Network PROFI

LanAgent

Владея информацией,
владеешь миром

Руководство пользователя

www.networkprofi.ru

Примечания

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

Предисловие

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

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

Содержание

1 О продукте LanAgent

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.
- Перехватывает сообщения мессенджеров: Skype, Viber, Jabber и т.д..
- Запоминает набираемый на клавиатуре текст.
- Следит за содержимым буфера обмена.
- Перехватывает посещённые сайты.
- Ведет мониторинг входящей и исходящей почты.
- 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 письма, отправляемые через web интерфейс, и выгрузку файлов в Интернет, в том числе на облачные хранилища (яндекс диск, google drive, OneDrive, Dropbox).
- 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 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.
- Скрытый режим работы агентов программы.

Особенности Enterprise версии:

- Обнаружение нестандартного поведения пользователей, при помощи аналитического модуля. В том числе, подозрительные изменения активности, например, необычно большое количество файлов, скопированное за день на USB накопитель. Или нетипично активную переписку. Анализ ведется на основе истории предыдущей работы этого пользователя за компьютером;
- Оповещения администратора системы о подозрительных событиях, совершенных пользователями: включение ПК в нерабочее время, переписка или отправка файлов в нерабочее время; копирование наружу ПК большого количества файлов (больше разрешенного); печать больше разрешенного количества документов и т.д.;
- возможность подключения модуля расширенного поиска (позволяет производить полнотекстовый поиск нарушений правил безопасности, т.е. с учетом синонимов, ошибочных вариантов написаний слов и т.д.). И наличие формы поиска по всем данным в консоли специалиста безопасности.
- постоянный круглосуточный режим работы серверной части программы (она реализована службой windows и для ее работы вход в windows не требуется).
- перехват писем, получаемых и отправляемых с использованием MS Exchange Server.
- возможность использования нескольких консолей специалистов безопасности с возможностью раздачи каждому из них прав на просмотр данных.
- оповещение о произошедших нарушениях правил безопасности на e-mail и icq.
- Встроенный планировщик отчетов с возможностью отправки отчетов на e-mail.
- наличие аналитического отчета по продуктивности использования рабочего времени.
- возможность ограничения доступа к файлам. Позволяет для конкретного файла, каталога или целого диска выдать права только на чтение или совсем запретить доступ (например, разрешить для флешек только чтение)
- режим конфиденциального документа. Для заданного перечня файлов, каталогов, - ставится режим доступа «только чтение» с запретом копировать фрагменты этих документов в буфер обмена или печатать их на принтере.
- Функция сбора данных с контролируемых компьютеров, находящихся вне локальной сети (через интернет), например, командировочного ноутбука.
- Расширенный поисковый модуль с возможностью полнотекстового поиска по всем собранным данным, а также поиска регулярных выражений (паспортные

данные, номера телефонов, ИНН и т.д.).

1.2 Для кого предназначена программа

LanAgent незаменимый помощник:

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

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

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

1.3 Как работает программа LanAgent

Рис. 1.1 – Структура LanAgent

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

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

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

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

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

Данный комплекс включает в себя следующие программы:

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

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

1. управление настройками агентов;
2. настройка политик безопасности;

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

Данный функционал реализован в программе LanAgent Admin.

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

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

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

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

1.4 Системные требования

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

Серверная часть.

Минимальные требования:

- Операционная система: Windows 7/8/8.1/10/11, 2008/2012/2016/2019; Linux.
- Процессор с частотой не менее 1,4 GHz.
- 512 MB оперативной памяти.
- 500 MB свободного места на диске.
- Открытые порты TCP/IP: входящие - 7657, 3050, 6587; исходящий – 47658. На компьютере с сервером LanAgent эти порты должны быть открытыми (если используется фаервол, то надо в нем их открыть).
- При опросе клиентов через интернет, нужно открыть также входящий порт 46658 tcp/ip (подробнее см. пункт 5.5 руководства).

Рекомендуемые требования:

- Операционная система: Windows 7/8/8.1/10/11, 2008/2012/2016/2019; Linux.
- Процессор 2-х или 4-х ядерный с частотой ядра от 3 GHz и выше.
- От 4 GB оперативной памяти.
- 15 GB свободного места на диске (зависит от количества компьютеров и настроек программы).
- Открытые порты TCP/IP: входящие - 7657, 3050, 6587; исходящий – 47658. На компьютере с сервером LanAgent эти порты должны быть открытыми (если используется фаервол, то надо в нем их открыть).
- При опросе клиентов через интернет, нужно открыть также входящий порт 46658 tcp/ip (подробнее см. пункт 5.5 руководства).

Пользовательская часть (агент).

Минимальные требования:

- Операционная система: Windows XP/Vista/7/8/8.1/10/11, Linux.
- Процессор с частотой не менее 1,4 ГГц.
- 512 MB оперативной памяти.
- 300 MB свободного места на диске.
- Открытые порты TCP/IP: входящий – 47658; исходящий – 7657, 46658 на компьютере с агентом (если используется фаервол, то надо в нем их открыть).

Рекомендуемые требования:

- Операционная система: Windows XP/Vista/7/8/8.1/10/11, Linux.
- Процессор с частотой 2,4 Ггц и выше.
- 1 GB оперативной памяти.
- 300 MB свободного места на диске.
- Открытые порты TCP/IP: входящий – 47658; исходящий – 7657, 46658 на компьютере с агентом (если используется фаервол, то надо в нем их открыть).

Операционные системы XP и Vista поддерживаются в ограниченном функционале.

Если требуется контролировать удаленную работу пользователей на терминальном сервере (на 2008/2012/2016/2019), то для этого потребуется дополнительно к версии Enterprise поставить специальный терминальный модуль. Он будет записывать данные по работе пользователей на сервере в основную базу Ентерпрайз.

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

Для просмотра перехваченных изображений напечатанных документов, на компьютере с LanAgent Viewer необходимо иметь установленную программу просмотра pdf файлов. Например, Adobe Acrobat Reader.

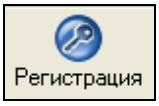
2 Регистрация LanAgent

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 и этот раздел пока пропустите.

Для активации вам необходимо:

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



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

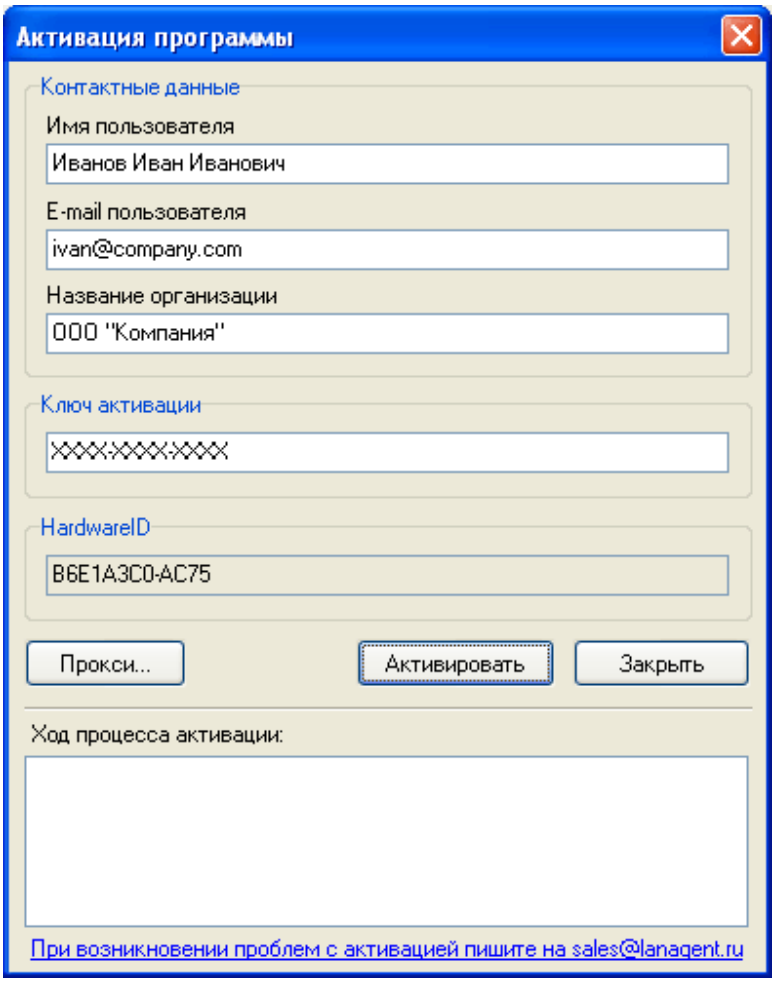


Рис. 2.1 - Активация программы

4. Нажмите кнопку "Активировать" и подождите некоторое время.
5. Если активация прошла успешно, то программа выдаст соответствующее сообщение.
6. Зарегистрируйте и перезапустите сервисы, при помощи «**Менеджера сервисов**»: регистрация сервисов производится нажатием кнопки «**Зарегистрировать сервисы**». При этом, после их регистрации, будет предложен перезапуск сервисов LA (подробней о «Менеджере сервисов» см. главу 4).

3 Быстрый запуск

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

3.1 Установка сервера LanAgent

Производится путем запуска установочного файла **LanAgent Enterprise Server.exe**. При этом будет произведена как установка СУБД (системы управления базой данных), так и сервисов серверной части LanAgent.
Запуск установочного файла надо произвести от имени Администратора (вариант выпадающего меню по нажатию правой клавише мыши на исполняемом файле).

3.1.1 Установка СУБД (системы управления базой данных)

В качестве СУБД для **LanAgent** выбрана FireBird 2.5. Ее установочный файл уже включен в состав инсталляционного пакета «**LanAgent Enterprise Server.exe**» и отдельно устанавливать ее не требуется.

Достаточно запустить указанный ранее установочный файл и следовать инструкциям инсталлятора.

Если на компьютере, на который ставится серверная часть Enterprise, уже имеется Firebird, то инсталлятор LanAgent выдаст вам запрос на изменение файла конфигурации СУБД.

Давать согласие на это имеет смысл только в том случае, если кроме LanAgent нет других программ, которые используют Firebird. В противном случае, произведенные изменения могут повлиять на их работу.

3.1.2 WEB интерфейс: настройка порта и https соединения

При установке серверной части LanAgent Enterprise, производится также установка веб сервисов, позволяющих работать с программой через браузер.

Также, автоматически генерируется самоподписанный сертификат, который будет использоваться для https соединения. Если у вас уже имеется свой сертификат SSL, то его можно скопировать в каталог C:\Program Files (x86)\LanAgent Enterprise\nginx\conf\certs и использовать взамен самоподписанного.

Чтобы воспользоваться веб интерфейсом, запустите браузер и в строке адреса введите IP адрес компьютера с серверной частью LanAgent.

По умолчанию, устанавливается соединение по порту 443.

Браузер при этом сообщит о не доверенном соединении (в случае, когда используется наш сгенерированный сертификат). Чтобы этого избежать, надо **внести сертификат в хранилище корневых сертификатов Windows** на компьютере, на котором запущен браузер.

Сделать это можно двумя способами:

- **Вручную**. Для этого скопировать файл сертификата C:\Program Files (x86)\LanAgent Enterprise\lanagent-web\nginx\conf\certs\ce.cer на нужный компьютер, например в каталог C:\Certs\ и выполнить в командной строке CMD: **certutil -user -addstore "Root" "C:\Certs\ca.cer"**
- **Автоматически**. Для этого надо запустить приложение LanAgent Enterprise Viewer, открыть в нем диалог настройки пути до базы данных. Нажать кнопку "Запросить путь к базе у сервера". При этом, вьюер предложит установить сертификат SSL в хранилище корневых сертификатов Windows. Это сработает для браузеров: Chrome, Yandex, Edge, Opera и других, использующих хранилище сертификатов Windows. Для браузера Firefox добавить сертификат надо будет самостоятельно. Для этого можно ознакомиться со статьей https://support.mozilla.org/ru/kb/nastrojka-centrov-sertifikacii-ca-v-firefox

Если на компьютере с серверной частью LanAgent уже запущен другой веб сервис на портах 80 и 433, то его нужно либо отключить, либо перенастроить веб сервис LanAgent на другой порт.

Так, на компьютерах с Windows Server, по умолчанию активен IIS. Если он не используется, то его надо отключить.

Настроить порты можно в файле конфига C:\Program Files (x86)\LanAgent Enterprise\ nginx\conf\nginx.conf

В нем есть строки:

```
server {
    listen 80 default_server;
    listen [::]:80 default_server;
```

а также:

```
server {
    listen 433 ssl default_server;
    listen [::]:433 ssl default_server;
```

Пропишите тут нужные значения портов. Тогда при открытии веб интерфейса адрес будет содержать, не только IP, а еще и порт. Пример: https:\\192.168.5.25:47777

3.2 Установка модуля администратора LanAgent Admin

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

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

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

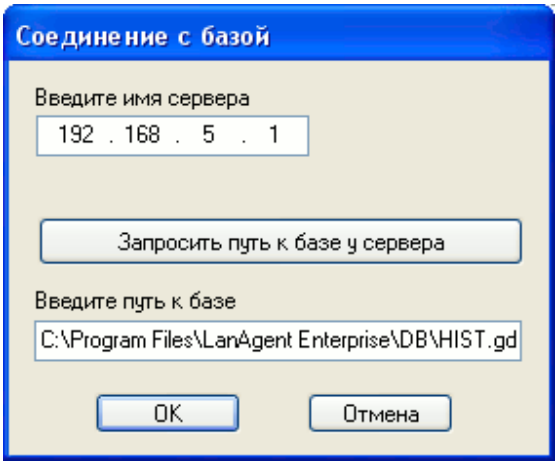


Рисунок 4 – Диалог соединения с базой

В этом диалоге требуется указать имя сервера, на котором установлена база, а также путь к файлу Hist.gdb. Сам путь можно получить от сервера LanAgent, нажав соответствующую кнопку (Запросить путь к базе у сервера). Если в ходе запроса пути к базе было выдано сообщение о невозможности подключения к серверу, то необходимо убедиться, что на сервере запущен сервис обмена LanAgent и обмен с сервером не блокируется фаерволом. Для этого нужны открытые порты 3050 и 6587.
Внимание! Не надо открывать общего доступа к указанному файлу базы данных, путь указывается исключительно для сервера!

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

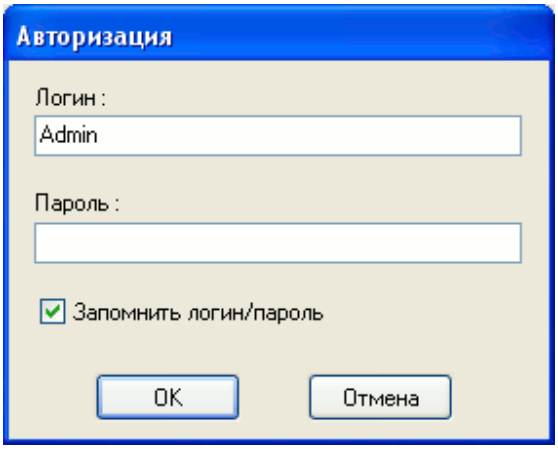


Рисунок 5 – Диалог авторизации

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

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

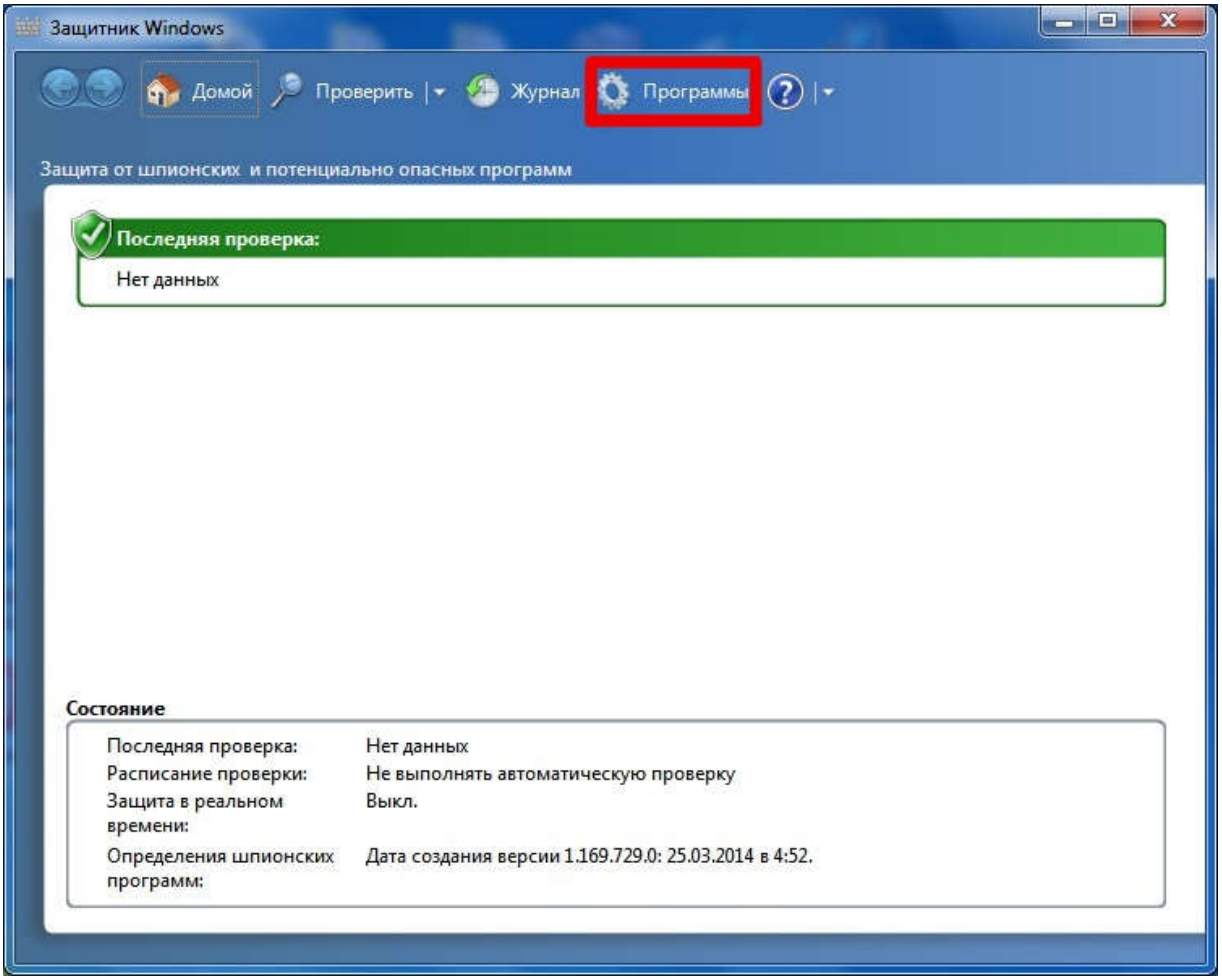
3.3 Настройка антивирусов

3.3.1 Защитник Windows

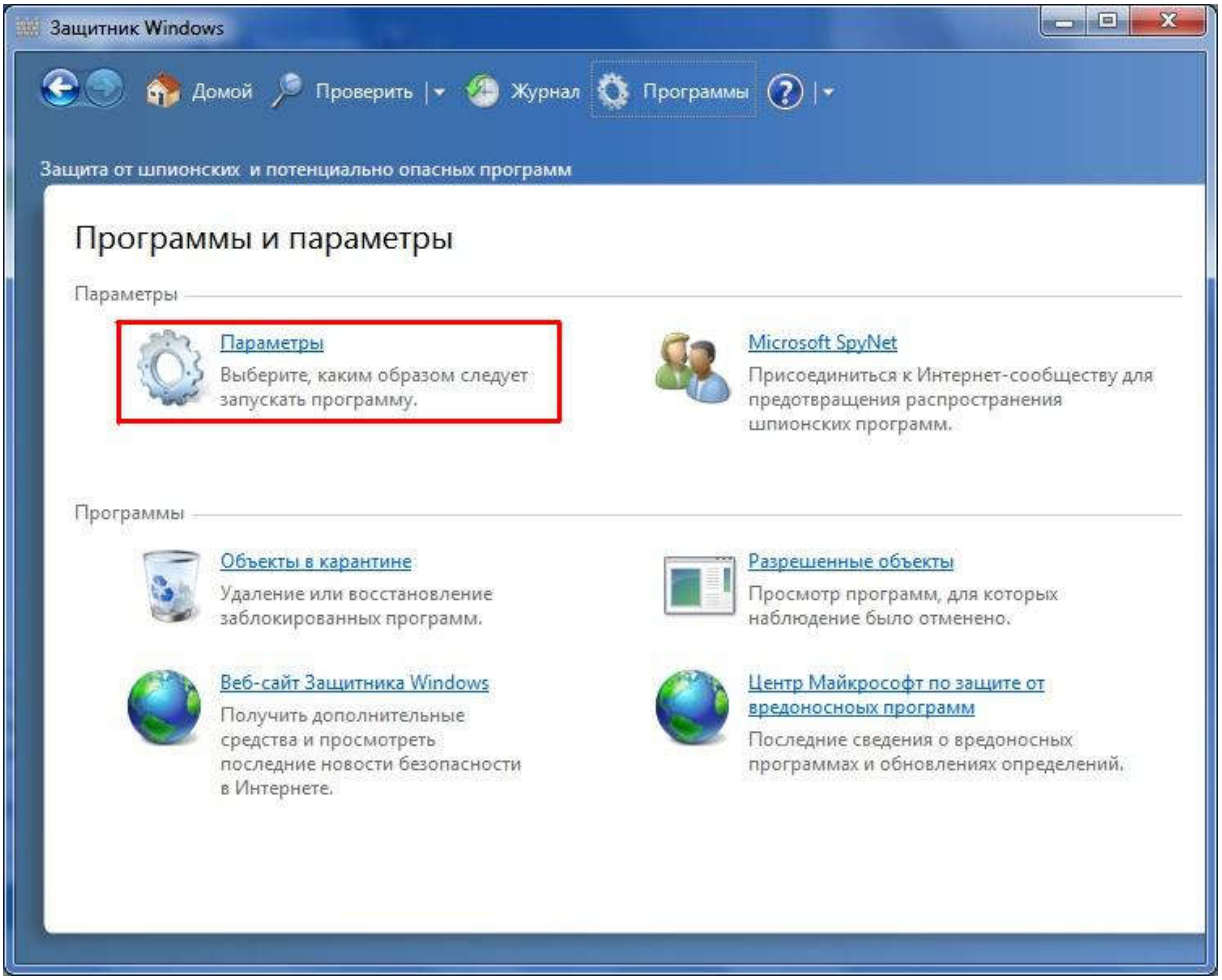
На компьютерах с операционной системой Windows 7/8 по умолчанию включен Защитник windows, это встроенный антивирус от Майкрософт. Не путайте его, пожалуйста, с брандмауером, это разные программы. Для корректной работы агента, желательно внести в настройках «Защитника» исключение на каталог установки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

Локальная настройка

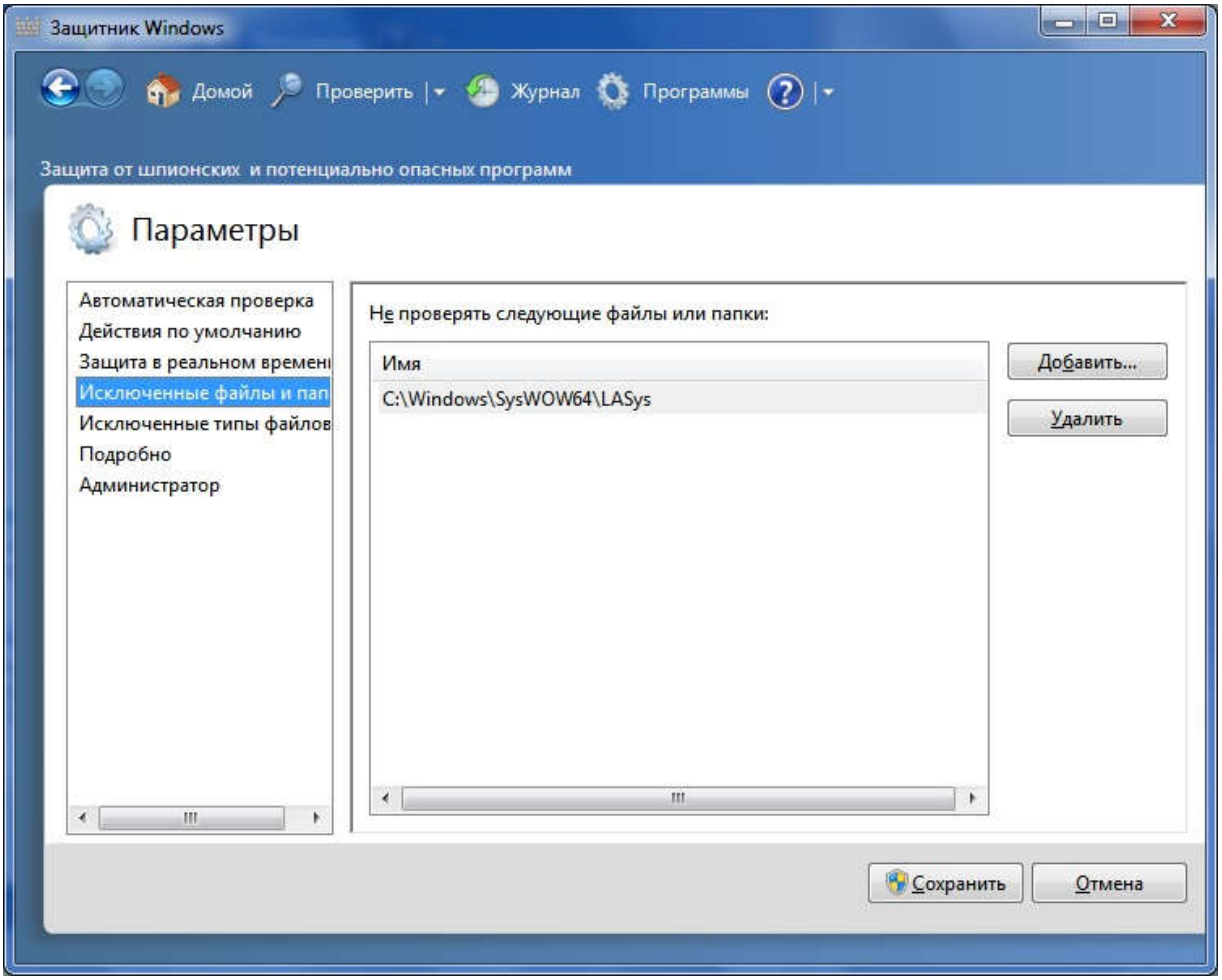
Для локальной настройки, выполните Пуск – в строке поиска программ наберите Защитник – выберите программу «Защитник Windows» из предложенного списка.



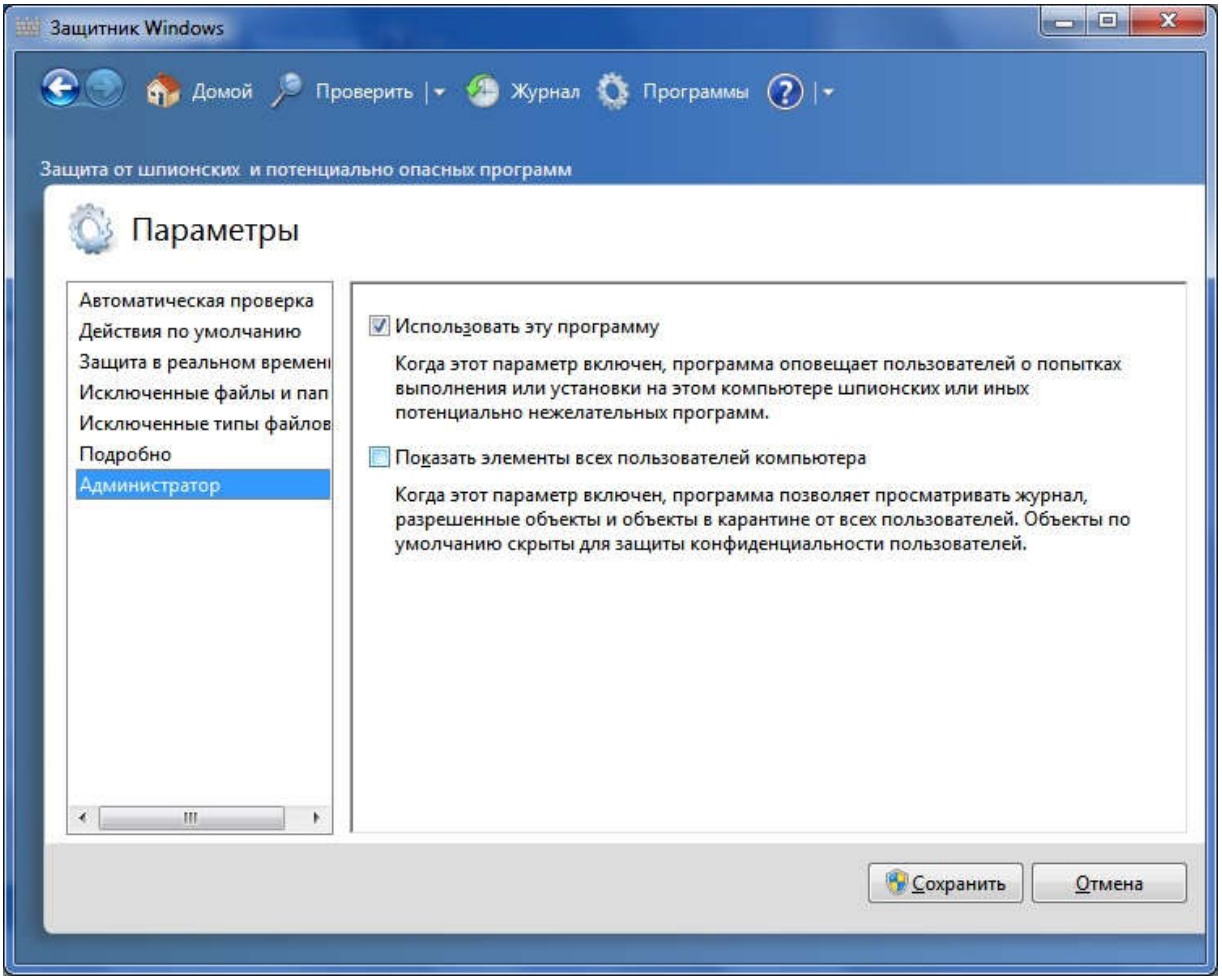
В открывшемся приложении нажмите кнопку «Программы» в верхнем меню. Далее, нажмите кнопку Параметры.



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

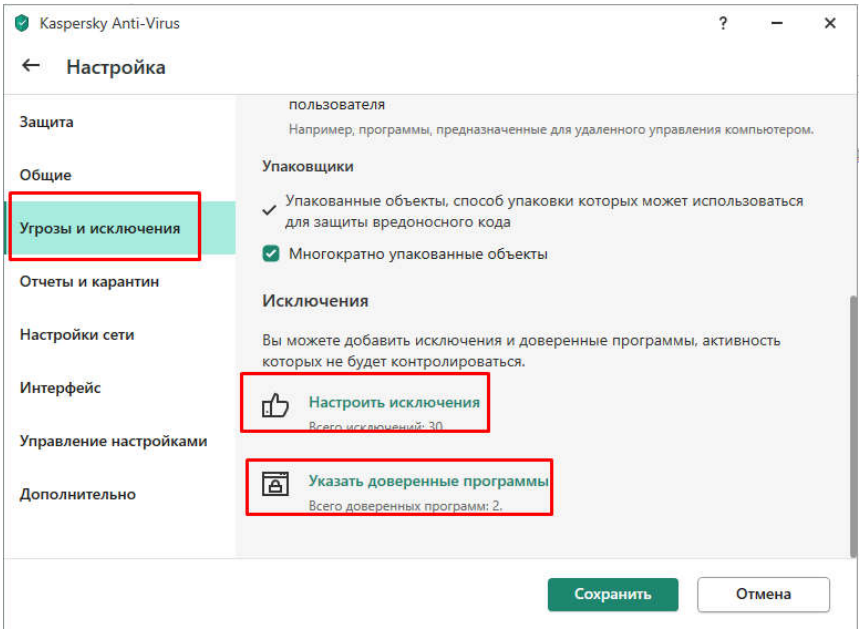
3.3.2 Антивирус Касперского

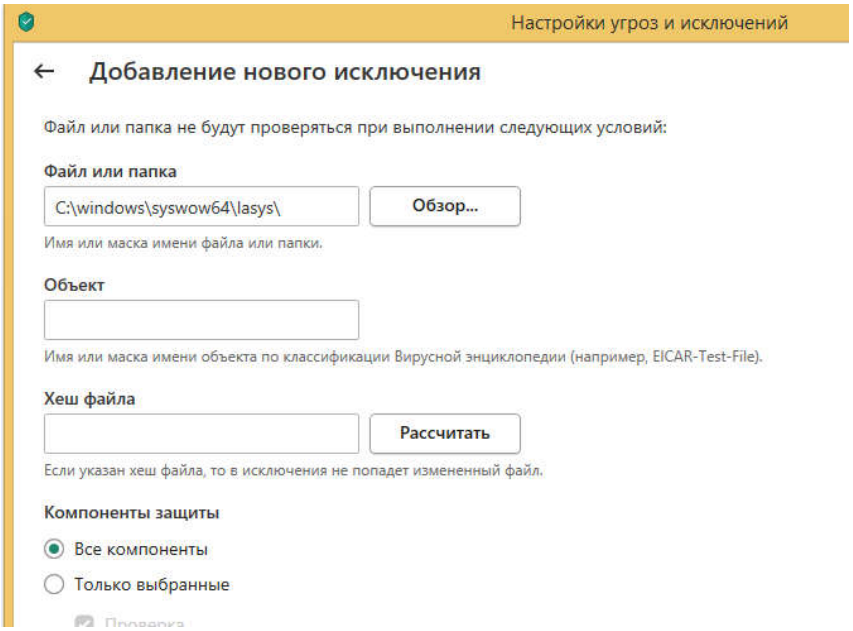
Для успешной дистанционной установки агента средствами программы LA Admin, желательно на целевом компьютере внести в исключение путь до файла инсталляции агента C:\windows\installservice.exe и Admin$\installservice.exe Это один и тот же путь.

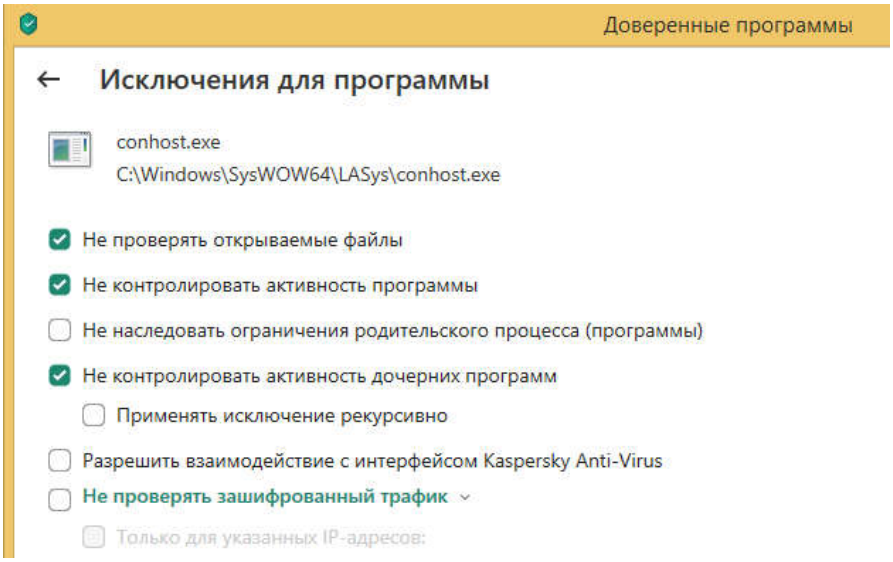
Все процессы следящего модуля имеют цифровую подпись и антивирусом не детектируются. Тем не менее, желательно внести в исключение антивируса либо сам каталог установки агента C:\windows\system32\lasys для 32 битных систем и syswow64\lasys для 64 битных, либо конкретные файлы system.exe, conhost.exe,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

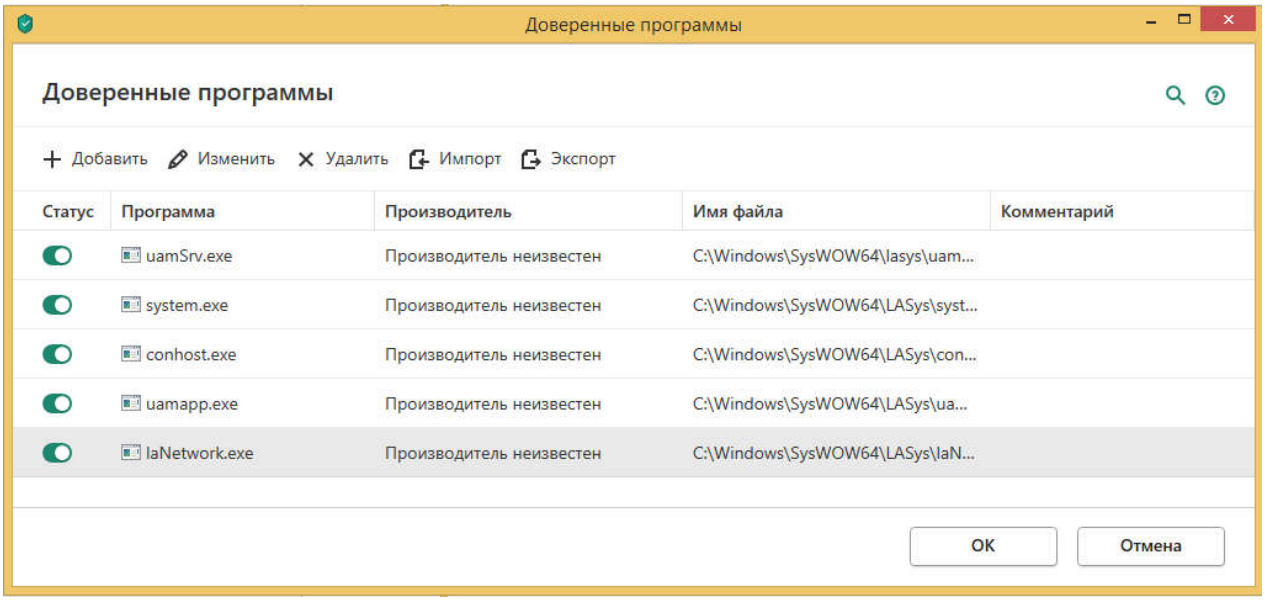
Это позволит избежать «сюрпризов» в виде ложных срабатываний антивируса в будущем.

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.




Настройки угроз и исключений
Добавление нового исключения
Файл или папка не будут проверяться при выполнении следующих условий:
Файл или папка
C:\windows\syswow64\lasys\
Обзор...
Имя или маска имени файла или папки.
Объект
Имя или маска имени объекта по классификации Вирусной энциклопедии (например, EICAR-Test-File).
Хеш файла
Рассчитать
Если указан хеш файла, то в исключения не попадет измененный файл.
Компоненты защиты
Все компоненты
Только выбранные


Доверенные программы
Исключения для программы
conhost.exe
C:\Windows\SysWOW64\LASys\conhost.exe
Не проверять открываемые файлы
Не контролировать активность программы
Не наследовать ограничения родительского процесса (программы)
Не контролировать активность дочерних программ
Применять исключение рекурсивно
Разрешить взаимодействие с интерфейсом Kaspersky Anti-Virus
Не проверять зашифрованный трафик
Только для указанных IP-адресов:



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

3.3.3 Антивирус НОД32

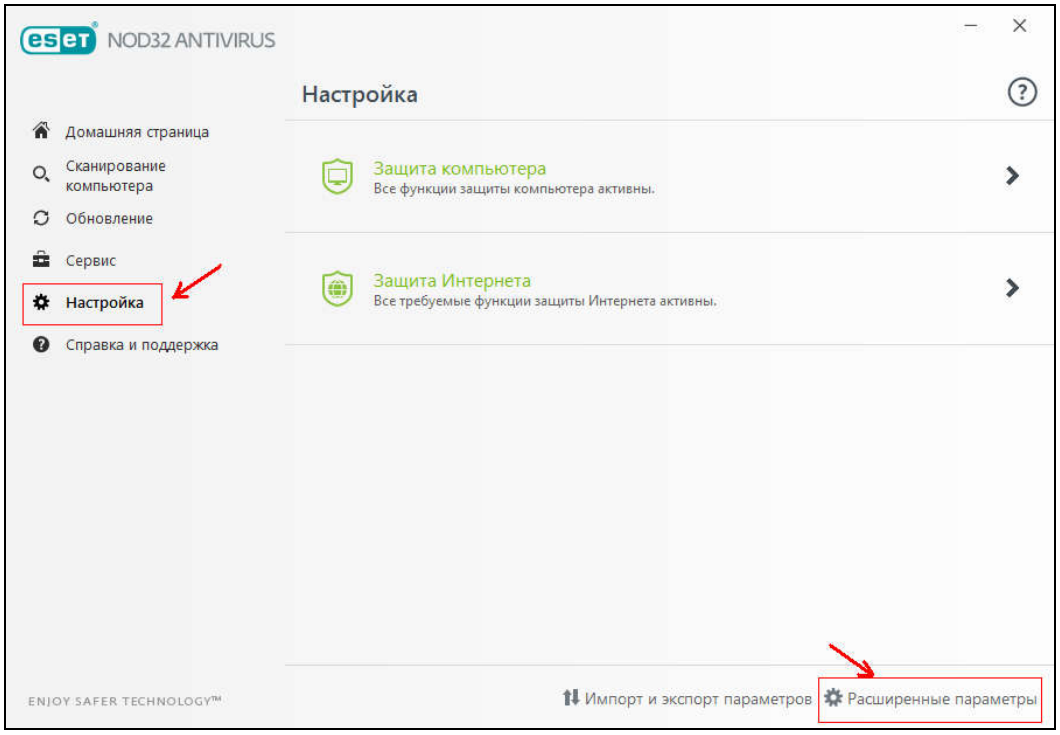
Принцип внесения исключений в НОД32 тот же, что и во все остальные антивирусы: для успешной дистанционной установки агента средствами программы LA Admin, желательно на целевом компьютере внести в исключение путь до файла инсталляции агента C:\windows\installservice.exe .

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.

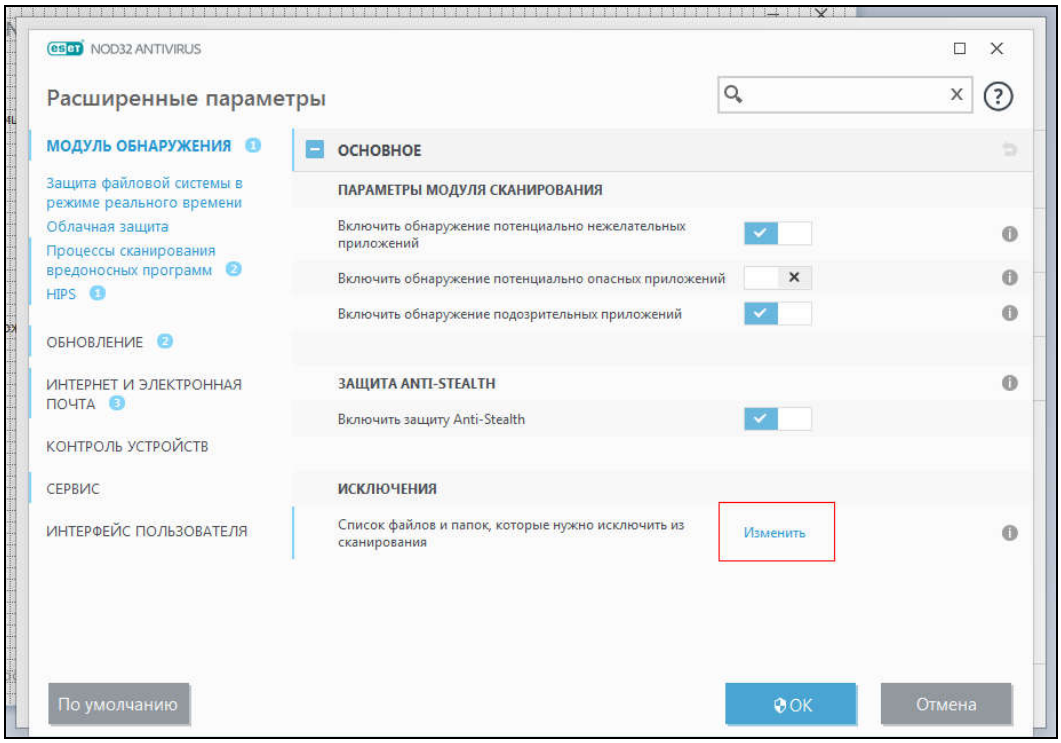
Все процессы следящего модуля имеют цифровую подпись и антивирусом не детектируются. Тем не менее, желательно внести в исключение антивируса либо сам каталог установки агента с файлами по маске: C:\windows\system32\lasys*.* для 32 битных систем и syswow64\lasys*.* для 64 битных, либо конкретные файлы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

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

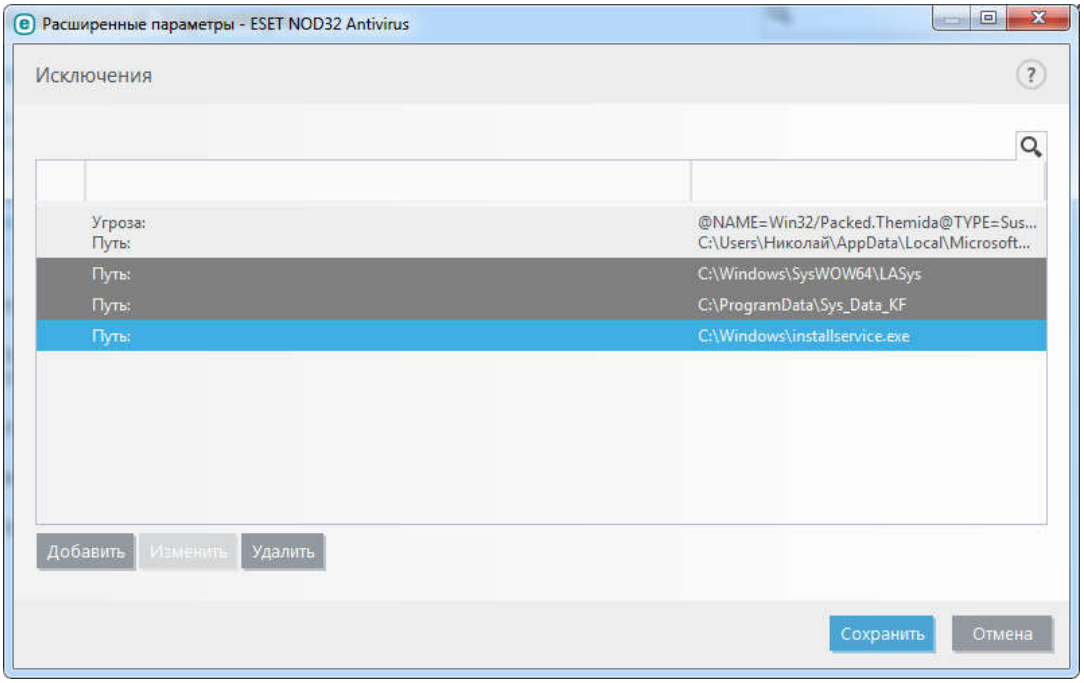
И для NOD32 надо добавить в исключение каталог временных файлов агента C:\ProgramData\Sys_Data_KF*.*



На пункте Исключения нажмите «Изменить»



И укажите в списке нужные пути исключений.



