Network
PROFI

LanAgent

Владея информацией,
владеешь миром

Руководство пользователя

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, а также позволяет заблокировать запуск определенных программ (по принципу списка запрещенных приложений).
- Определяет подключение и отключение носителей информации.
- Делает снимки экранов мониторов.
- Запоминает набираемый на клавиатуре текст.
- Перехватывает сообщения ICQ и Mail.ru Agent
- Следит за содержимым буфера обмена.
- Производит теневое копирование файлов, копируемых на съемные usb носители или редактируемых на них.
- Позволяет заблокировать подключение таких типов устройств как USB накопители, CD/DVD ROM, флоппи-дисководы, а также создать список разрешенных USB накопителей.
- Перехватывает посещённые сайты.
- Ведет мониторинг входящей и исходящей электронной почты.
- Перехватывает почту, отправляемую через web интерфейс, а также выгружаемые в интернет файлы.
- Позволяет заблокировать посещение определенных сайтов (по принципу белых и черных списков).
- Запоминает установку и удаление программ.
- Ведет статистику создания и удаления файлов.
- Ведет учет документов, отправленных на печать на принтер.
- Отслеживает включение/выключение компьютера.

- Логирует работу с общими ресурсами компьютера.
- Расширенная система аналитических отчетов.
- 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.

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 порты: 47658 и 7657. 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 XP/2003/2008/Vista/7/8/8.1/10/2012/.
- Процессор с частотой 1 Ггц.
- 512 MB оперативной памяти.
- 300 MB свободного места на диске.
- Открытые порты TCP/IP: входящий - 7657; исходящий – 47658.

Рекомендуемые требования:

- Операционная система: Windows XP/2003/2008/Vista/7/8/8.1/10/2012.
- Процессор с частотой не менее 2 Ггц.
- 1 ГБ оперативной памяти.
- 15 ГБ свободного места на диске (зависит от количества компьютеров и настроек программы).
- Открытые порты TCP/IP: входящий - 7657; исходящий – 47658.

Пользовательская часть (агент).

Минимальные требования:

- Операционная система: Windows XP/Vista/7/8/8.1/10.
- Процессор Pentium 3 и выше.
- 512 MB оперативной памяти.
- 100 MB свободного места на диске.
- Открытые порты TCP/IP: входящий – 47658; исходящий – 7657.

Рекомендуемые требования:

- Операционная система: Windows XP/Vista/7/8/8.1/10.
- Процессор с частотой 1 Ггц и выше.
- 1 ГБ оперативной памяти.
- 300 MB свободного места на диске.
- Открытые порты TCP/IP: входящий – 47658; исходящий - 7657 (если используется фаервол, то надо в нем их открыть)

Для просмотра видео/аудио записей, выполненных с web камеры, установленной на контролируемом компьютере, на компьютере с административной консолью понадобится медиа - проигрыватель.

Для просмотра изображений отправленных на печать документов, на компьютере с административной частью потребуется программа просмотра pdf документов.

2 Регистрация LanAgent

2.1 Активация программы

Если у вас уже приобретена лицензия, то ниже инструкция по ее активации. Если у вас пока ознакомительная версия, то она будет работать без регистрации 15 дней.

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.

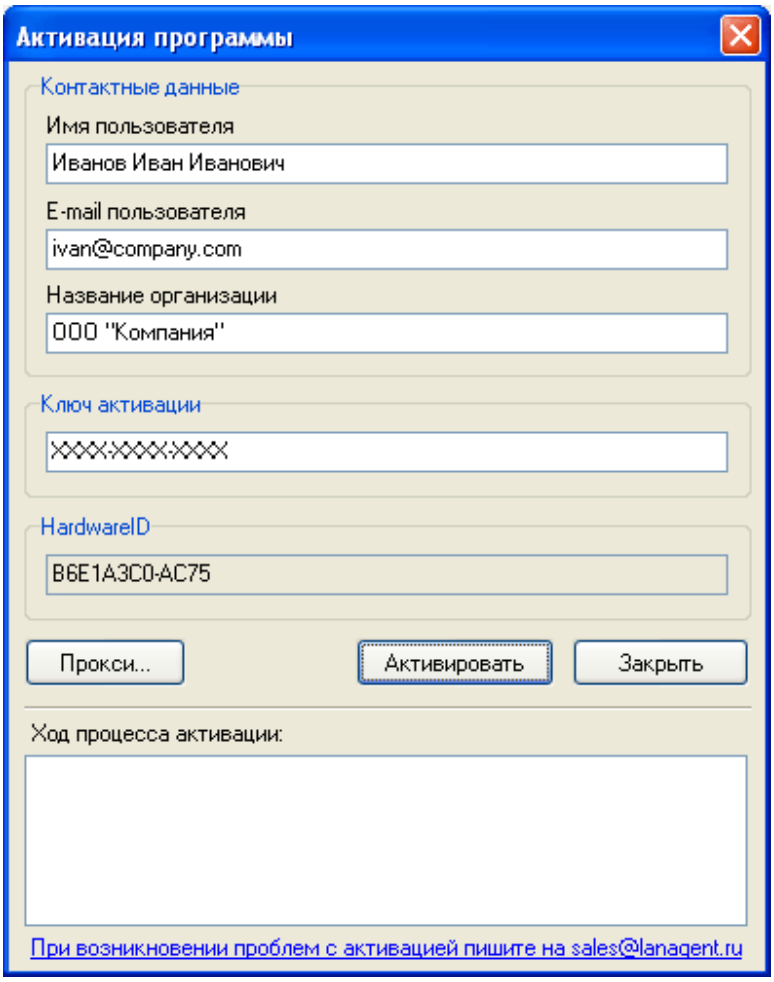


Рис. 2.1 - Активация программы

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

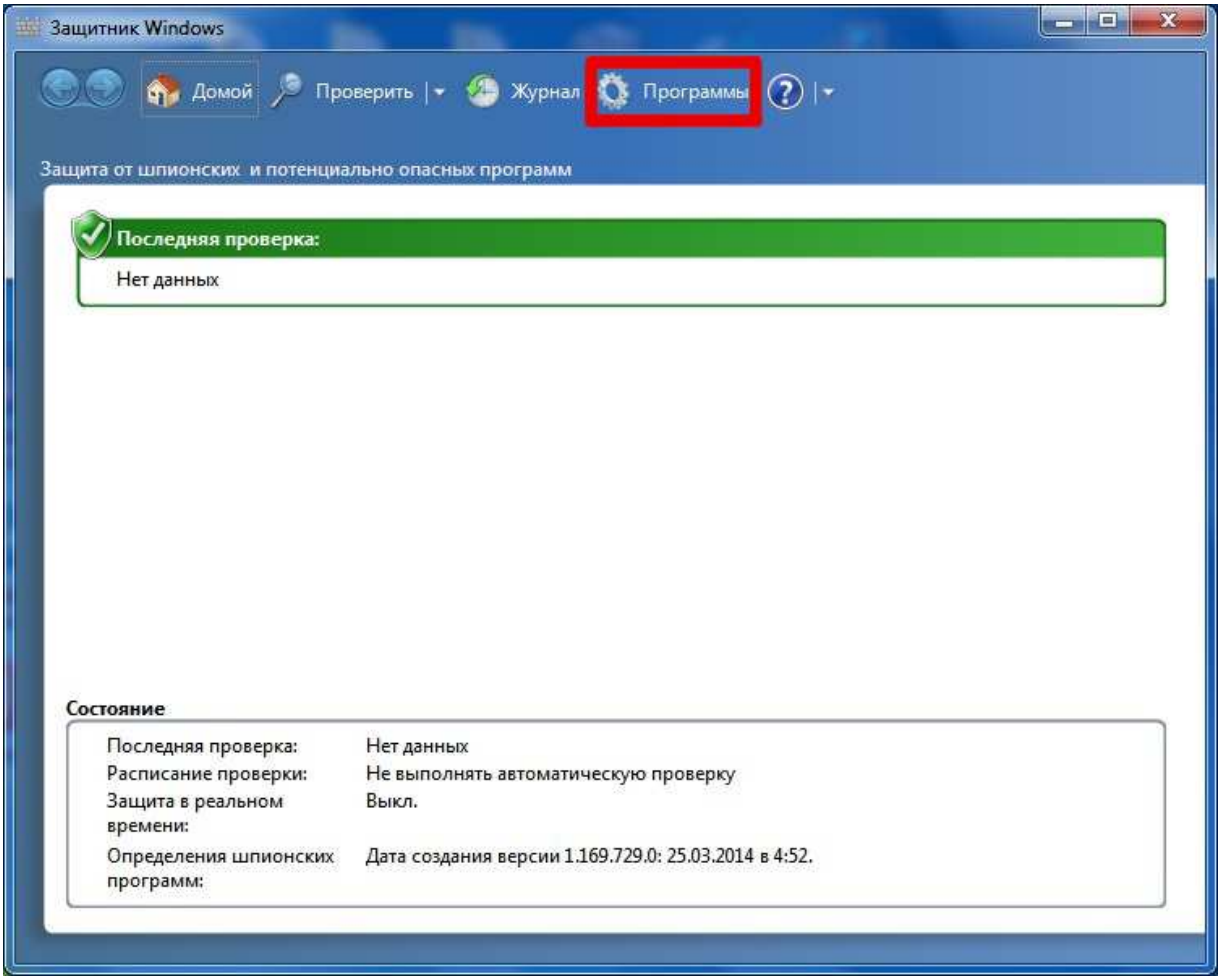
3.2 Настройка антивирусов

3.2.1 Защитник Windows

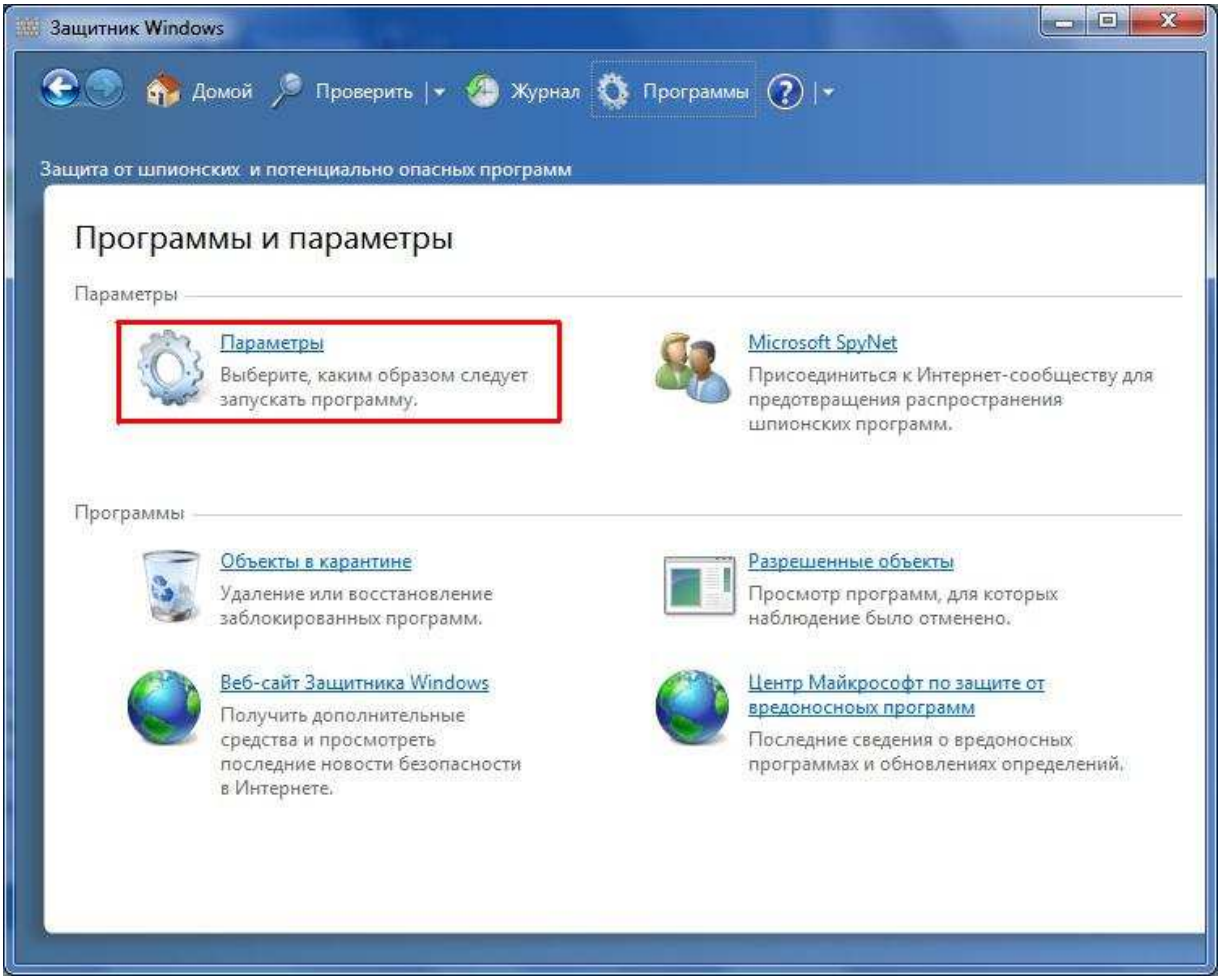
На компьютерах с операционной системой Windows 7/8/10 по умолчанию включен Защитник windows, это встроенный антивирус от Майкрософт. Не путайте его, пожалуйста, с брандмауером, это разные программы. Для корректной работы агента, желательно внести в настройках «Защитника» исключение на каталог установки агента. Это можно сделать как локально (непосредственно на контролируемом компьютере), так и через групповые политики.

Локальная настройка

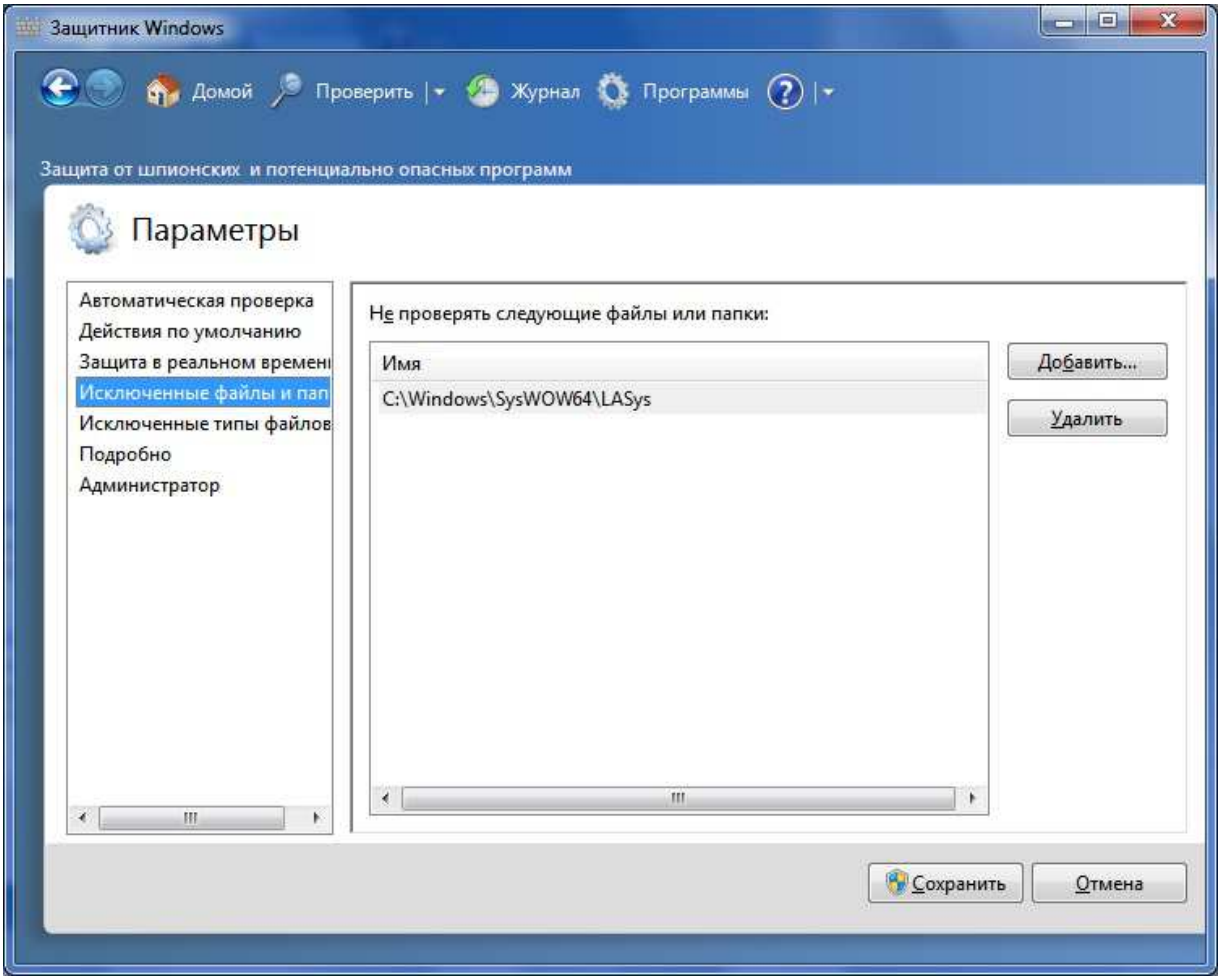
Для локальной настройки, выполните Пуск – в строке поиска программ наберите Защитник – выберите программу «Защитник Windows» из предложенного списка.



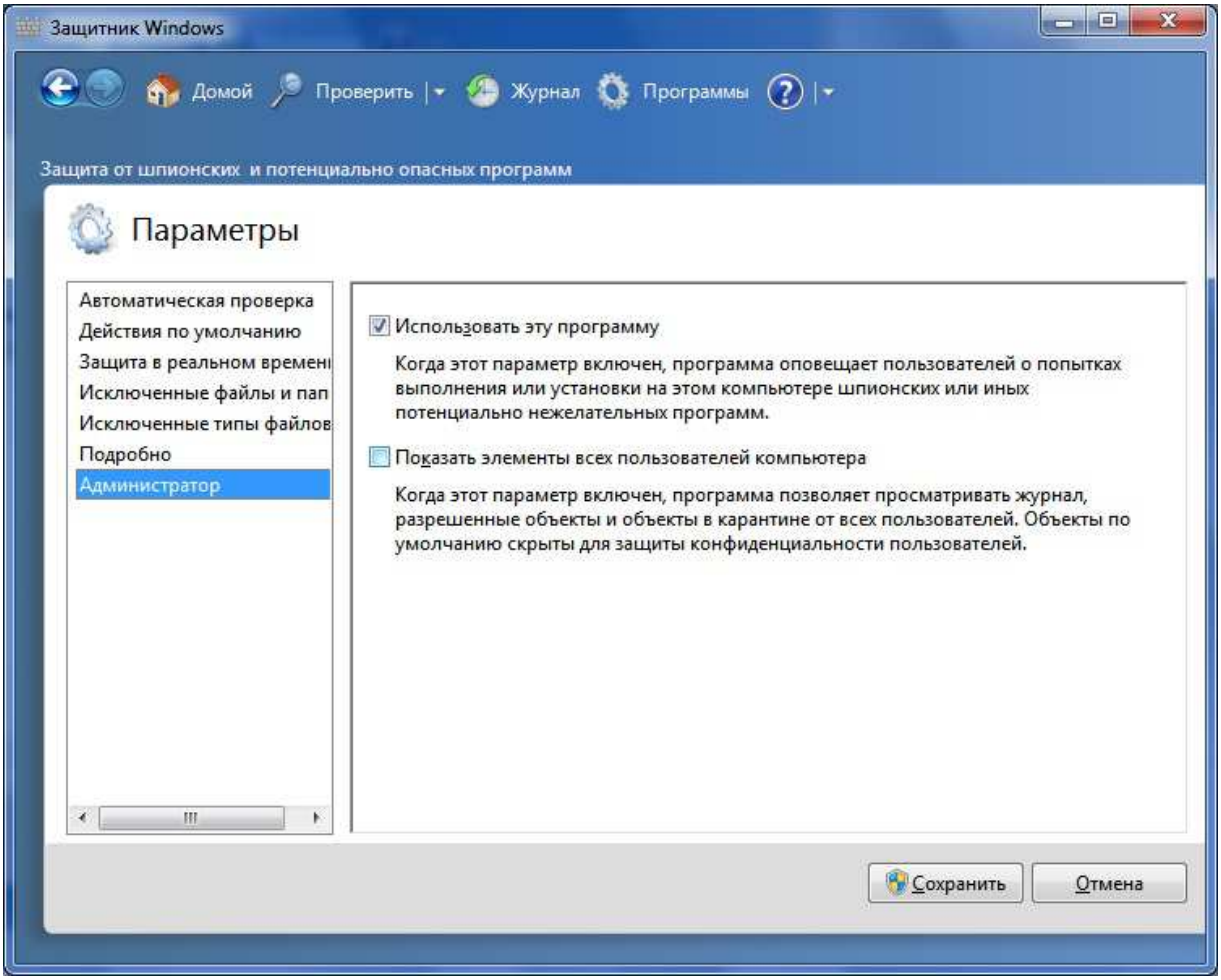
В открывшемся приложении нажмите кнопку «Программы» в верхнем меню. Далее, нажмите кнопку Параметры.



Перейдите на пункт «Исключенные файлы и папки». Надо добавить в исключение каталог установки агента. Для 32 битных систем это system32\lasys, для 64 битных систем – syswow64\lasys. Каталог скрытый и системный. Для того, чтобы Защитник Windows смог его увидеть, надо в проводнике нажать Alt, в появившемся меню выбрать Сервис – Параметры папок… В открывшемся окне перейти на пункт Вид и там поставить галочку на пункте «Показывать скрытые файлы, папки и диски» и убрать галочку с пункта «Скрывать защищенные системные файлы». После этого в перечне папок для исключений появится папка LASys. После ее добавления указанные опции можно вернуть к исходному состоянию.



Если на компьютере установлен качественный антивирус, то Защитник windows можно и совсем отключить. Для этого надо убрать галочку «Использовать эту программу» на пункте «Администратор».



Настройка Защитника через групповые политики.

Дистанционная настройка защитника заключается в добавлении на нужные компьютеры ключей реестра. Ниже указаны конкретные ветки:

Ключ реестра для отключения Защитника:
;Использовать эту программу
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows Defender]
"DisableAntiSpyware"=dword:00000000

Исключение каталога
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows Defender\Exclusions\Paths]
"ИМЯ_ПАПКИ"=dword:00000000

Где в названии параметра «ИМЯ_ПАПКИ» нужно ввести полный путь к папке или файлу, который будет исключен из сканирования.

Пример:
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows Defender\Exclusions\Paths]
"C:\windows\system32\lasys"=dword:00000000

Для 64 битных систем ключ будет:
"C:\windows\syswow64\lasys"=dword:00000000

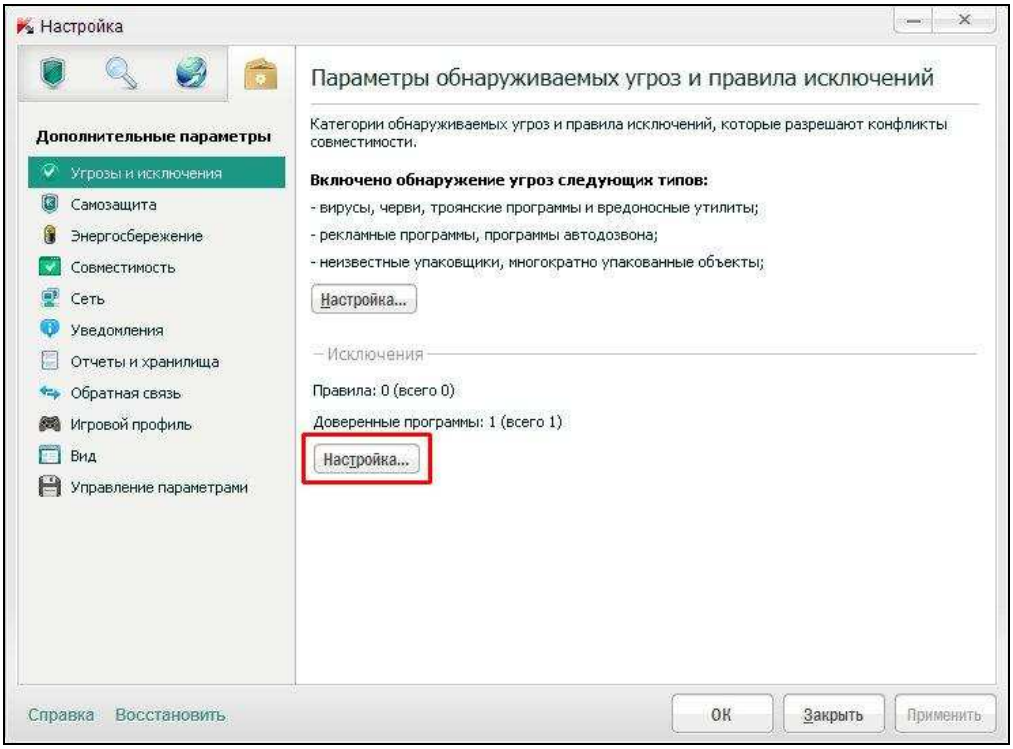
3.2.2 Антивирус Касперского

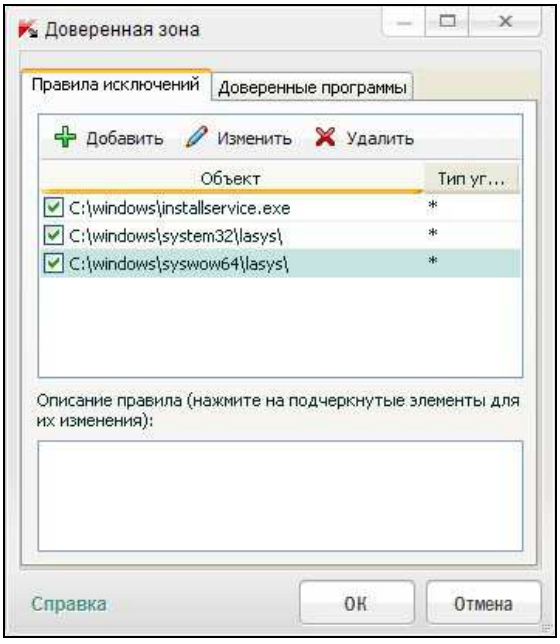
Для успешной дистанционной установки агента средствами программы LA Admin, желательно на целевом компьютере внести в исключение путь до файла инсталляции агента C:\windows\installservice.exe и Admin$\installservice.exe Это один и тот же путь.

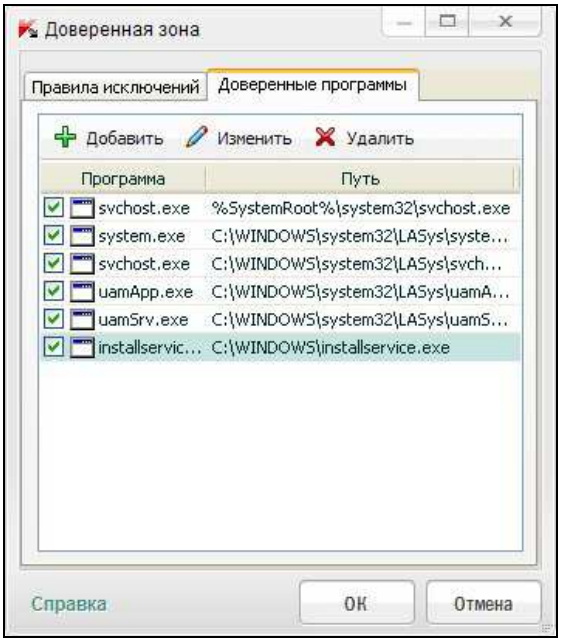
Все процессы следящего модуля имеют цифровую подпись и антивирусом не детектируются. Тем не менее, желательно внести в исключение антивируса либо сам каталог установки агента C:\windows\system32\lasys для 32 битных систем и syswow64\lasys для 64 битных, либо конкретные файлы system.exe, svchost.exe, uamApp.exe, uamSrv.exe, sys.dll, sysl.dll, laNetwork.exe из каталога установки агента.

Это позволит избежать «сюрпризов» в виде ложных срабатываний антивируса в будущем.

Особенность антивируса Касперского заключается в том, что в нем есть два места для внесения исключения: «Правила исключений» и «Доверенные программы». Вносить исключение надо в оба эти места.


Настройка
Параметры обнаруживаемых угроз и правила исключений
Дополнительные параметры
Угрозы и исключения
Самозащита
Энергосбережение
Совместимость
Сеть
Уведомления
Отчеты и хранилища
Обратная связь
Игровой профиль
Вид
Управление параметрами
Категории обнаруживаемых угроз и правила исключений, которые разрешают конфликты совместимости.
Включено обнаружение угроз следующих типов:
- вирусы, черви, троянские программы и вредоносные утилиты;
- рекламные программы, программы автодозвона;
- неизвестные упаковщики, многократно упакованные объекты;
Настройка...
Исключения
Правила: 0 (всего 0)
Доверенные программы: 1 (всего 1)
Настройка...
Справка
Восстановить
ОК
Закрыть
Применить


Доверенная зона
Правила исключений
Доверенные программы
Добавить
Изменить
Удалить
Объект
Тип уг...
C:\windows\installservice.exe *
C:\windows\system32\lasys\ *
C:\windows\syswow64\lasys\ *
Описание правила (нажмите на подчеркнутые элементы для их изменения):
Справка
ОК
Отмена



Эта часть общая для всех версий Касперского. Ее будет достаточно для большинства версий этого антивируса.

3.2.3 Антивирус НОД32

Принцип внесения исключений в НОД32 тот же, что и во все остальные антивирусы: для успешной дистанционной установки агента средствами программы LA Admin, желательно на целевом компьютере внести в исключение путь до файла инсталляции агента C:\windows\installservice.exe .

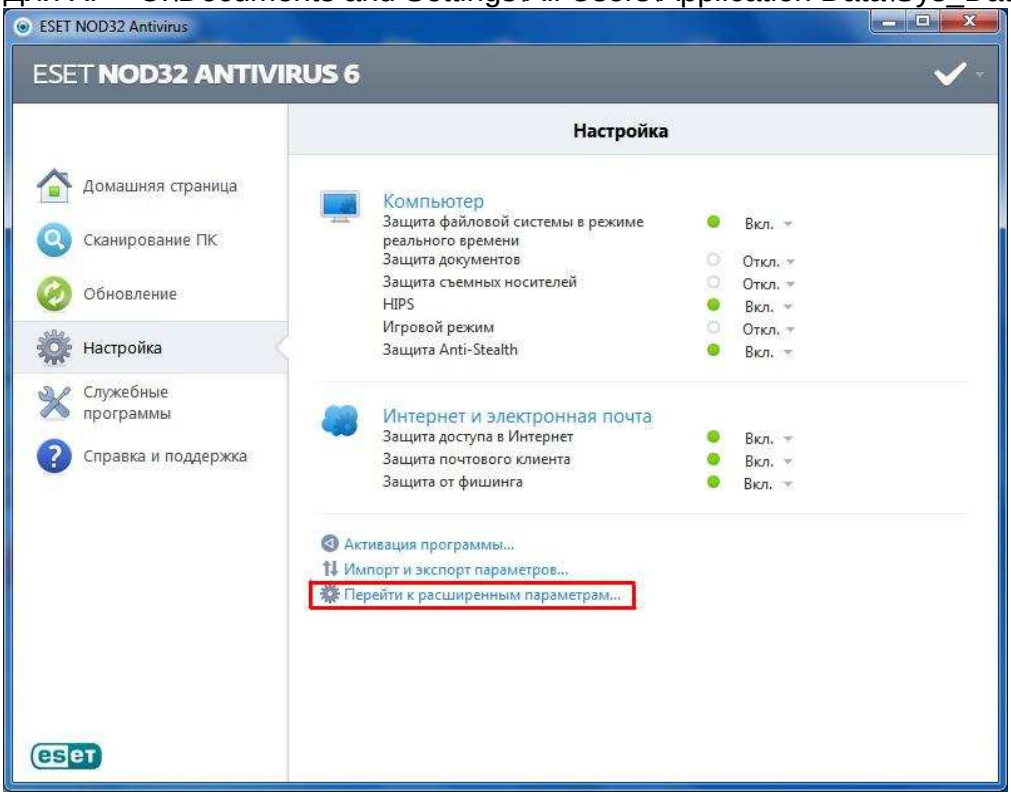
При инсталляции агента через msi файл, происходит распаковка файлов из пакета во временный каталог, поэтому, при возникновении сложностей с антивирусом, надо на это время или приостановить антивирус или опять же временно внести темповый каталог в исключение.

