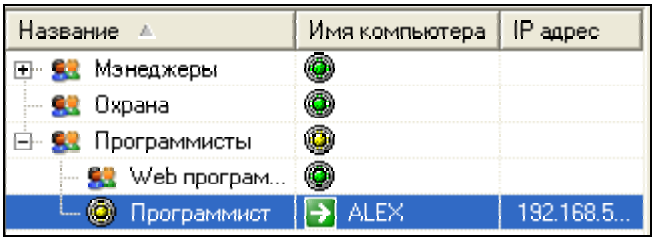


Рис. 22 – «Светофор» списка компьютеров

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 содержат соответствующий значок (см рисунок). А перед именем закладки, содержащей записи с нарушением стоит восклицательный знак.

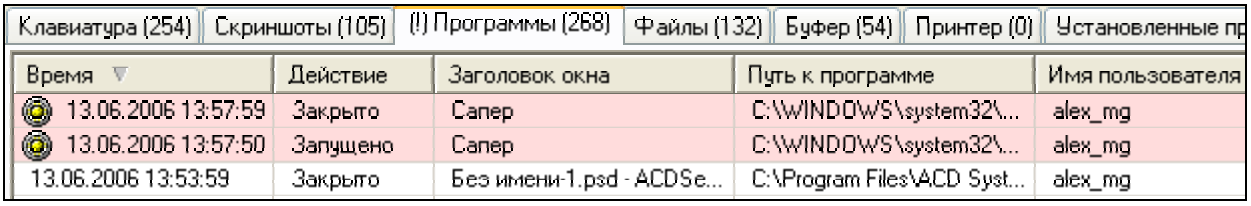


Рис. 23 – «Светофор» событий в логах

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!

4.7 Список правил безопасности

Призван облегчить процедуру контроля за соблюдением политик безопасности и использования компьютерной техники работниками организации. Реализован в виде списка, в котором для каждого компьютера по каждому из видов информации (программы, буфер обмена, клавиатура, ...) указываются контролируемые (запрещенные) строки и класс их опасности.

Рассмотрим заполнение правил на конкретных примерах:

1. Установка правила для запускаемых программ на примере игры "Сапер". Если вы знаете имя запускающего файла программы (в данном случае winmine.exe), для которой хотите создать правило, то можно сразу перейти к диалогу заполнения. (на панели управления основного окна программы **LanAgent** выбрать меню "Опции->Настройки программы...->Редактировать список шаблонов). Здесь в правой части

окна выбираем нужную закладку (в нашем примере "Программы"), в поле "Контролируемая строка" пишем имя exe-файла. Устанавливаем класс опасности (1 - "желтый", 2 - "красный"). Если правило устанавливается только для одного конкретного компьютера, то выбираем именно его из выпадающего списка и нажимаем кнопку "**Добавить**". Если правило устанавливается для всех компьютеров, то тогда нажимаем кнопку "**Добавить всем**". Список созданных правил, по соответствующим разделам для каждого компьютера, отображается в виде таблицы.

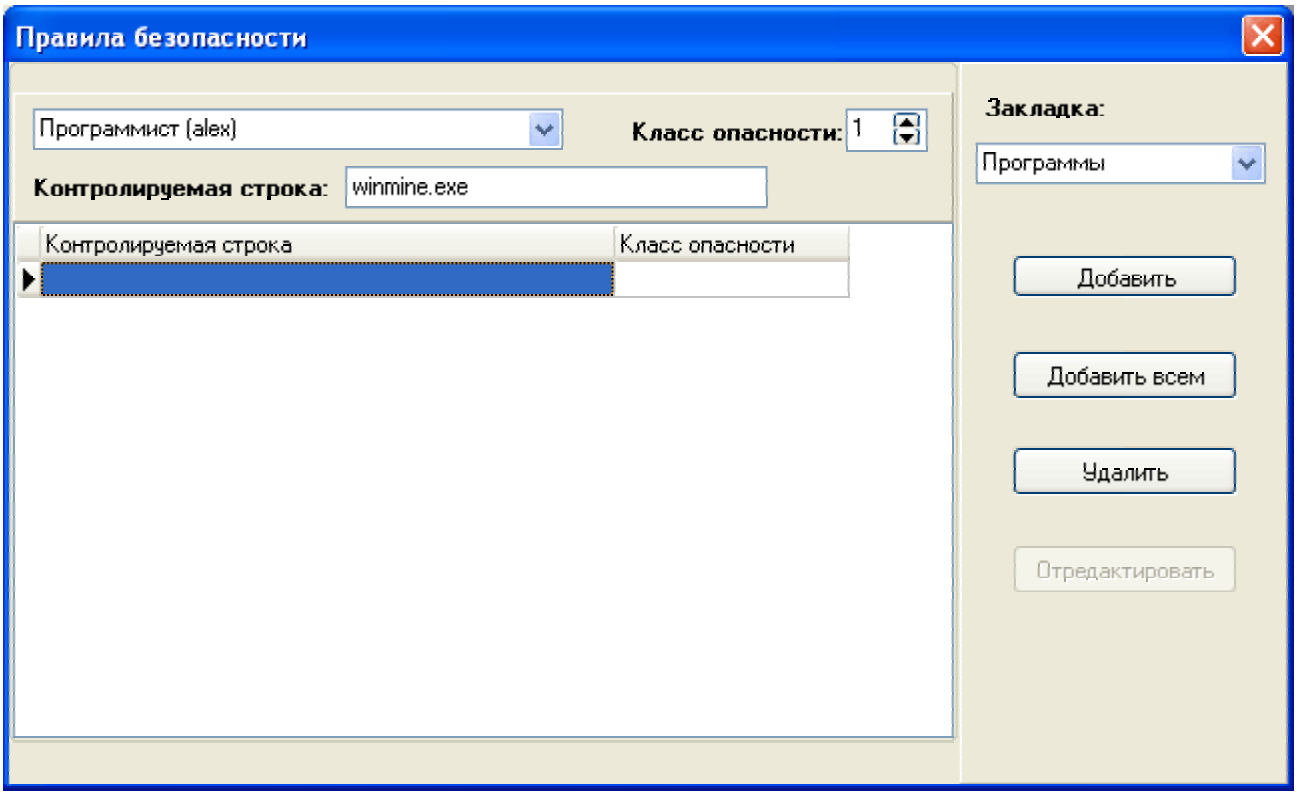


Рис. 24 – Диалог назначения правил безопасности

Кроме того, в программе реализована возможность быстрого заполнения правил: для этого в окне просмотра логов (событий, произошедших на компьютерах) встаньте курсором на ту строку, которую хотите занести, и в выпадающем меню (вызываемом щелчком правой клавиши мыши) выберите пункт "**Пометить как запрещенное**".