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

3.3.4 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, conhost.exe, uamApp.exe, uamSrv.exe, sys.dll, laNetwork.exe из каталога установки агента.

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

3.4 Установка агентов

3.4.1 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.

3.4.2 Удаленная установка агентов

Для этого воспользуйтесь диалогом установки агентов, который вызывается в администраторской части LanAgent кнопкой "**Добавить**" (кнопка с плюсом).

Среди доступных вариантов есть сканирование диапазона IP адресов, получение списка компьютеров из Active Directory, работа со списком компьютеров (для установки и удаления следящего модуля на компьютеры, ранее внесенные в список мониторинга). Также есть вариант добавления «remote» пользователей – это для случая, когда следящий модуль настроен для передачи данных серверу через интернет.

Универсальный вариант – сканирование диапазона IP адресов. Он будет работать и в сети с доменом и с обычной рабочей группой.

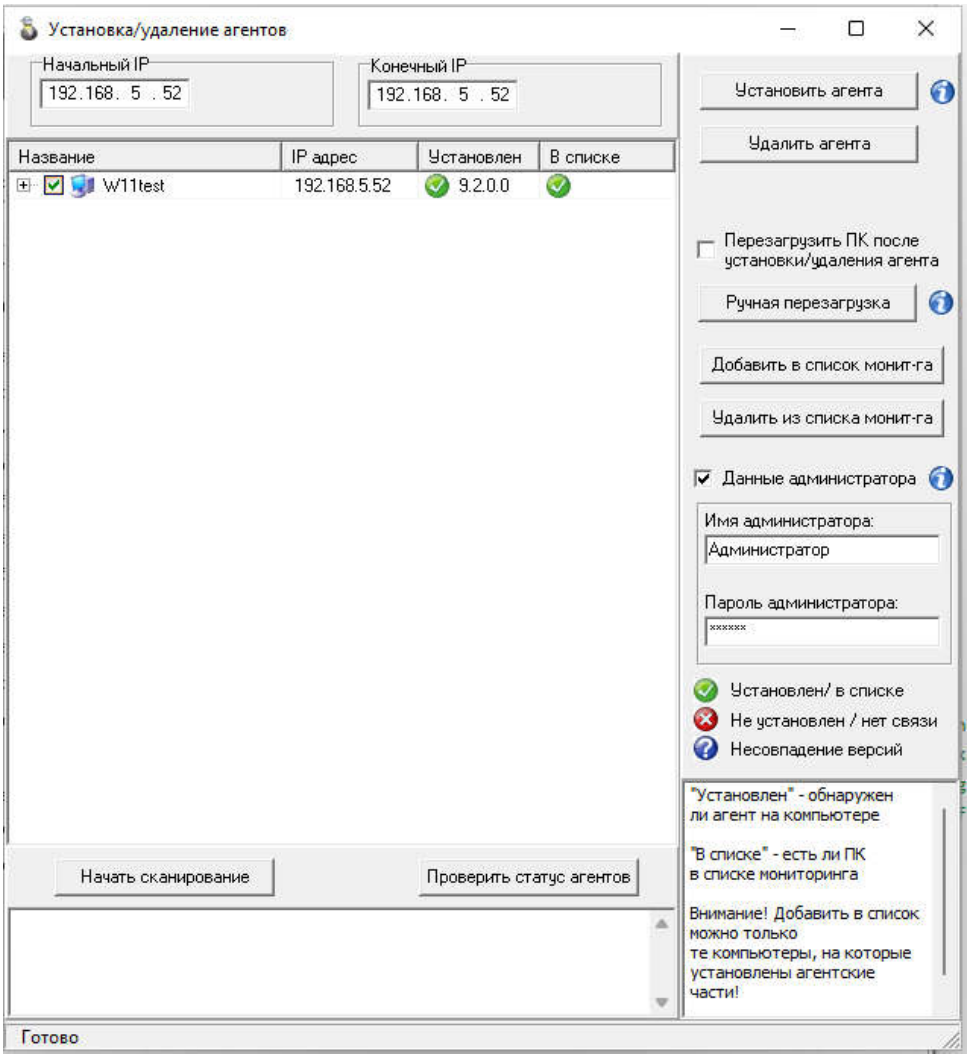
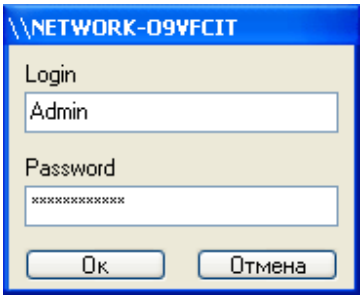


Рис 3.1 – Диалог установки/удаления агентов

После открытия окна, введите диапазон IP адресов, который надо просканировать и нажмите кнопку «Начать сканирование». При этом будет отображен список найденных компьютеров и наличие на них установленного следящего модуля. 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 систем, syswow64\lasys – для 64 битных. Рекомендуем внести его в исключение антивируса. 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.

3.4.3 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.

На ОС Win 7/8/8.1/10/11 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) -> Центр управления сетями и общим доступом (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 lanagent.ru/localsp.reg

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 его в исключение антивируса. В пункте 3.3 данного руководства есть более подробная информация по настройкам антивирусов.

3.4.4 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

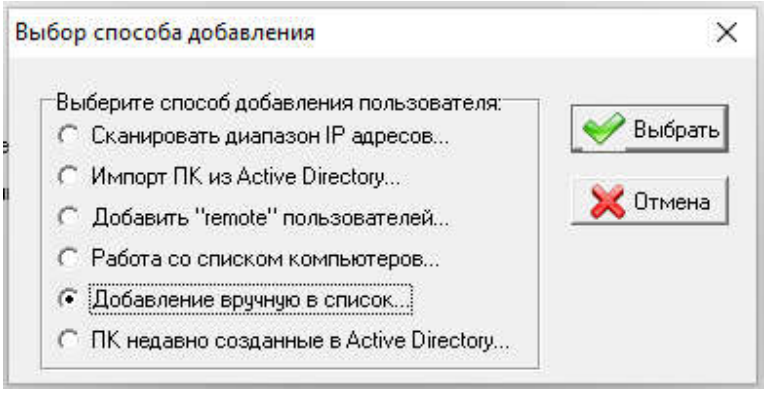
базе знаний Microsoft:

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/)

3.5 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:

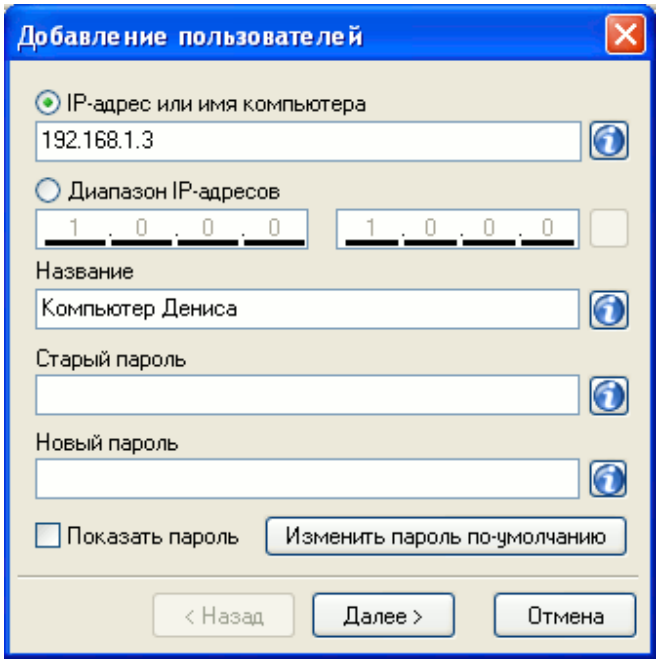


Рис. 3.2 - Добавление компьютера в список мониторинга

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:

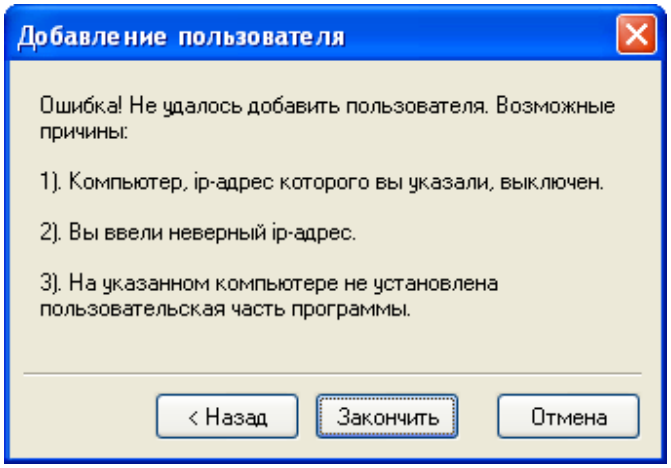


Рис. 3.3 – Ошибка добавления в список

Чтобы изменить параметры подключения, нажмите кнопку "Назад".

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

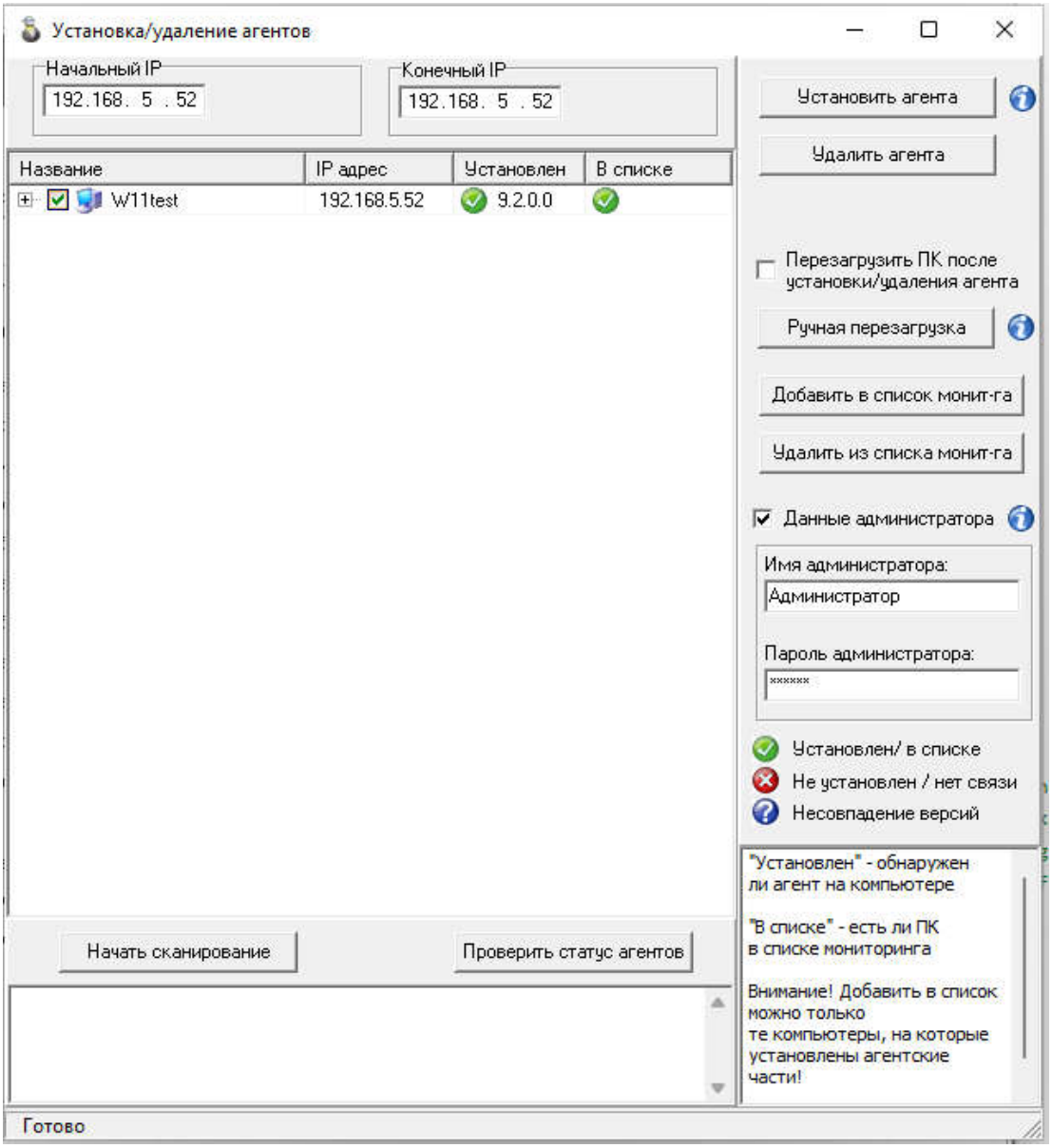
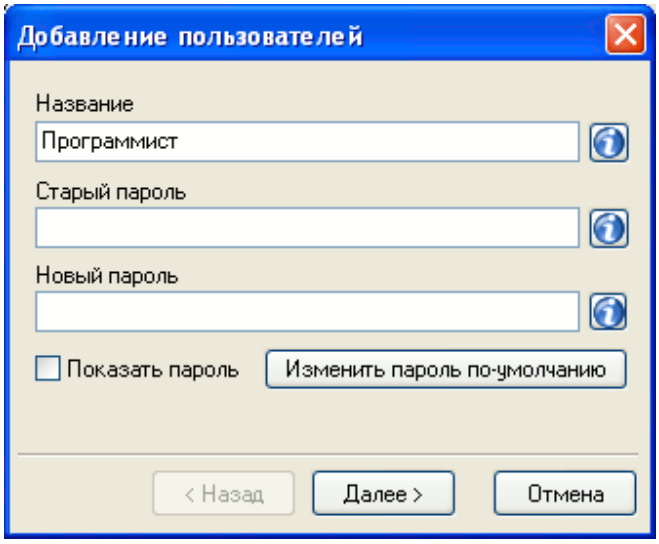


Рис. 3.4 – Диалог установки/удаления агентов

После открытия окна, введите диапазон IP адресов, который надо просканировать и нажмите кнопку «Начать сканирование». При этом будет отображен список найденных компьютеров и наличие на них установленного следящего модуля. 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:

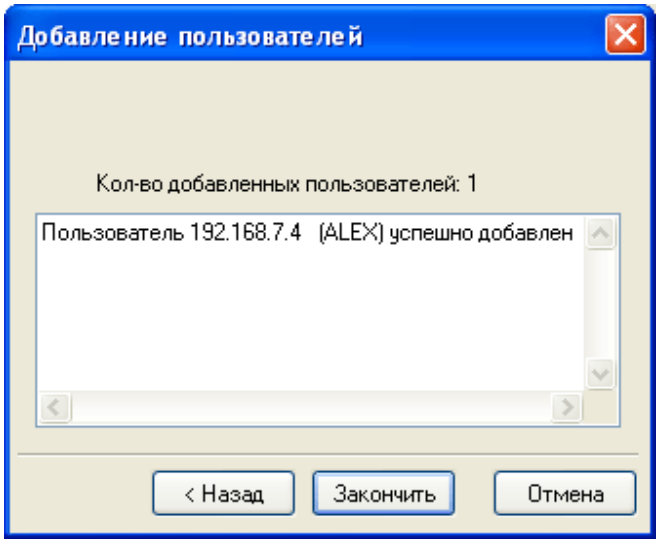


Если в предыдущем окне был выбран только один компьютер для добавления в список, то поле "Название" будет доступно для заполнения. Его содержимое в дальнейшем будет отображаться в списке мониторинга. Поэтому заполните его **понятным вам** названием. В случае добавления сразу нескольких компьютеров, данное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

3.6 Создание групп пользователей

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

При этом откроется следующее диалоговое окно:

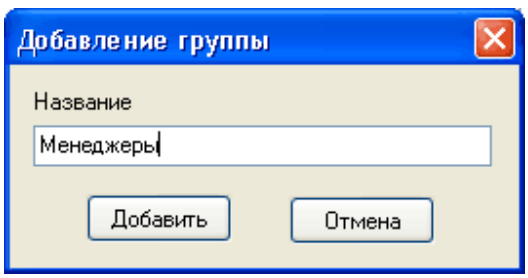
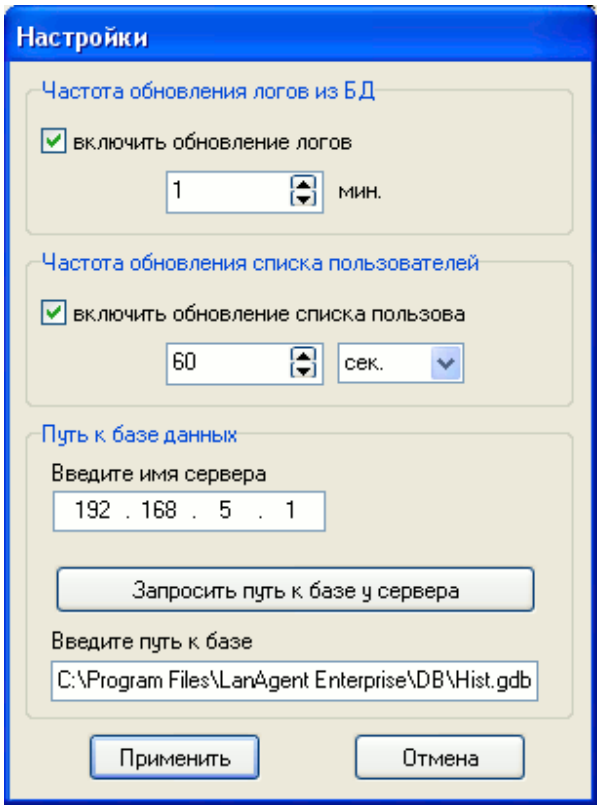


Рис. 3.5 – Добавление группы пользователей

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

3.7 Установка LanAgent View

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



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

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

На компьютере с LA Viewer должны быть открыты порты 3050 и 6587 tcp/ip.

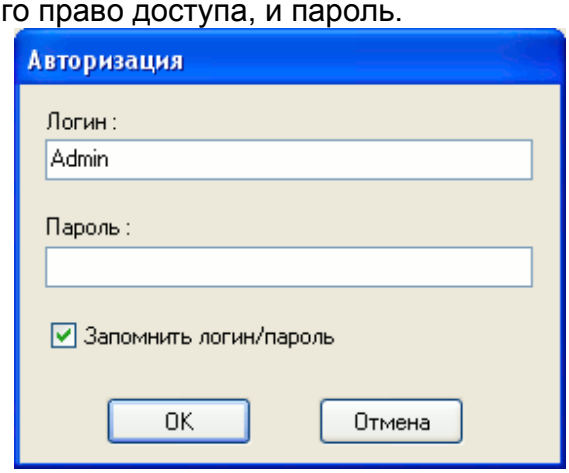
Кроме приложения LA Viewer, можно также использовать веб интерфейс (в нем реализованы все функции, имеющиеся во вьюере). Запустить его можно открыв браузер и набрав в нем в строке адреса IP адрес сервера.

Другой вариант – при запуске приложения вьюера будет предложено запустить веб интерфейс. При положительном ответе, вьюер откроет браузер на нужной странице.

По умолчанию, веб сервер LanAgent использует самоподписанный сертификат для https соединения. Чтобы сообщение о не доверенном соединении не появлялось каждый раз в браузере, можно внести этот сертификат в список доверенных на компьютере.

При запросе пути до базы данных во вьюере, также, появится диалог с предложением установить сертификат в хранилище доверенных. Чтобы это сделать, нажмите Да в диалоге и потом подтвердите разрешение в сообщении от Windows.

После установки пути до базы данных, программа попросит ввести имя пользователя, имеющего право доступа, и пароль.



В зависимости от прав доступа, для пользователя будут доступны соответствующие категории информации. Администратор имеет полный доступ. (подробнее о правах доступа, их назначении и изменении смотрите в пункте 5.4 – «Закладка Контроль»)

Начиная с 9-ой версии LanAgent Enterprise, основным интерфейсом просмотра данных стал web интерфейс (работа через браузер). Для его открытия достаточно в браузере открыть страницу, указав в качестве адреса IP адрес компьютера с серверной частью.

4 Работа с LanAgent Server

Для управления сервисами **LanAgent Enterprise** предусмотрена специальная утилита – Менеджер сервисов (**LanAgent Enterprise ServiceControl**):

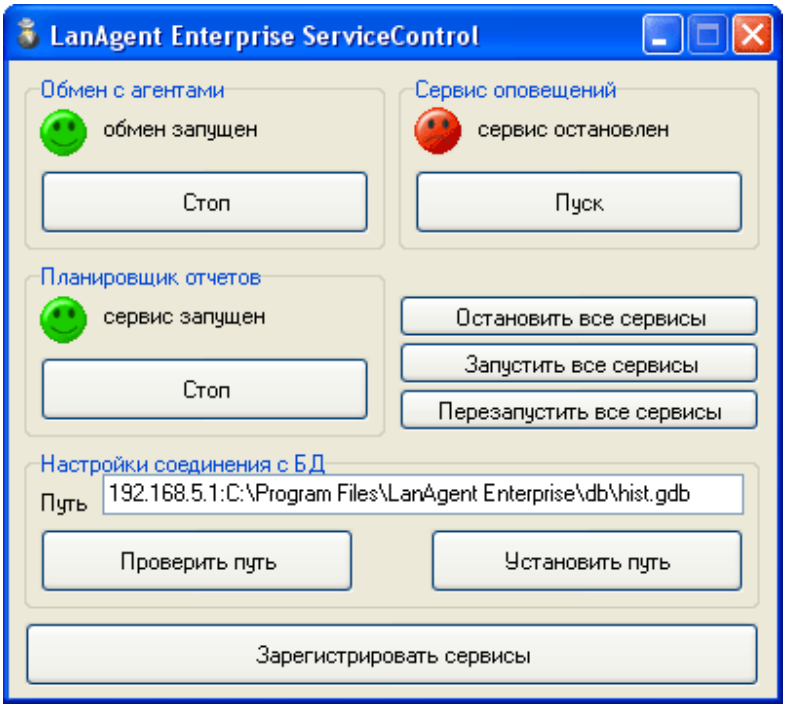


Рисунок 4.1 – Менеджер сервисов

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

4.1 Если не запускается сервис обмена с агентами

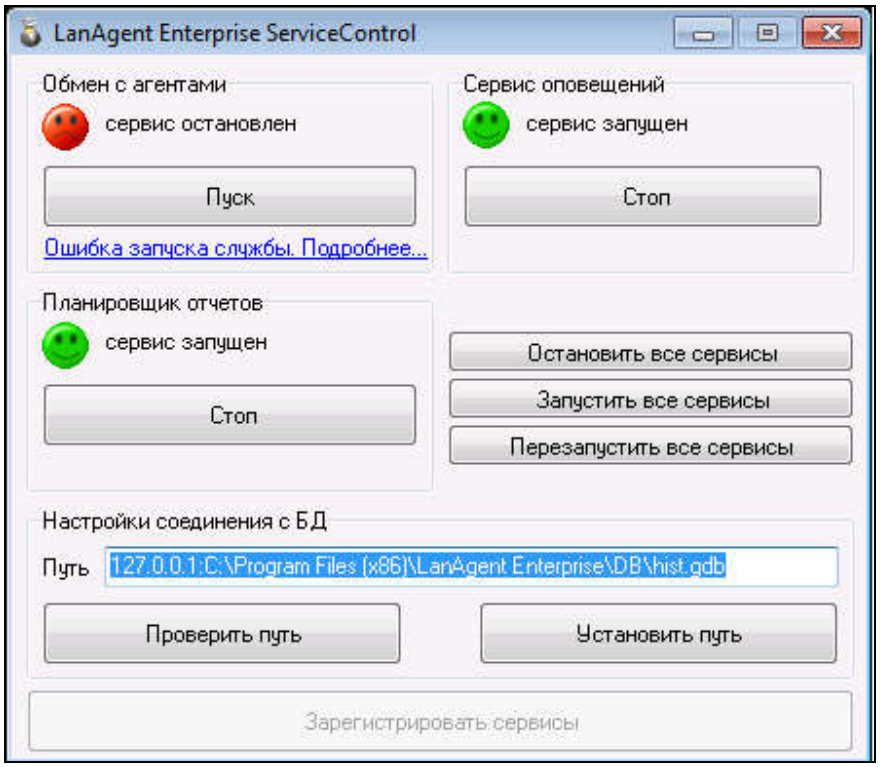
Причин, по которым не запускается сервис обмена с агентами, может быть несколько:

1). Если изменился состав оборудования на серверном ПК. Это может быть, например, изменение объема оперативной памяти или изменение состава жестких дисков.

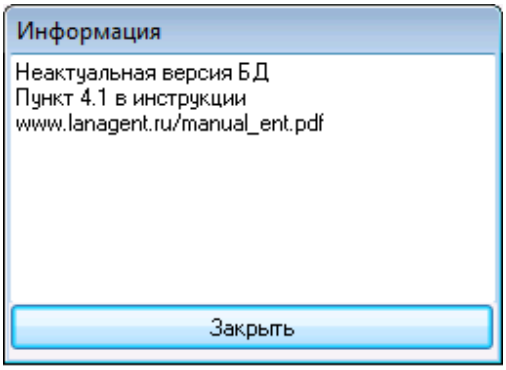
Если сервер LanAgent установлен на виртуальной машине с динамическим увеличением размера жесткого диска, то это также будет приводить к «слетанию» активации. Чтобы этого избежать – задайте фиксированный размер жесткого диска виртуалки.

Решением данной ситуации будет переактивации программы. Подробнее в пункте 2 данного руководства.

2). Когда сервис обмена с агентами не запускается сразу после обновления версии LanAgent с версии 6.2 или более ранней чем 6.2. Либо при переключении на другую копию базы данных.



В этом случае сразу под статус службы будет ссылка на подробности об ошибке.



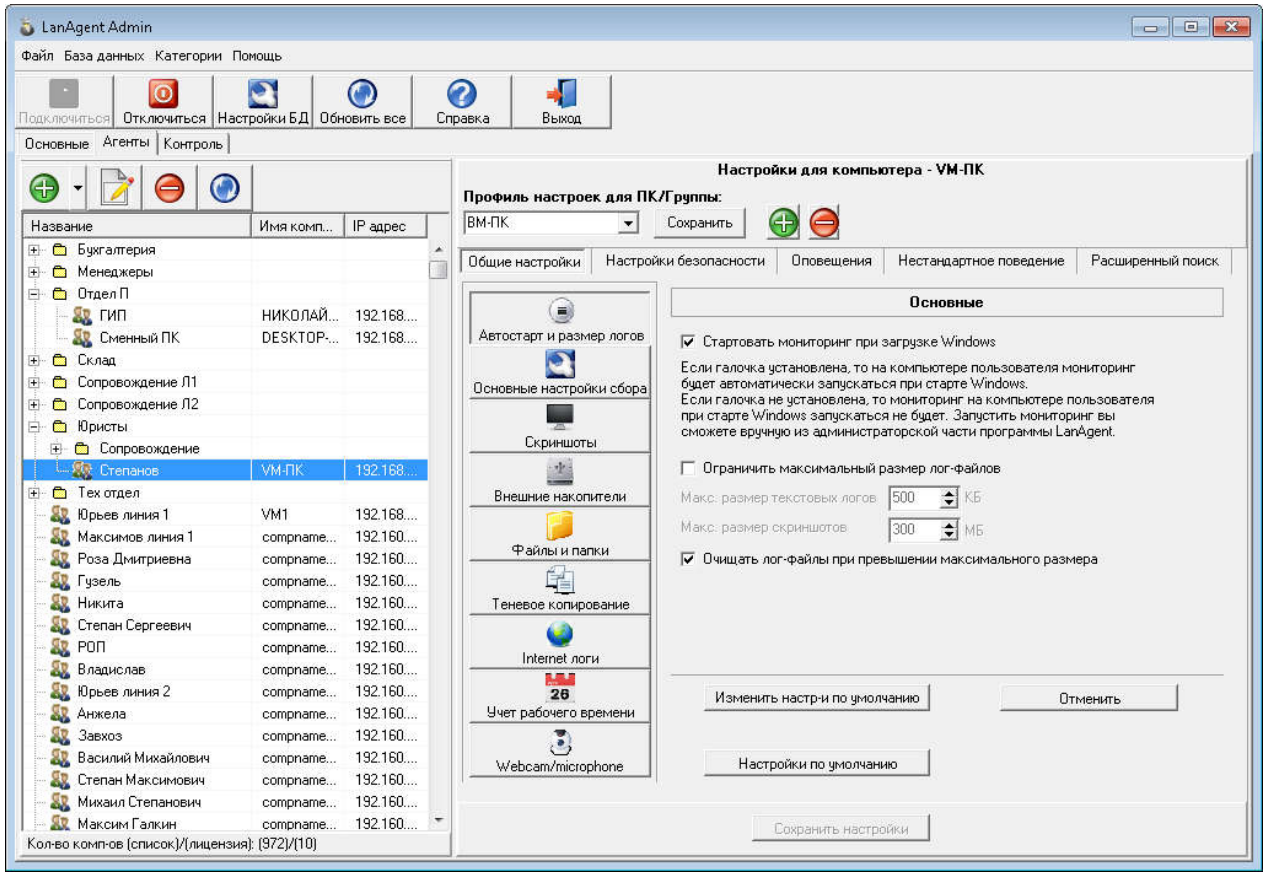
Начиная с версии 6.3, в LanAgent Enterprise использует Firebird 2.5. Более ранние версии использовали Firebird 1.5.

Специальная утилита апдейта базы данных до нужной версии Firebird расположена в каталоге установки сервер LanAgent. Папка DbMigration.

В процессе инсталляции сервера апдейт базы с более ранних версий должен произойти автоматически. Тем не менее, если в его процессе произошли ошибки, либо если уже после установки сервера была выбрана другая база данных, то процесс апдейта можно сделать вручную.

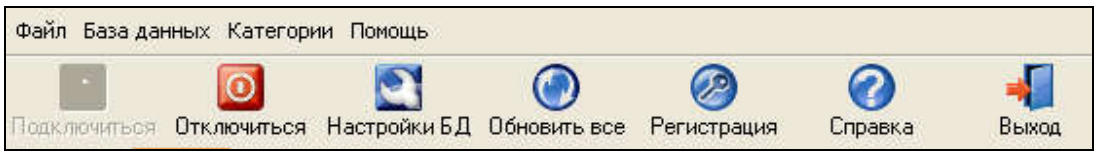
Для этого в LanAgent ServiceControl задайте путь до нужного файла базы данных. Остановите все сервисы LanAgent. Убедитесь, что на сервере установлен Firebird версии 2.5. И запустите с правами администратора консоль UpdateFireBird.exe. Это удобнее сделать через командную строку cmd, чтобы видеть результат выполнения утилиты. При возникновении ошибок будет создан файл error.log.

5 Работа с LanAgent Admin

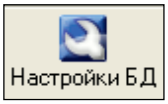


Как видно из рисунка, программа состоит из трех закладок («**Основные**», «**Агенты**», «**Контроль**»), на которых расположены соответствующие настройки и панели инструментов.

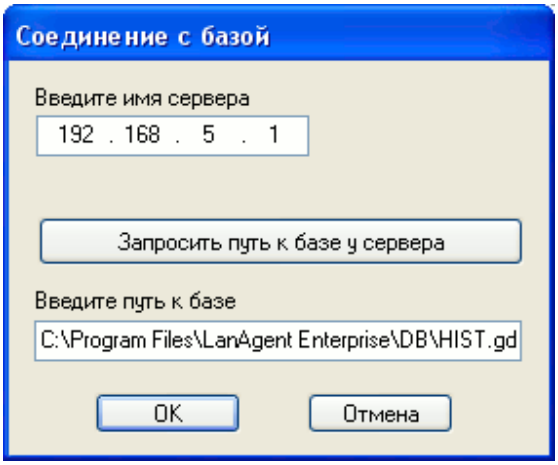
5.1 Панель инструментов



Назначение кнопок панели инструментов:



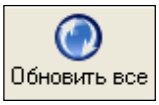
– вызывает диалог настройки подключения к базе данных:



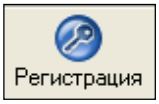
В этом диалоге требуется указать имя сервера, на котором установлена база, а также путь к файлу HIST.gdb
Внимание! Не надо открывать общего доступа к указанному файлу, путь указывается исключительно для сервера!

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

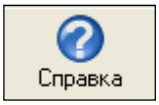
– отсоединяет **LanAgent Admin** от базы данных.



– производит обновление всех списков.



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



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

– закрывает программу.

Названные выше действия также продублированы в выпадающем меню.

5.2 Закладка «Основные»

Содержит системные и общесистемные настройки.

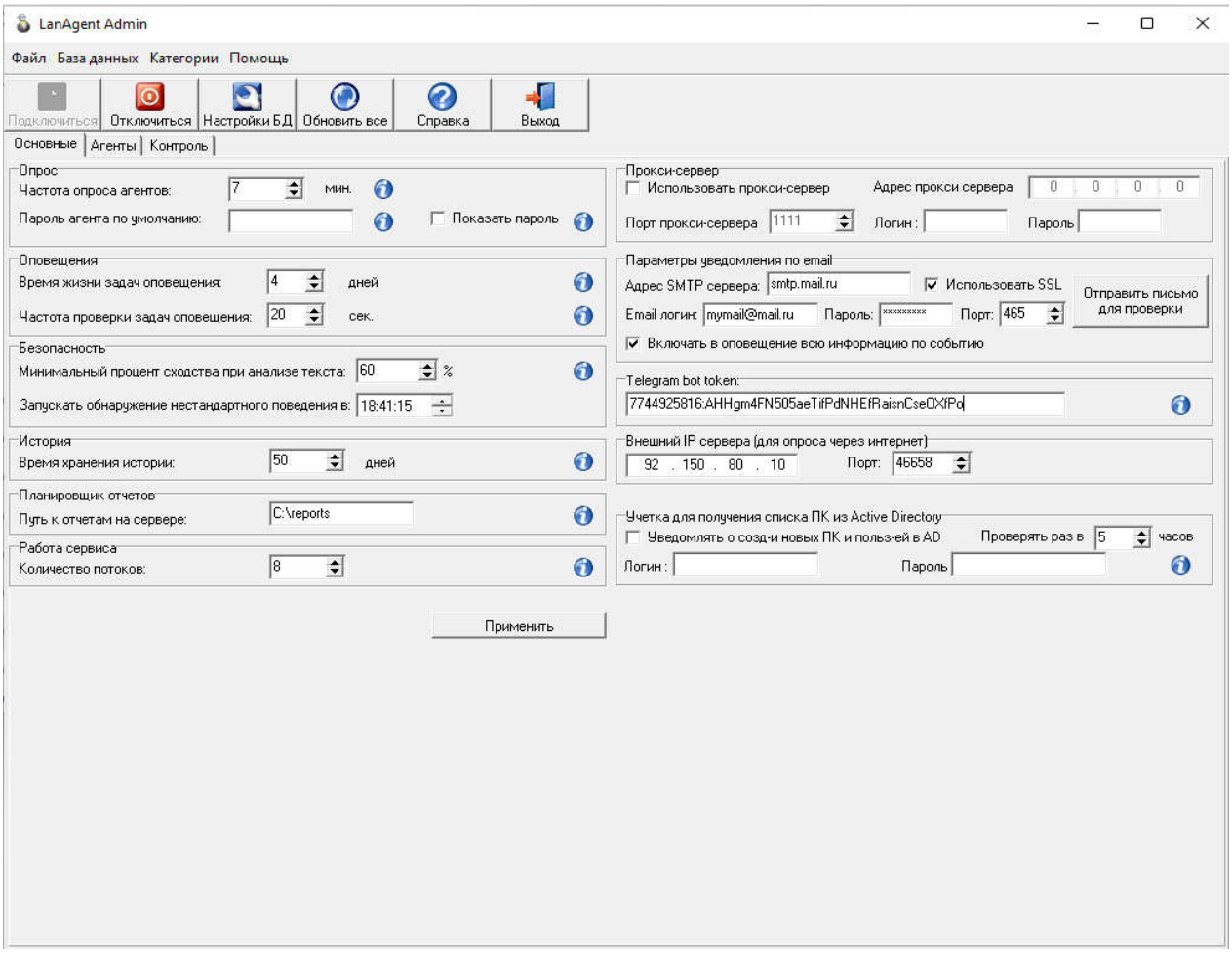


Рисунок 5.1 – Закладка «Основные» LanAgent Admin

Опрос:

Частота опроса агентов – задается периодичность, с который производится опрос агентов серверной частью.
Пароль агента по-умолчанию – здесь можно задать пароль для агента, который будет использоваться по-умолчанию в диалоге добавления агентов в список мониторинга.
Показать пароль – установите данную галочку, если хотите чтобы пароль отображался. В противном случае он будет выводиться на экран в виде ****

Оповещения:

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

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

Безопасность:

Минимальный процент сходства при анализе текста – определяет минимальный процент совпадения анализируемого текста и эталонных фраз (задаваемых при определений правил безопасности), при котором считается, что анализируемый текст содержит в себе такую фразу.

История:

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

Работа сервиса:

Количество потоков – определяет количество потоков обмена с агентами. Чем больше потоков, тем быстрее производится обновление статуса компьютеров и сбор логов, но тем больше ресурсов требуется от компьютера, на котором установлена серверная часть программы.

Прокси-сервер:

Использовать прокси-сервер – если на сервере (на компьютере, на котором установлена серверная часть LanAgent) нет прямого выхода в интернет, то для работы сервиса оповещений (для пересылки оповещений о нарушениях правил безопасности на e-mail), а также для отправки сформированных отчетов (сервисом отчетов) на e-mail, необходимо поставить данную галочку и прописать параметры прокси сервера: IP адрес, порт, логин и пароль. В том случае, если логин и пароль для выхода через прокси сервер не требуется, оставьте данные поля пустыми.

Параметры уведомления по email:

Указанные в данном разделе параметры почтовой учетки будут использоваться для отправки уведомлений о нарушениях политик безопасности, а также для отправки писем планировщиком отчетов (от имени этой учетной записи почты будет происходить рассылка). Они заполняются точно также, как в почтовом клиенте.

Внешний IP сервера (для опроса через интернет):

В том случае, когда опрос контролируемых компьютеров надо производить через Интернет (они находятся не в локальной сети), необходимо указать внешний «белый» IP адрес сервера. Клиенты будут использовать его для подключения. Если

в основной сети выход в интернет через роутер, то на нем надо пробросить порт 46658 tcp/ip.

Telegram bot token:

LanAgent позволяет использовать Telegram для отправки уведомлений о нарушениях, а также для отправки кода 2-х факторной авторизации. Для этого необходимо создать Telegram бота (подробная инструкция по его созданию – в разделе 5.12). В данное поле необходимо вставить значение токена созданного бота.

5.3 Закладка «Агенты»

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

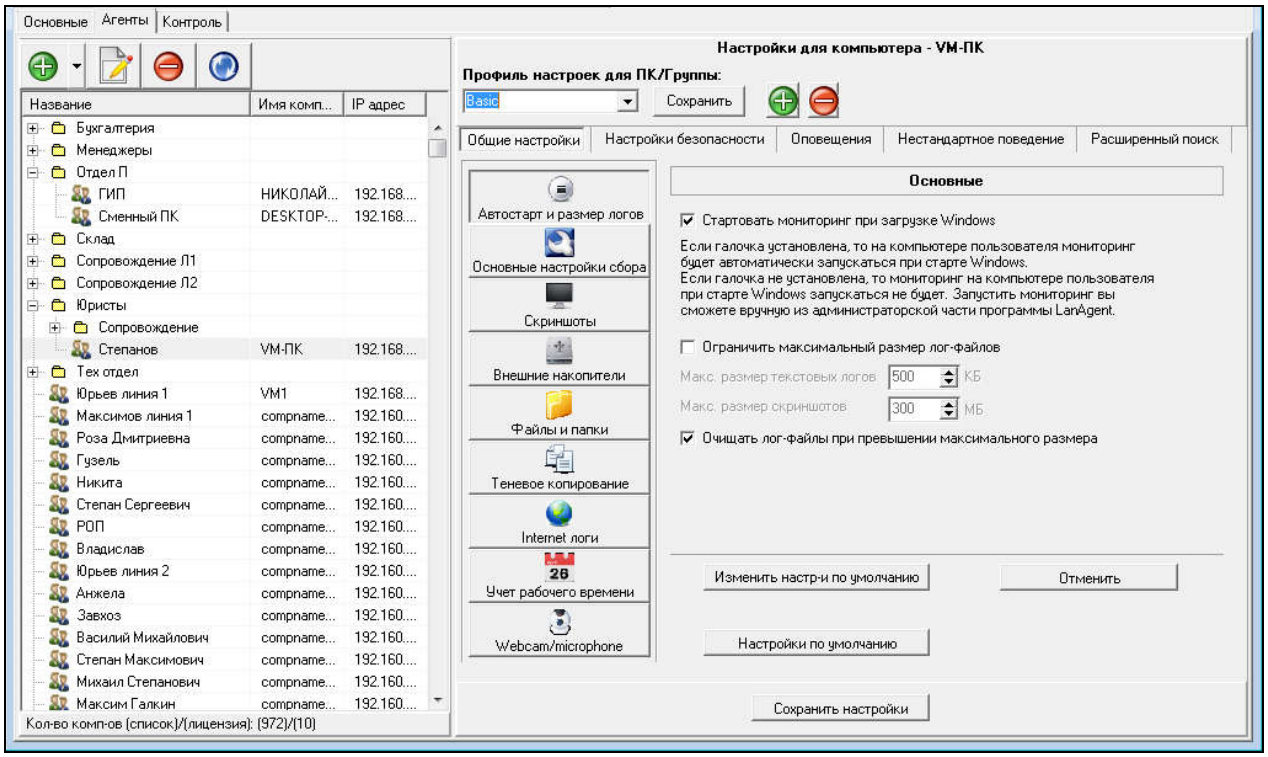
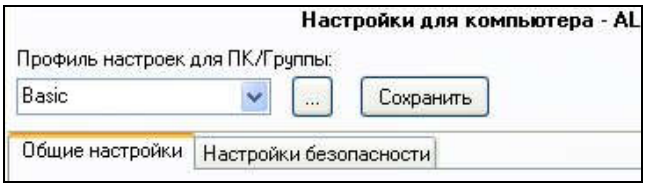


Рисунок 5.2 – Закладка «Агенты» LanAgent Admin

В левой части окна расположен список мониторинга.
Для добавления нового компьютера или группы в список, необходимо нажать кнопку  Процесс добавления компьютеров подробно описан в пункте 3.4

Начиная с версии 5.3, все настройки (кроме настроек Web камер) задаются для профиля. Имя связанного с компьютером профиля отображается над вкладками

настроек. При необходимости сменить его – выберите нужный из списка (или создайте новый) и нажмите кнопку «**Сохранить**» справа от имени профиля.



Соответственно, при сохранении, настройки будут применены для всех компьютеров, связанных с редактируемым профилем.

5.3.1 Общие настройки

Настройки агента в целом, состоят из следующих видов настроек: Общие настройки, Настройки безопасности, Оповещения и Нестандартное поведение.
Настройка агентов программы LanAgent производится удаленно из административной части программы. Для этого достаточно выбрать двойным кликом нужный компьютер из списка для мониторинга. При этом откроются настройки связанного с ним профиля.