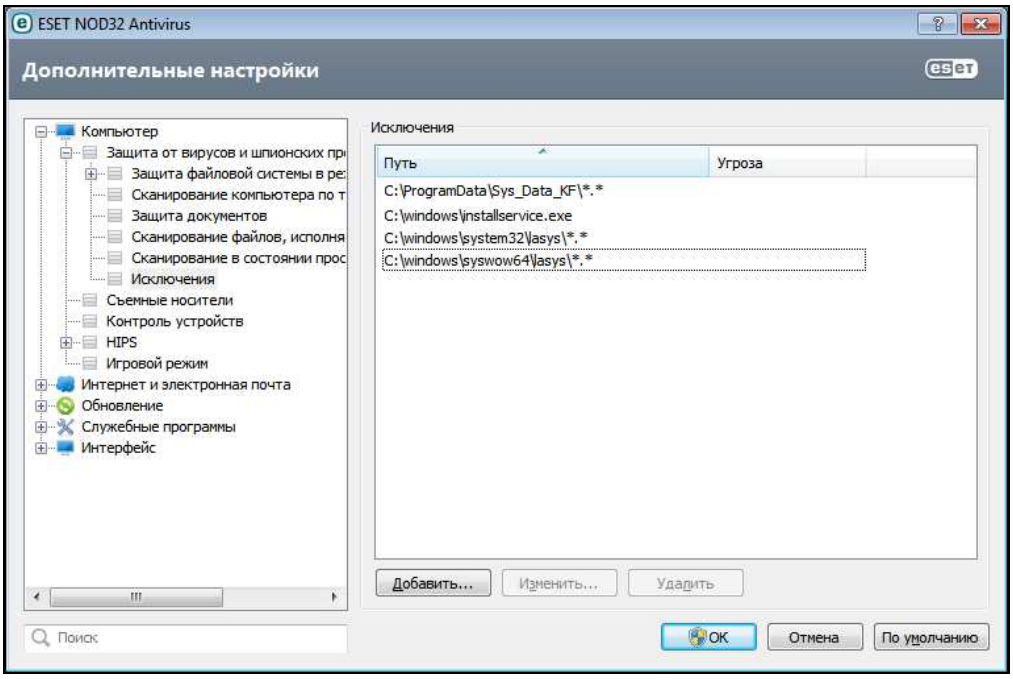
Все процессы следящего модуля имеют цифровую подпись и антивирусом не детектируются. Тем не менее, желательно внести в исключение антивируса либо сам каталог установки агента с файлами по маске: C:\windows\system32\lasys*.* для 32 битных систем и syswow64\lasys*.* для 64 битных, либо конкретные файлы system.exe, svchost.exe, uamApp.exe, uamSrv.exe, sys.dll, sysl.dll, laNetwork.exe из каталога установки агента.

Это позволит избежать «сюрпризов» в виде ложных срабатываний антивируса в будущем.

И для NOD32 надо добавить в исключение каталог временных файлов агента. На компьютерах с Windows 7 и новее это C:\ProgramData\Sys_Data_KF*.*

Для XP - C:\Documents and Settings\All Users\Application Data\Sys_Data_KF*.*





Это необходимо для того, чтобы файловый сканер антивируса не реагировал на файлы агента.

3.2.4 Антивирусы Avast, DrWeb, Avira.

Принцип внесения исключений в эти антивирусы тот же, что и во все остальные: для успешной дистанционной установки агента средствами программы LA Admin, надо на целевом компьютере внести в исключение путь до файла инсталляции агента C:\windows\installservice.exe .

При инсталляции агента через msi файл, происходит распаковка файлов из пакета во временный каталог, поэтому, при возникновении сложностей с антивирусом, надо на это время или приостановить антивирус или опять же временно внести темповый каталог в исключение.

Все процессы следящего модуля имеют цифровую подпись и антивирусом не детектируются. Тем не менее, желательно внести в исключение антивируса либо сам каталог установки агента с файлами по маске: C:\windows\system32\lasys*.* для 32 битных систем и syswow64\lasys*.* для 64 битных, либо конкретные файлы system.exe, svchost.exe, uamApp.exe, uamSrv.exe, sys.dll, laNetwork.exe из каталога установки агента.

Это позволит избежать «сюрпризов» в виде ложных срабатываний антивируса в будущем.

3.3 Установка агентов

3.3.1 Локальная установка агентов

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

3.3.2 Удаленная установка агентов

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

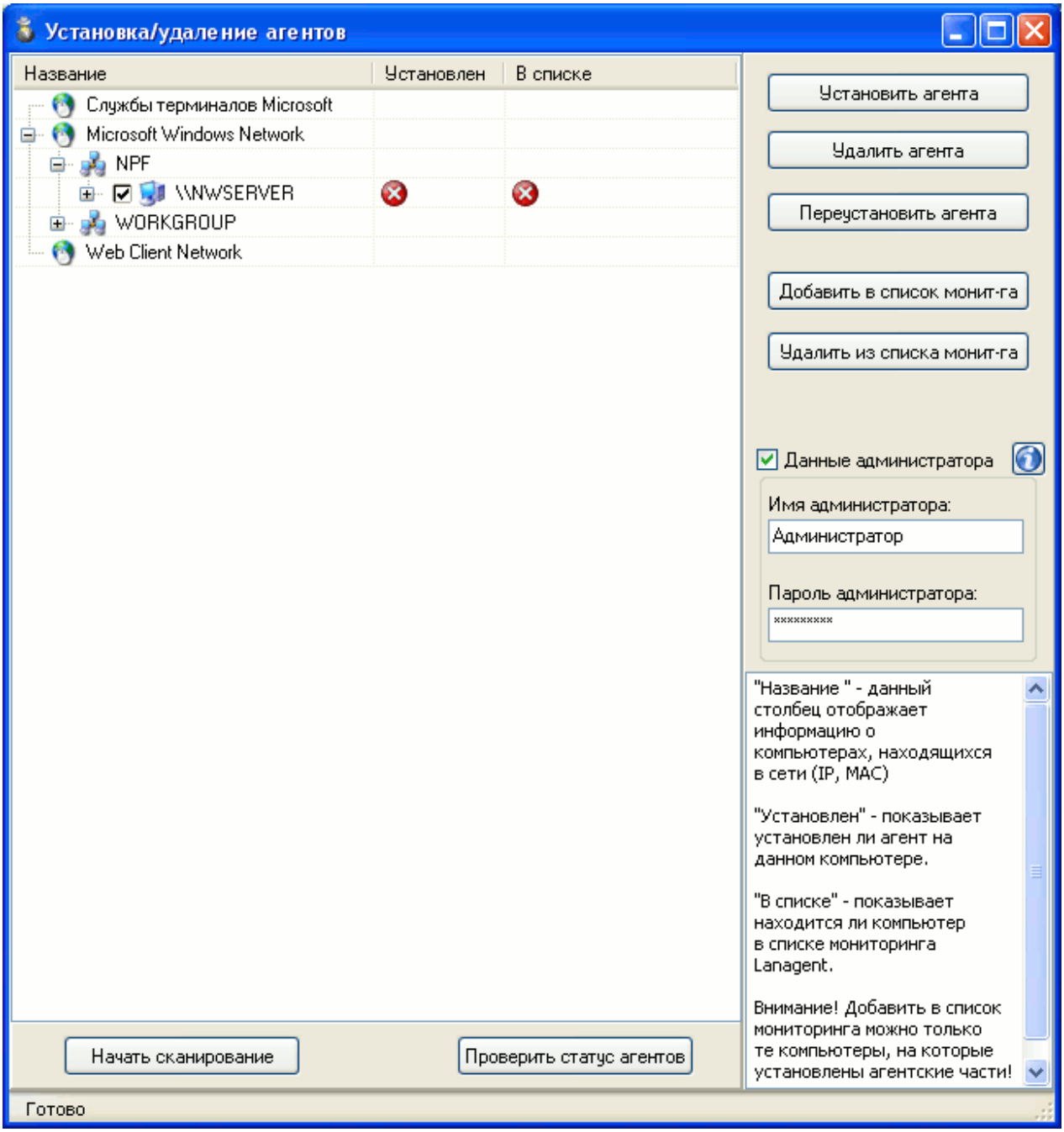
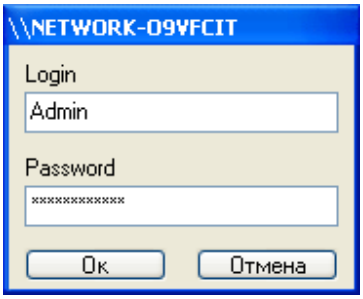


Рис 3.1 – Диалог установки/удаления агентов

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

Далее, надо отметить галочками компьютеры, на которые необходимо установить агентов и нажать кнопку "**Установить агента**". Если для всех выбранных

компьютеров может быть использована одна и та же связка логин/пароль, то можно задать ее один раз в панели в правой части окна и поставить галочку "Данные администратора" (так, как это сделано на экране выше). В противном случае для каждого выбранного компьютера будет вызван диалог ввода логина и пароля администратора.



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

Рекомендуем внести в исключение в антивирусе следующие пути: "Admin$\installservice.exe" и "C:\Windows\installservice.exe" это необходимо, чтобы антивирус не блокировал сам файл установки агента. Каталог установки агента по умолчанию system32\lasys для 32 битных и syswow64\lasys для 64 битных систем. Рекомендуем внести в исключение файлы агента (system.exe, svchost.exe, sys.dll, sysl.dll, la_print.dll, lanetmon.dll, uamApp.exe и uamSrv.exe) из данного каталога. В пункте 3.3 данного руководства есть более подробная информация по настройкам антивирусов.

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

3.3.3 Устранение возможных проблем при удаленной установке агентов

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

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

Возможные причины:

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

Проверьте еще раз их правильность.

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

Необходимо выключить данную опцию. Для этого откройте папку "Мой компьютер", в меню "Сервис" выберите пункт "Свойства папки...". Далее перейдите на вкладку "Вид" и уберите галочку на строке "Использовать простой общий доступ к файлам". Подтвердите изменения кнопкой "ОК" или "Применить".

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

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

4.Отсутствует служебный ресурс ADMIN$ на удаленном компьютере (для XP).

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

Параметр - AutoShareWks типа REG_DWORD

то установить его в "1".

Для операционной системы Windows 7 инструкция приведена ниже.

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

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

6.Не настроен фаервол.

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

7.Процесс установки блокируется антивирусом.

Рекомендуем внести в исключение в антивирусе следующие пути: "Admin$\installservice.exe" и "C:\Windows\installservice.exe" это необходимо, чтобы антивирус не блокировал сам файл установки агента. Каталог установки агента по умолчанию system32\lasys для 32 битных систем, syswow64\lasys – для 64 битных. Рекомендуем внести в исключение файлы агента (system.exe, svchost.exe, sys.dll,

sysl.dll, la_print.dll, lanetmon.dll, uamApp.exe и uamSrv.exe) из данного каталога. В пункте 3.3 данного руководства есть более подробная информация по настройкам антивирусов.

Установка агента на Windows Vista/ 7/8/8.1/10.

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

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

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

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

3.3.4 Установка агентов через групповые политики Active Directory

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

Назначение установки программы

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

Создание распределительного пункта (distribution point)

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

1. Зайдите на публичный сервер под администратором

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

Создания объекта групповой политики (GPO)

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

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

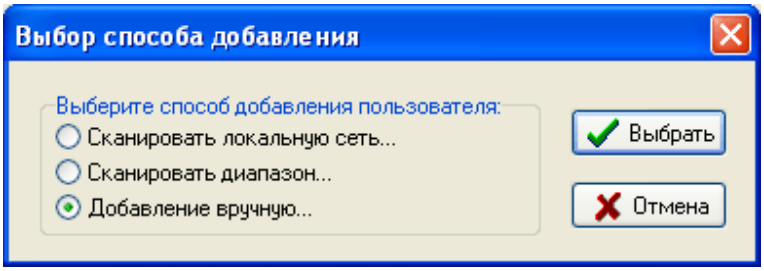
Для получения дополнительной информации по вопросу удаленной установки программного обеспечения в сети под управлением домена Windows обратитесь к базе знаний Microsoft:

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/)

3.4 Создание списка компьютеров для мониторинга

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

При этом откроется окно выбора способа добавления:



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

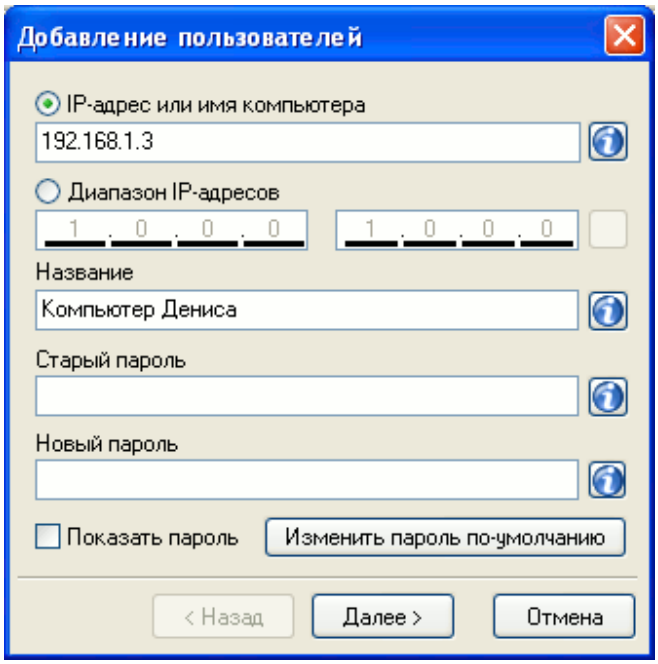


Рис. 3.2 - Добавление компьютера в список мониторинга

Добавить компьютеры в список можно 2-мя способами:

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

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

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

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

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

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

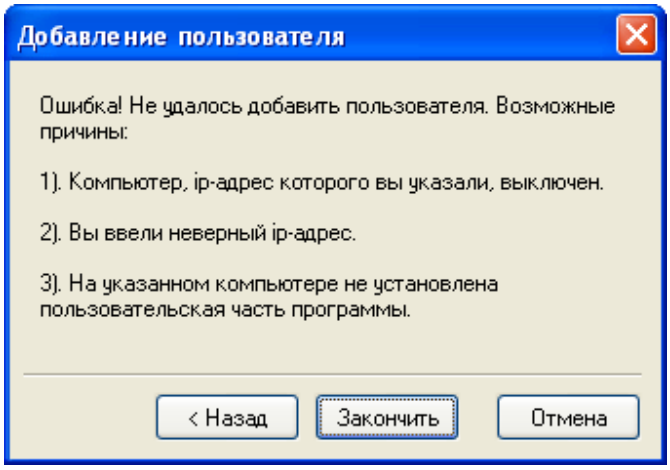


Рис. 3.3 – Ошибка добавления в список

Чтобы изменить параметры подключения, нажмите кнопку "Назад".

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

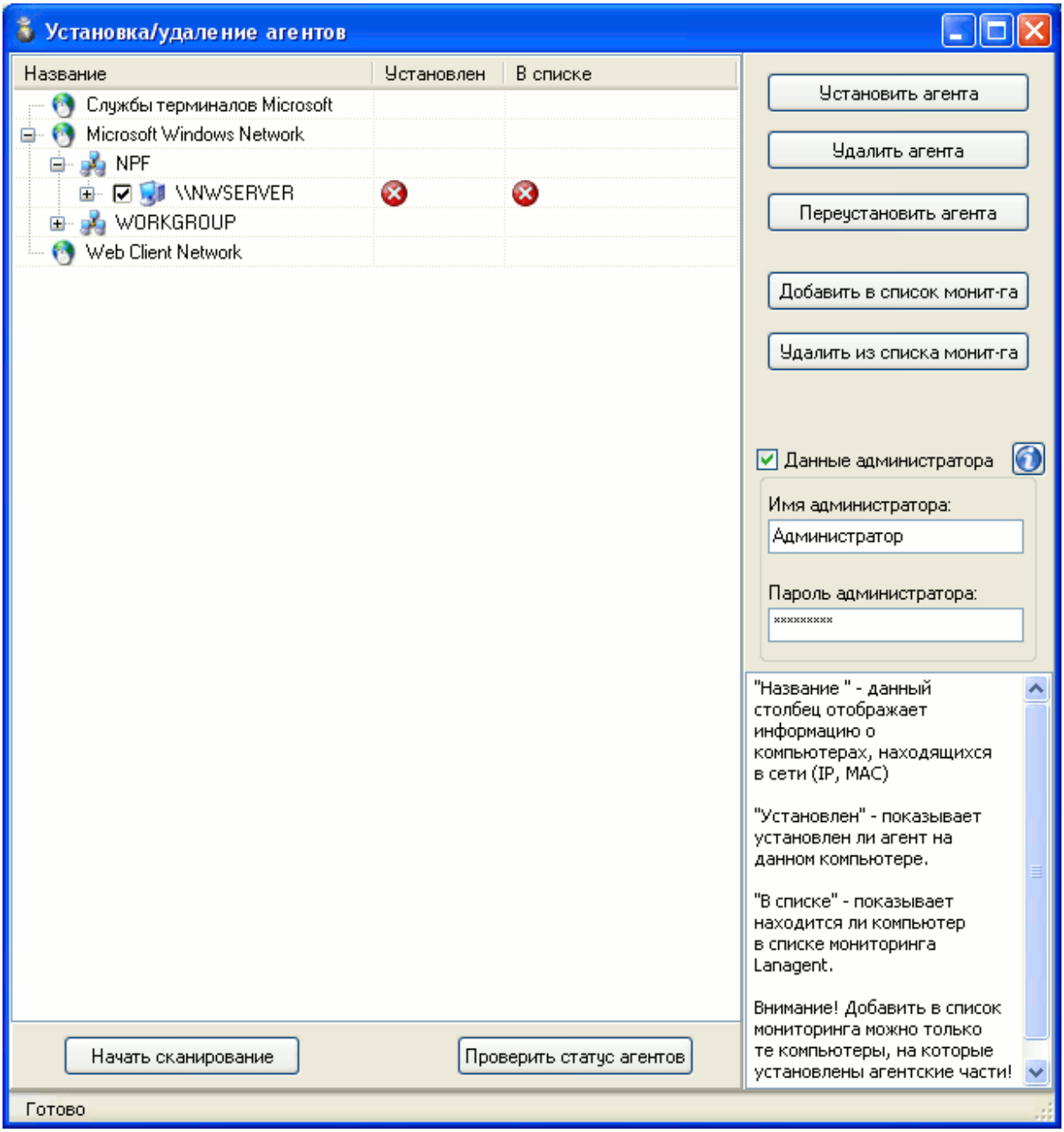
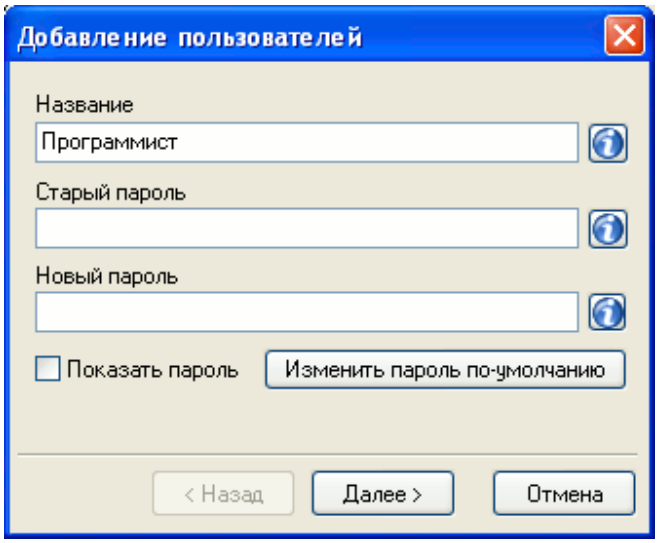


Рис. 3.4 – Диалог установки/удаления агентов

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

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

При этом откроется следующее диалоговое окно:

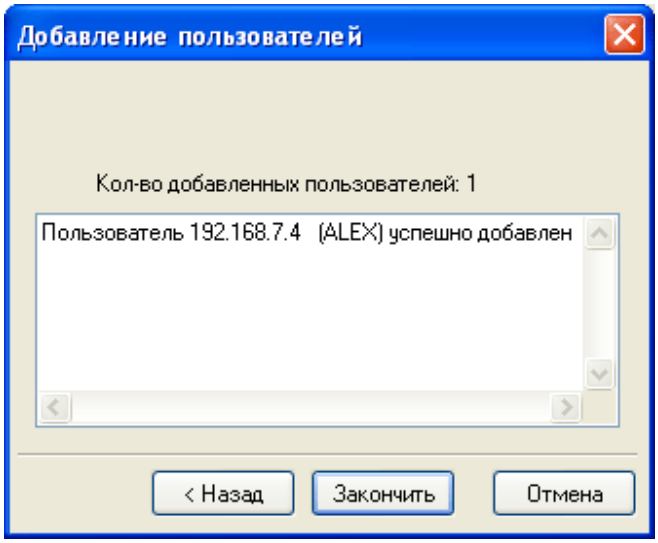


Если в предыдущем окне был выбран только один компьютер для добавления в список, то поле "Название" будет доступно для заполнения. Его содержимое в дальнейшем будет отображаться в списке мониторинга. Поэтому заполните его **понятным вам** названием. В случае добавления сразу нескольких компьютеров, данное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

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

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

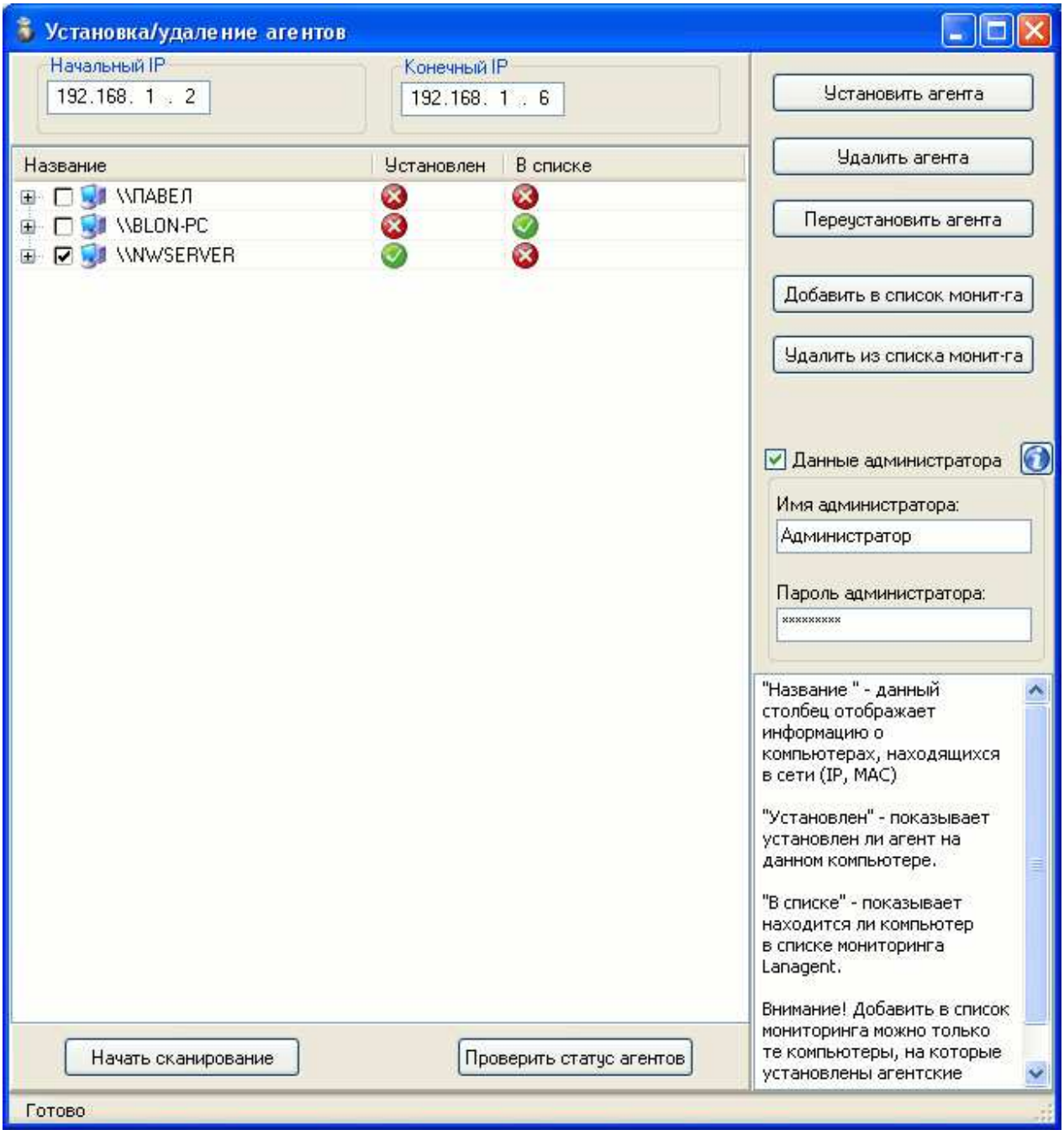
После нажатия кнопки "Далее", будет произведена проверка подключения к программе-агенту, установленной на контролируемом компьютере. Если подключение произведено успешно, то данный компьютер будет добавлен в список, иначе будет сообщено об ошибке.



Чтобы изменить параметры подключения, нажмите кнопку "Назад".

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

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



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

3.5 Создание групп пользователей

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

При этом откроется следующее диалоговое окно:

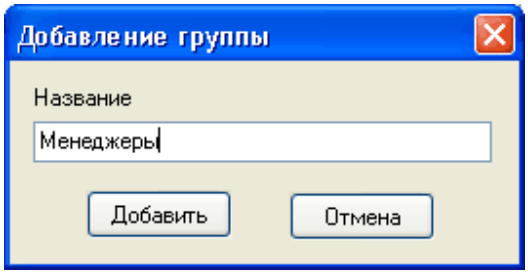


Рис. 3.5 – Добавление группы пользователей

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

3.6 Переход с предыдущих версий

При обновлении версии **LanAgent Standard**, преобразование базы данных производится автоматически. Перед установкой новой версии, рекомендуем сделать резервную копию базы (скопировав каталог базы DB в отдельное место на диске). Административная часть программы при этом должна быть закрыта. Рекомендуемый порядок обновления следующий:

1). деинсталлировать агентов текущей версии (тем способом и теми файлами, при помощи которых происходила установка).
2). сделать резервную копию базы на компьютере с административной частью программы.
3). поставить административную часть новой версии LanAgent поверх старой
4). установить агентов новой версии.

3.7 Исключение сайтов и программ из контроля агентом

Для того, чтобы производить контроль зашифрованного SSL трафика (веб почты, соц. сетей и др.), агент встраивается в сетевой обмен между браузером (или другой программой, генерирующей трафик) и интернет ресурсом. Это может мешать работе некоторых сайтов, таких как, банк – клиенты, т.к. они тщательно контролируют подлинность пользователя.

Для решения данного вопроса, достаточно внести такой интернет ресурс (или программу, если нужно чтобы агент перестал полностью контролировать ее трафик) в исключение фильтрации трафика в настройках агента.

Для этого запустите LA Admin, перейдите в ней в настройки клиентского модуля и откройте раздел Internet-логи. Там нажмите кнопку «Контролируемые порты и Исключения из фильтрации трафика». В открывшемся окне перейдите на вкладку «Исключения SSL», если требуется исключить из контроля трафика интернет-ресурс, либо на вкладку «Исключение приложений», если надо исключить из контроля трафика целиком программу.

Для исключения программы, надо внести в список имя ее исполняемого файла. Для исключения веб сайта, надо внести в список его домен без слешей и без “www”. Пример: sbrf.ru

4 Работа с программой

Интерфейс программы LanAgent включает в себя следующие элементы:

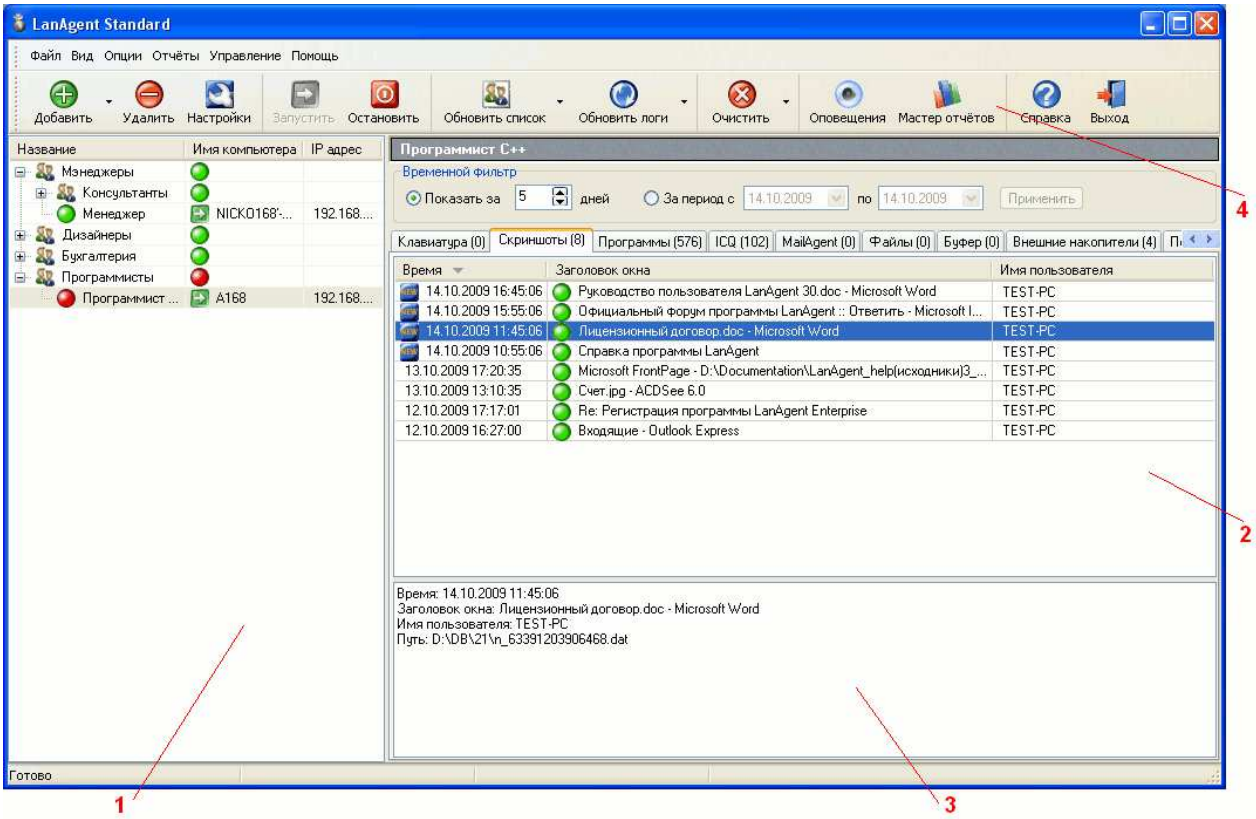


Рис. 4.1 – Главное окно программы

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

4.1 Список компьютеров для мониторинга

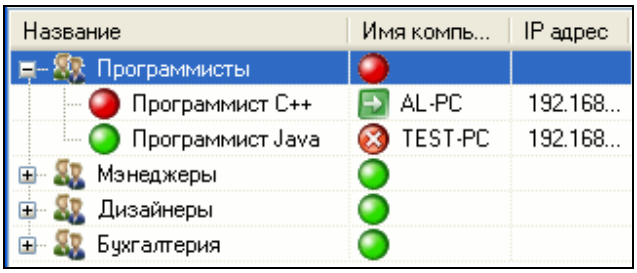


Рис. 4.2 – Окно списка мониторинга

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);

 - процесс агентского приложения был выгружен пользователем.