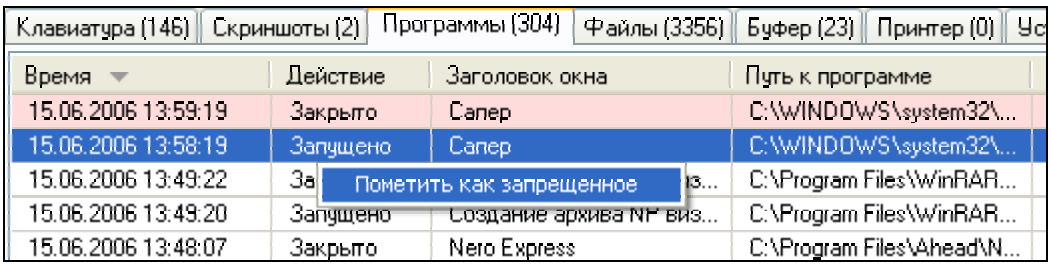


Рис. 25 – Вызов диалога правил безопасности из окна просмотра логов

При этом откроется описанный выше диалог, но в нем уже будет выбрана нужная закладка (с которой он был вызван) и в поле "Контролируемая строка" уже будет стоять имя нужного файла.

2. Установка правила для текста, копируемого в буфер обмена. Принципы заполнения те же самые, что и для запускаемых программ. Только необходимо выбрать соответствующую закладку "Буфер обмена" и в качестве контролируемой строки задать тот текст, при обнаружении которого в содержимом буфера обмена, программа будет определять содержимое как опасное. В текущей версии LanAgent, данное правило сработает только при **строгом соответствии** текста в шаблоне и просматриваемого текста.

Редактирование правил:

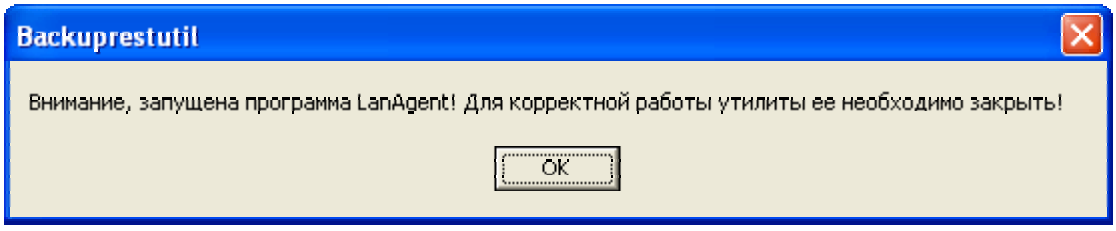
Для того чтобы отредактировать уже созданное правило, необходимо выделить его в таблице, внести требуемые изменения в поле "Контролируемая строка" или в "Класс опасности" и нажать кнопку "**Отредактировать**", расположенную в правой части окна.

Удаление правил:

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

4.8 Архивирование статистики (логов)

С целью защиты информации (базы логов) от потери, например в случае сбоев, имеется возможность резервного копирования/восстановления (backup/restore) базы. Данная возможность реализована в виде отдельной утилиты (файл "**BackupRestUtil.exe**"). **Внимание!** Для корректной работы утилиты **необходим монопольный доступ** к базе данных, поэтому перед выполнением как резервного копирования так и восстановления данных, **необходимо закрыть программу LanAgent**. Если LanAgent запущен, утилита вам об этом напомнит при помощи сообщения.



Внешний вид самой утилиты представлен ниже:

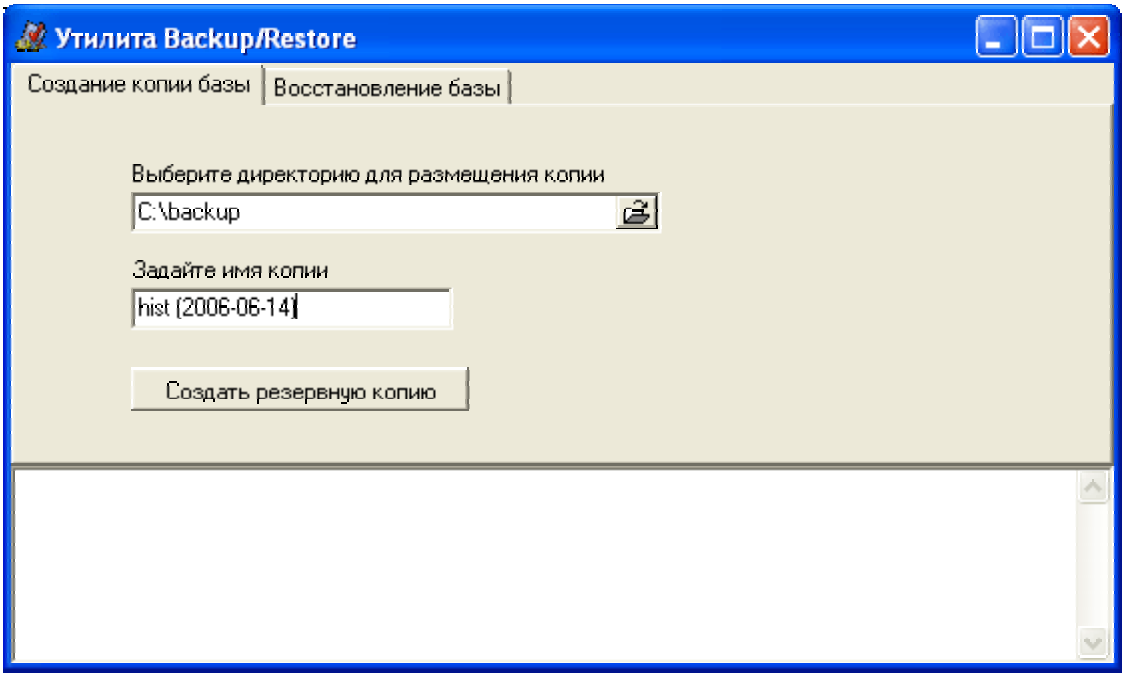


Рис. 26 – Утилита создания резервной копии базы

Для создания резервной копии (backup) необходимо выбрать каталог где она будет размещена и имя файла копии, а затем нажать кнопку "**Создать резервную копию**". Результатом резервного копирования для данного примера будут файл "hist (2006-06-14).gbk" и каталог с копией скриншотов "pic_hist (2006-06-14)". Ход выполнения операции будет показываться в нижней части окна.