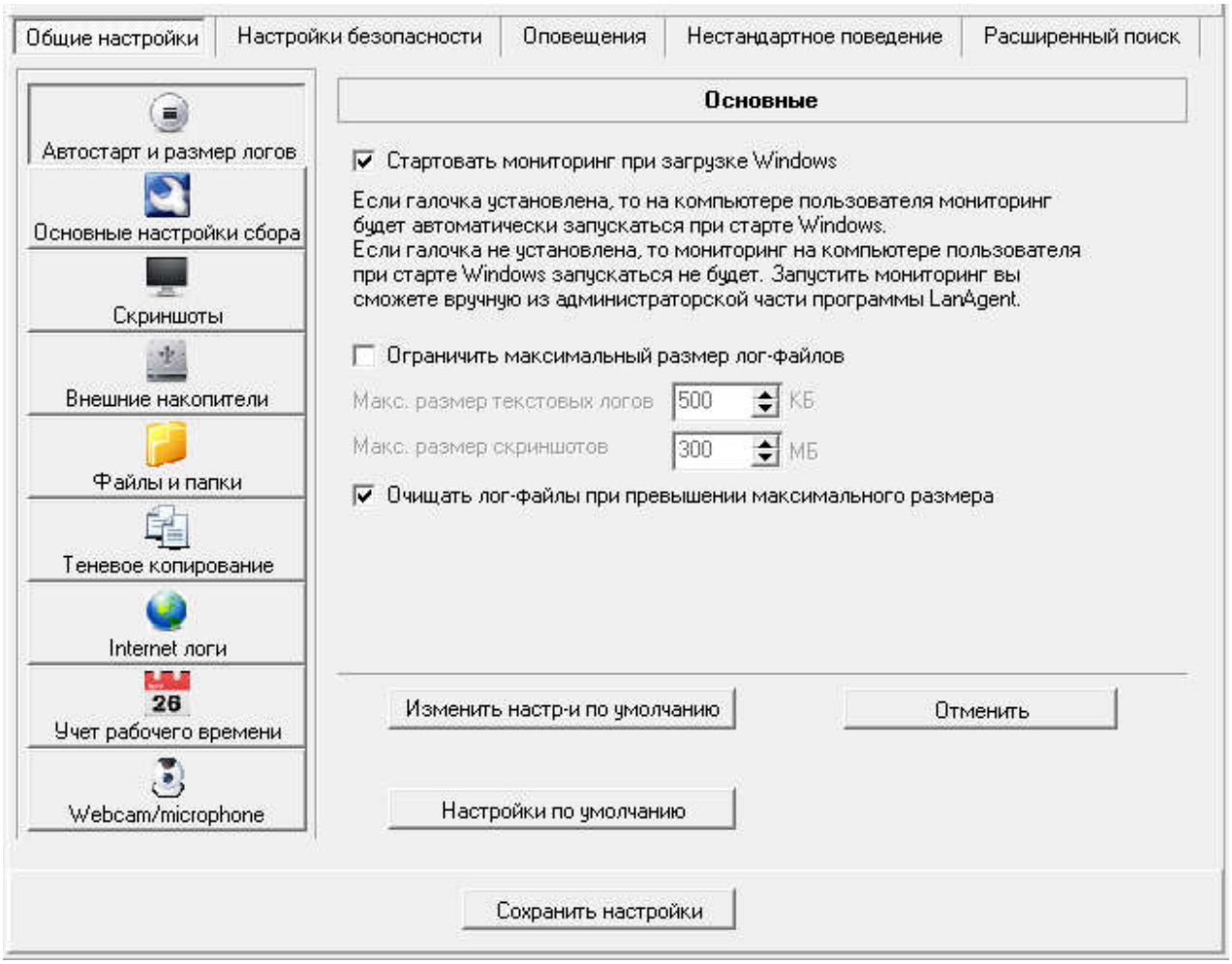


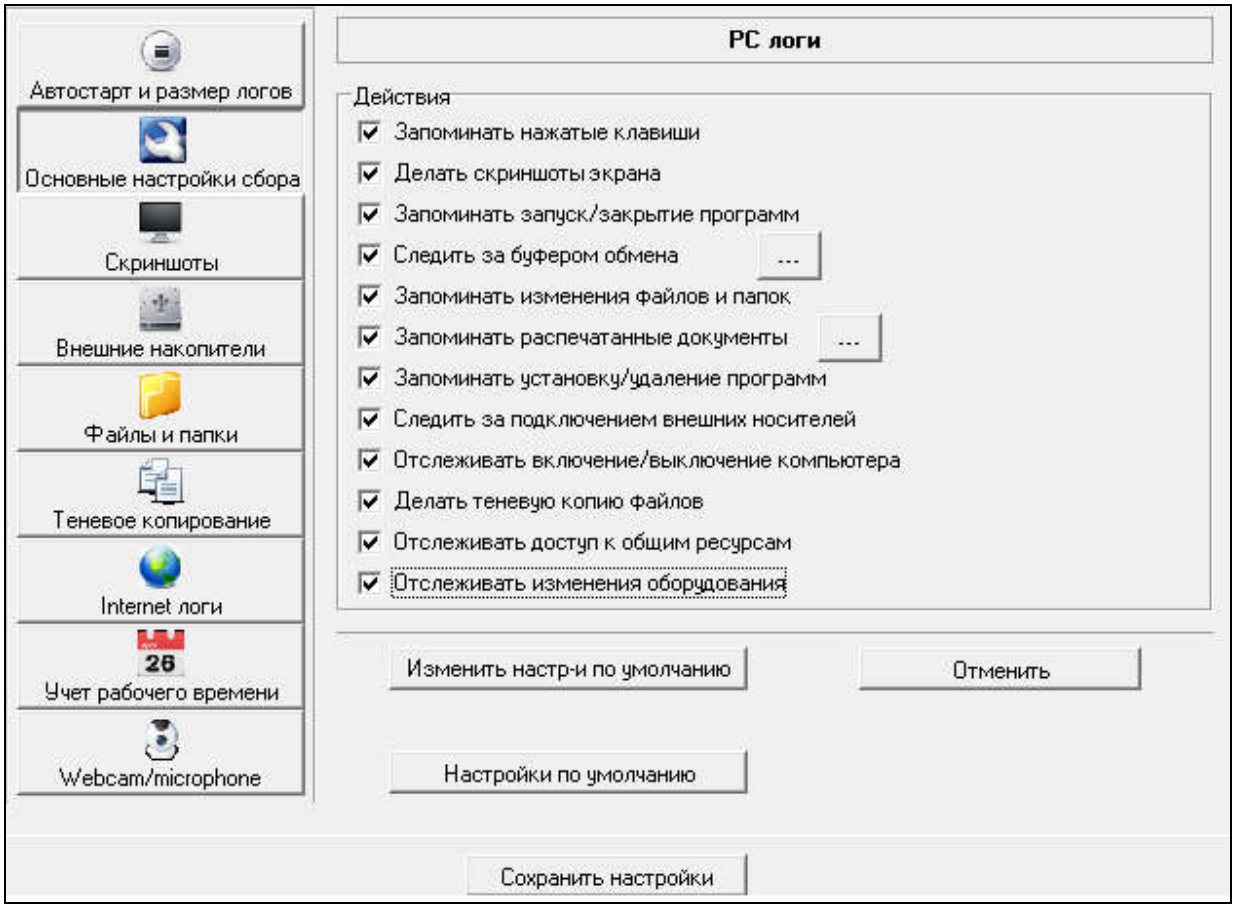
Рис. 5.3 – Главное окно настроек агентов

Автостарт и размер логов:

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.

Основные настройки сбора:



Установите галочки для тех видов данных, которые требуется собирать.

Для буфера обмена и мониторинга распечатанных документов есть дополнительные опции настройки. Для буфера это перехватывать или нет изображения, попадающие в буфер.

Для контроля напечатанных документов – сохранять ли изображение документа.

Для некоторых видов данных, таких как **Скриншоты. Внешние накопители, Файлы и папки, Теневое копирование, Internet логи и Вебкамера**, выделены самостоятельные пункты настройки. Их разберем далее.

Скриншоты:

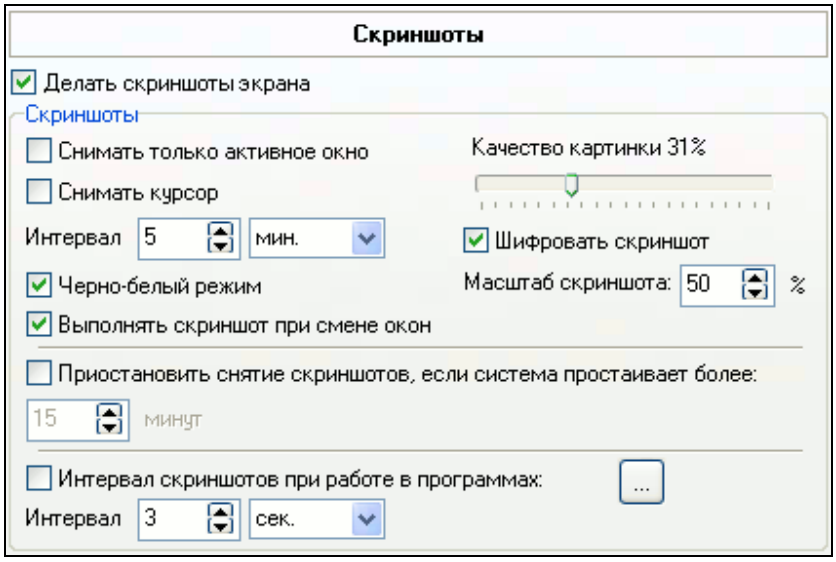


Рис. 5.5 – Настройки контроля снимков экранов

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

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

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

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

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

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.

Внешние накопители:

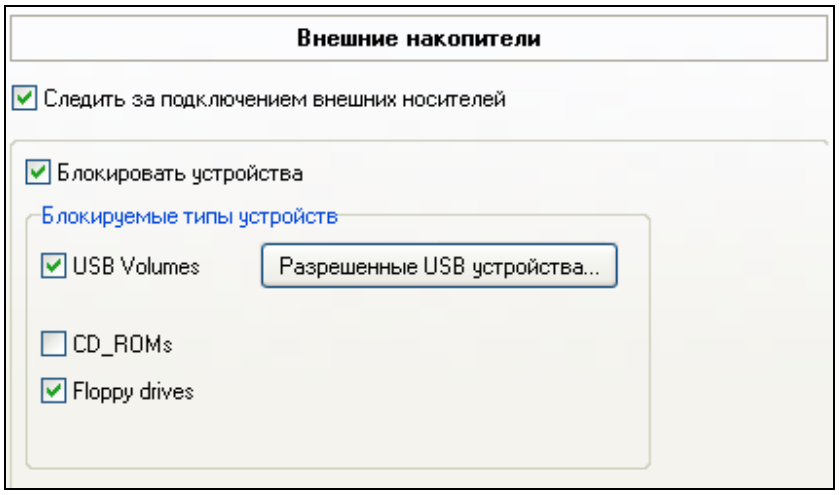


Рис. 5.14 – Настройки контроля подключения носителей

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

Файлы и папки:

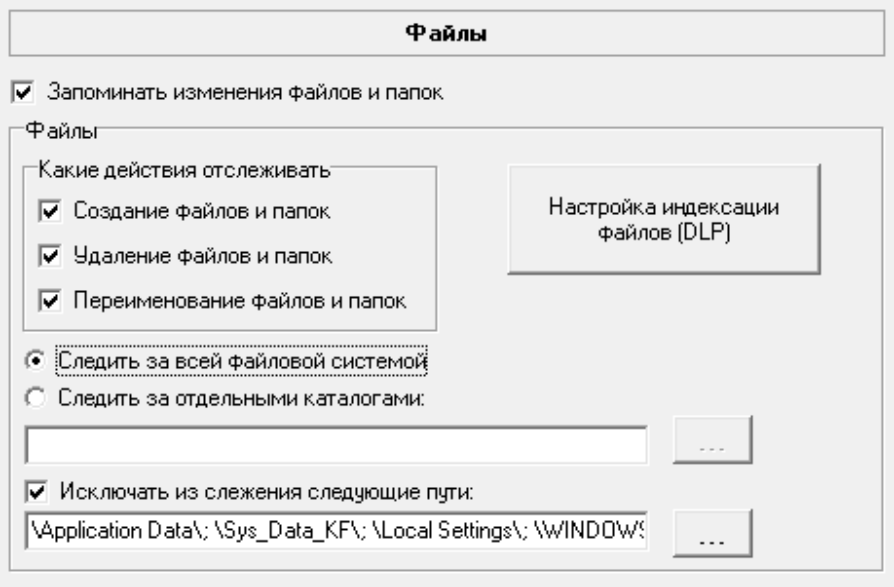


Рис. 5.8 – Настройки ведения мониторинга файловой системы

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

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

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

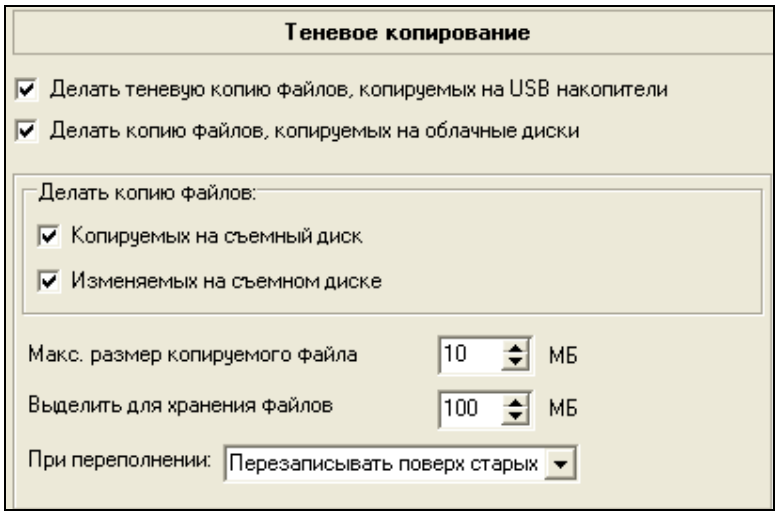
Следить за всей файловой системой - наблюдение будет производится за всеми файлами на всех дисках компьютера.

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.

Настройка индексации файлов (DLP) - для версии DLP можно настроить индексацию документов на локальных дисках контролируемых компьютеров. Подробнее это настройка разобрана в пункте 5.3.6.

Теневое копирование:



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

Делать копию файлов, копируемых на облачные диски – при установленной галочке будет делаться копия файлов, копируемых на облачные хранилища (яндекс диск, google drive, OneDrive, DropBox).

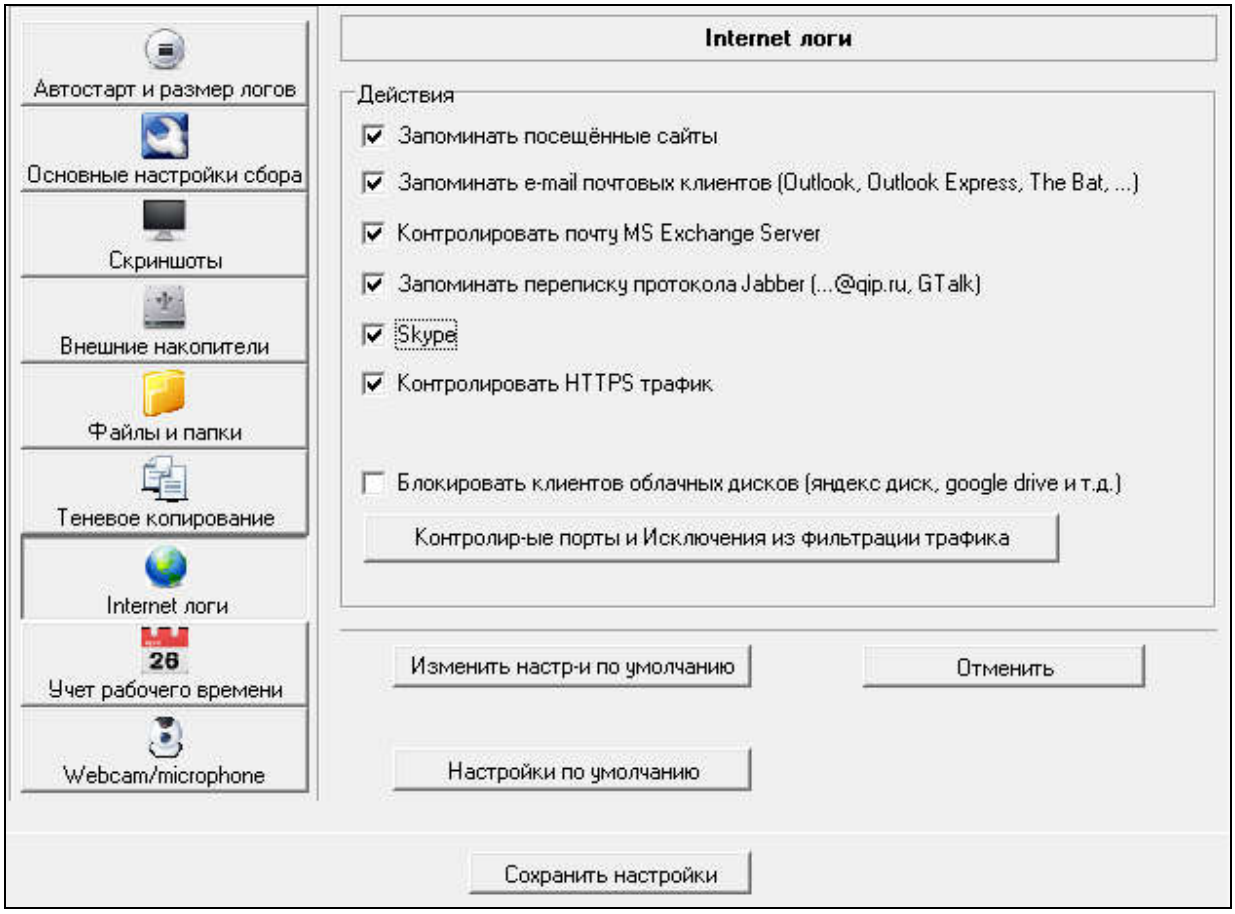
Копируемых на съемный диск - установите эту галочку, чтобы программа производила теневое копирование в том случае, когда файлы копируются на съемный диск.

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.

Internet логи - действия:



Опция **Запоминать e-mail почтовых клиентов –** определяет будет ли производиться перехват электронных писем, отправляемых и получаемых с использованием любых почтовых клиентов (Outlook, Outlook Express, The Bat, ...)

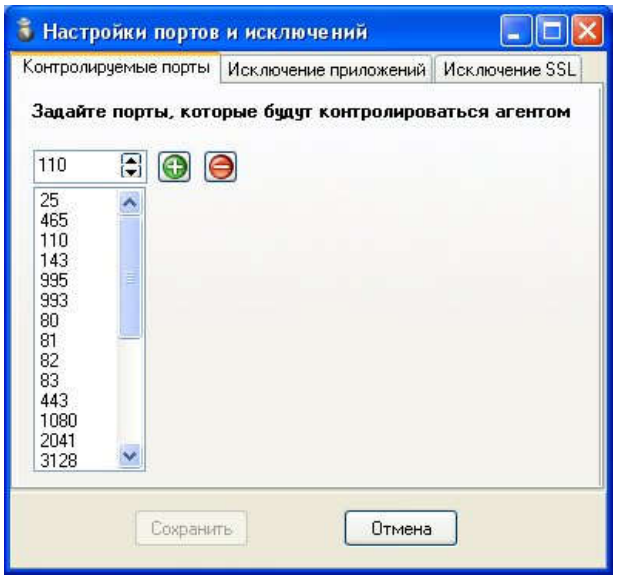
Контролировать почту MS Exchange Server – включите данную опцию, когда на контролируемых компьютерах используется почтовый клиент MS Outlook, и в качестве сервера применяется Exchange Server. В этом случае перехват почты будет производиться через специальную надстройку, встраиваемую непосредственно в Outlook.

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, ...

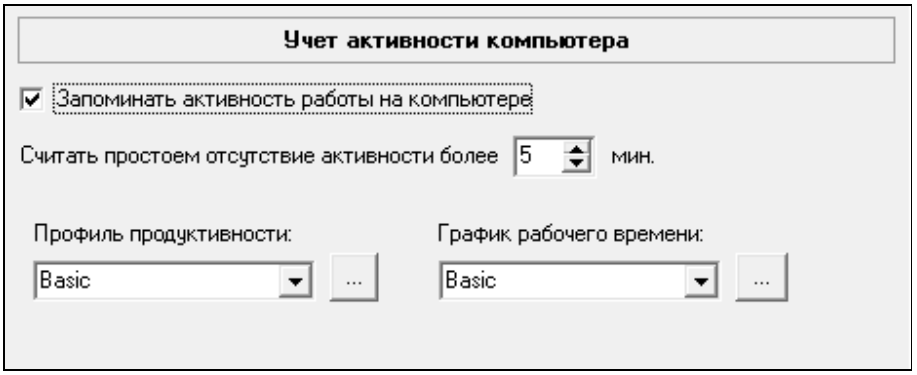
Контролировать HTTPS трафик – при установленной галочке, агент будет контролировать трафик, проходящий по шифрованным соединениям. Для этого агенту приходится подменять сертификат SSL для контролируемых сайтов.

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



Учет рабочего времени:



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.

Также в данном пункте настроек можно выбрать график рабочего времени и профиль продуктивности.

Профиль продуктивности – определяет категории программ и сайтов, которые для данного профиля настроек будут считаться продуктивными, непродуктивными и нейтральными.

Профилей продуктивности может быть столько, сколько у вас в организации различных категорий сотрудников.

Пример: для бухгалтера продуктивными ресурсами могут быть 1С, справочные системы, поисковики. А соц сети – непродуктивными. В тоже время, для специалиста по персоналу – соц сети могут быть основным инструментом и для него время, проведенное в них, будет продуктивным.

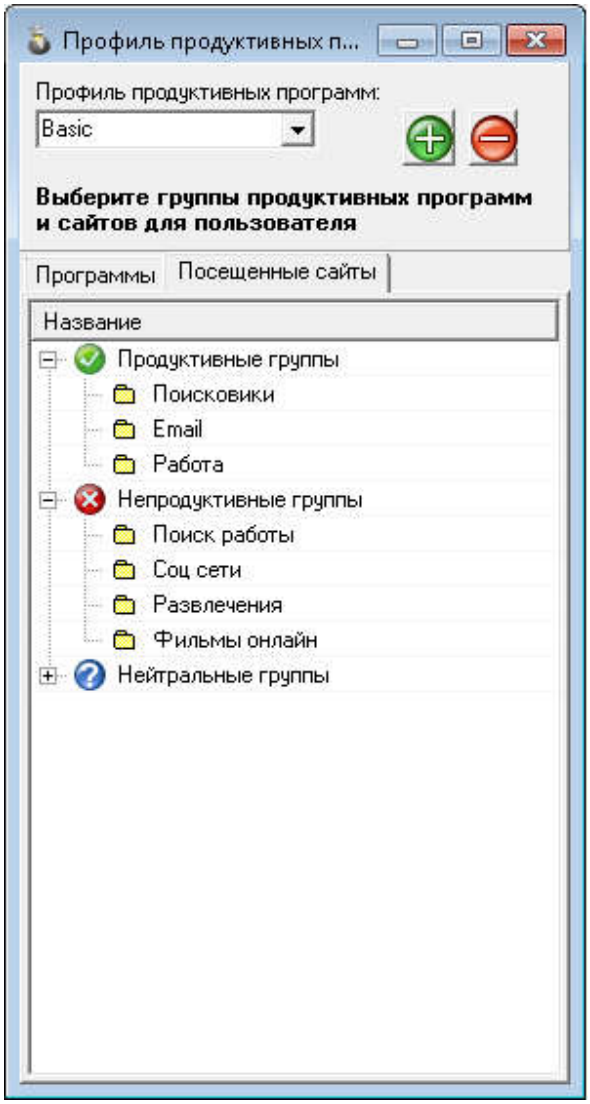
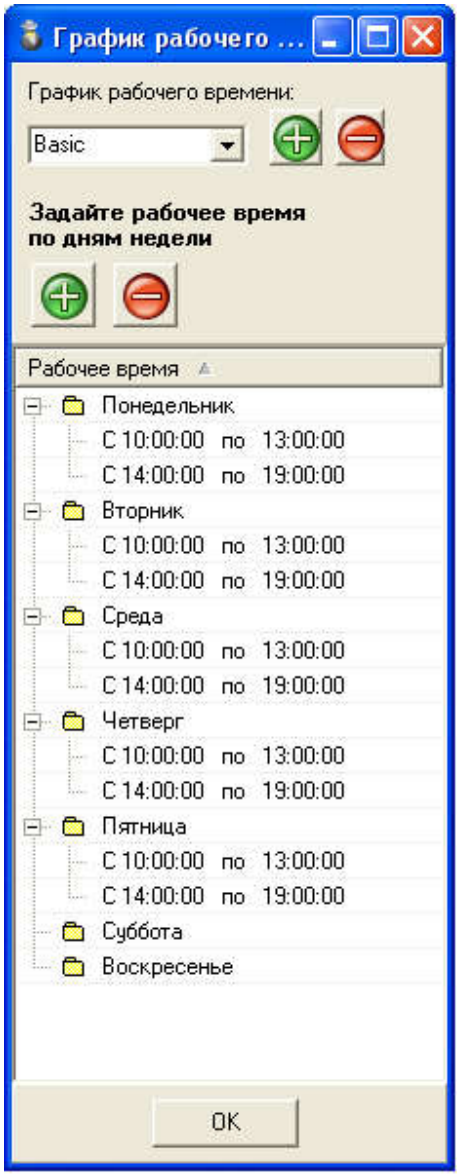


График рабочего времени – определяет рабочие дни и внутри каждого дня интервалы рабочего времени.

Эта информация используется для выявления нарушений правил безопасности и трудовой дисциплины и оповещения о них администратора системы.



Можно создать несколько графиков рабочего времени, в зависимости от бизнес-процесса в компании.

Webcam/microphone:

Путь для сохранения файлов на «шаре» сервера – по мере создания файлов видео/аудио/снимков с камеры, клиентский модуль будет сам их копировать в каталог, заданный в данном поле настроек. Если вместо пути на сервере указать локальный путь, то копирование файлов с контролируемого компьютера будет производиться серверной частью LanAgent Enterprise.

Резервный путь на локальном компьютере – используется для временного хранения файлов в том случае, когда сервер по какой-то причине не доступен (не доступен основной путь для сохранения файлов).

Логин подключения и **Пароль подключения** – укажите в этих полях данные учетной записи Windows, имеющей права на запись в «расшаренный» каталог на сервере.

Прекращать запись если осталось свободного места менее – когда свободного места на диске окажется менее заданного значения, запись новых файлов прекратится.

Записывать видео – если включить данную опцию, то следящий модуль будет производить запись видео файлов заданной длительности все время, пока компьютер включен. Запись можно производить со звуком или без него.

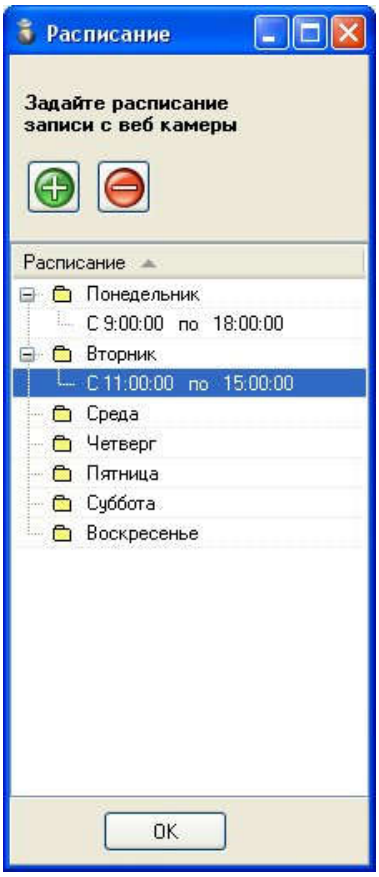
Записывать звук с микрофона – если включить данную опцию, то следящий модуль будет производить постоянную запись звука с микрофона компьютера. Длительность файлов задается соответствующей настройкой.

Делать снимки с вебкамеры каждые – задает периодичность выполнения снимков с web камеры, подключенной к компьютеру.

Для каждого компьютера индивидуально задаются устройства, используемые для записи изображения и звука. Окно выбора устройства появится автоматически при установке галочки записи видео/звука/снимков. Либо можно открыть его нажатием

кнопки «**Выбрать устройство**». Если контролируемый компьютер по какой-то причине недоступен, то будет выдано соответствующее всплывающее уведомление.

ПО РАСПИСАНИЮ - когда включена данная опция, выполнение записи видео/звука/снимков происходит строго в соответствии с заданным расписанием.



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

5.3.2 Настройки безопасности

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

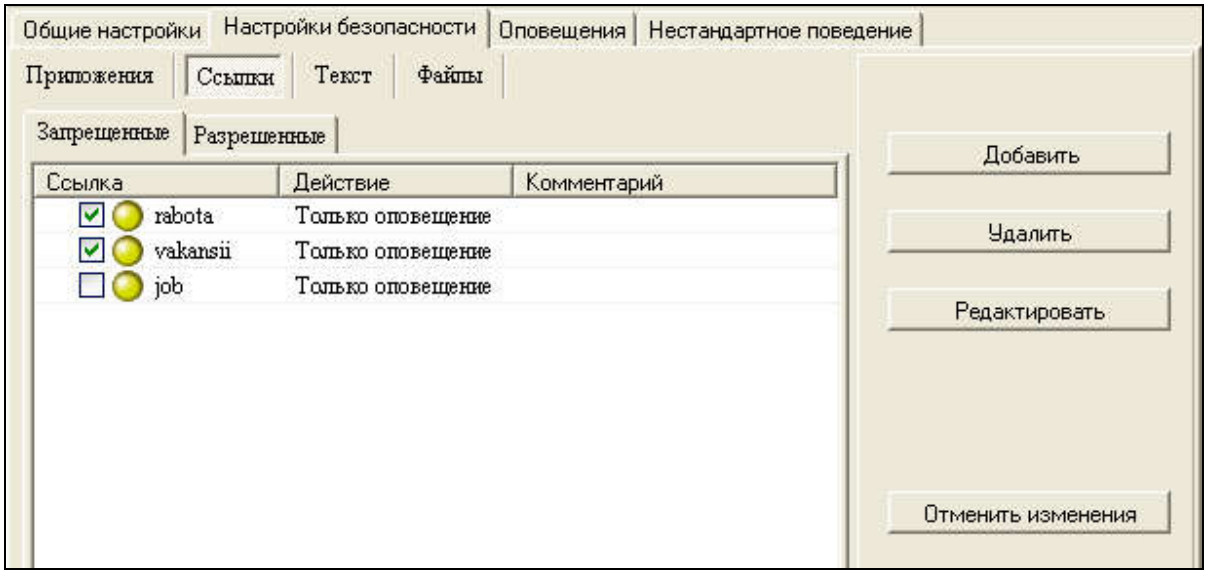


Рис. 5.16 – Список правил безопасности

Настройки агента в целом, состоят из следующих видов настроек: Общие настройки, Настройки безопасности, Оповещения и Нестандартное поведение. Настройки безопасности, в свою очередь, разбиты на 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).

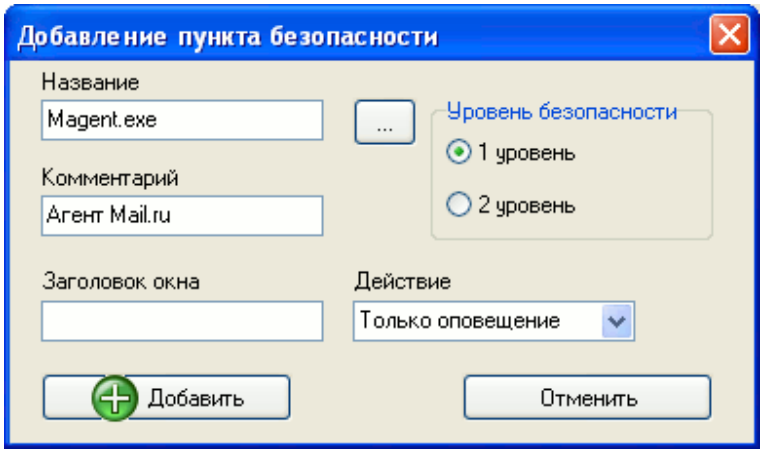
На закладке **«Файлы»** указываются непосредственно имена файлов, открытие/закрытие которых будет считаться нарушением правил.

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

Рассмотрим заполнение правил безопасности на конкретных примерах:

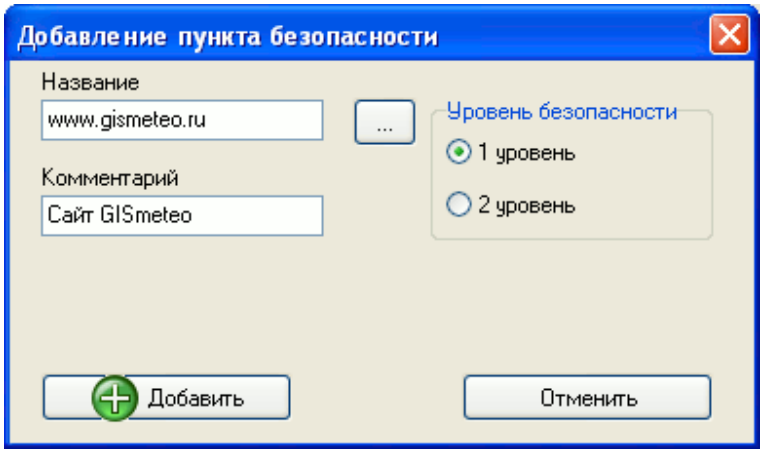
1. Допустим, мы хотим, чтобы программа MailAgent подсвечивалась в логах запуска программ, как запрещенная. Для это в окне настроек безопасности, переходим на закладку приложения и нажимаем кнопку **«Добавить»** (в правой части окна). При этом откроется окно добавления пункта безопасности. В поле **«Название»** 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.



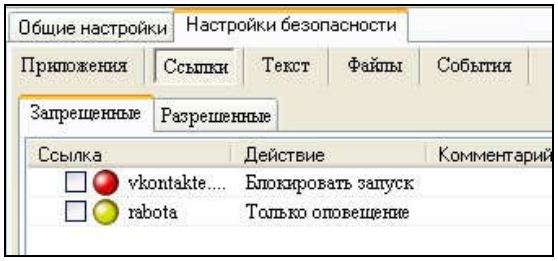
После нажатия кнопки **«Добавить»**, данное правило будет сохранено.

***ВАЖНО**. Список правил на вкладке это просто словарь. Для того, чтобы включить использование правила для профиля настроек, надо поставить рядом со строкой нужного правила галочку и нажать кнопку **Сохранить**.*

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».

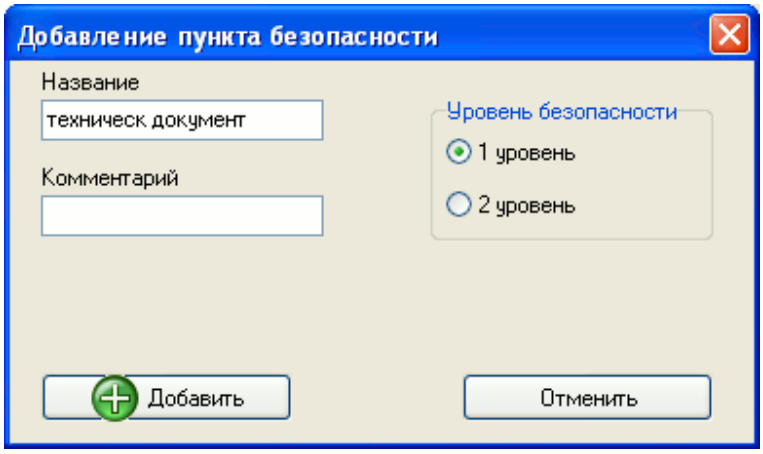


Также в LanAgent есть возможность блокировать открытие пользователем ссылок. Принцип настройки данной опции тот же, что и для программ: выбрать в качестве действия пункт "Блокировать". При этом можно задать и список запрещенных, и список разрешенных ресурсов. Это позволяет как запретить доступ к каким-то определенным сайтам, так и наоборот, оставить разрешение на посещение корпоративных ресурсов, закрыв доступ ко всем остальным.

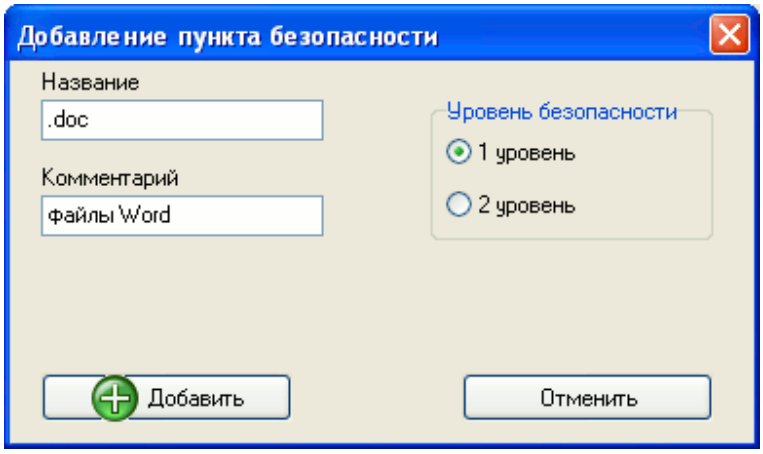


Например, если в список "Запрещенные" внести запись ".ru", а в список "Разрешенных" внести, например, "mail.ru", то из всех веб ресурсов зоны RU пользователю будет разрешено посещение только ресурса mail.ru.

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



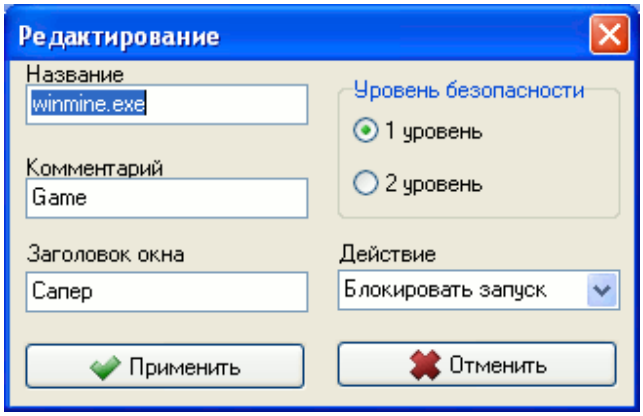
4. Закладка **«Файлы»**. Допустим мы хотим запретить работу с любыми текстовыми документами с расширением .doc. Тогда в поле **«Название»** мы соответственно внесем всё расширение.



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

Редактирование правил:

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



Удаление правил:

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

5.3.3 Оповещения

Оповещения в свою очередь подразделяются на «**Оповещения безопасности**» и «**Оповещения продуктивности**».

Оповещения безопасности

На данной закладке происходит настройка оповещений специалиста безопасности о потенциально опасных событиях, таких как отправка писем на внешнюю почту (как через почтового клиента, так и через браузер), копировании файлов на USB накопитель, выгрузке их в интернет. Это делается с учетом размеров файлов и графика рабочего времени (подробнее о его настройке см. пункт 5.8 данного руководства).

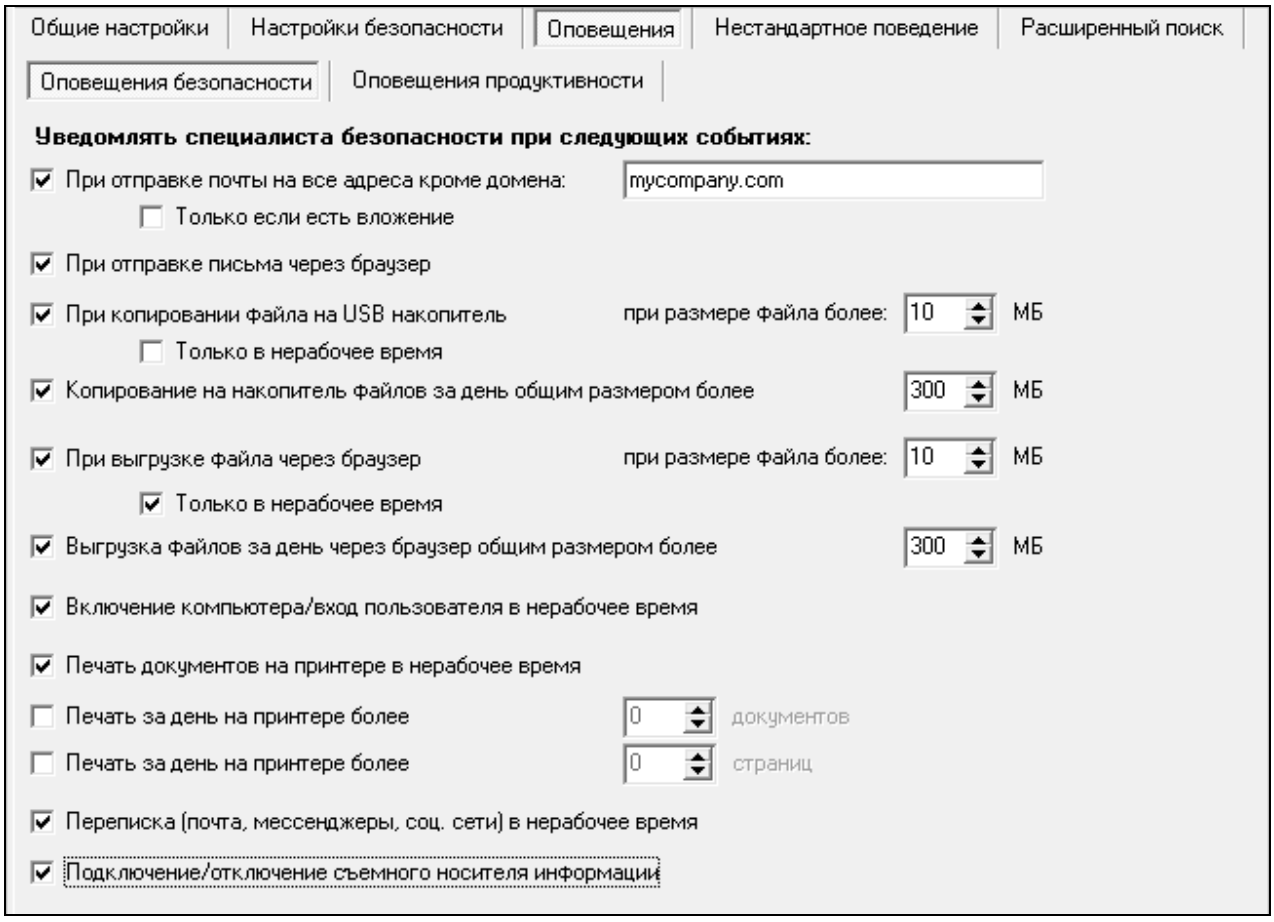
Оповещение о данных событиях может производиться как напрямую в консоль специалиста безопасности, так и на электронную почту специалиста.

Ниже более подробное описание по оповещениям.

Оповещение **при отправке почты на все адреса, кроме домена** – срабатывает в случае отправки электронного письма на любой из адресов, кроме адресов, домен которых указан в специальном поле. Если в этом поле указать домен компании, тогда программа будет оповещать только о внешней переписке сотрудников (о письмах, уходящих наружу организации).

Отправка писем на адреса в домене компании будет считаться внутрикорпоративной перепиской и уведомлений о ней не будет происходить.

Также, можно указать дополнительную опцию для этого пункта настроек - оповещать только если письмо содержит вложение.



При отправке письма через браузер – сработает при отправке любого письме веб почты.

Для оповещения **при копировании файлов на USB накопители**, можно задать размер файла, при превышении которого будет отправляться оповещение. Если его надо делать на любой файл, то оставьте значение = 0 МБ.

При включенной доп. опции «**Только в нерабочее время**» оповещение будет происходить только для случаев копирования файлов в нерабочее время.

Копирование на накопитель файлов за день общим размером более – позволяет уведомлять специалиста безопасности в том случае, если суммарный объем скопированных пользователем за день файлов превысит указанный объем.

При выгрузке файла через браузер: имеет дополнительные опции - размер выгружаемого файла и «только в нерабочее время». Это позволяет настроить

уведомления как на любую выгрузку файлов пользователем в интернет, так и на отправки до или после окончания рабочего дня.

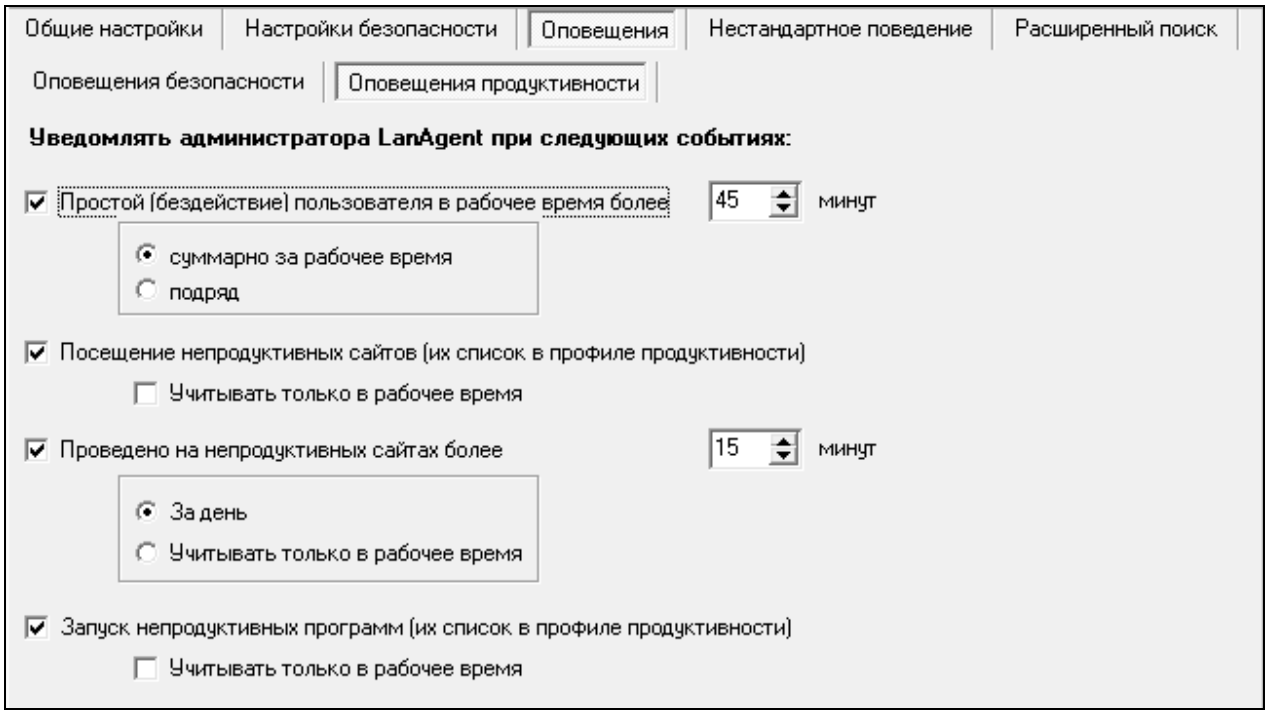
Выгрузка файлов за день через браузер – позволяет определить значение суммарного объема файлов, при превышении которого lanagent уведомит специалиста безопасности.