- 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);
- ICQ (сообщения, отправляемые и получаемые по протоколу icq)$
- MailAgent (сообщения получаемые и отправляемые с использованием программы Mail.ru Agent);
- 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 (история включения и выключения компьютеров пользователей);
- Теневое копирование (копия файлов, скопированных пользователем на съемные USB носители информации);
- Почта (переписка по электронной почте);
- MSN (сообщения, полученные и отправленные с использованием протокола MSN);
- Jabber (сообщения, полученные и отправленные с использованием протокола Jabber);
- Сеть:Доступ (информация по подключениям пользователей к общим ресурсам компьютера);
- Сеть:Файлы (информация о непосредственно обращениях к файлам на общих ресурсах компьютера);
- Skype Text (текстовая переписка в Скайпе);
- Skype Files (передаваемые через скайп файлы и записи разговоров);
- Соц. сети (сообщения передаваемые в соц. сетях);
- Web почта (письма, отправляемые через браузер);
- Выгрузка файлов (отображаются файлы, выгруженные в интернет через браузер);
- Webcam/microphone (записи видео и звука с веб камер, а также снимков с них).

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

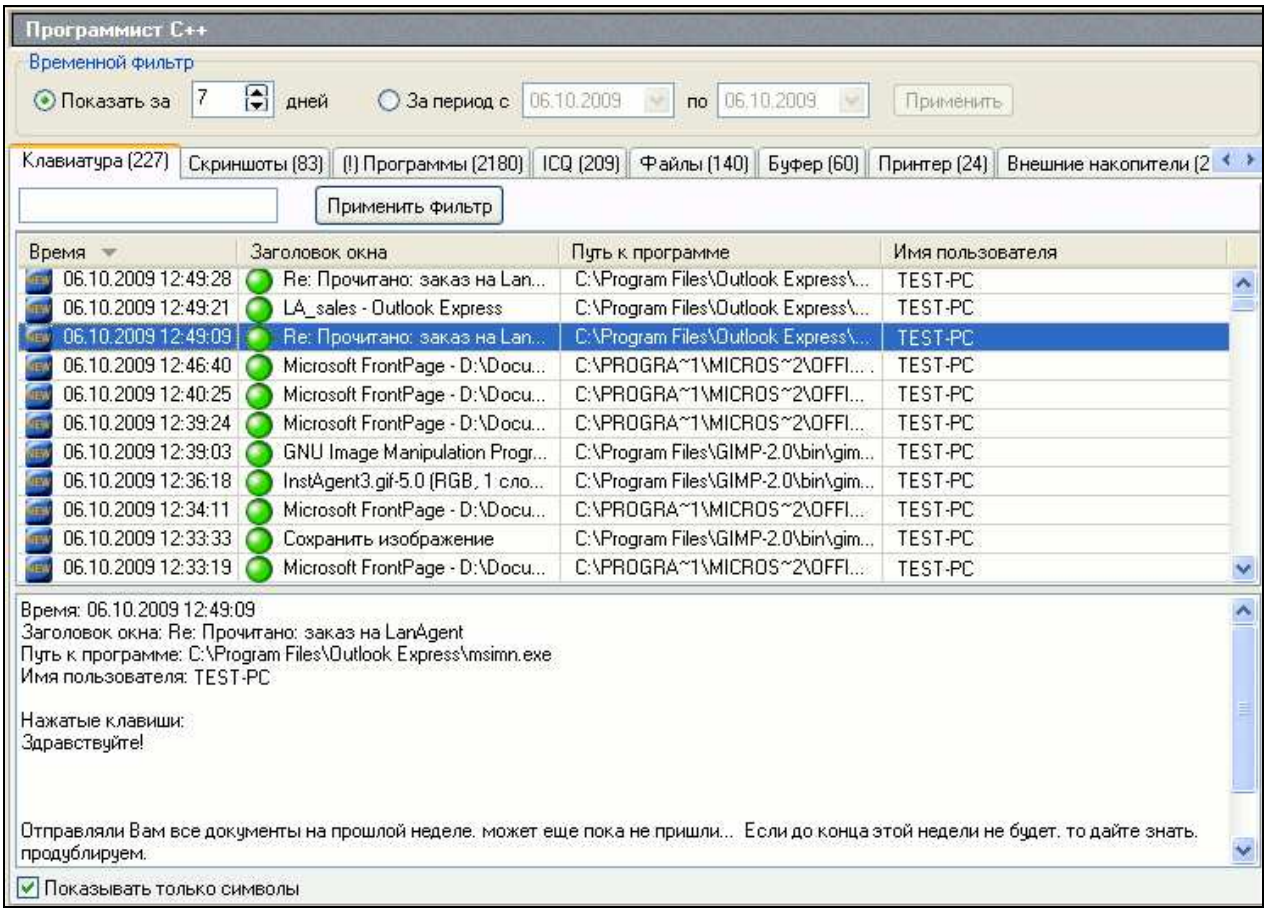


Рис. 4.3 – Окно логов клавиатуры

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.

По любой из категорий логов можно сформировать отчет - выборку именно по тем данным, которые Вы видите на экране. Для этого достаточно щелкнуть по любой из строк правой клавишей мыши и выбрать из выпадающего меню вариант "Сделать отчет".

4.2.2 Скриншоты

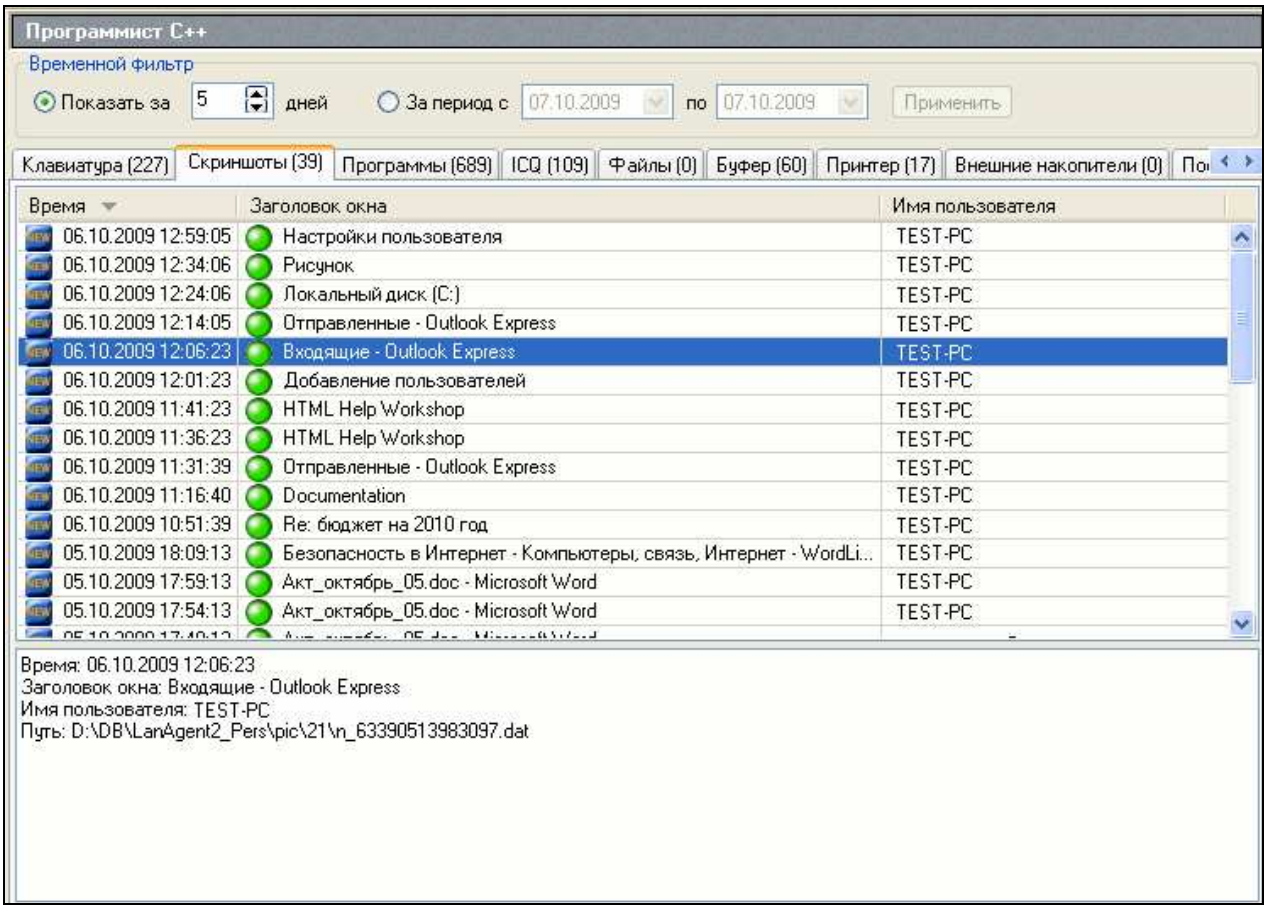


Рис. 4.4 – Окно логов снимков экранов (скриншотов)

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.

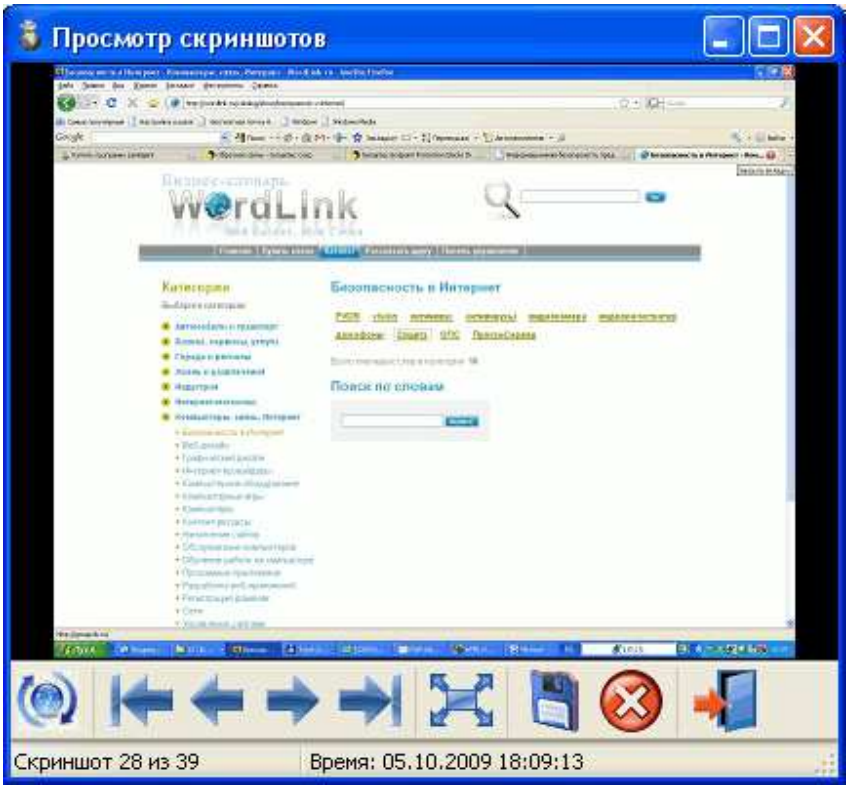


Рис. 4.5 – Окно просмотра скриншотов

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:

 - 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 все скриншоты.

 - закрыть окно просмотра скриншотов.

По любой из категорий логов можно сформировать отчет - выборку именно по тем данным, которые Вы видите на экране. Для этого достаточно щелкнуть по любой из строк правой клавишей мыши и выбрать из выпадающего меню вариант "Сделать отчет".

4.2.3 Программы

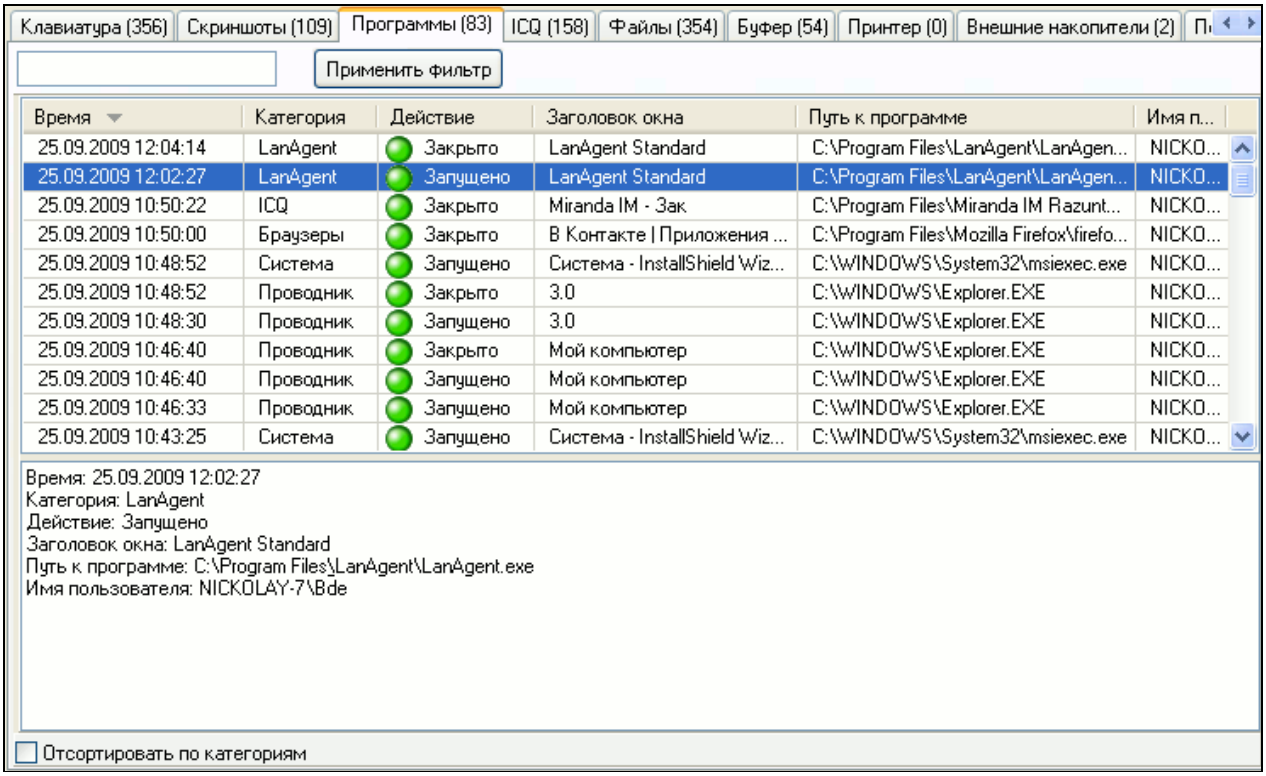
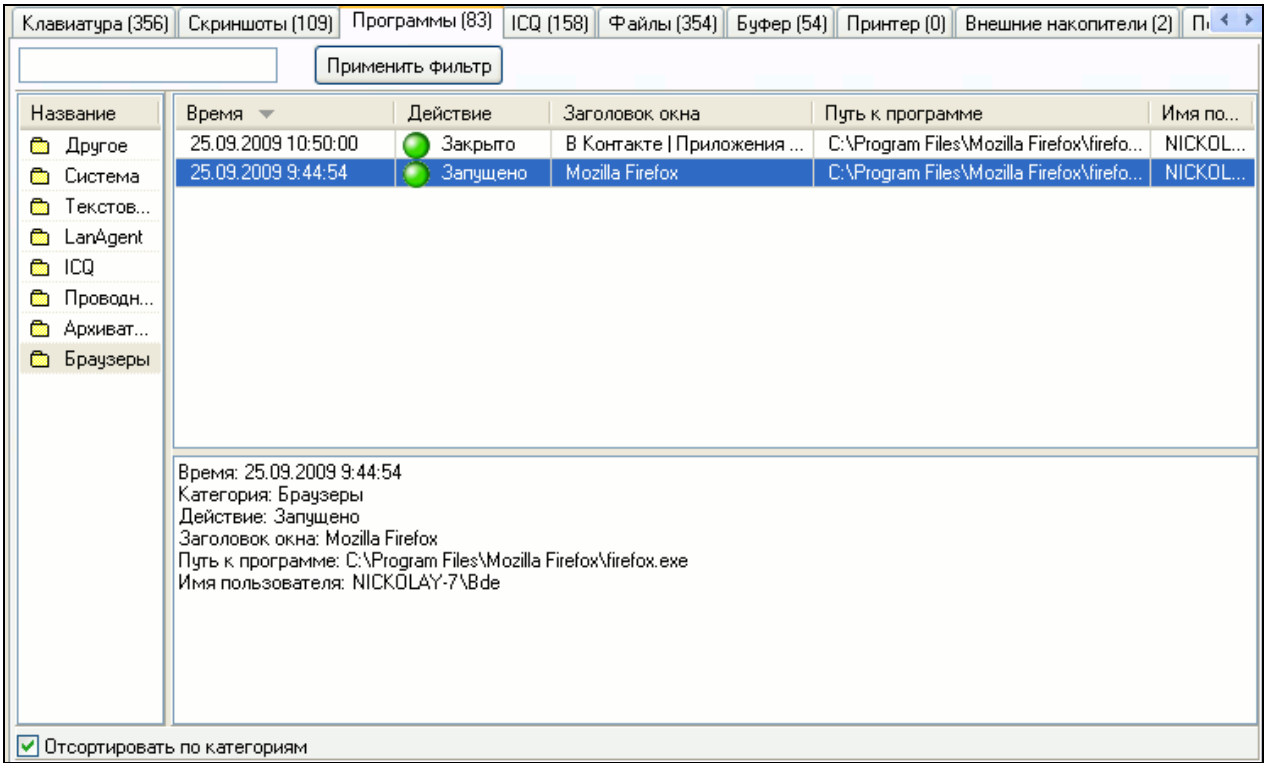


Рис. 4.6 – Окно логов программ

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.

При выборе опции "Отсортировать по категориям", можно просматривать статистику запуска/закрытия программ, относящихся к конкретной категории:



Подробнее о создании категорий и распределении программ по ним, смотрите в пункте 4.13.

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.

По любой из категорий логов можно сформировать отчет - выборку именно по тем данным, которые Вы видите на экране. Для этого достаточно щелкнуть по любой из строк правой клавишей мыши и выбрать из выпадающего меню вариант "Сделать отчет".

4.2.4 Буфер обмена

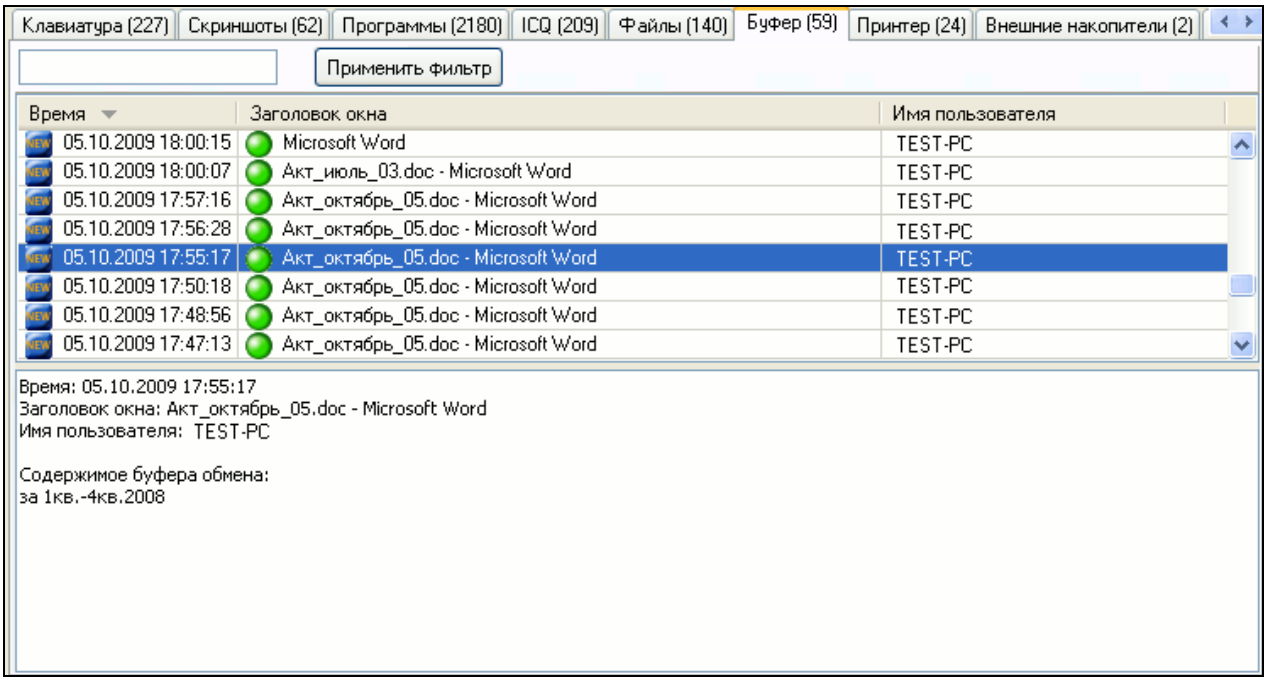


Рис. 4.7 – Окно логов буфера обмена

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.

По любой из категорий логов можно сформировать отчет - выборку именно по тем данным, которые Вы видите на экране. Для этого достаточно щелкнуть по любой из строк правой клавишей мыши и выбрать из выпадающего меню вариант "Сделать отчет".

4.2.5 Файлы

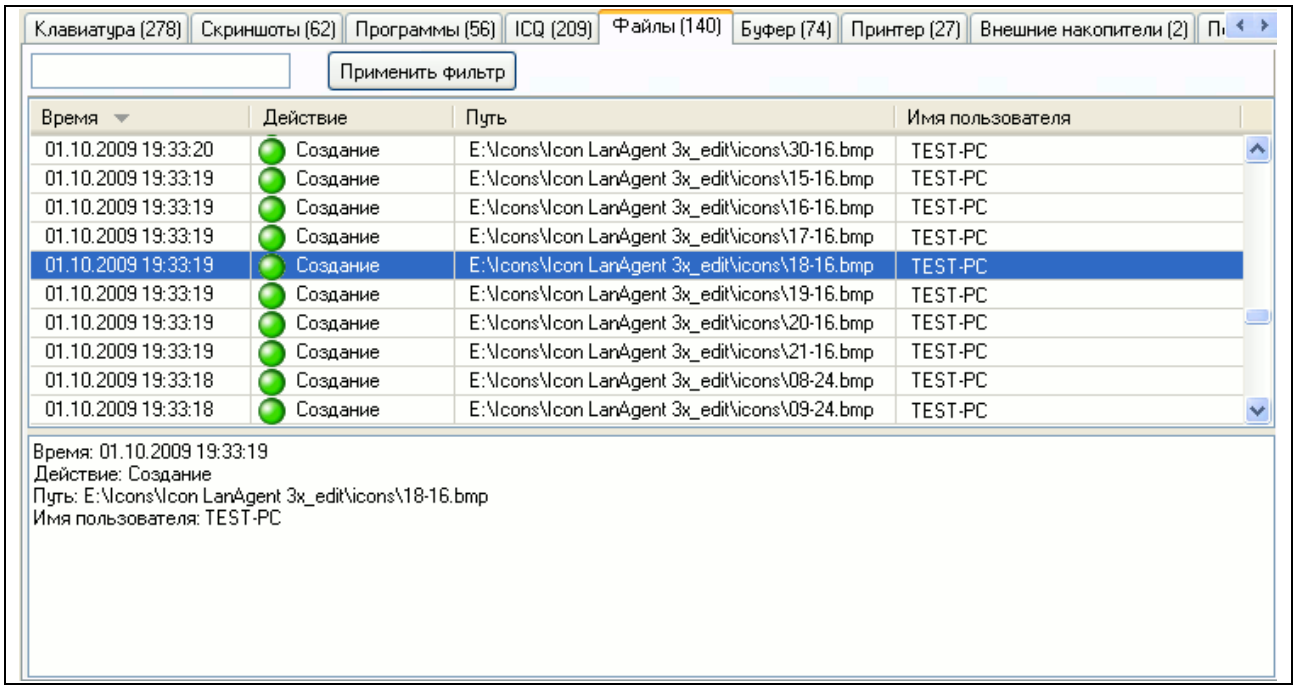


Рис. 4.8 – Окно статистики создания/удаления файлов

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.

По любой из категорий логов можно сформировать отчет - выборку именно по тем данным, которые Вы видите на экране. Для этого достаточно щелкнуть по любой из строк правой клавишей мыши и выбрать из выпадающего меню вариант "Сделать отчет".

4.2.6 Принтер

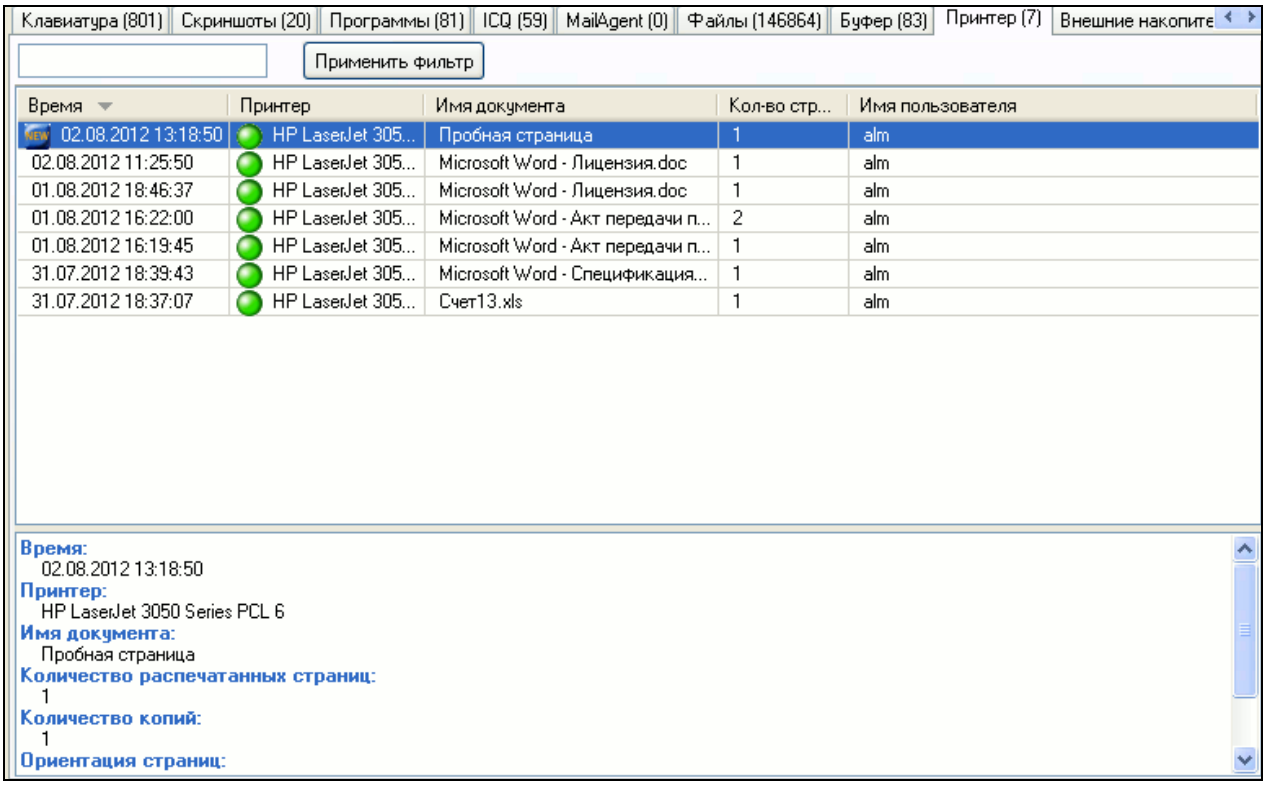


Рис. 4.9 – Окно логов принтеров

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.

4.2.7 Установленные программы

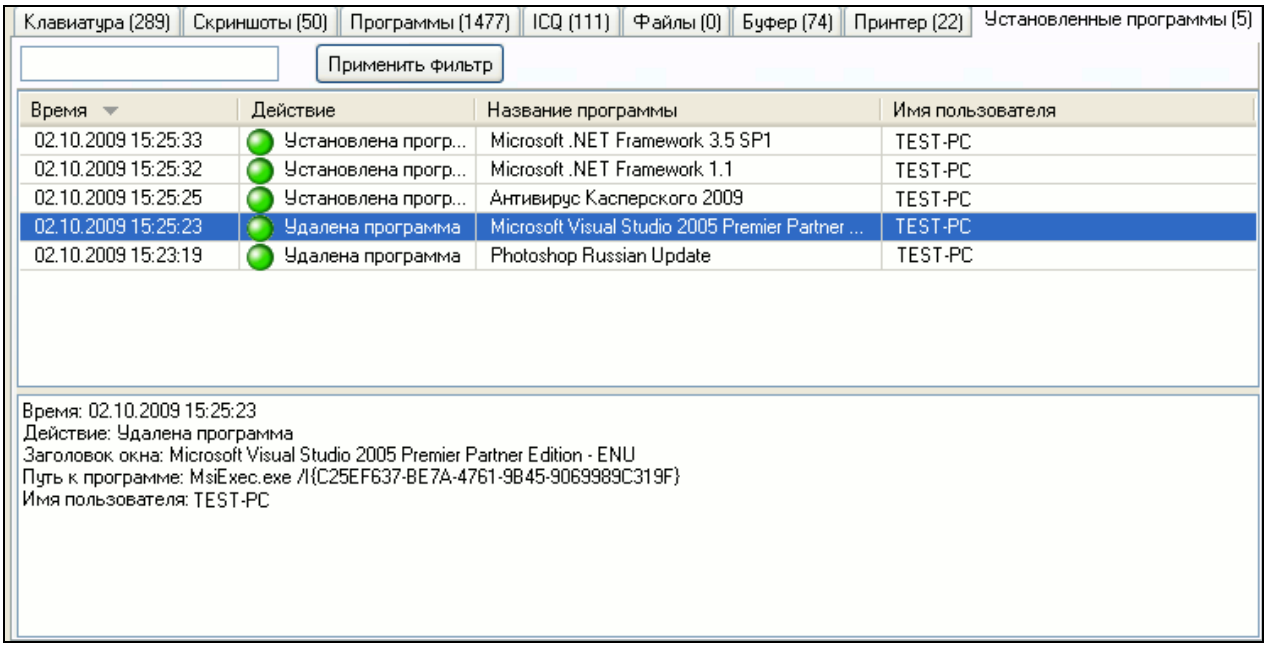


Рис. 4.10 – Окно логов установки/удаления программ

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.