Внимание! Нельзя производить самостоятельное копирование или архивирование (любыми архиваторами) **работающей** базы! Это может привести к нарушению ее работоспособности. Для выполнения резервного копирования пользуйтесь описанной выше утилитой.

Восстановление резервной копии базы

Для произведения восстановления базы статистики из резервной копии, воспользуйтесь той же утилитой "**BackupRestUtil.exe**".

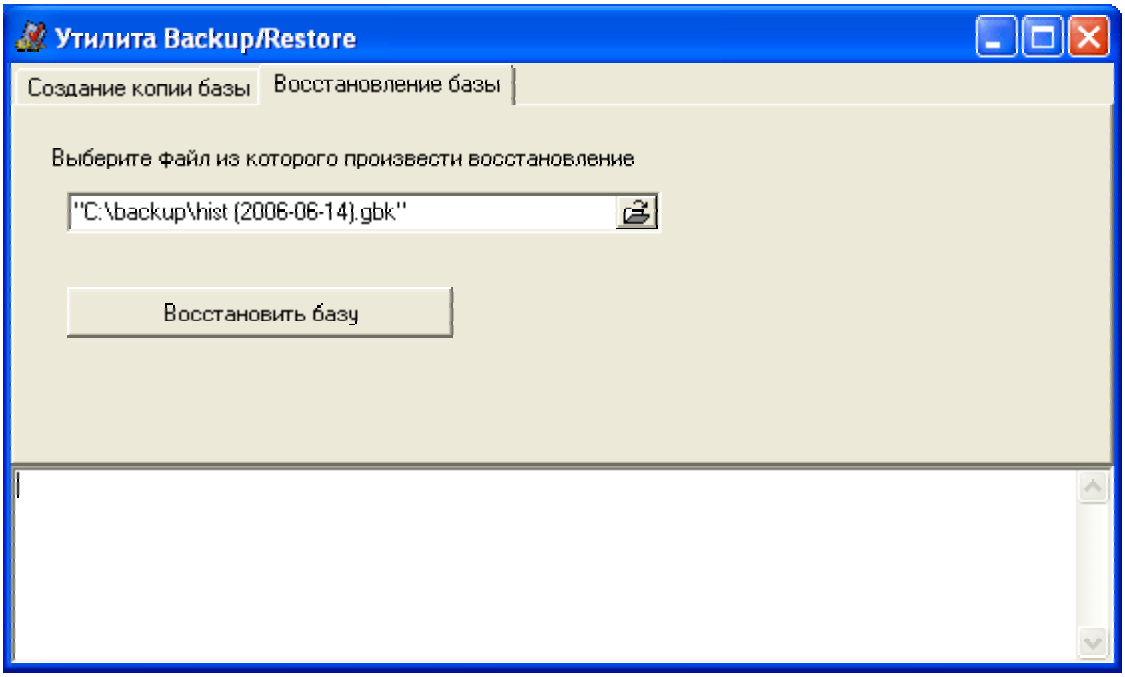


Рис. 27 – Утилита восстановления базы из копии

Здесь необходимо указать имя файла, из которого требуется произвести восстановление и нажать кнопку "**Восстановить базу**". Ход выполнения операции будет показываться в нижней части окна.

4.9 Настройки программы

4.9.1 Настройка программы администратора

В данный раздел можно попасть, выбрав пункт "Настройки программы..." в меню "**Опции**".

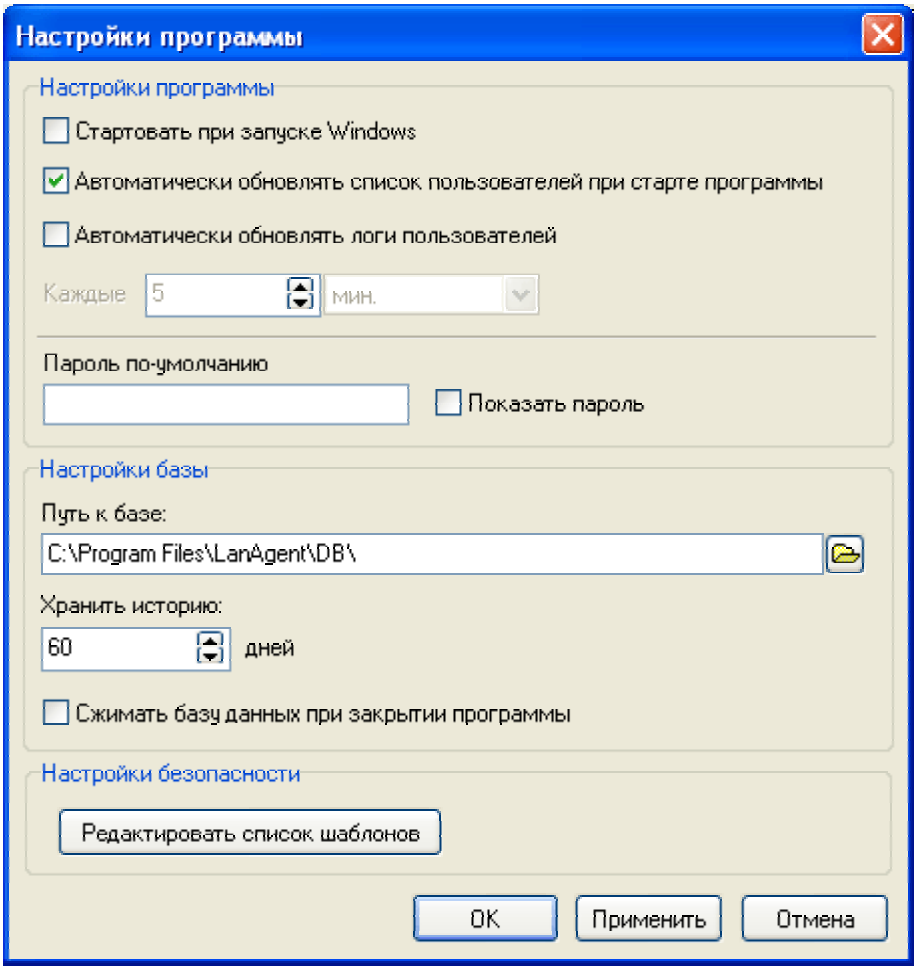


Рис. 28 – Настройки программы администратора

Стартовать при загрузке Windows - установите эту галочку, если хотите чтобы при загрузке операционной системы автоматически запускалась администраторская часть **LanAgent**.