Изменение конфигурации оборудования на ПК – сработает при установке или отключении пользователем комплектующих компьютера: снятии планки оперативной памяти, видеокарты, …

Оповещение произойдет сразу после обнаружения изменений.

Оповещения продуктивности

Позволяет определить список событий, касающийся продуктивности работы сотрудников, на которые будет происходить уведомление администратора системы.



Список непродуктивных сайтов и программ задается в Профиле продуктивности.

Выбрать его можно в **Настройки агента – Общие настройки – Учет рабочего времени – Профиль продуктивности**. (пункт 5.3.1 данного руководства).

Редактирование профилей продуктивных программ доступно через верхнее меню LA Admin. Категории – Настроить профиль продуктивных программ.

Применение настроек происходит по нажатию кнопки «Сохранить настройки».

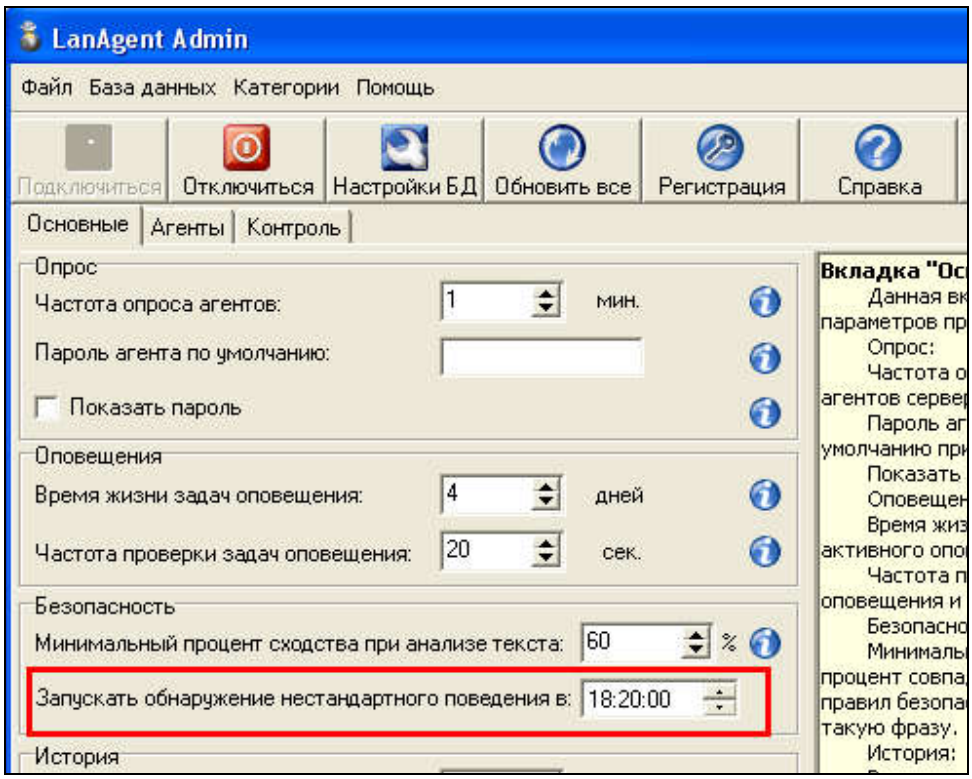
5.3.4 Нестандартное поведение

На данной закладке происходит настройка оповещений специалиста безопасности об отклонении поведения пользователя от типичного. Для этого требуется наличия данных по контролируемому пользователю за предыдущие дни.

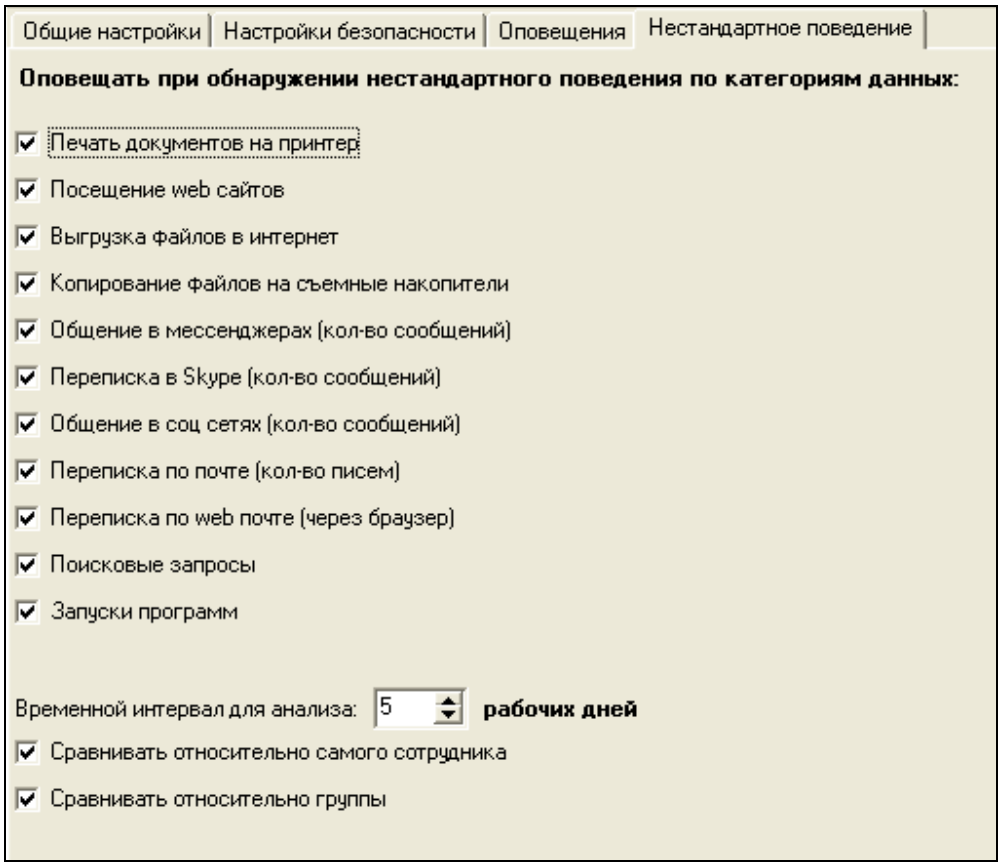
Пример: если при обычном режиме работы сотрудник печатает в день от 7 до 12 документов, то печать 20 документов за текущий день будет отклонением от стандартного поведения.

Чем за больший период времени имеется накопленная статистика, тем точнее будет работать алгоритм выявления отклонений.

Проверка и выявление нетипичной активности производится один раз за день. Время проведения анализа определяется в LA Admin на вкладке настроек Основные.



Категории данных, которые будут учитываться в сравнении, задаются как показано на рисунке ниже.



Временной интервал анализа – определяет объем данных, относительно которого будет определять отклонение.

Сравнение новых данных пользователя можно делать как относительно данных по нему же за предыдущие периоды, так и относительно данных по всем сотрудникам группы, в которую входит пользователь.

Пример: сотрудник входит в отдел «Бухгалтерия» и нестандартное количество напечатанных документов по нему определяется в сравнении с другими бухгалтерами.

Применение настроек происходит по нажатию кнопки «Сохранить настройки».

5.3.5 Расширенный поиск (в EnterpriseDLP)

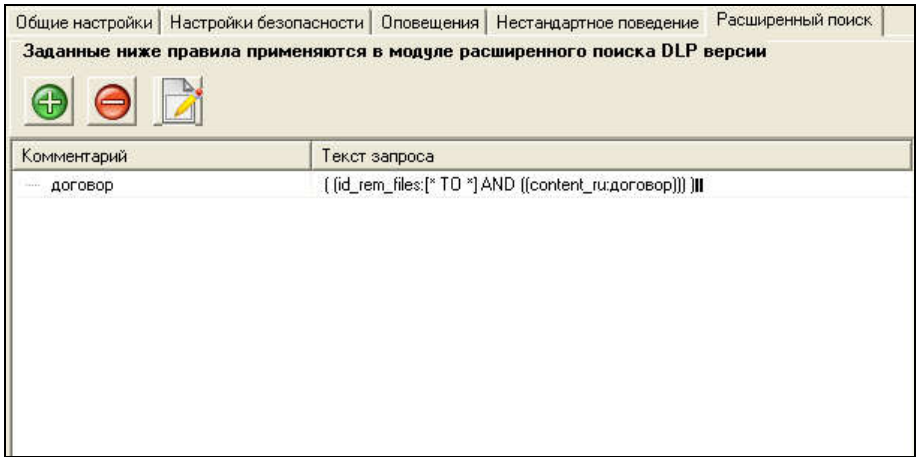
Для версии EnterpriseDLP становится доступна вкладка настроек «**Расширенный поиск**». Она позволяет задать составные правила для ключевых фраз, которые

будут искаться внутри перехваченных файлов вложений почты, скопированных на внешние накопители, напечатанных на принтер документах и т.д.

И на ней же можно включить поиск в собранных данных регулярных выражений (номеров телефонов, паспортных данных и т.д.).

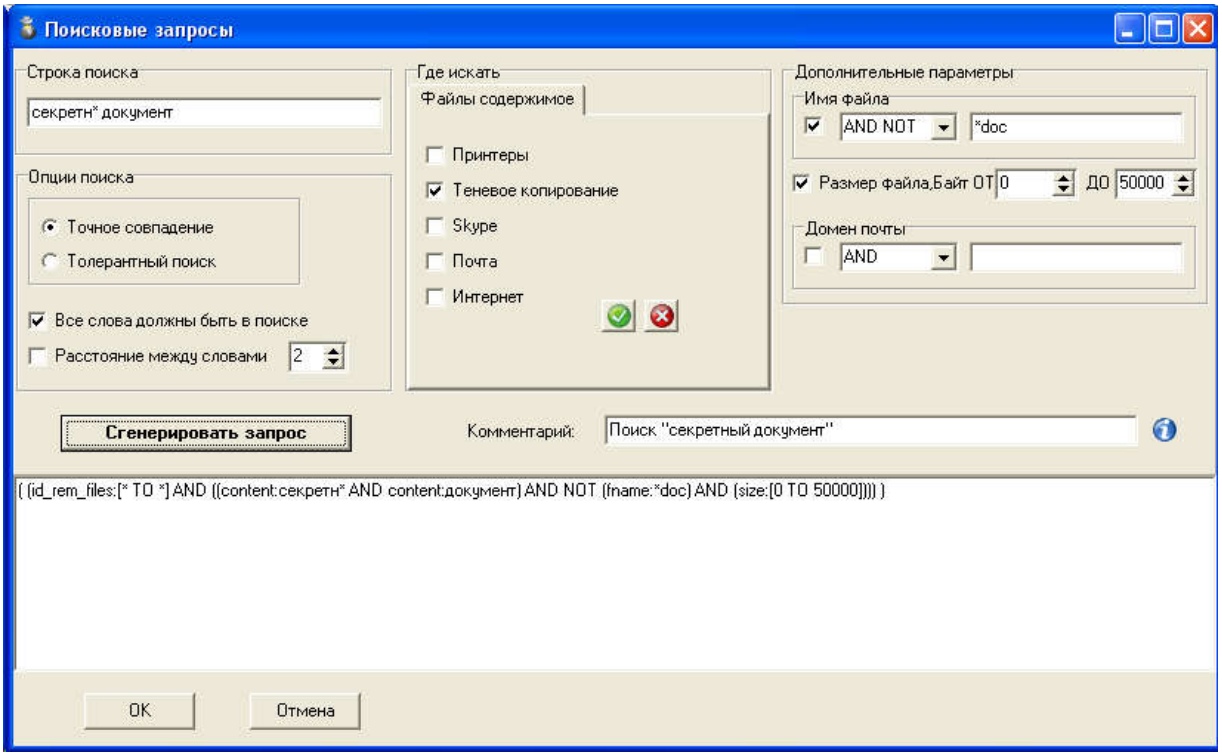
Задание правил расширенного поиска.

Задание правил поиска по файлам происходит в программе LA Admin в настройках агентов. На вкладке «Расширенный поиск»



Для добавления нового правила, нажмите кнопку с плюсом. Для редактирования созданного ранее правила, выберите его в списке правил и нажмите кнопку со значком блокнота.

При этом откроется следующее окно:



В нем в строке поиска задайте фразу, на которую будет срабатывать правило безопасности.
При необходимости поиска по части слова, используйте значок звездочки *

Пример: *шин* - в результатах поиска будет машина, шиномонтаж и т.д.

Опция «точное совпадение» подойдет для случаев, когда в искомом тексте слово или фраза не содержит опечаток или намеренного искажения. Морфология (различные варианты окончания) при этом учитывается
Опция «Толерантный поиск» применяется для случаев, когда в искомом тексте возможны опечатки, намеренные искажения текста (замена буквы Русского алфавита на аналогичную латинскую, замена буквы на цифру и т.д.)
Также, такой вариант поиска подойдет для транслита.

Опция «Все слова должны быть в поиске». Применима для тех случаев, когда задана фраза, а не отдельное слово и необходимо показать только те результаты, в которых содержатся все слова из этой фразы.

При этом дополнительной опцией можно задать допустимое расстояние между словами (при котором найденный текст будет считаться соответствующим условию).

Производить поиск можно в данных, полученных из разных источников: в изображениях напечатанных документов, файлах теневой копии (перехваченных при копировании на флешку), выгруженных в интернет, отправленных по почте.

В качестве дополнительных опций автоматического поиска можно задать ограничение на размер файла (поиск будет происходить только по файлам подходящим по размеру).

Можно указать имя или расширение файла, также использую звездочку. И задать условие AND, OR, AND NOT в зависимости от которого поиск будет включать или наоборот исключать указанные имена.

Аналогично, можно указать домен почты, на который отправлялись письма.
И делать поиск только по тем письмам, которые отправлялись на этот домен, или наоборот, по всем, кроме писем, отправленным на этот домен.

Комментарий необходим для того, чтобы в последствии было проще понять назначение данного правила. Он обязателен к заполнению.

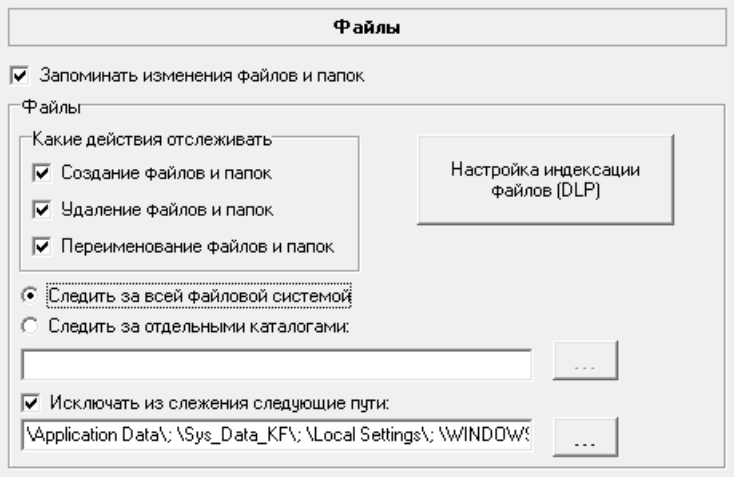
При нажатии кнопки «Сгенерировать запрос», можно просмотреть сформированный текст запроса, как его будет отрабатывать поисковый модуль. Вносить изменения вручную в него можно, но только если вы владеете синтаксисом запросов поискового ядра Solr.

5.3.6 Настройка индексации файлов (в EnterpriseDLP)

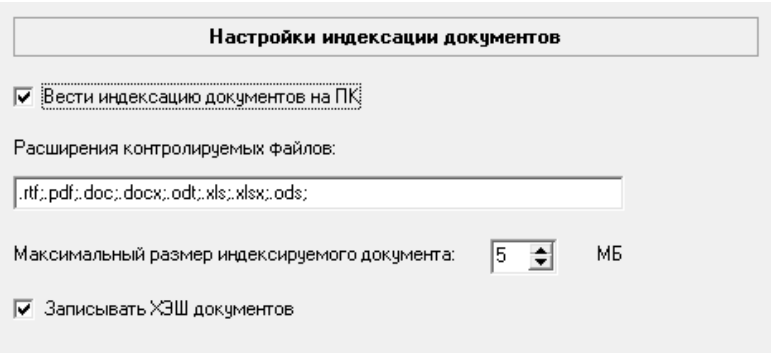
Для версии EnterpriseDLP можно включить индексацию документов на локальных дисках контролируемых компьютеров.

Для проведения такой настройки, перейдите на пункт настроек агента:

Общие настройки - Файлы и папки



Там нажмите кнопку «Настройки индексации файлов (DLP)».

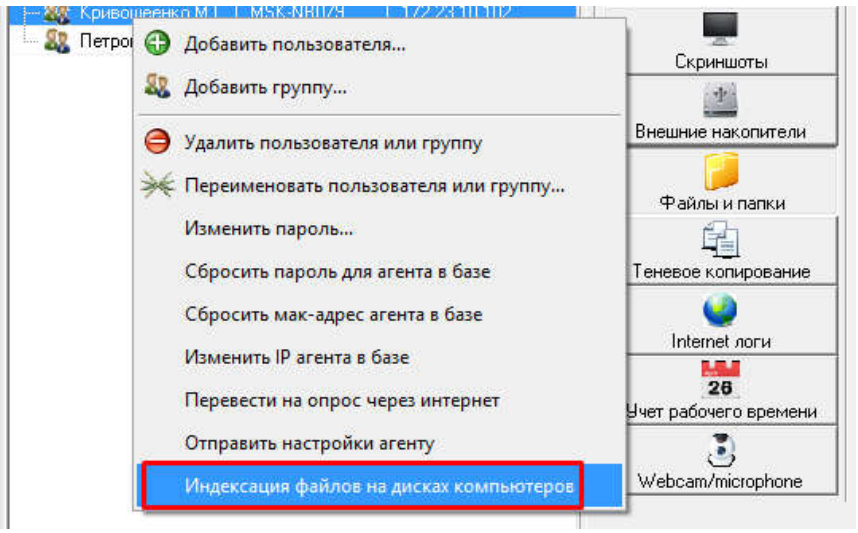


Здесь можно задать перечень расширений, которые агент должен индексировать, а также можно ограничить максимальный размер индексируемых файлов.

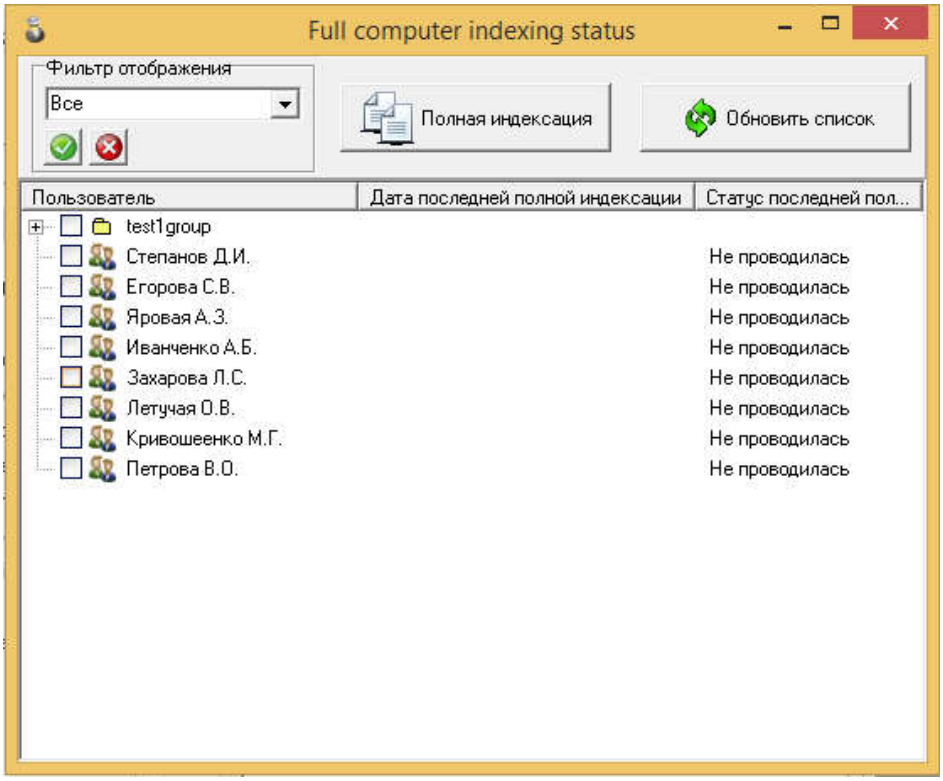
Сама индексация документов может происходить в 2-х режимах:

- по мере внесения изменений в документы на контролируемом компьютере (или появлении на нем новых документов).
- По команде на проведение полной индексации из админки. В этом режиме, индексация будет проведена для всех документов, имеющихся на компьютере.

Первый режим работает автоматически, после включения опции «Вести индексацию документов на ПК».
Для запуска второго режима, щелкните правой клавишей мыши на любом компьютере в списке.



При этом откроется следующее окно:



В нем отображается статус и дата последней полной индексации. Также с его помощью можно поставить задачу на проведение полной индексации документов для выбранных компьютеров.

5.4 Закладка «Контроль»

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

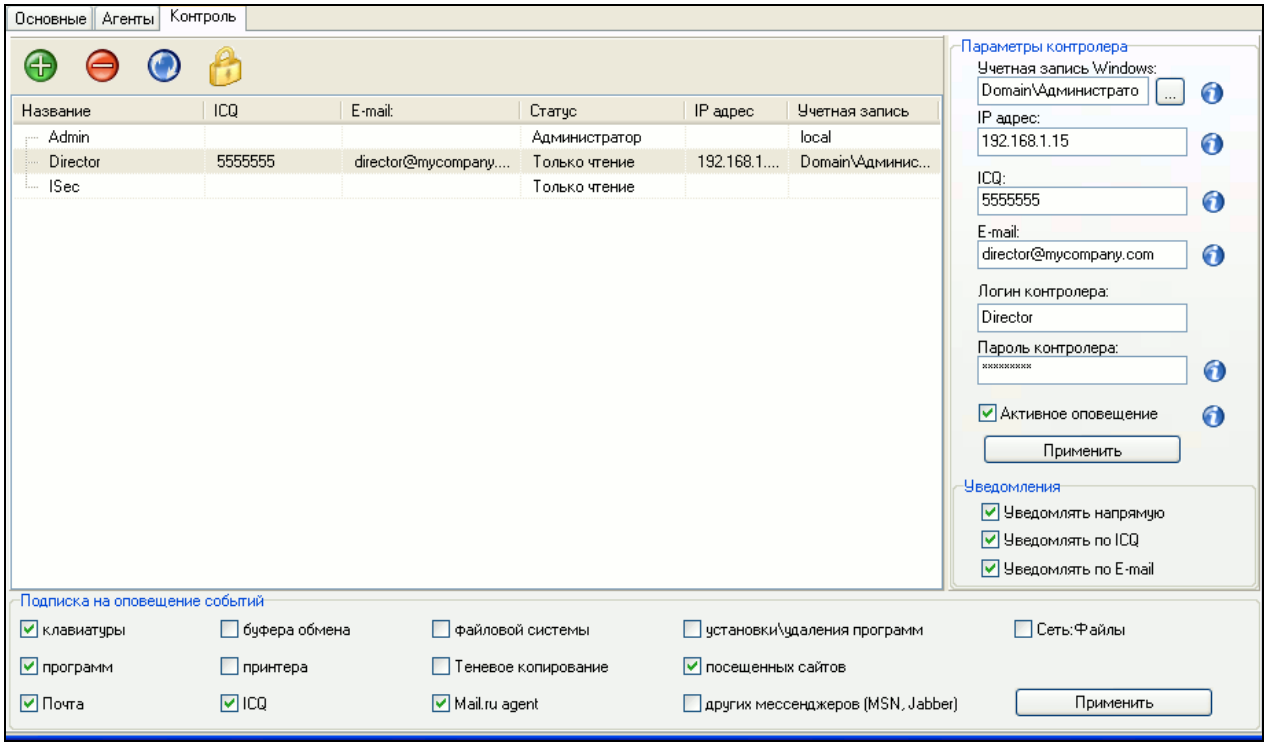


Рисунок 5.17 – Закладка «Контроль» LanAgent Admin

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

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

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

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

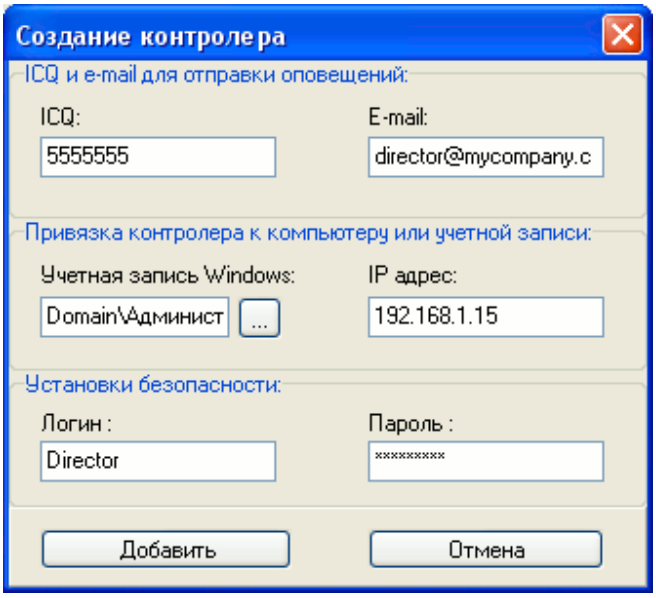


Рисунок 36 - Диалог добавления контролера

Поля **«ICQ»** и **«E-mail»** будут использоваться для адресации оповещений, на которые данный пользователь будет подписан. Они не являются обязательными.

Значения, введенные в поля **«Логин»** и **«Пароль»,** данный пользователь будет вводить в диалоге авторизации в качестве логина и пароля соответственно при запуске программ **LanAgent View** или **LanAgent Admin**.

Поля **IP адрес** и **Учетная запись Windows** определяют IP адрес компьютера, на котором можно войти в программу LA View под данным логином и учетную запись windows в которой можно осуществить вход. **Задание данных полей не обязательно, но если они указаны, то зайти в LA View можно будет только с этого IP и только под указанной учеткой windows**.

По окончанию заполнения, нажмите кнопку «Добавить», для внесения пользователя в список.

Для удаления уже существующего пользователя, нажмите кнопку 

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

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

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

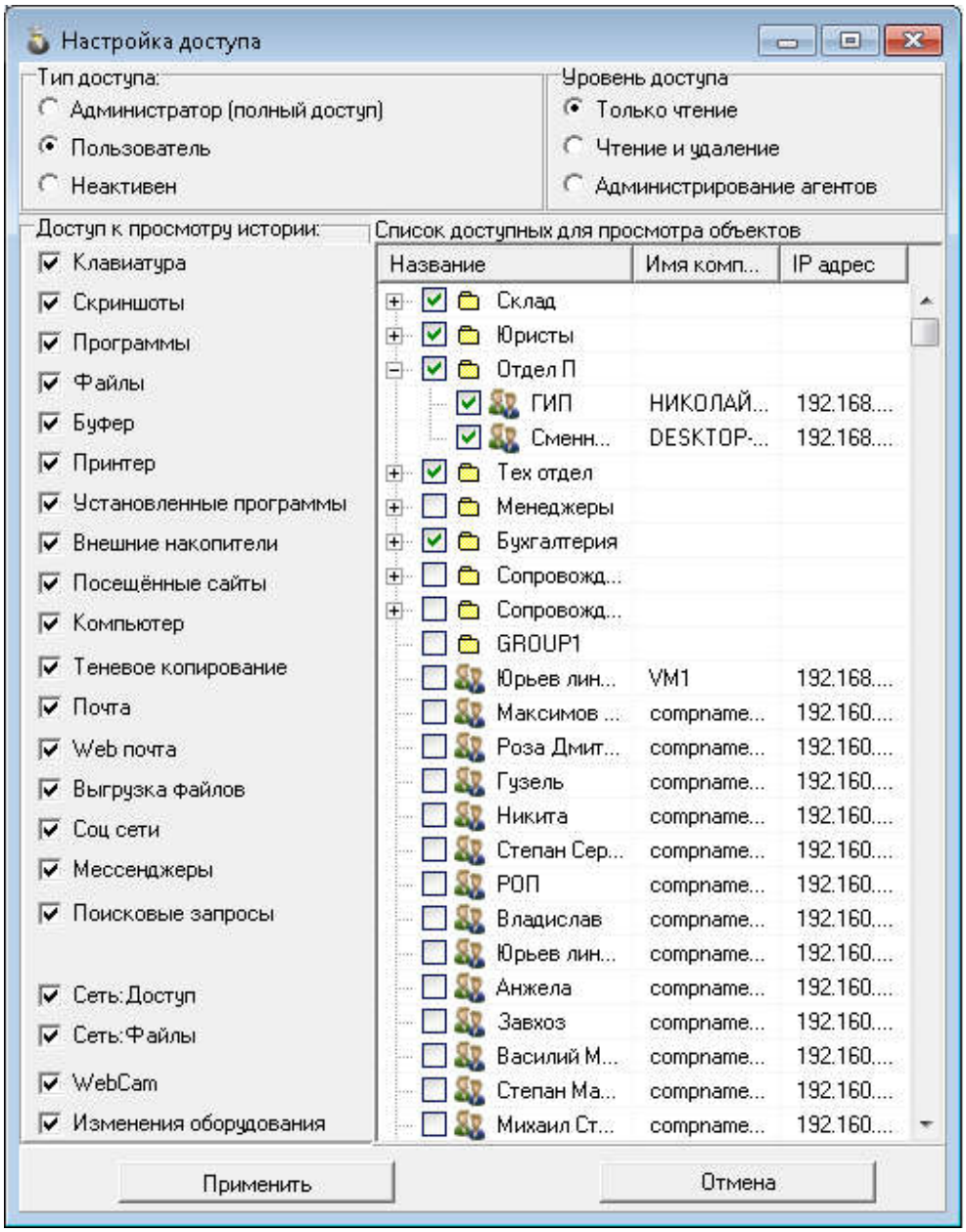


Рисунок 5.18 – Окно настройки доступа

Возможны три типа пользователей: Администратор (обладает неограниченными правами) Пользователь (для него возможны 3 уровня доступа к данным: «Только чтение», «Чтение и удаление» и «Администрирование агентов») и Неактивен (учетные записи с данным типом соответственно не имеют никаких прав доступа).
Обычный пользователь не имеет доступа к **LanAgent Admin**, а в **LanAgent View** для него недоступна системная история (Log).
В случае если для пользователя выбран режим доступа «Администрирование агентов», то у него есть доступ к LA Admin, но только ко вкладке Агенты. Это

позволяет производить переустановку следящий модулей программы, добавлять и удалять их в списке, но не дает доступа к настройкам контролеров.

Права для категории Пользователь на просмотр данных по категориям определяются ниже, в окне «Доступ к просмотру истории». По-умолчанию у вновь созданного пользователя уже есть право на просмотр всех типов истории. Для запрещения доступа к определенной категории, достаточно убрать галочку рядом с ней и, затем, нажать кнопку «**Применить**».
Также, для каждого пользователя необходимо указывать список компьютеров, собранную информацию с которых он имеет право просматривать. Для пользователя с правами администратора по-умолчанию доступны для просмотра все контролируемые компьютеры.

Подписка на оповещения:

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

Уведомления:

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

- **Уведомлять напрямую** – требует запущенной у специалиста безопасности программы **LanAgent View.** При возникновении события, **LanAgent View** выдаст соответствующее сообщение на экран и, при необходимости, перейдет на соответствующую строку истории событий. (необходимо заполнение параметров «**Имя компьютера**» и «**IP адрес**»)

- **Уведомлять по E-mail** – при возникновении события, специалисту безопасности придет письмо, на указанный в соответствующем поле настройки электронный ящик, в котором будет содержаться тип события, время его возникновения, на каком компьютере оно произошло (необходимо заполнение параметра «**E-mail**»)

Активное оповещение:

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

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

5.5 Опрос контролируемых компьютеров через Интернет

Начиная с версии 5.3 Enterprise, опрос контролируемых компьютеров может производиться через Интернет. В этом случае, клиентский модуль программы будет сам устанавливать соединение до серверного компьютера. Для этого необходимо обеспечить возможность доступа к нему извне локальной сети по IP адресу.

Возможны две ситуации: 1). Когда какой-то из уже добавленных в список мониторинга компьютеров надо перевести на удаленный режим опроса. И сам компьютер пока еще находится в локальной сети.
2). Если контролируемый компьютер еще не внесен в список мониторинга.

В первом случае, достаточно щелкнуть по компьютеру в списке мониторинга правой клавишей мыши и выбрать в выпадающем меню вариант «**Перевести на опрос через интернет**». Предварительно, необходимо заполнить поле настроек «**Внешний IP сервера (для опроса через интернет)**» на вкладке «**Основные**».

Во втором случае, после установки клиентского модуля на контролируемый компьютер, надо установить на нем ключ реестра (выложен по ссылке www.lanagent.ru/RegFeed.rar) предварительно отредактировав в нем значение IP адреса сервера. И перезагрузить компьютер.

После этого, его можно будет добавить в список мониторинга в LA Admin через диалог «Добавить “remote” пользователей…»

Клиент будет подключаться к серверу при работе через интернет через порт 46658 tcp/ip.

5.6 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

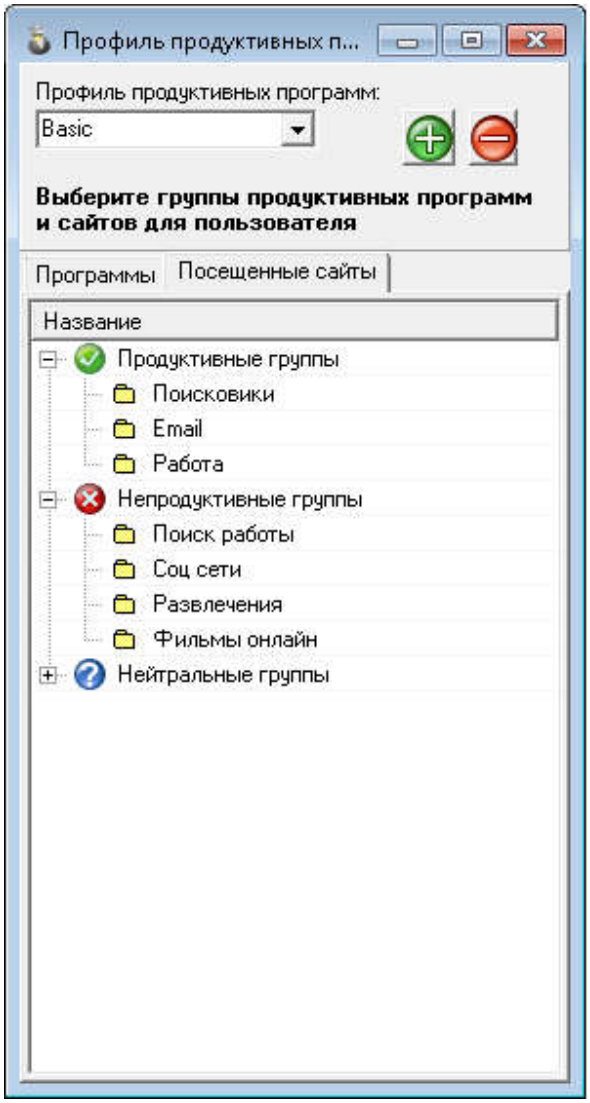
Сохраните настройки, для их отправки на контролируемые компьютеры.

5.7 Настройка профиля продуктивных программ/сайтов

Настройка профиля продуктивных приложений и сайтов, позволяет составлять отчет о продуктивности работы пользователей. Каждому компьютеру или группе компьютеров можно задать свой профиль в общем окне настроек.

Также редактирование профилей продуктивных программ доступно через верхнее меню LA Admin. Категории – Настроить профиль продуктивных программ.

Внесение в список продуктивных производится для заданных категорий программ и сайтов.

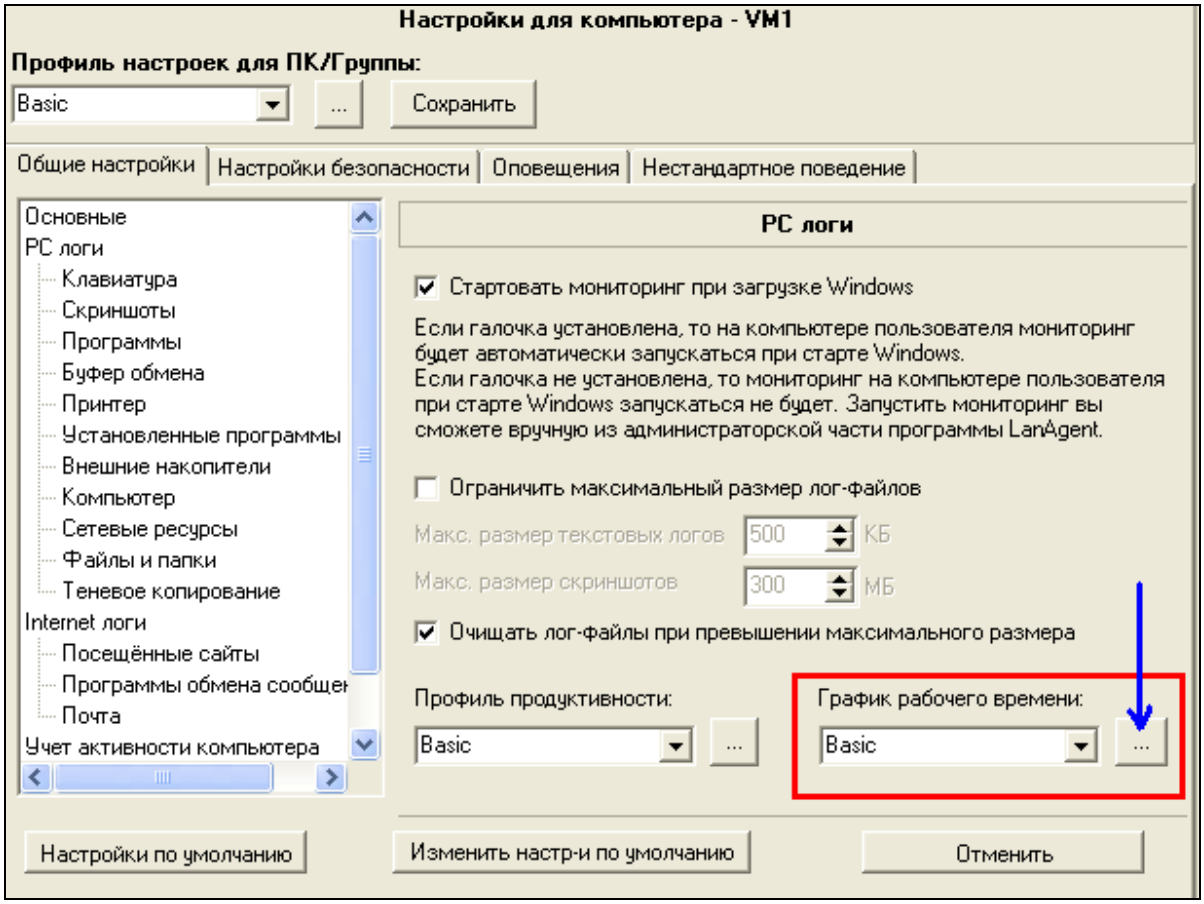


5.8 Настройка графика рабочего времени

Наличие заданного графика рабочего времени требуется для работы некоторых оповещений безопасности (в том случае, если требуется уведомление специалиста безопасности о копировании и выгрузке файлов в нерабочее время, активности на компьютере в нерабочее время и т.д.).

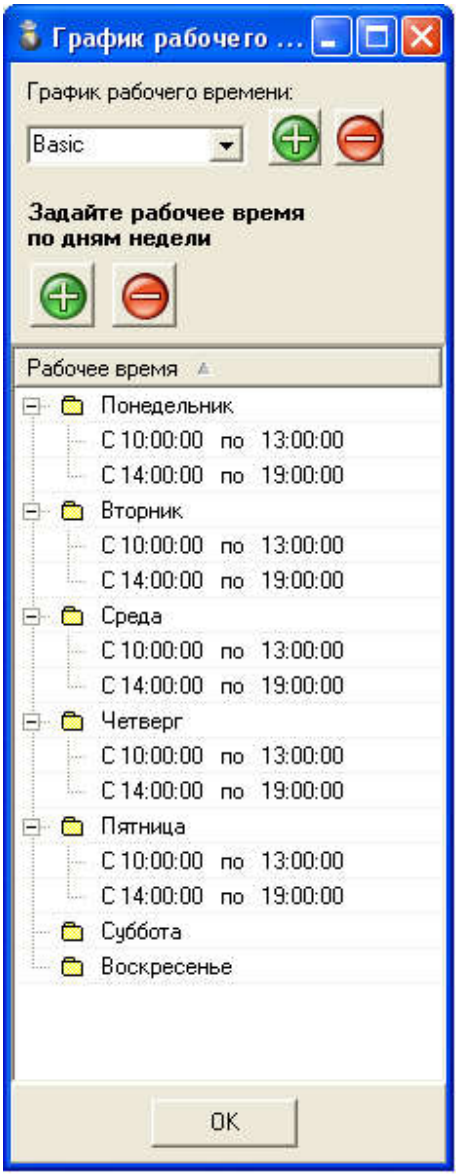
Также, график рабочего времени используется в отчетах.

Если в компании нет единого для всех режима работы, то можно создать несколько графиков и для каждого профиля настроек указать какой из графиков времени для него будет действовать.



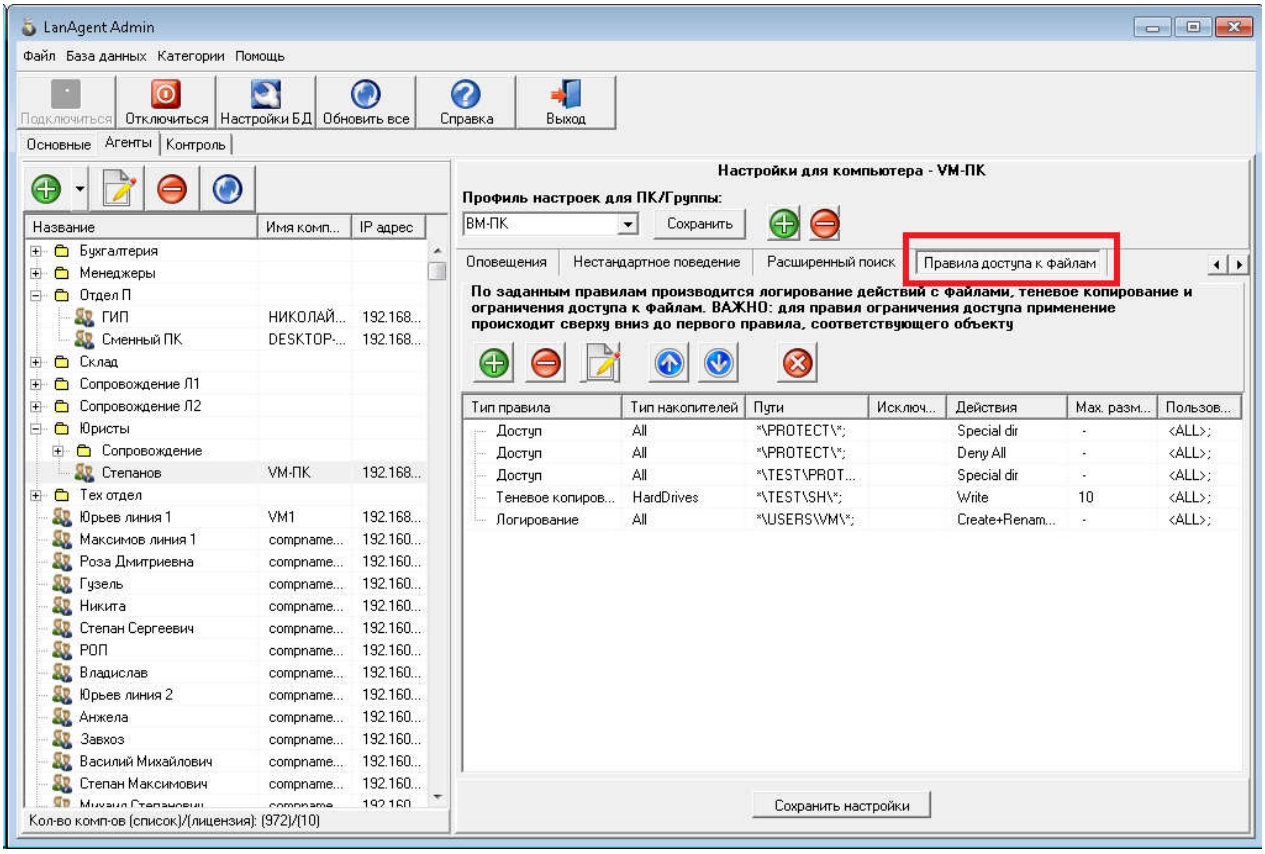
Для изменения рабочих часов внутри графика, нажмите кнопку с троеточием (на рисунке на нее показывает синяя стрелка).