По любой из категорий логов можно сформировать отчет - выборку именно по тем данным, которые Вы видите на экране. Для этого достаточно щелкнуть по любой из строк правой клавишей мыши и выбрать из выпадающего меню вариант "Сделать отчет".

4.2.8 Внешние накопители

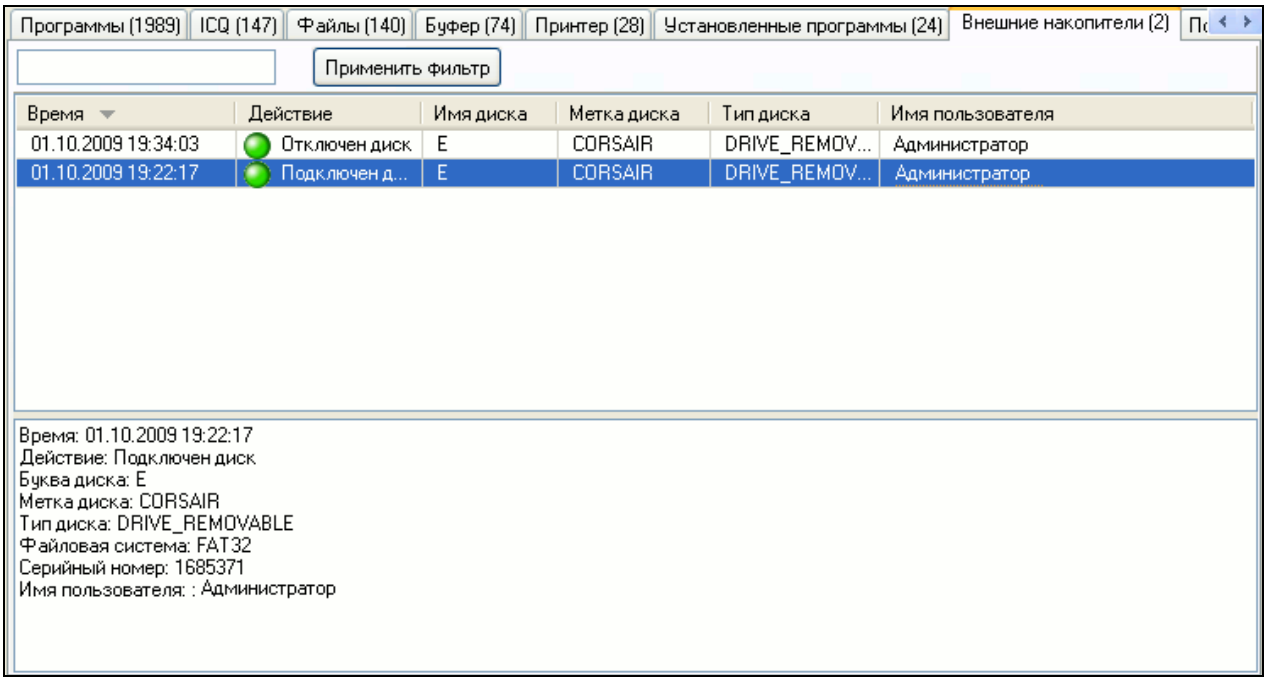


Рис. 4.11 – Окно логов подключения/отключения носителей информации

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.

По любой из категорий логов можно сформировать отчет - выборку именно по тем данным, которые Вы видите на экране. Для этого достаточно щелкнуть по

любой из строк правой клавишей мыши и выбрать из выпадающего меню вариант "Сделать отчет".

4.2.9 Посещённые сайты

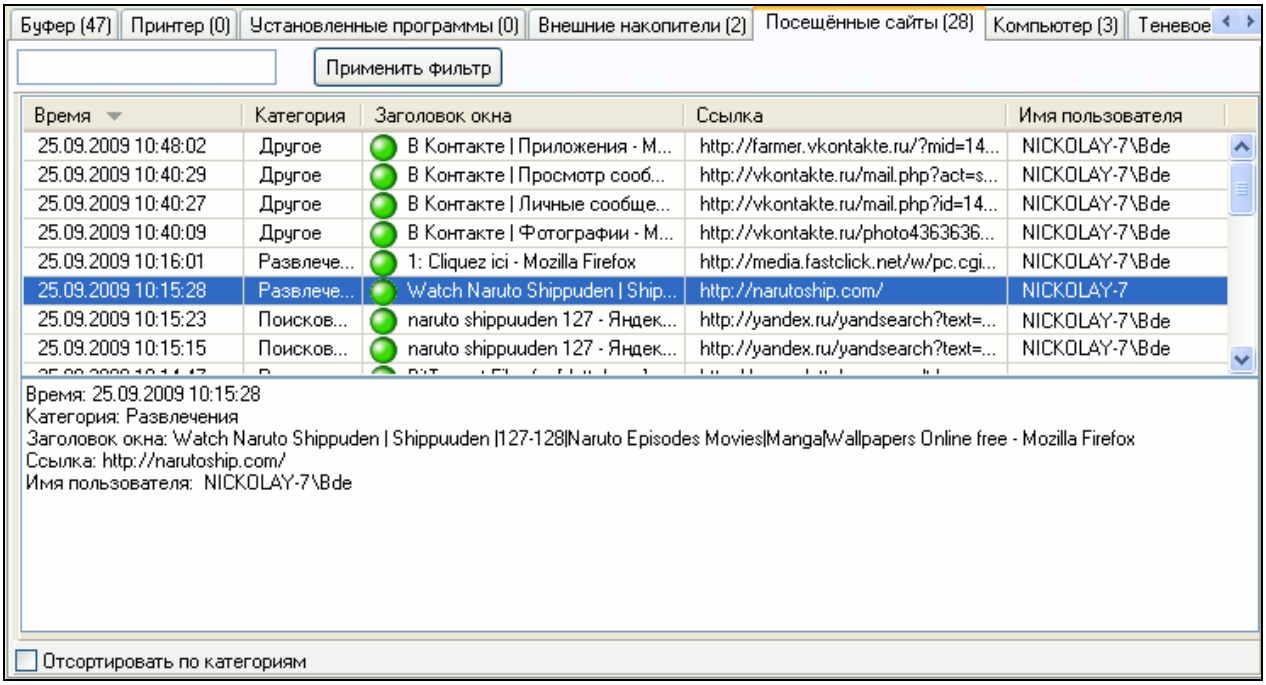
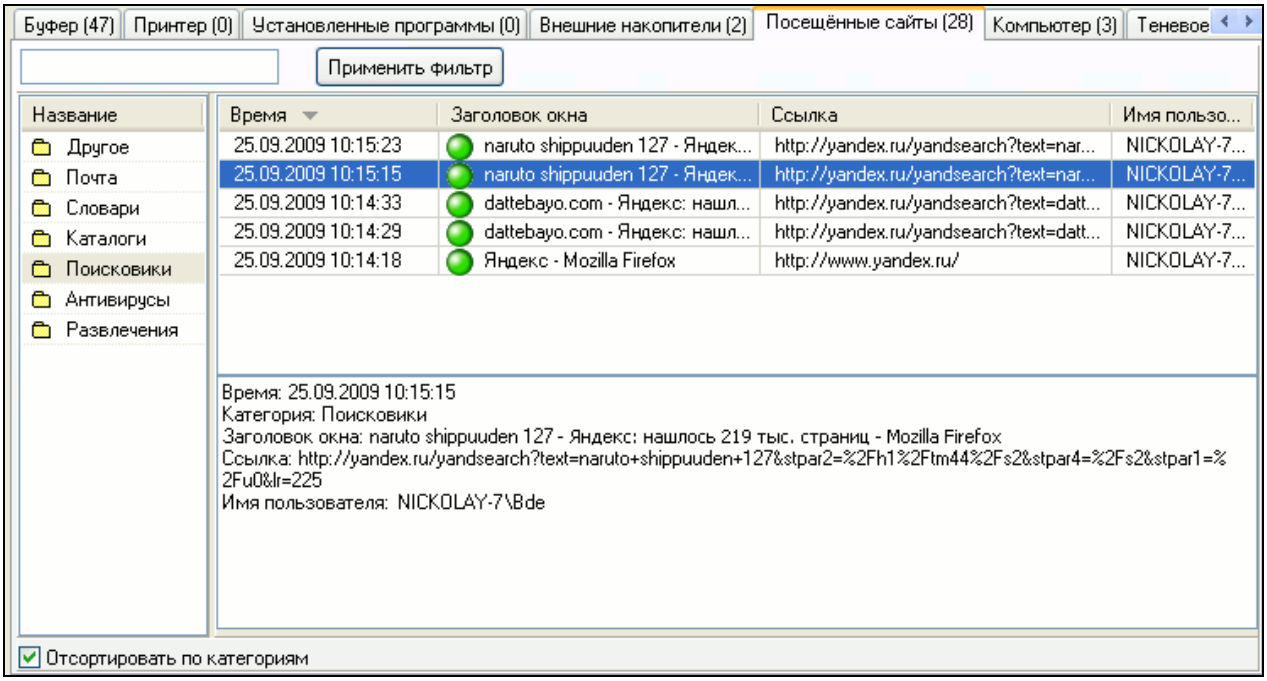


Рис. 4.12 – Окно логов посещенных сайтов

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.

При выборе опции "Отсортировать по категориям", можно просматривать статистику посещения веб-сайтов, относящихся к конкретной категории:



Подробнее о создании категорий и распределении посещенных сайтов смотрите в пункте 4.13.

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.

По любой из категорий логов можно сформировать отчет - выборку именно по тем данным, которые Вы видите на экране. Для этого достаточно щелкнуть по любой из строк правой клавишей мыши и выбрать из выпадающего меню вариант "Сделать отчет".

4.2.10 Компьютер

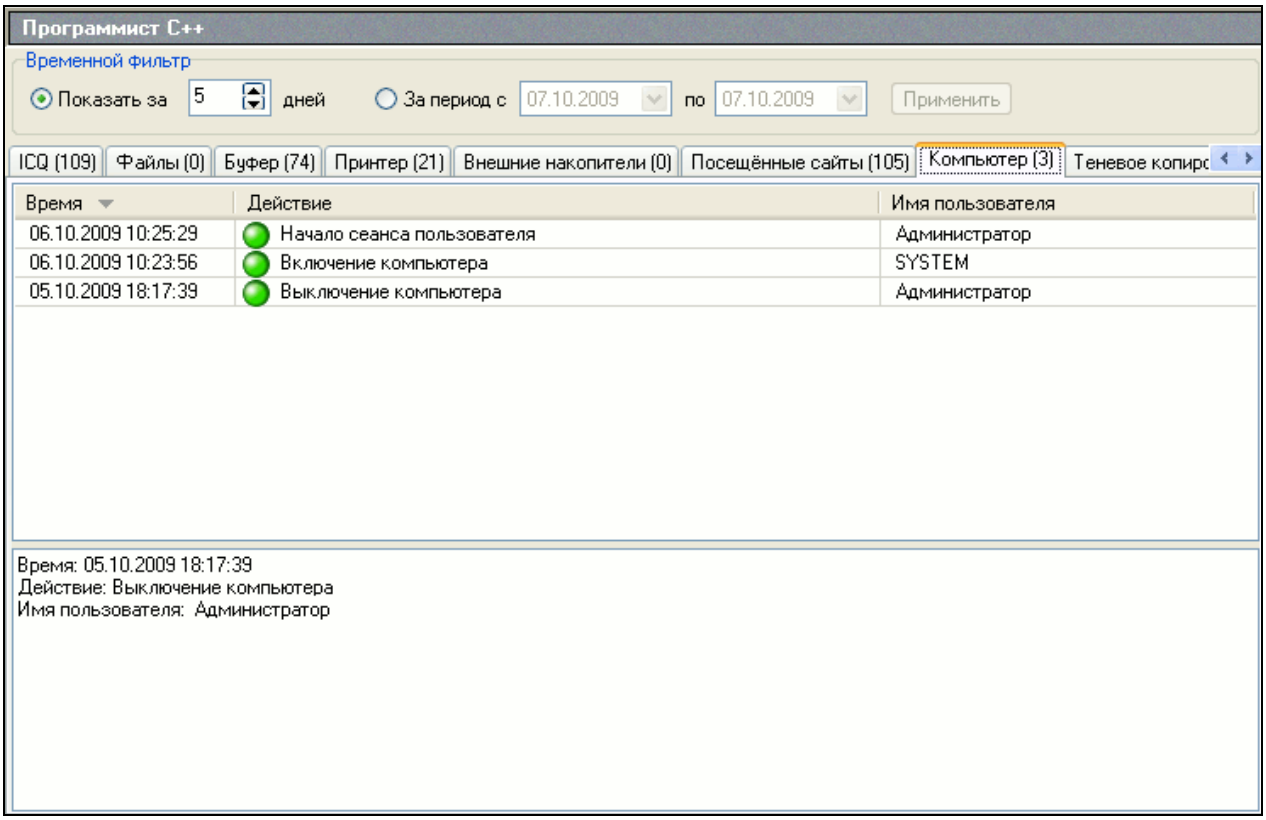


Рис. 4.13 – Окно статистики включения/выключения компьютера

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 события, какое конкретно действие было произведено (включён компьютер, начало сеанса пользователя, запуск ScreenSaver, выключение компьютера), 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.

По любой из категорий логов можно сформировать отчет - выборку именно по тем данным, которые Вы видите на экране. Для этого достаточно щелкнуть по любой из строк правой клавишей мыши и выбрать из выпадающего меню вариант "Сделать отчет".

4.2.11 ICQ

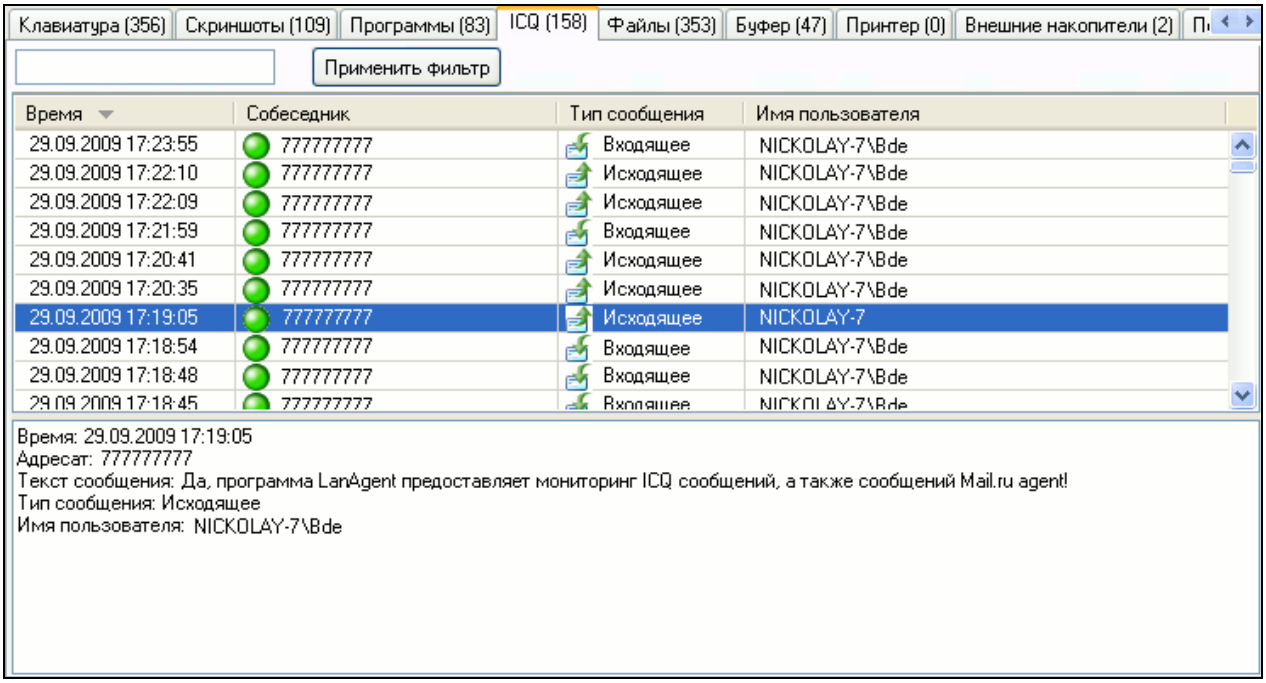


Рис. 4.14 – Окно статистики ICQ

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 диапазон логов.

По любой из категорий логов можно сформировать отчет - выборку именно по тем данным, которые Вы видите на экране. Для этого достаточно щелкнуть по любой из строк правой клавишей мыши и выбрать из выпадающего меню вариант "Сделать отчет".

4.2.12 Mail.ru Agent

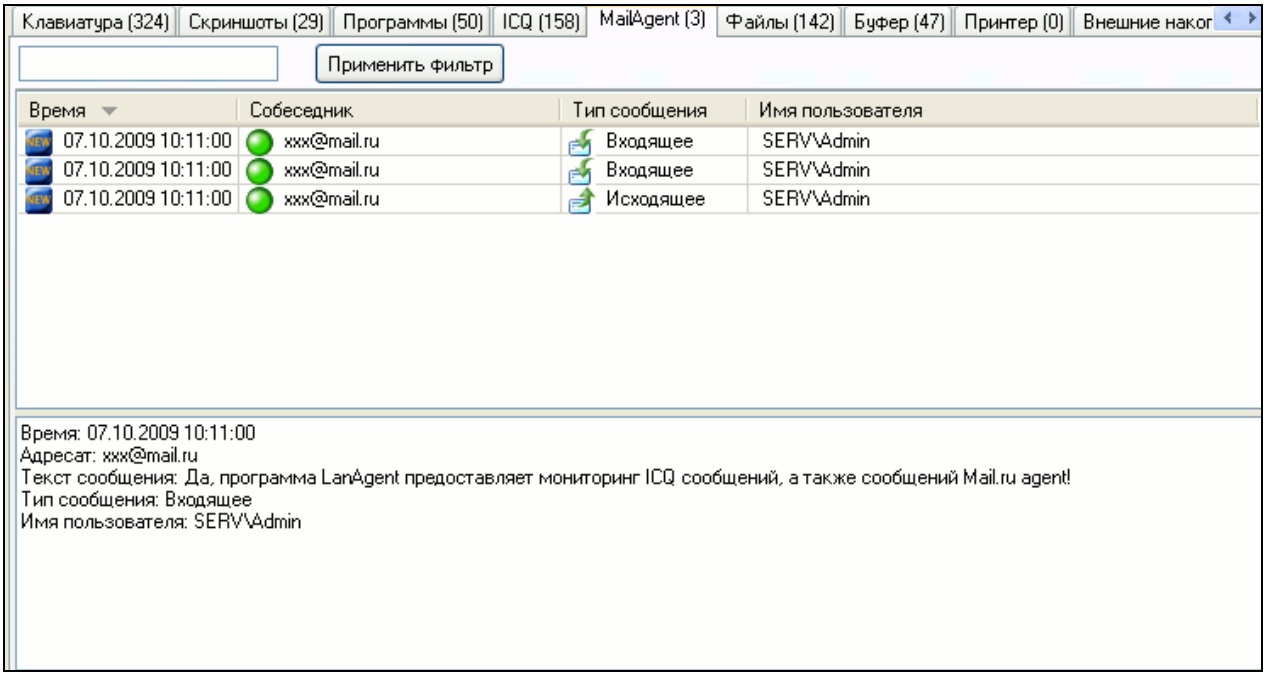


Рис. 4.15 – Окно статистики Mail.ru Agent

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 диапазон логов.

По любой из категорий логов можно сформировать отчет - выборку именно по тем данным, которые Вы видите на экране. Для этого достаточно щелкнуть по любой из строк правой клавишей мыши и выбрать из выпадающего меню вариант "Сделать отчет".

4.2.13 Теневое копирование

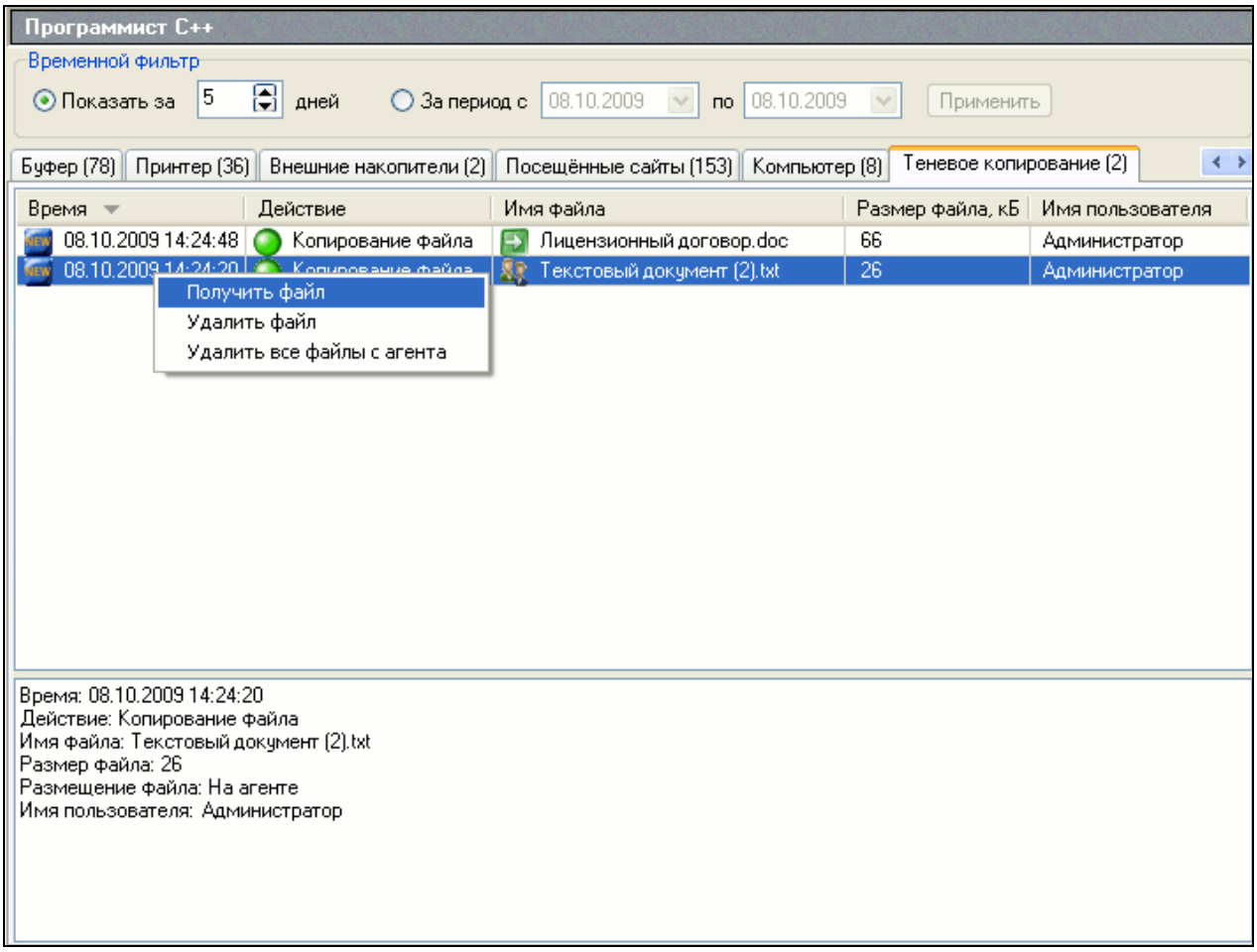


Рис. 4.15 – Окно статистики теневого копирования

На этой странице находится информация о теневых копиях файлов, скопированных на внешние устройства, такие как флэш, SD, USB-диски, ... или измененных на данных устройствах. В заголовке закладки в скобках указано количество записей в таблице. Данные в таблице могут быть отсортированы по любому из столбцов,

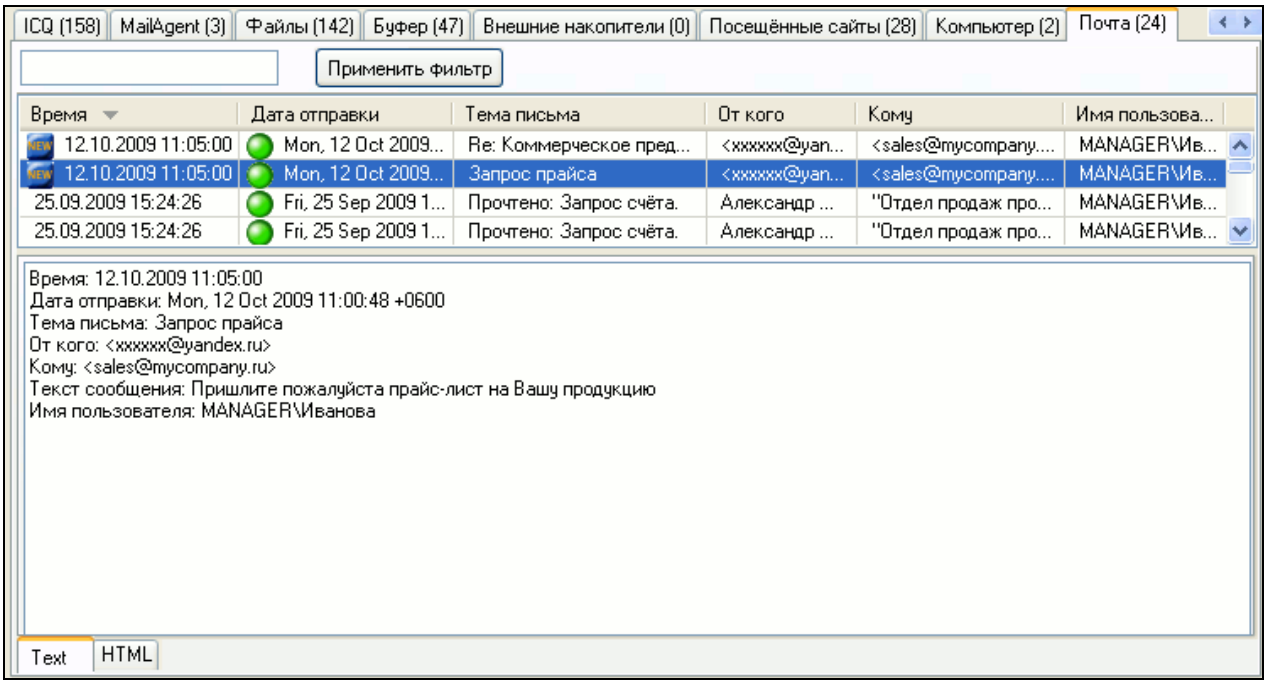
например по убыванию времени (то есть последняя информация содержится вверху таблицы). В таблице содержится следующая информация: дата и время копирования или модификации файла, какое действие было произведено (копирование или модификация), имя файла, размер файла, а также имя пользователя. Для перемещения по таблице можно пользоваться как мышкой, так и стрелками курсора. В текстовом поле под таблицей отображается вся информация из таблицы, а также указано где находится выбранный файл на данный момент (на контролируемом компьютере или уже загружен на сервер). 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.

Для того чтобы просмотреть файл на своем компьютере, надо перейти на нужную строку и в выпадающем меню, вызываемом по нажатию правой клавиши мыши, выбрать вариант "Получить файл". При этом если файл еще находится на контролируемом компьютере, то он будет оттуда скопирован. Если файл уже был получен ранее, то тогда просто откроется окно диалога сохранения файла. Укажите в нем куда его сохранить. Если файл не представляет интереса, то его можно удалить как из базы данных, так и с контролируемого компьютера без загрузки.

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.

По любой из категорий логов можно сформировать отчет - выборку именно по тем данным, которые Вы видите на экране. Для этого достаточно щелкнуть по любой из строк правой клавишей мыши и выбрать из выпадающего меню вариант "Сделать отчет".