Автоматически обновлять список пользователей при старте программы - установите эту галочку, если хотите чтобы при загрузке программы производилась автоматическая проверка состояния агентов на контролируемых компьютерах (запущен/остановлен/не доступен). По умолчанию данная опция включена.

Автоматически обновлять логи пользователей - если данная опция включена, то через заданный промежуток времени (например каждые 5 минут) будет производится обновление логов для всех компьютеров, включенных в список мониторинга. Если опция выключена, то обновление логов нужно будет производить вручную, нажав на кнопку "**Обновить логи**" или выбрав соответствующий пункт в меню "**Управление**".

Пароль по-умолчанию - здесь можно задать пароль на доступ к агентам, который будет использоваться по-умолчанию для всех добавляемых агентов. Задавать пароль можно для того, чтобы только вы могли получать логи. По-умолчанию это

поле пустое. Если у вас нет особой надобности защищать соединения паролем, то можно оставить это поле пустым.

Опция **Показать пароль** регулирует отображение пароля при его наборе в данном окошке. При выбранной опции вы будете видеть набираемые символы в том виде, как они есть. При отключенной опции - при наборе символы будут отображаться в виде звездочек *.

Путь к базе - здесь задается путь к каталогу, в котором расположена база логов. По-умолчанию это подкаталог DB в каталоге программы.

Хранить историю - здесь указывается сколько дней хранить информацию, собранную с контролируемых компьютеров. Данные старше указанного срока будут удаляться.

Сжимать базу данных при закрытии программы - если данная опция включена, то при закрытии программы будет производиться очистка базы данных от удаленных записей. Это займет некоторое время.

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

4.9.2 Настройка агента

Настройка агентов программы LanAgent производится удаленно из базовой части программы. Для этого достаточно выбрать нужный компьютер из списка для мониторинга и нажать кнопку «Настройки» в панели управления. Также имеется возможность групповой настройки агентов.

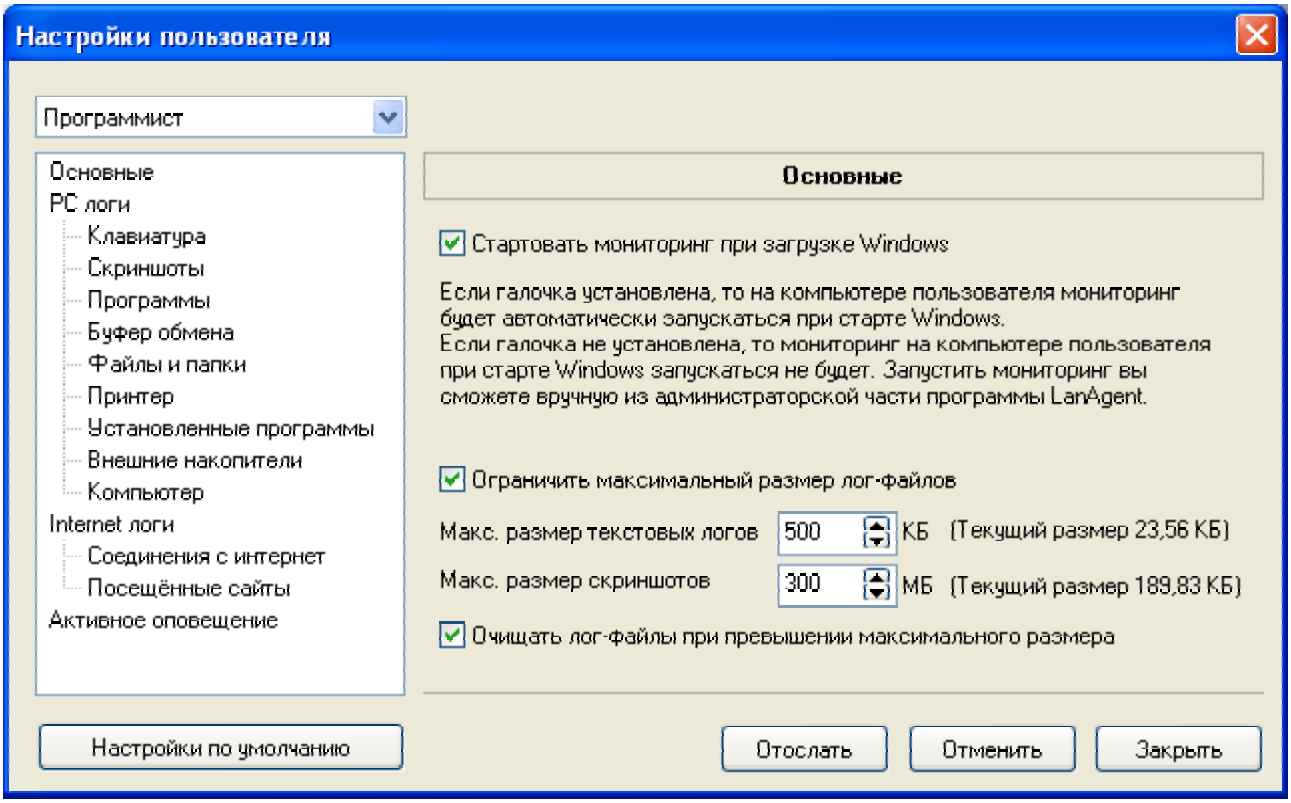


Рис. 29 – Главное окно настроек агентов

Можно изменять настройки для каждого пользователя отдельно или для всех сразу. Чтобы изменить настройки для всех пользователей, выберите в выпадающем списке "Все пользователи".

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:

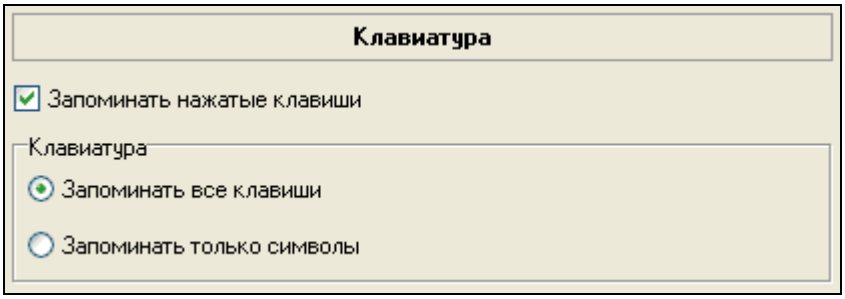


Рис. 30 – Настройки контроля клавиатуры агентов

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:

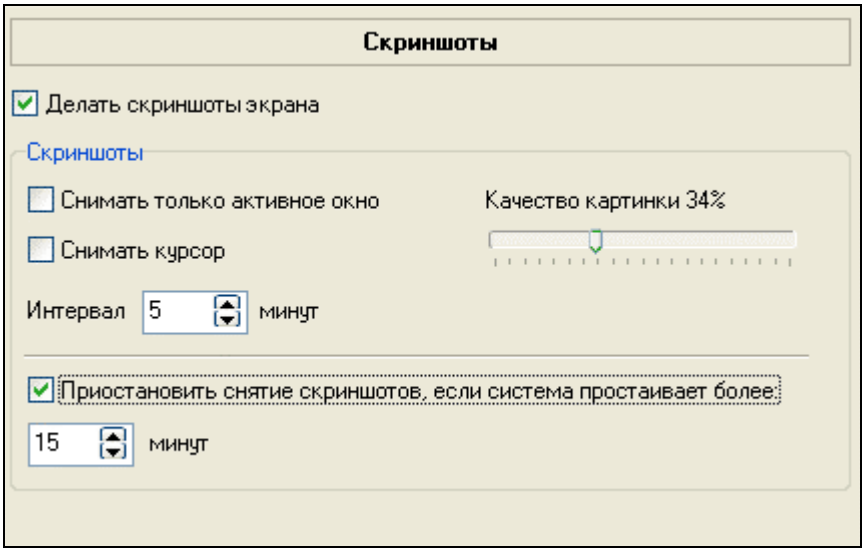


Рис. 31 – Настройки контроля снимков экранов

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:

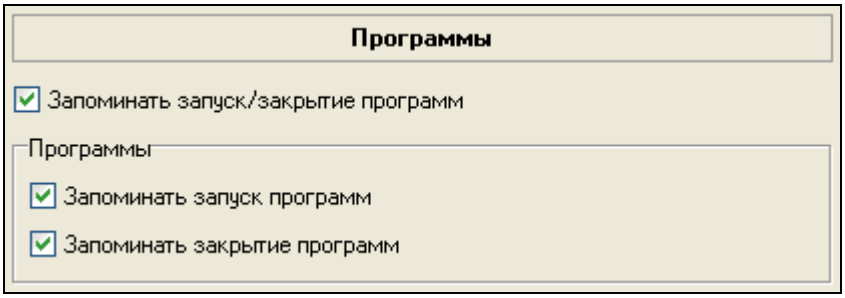


Рис. 32 – Настройки контроля запуска/закрытия программ

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:

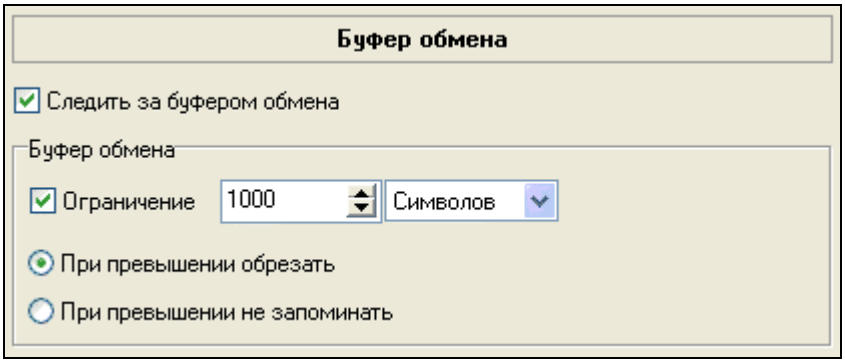


Рис. 33 – Настройки контроля буфера обмена

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:

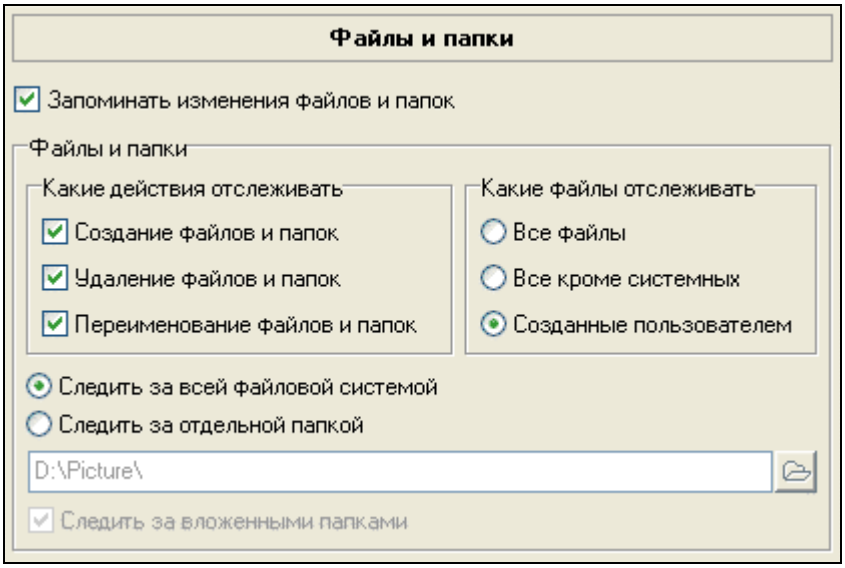


Рис. 34 – Настройки ведения мониторинга файловой системы

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 всей файловой системой - наблюдение будет производится за всеми файлами на всех дисках компьютера.

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:

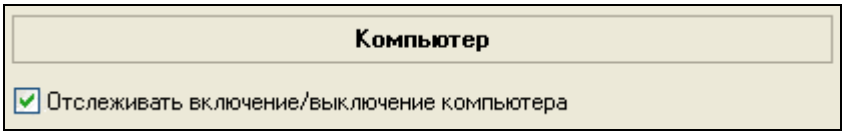


Рис. 35 – Настройки статистики включения/выключения компьютера

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

Internet логи - действия:

Запоминать соединения с интернет - установите эту галочку, чтобы программа фиксировала моменты захода и выхода из интернет.

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

Соединения с интернет:

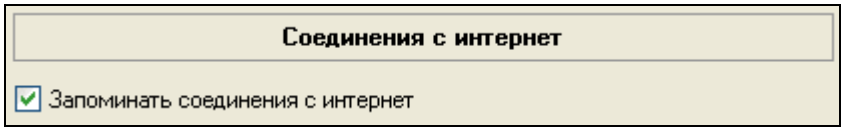


Рис. 36 – Настройки контроля соединений с Интернет

Запоминать соединения с интернет - установите эту галочку, чтобы программа фиксировала моменты захода и выхода из интернет.