Время задается именно работы. Например, с 8:00 до 12:00, далее с 13:00 до 17:00 и так по всем рабочим дням.



5.9 Ограничение доступа к файлам в EnterpriseDLP

Ограничение доступа к файлам в программе LanAgent EnterpriseDLP производится путем настройки специальных правил в профиле настроек.



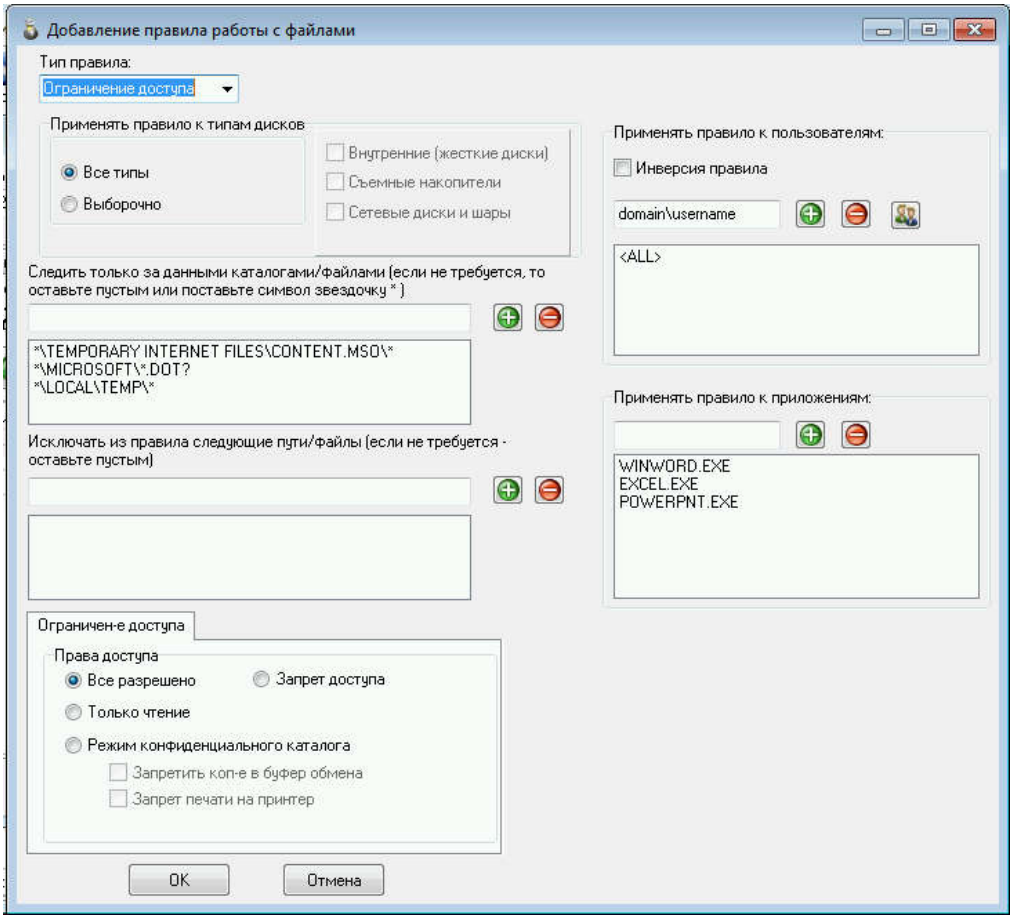
Для этого щелкните дважды по любому из компьютеров или группе компьютеров. В правой части окна откроются настройки связанного с ним профиля настроек. Перейдите на пункт настроек «Правила доступа к файлам».

Ниже разберем пример задания правил для следующей задачи:

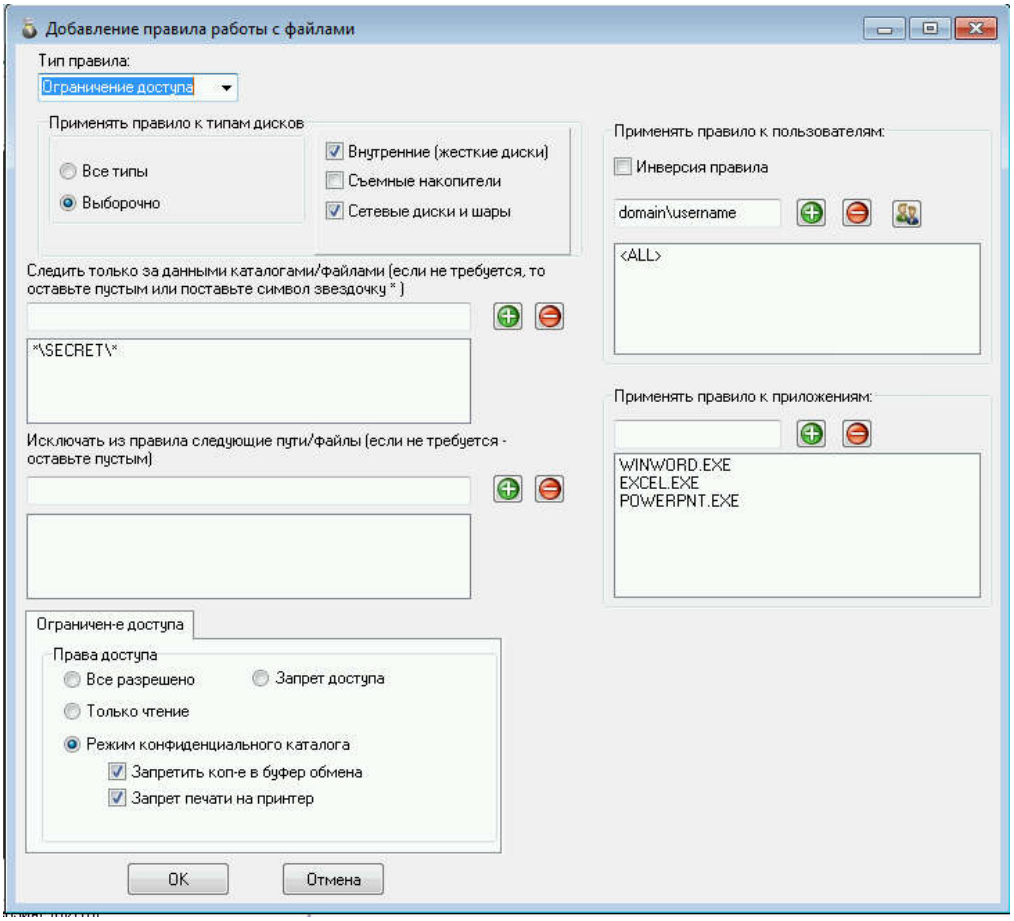
Необходимо обеспечить работу пользователя в специально созданном каталоге (для примера с именем secret) на расшаренном сетевом ресурсе на сервере в офисных приложениях (Word, Excel) так, чтобы он имел возможность редактировать файлы, но не мог скопировать их в другой каталог. И аналогично для такого же каталога на жестком диске компьютера.

Поскольку речь идет об офисном пакете и работе по сети, то для решения данной задачи потребуется три правила.

1). Первым правилом необходимо разрешить программам из офисного пакета доступ к каталогам
\Temporary internet files\content.mso
\microsoft.dot?
\local\temp
\MICROSOFT\WINDOWS.tmp



2). Задаем непосредственно правило ограничения доступа

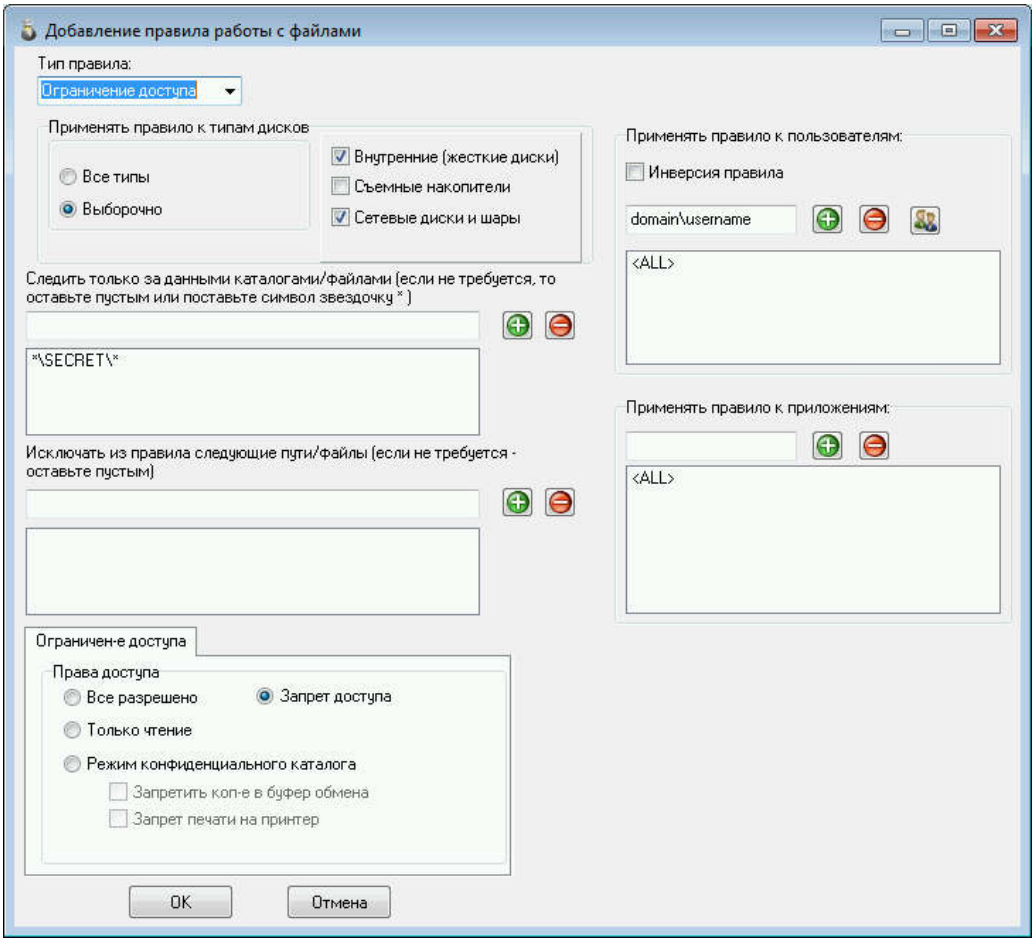


Для работы офисных пакетов добавляем в список программ, для которых действует правило: winword.exe, excel.exe, powerpnt.exe, …

Для работы PDF24 Creator: pdf24-creator.exe , pdf24-doctool.exe

Для работы autocad и autocad lt: acad.exe , acadlt.exe

3). Для того, чтобы нельзя было получить доступ к файлам в защищенном каталоге из сторонних программ, мы создаем третье правило, где запрещаем всем приложениям работу с защищенным каталогом.



ВАЖНО. Обратите внимание на то, что применение правил происходит сверху вниз, поэтому важна очередность их расположения в списке. Очередность правил определяется изначально порядком их создания, также их можно передвигать выше или ниже по списку правил специальными кнопками со стрелочками вверх и вниз.

Выполнится первое из правил, которое подойдет по условию. Т.е. если сначала разрешить программе доступ к файлу, а вторым правилом запретить доступ этой же программе к этому же файлу, то при запуске этой программы и открытии в ней файла, выполнится первое правило, разрешающее доступ, а второе исполняться не будет.

5.10 Настройка логирования файловых операций и теневого копирования в EnterpriseDLP

Создание данных правил происходит аналогично созданию правил ограничения доступа. Задается тип дисков, для которых будет действовать правило, можно задать конкретные каталоги и исключение из правил. Указать для каких учетных записей windows правило будет применяться.

Для правил логирования, рекомендуем задать список путей исключений:
\Application Data
\Sys_Data_KF
\Local Settings
\WINDOWS
\Program Files
\System Volume Information
* \AppData*
\ProgramData
*\ntuser.dat
\Program Files (x86)

Либо настраивать логирование файловых операций для конкретных каталогов. В противном случае, если в качестве адреса контроля задать просто * и не настроить исключений, количество перехваченных событий будет слишком большим и абсолютно не информативным.

5.11 Работа с технологией VDI

LanAgent Enterprise может работать и в том случае, когда применяется технология виртуальных рабочих станций VDI.

Для этого надо установить следящий модуль агента на "золотой образ" виртуальной машины, которая будет тиражироваться у пользователей. Для него же, следует провести и все требуемые настройки агента: какие данные собирать, частоту скриншотов, правила блокировки и т.д.

Кроме инсталляции агента, на образ также надо установить ключ реестра, содержащий IP адрес серверного компьютера и частоту передачи данных на него. Образец ключа выложен по ссылке: lanagent.ru/client.zip Частота передачи данных на сервер в нем выставлена каждые 5 минут.

В список мониторинга в LanAgent Admin надо будет добавить не компьютеры, а пользователей.

Удобно воспользоваться диалогом добавления терминальных пользователей. Далее, выберите вариант выбора пользователей домена. Из Active Directory будет подгружен список всех пользователей вместе с группами. Выберите интересующих пользователей и добавьте их в список.

Передача данных на сервер будет производиться по порту 47660 tcp/ip.

5.12 Настройка оповещений через Telegram

LanAgent позволяет использовать отправку сообщений в Telegram специалиста безопасности или администратора системы для оповещений о событиях безопасности и использования 2-х факторной авторизации.

Для того, чтобы это работало, потребуется:

1. Чтобы на компьютере с серверной частью LanAgent Enterprise был установлен и запущен сервис Web интерфейса (если у Вас он не установлен, то обратитесь в тех поддержку support@lanagent.ru)
2. Необходимо создать Telegram бота и сохранить в админке LanAgent его токен. Этот бот будет использоваться для рассылки. Мы специально не стали использовать созданного нами бота, чтобы через нас не проходили никакие Ваши данные.
3. После подключения бота, каждому пользователю интерфейса LanAgent (специалистам безопасности и администратору), которому требуется получать Telegram рассылку, надо будет активировать свою подписку на этого бота.

Создание Telegram бота

1. Запустить @BotFather (https://t.me/botfather) и получить базовый список команд для работы с ботами.

Первая и самая главная — /newbot, создание нового бота. Программа предложит нам придумать название нашему роботу.

2. Придумать название. Можно вписать любое имя, какое хочется. оно будет отображаться в контактах и чатах.

3. Придумать логин. Пишем боту придуманное название и он предлагает нам выбрать для бота логин. Программа предупредит, что логин должен заканчиваться на «bot».

Логин должен быть уникальным, программа не пропустит имя пользователя, если оно уже занято. А еще он должен быть написан на латинице (с цифрами и нижним подчеркиванием), содержать от 5 до 32 символов.

3. Сохранить токен. Бот-отец пришлет вам токен вашего бота. Сохраните его в текстовом файле, например, в блокноте. Это ключ для доступа к HTTP API, с помощью которого вы будете программировать робота, получать и отправлять сообщения.

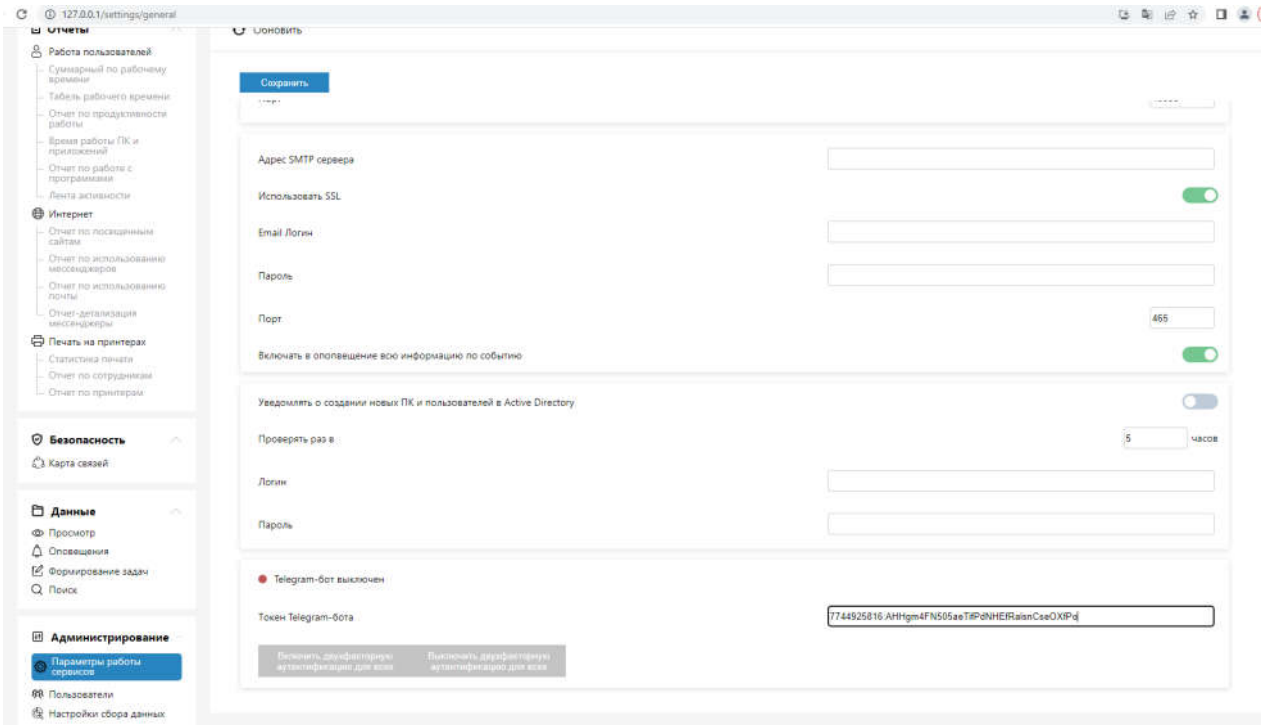
Запомнить получится вряд ли, выглядит он примерно вот так: 7744925816:AHHgm4FN505aeTifPdNHEfRaisnCseOXfPo

4. Необязательный пункт. Можно добавить аватар, описание, приветственное сообщение. Жмем /help и получаем перечень базовых команд.

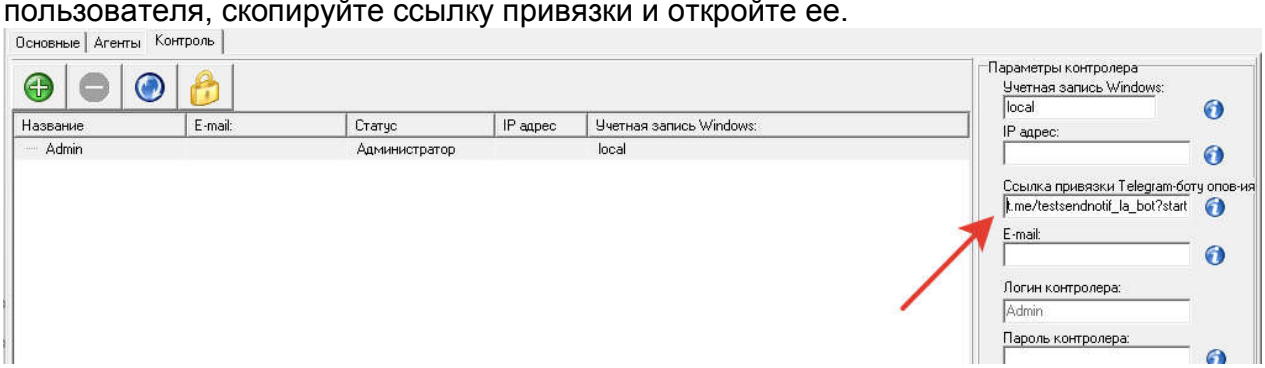
Тут будут в том числе команды для изменения описания (/setdescription), информации о боте (/setabouttext), для загрузки аватара (/setuserpic) и другие.

ГОТОВО!

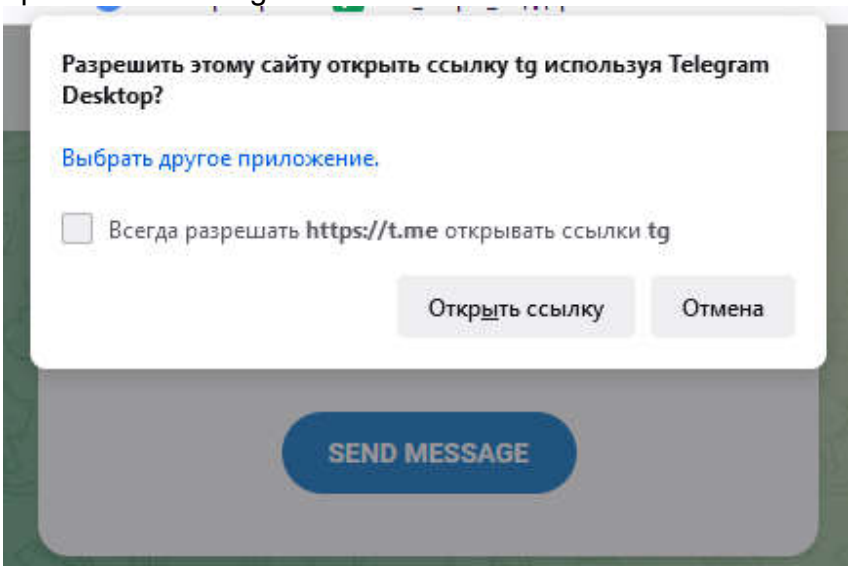
Полученный токен надо ввести в админке на вкладке настроек Основные в классической консоли или на пункте меню «Параметры работы сервисов» в веб интерфейсе.



После сохранения токена бота, в свойствах пользователей LanAgent появится ссылка для подписки на оповещения от этого бота.
В приложении админки перейдите на вкладку Контроль, выберите нужного пользователя, скопируйте ссылку привязки и откройте ее.

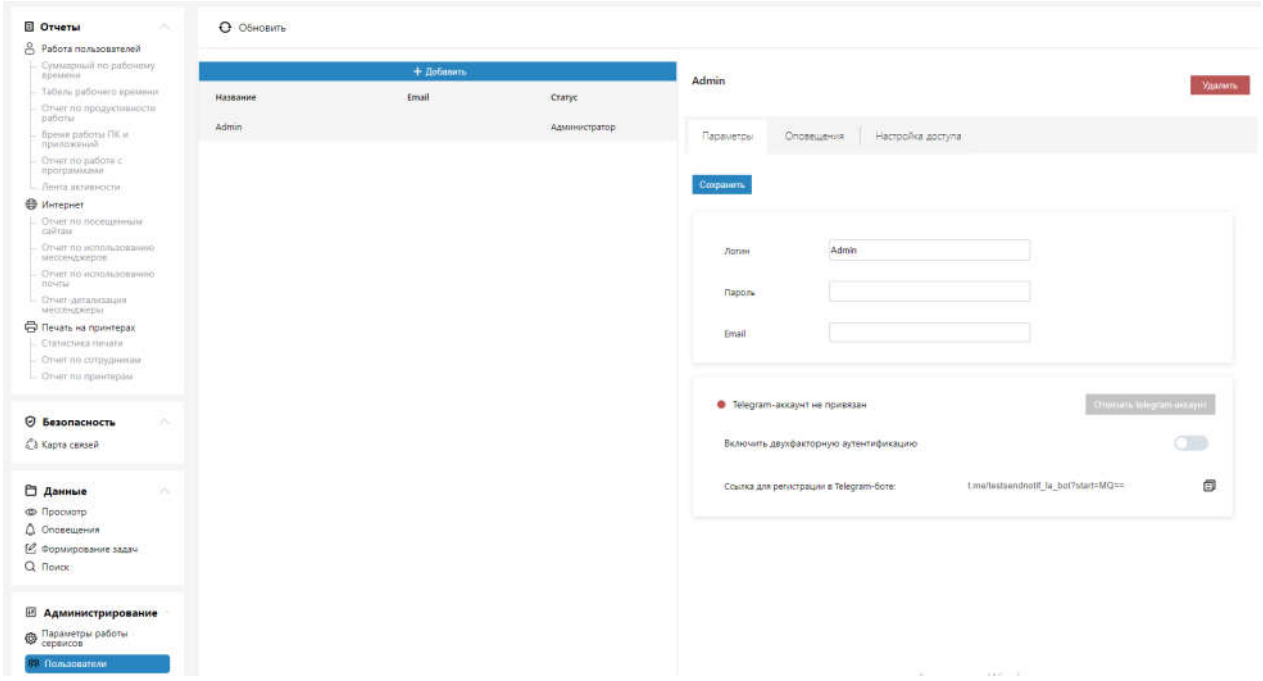


Если открыть ссылку в браузере, Вам будет предложено использовать открыть ее в приложении Telegram.

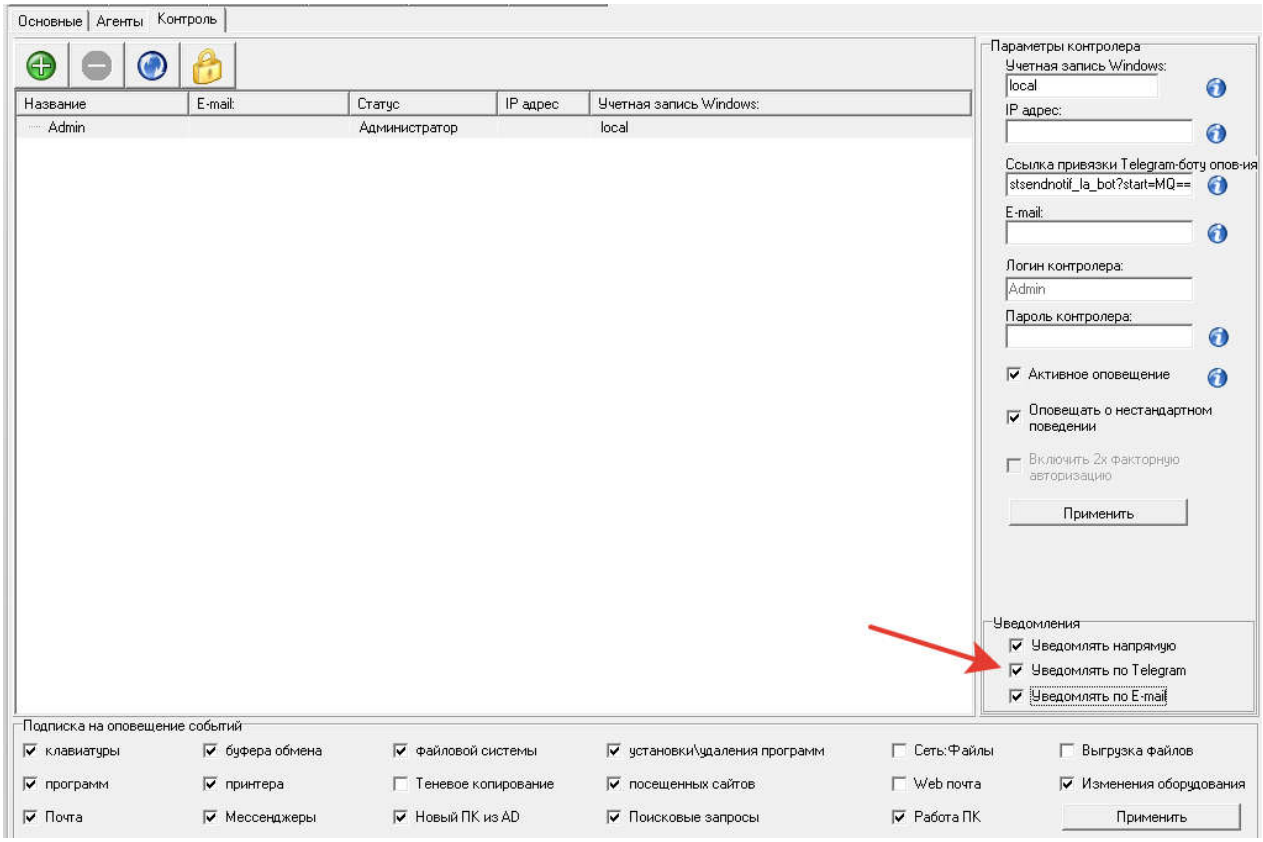


В Telegram откроется чат с созданными вами ранее ботом. Для подписки на оповещения от него достаточно передать ему команду /start

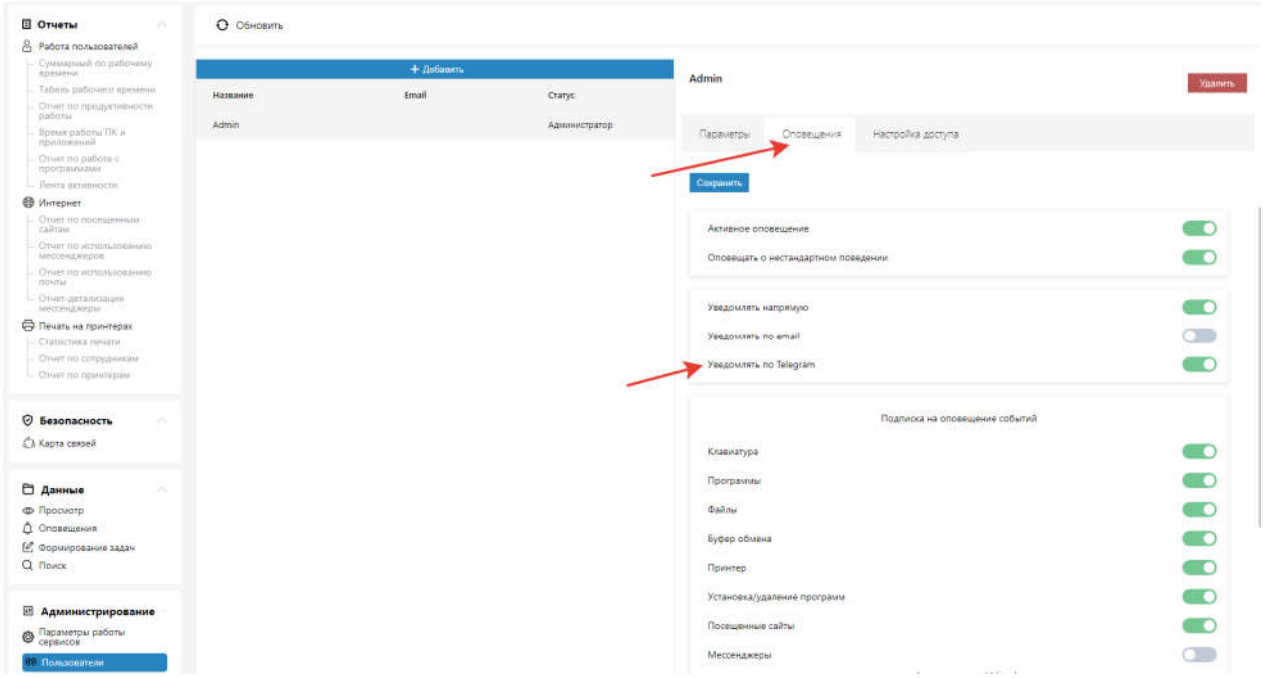
В Web интерфейсе ссылка расположена в пункте меню Пользователи:



Последний штрих для получения уведомлений на Telegram, это включить данную опцию уведомления.
В приложении LA Admin это делается также на вкладке Контроль для выбранного пользователя:



В Web интерфейсе эта настройка расположена на соседней вкладке:

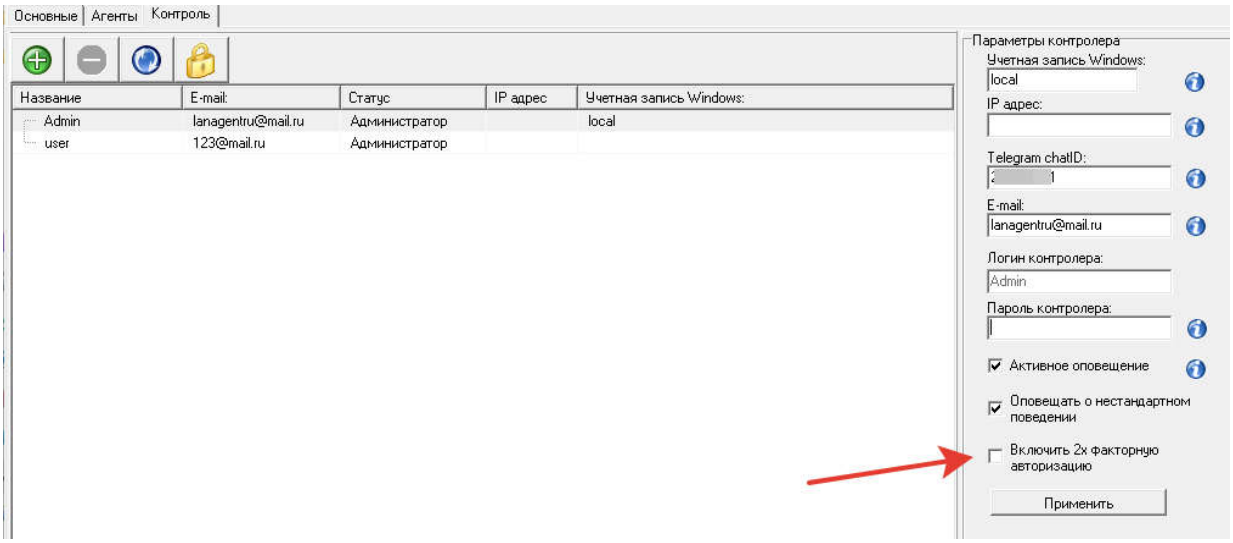


5.13 Включение 2-х факторной авторизации

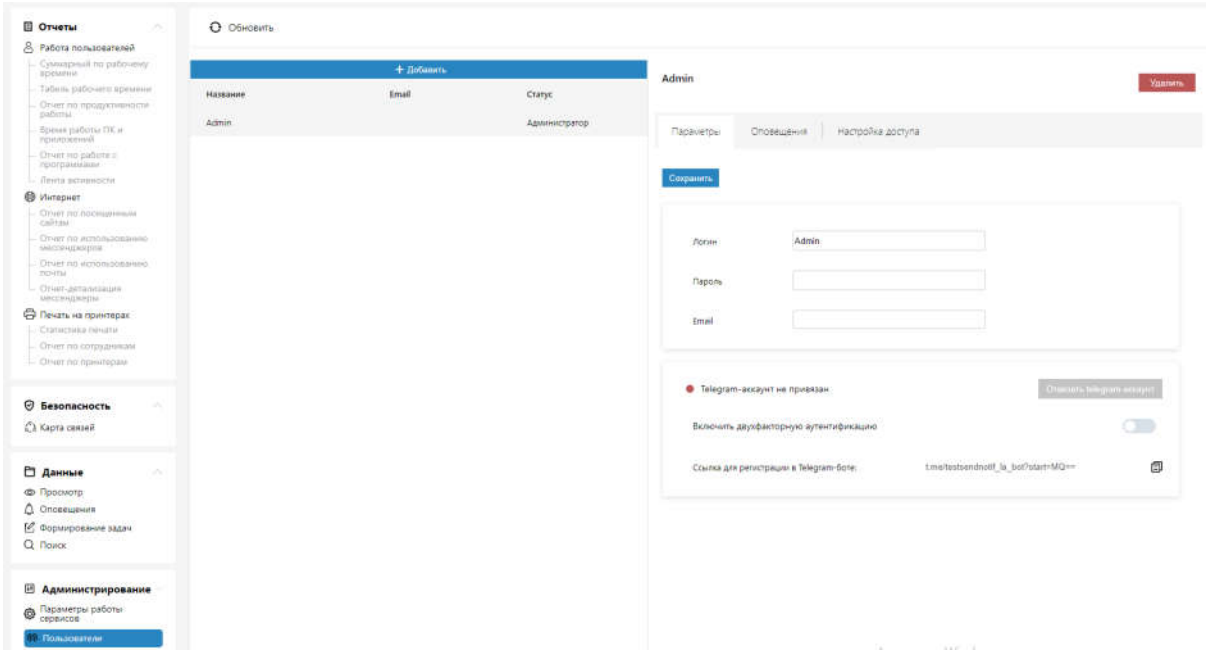
LanAgent позволяет использования 2-х факторную авторизацию посредством отправки кода подтверждения на Telegram.

Для этого необходимо иметь установленный и запущенный сервис Web интерфейса, а также подключить Telegram бота и подписаться на него каждому пользователю LanAgent, которому надо получать такую рассылку. Подробно процесс настройки оповещения и подключения бота описан в предыдущем пункте, 5.12.

Когда настройки Telegram бота проведены, для включения 2-х факторной авторизации, достаточно поставить соответствующую галочку в админке.



В веб интерфейсе настройка аналогична:



При включенной 2-х факторной авторизации зайти в приложения LA Admin, LA Viewer, а также в Web интерфейс можно будет только введя правильные логин и пароль, а также правильный код авторизации. Код присылается на telegram авторизующегося пользователя LanAgent.

6 Работа с LanAgent View

Интерфейс программы LanAgent View включает в себя следующие элементы:

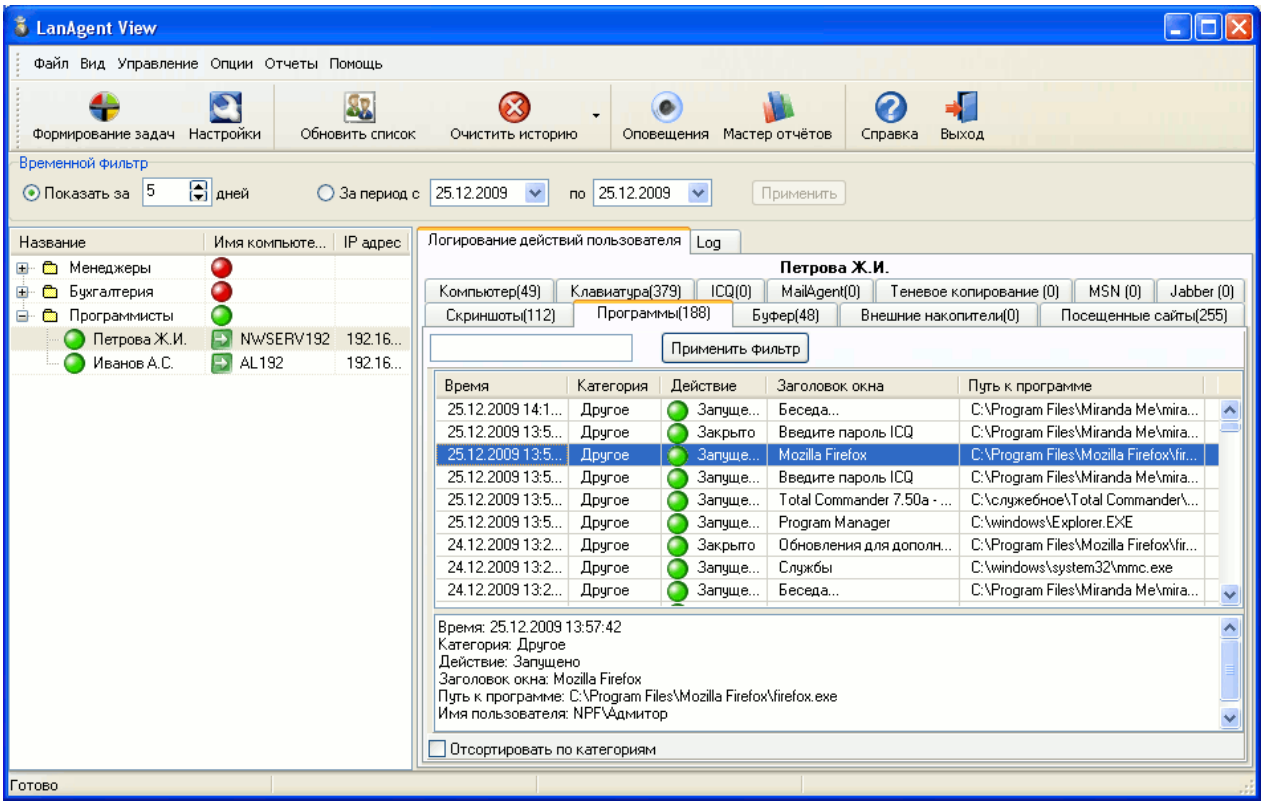


Рис. 6.1 – Главное окно программы

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

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

6.1 Список компьютеров для мониторинга

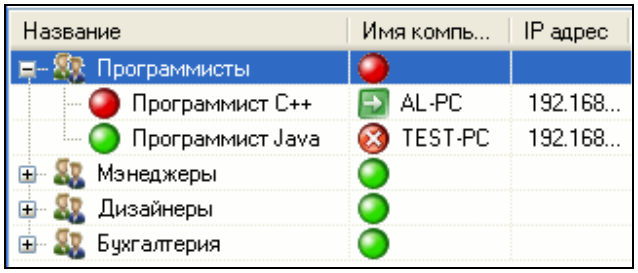


Рис. 6.2 – Окно списка мониторинга

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 (это производится при помощи программы LanAgent Enterprise Admin).

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

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

Таблица состоит из следующих столбцов:

- **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.

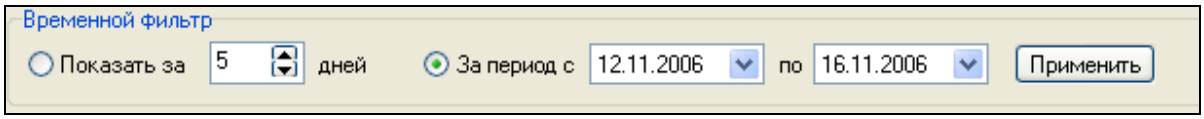
6.2 Окно просмотра истории активности контролируемых компьютеров

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

- Клавиатура (хранит текст, набираемый пользователем на клавиатуре);
- Скриншоты (содержит список произведенных снимков экранов мониторов);
- Программы (история запуска и закрытия программ);
- Буфер (хранит текст, копируемый пользователями в буфер обмена);
- Файлы (содержит статистику создания, удаления и переименовывания файлов);
- Принтер (перечень документов, отправленных на печать на принтер);
- Установленные программы (история установки и удаления программ);
- Внешние накопители (хранит события подключения и отключения носителей информации);
- Посещенные сайты (перечень посещенных пользователями сайтов);
- Компьютер (история включения и выключения компьютеров пользователей);
- Мессенджеры текст;
- Мессенджеры аудио+файлы;
- Теневое копирование (список файлов, скопированных пользователем на съемный usb накопитель);
- Почта (письма, отправленные пользователем через почтовые клиенты (Outlook, Outlook Express, …));
- Сеть (обращения к общим ресурсам компьютера и к файлам, расположенным на общих ресурсах);
- Web почта (письма, отправленные пользователем через веб интерфейс);

- Выгрузка файлов (файлы выгруженные пользователем в Интернет, а также параметры, отправленные по запросам web сайтов);
- Соц. сети;
- Webcam/microphone (видео и аудио записи, выполненные через веб камеру или микрофон, подключенный к контролируемому ПК);
- Изменения оборудования (история изменения комплектующих компьютера)

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



6.2.1 Клавиатура

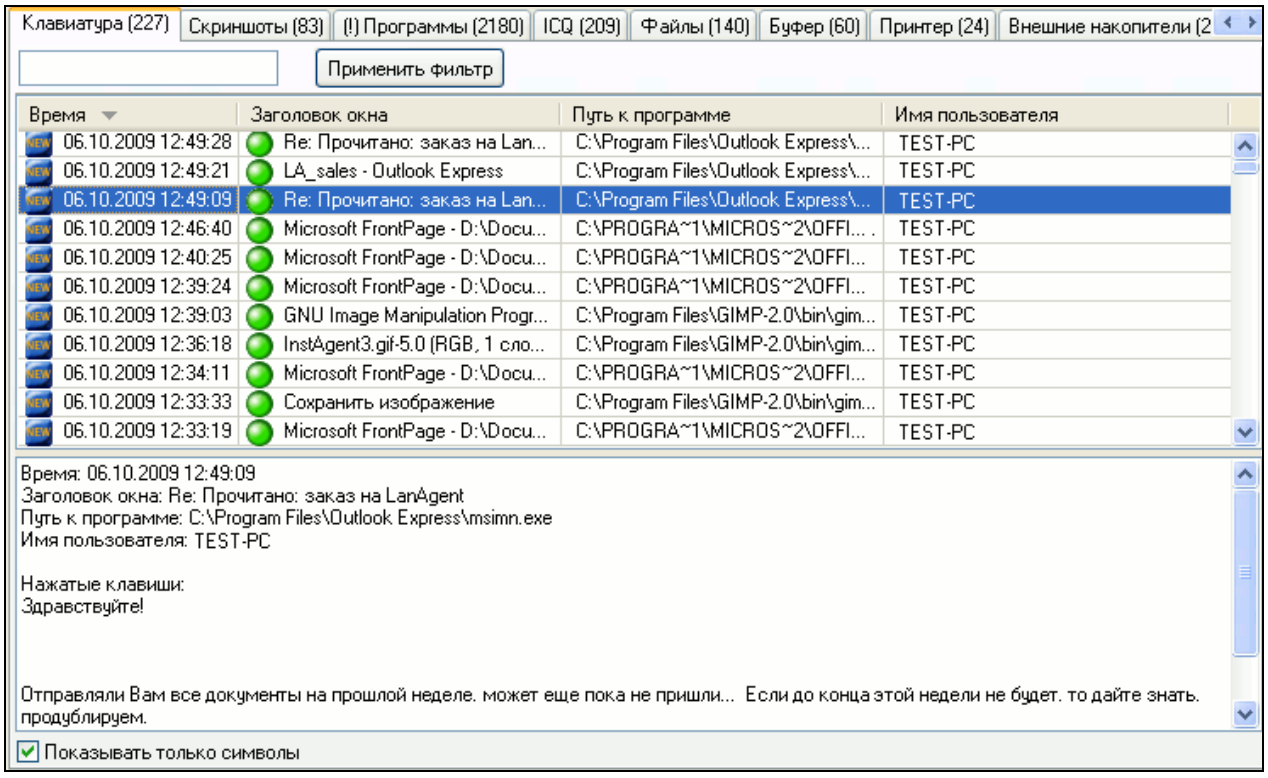


Рис. 6.3 – Окно логов клавиатуры

На этой странице находится информация по нажатым на клавиатуре клавишам, что позволяет, например, просмотреть текст, набранный пользователем. В заголовке закладки в скобках указано количество записей в таблице. Данные в таблице могут быть отсортированы по любому из столбцов, например по убыванию времени (то

есть последняя информация содержится вверху таблицы). В таблице содержится следующая информация: дата и время нажатия клавиш, заголовок окна и полный путь к программе, где набиралась информация, а также имя пользователя. Для перемещения по таблице можно пользоваться как мышкой, так и стрелками курсора. В текстовом поле под таблицей отображается вся информация из таблицы по данной записи для более удобного просмотра, а также нажатые клавиши. Соотношение высоты таблицы и текстового поля можно изменять. Для этого надо поместить курсор мыши на границе таблицы и текстового поля (при этом курсор изменит вид), прижать левую кнопку мыши и потянуть вверх или вниз.