4.2.14 Почта

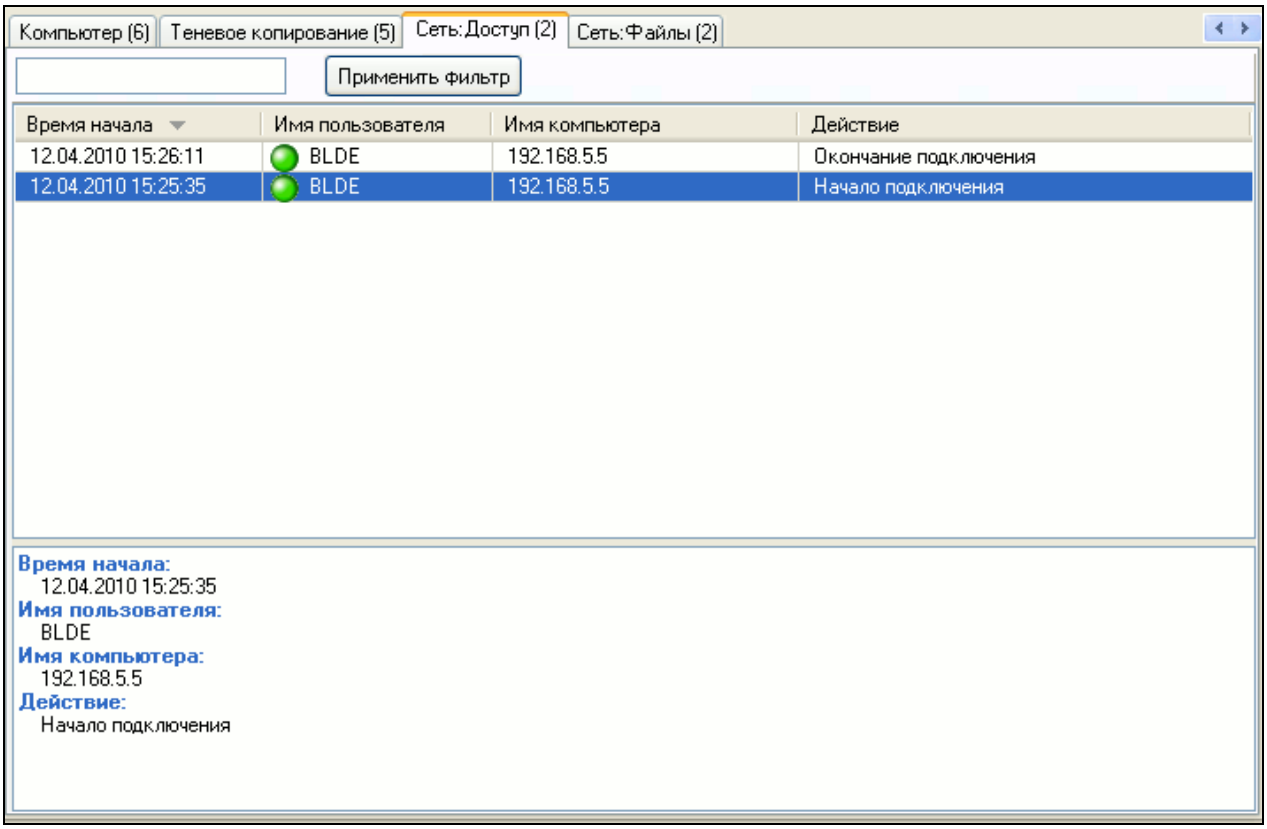


На этой странице находится информация по перехваченным электронным письмам. В заголовке закладки в скобках указано количество записей в таблице. Данные в таблице могут быть отсортированы по любому из столбцов, например по убыванию времени (то есть последняя информация содержится вверху таблицы). В таблице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

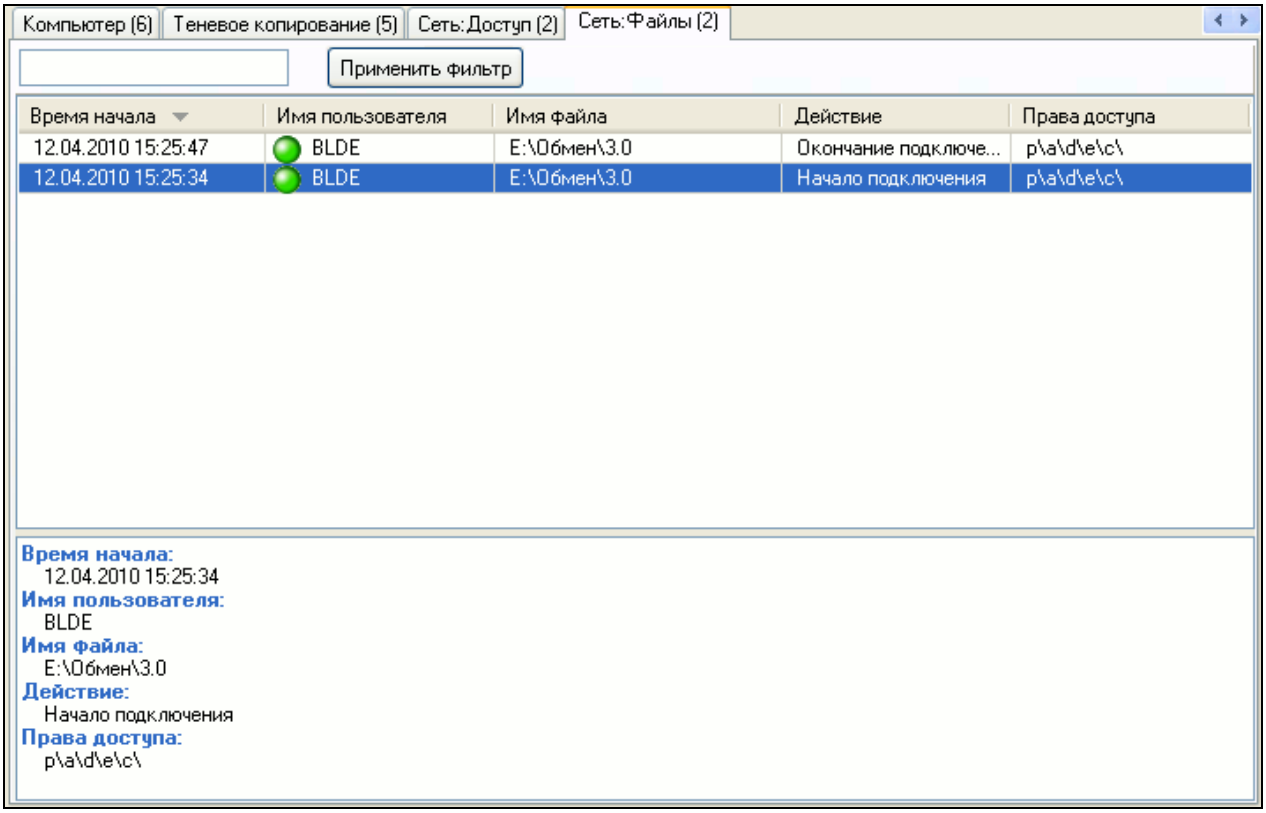
По любой из категорий логов можно сформировать отчет - выборку именно по тем данным, которые Вы видите на экране. Для этого достаточно щелкнуть по любой из строк правой клавишей мыши и выбрать из выпадающего меню вариант "Сделать отчет".

4.2.15 Сеть



На этой странице находится информация по подключениям пользователей к общим ресурсам компьютера. 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 начала или окончания подключения, Имя пользователя, Имя компьютера, с которого происходило подключение к общему ресурсу, а также само действие (Начало или окончание подключения). 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.



На данной странице находится информация о непосредственно обращениях к файлам на общих ресурсах компьютера. Для каждого обращения указываются права доступа:

r - права на чтение;

w - права на запись;

c - права на создание файлов и каталогов;

e - права на запуск файлов;

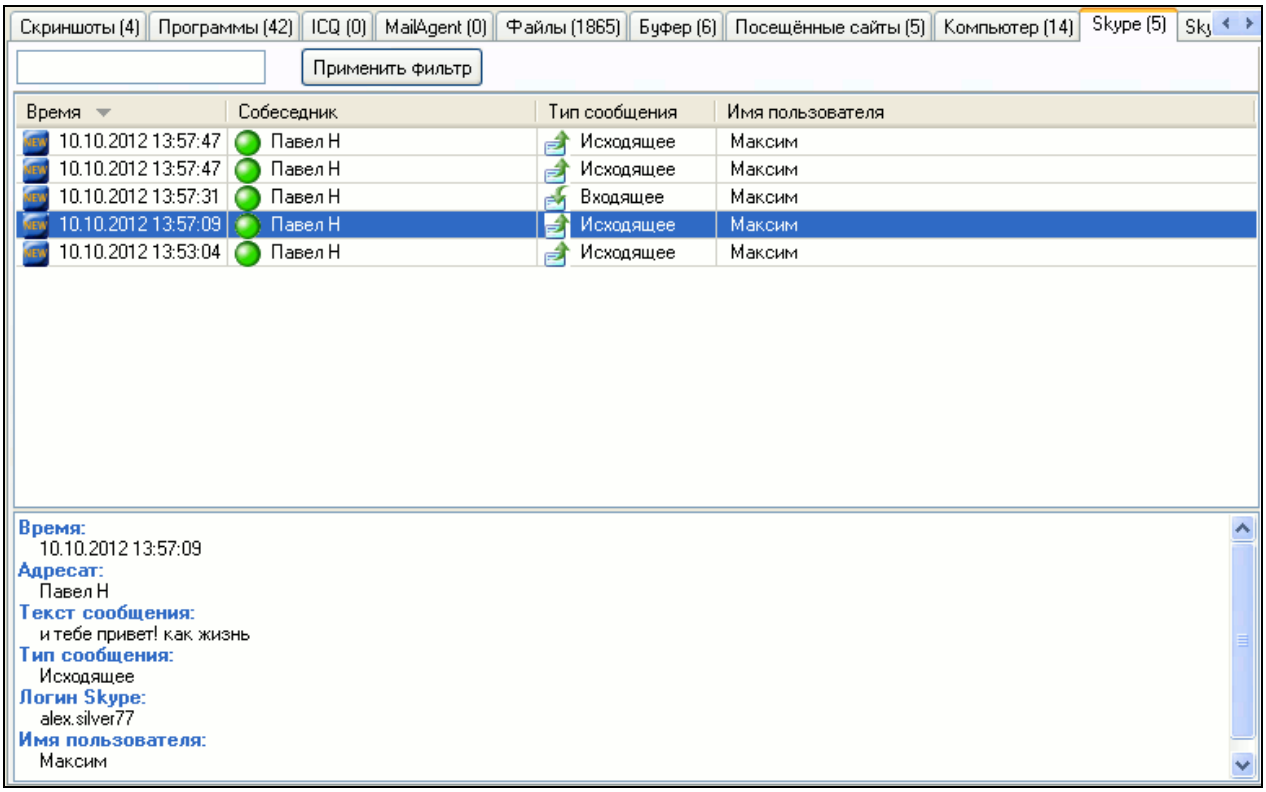
d - права на удаление файлов и каталогов;

a - права на изменение атрибутов файлов и папок;

p - права на изменение разрешений (прав доступа) к файлам и папкам.

По любой из категорий логов можно сформировать отчет - выборку именно по тем данным, которые Вы видите на экране. Для этого достаточно щелкнуть по любой из строк правой клавишей мыши и выбрать из выпадающего меню вариант "Сделать отчет".

4.2.16 Skype

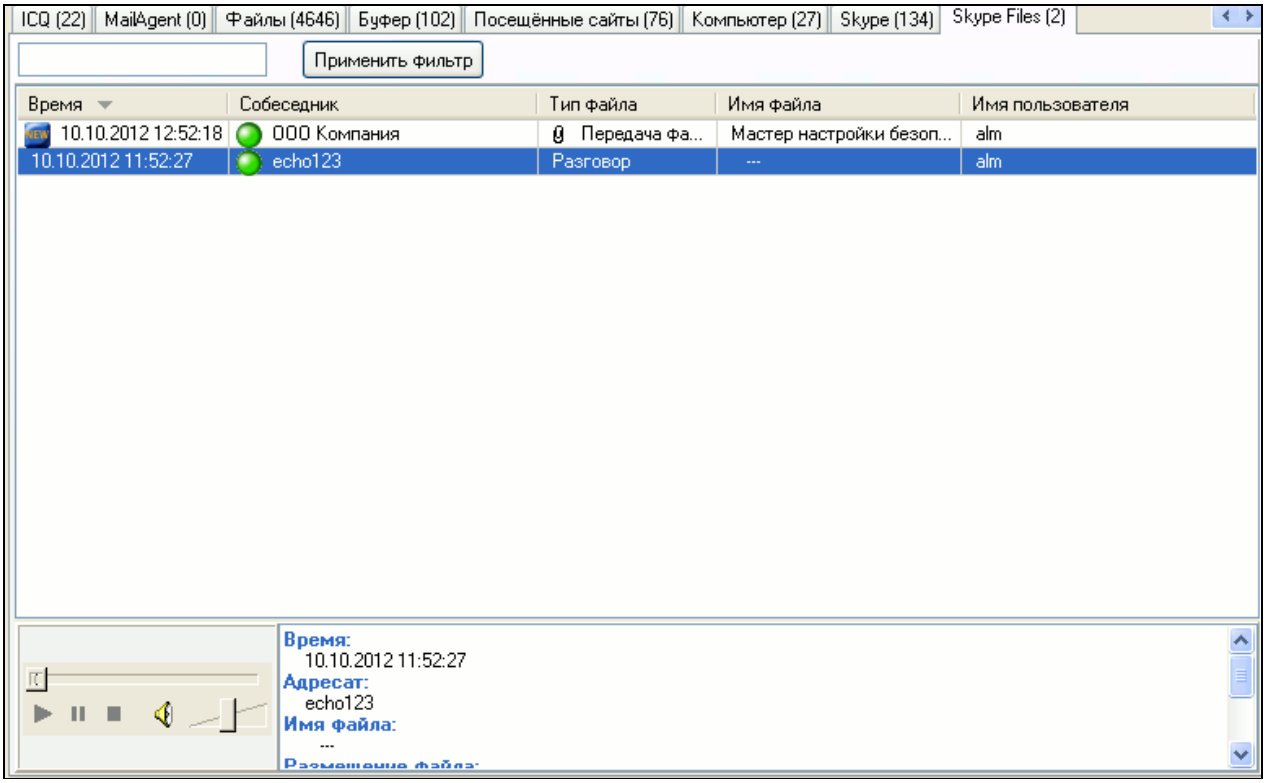


На этой странице находится информация по перехваченным сообщениям Skype. В заголовке закладки в скобках указано количество записей в таблице. Данные в таблице могут быть отсортированы по любому из столбцов, например по убыванию времени (то есть последняя информация содержится вверху таблицы). В таблице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

По любой из категорий логов можно сформировать отчет - выборку именно по тем данным, которые Вы видите на экране. Для этого достаточно щелкнуть по любой из строк правой клавишей мыши и выбрать из выпадающего меню вариант "Сделать отчет".

4.2.17 Skype Files

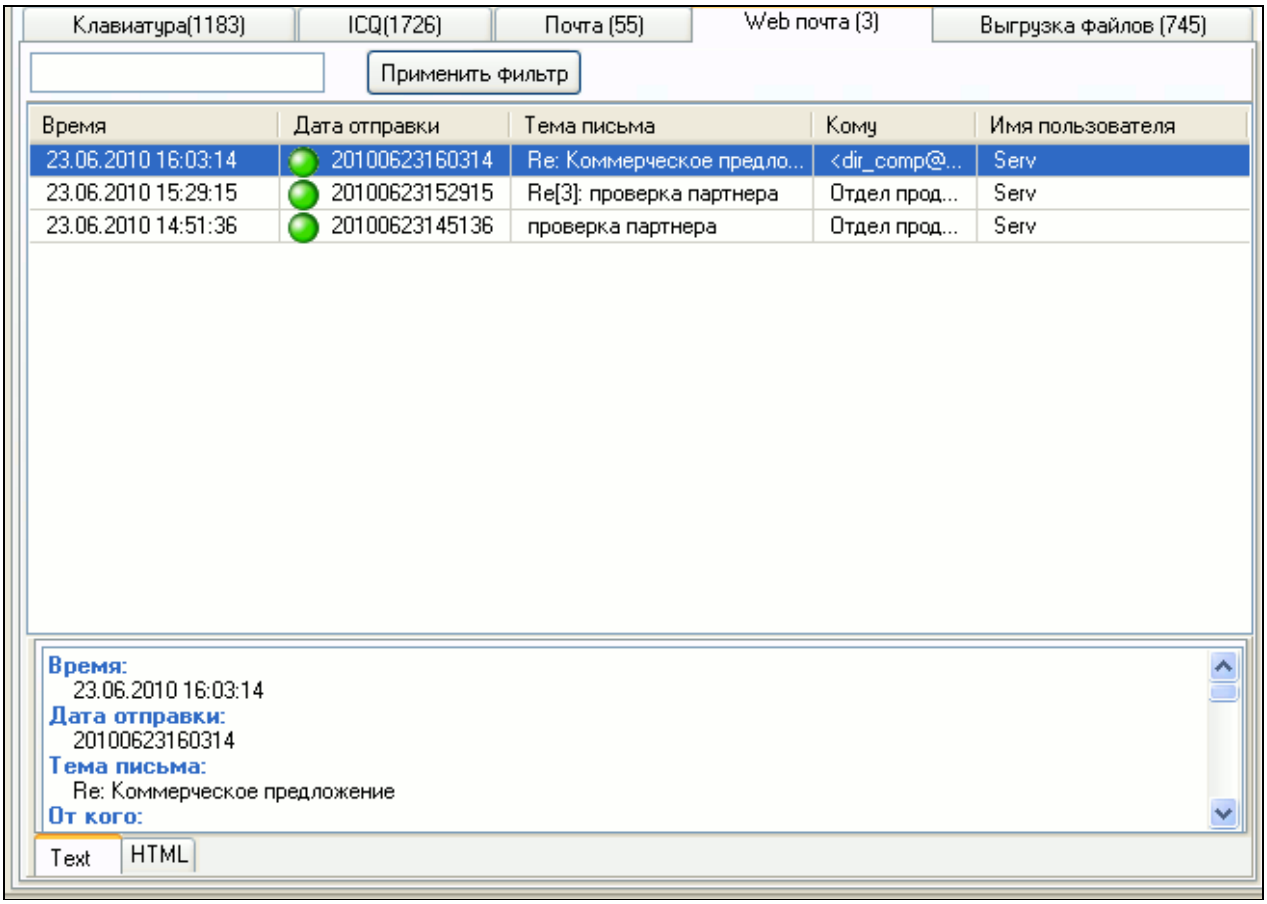


На этой странице находится информация по голосовым сообщениям (звонкам) Skype, а также передаче файлов через Skype. В заголовке закладки в скобках указано количество записей в таблице. Данные в таблице могут быть отсортированы по любому из столбцов, например по убыванию времени (то есть последняя информация содержится вверху таблицы). В таблице содержится следующая информация: дата и время звонка или передачи файла, собеседник, тип файла (Разговор или Передача файла), а также имя пользователя. В случае передачи файла, будет указано его имя. 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 прослушивания звукового файла разговора или сохранения переданного файла, щелкните дважды на интересующей строке истории.

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.

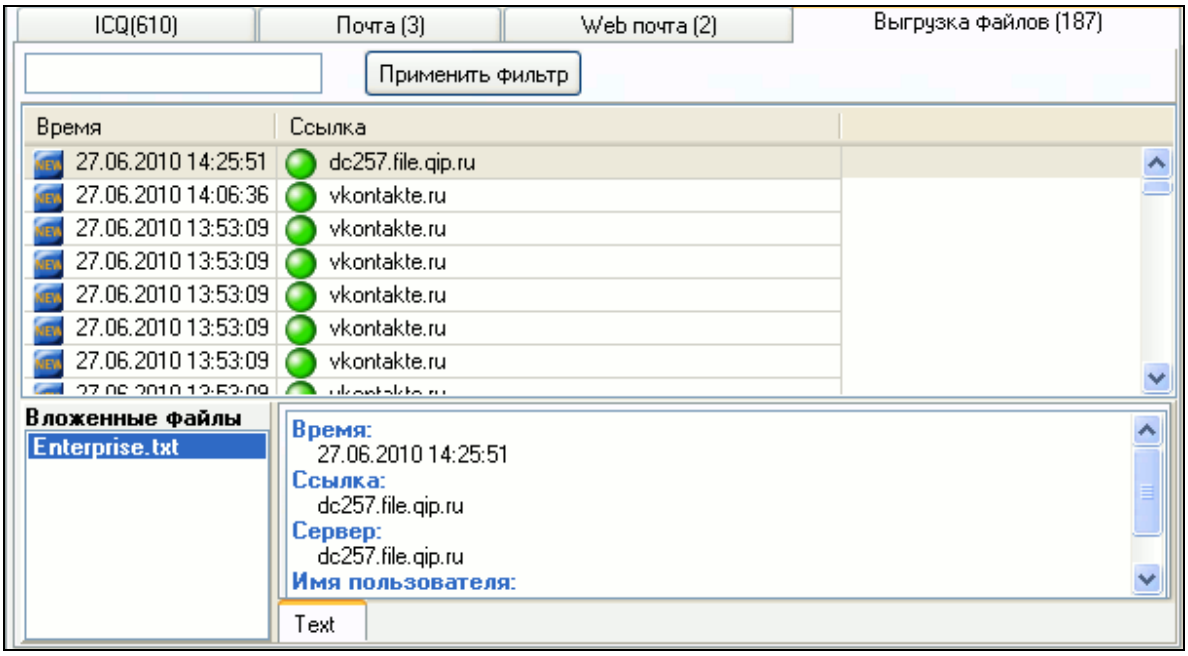
4.2.18 Web почта



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 диаппазон логов.

4.2.19 Выгрузка файлов

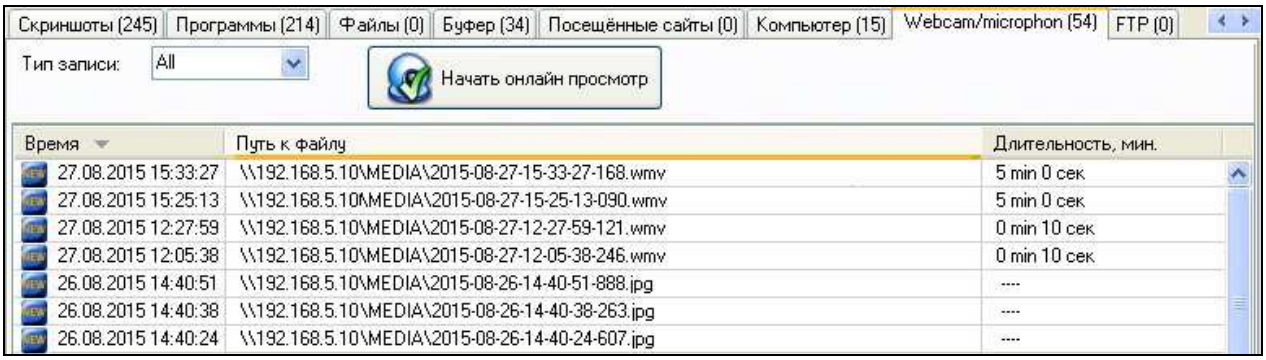


На этой странице находится информация по файлам, выгруженным пользователем в Интернет.

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 диаппазон логов.

4.2.20 Webcam/microphone



На этой вкладке отображаются созданные через веб камеру на контролируемом компьютере видео/аудио записи, а также снимки с веб камеры. Размещение файлов производится в специальном каталоге на сервере, доступ к которому должен быть открыт для пользователя административной консоли.

Просмотреть запись или снимок можно щелкнув дважды на соответствующей строке истории.

Для начала просмотра изображения с веб камеры в режиме реального времени, нажмите кнопку «Начать онлайн просмотр». При этом будет запущен Windows Media Player и в нем начнется трансляция изображения. Если данная программа не установлена (ее может не быть на серверных ОС), то ее нужно включить через установку компонентов Windows в Панели управления.

4.3 Панель инструментов

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

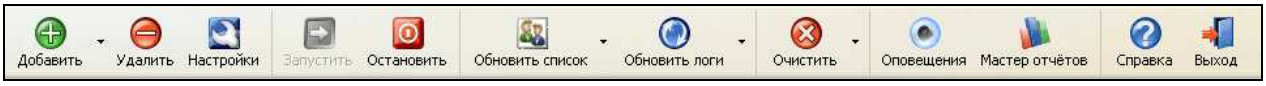
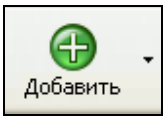


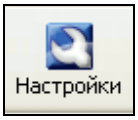
Рис. 4.17 – Панель инструментов

Назначение кнопок панели инструментов:



- добавить группу или компьютер в список мониторинга.

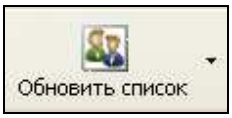
- удалить компьютер из списка мониторинга.



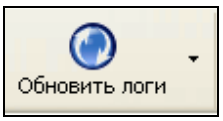
- открыть окно настроек пользовательской части программы.

- запустить мониторинг на выбранном компьютере.

- остановить мониторинг на выбранном компьютере.



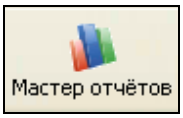
- обновить список компьютеров и состояний мониторинга.



- обновить содержимое логов для всех пользователей.

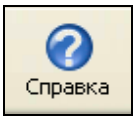
- очистка содержимого логов. Включает в себя следующие пункты:
  - очистить выбранную категорию,
  - очистить все логи пользователя,
  - очистить все логи для всех пользователей.

- 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 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:

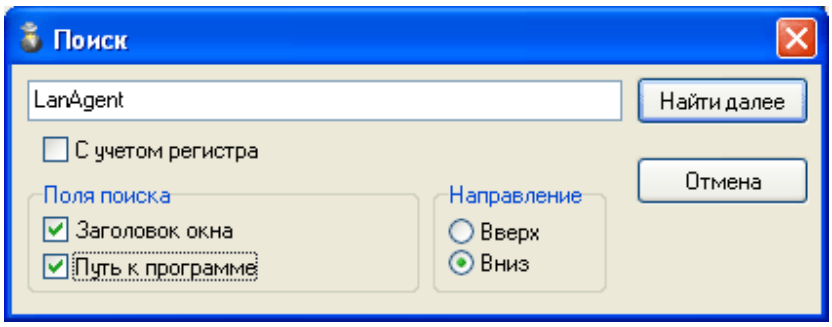


Рис. 4.18 – Диалог поиска по логам

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".

4.6 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 4.10.

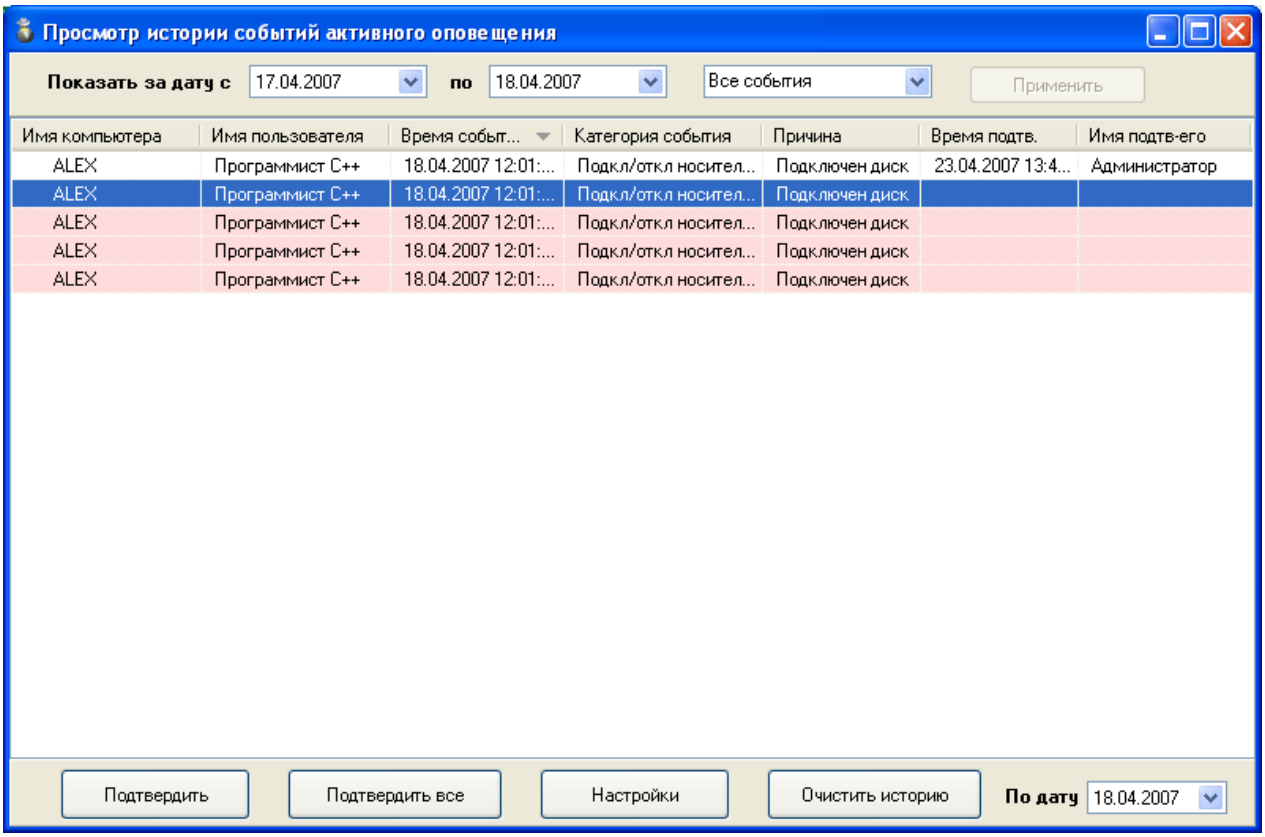


Рис. 4.19 – Окно истории активного оповещения

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.

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").

4.7 «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 пользователя "Программист" имеются значительные нарушения, поэтому статус его опасности "красный".

Рис. 4.20 – «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. 4.21 – «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!

4.8 Список правил безопасности

Призван облегчить процедуру контроля за соблюдением политик безопасности и использования компьютерной техники работниками организации.

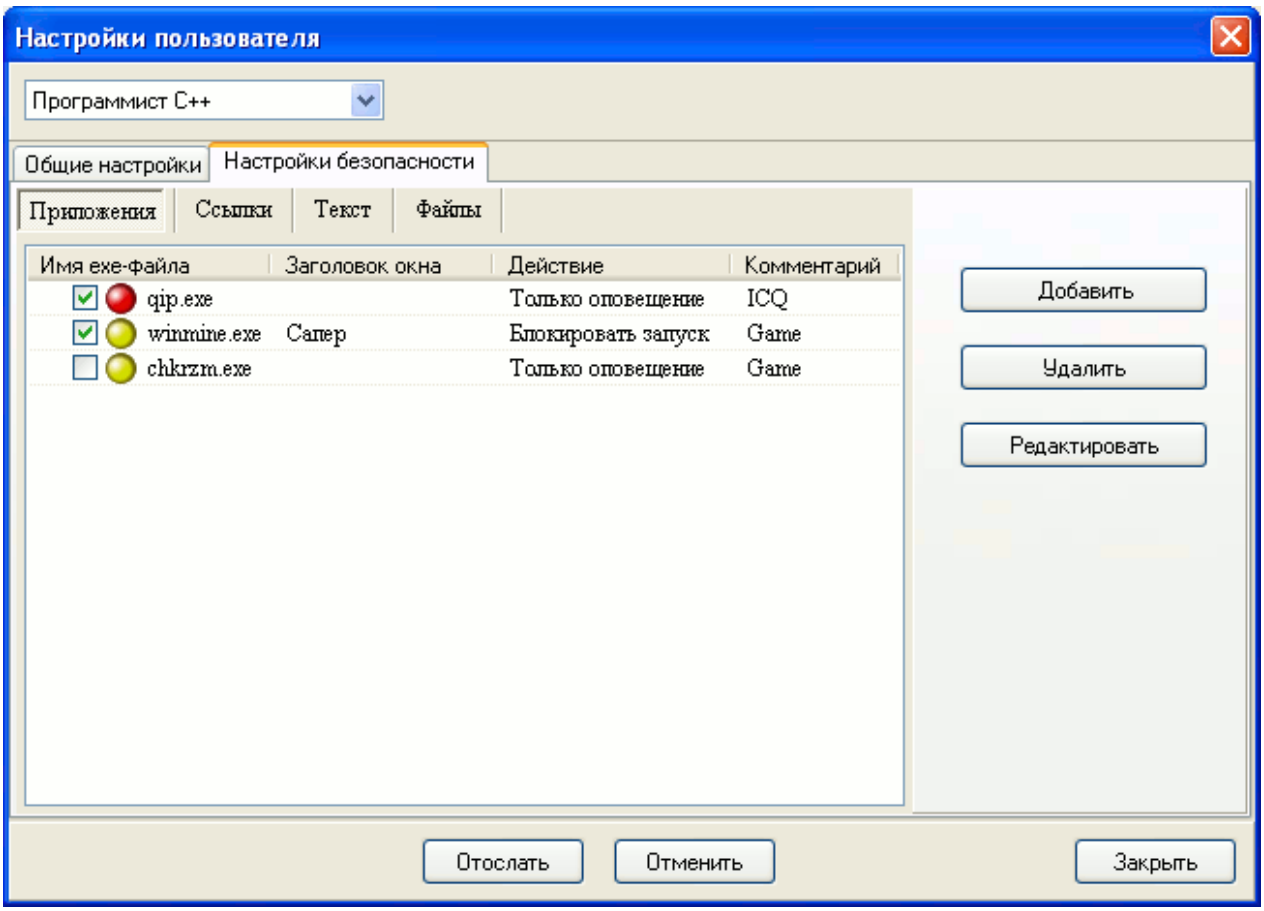


Рис. 4.22 – Список правил безопасности

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).