Посещённые сайты:

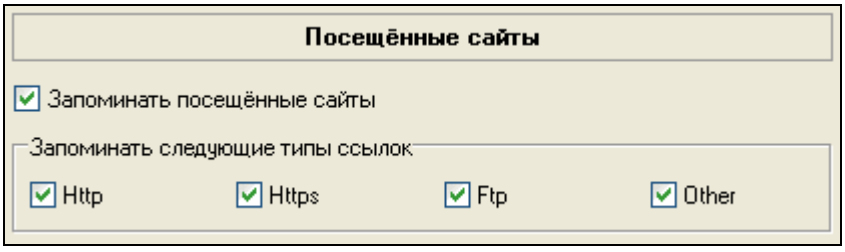


Рис. 37 – Настройки контроля посещенных сайтов

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

Принтер:

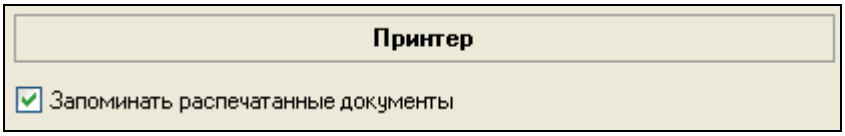


Рис. 38 – Настройки контроля принтеров

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

Установленные программы:

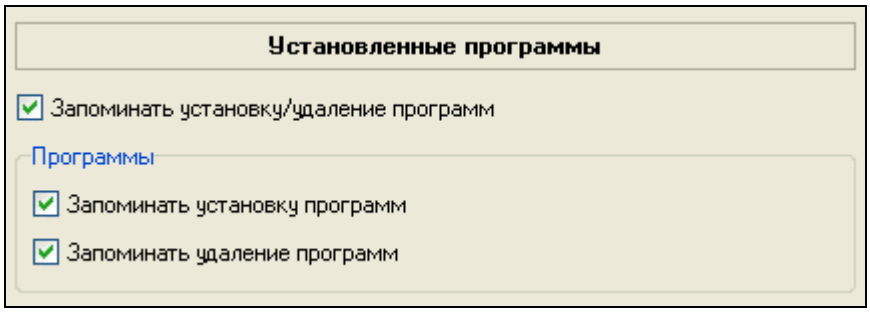


Рис. 39 – Настройки контроля установленных программ

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:

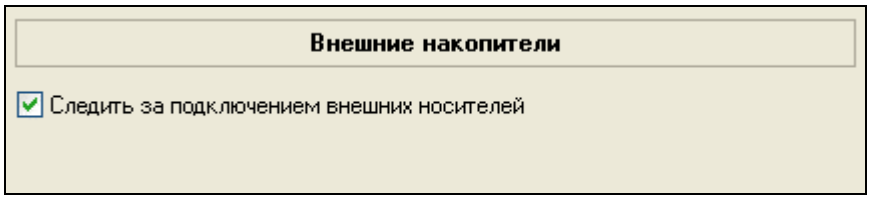


Рис. 40 – Настройки контроля подключения носителей

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.

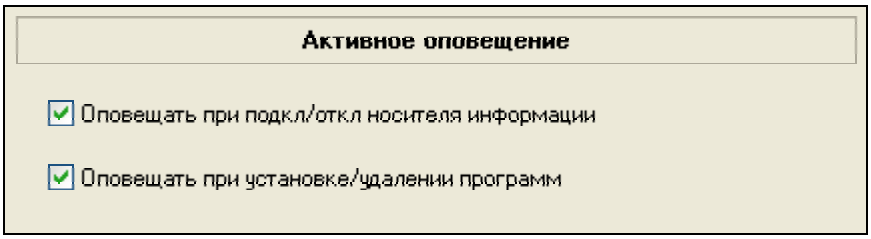


Рис. 41 – Настройки активного оповещения

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

4.10 Составление отчетов

4.10.1 Настройка

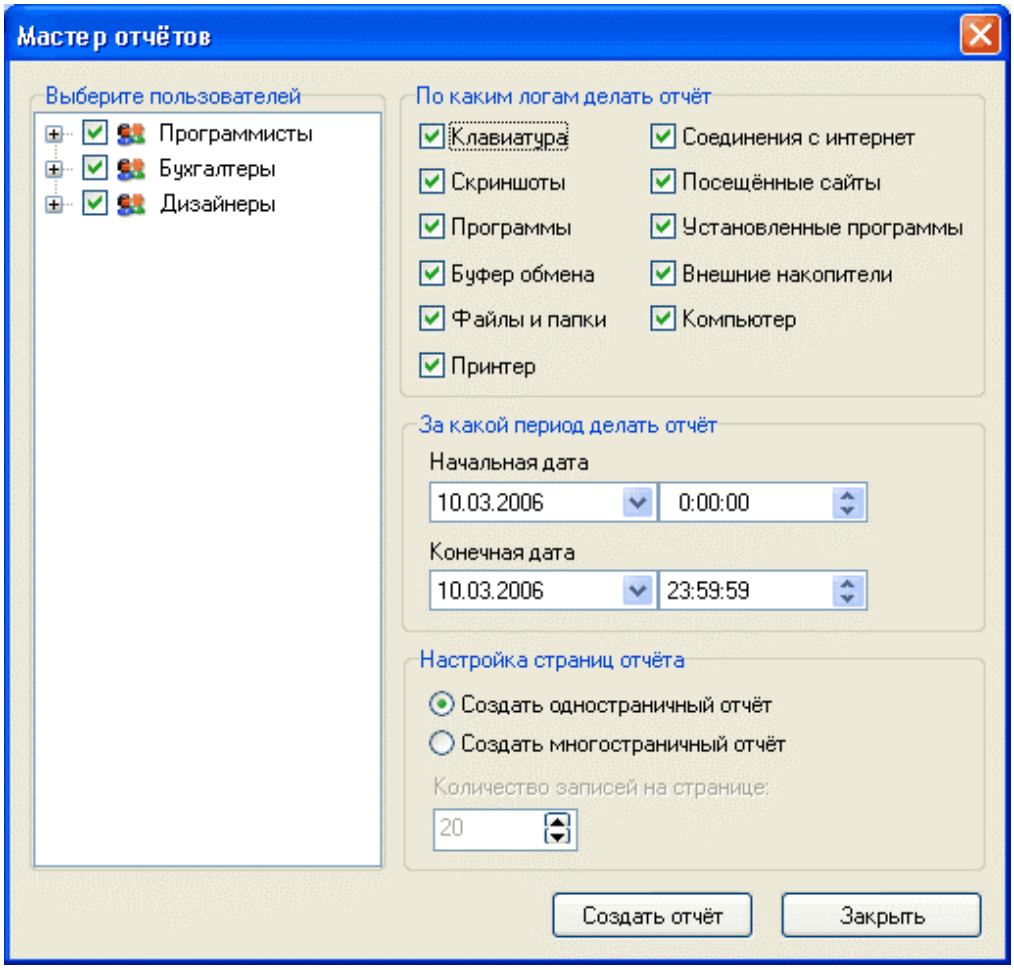


Рис. 42 – Окно конфигурации отчета

Выберите пользователей:

Выберите, установив галочку, тех пользователей, данные по которым вы хотите видеть в отчете.