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

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

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

"Регистрирует все нажатия клавиш"

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

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".

6.2.2 Скриншоты

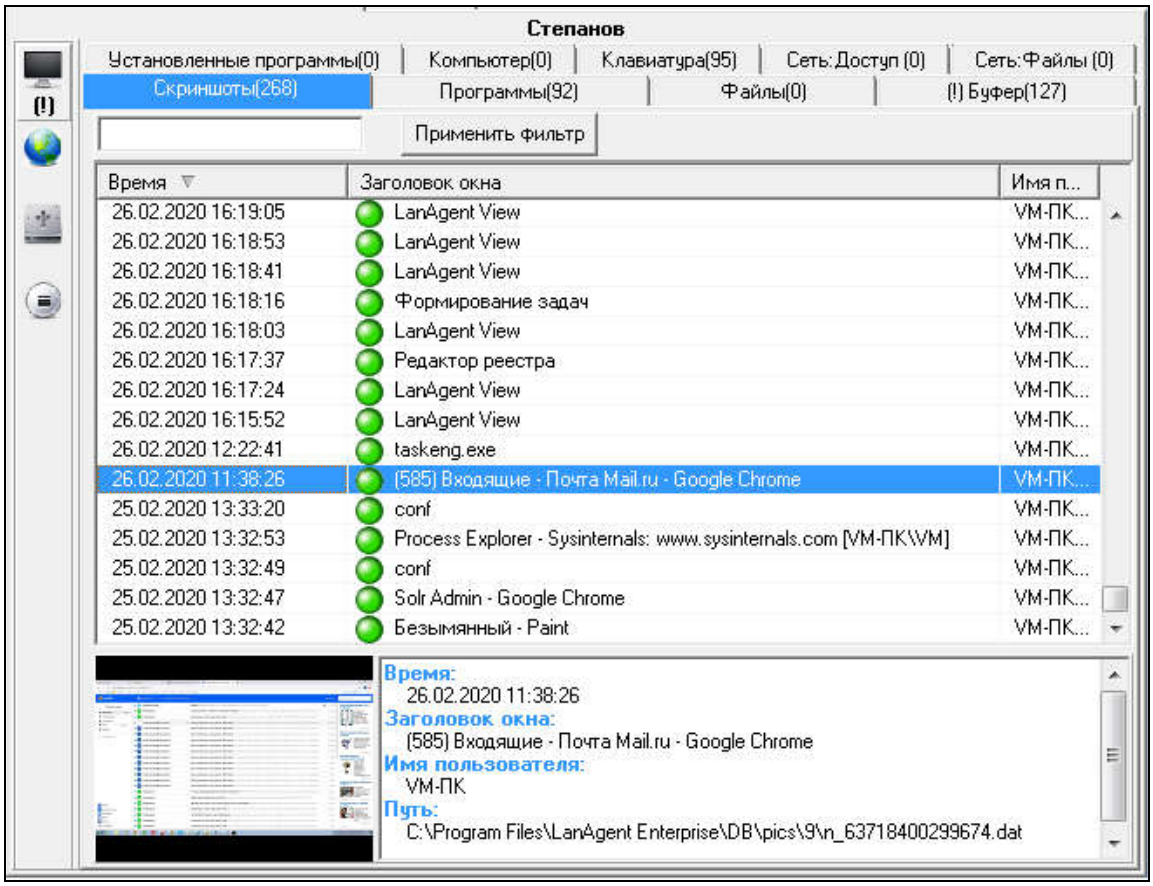


Рис. 6.4 – Окно логов снимков экранов (скриншотов)

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

Соотношение высоты таблицы и текстового поля можно изменять. Для этого надо поместить курсор мыши на границе таблицы и текстового поля (при этом курсор изменит вид), прижать левую кнопку мыши и потянуть вверх или вниз.

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

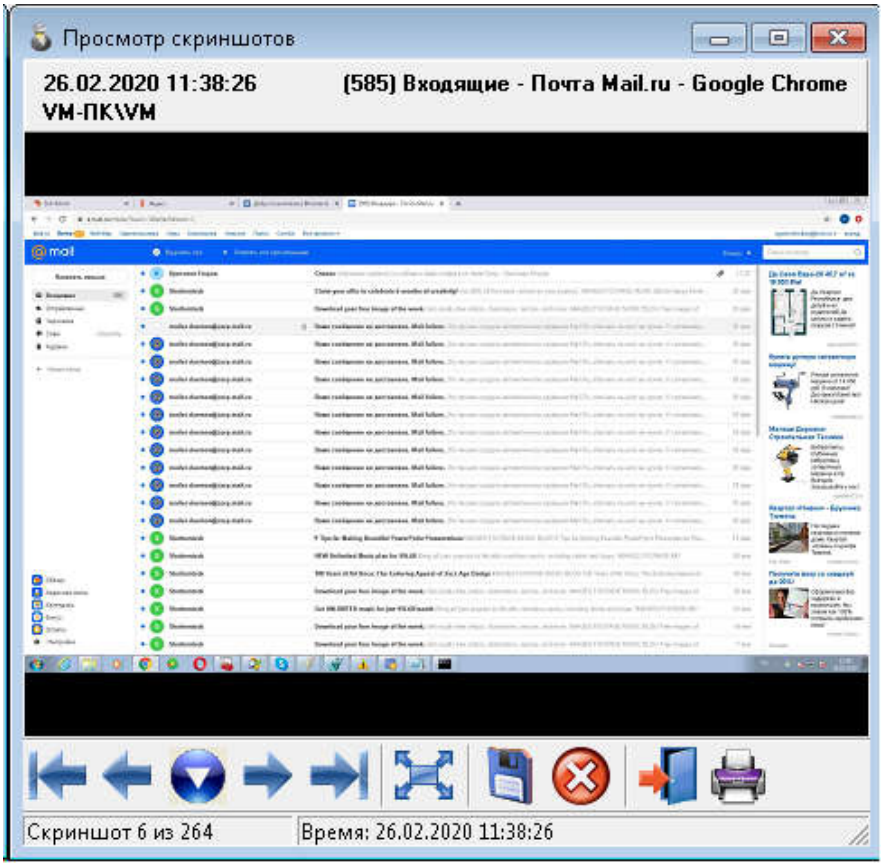


Рис. 6.5 – Окно просмотра скриншотов

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

Назначение кнопок панели инструментов:

 - переместиться к первому скриншоту (в начало).

 - показать предыдущий скриншот.

 - показать следующий скриншот.

 - переместиться к последнем скриншоту (в конец).

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

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

 - удалить скриншот.

 - удалить все скриншоты.

 - закрыть окно просмотра скриншотов.

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".

6.2.3 Программы

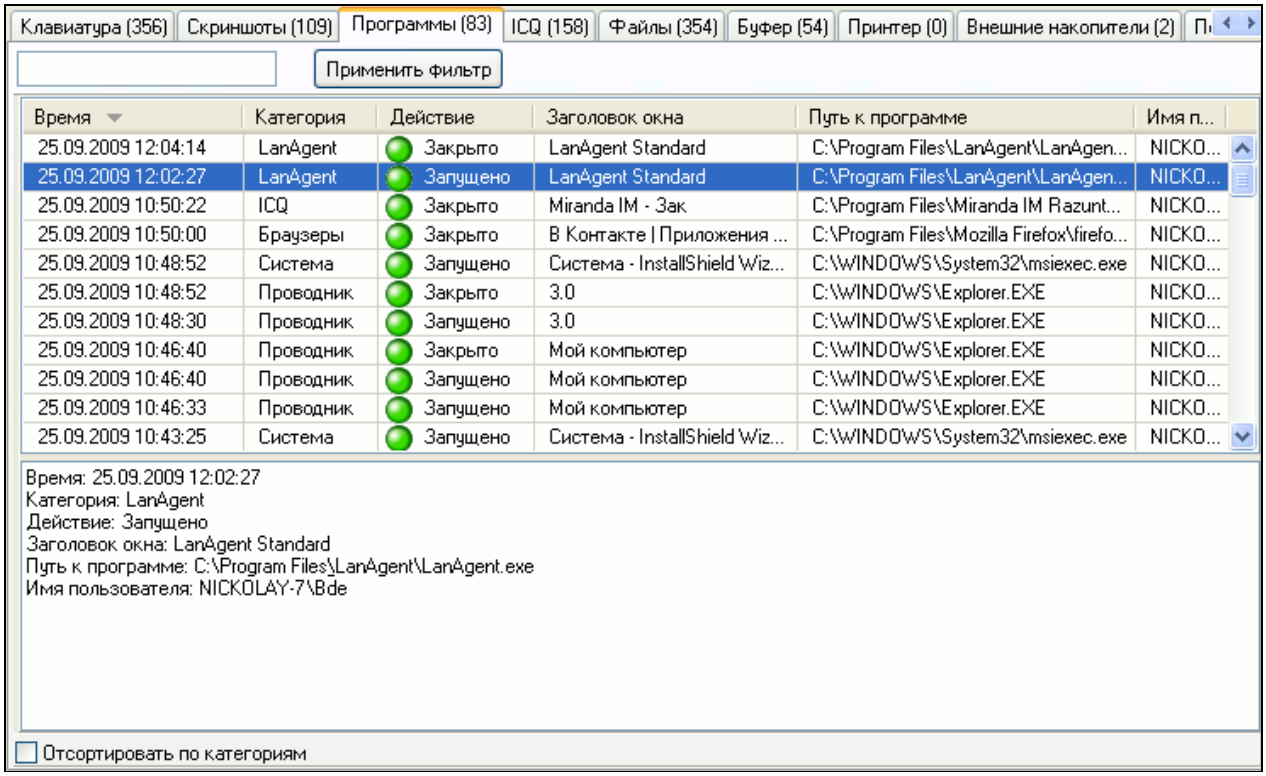
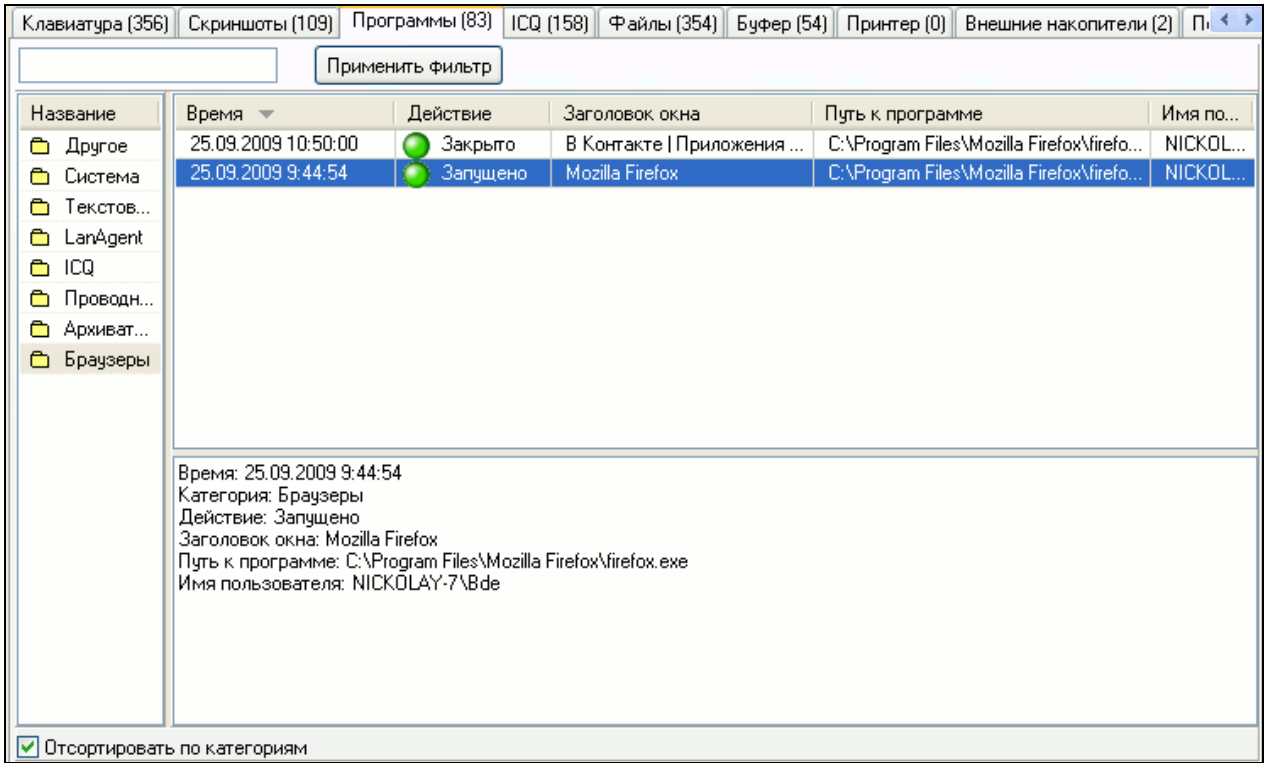


Рис. 6.6 – Окно логов программ

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

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



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".

6.2.4 Буфер обмена

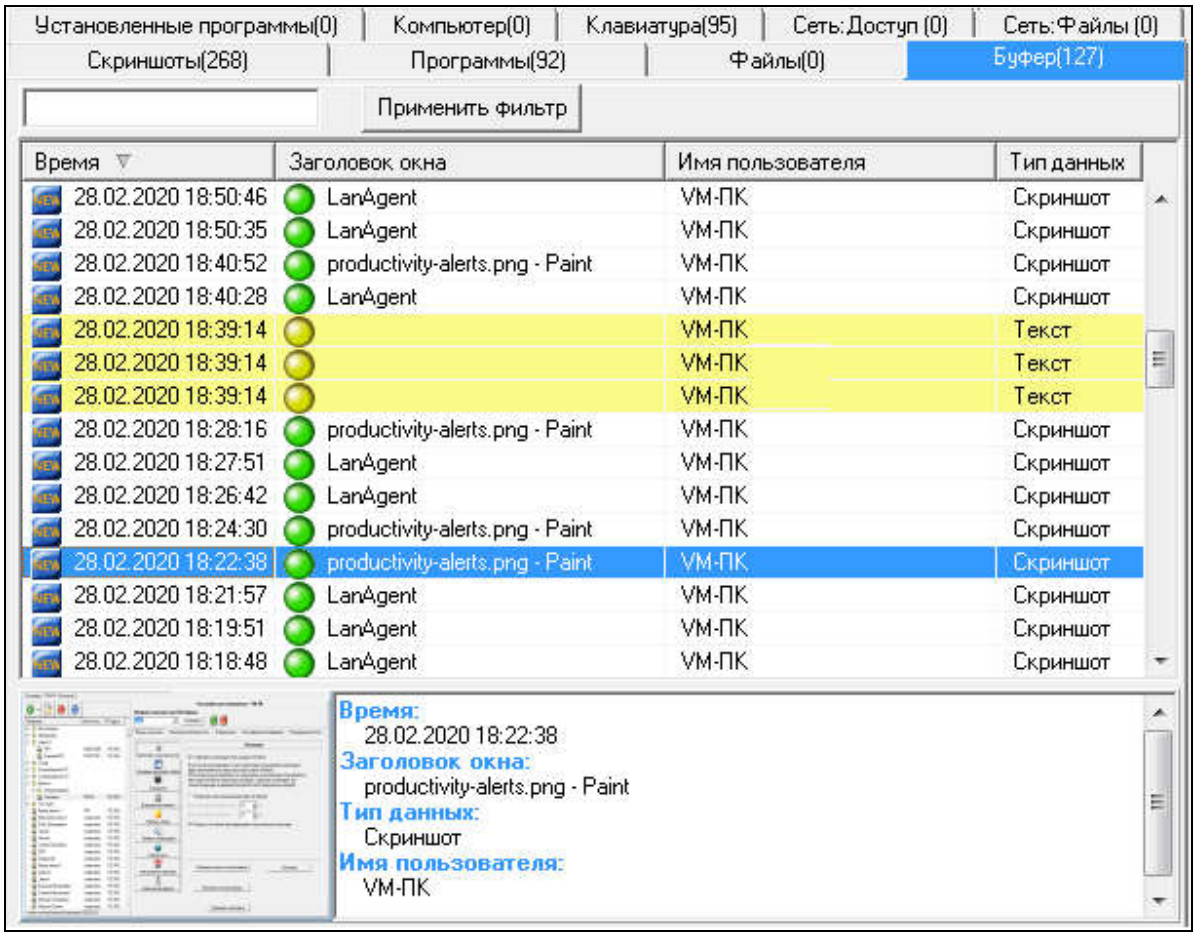


Рис. 6.7 – Окно логов буфера обмена

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

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

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".

6.2.5 Файлы

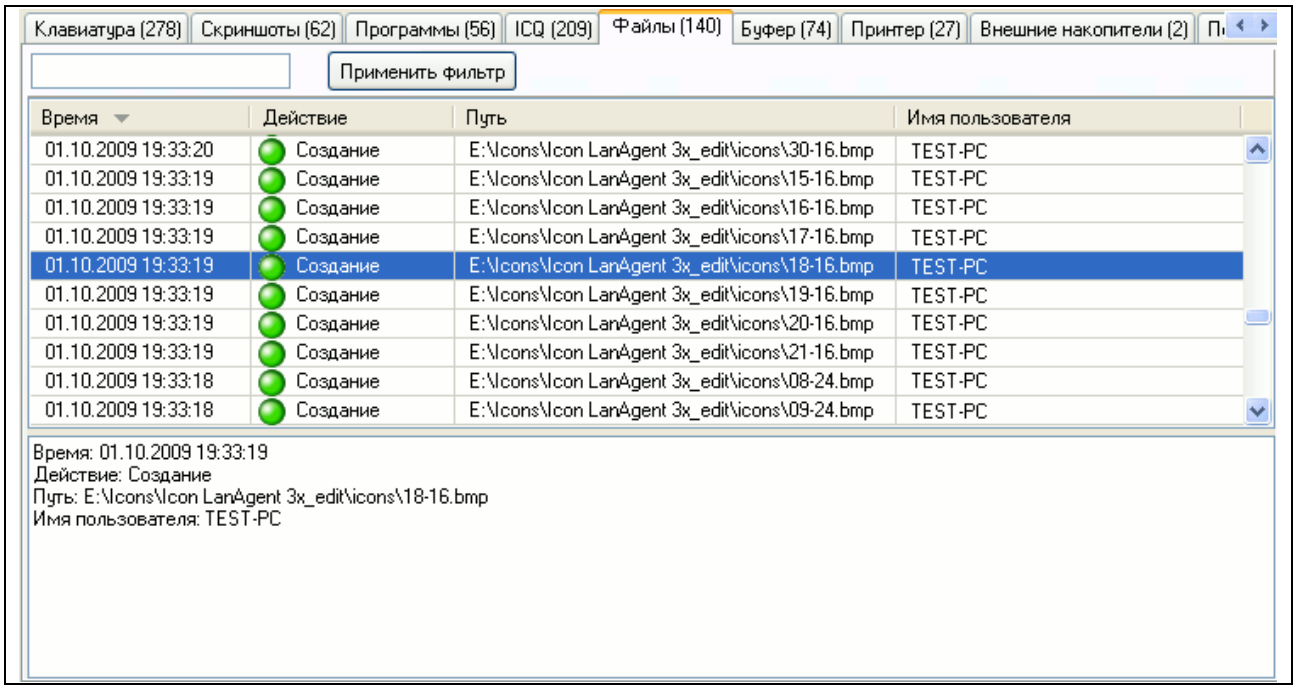


Рис. 6.8 – Окно статистики создания/удаления файлов

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

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

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

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".

6.2.6 Принтер

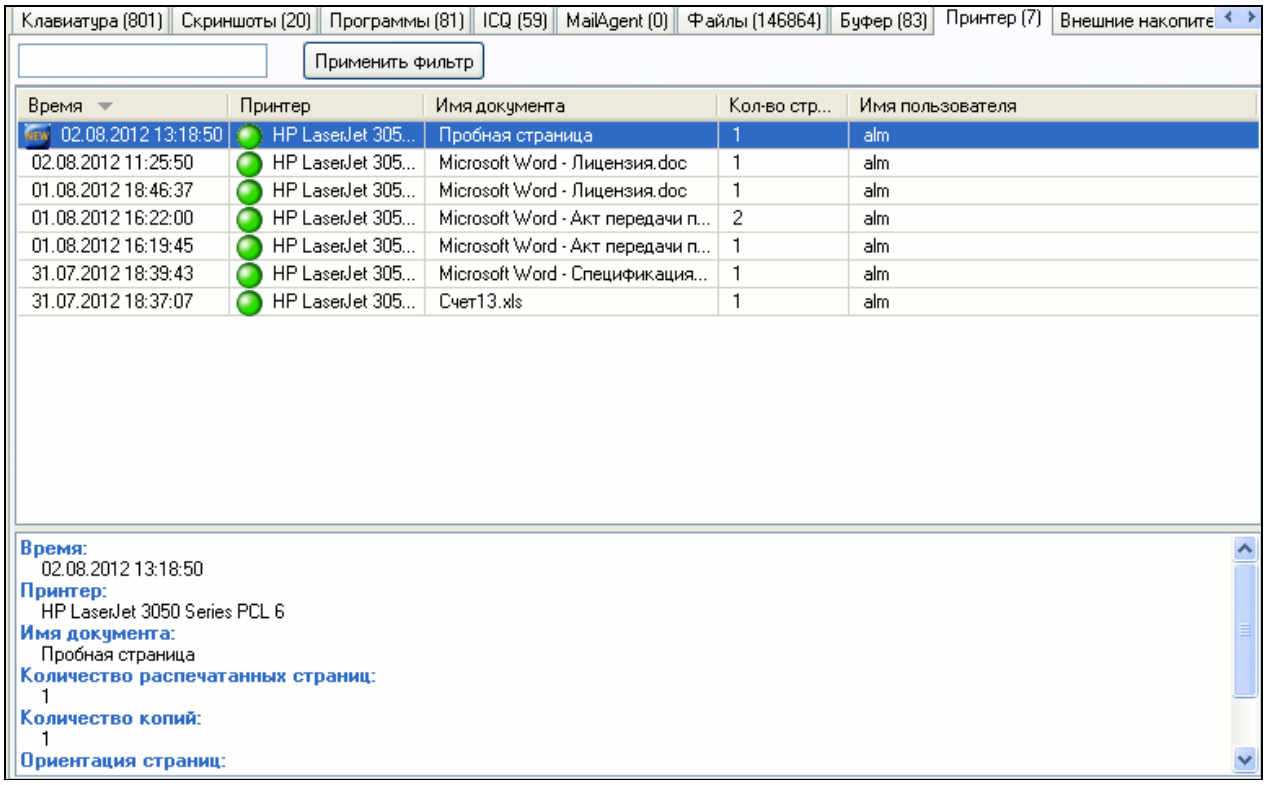


Рис. 6.9 – Окно логов принтеров

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

Для просмотра изображения напечатанного документа, кликните дважды в таблице по той записи, для которой хотите просмотреть содержимое. При этом документ откроется в программе, настроенной для просмотра PDF файлов.

6.2.7 Установленные программы

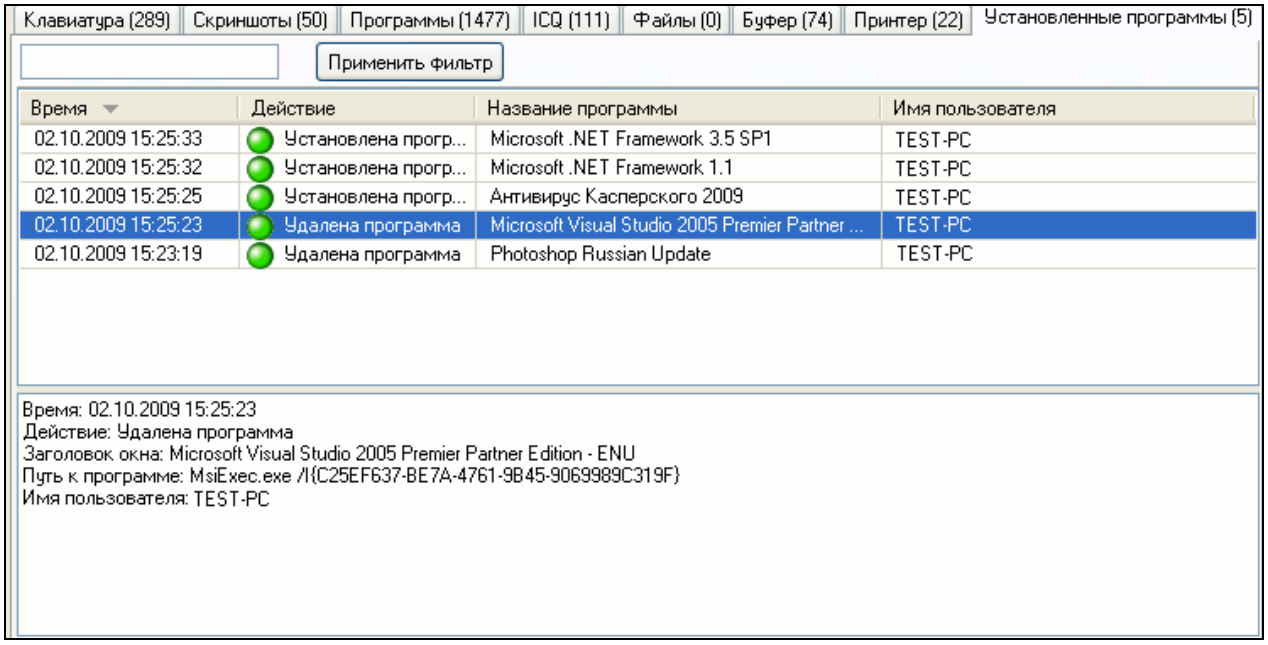


Рис. 6.10 – Окно логов установки/удаления программ

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

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

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

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".

6.2.8 Внешние накопители

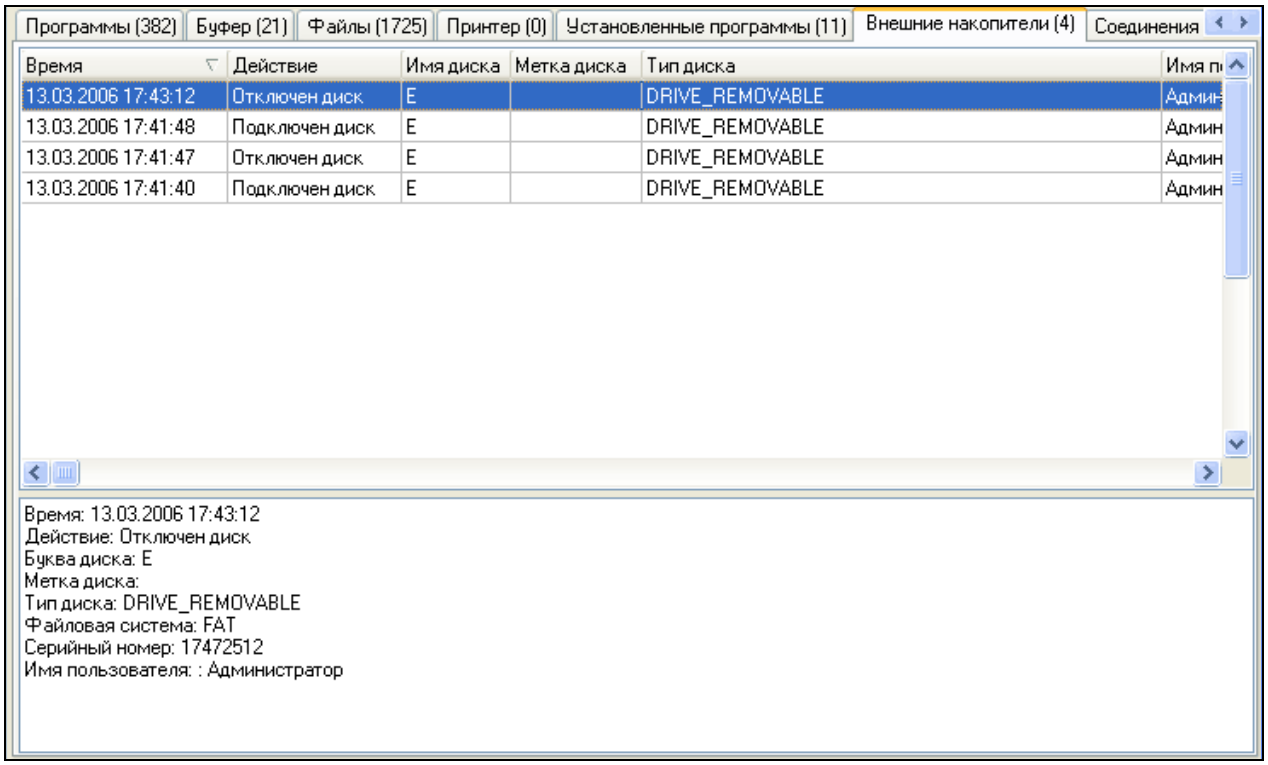


Рис. 6.11 – Окно логов подключения/отключения носителей информации

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".

6.2.10 Посещённые сайты

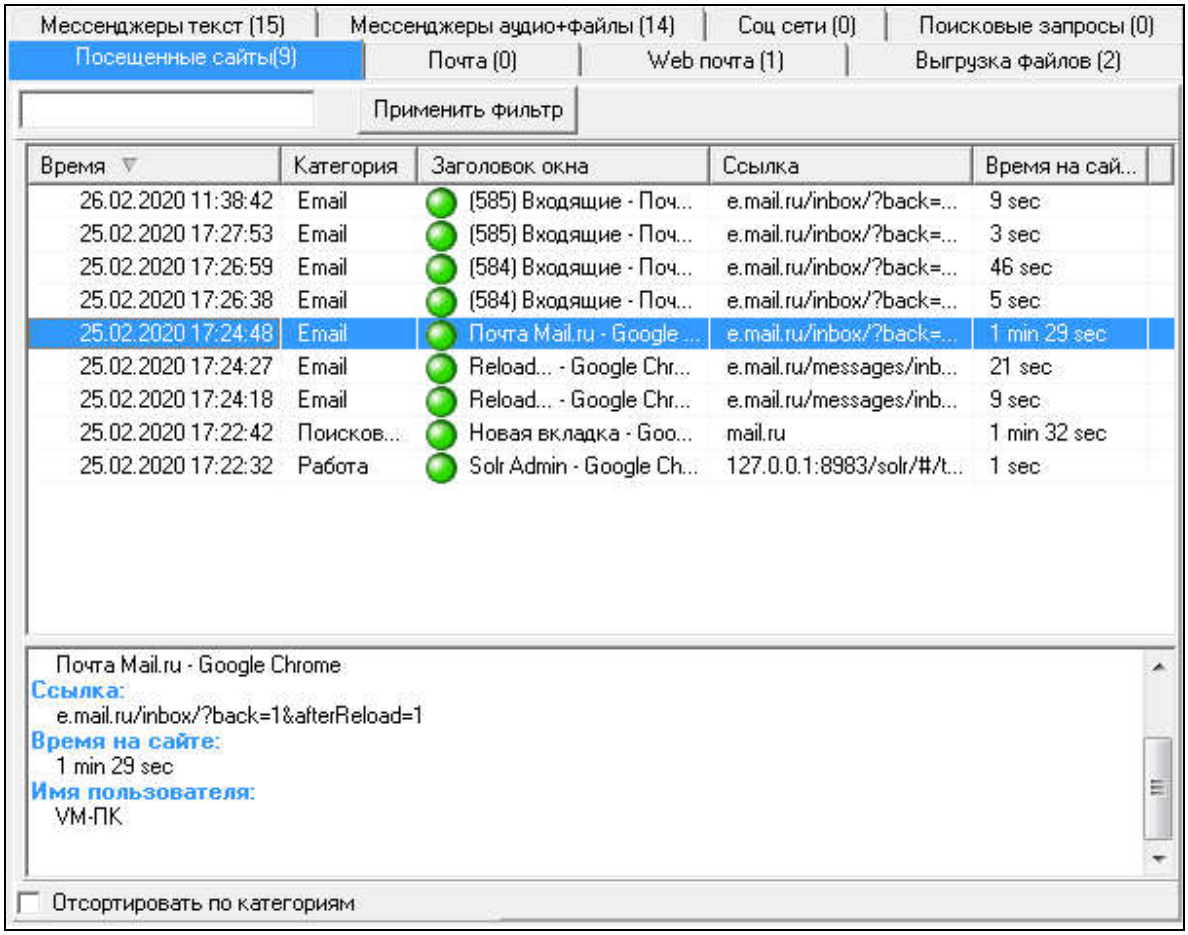
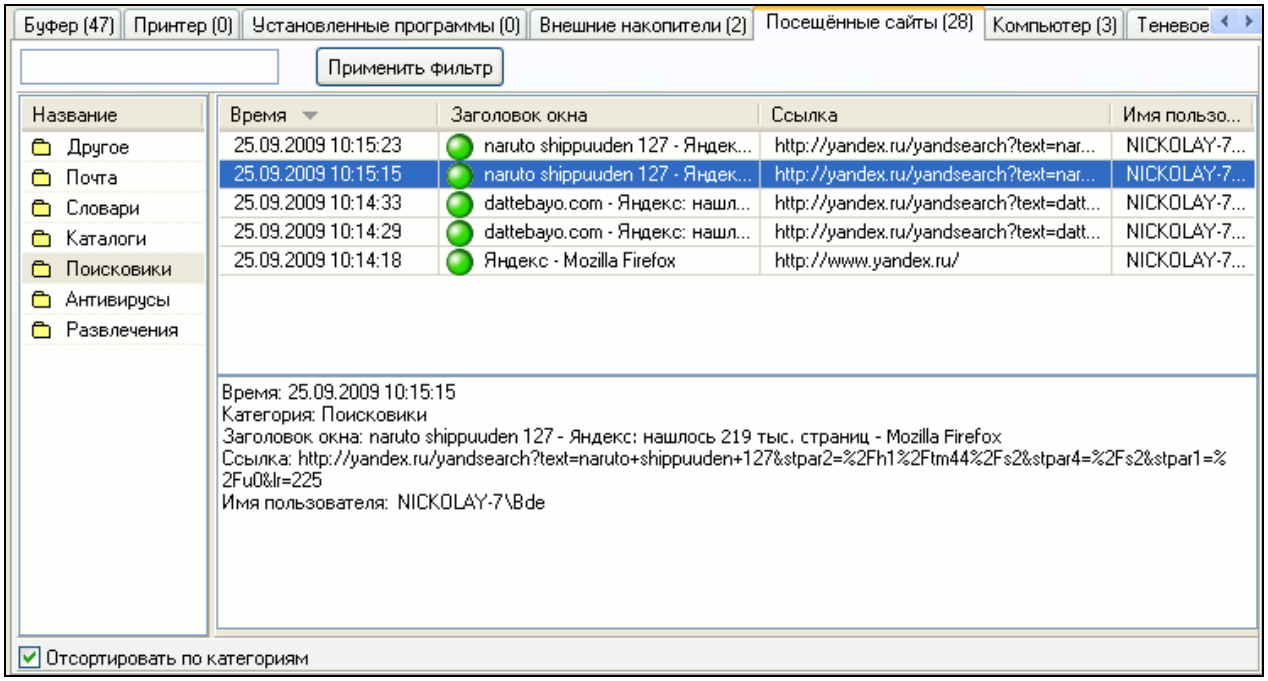


Рис. 6.13 – Окно логов посещенных сайтов

На этой странице находится информация о посещённых веб-сайтах. В заголовке закладки в скобках указано количество записей в таблице. Данные в таблице могут

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

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



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".

6.2.11 Компьютер

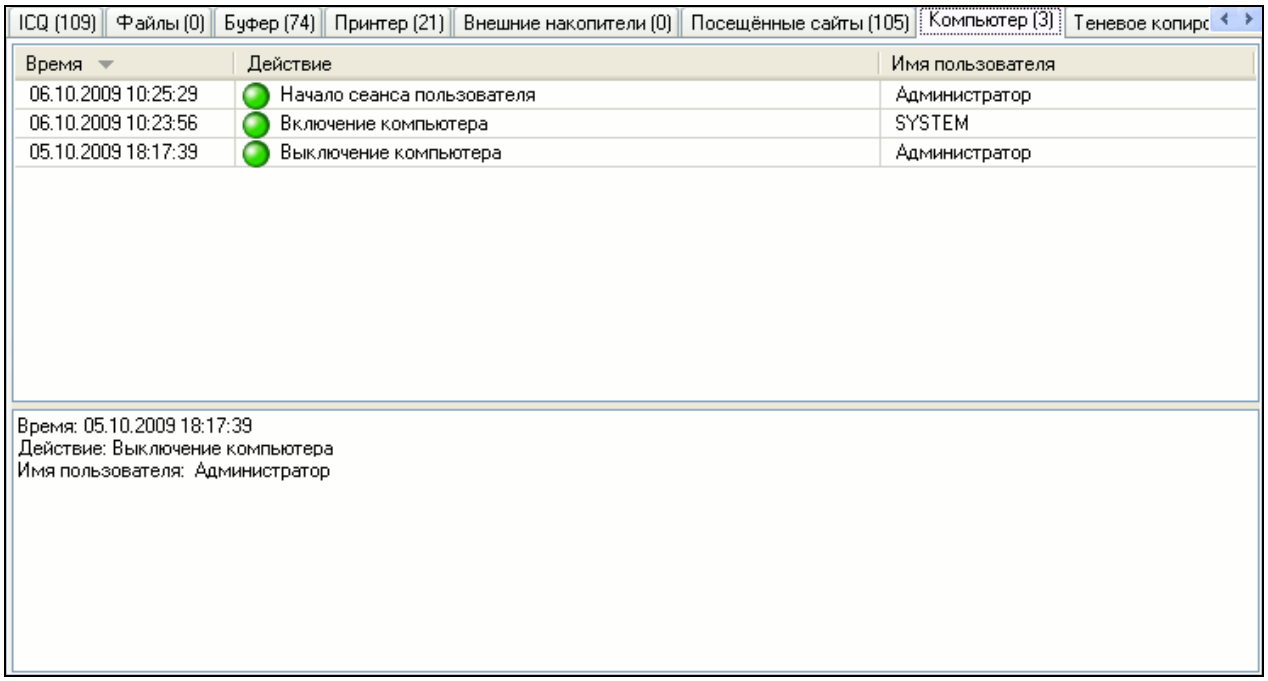


Рис. 6.14 – Окно статистики включения/выключения компьютера

На этой странице находится история включений/выключений контролируемых компьютеров. В заголовке закладки в скобках указано количество записей в таблице. Данные в таблице могут быть отсортированы по любому из столбцов, например по убыванию времени (то есть последняя информация содержится вверху таблицы). В таблице содержится следующая информация: дата и время включения или выключения компьютера, какое конкретно действие было произведено (включён компьютер или выключен), а также имя пользователя. Для перемещения по таблице можно пользоваться как мышкой, так и стрелками курсора. В текстовом поле под таблицей отображается вся информация из таблицы по данной записи для более удобного просмотра. Соотношение высоты таблицы и текстового поля можно изменять. Для этого надо поместить курсор мыши на границе таблицы и текстового поля (при этом курсор изменит вид), прижать левую кнопку мыши и потянуть вверх или вниз.

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

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".

6.2.12 Мессенджеры текст

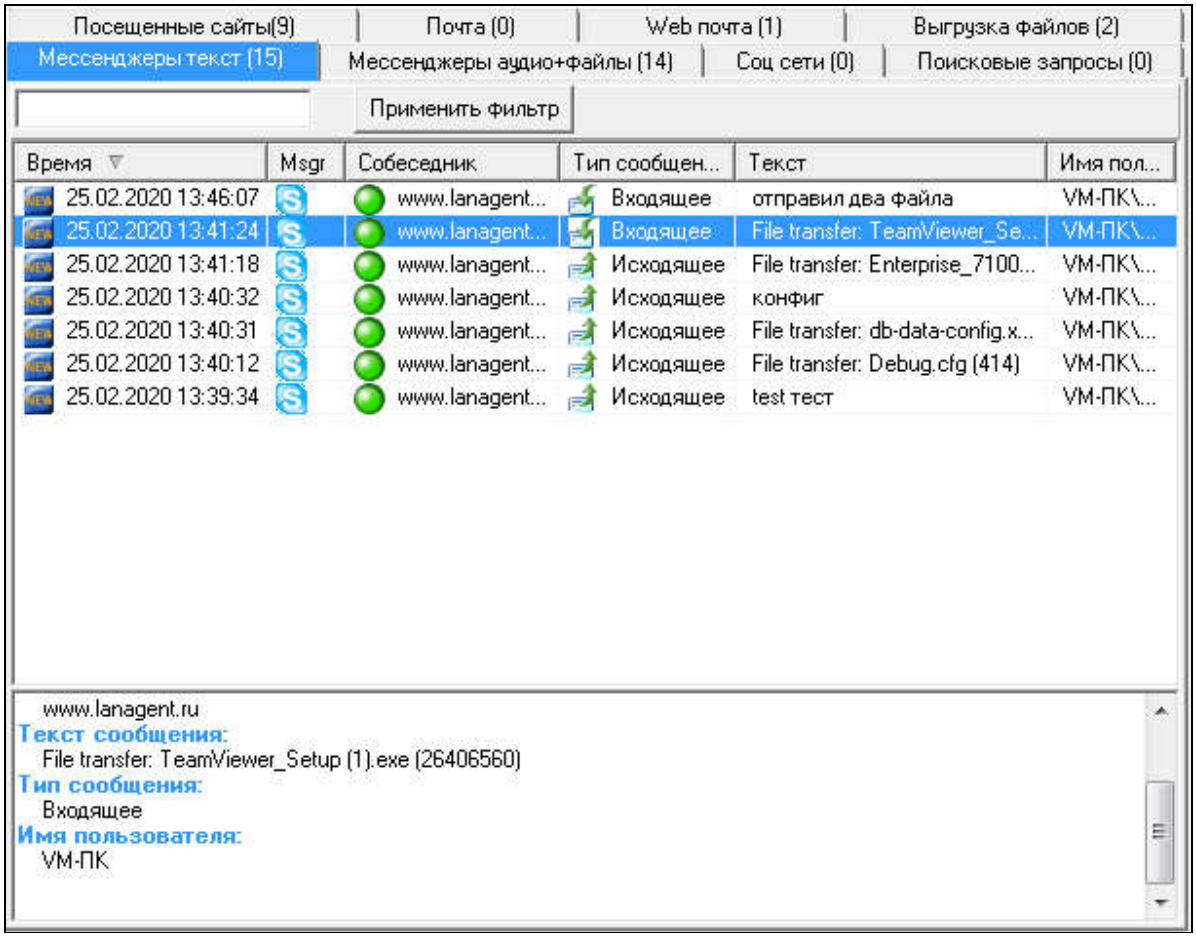


Рис. 6.15 – Окно статистики ICQ

На этой странице находится информация по перехваченным в мессенджерах сообщениям. 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.