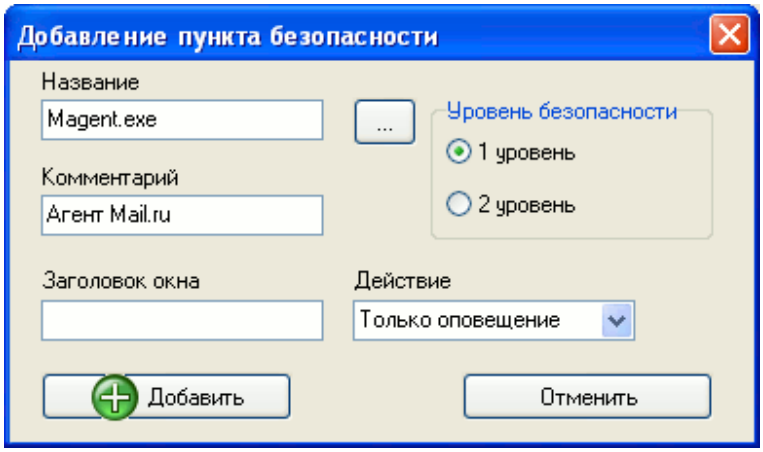
На закладке **«Файлы»** указываются непосредственно имена файлов, открытие/закрытие которых будет считаться нарушением правил.

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:

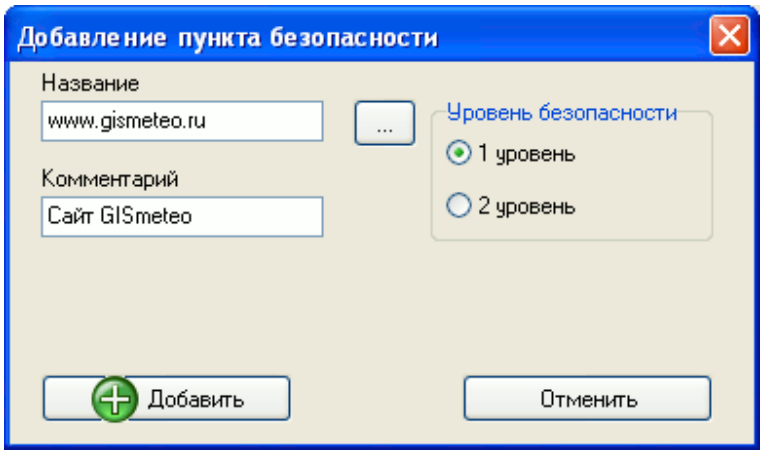
1. Допустим, мы хотим, чтобы программа MailAgent подсвечивалась в логах запуска программ, как запрещенная. Для это в окне настроек безопасности, переходим на закладку приложения и нажимаем кнопку **«Добавить»** (в правой части окна). При этом откроется окно добавления пункта безопасности. В поле **«Название»** записываем имя exe файла (в нашем случае это Magent.exe). Также имя exe файла можно выбрать из списка (кнопка справа от поля "Название"). Далее определяем уровень безопасности (1-ый соответствует желтому цвету светофора, 2-ой - красному). При желании можно указать комментарий, например, как на рисунке. Дополнительно можно указать заголовок окна программы. Это поле может быть полезно в том случае, если пользователь намеренно изменит имя exe файла программы, тогда идентификация будет произведена по заголовку окна. Для категории "Программы" можно выбрать действие, которое будет выполняться агентом при запуске пользователем запрещенных программ. Возможные варианты: Только оповещение, Блокировать запуск, Блокировать запуск с выводом пользователю на экран предупреждения.



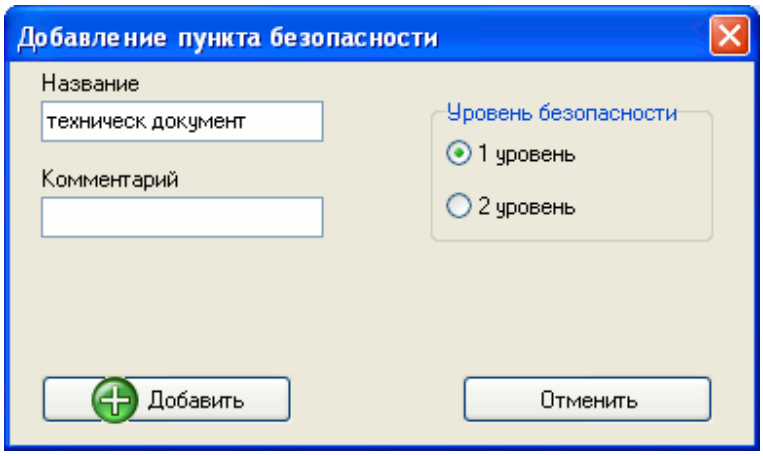
После нажатия кнопки **«Добавить»**, данное правило будет сохранено.

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,

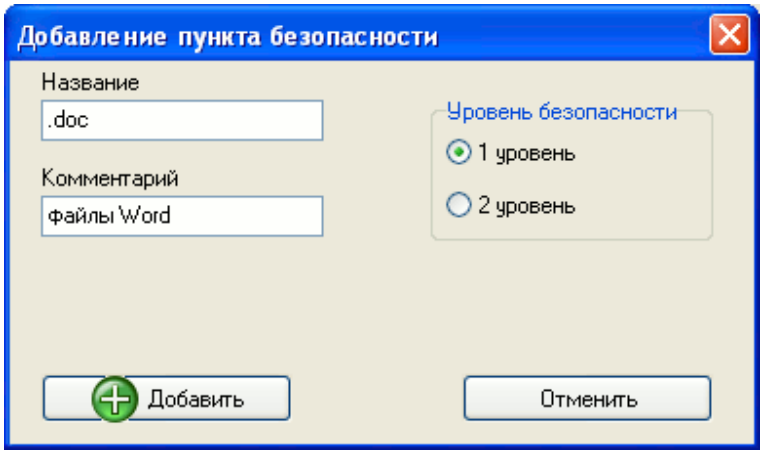
«http://www.gismeteo.ru/towns/34172.htm». Если необходимо отлавливать еще и ссылки типа «http://www.forum.gismeteo.ru», то необходимо в качестве названия задать более короткую строку, например просто «gismeteo».



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.



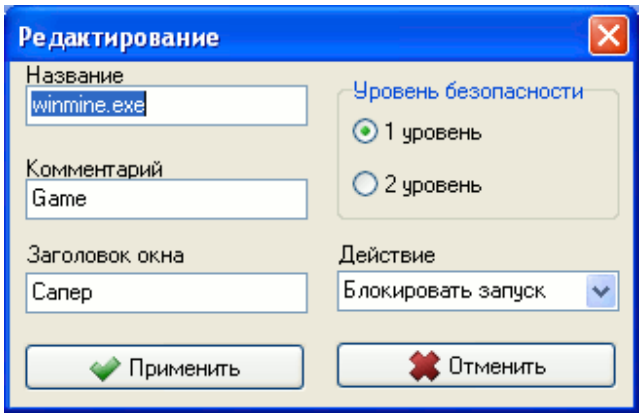
4. Закладка **«Файлы»**. Допустим мы хотим запретить работу с любыми текстовыми документами с расширением .doc. Тогда в поле **«Название»** мы соответственно внесем всё расширение.



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.

4.9 Архивирование статистики (логов)

С целью защиты информации (базы логов) от потери, например в случае сбоев, желательно периодически делать резервные копии базы данных.

Проще всего это сделать, создав копию каталога базы DB.

Важно! Перед копирование каталога базы необходимо закрыть административную часть LanAgent. Копировать базу можно только в тот момент, когда с ней никто не работает, иначе копия получится поврежденной.

4.10 Настройки программы

4.10.1 Настройка программы администратора

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

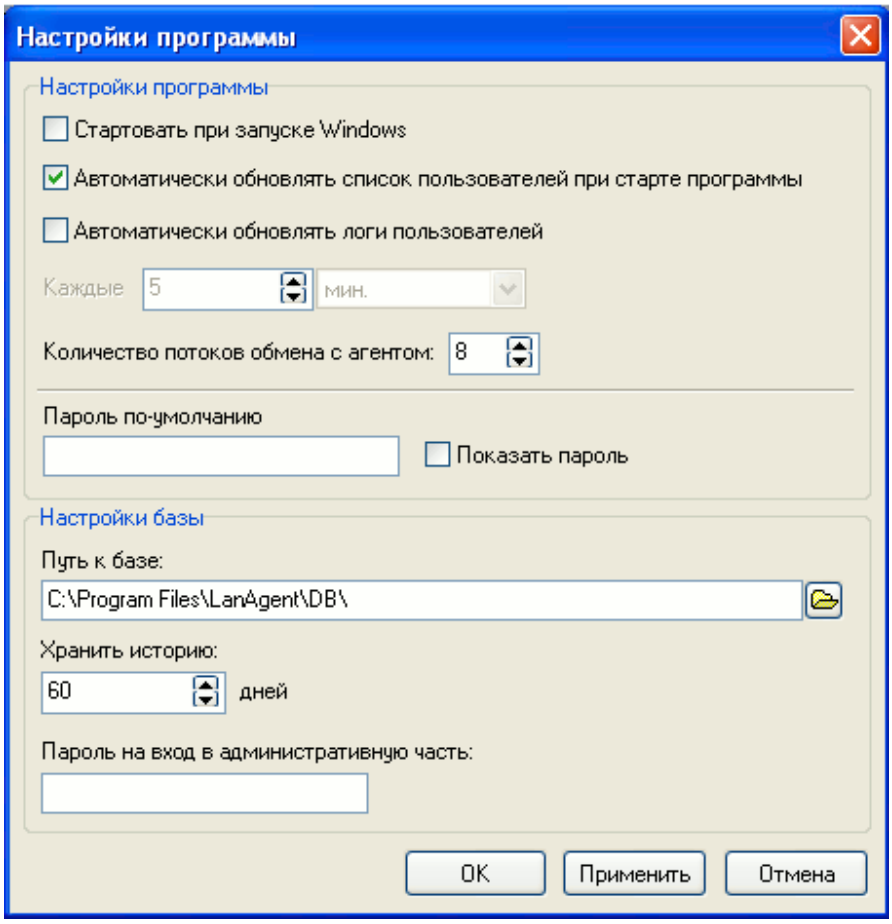


Рис. 4.21 – Настройки программы администратора

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**".

Количество потоков обмена с агентом - начиная с версии 2.0, обмен с агентами ведется в многопоточном режиме. Данная настройка позволяет изменять количество потоков обмена. Оптимальное количество определяется индивидуально и зависит от следующих параметров: производительности компьютера, на котором стоит администраторская часть, количества агентов, с которыми производится обмен, производительности и загруженности локальной сети и др.

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.

Пароль на вход в административную часть - если есть необходимость, то запишите в данное поле пароль.

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

4.10.2 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.

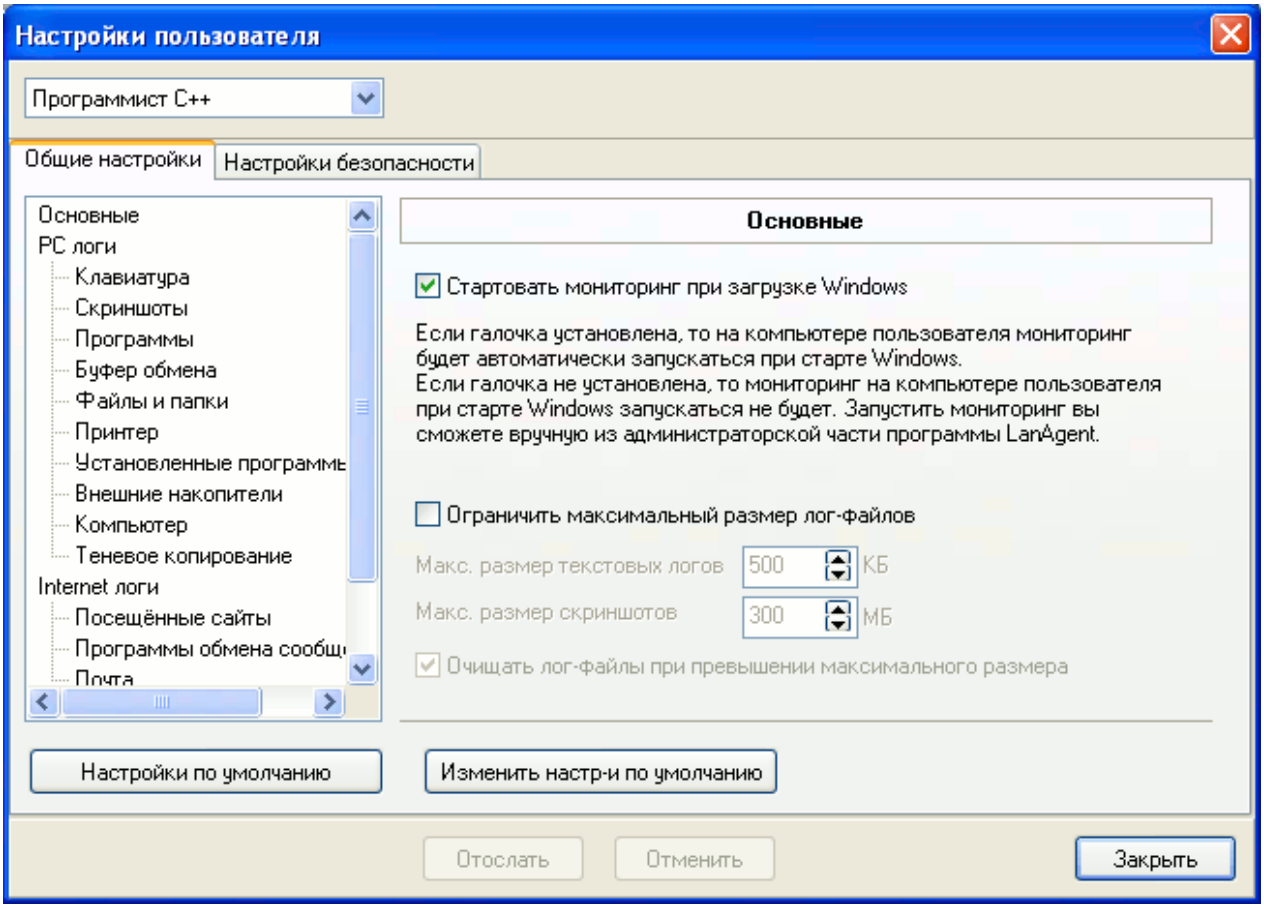


Рис. 4.22 – Главное окно настроек агентов

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.

Делать теневую копию файлов - установите эту галочку, чтобы программа осуществляла теневое копирование файлов, копируемых на usb носители или изменяемых на них.

Отслеживать доступ к общим ресурсам - установите эту галочку, чтобы программа логировала подключение пользователей к общим ресурсам компьютера, а также запоминала к каким файлам происходило обращение.

Клавиатура:

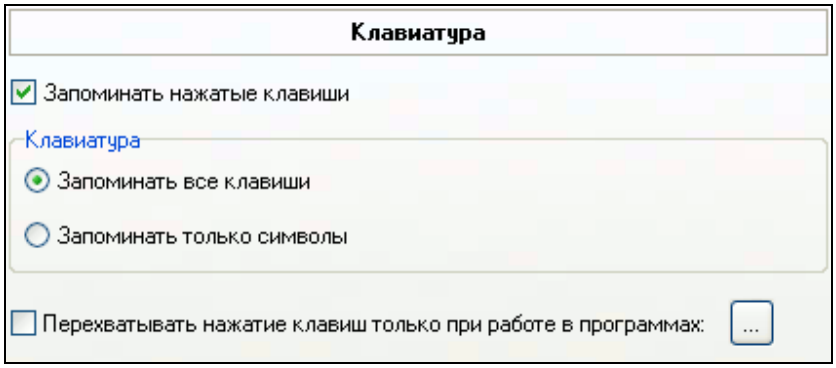
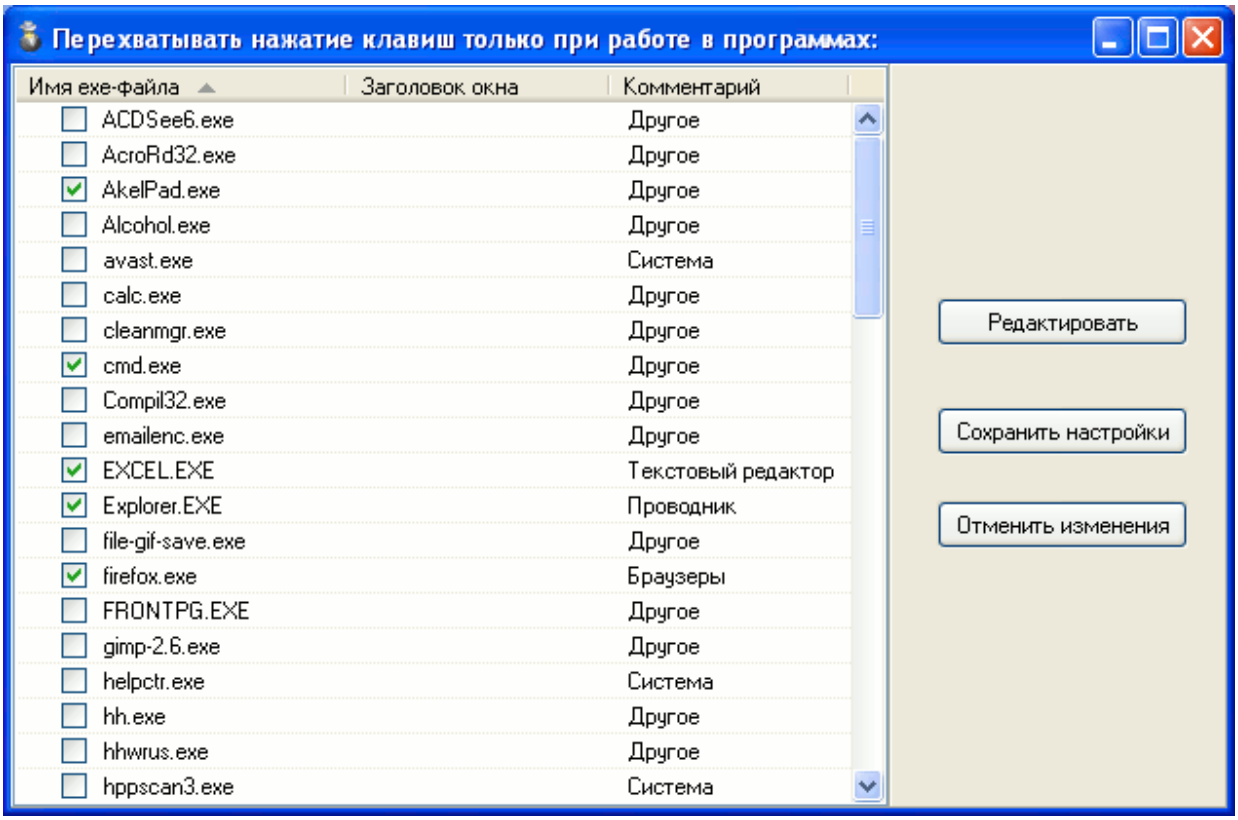


Рис. 4.23 – Настройки контроля клавиатуры агентов

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.

Перехватывать нажатие клавиш только при работе в программах - если данная опция включена, то агент будет перехватывать набор текста на клавиатуре только при работе в указанных программах.



Скриншоты:

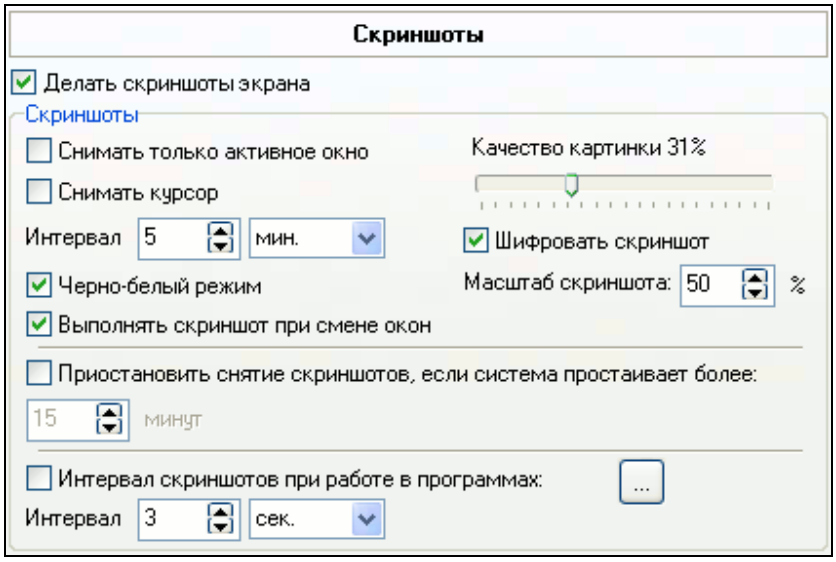


Рис. 4.24 – Настройки контроля снимков экранов

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.

Шифровать скриншот - если данная опция включена, но созданные агентом скриншоты будут зашифрованы. Если отключена, то скриншоты будут созданы в "открытом" виде.

Черно-белый режим - если данная опция включена, то снимки экрана будут производиться в черно-белом режиме (градации серого), что уменьшит размер, занимаемый каждым из снимков на диске.

Выполнять скриншот при смене окон - если данная опция включена, то при каждой смене окон программ будет происходить выполнение скриншота. Таким образом повышается информативность данного мониторинга.

Масштаб скриншота - скриншот будет уменьшен до указанного в процентах размера от изначального. 100% - снимок в полном размере (без уменьшения). Данная опция позволяет уменьшить занимаемое каждым скриншотом на диске место.

Интервал скриншотов при работе в программах - если данная опция включена, то в те моменты времени, когда активно окно любой из выбранных из списка программ, агент будет делать снимки экрана монитора с указанным интервалом. В примере это 3 секунды. Это позволяет для отдельных программ выполнять скриншоты чаще, чем при работе в остальных приложениях.

Программы:

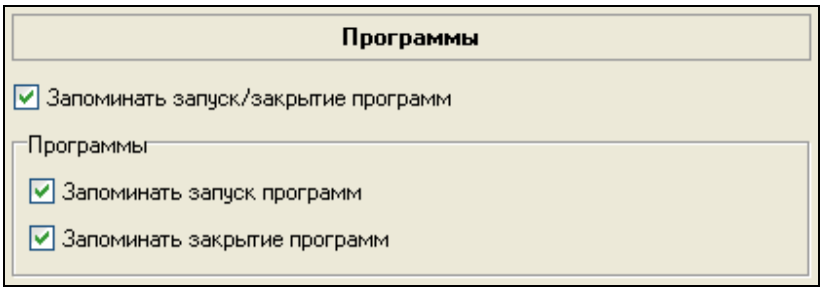


Рис. 4.25 – Настройки контроля запуска/закрытия программ

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:

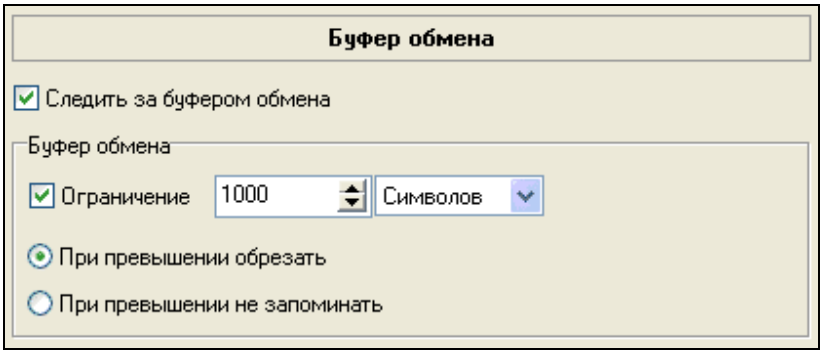


Рис. 4.26 – Настройки контроля буфера обмена

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:

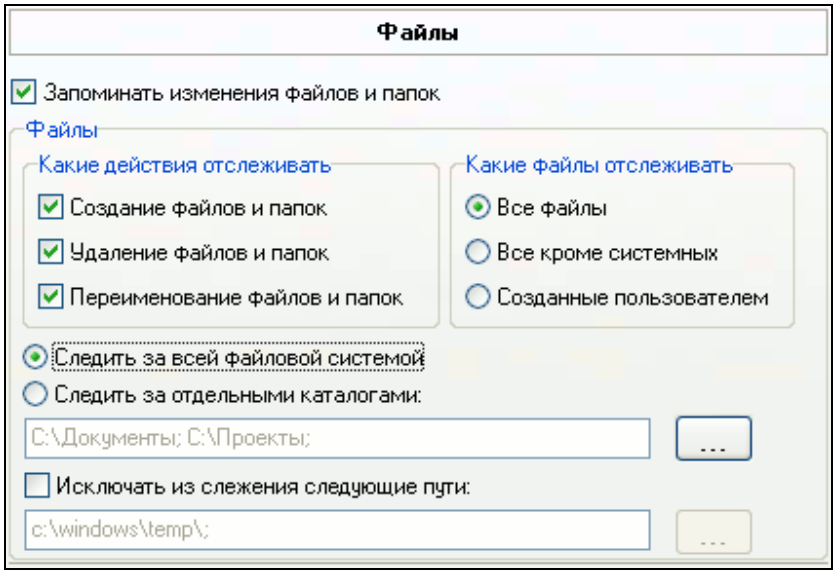


Рис. 4.27 – Настройки ведения мониторинга файловой системы

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 отдельными каталогами - наблюдение будет производится только за теми файлами, которые расположены в указанных каталогах. **Внимание!** Когда включена данная опция, "теневое копирование" файлов на съемные диски становится недоступным.

Исключать из слежения следующие пути - если данная опция включена, то из мониторинга файловой системы будут исключены указанные в соответствующем поле пути.

Компьютер:

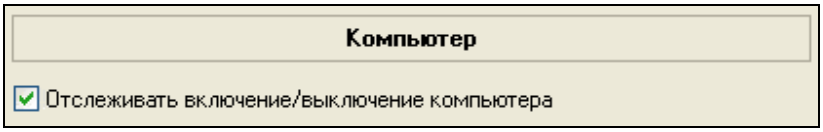
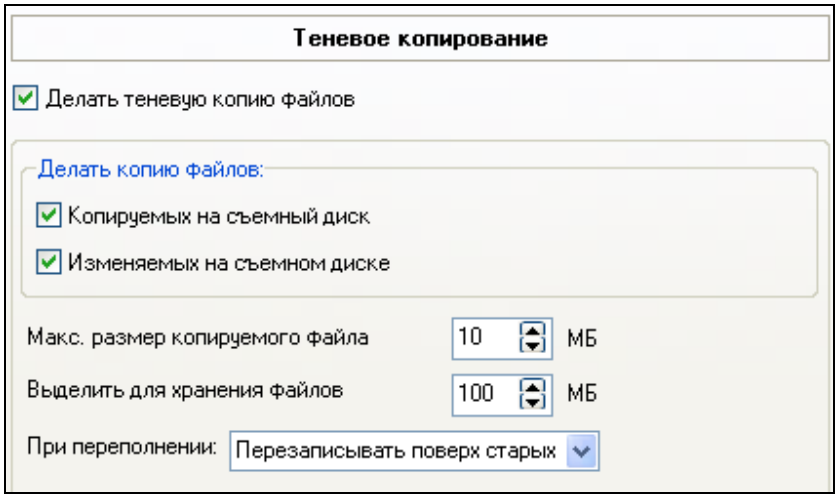


Рис. 4.28 – Настройки статистики включения/выключения компьютера

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

Теневое копирование:



Делать теневую копию файлов - установите эту галочку, чтобы программа осуществляла теневое копирование файлов, копируемых на usb носители или изменяемых на них.

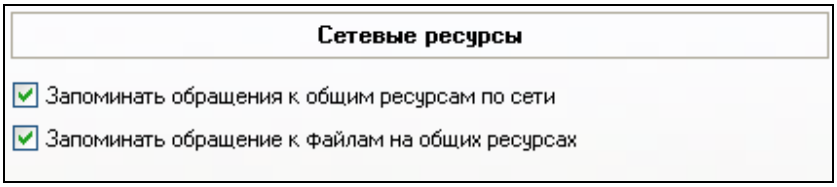
Копируемых на съемный диск - установите эту галочку, чтобы программа производила теневое копирование в том случае, когда файлы копируются на съемный диск.

Изменяемых на съемном диске - установите эту галочку, чтобы программа производила теневое копирование в том случае, когда файлы изменяются (редактируются) на самом съемном диске.

Макс. размер копируемого файла - если на съемный диск будет копироваться файл большего размера, чем данное значение, теневая копия такого файла произведена не будет. Будьте осторожны при установке больших значений для данного поля, т.к. это приведет к повышенной нагрузке на локальную сеть и будет занимать много места на диске.

Выделить для хранения файлов - здесь определяется сколько места на контролируемом компьютере будет выделено под хранение "теневых" файлов. При переполнении будет произведено одно из указанных действий: либо новые файлы не будут писаться, либо новые файлы будут перезаписываться поверх старых.

Сетевые ресурсы:



Запоминать обращение к общим ресурсам по сети - установите эту галочку, чтобы программа запоминала обращение к общим ресурсам компьютера пользователей по сети.

Запоминать обращение к файлам на общих ресурсах - установите эту галочку, чтобы программа запоминала обращения по сети к конкретным файлам, расположенным на общих ресурсах компьютера.

Internet логи - действия:

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

Запоминать переписку ICQ - установите эту галочку, чтобы программа перехватывала сообщения ICQ с любых icq клиентов: ICQ, QIP, Miranda, ...

Запоминать переписку MailAgent - установите эту галочку, чтобы программа перехватывала переписку через Mail.ru Agent.

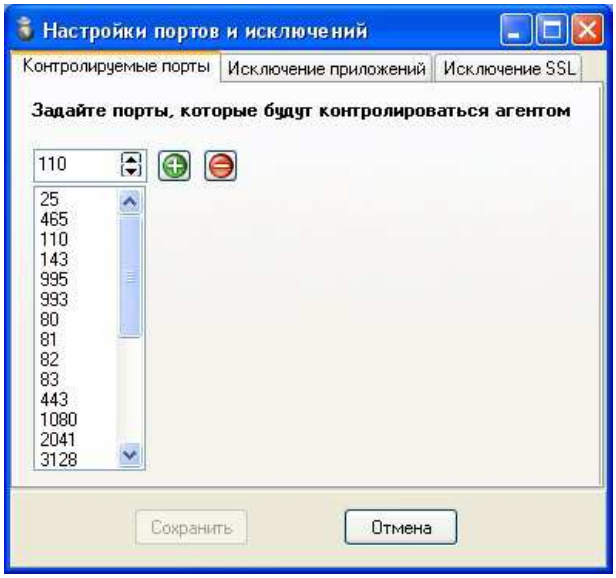
Запоминать e-mail почтовых клиентов - установите эту галочку, чтобы программа перехватывала электронные письма, отправляемые и получаемые с использованием любых почтовых клиентов (Outlook, Outlook Express, The Bat, ...)

Запоминать переписку MSN - установите эту галочку, чтобы программа перехватывала сообщения по протоколу MSN.

Запоминать переписку протокола Jabber - установите эту галочку, чтобы программа перехватывала сообщения, отправленные и полученные с использованием протокола Jabber. Например, при работе в программах QIP Infium, GTalk, ...

Контролировать HTTPS трафик – при установленной галочке, агент будет контролировать трафик, проходящий по шифрованным соединениям.