По каким логам делать отчёт:

Клавиатура - установите эту галочку, если хотите включить в отчёт информацию о нажатых клавишах.

Скриншоты - установите эту галочку, если хотите включить в отчёт сделанные программой скриншоты.

Программы - установите эту галочку, если хотите включить в отчёт информацию о запущенных/закрытых программах.

Буфер обмена - установите эту галочку, если хотите включить в отчёт информацию о содержимом буфера обмена.

Файлы и папки - установите эту галочку, если хотите включить в отчёт информацию об изменениях в файловой системе.

Компьютер - установите эту галочку, если хотите включить в отчёт информацию о включении/выключении компьютера.

Соединения с интернет - установите эту галочку, если хотите включить в отчёт информацию о выходах в интернет.

Посещённые сайты - установите эту галочку, если хотите включить в отчёт информацию о веб-сайтах, на которых был пользователь.

Принтер - установите эту галочку, если хотите включить в отчёт информацию об отправленных на печать документах.

Установленные программы - установите эту галочку, если хотите включить в отчёт информацию о установленных и удаленных программах.

Внешние накопители - установите эту галочку, если хотите включить в отчёт информацию о подключенных и отключенных носителях информации.

За какой период делать отчёт:

Начальная дата - дата, начиная с которой включать данные в отчёт.

Конечная дата - дата, до которой включать данные в отчёт.

Настройка страниц отчёта:

Создать одностраничный отчёт - будет создана одна html-страница. Не рекомендуем создавать одностраничный отчёт, если у Вас много записей.

Создать многостраничный отчёт - будет создано несколько html-страниц. Количество страниц отчёта зависит от того, сколько записей Вы хотите разместить на одной странице.

Количество записей на странице - выберите количество записей, которое будет располагаться на каждой странице многостраничного отчёта.

4.10.2 Создание отчёта

После того, как Вы установили все параметры создания отчёта, нажмите кнопку **"Создать отчёт"**.

Появится диалоговое окно, в котором Вам необходимо указать путь, по которому следует сохранить отчёт.
Если сохранение отчёта займёт длительное время, то увидите прогрессию, которая будет информировать Вас о ходе работы.

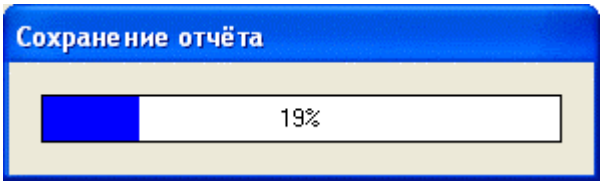


Рис. 43 – Сохранение отчета

После того, как отчёт будет сохранён, Вы сможете просмотреть его.

4.11 Удаление программы

Если возникла необходимость произвести удаление программы, например при переходе на следующую версию программы, то это производится в два этапа: удаление базовой части (программы Администратор) и удаление агентов с контролируемых компьютеров.

4.11.1 Удаление программы LanAgent с компьютера администратора

Для удаления базовой программы LanAgent вы можете использовать стандартные средства Windows, 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 "LanAgent" и нажмите кнопку "Удалить" ("Remove").

4.11.2 Удаление агентов

Для локального удаления агента с компьютера, необходимо запустить на нем файл "user.msi" и далее в меню выбрать вариант "Удалить" ("Remove").

Удаленное удаление агентов на данный момент реализовано для сетей с доменом.

Создание распределительного пункта (distribution point)

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

1. Зайдите на публичный сервер под администратором

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

Создания объекта групповой политики (GPO)

1. Запустите оснастку **Active Directory – пользователи и компьютеры** (Active Directory Users and Computers).
   *Примечание: Оснастку **Active Directory – пользователи и компьютеры** можно запустить так: Пуск, Программы, Администрирование, Active Directory – пользователи и компьютеры.*

2. В дереве консоли кликните правой клавишей мышки на вашем домене и выберите свойства.
3. Перейдите на вкладку **Групповая политика** и нажмите **Создать**.
4. Напишите желаемое имя вашей политики (например ***LanAgent distribution***) и нажмите **Enter**.
5. Нажмите **Свойства** и перейдите на вкладку **Безопасность**.
6. Отметьте **Применение групповой политики** для необходимой группы, затем нажмите **OK**.

Удаление пакета

1. Запустите оснастку **Active Directory – пользователи и компьютеры** (Active Directory Users and Computers).
2. Кликните правой клавишей мыши на имени вашего домена и выберете **Свойства**.
3. Перейдите на вкладку **Групповая политика** и выбрав нужную политику нажмите **Изменить**.
4. Разверните ветвь **Конфигурация компьютера**, **Конфигурация программ**
5. Выберите ту программу, которую вы желаете обновить и кликнете на ней правой клавишей мыши в появившемся окне выберите **Все задачи**, **Удалить**.
6. Выберите одно из следующего:

   - **Немедленное удаления этого приложения с компьютеров всех пользователей**
   - **Разрешить использование уже установленного приложения но запретить установку нового**

7. Выйдите из групповой политики и нажмите **OK**.

5 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.

5.1 Типичные действия

1 Добавление компьютера в список мониторинга

Для добавления нового компьютера в список мониторинга, необходимо нажать кнопку "Добавить" 

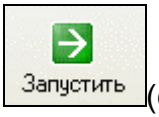
панели инструментов LanAgent или выбрать соответствующий пункт "Добавить пользователя" из меню "Файл".

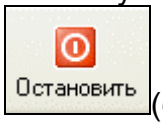
2. Удаление компьютера из списка мониторинга

Для удаления определенного компьютера из списка мониторинга, необходимо встать на строку, соответствующую данному компьютеру в списке и нажать кнопку "Удалить" 

панели инструментов LanAgent или выбрать соответствующий пункт "Удалить пользователя" из меню "Файл".