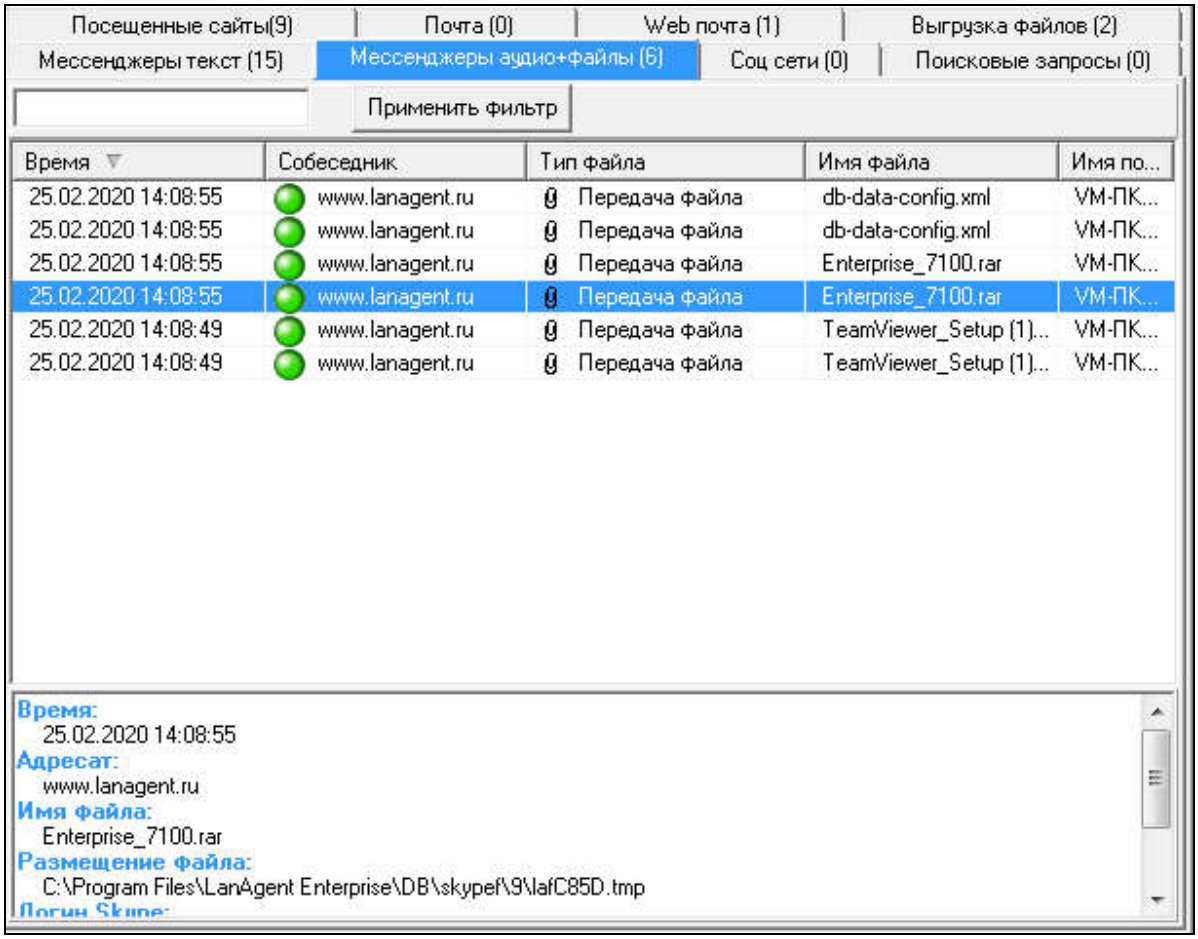
В текстовом поле под таблицей отображается вся информация из таблицы по данной записи для более удобного просмотра. Соотношение высоты таблицы и текстового поля можно изменять. Для этого надо поместить курсор мыши на границе таблицы и текстового поля (при этом курсор изменит вид), прижать левую кнопку 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".

6.2.13 Мессенджеры Файлы и аудио



На этой странице находится информация по голосовым сообщениям (звонкам) мессенджеров, таких как Skype, например, а также передаче файлов через них.

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.

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.

6.2.14 Теневое копирование

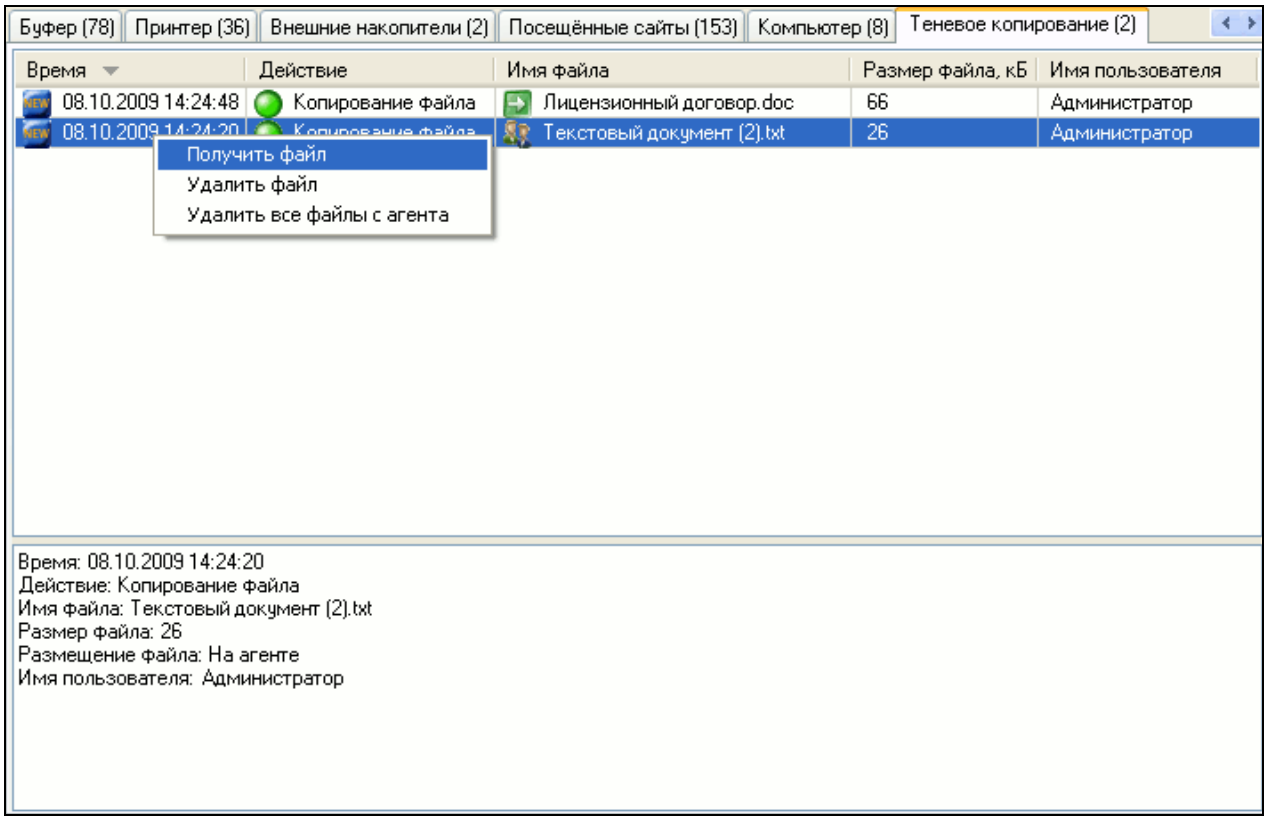


Рис. 6.16 – Окно статистики теневого копирования

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,

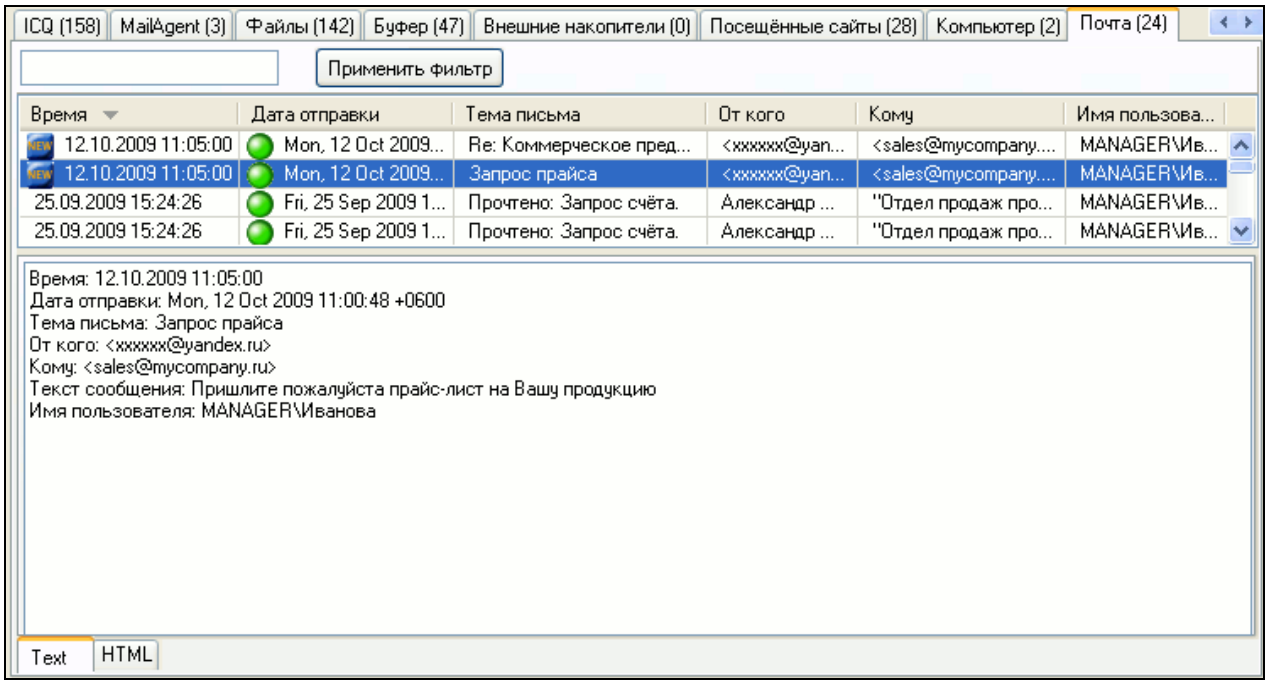
например по убыванию времени (то есть последняя информация содержится вверху таблицы). В таблице содержится следующая информация: дата и время копирования или модификации файла, какое действие было произведено (копирование или модификация), имя файла, размер файла, а также имя пользователя. Для перемещения 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 откроется окно диалога сохранения файла. Укажите в нем куда его сохранить. Если файл не представляет интереса, то его можно удалить.

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".

6.2.15 Почта

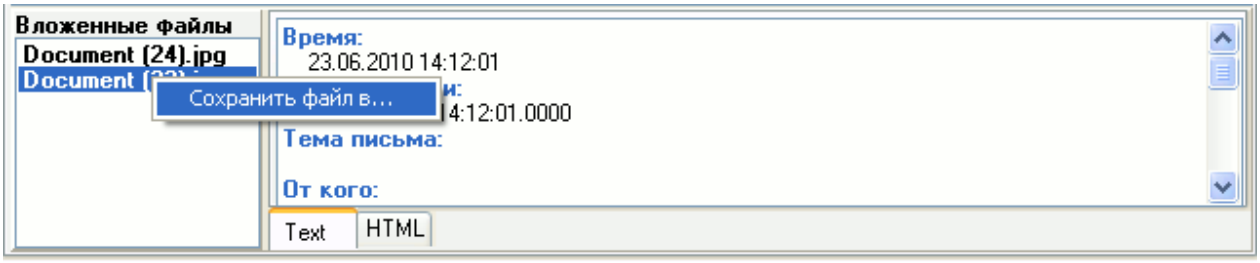


На этой странице находится информация по перехваченным электронным письмам. В заголовке закладки в скобках указано количество записей в таблице. Данные в таблице могут быть отсортированы по любому из столбцов, например по убыванию времени (то есть последняя информация содержится вверху таблицы). В таблице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

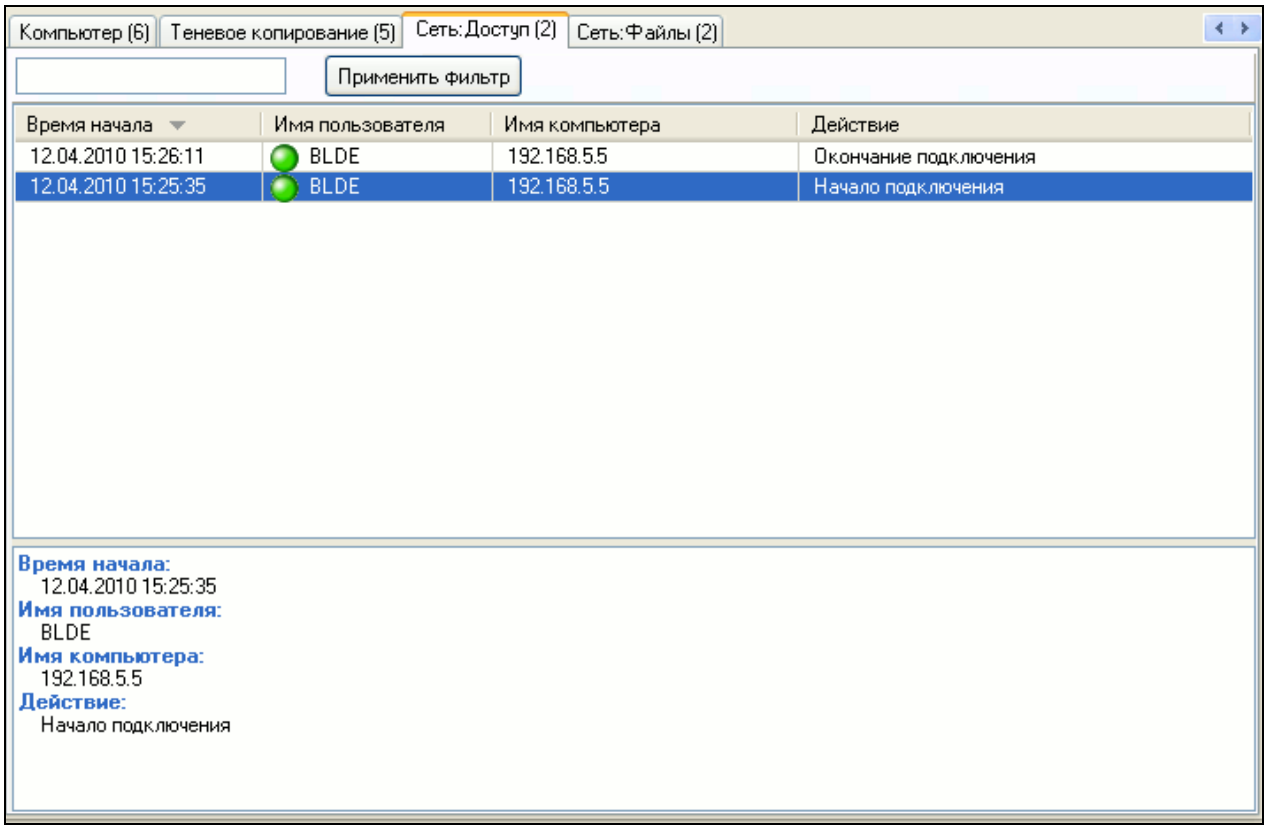
Также имеется возможность установить фильтр по времени возникновения событий. Тогда будут отображаться только те записи, которые соответствуют указанному условию. Возможны два варианта: указать период в днях от текущего, за который показывать логи или задать период конкретными датами, началом суток которых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

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



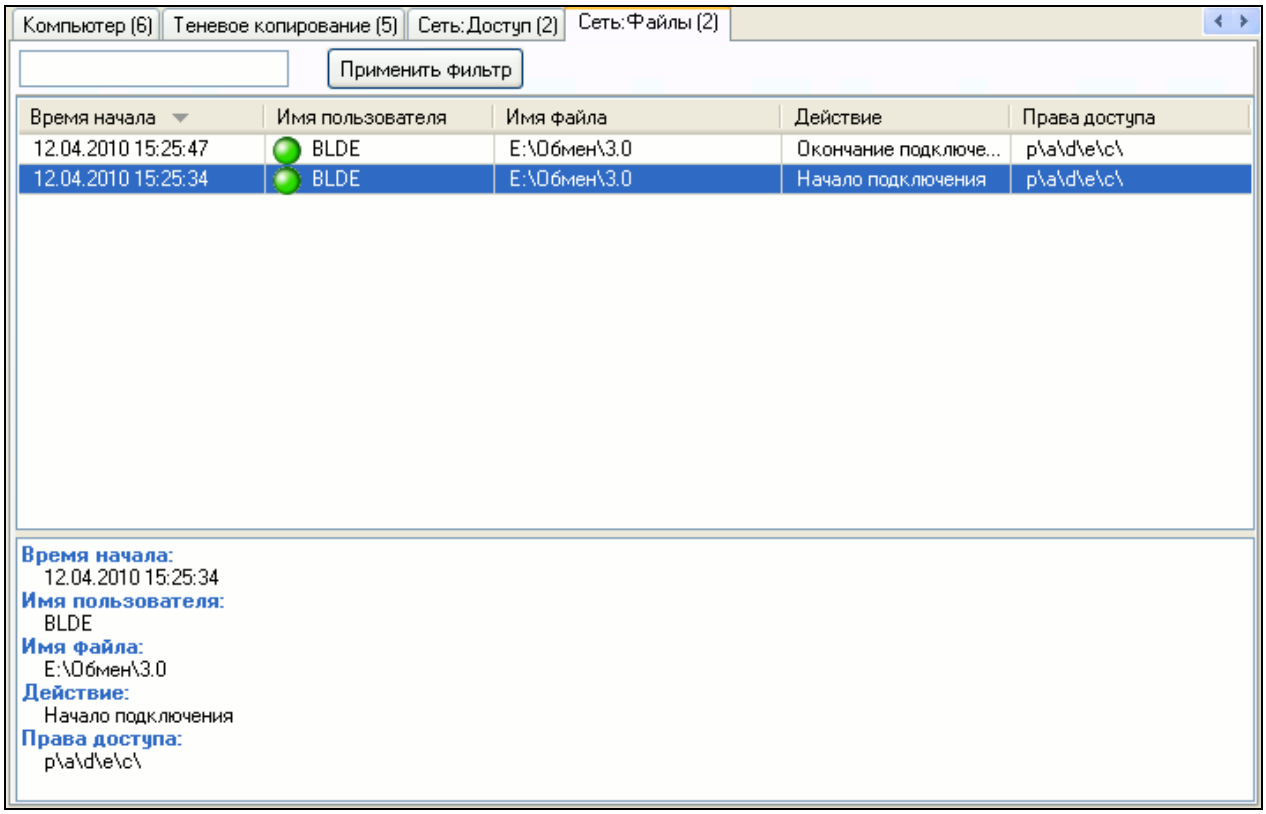
6.2.16 Сеть



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;

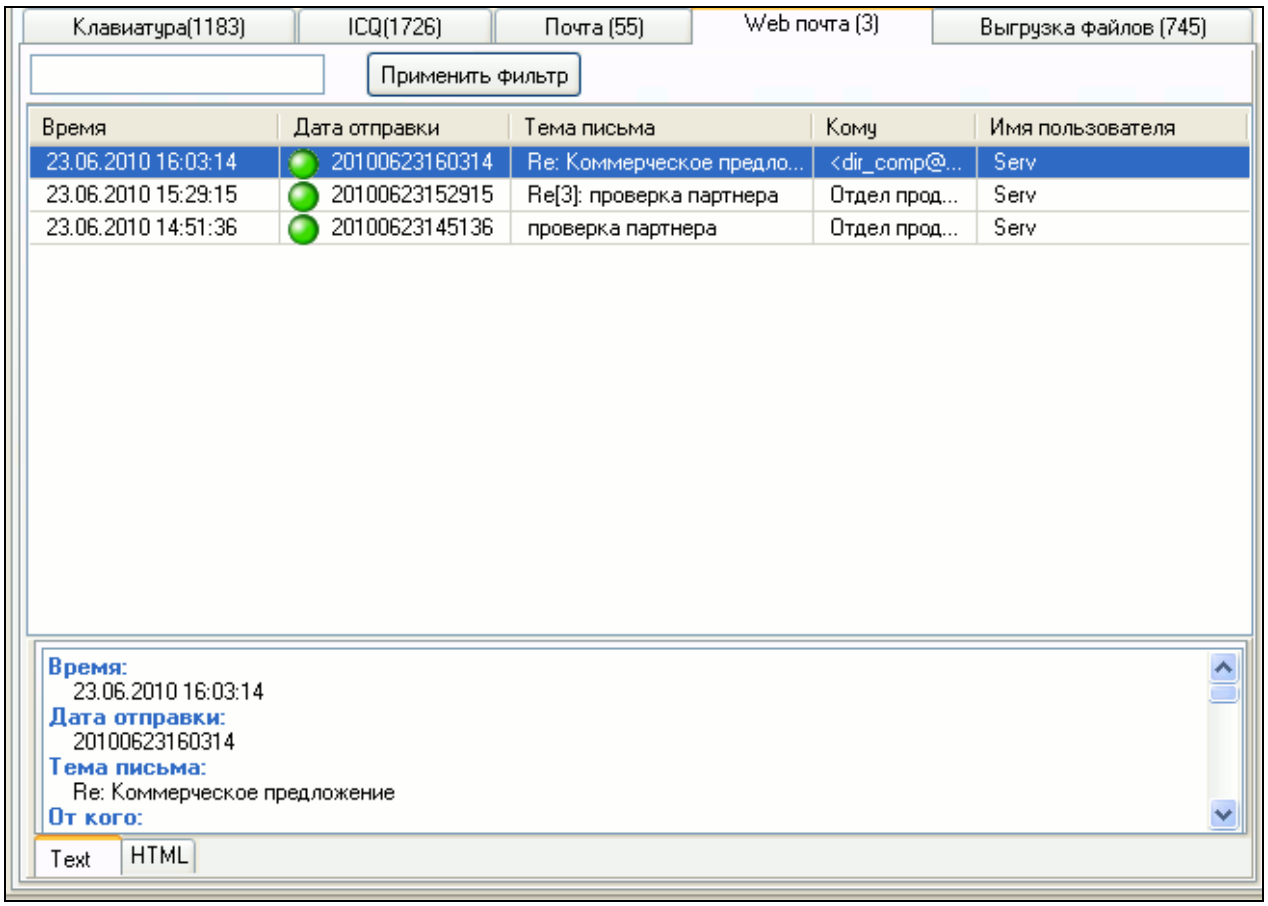
d - права на удаление файлов и каталогов;

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".

6.2.17 Web почта

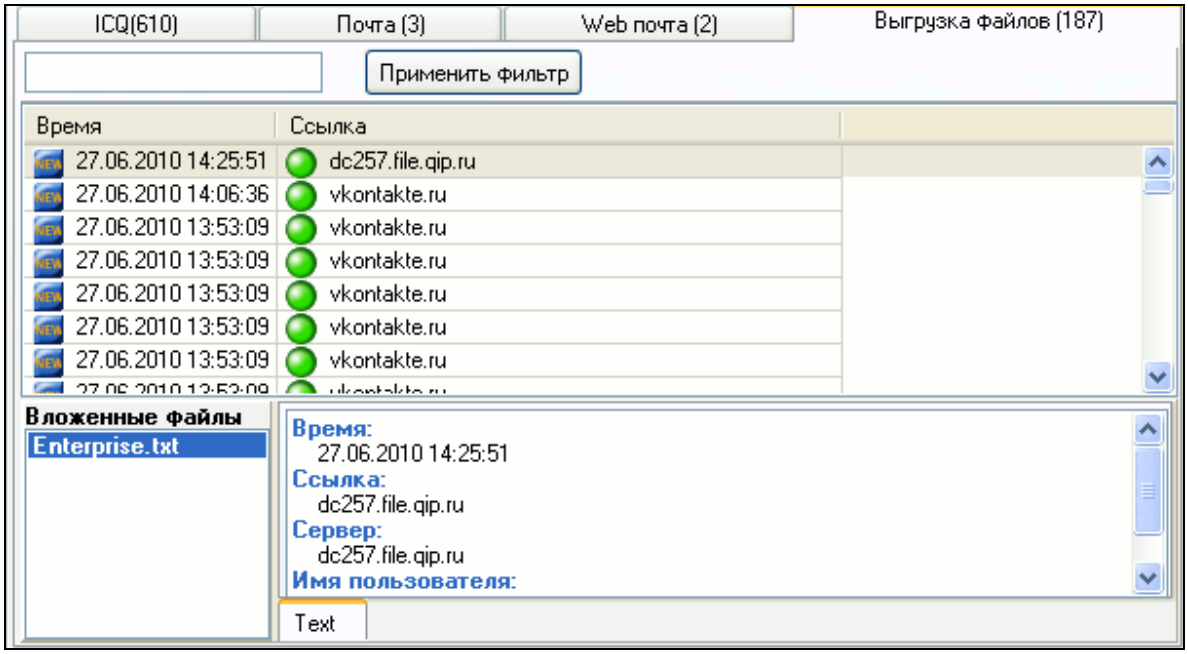


На этой странице находится информация по письмам, отправленным пользователем через web интерфейс. В заголовке закладки в скобках указано количество записей в таблице. Данные в таблице могут быть отсортированы по любому из столбцов, например по убыванию времени (то есть последняя информация содержится 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.

6.2.18 Выгрузка файлов

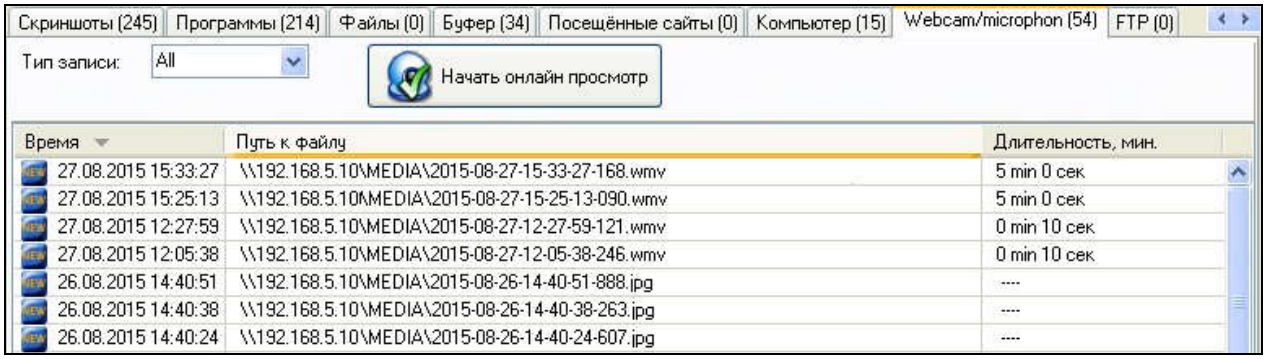


На этой странице находится информация по файлам, выгруженным пользователем в Интернет.

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.

6.2.19 Webcam/microphone



На этой вкладке отображаются созданные через веб камеру на контролируемом компьютере видео/аудио записи, а также снимки с веб камеры. Если в качестве хранилища для файлов выбран специальный каталог на сервере, то необходимо открыть к нему доступ для пользователя консоли просмотра данных.

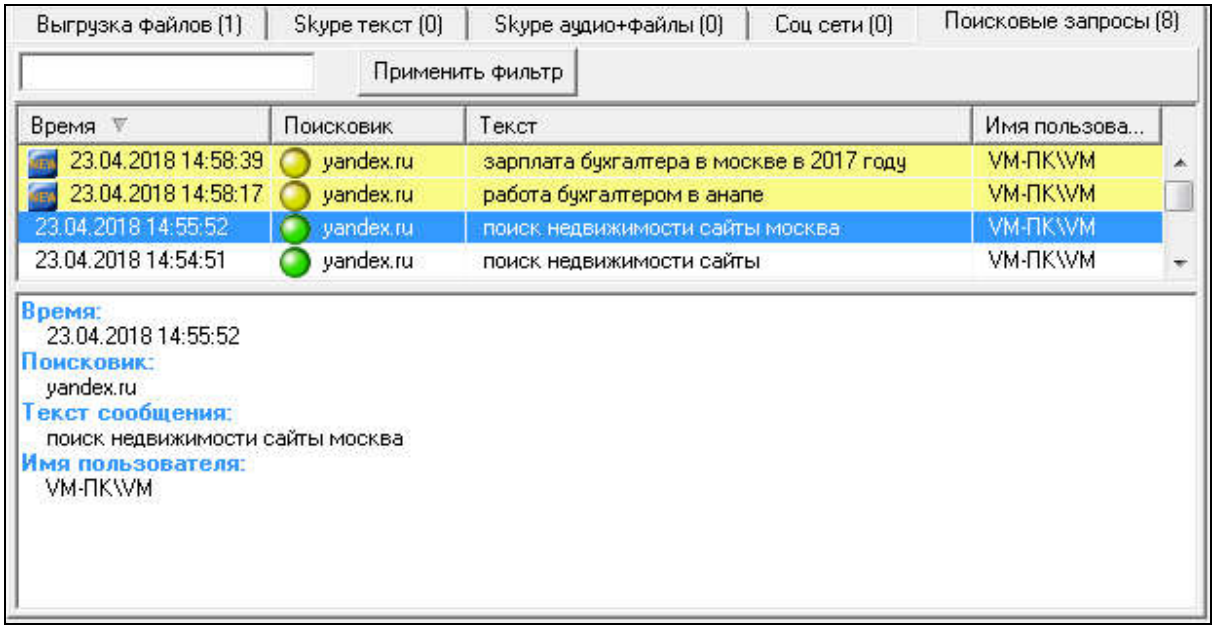
Просмотреть запись или снимок можно щелкнув дважды на соответствующей строке истории.

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.

6.2.20 Изменения оборудования

На данной вкладке отображаются события изменения состава комплектующих контролируемого компьютера. Так, если на нем будет отключена одна из планок оперативной памяти, или заменена видеокарта, то LanAgent оповестит об этом. Событие изменения оборудования будет показано на этой вкладке вьюера, а также будет создано событие оповещения (в окне Оповещения).

6.2.21 Поисковые запросы



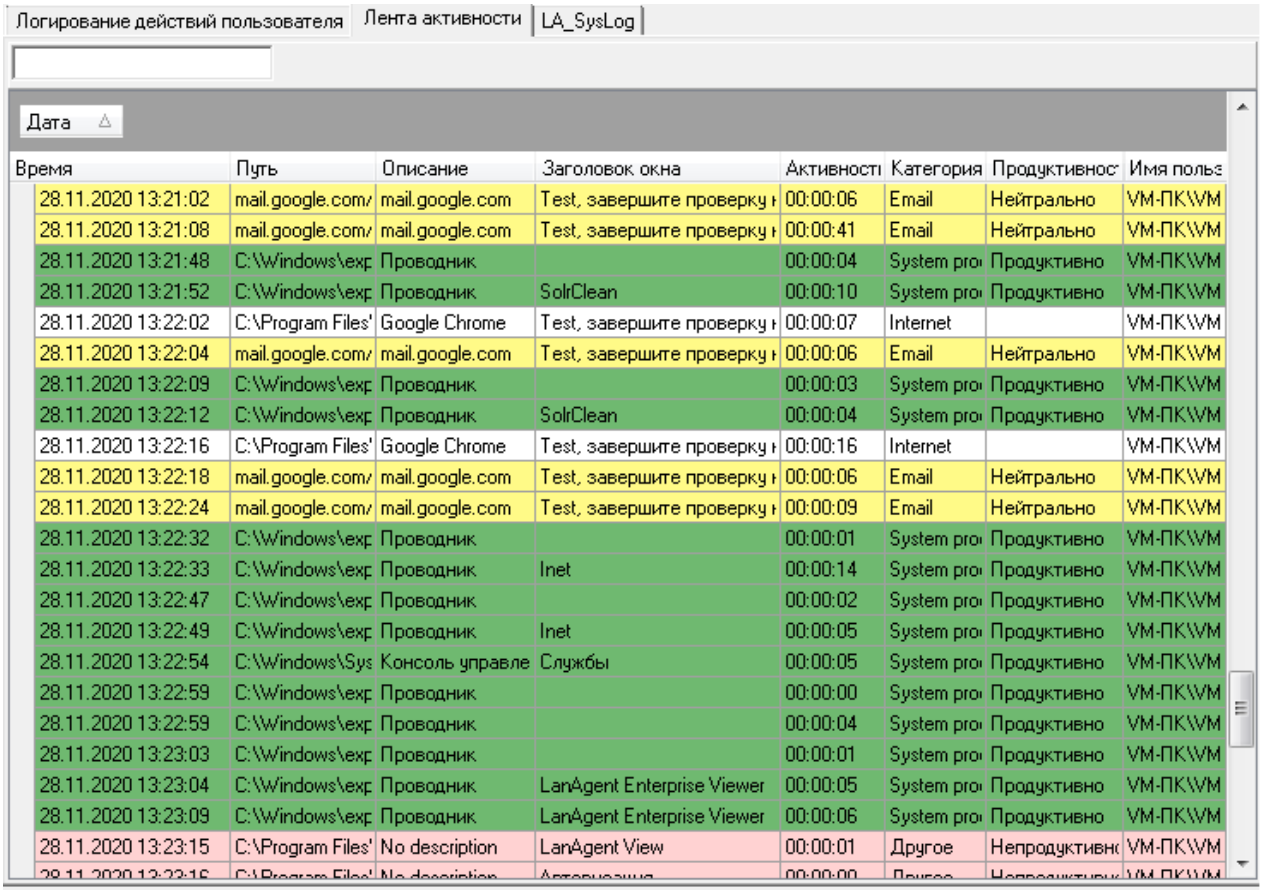
На этой вкладке показываются перехваченные поисковые запросы пользователей. Данные можно отсортировать по любому из столбцов. Также есть возможность поиска по содержимому.

6.3 Лента активности

Является детализацией рабочего дня и содержит в хронологическом порядке события включения/выключения компьютера, работы в программах и сайтах с указанием продолжительности. Строится для конкретного сотрудника за определенный день (если за период, то с разбивкой информации по дням).

Содержит:

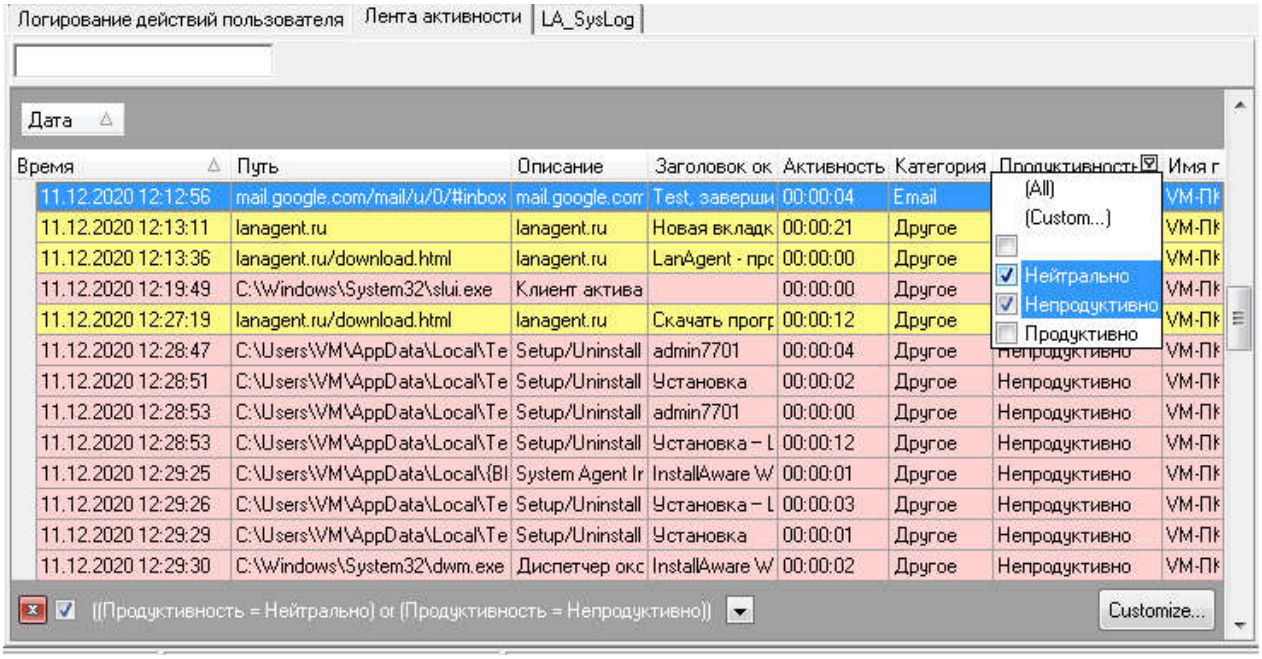
- время события
- путь программы или адрес сайта
- описание (название программы или домен сайта)
- заголовок окна программы или сайта
- время активности в часах-минутах-секундах
- к какой категории программ или сайтов относится (Почта, Офис и т.д.)
- признак продуктивности: продуктивно/непродуктивно/нейтрально в соответствии с профилем продуктивности сотрудника.



Время	Путь	Описание	Заголовок окна	Активности	Категория	Продуктивнос	Имя польз
28.11.2020 13:21:02	mail.google.com/	mail.google.com	Test, завершите проверку н	00:00:06	Email	Нейтрально	VM-ПК\VM
28.11.2020 13:21:08	mail.google.com/	mail.google.com	Test, завершите проверку н	00:00:41	Email	Нейтрально	VM-ПК\VM
28.11.2020 13:21:48	C:\Windows\exp	Проводник		00:00:04	System pro	Продуктивно	VM-ПК\VM
28.11.2020 13:21:52	C:\Windows\exp	Проводник	SolrClean	00:00:10	System pro	Продуктивно	VM-ПК\VM
28.11.2020 13:22:02	C:\Program Files'	Google Chrome	Test, завершите проверку н	00:00:07	Internet		VM-ПК\VM
28.11.2020 13:22:04	mail.google.com/	mail.google.com	Test, завершите проверку н	00:00:06	Email	Нейтрально	VM-ПК\VM
28.11.2020 13:22:09	C:\Windows\exp	Проводник		00:00:03	System pro	Продуктивно	VM-ПК\VM
28.11.2020 13:22:12	C:\Windows\exp	Проводник	SolrClean	00:00:04	System pro	Продуктивно	VM-ПК\VM
28.11.2020 13:22:16	C:\Program Files'	Google Chrome	Test, завершите проверку н	00:00:16	Internet		VM-ПК\VM
28.11.2020 13:22:18	mail.google.com/	mail.google.com	Test, завершите проверку н	00:00:06	Email	Нейтрально	VM-ПК\VM
28.11.2020 13:22:24	mail.google.com/	mail.google.com	Test, завершите проверку н	00:00:09	Email	Нейтрально	VM-ПК\VM
28.11.2020 13:22:32	C:\Windows\exp	Проводник		00:00:01	System pro	Продуктивно	VM-ПК\VM
28.11.2020 13:22:33	C:\Windows\exp	Проводник	Inet	00:00:14	System pro	Продуктивно	VM-ПК\VM
28.11.2020 13:22:47	C:\Windows\exp	Проводник		00:00:02	System pro	Продуктивно	VM-ПК\VM
28.11.2020 13:22:49	C:\Windows\exp	Проводник	Inet	00:00:05	System pro	Продуктивно	VM-ПК\VM
28.11.2020 13:22:54	C:\Windows\Sys	Консоль управле	Службы	00:00:05	System pro	Продуктивно	VM-ПК\VM
28.11.2020 13:22:59	C:\Windows\exp	Проводник		00:00:00	System pro	Продуктивно	VM-ПК\VM
28.11.2020 13:22:59	C:\Windows\exp	Проводник		00:00:04	System pro	Продуктивно	VM-ПК\VM
28.11.2020 13:23:03	C:\Windows\exp	Проводник		00:00:01	System pro	Продуктивно	VM-ПК\VM
28.11.2020 13:23:04	C:\Windows\exp	Проводник	LanAgent Enterprise Viewer	00:00:05	System pro	Продуктивно	VM-ПК\VM
28.11.2020 13:23:09	C:\Windows\exp	Проводник	LanAgent Enterprise Viewer	00:00:06	System pro	Продуктивно	VM-ПК\VM
28.11.2020 13:23:15	C:\Program Files'	No description	LanAgent View	00:00:01	Другое	Непродуктивно	VM-ПК\VM

Сортировку и фильтрацию данных можно производить по любому из столбцов таблицы.

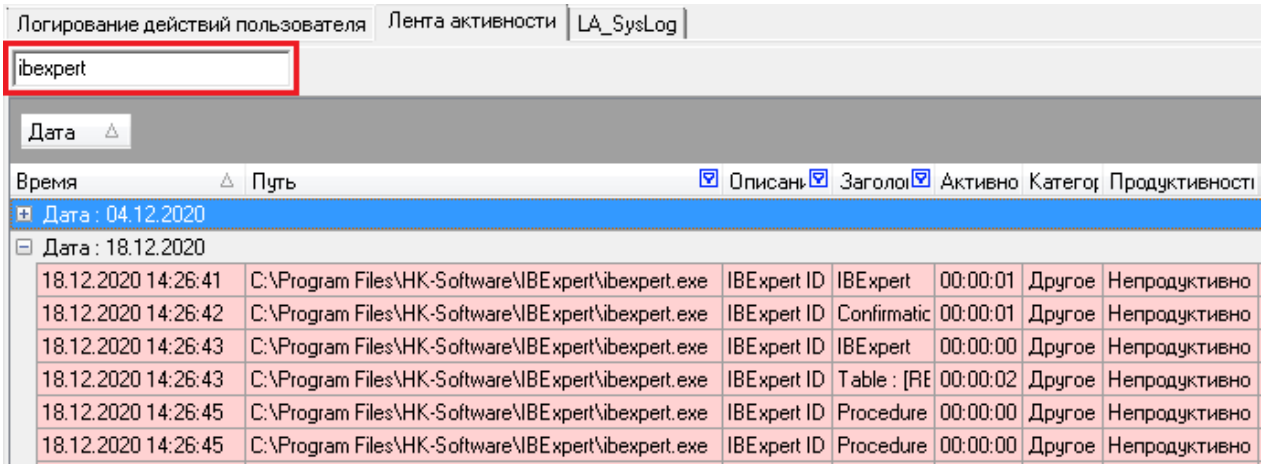
Например, оставить отображение только непродуктивных программ и сайтов



Для группировки данных, перетяните мышкой заголовок нужного столбца на серое поле, там, где на картинке уже расположена колонка «Дата».

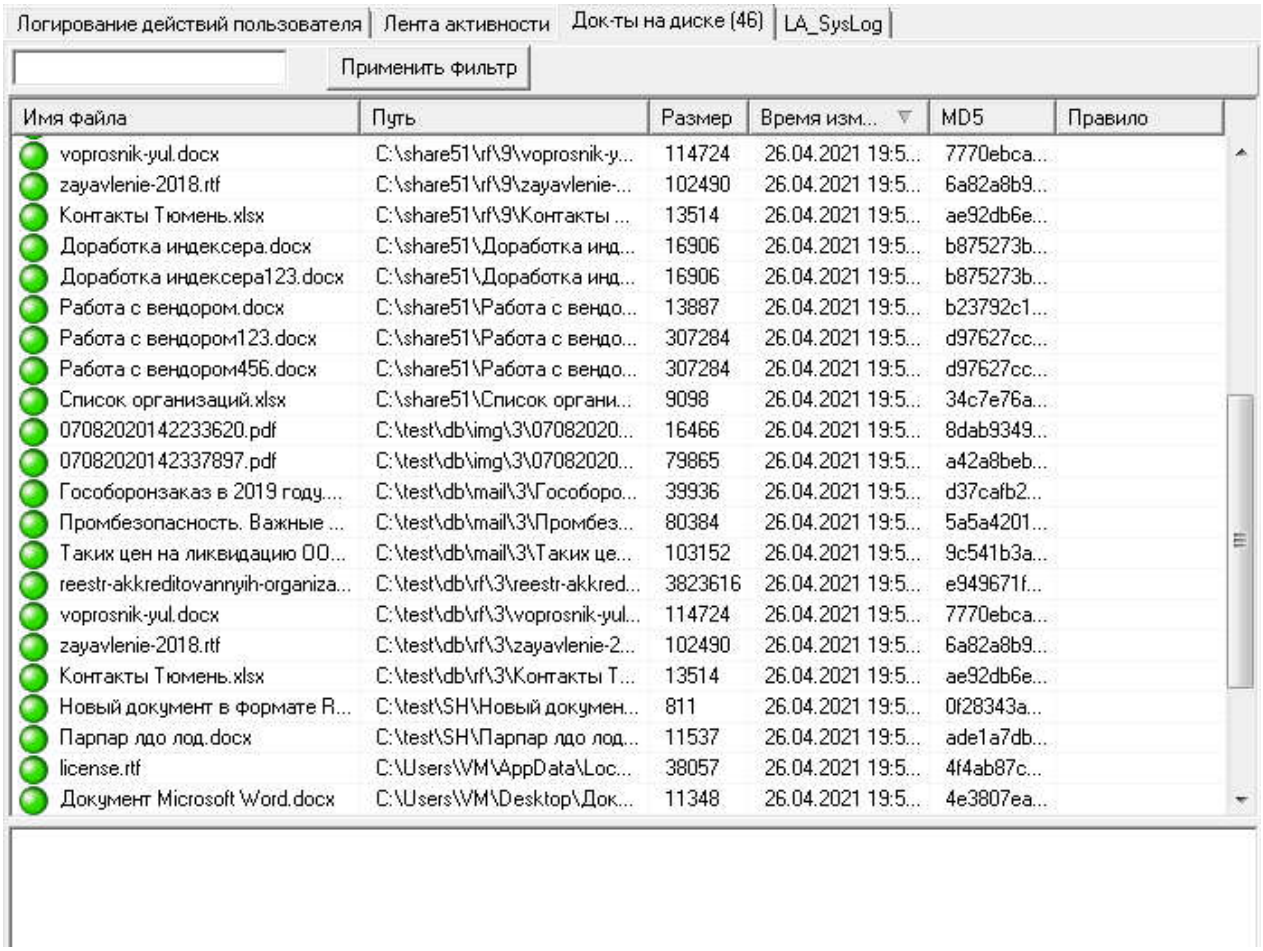
Для фильтрации – щелкните на заголовок столбца и у него на значок фильтра.

Если Вас интересует какая-то определенная программа, то можно ввести ее наименование в поле фильтра в верху страницы:



6.4 Документы на диске (DLP)

Версия LanAgent EnterpriseDLP позволяет производить индексацию документов на локальных дисках рабочих станций сотрудников. Проиндексированные документы будут показываться на соответствующей вкладке в LanAgent Viewer.



Щелкнув на строку интересующего документа, можно просмотреть его содержимое.

При помощи поля фильтра, можно оставить в списке нужный документ.

По проиндексированным документам также производится проверка и заданных в админке правил, в том числе, ключевых слов.

Если какое-то из правил сработает, то в строке документа, для которого оно нашлось, в колонке «Правило» оно будет показано.