Контролируемые порты и Исключения из фильтрации трафика - при нажатии данной кнопки будет открыто дополнительное окно настройки. В нем можно задавать список контролируемых агентом портов, а также исключить из контроля трафика определенные приложения или сайты. Для исключения приложения, надо на вкладке «Исключение приложений» добавить в список имя исполняемого файла приложения. Для исключения сайта, надо добавить на вкладке «Исключение SSL» в список домен данного сайта, без https и без слешей. Пример: sbrf.ru



Посещённые сайты:

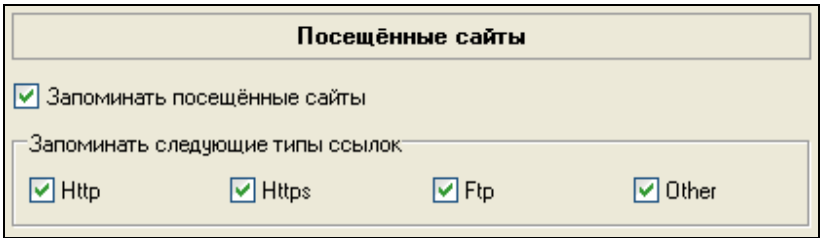
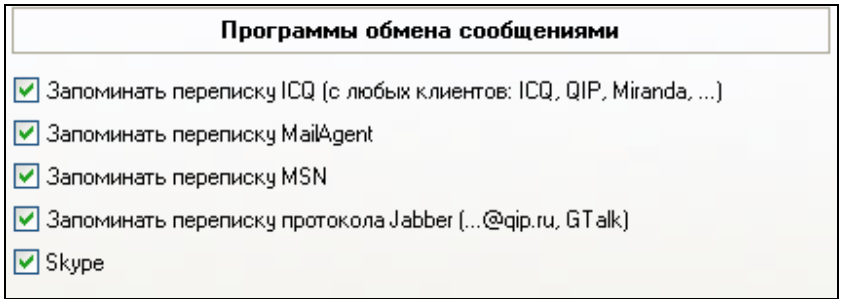


Рис. 4.30 – Настройки контроля посещенных сайтов

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

Программы обмена сообщениями:



Почта:

Если нет необходимости контролировать почту от почтовых клиентов, то уберите галочку для данного пункта.

Принтер:

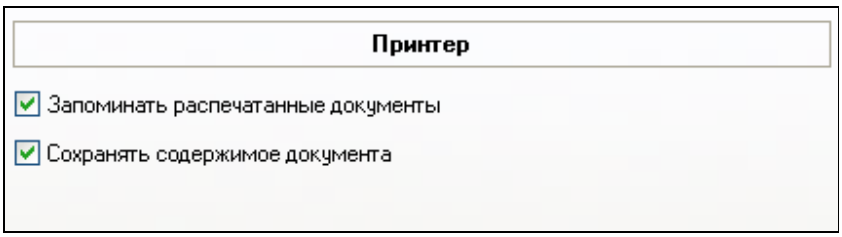


Рис. 4.31 – Настройки контроля принтеров

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

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

Установленные программы:

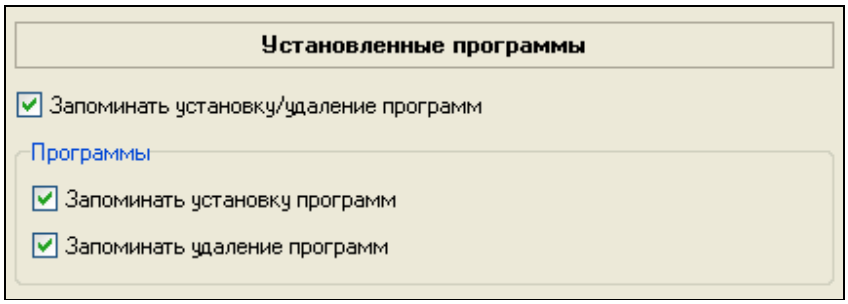


Рис. 4.32 – Настройки контроля установленных программ

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:

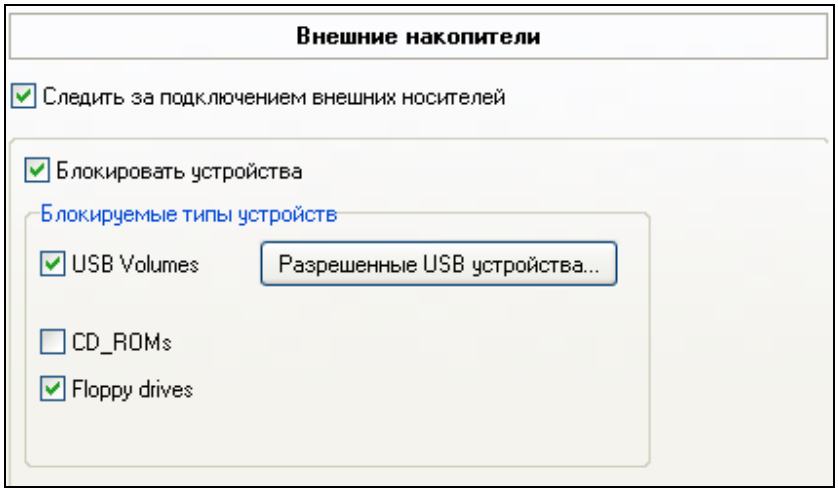


Рис. 4.33 – Настройки контроля подключения носителей

Следить за подключением внешних носителей - установите эту галочку, чтобы программа отслеживала подключение и отключение внешних носителей информации.
Блокировать устройства - включите данную опцию, если необходимо производить блокировку подключения накопителей на контролируемом ПК. Ниже приведены типы устройств, которые можно заблокировать. Для USB накопителей можно задать список разрешенных устройств (работа с устройствами из списка будет разрешена, все остальные - будут блокироваться). Для этого надо нажать кнопку "Разрешенные USB устройства..." и в открывшемся окне перенести нужные серийные номера из списка в правой части окна в список в левой. Если какое-то из устройств будет разрешенным для всех компьютеров, то его можно добавить в список разрешенных для всех соответствующей кнопкой.

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.

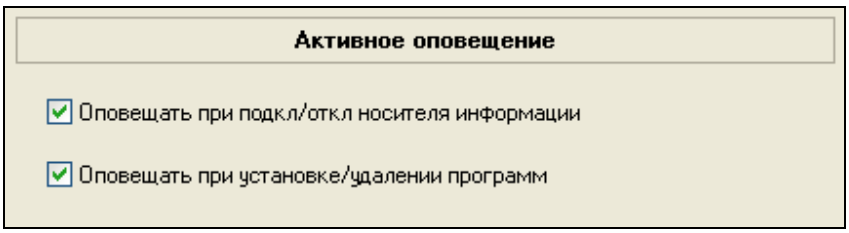
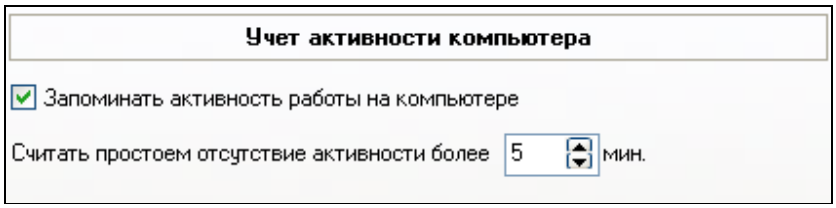


Рис. 4.34 – Настройки активного оповещения

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.

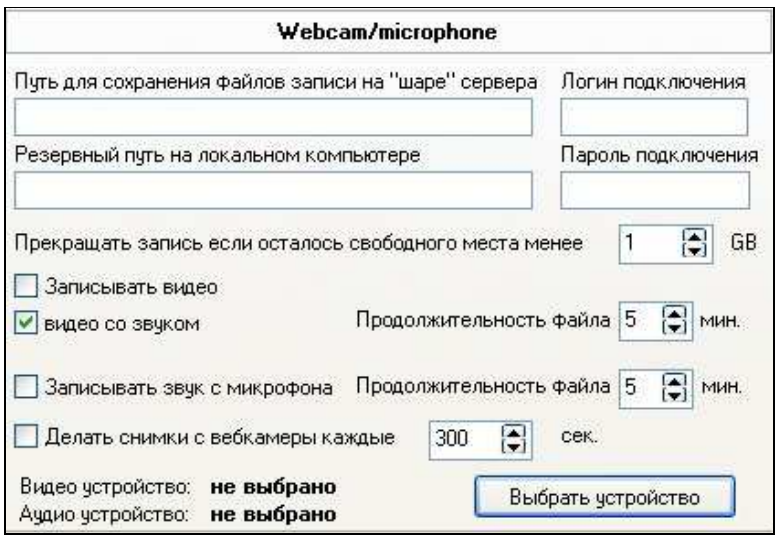
Учет активности компьютера:



Запоминать активность работы компьютера - установите данную галочку, если хотите чтобы программа вела подсчет времени активной работы и простоя компьютера.

Считать простоем отсутствие активности более - укажите значение времени, при превышении которого при отсутствии активности на компьютере считается, что компьютер простаивает.

Webcam/microphone:



Путь для сохранения файлов на «шаре» сервера – для хранения видео/аудио файлов и снимков, полученных с web камеры контролируемого компьютера, необходимо на сервере (компьютере, который большую часть времени будет включен), создать каталог с открытым доступом по сети. **Для данного каталога надо**

задать права на просмотр информации для учетной записи Windows, под которой происходит работа на компьютере с административной консолью LA Standard, а также создать еще одну учетную запись с правами на запись данных в данный каталог. Параметры этой второй учетной записи (логин и пароль) надо указать в соответствующих полях справа от полей путей размещения файлов. Без указания этих данных, будет невозможно скопировать файлы в открытый сетевой каталог на сервере.

Резервный путь на локальном компьютере – данный путь на локальном компьютере будет использоваться для временного размещения аудио/видео файлов в случае, когда каталог на сервере по какой-то причине стал недоступен. После восстановления доступа к серверу, файлы из резервного каталога будут перемещены на сервер. Если данный путь не задать, то агент будет использовать для временного размещения файлов свой штатный каталог, расположенный на системном диске.

Прекращать запись если осталось свободного места менее – когда на диске, на который производится запись файлов, останется места менее указанного значения, дальнейшая запись видео и аудио будет прекращена.

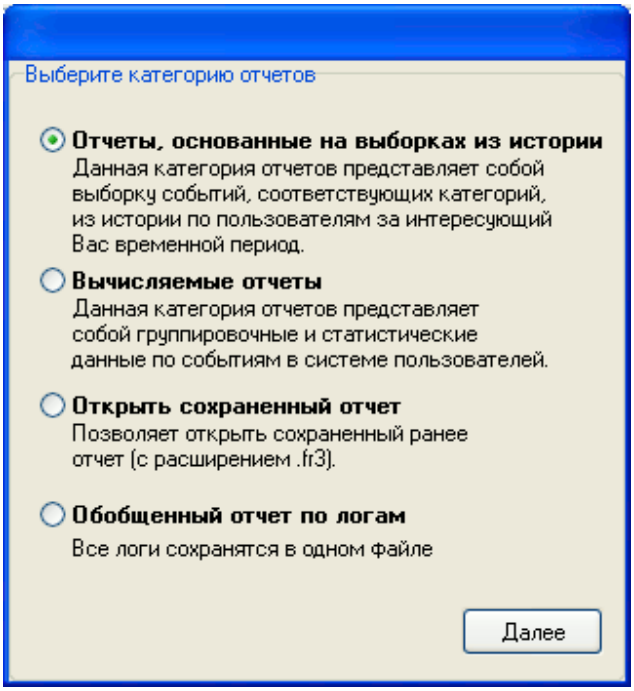
Записывать видео, Записывать звук с микрофона, Делать снимки с веб камеры – выберите наиболее подходящее для решения Вашей задачи действие. Для видео и аудио файлов задается продолжительность каждой записи. Запись будут вестись непрерывно, пока контролируемый компьютер включен. Для снимков с веб камеры задается интервал их выполнения.

При включении записи видео или звука, в обязательном порядке будет предложено выбрать видео и аудио устройства, через которые запись будет производиться. Изменить выбор устройств можно нажав кнопку «**Выбрать устройство**».

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". При нажатии кнопки "Изменить настр-и по умолчанию", текущие настройки станут настройками по умолчанию.

4.11 Составление отчетов

При вызове мастера отчетов откроется следующее окно:



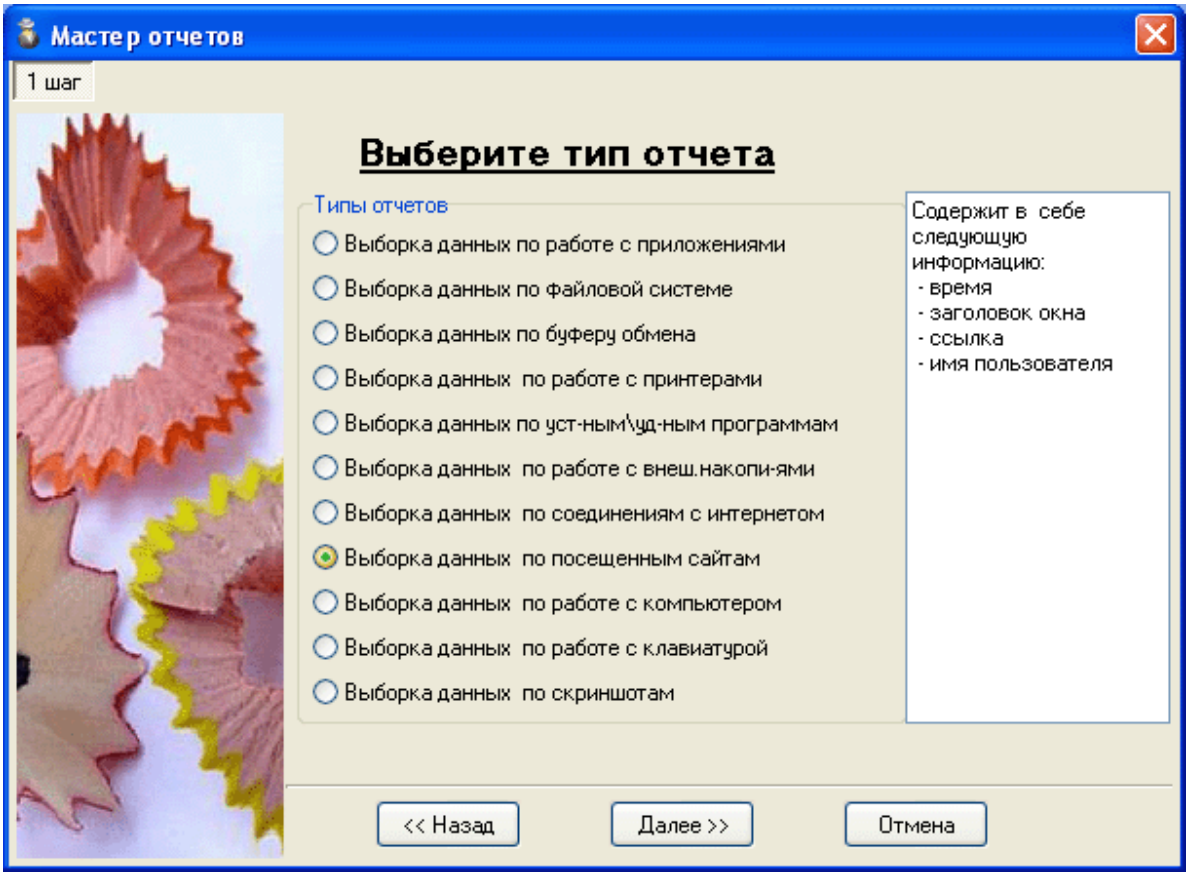
Как видно из рисунка, отчеты имеются 2-х категорий, каждая из которых содержит свой набор отчетов: это **«Вычисляемые отчеты»** (полученные на основе статистического анализа информации) и **«Отчеты, основанные на выборках из истории»**, которые по структуре повторяют выбираемые данные в окне просмотра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

Созданные ранее отчеты, сохраненные через интерфейс программы (файлы с расширением .fr3), можно открыть, выбрав третий пункт: **"Открыть сохраненный отчет".**

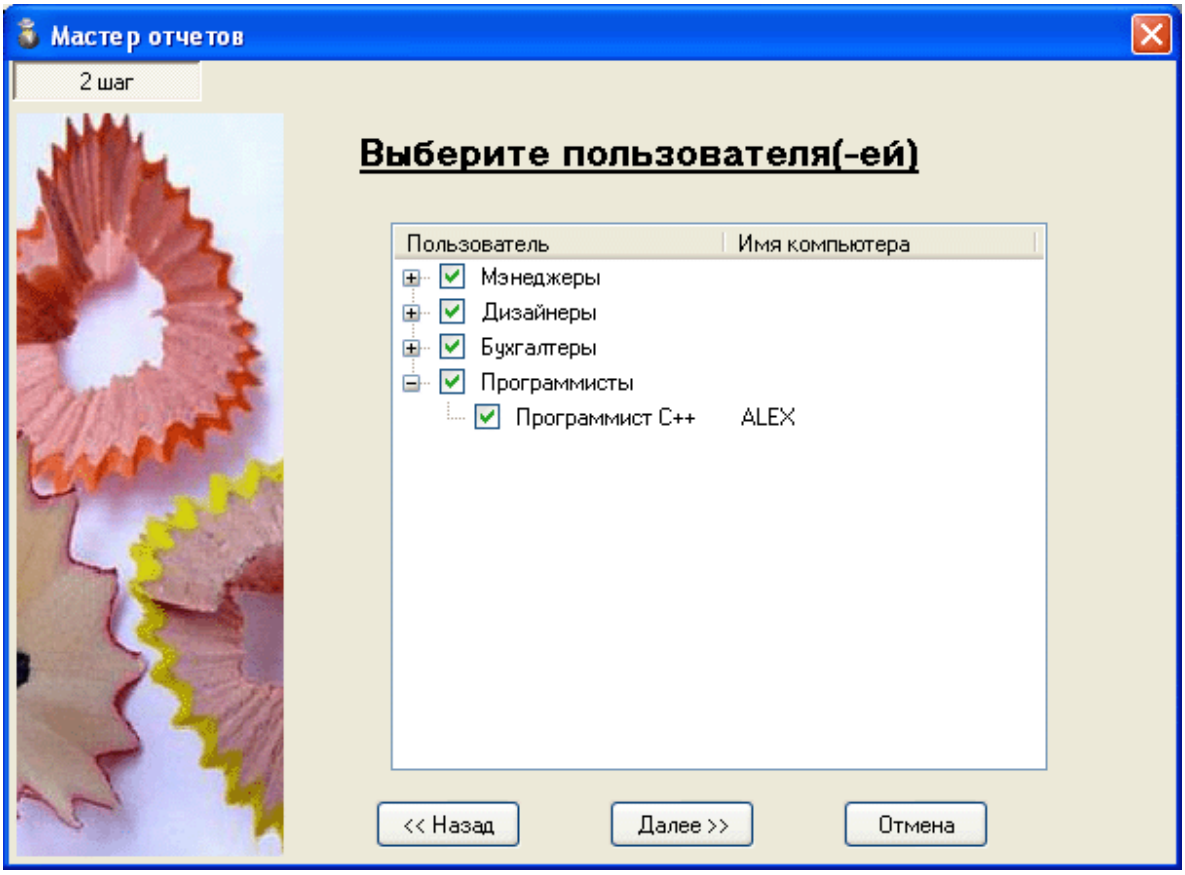
Также, через данную форму можно сформировать **обобщенный отчет в html формате**.

4.11.1 Отчеты - выборки

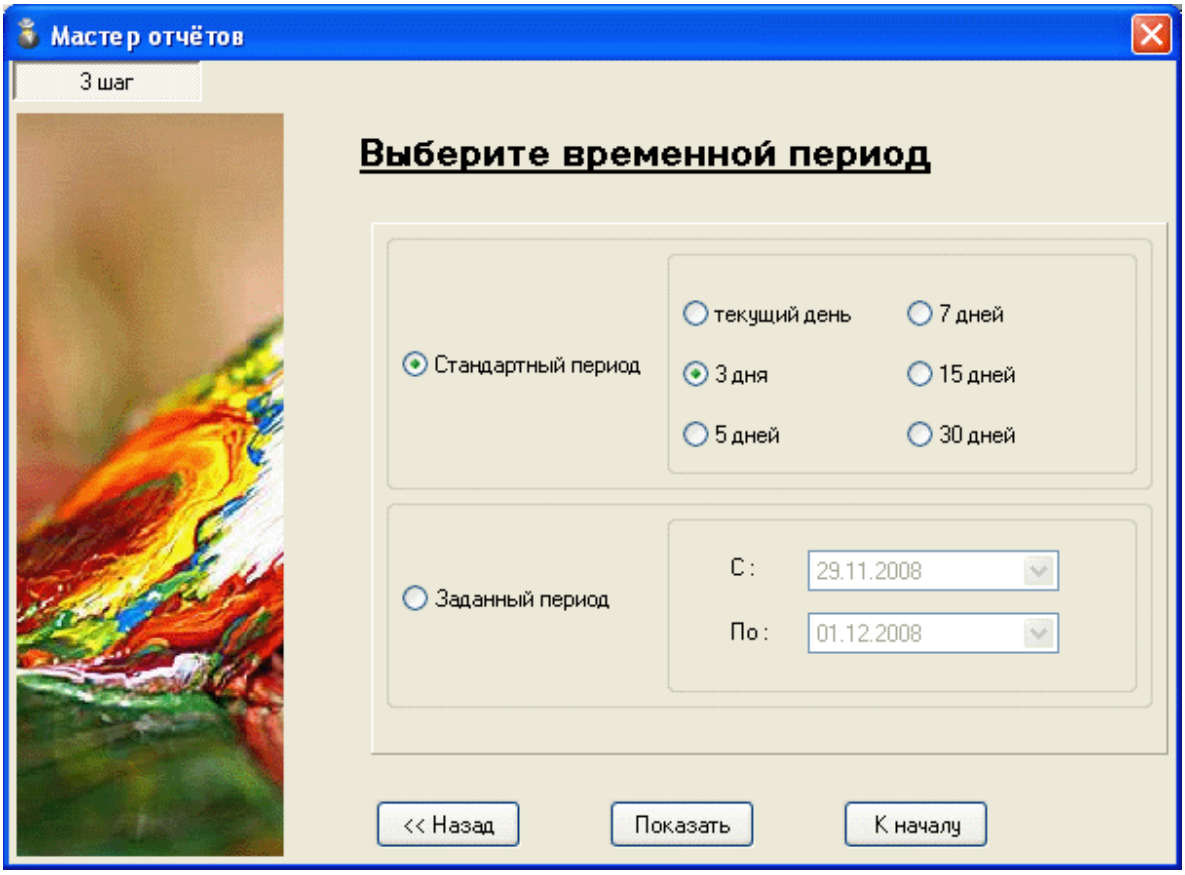
Набор отчетов-выборок имеет следующий вид:



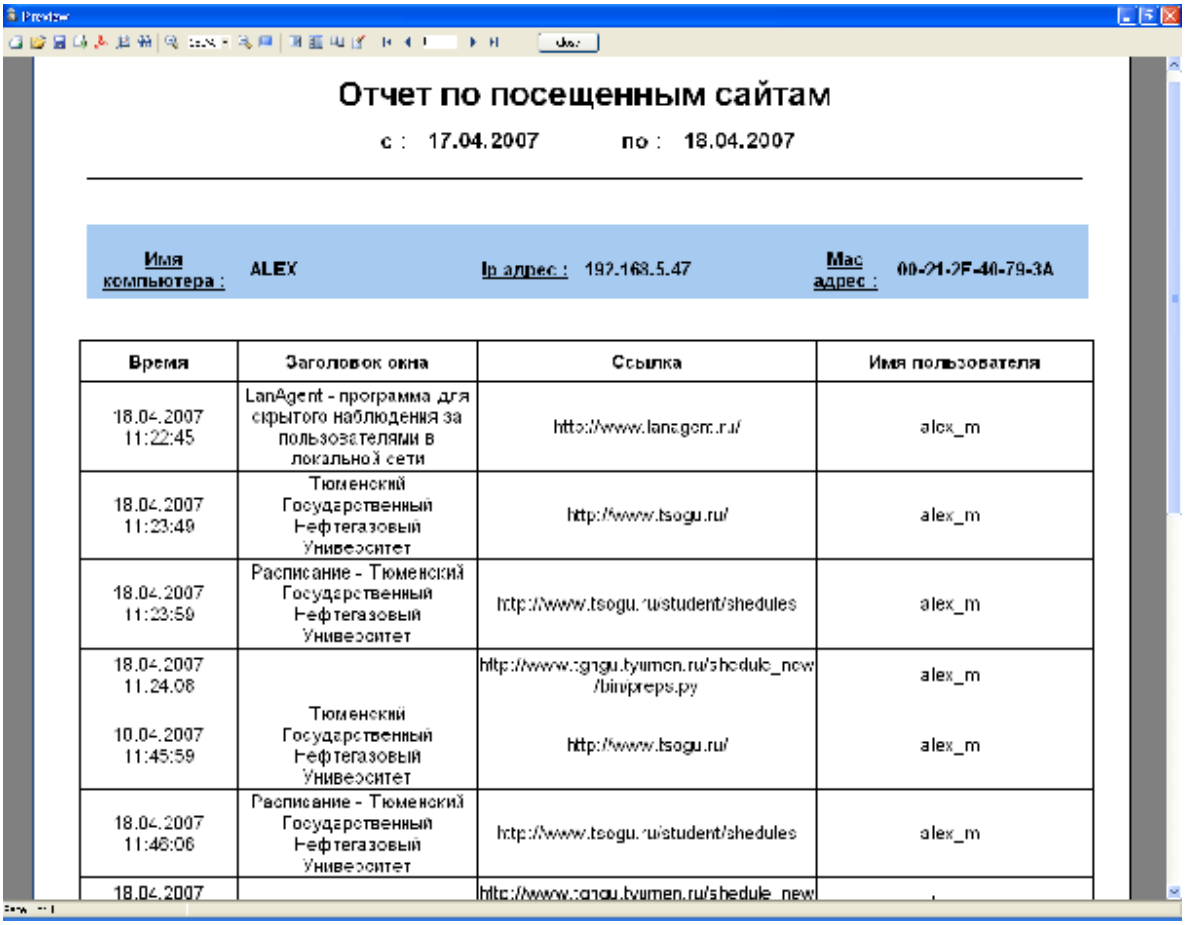
Выберите из списка нужный тип отчета и нажмите кнопку **"Далее"**. В открывшемся окне укажите компьютеры, для которых будет составляться отчет.



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

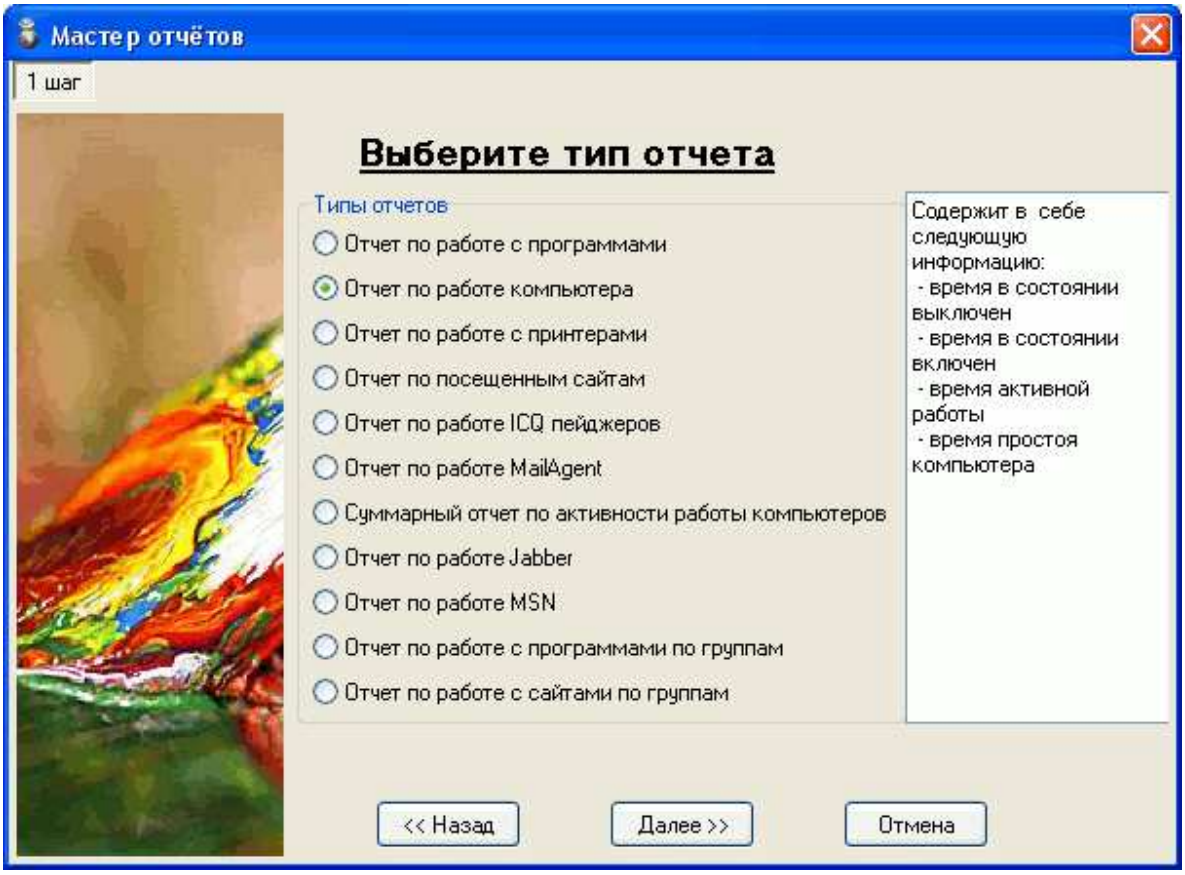
Имя компьютера : ALEX Ip адрес : 192.168.5.47 Mac адрес : 00-21-2F-40-79-3A

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	Тюменский Государственный Нефтегазовый Университет	http://www.cgngu.tyumen.ru/shedule_new/bin/preps.py	alex_m
10.04.2007 11:45:59		http://www.tsogu.ru/	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.cgngu.tyumen.ru/shedule_new/	

Также отчет - выборка может быть сформирован по любой из категорий логов непосредственно в окне просмотра логов. Для этого достаточно щелкнуть по любой из строк правой клавишей мыши и выбрать из выпадающего меню вариант "Сделать отчет".