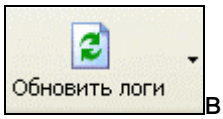
3. Запуск или остановка мониторинга на нужном компьютере

Для запуска или остановки мониторинга, выберите из списка мониторинга (таблица в левой части программы) нужный компьютер. Далее щелкните на кнопке "Запустить" 

(если хотите запустить мониторинг) или "Остановить" 

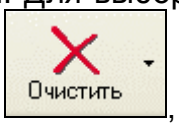
(если хотите его остановить). Эти же действия можно выполнить, выбрав соответствующие пункты из меню "Управление".

4. Обновление логов

Обновить логи можно нажав кнопку "Обновить логи" 

в панели инструментов или выбрав соответствующий пункт "Обновить логи пользователей" в меню "Управление". При этом произойдет обновление логов для всех запущенных пользователей.

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".

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.

5.2 Часто задаваемые вопросы

1. Как просмотреть снимки экранов мониторов (скриншоты)?

Выберите интересующий вас компьютер из списка компьютеров для 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 в операционных системах семейства Windows:

- Windows 98
- Windows ME
- Windows NT
- Windows 2000/Server
- Windows XP
- Windows 2003 Server

3. Каковы системные требования программы LanAgent?

Ввиду клиент-серверной архитектуры программы LanAgent требования к аппаратному обеспечению формулируются для каждого компонента отдельно.

Администраторская часть.

Минимальные требования:

- Операционная система: Windows 98/Me/2000/XP.
- Процессор Pentium 3 и выше.
- 128 MB оперативной памяти.
- 30 MB свободного места на диске.

Рекомендуемые требования:

- Операционная система: Windows 98/Me/2000/XP.
- Процессор Pentium 4 с частотой не менее 2 GHz.
- 512 MB оперативной памяти.
- 15 GB свободного места на диске (зависит от количества компьютеров и настроек программы).

Пользовательская часть (агент).

Минимальные требования:

- Операционная система: Windows 98/Me/2000/XP.
- Процессор Pentium 2 и выше.
- 32 MB оперативной памяти.
- 5 MB свободного места на диске.

Рекомендуемые требования:

- Операционная система: Windows 98/Me/2000/XP.
- Процессор Pentium 3 и выше.
- 128 MB оперативной памяти.
- 100 MB свободного места на диске.

4. В каком виде хранится информация на компьютерах пользователей?

На компьютерах пользователей собранная информация хранится в зашифрованных файлах. Она будет храниться там до тех пор, пока от администраторской части не поступит запрос на получение логов. После отправки лог-файлы на контролируемом компьютере будут очищены. Информация обмена между базовой частью и агентом передается по сети в зашифрованном виде. Для доступа к агентам используется система паролей. После получения информации базовой частью, она помещается в централизованную базу данных.

5. Как долго может храниться информация у пользователя?

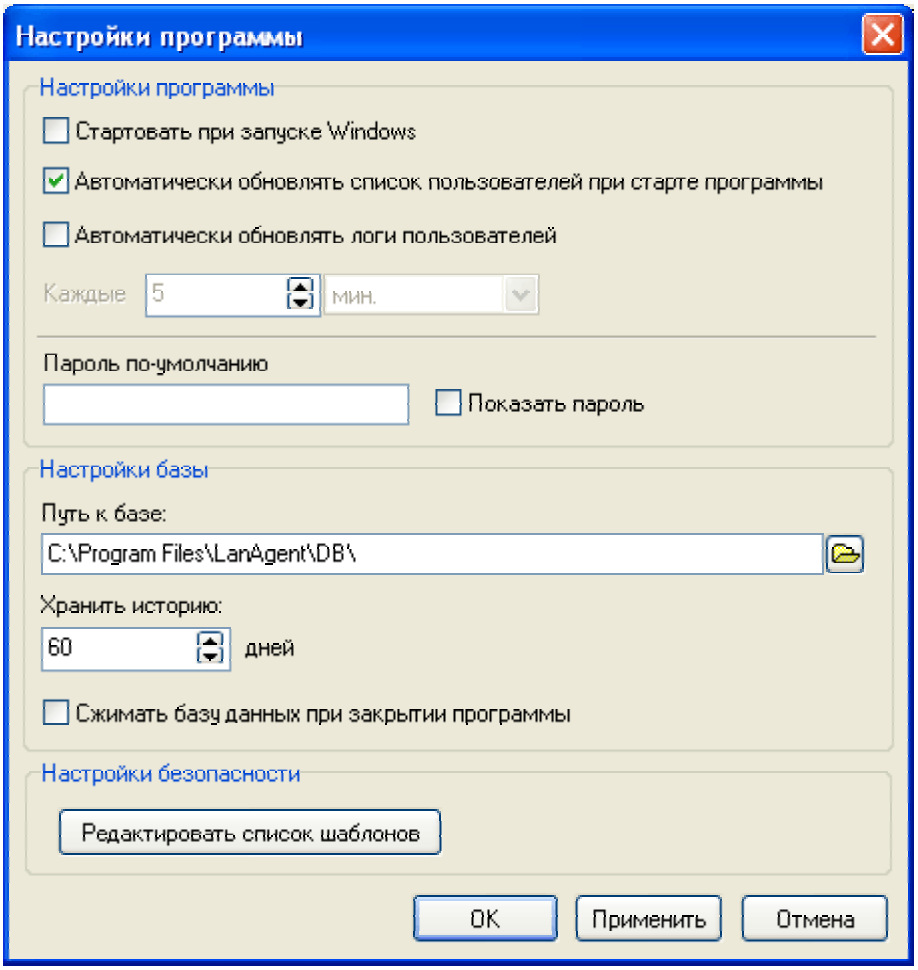
Логи на компьютере пользователя могут храниться сколь угодно долго. Теоретически их размер ограничен только размером свободного дискового пространства. Тем не менее имеется возможность ввести ограничение на их размер, тогда при его превышении будет происходить постепенное затирание старой информации более новой. Начнется оно с наиболее старых записей.

6. Агент установлен на компьютере пользователя, но добавить его в список в администраторской части программы не получается.

Возможно вы неправильно ввели ip-адрес компьютера пользователя. Возможно у вас проблемы с локальной сетью; попробуйте пропинговать компьютер пользователя.

7. Как установить срок хранения логов в базе?

Для этого в главном меню программы выберите "Опции->Настройки программы". В нижней части открывшегося окна имеется пункт "Хранить историю". Задайте здесь требуемую длительность хранения в днях и нажмите кнопку "Применить".



8. Как создать резервную копию базы?

Подробное описание процессов создания резервной копии базы и восстановления базы из резервной копии приведено в разделе 4.8.