4.11.2 Вычисляемые отчёты

Набор вычисляемых отчетов имеет следующий вид:

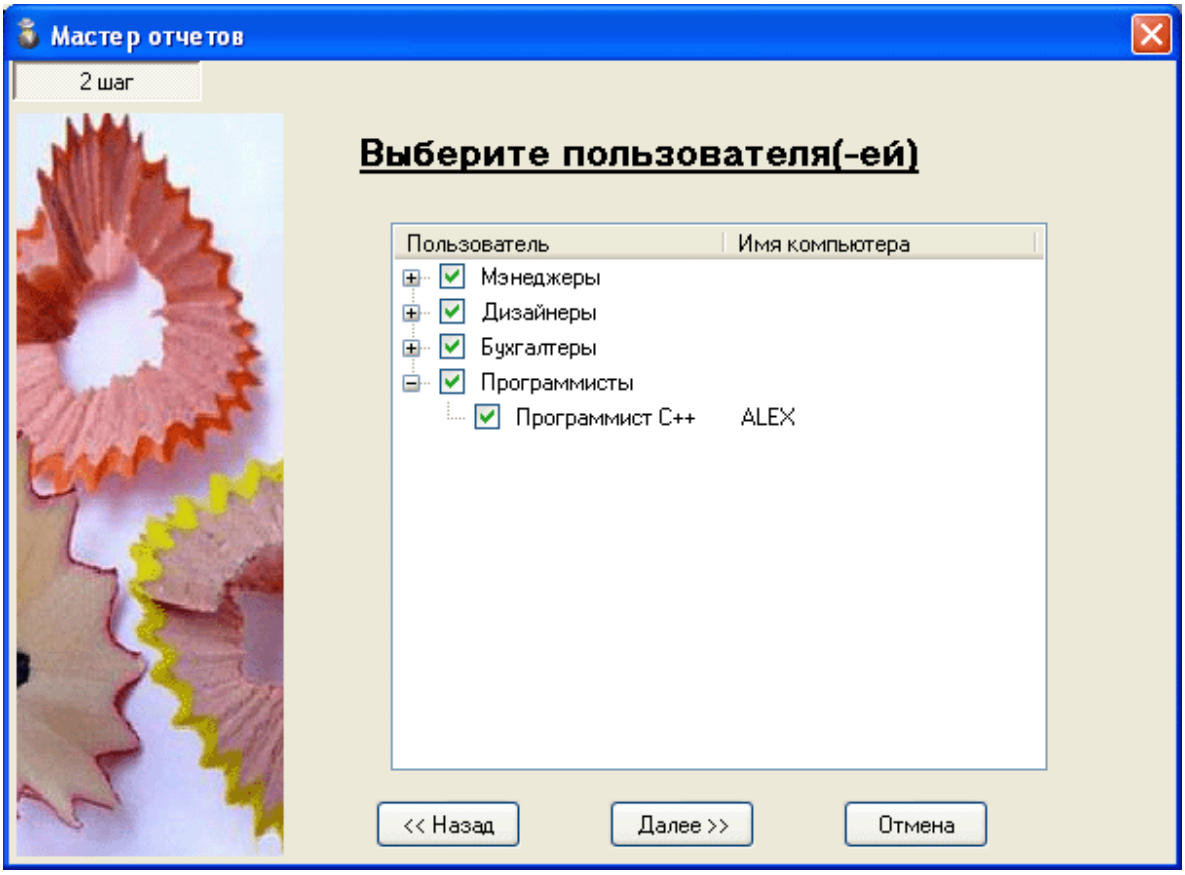


Это статистика по работе программ (содержит следующие данные: названия, количество запусков, общее время работы, процент от общего числа запусков); Статистика работы с компьютером (время работы, время простоя, количество вкл/выкл); Статистика использования принтеров (на каком принтере сколько раз печатали,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

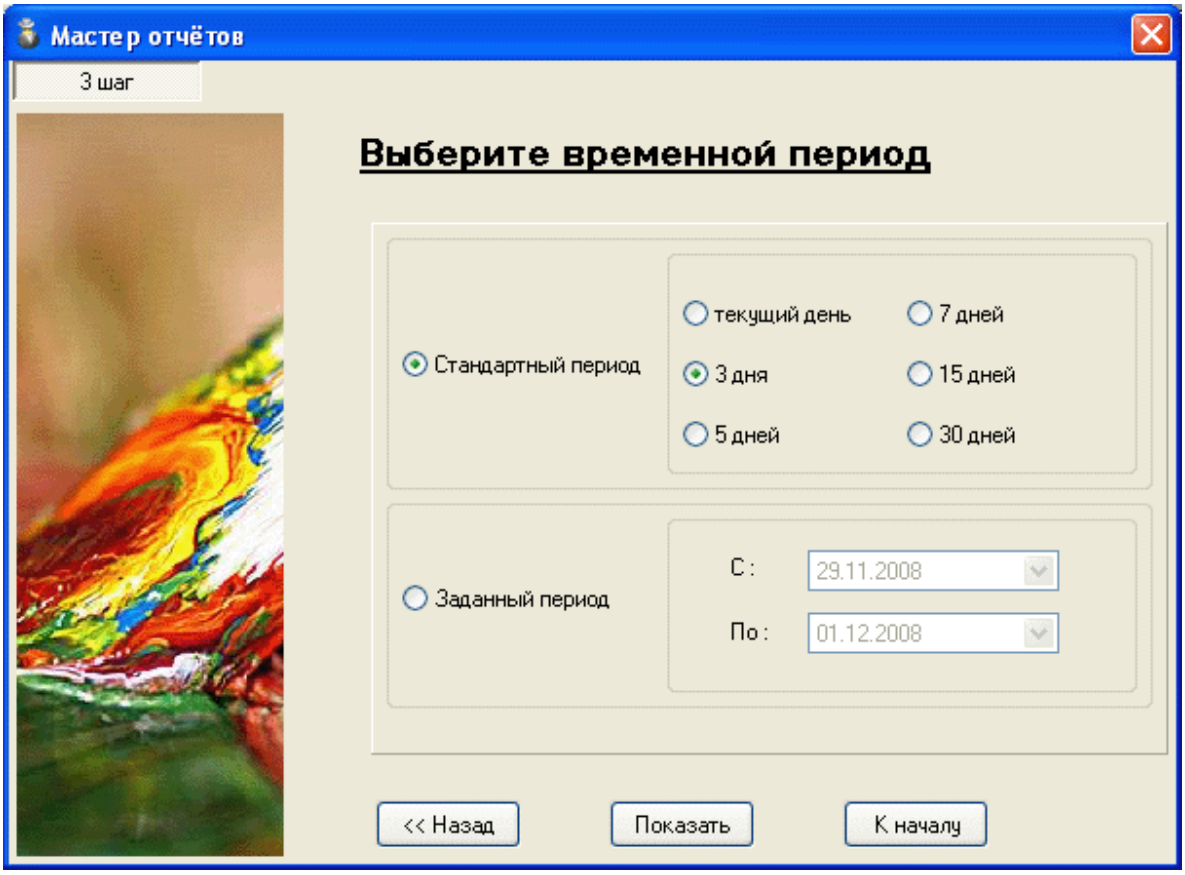
Также имеются отчеты по работе с программами и посещению веб сайтов **с разбивкой информации по группам** (категориям). В таких отчетах наглядно показывается какая категория программ (Офисные программы, Развлечения, ... и т.д.) или сайтов занимает у пользователя больше всего времени.

Суммарный отчет по активности работы компьютеров содержит такую информацию, как таблица времен начала и окончания работы каждого из компьютеров, средняя длительность рабочего дня, время активной работы на компьютерах, а также сравнительные гистограммы.

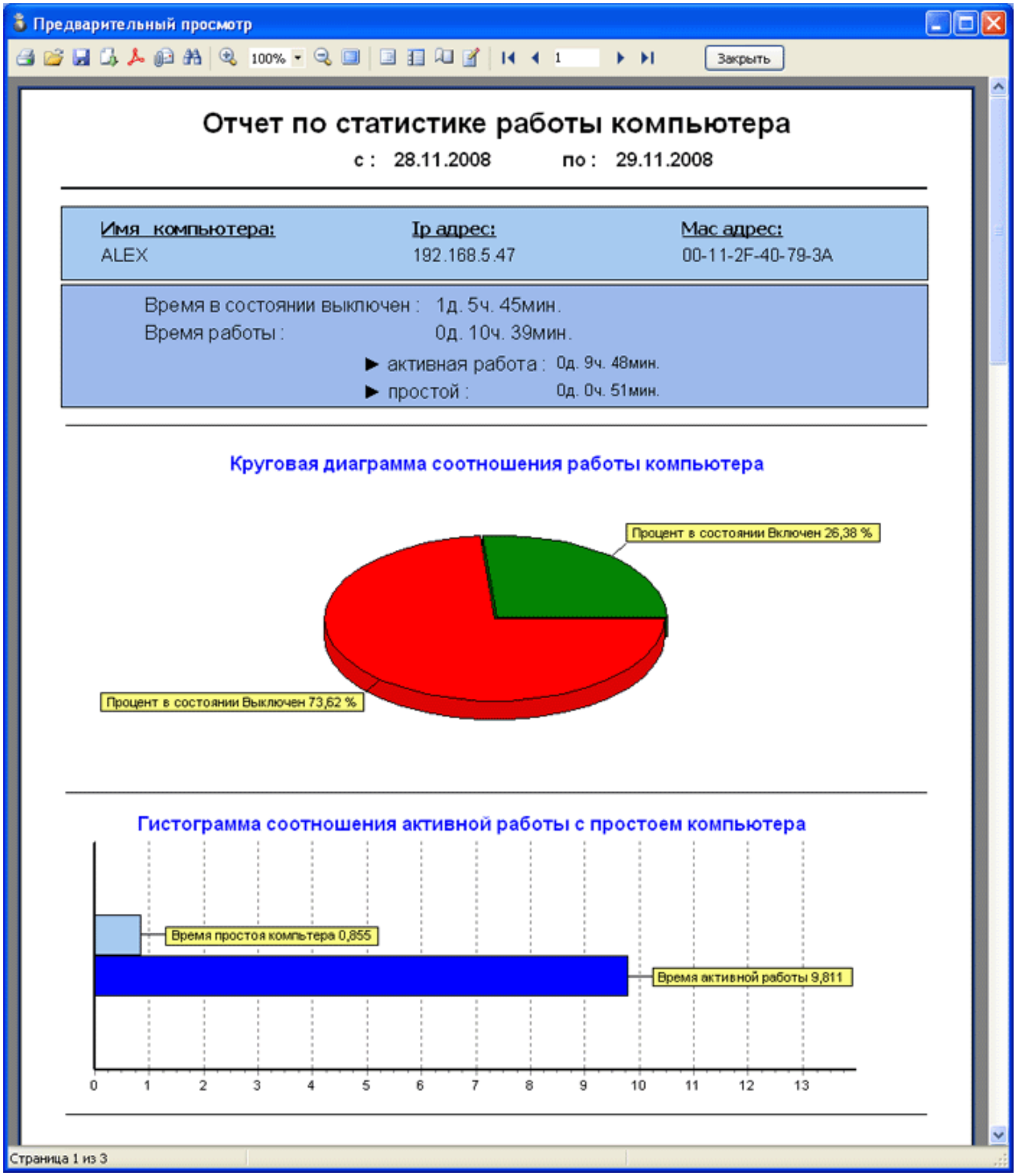
Выберите из списка нужный тип отчета и нажмите кнопку **"Далее"**. В открывшемся окне укажите компьютеры, для которых будет составляться отчет.



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

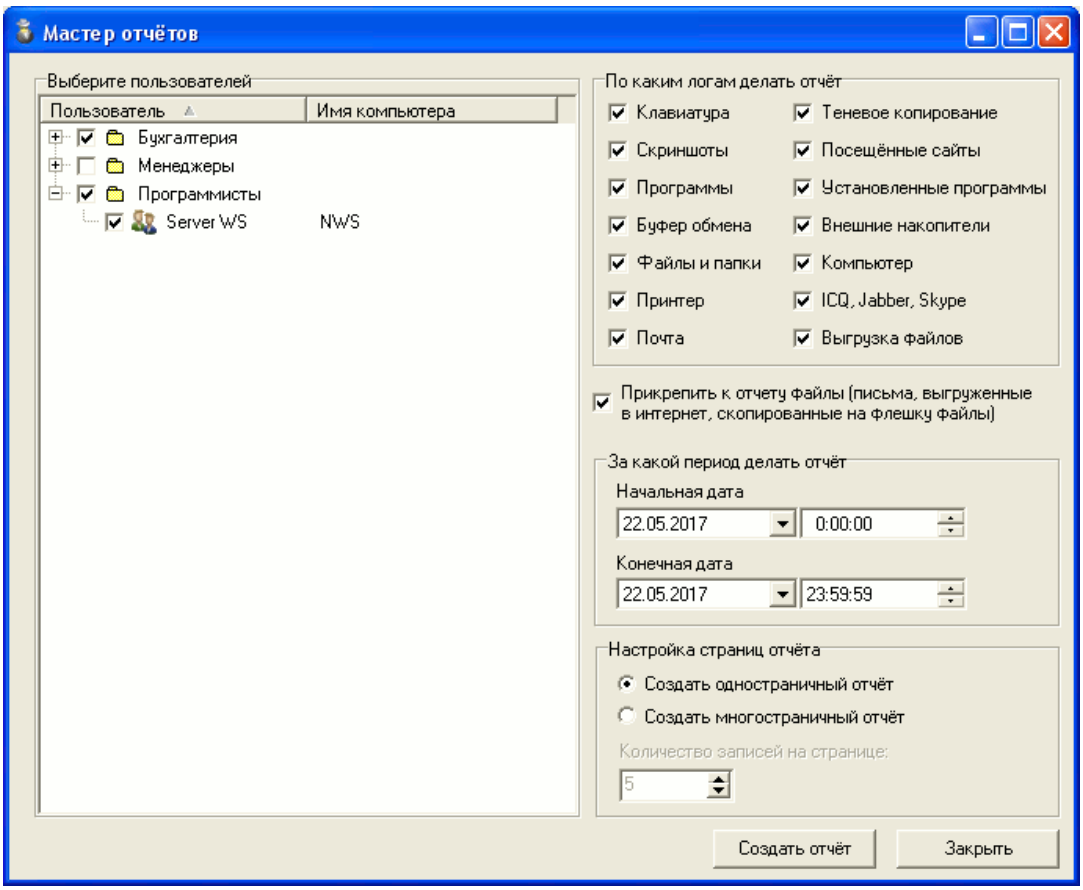


Ниже представлен пример вычисляемого отчета по статистике работы компьютера.


Предварительный просмотр
100%
1
Закрыть
Отчет по статистике работы компьютера
с : 28.11.2008 по : 29.11.2008
Имя компьютера:
ALEX
Ip адрес:
192.168.5.47
Mac адрес:
00-11-2F-40-79-3A
Время в состоянии выключен : 1д. 5ч. 45мин.
Время работы : 0д. 10ч. 39мин.
► активная работа : 0д. 9ч. 48мин.
► простой : 0д. 0ч. 51мин.
Круговая диаграмма соотношения работы компьютера
Процент в состоянии Включен 26,38 %
Процент в состоянии Выключен 73,62 %
Гистограмма соотношения активной работы с простоем компьютера
Время простоя компьютера 0,855
Время активной работы 9,811
0 1 2 3 4 5 6 7 8 9 10 11 12 13
Страница 1 из 3

4.11.3 Обобщенный отчет по логам (в html формате)

Данный отчет позволяет отобразить все события, произошедшие на компьютере в хронологической последовательности.



Для этого достаточно выбрать категории событий, которые требуется включить в отчет, задать временной интервал его выполнения.

Данный отчет позволяет включить в себя также и все файлы данных: файлы писем, вложенных файлов, копии файлов, размещенных на USB накопители и т.д. Это регулируется соответствующей опцией.

Сам отчет можно создать как одностраничный html документ или многостраничный.

Выбрав нужные опции, нажмите кнопку «Создать отчет» и выберите каталог для его сохранения.

4.12 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.

4.12.1 Удаление программы LanAgent с компьютера администратора

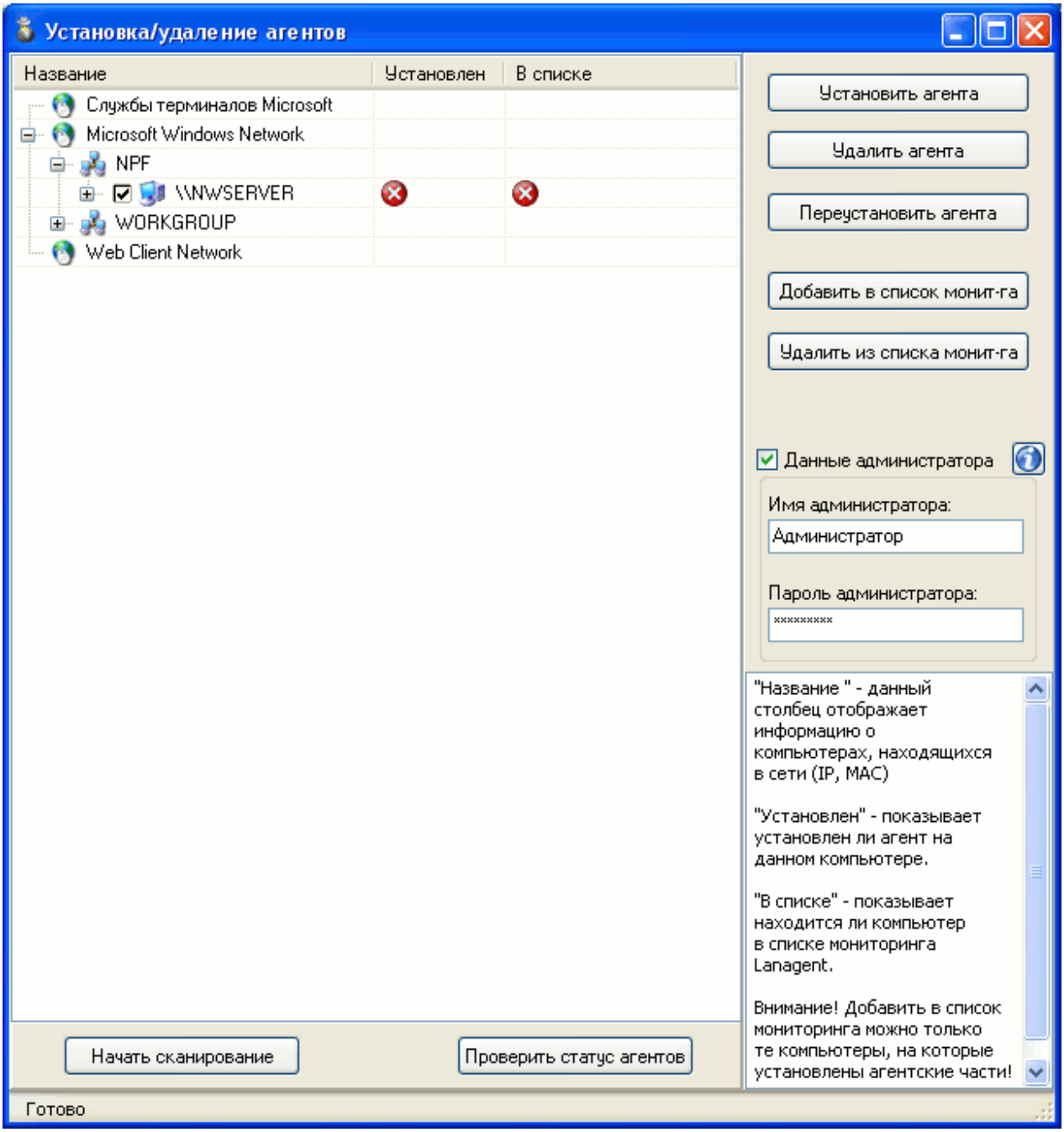
Для удаления базовой программы LanAgent вы можете использовать стандартные средства Windows, как и для любого другого приложения. Для этого в "Панели управления" ("Control Panel") выбрать пункт "Установка и удаление программ" ("Add and remove programs"), выберите в списке "LanAgent" и нажмите кнопку "Удалить" ("Remove").

4.12.2 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

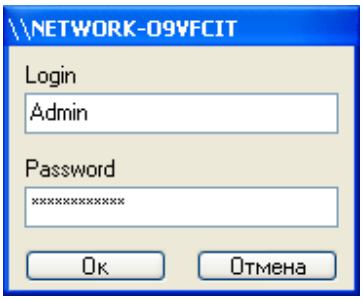
Для этого воспользуйтесь диалогом установки/удаления агентов, который вызывается в администраторской части LanAgent кнопкой "**Добавить**".



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

Далее, надо отметить галочками компьютеры, на которых необходимо удалить агентскую часть программы и нажать кнопку "**Удалить агента**". Если для всех выбранных компьютеров может быть использована одна и та же связка логин/пароль, то можно задать ее один раз в панели в правой части окна и поставить

галочку "Данные администратора" (так, как это сделано на экране выше). В противном случае для каждого выбранного компьютера будет вызван диалог ввода логина и пароля администратора.



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

Если в процессе удаления возникнут ошибки, то они будут выведены на экран в виде сообщений.

Подробней об устранении ошибок при деинсталляции агентов можно посмотреть в пункте 3.2.3.

Также, удаление агентов в сетях с доменом можно произвести при помощи групповых политик.

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

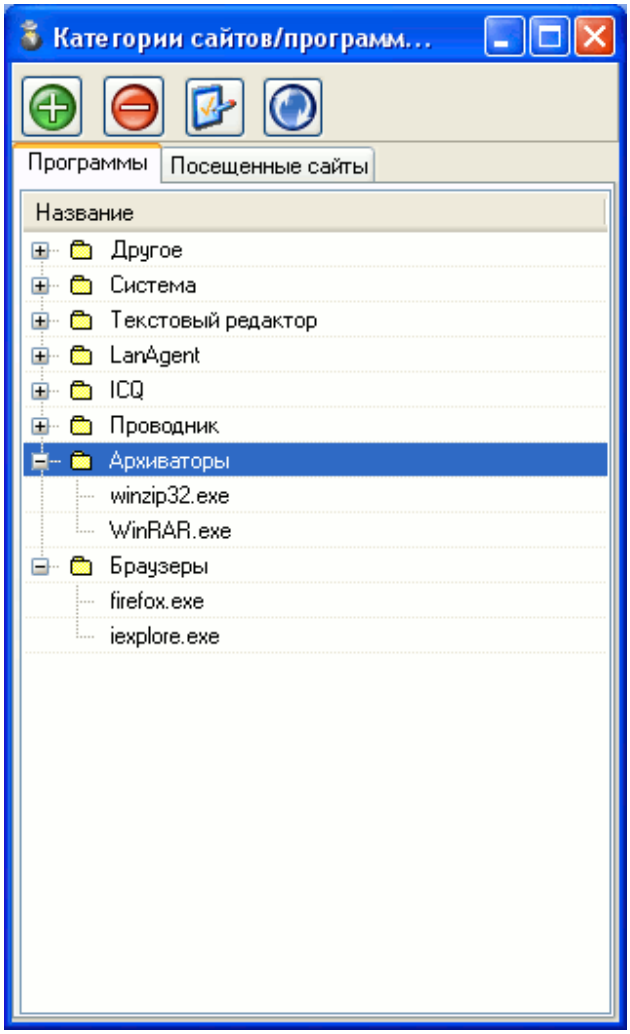
1. Запустите оснастку **Active Directory – пользователи и компьютеры** (Active Directory Users and Computers).
2. Кликните правой клавишей мыши на имени вашего домена и выберете **Свойства**.
3. Перейдите на вкладку **Групповая политика** и выбрав нужную политику нажмите **Изменить**.
4. Разверните ветвь **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**.

4.13 Категории программ/сайтов

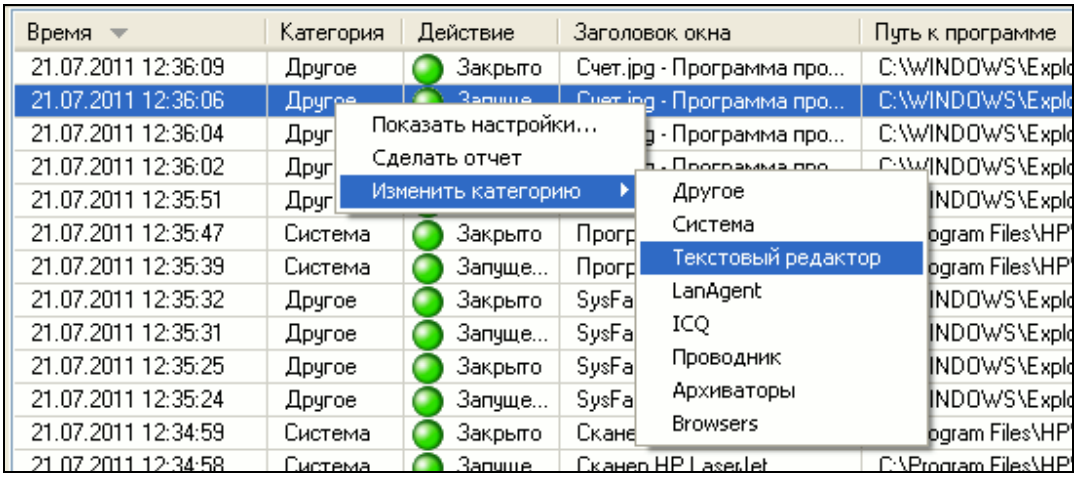
Начиная с версии 3.0, в LanAgent имеется возможность распределить все программы, запускаемые на пользовательских компьютерах, и все посещаемые сайты по категориям. Например: "Развлечение" или "Офисные программы". Категория будет отображаться при просмотре логов работы с программами и посещения веб-сайтов, Также можно формировать по категориям аналитические отчеты. Окно работы с категориями можно открыть, выбрав в верхней панели "Отчеты"->"Категории сайтов/программ..."



По-умолчанию новые программы и сайты заполняются в категорию "Другое". Заполнение списка происходит по мере запуска пользователями программ.

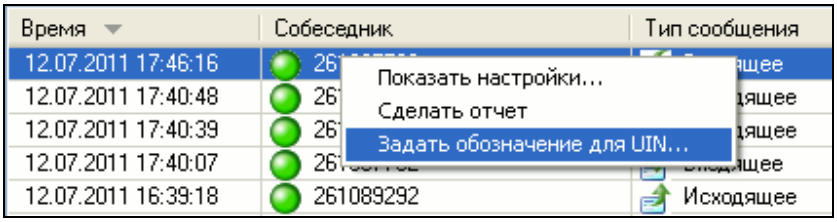
Для создания новой категории, нажмите кнопку  Перемещение программ из одной категории в другую осуществляется обычным "перетаскиванием".

Также, переместить программу или сайт в нужную категорию можно и через сам интерфейс просмотра данных (на закладке "Программы" или "Посещенные сайты" соответственно). Для этого достаточно щелкнуть на строке с программой/сайтом правой клавишей мыши и выбрать в выпадающем меню вариант Изменить категорию и далее выбрать нужную категорию из списка имеющихся.

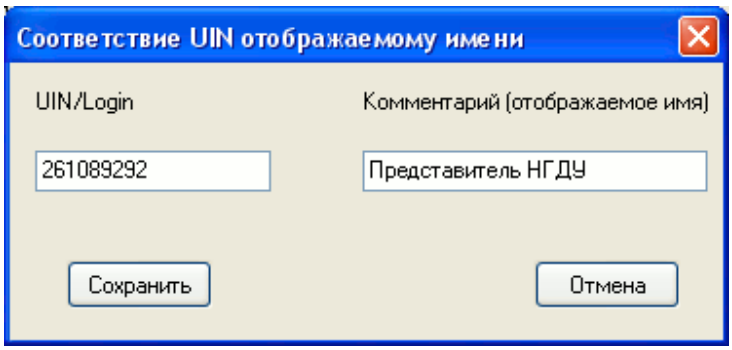


4.14 Комментарии для UIN/логинов

Для более удобного разбора переписки ICQ, QIP, MSN и других программ обмена короткими сообщениями, в LanAgent есть возможность задать комментарий (описание) для конкретного UIN icq или логина других мессенджеров. Сделать это можно прямо из окна просмотра переписки, щелкнув на нужной строке правой клавишей мыши и выбрав в выпадающем меню вариант "Задать обозначение для UIN...".



При этом откроется следующее окно. Задайте в нем комментарий и нажмите кнопку Сохранить.



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.

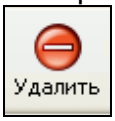
5.1 Типичные действия

1 Добавление компьютера в список мониторинга

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

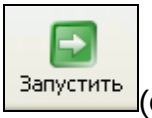
панели инструментов LanAgent или выбрать соответствующий пункт "Добавить пользователя" из меню "Файл".

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".

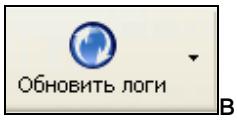
3. Запуск или остановка мониторинга на нужном компьютере

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" 

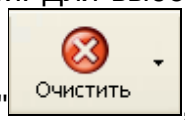
(если хотите его остановить). Эти же действия можно выполнить, выбрав соответствующие пункты из меню "Управление".

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 XP
- Windows 2003 Server
- Windows 2008 Server
- Windows Vista
- Windows 7/8/8.1/10

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 /XP/2003/2008/Vista/7/8/8.1/10.
- Процессор с частотой 1 Ггц и выше.
- 512 МБ оперативной памяти.
- 300 МБ свободного места на диске.
- Наличие установленного XPS Viewer.

Рекомендуемые требования:

- Операционная система: Windows XP/2003/2008/Vista/7/8/8.1/10.
- Процессор с частотой не менее 2 Ггц.
- 1 ГБ оперативной памяти.
- 15 ГБ свободного места на диске (зависит от количества компьютеров и настроек программы).
- Наличие установленной программы просмотра PDF файлов.

Пользовательская часть (агент).

Минимальные требования:

- Операционная система: Windows XP/2003/2008/Vista/7/8/8.1/10.
- Процессор Pentium 3 и выше.
- 256 МБ оперативной памяти.
- 100 МБ свободного места на диске.

Рекомендуемые требования:

- Операционная система: Windows XP/2003/2008/Vista/7/8/8.1/10.
- Процессор с частотой 1 Ггц и выше.
- 512 МБ оперативной памяти.
- 300 МБ 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?

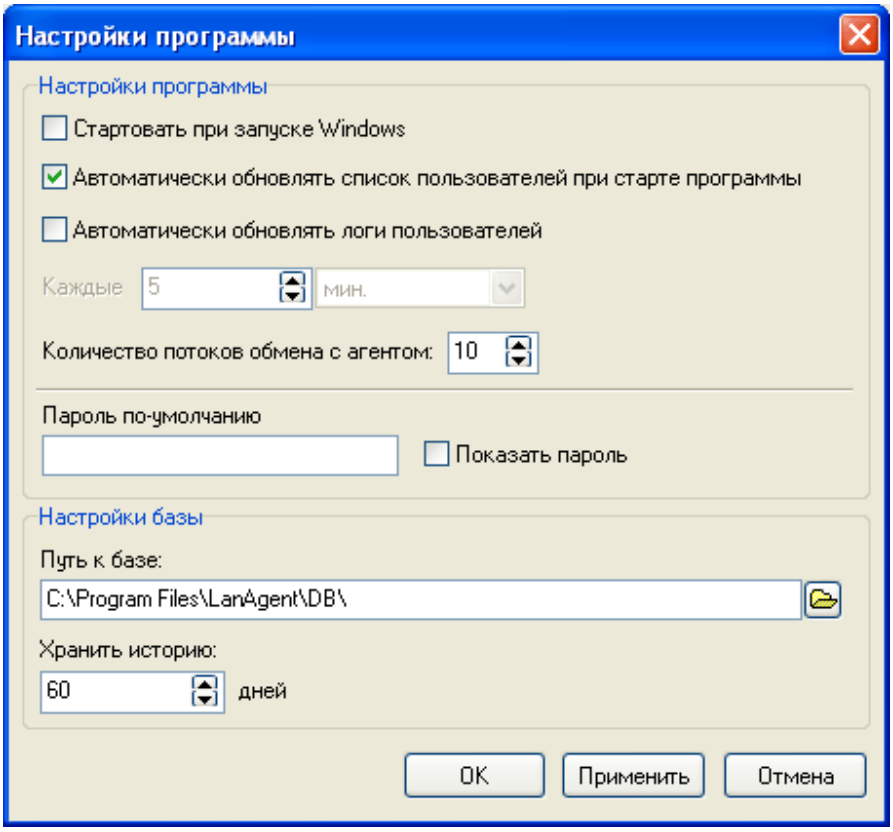
Логи на компьютере пользователя могут храниться сколь угодно долго. Теоретически их размер ограничен только размером свободного дискового пространства. Тем не менее имеется возможность ввести ограничение на их размер, тогда при его превышении будет происходить постепенное затирание старой информации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

Проще всего сделать копию каталога базы данных при закрытой административной консоли (чтобы с базой данных в этот момент никто не работал).