6.5 Панель инструментов

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

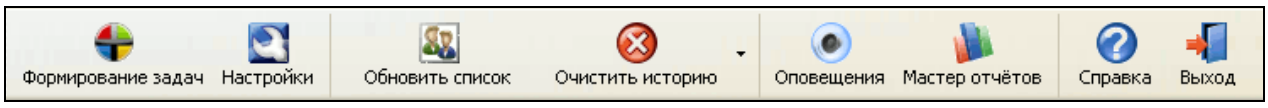
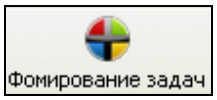
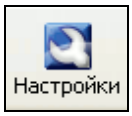


Рис. 6.17 – Панель инструментов

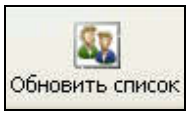
Назначение кнопок панели инструментов:



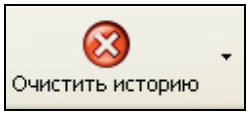
- открыть окно формирования задач для агентов.



- открыть окно настроек подключения к базе данных.

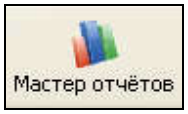


- обновить список компьютеров и их статус из базы данных.

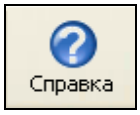


- очистка содержимого логов. Включает в себя следующие пункты:
  - удалить текущую запись,
  - очистить выбранную категорию,
  - очистить все логи пользователя.

- открыть окно истории активного оповещения.



- открыть окно мастера отчетов.



- вызов файла справки.

- выйти из программы.

6.6 Поиск по данным

Для поиска ключевого слова в рамках определенной вкладки данных, можно воспользоваться специальным фильтром. Его строка размещена непосредственно над данными. В этом случае в списке останутся только те записи, которые данное слово содержат.

Также, можно воспользоваться диалогом поиска, нажав комбинацию клавиш **<Ctrl>+<F>**. Перед вами появится окно поиска. Так, применимо к закладке **"Программы",** например, оно будет иметь следующий вид:

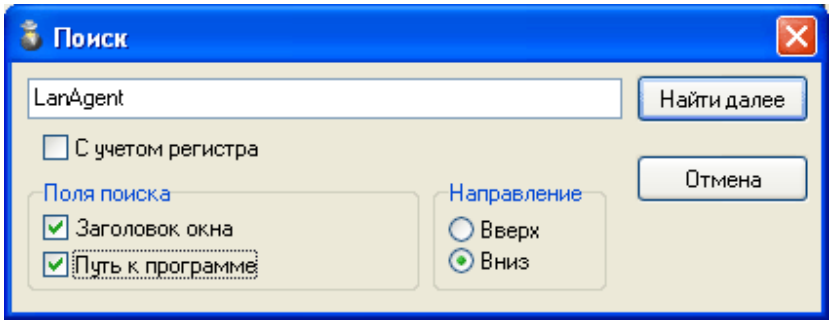


Рис. 6.18 – Диалог поиска по логам

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".

6.4.1 Поиск по всем данным всех компьютеров

Для версии **EnterpriseDLP** доступен расширенный поиск по собранным данным. Для этого, на компьютер с серверной частью Enterprise необходимо установить специальный поисковый модуль.

Он обеспечивает возможность полнотекстового поиска по всем собранным данным по всем компьютерам. После его установки, в LanAgent Viewer на панели инструментов станет доступна кнопка «Поиск в данных».

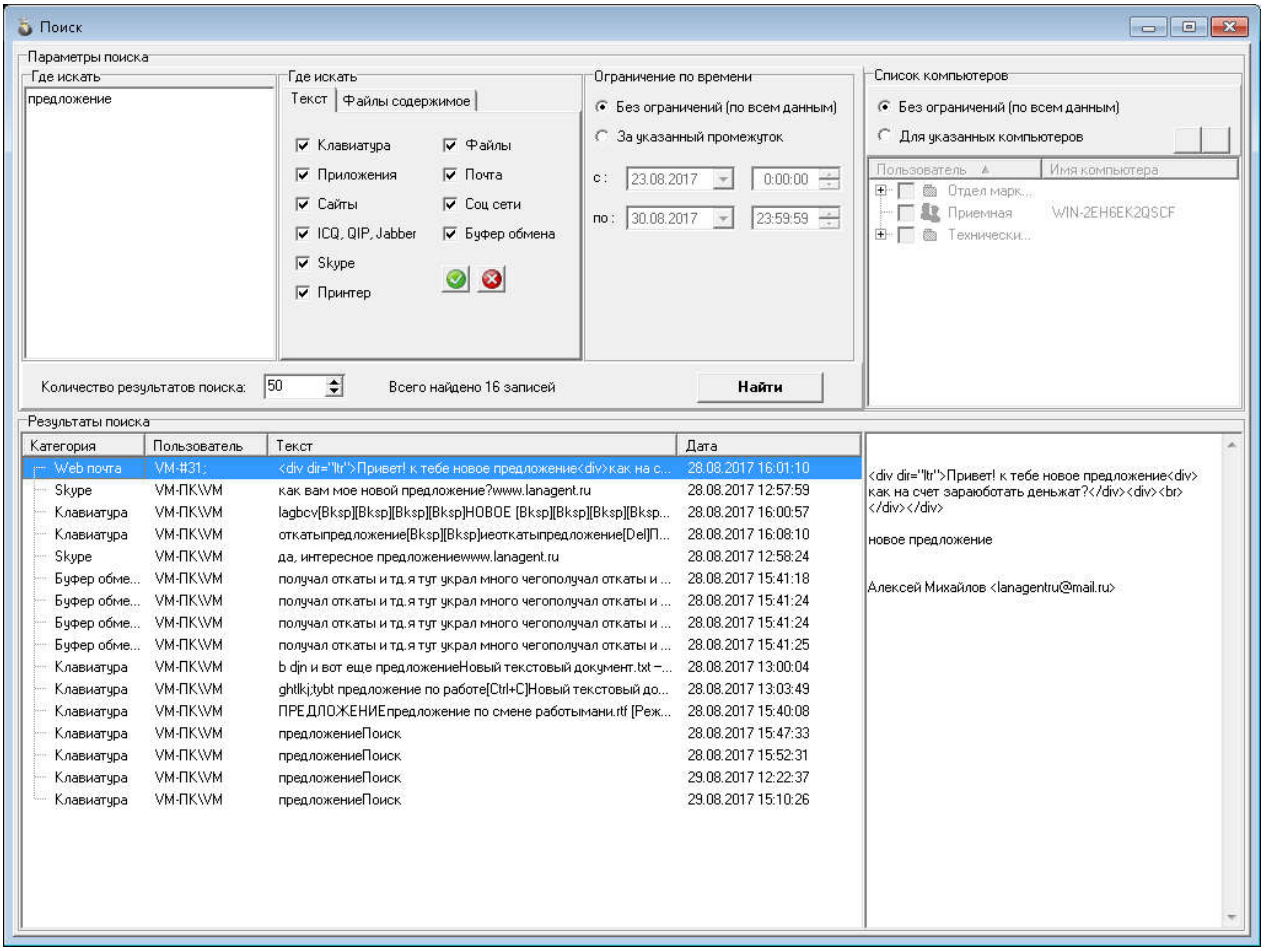
Для открытия окна поиска, нажмите в LanAgent Viewer кнопку «**Поиск в данных**».

В открывшемся окне выберите категории данных, в которых надо проводить поиск, за какой промежуток времени данные учитывать и по каким компьютерам.

Поиск по данным со всех компьютеров и без ограничений по времени выборки происходит быстрее.

Для поиска ключевой фразы в файлах (вложениях почты, отправленных на печать документах и т.д.) задайте области поиска на вкладке «Файлы содержимое».

Для начала поиска, нажмите кнопку «**Найти**».



6.4.2 Карта движения файлов

В версии **EnterpriseDLP** можно просмотреть движение интересующего эталонного файла по всем контролируемым компьютерам. Как вариант, это может быть какой-то конфиденциальный документ, с которым имеет возможность работать несколько сотрудников.

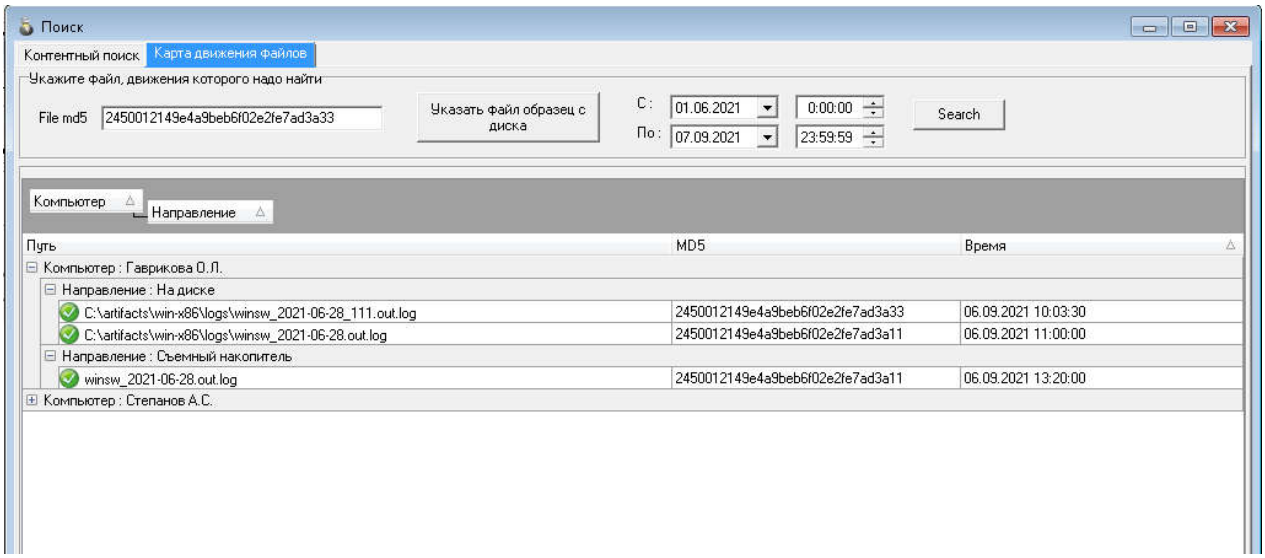
Показано будет: на каких компьютерах такой файл есть сейчас или появлялся ранее. Его копирования в рамках компьютера, переименования, редактирования.

Т.е. если пользователь внес изменения в файл, то он все равно будет отображен в результатах поиска.

Если пользователь копировал файл на съемные накопители или отправлял через браузер, то это также будет показано.

Для начала построения карты движения, нажмите кнопку «Указать файл образец с диска» и выберите нужный файл. Либо, внесите вручную md5 эталонного файла,

если оно уже известно. Поиск будет происходить по истории за заданный временной период.



6.5 Активное оповещение

Служит для оперативного оповещения специалиста службы безопасности о таких опасных действиях пользователей, как подключение носителей информации, установка программ. При осуществлении пользователем указанных выше действий, агентская часть программы LanAgent передаст эту информацию на базовый компьютер, не дожидаясь команды обновления логов. Полученные события отображаются в специальном окне истории активного оповещения (см. рисунок ниже). Настроить активное оповещение (для каких событий его производить) можно индивидуально для каждого компьютера на закладке «Агенты» программы LanAgent Admin. Подробно о настройках можно посмотреть в разделе 5.3.2.

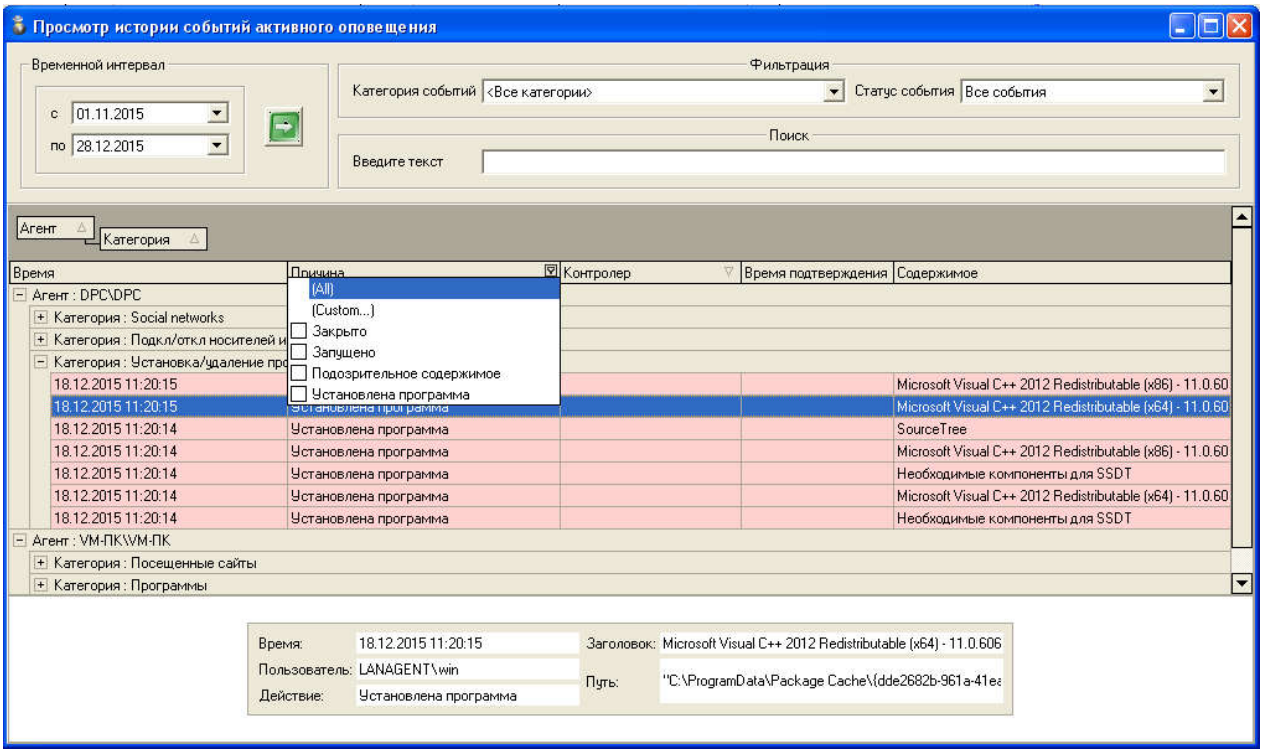


Рис. 6.19 – Окно истории активного оповещения

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

Группировку, сортировку и фильтрацию событий можно производить по любой из колонок данных. Для выбора колонки для группировки, просто перетащите ее мышкой на серое поле над таблицей.

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

Любое пришедшее событие требует подтверждения (квитирования). Смысл данного действия в том, чтобы обеспечить гарантированную доставку информации непосредственно до специалиста безопасности, который легко сможет увидеть какие

сообщения он уже просматривал, а какие еще нет. Кроме того, теперь он не сможет просто проигнорировать сообщение, т.к. кроме информации о самом событии также хранится информация и о времени его подтверждения.

6.6 «Светофор» безопасности

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

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

Как видно из приведенного ниже рисунка, у пользователя "Программист" имеются значительные нарушения, поэтому статус его опасности "красный".

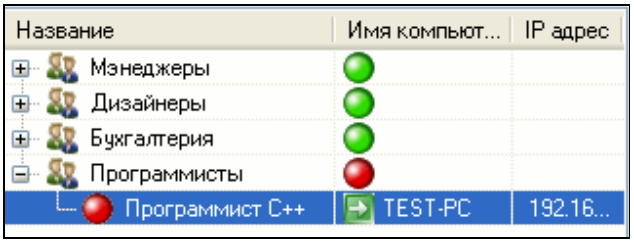


Рис. 6.20 – «Светофор» списка компьютеров

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. 6.21 – «Светофор» событий в логах

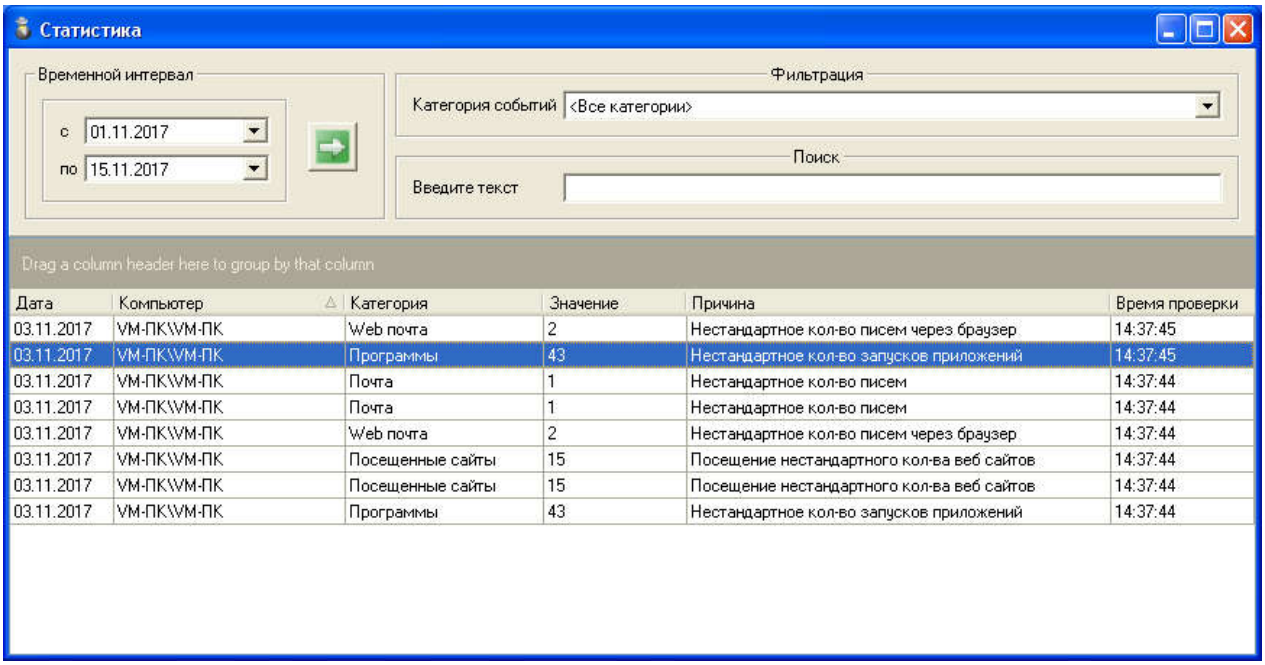
Таким образом, при правильно подобранном наборе правил, снижается необходимость просмотра логов каждого пользователя.

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

6.7 Просмотр оповещений о нестандартной активности пользователя

Просмотреть результаты поиска нестандартного поведения пользователей, можно нажав кнопку "Статистика" в панели инструментов.

Само окно имеет следующий вид:



В нем показывается по каким компьютерам были замечены отклонения и в каких категориях событий.

Для перехода к просмотру событий в интересующей категории, выделите строку истории, щелкните правой клавишей мыши и выберите в выпадающее меню «Перейти к записям истории».

6.8 Настройка LanAgent View

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

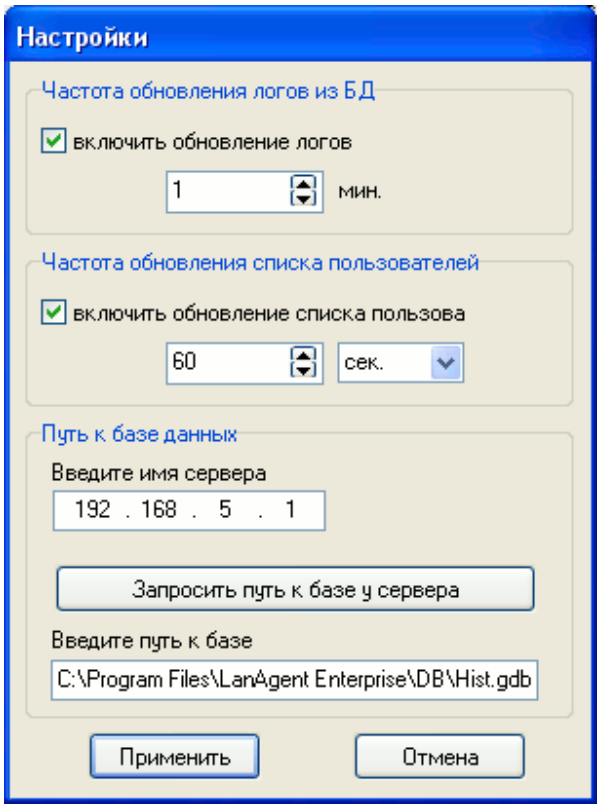


Рис. 6.22 – Настройки программы LanAgent View

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

Включить обновление списка пользователей - установите эту галочку, если хотите чтобы программа автоматически производила обновление списка

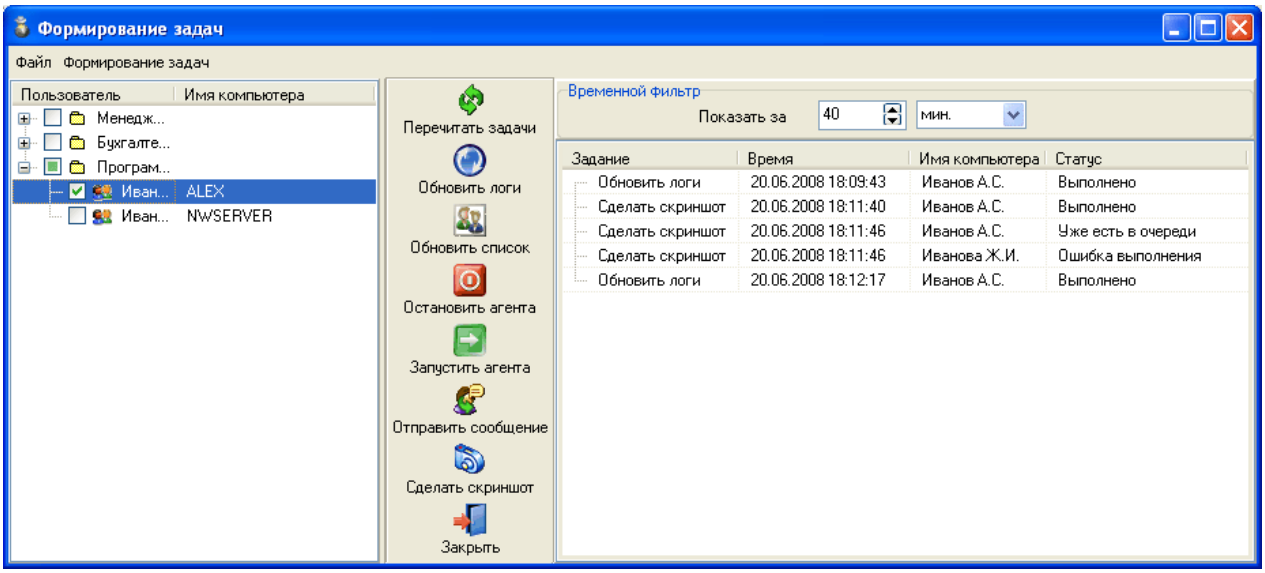
пользователей из базы данных. При этом будет происходить также и обновление статуса для компьютеров. Ниже указывается периодичность обновления списка.

Путь к базе данных - здесь задается путь по которому размещена база данных LanAgent. Он состоит из 2-х частей: ip адреса (или имени) компьютера, на котором расположена база и пути к каталогу, в котором она непосредственно расположена. Сам путь можно получить от сервера LanAgent, нажав соответствующую кнопку (Запросить путь к базе у сервера). Если в ходе запроса пути к базе было выдано сообщение о невозможности подключения к серверу, то необходимо убедиться, что на сервере запущен сервис обмена LanAgent и обмен с сервером не блокируется фаерволом.

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

6.9 Формирование задач

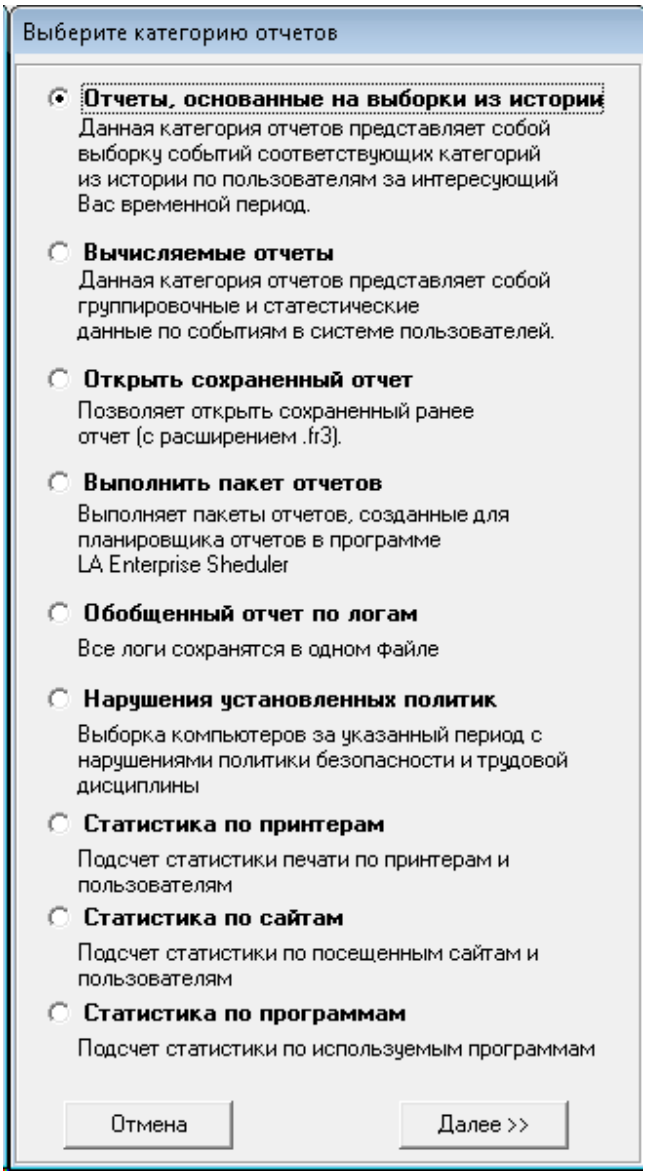
Окно формирования задач можно открыть, нажав кнопку "**Формирование задач**" в панели инструментов или выбрав соответствующий пункт в выпадающем меню «Управление».



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

6.10 Составление отчетов

При вызове мастера отчетов откроется следующее окно:



Как видно из рисунка, отчеты имеются нескольких 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.

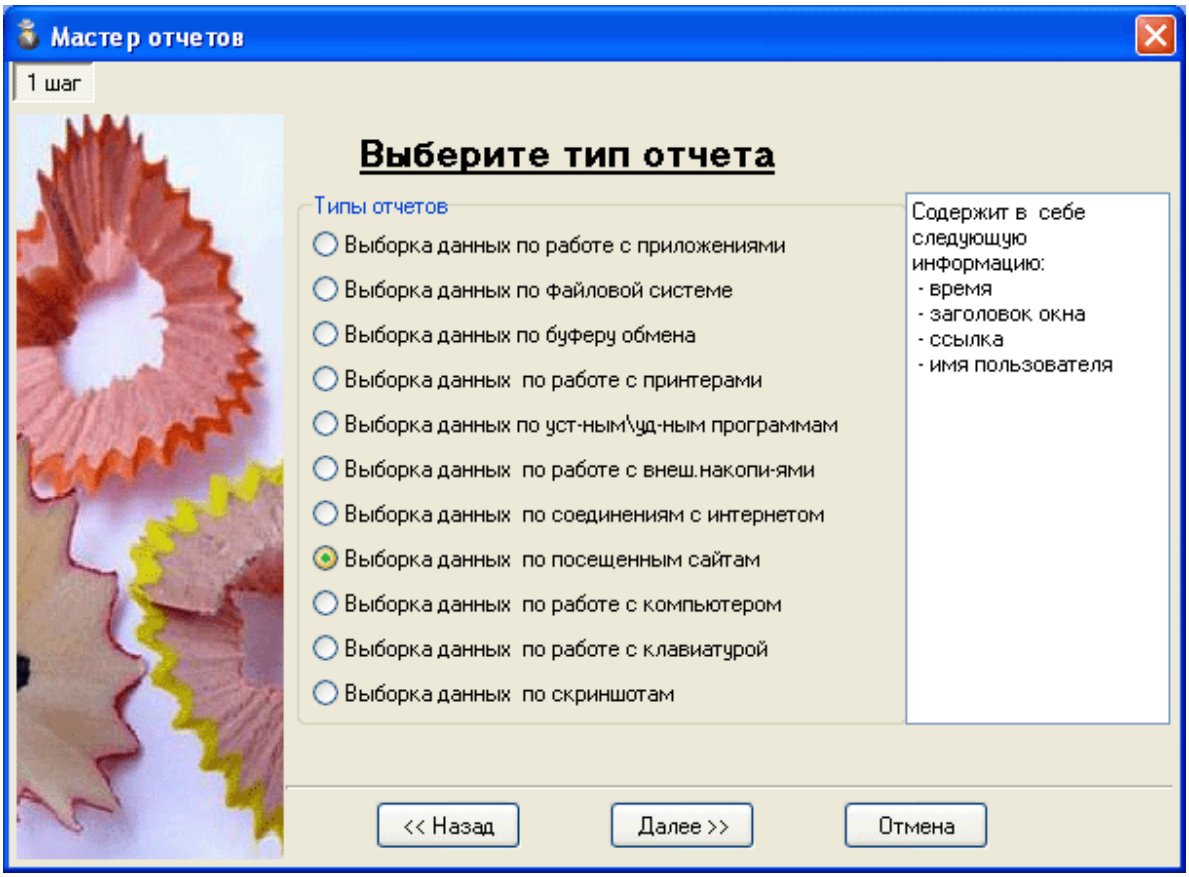
Также, через данную форму можно **открыть сохраненный ранее отчет**, выполнить **пакет отчетов**, составленный ранее в Планировщике отчетов, сформировать **обобщенный отчет в html формате** или открыть форму, **содержащую все**

нарушения правил безопасности и трудовой дисциплины по контролируемым компьютерам.

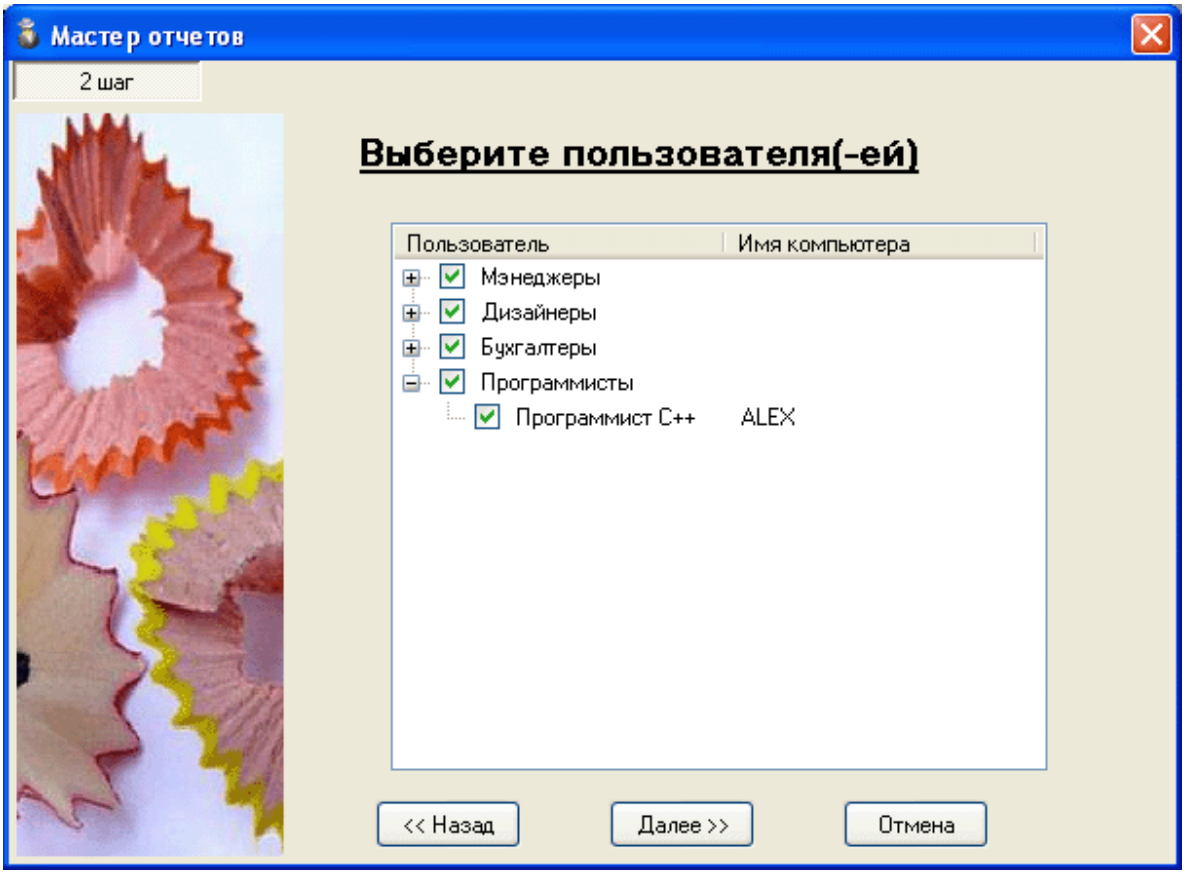
Отдельными пунктами представлена интерактивная статистика по посещению сайтов, по напечатанным на принтер документам и по работе с программами.

6.11 Отчеты - выборки

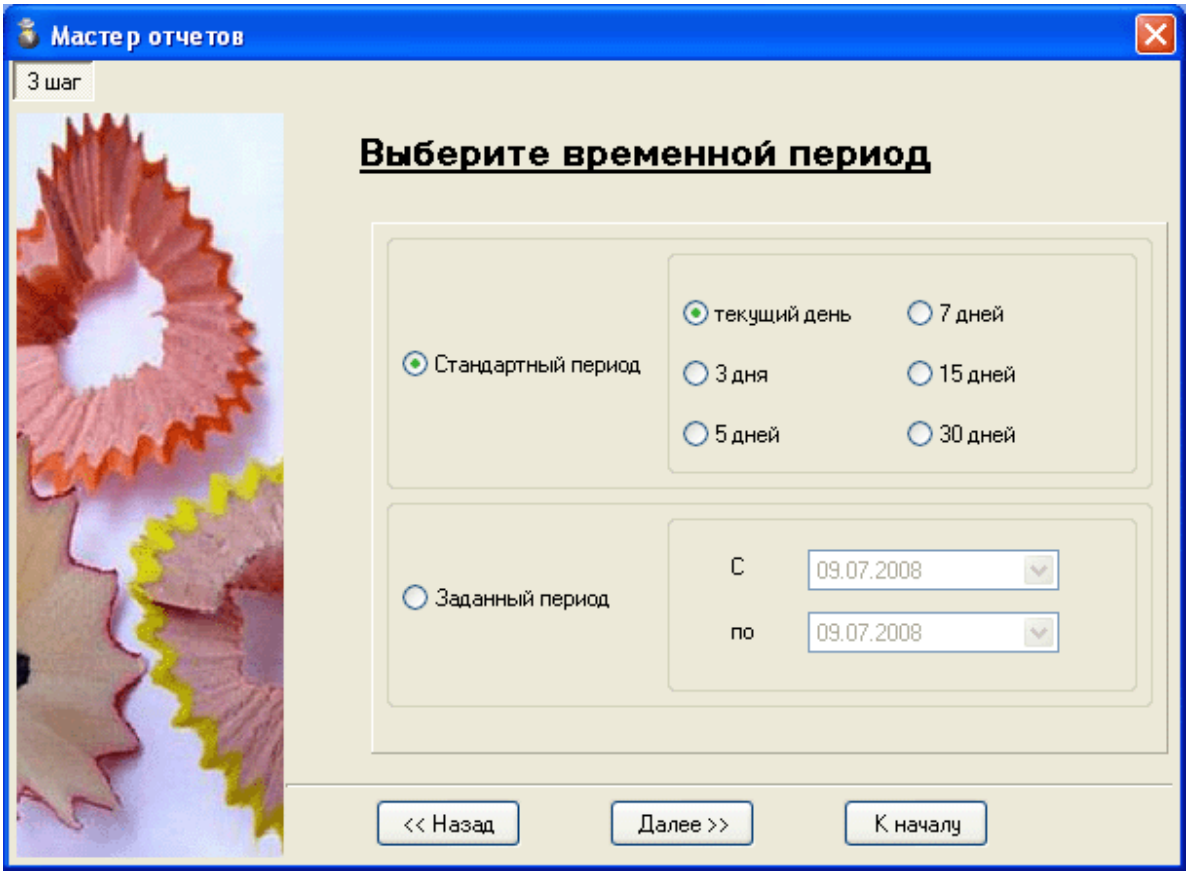
Набор отчетов-выборок имеет следующий вид:



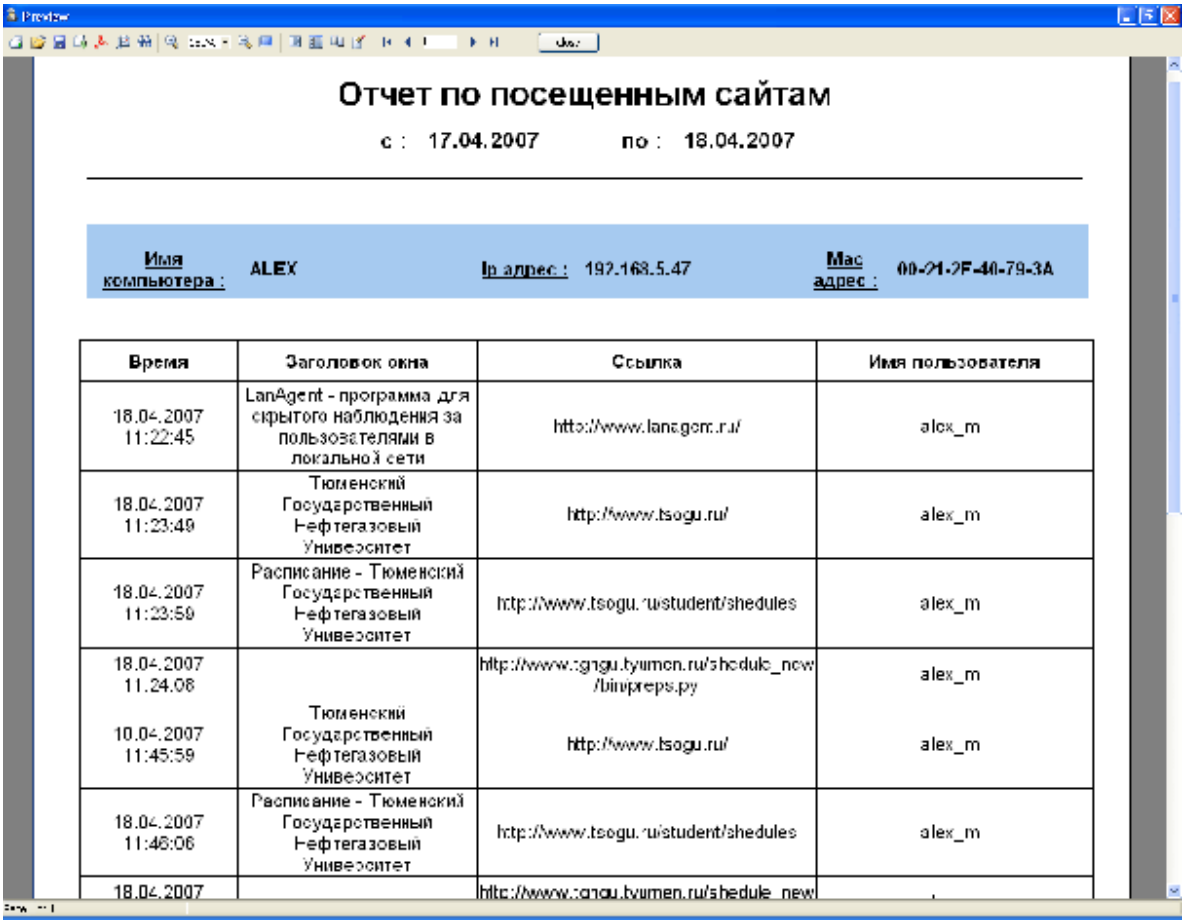
Выберите из списка нужный тип отчета и нажмите кнопку **"Далее"**. В открывшемся окне укажите компьютеры, для которых будет составляться отчет.



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".

6.12 Вычисляемые отчёты

Вычисляемые (аналитические) отчеты в версии LanAgent Enterprise, сгруппированы по трем категориям:

- отчеты по работе ПК и в программах;
- отчеты, связанные с Интернет
- отчеты по печати документов на принтере.

В них ведется подсчет отработанных сотрудниками часов, ведется табель учета рабочего времени, статистика использования программ. Они позволяют просмотреть

в целом количество прогулов, часов переработки/недоработки, часов, отработанных в выходные дни.

Каждый из аналитических отчетов имеет как интерактивный вид, так и вариант для печати.

Интерактивный формат отчета позволяет в один клик переходить из общих отчетов в детализацию информации по конкретному сотруднику и возвращаться обратно к общему виду.

Отчет может быть отсортирован и сгруппирован по любому из столбцов. Также можно применять фильтрацию по конкретному значению.

Например, можно отчет по использованию программ сгруппировать по продуктивности. Тогда отдельно будут показаны продуктивные, непродуктивные и нейтральные программы, используемые сотрудником.

Либо, задать фильтр и увидеть всех работников, использовавших 1С и просмотреть сколько времени они в этом приложении провели.

Также, в один клик можно экспортировать отчет в PDF, Excel или Word документ.

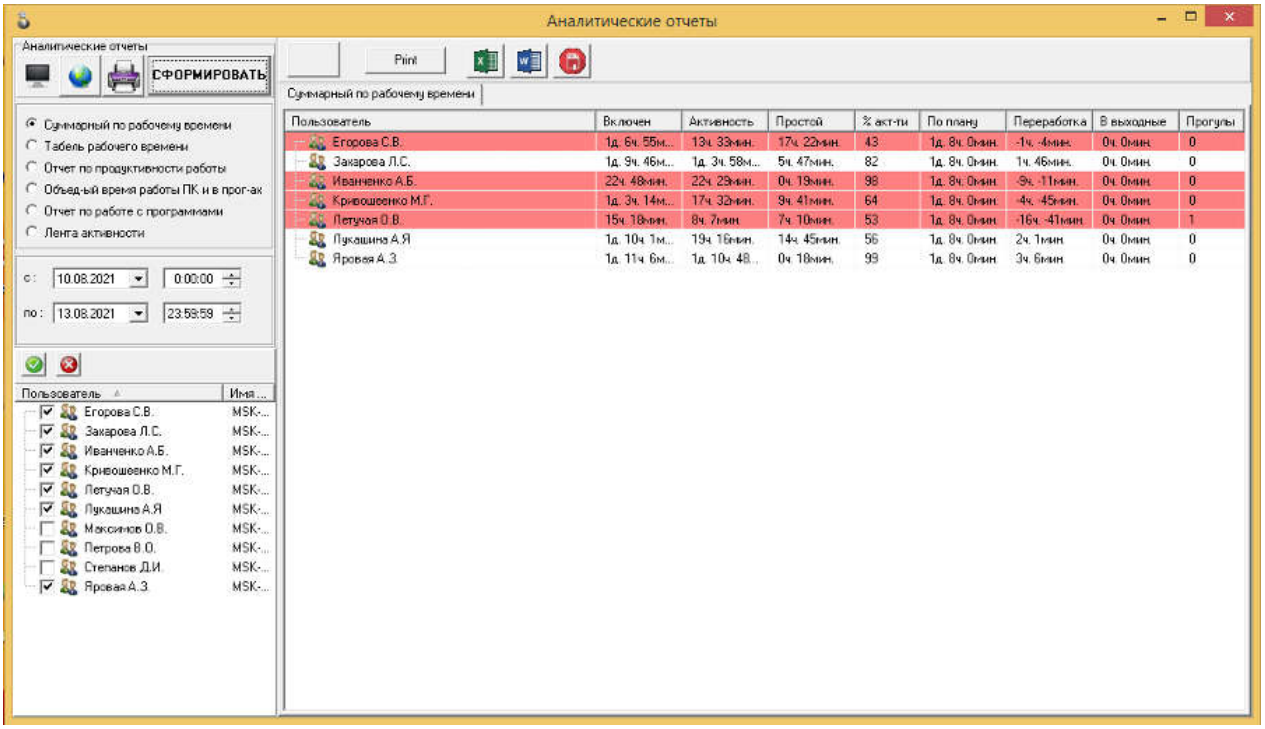
Любой из отчетов или даже даже комплект отчетов, может формироваться по расписанию и отправить на почту. Можно задать для каких сотрудников формировать отчет, какие виды отчетов, за какой интервал. И указать email для отправки полученного пакета. Таких пакетов можно сформировать сколько угодно и настроить под каждого специалиста, работающего с системой.

Теперь, распишем имеющиеся отчеты подробнее**.**

6.12.1 Суммарный отчет по рабочему времени.

Содержит по выбранным отделам или конкретным сотрудникам в одной таблице информацию о:

- часах, отработанных за период построения отчета
- процент активности (какой % приходится на активность, а какой на простой)
- суммарное время активной работы за выбранный период (время работы за минусом простоя)
- количество часов переработки или недоработки в соответствии с графиком рабочего времени.
- количество прогулов
- количество часов, отработанных в выходные дни.



Красным цветом выделены те сотрудники, у которых за период построения отчета есть недоработка или прогулы.

Версия этого отчета для печати:

Суммарный отчет по рабочему времени

с: 10.08.2021 по: 13.08.2021 23:59:59

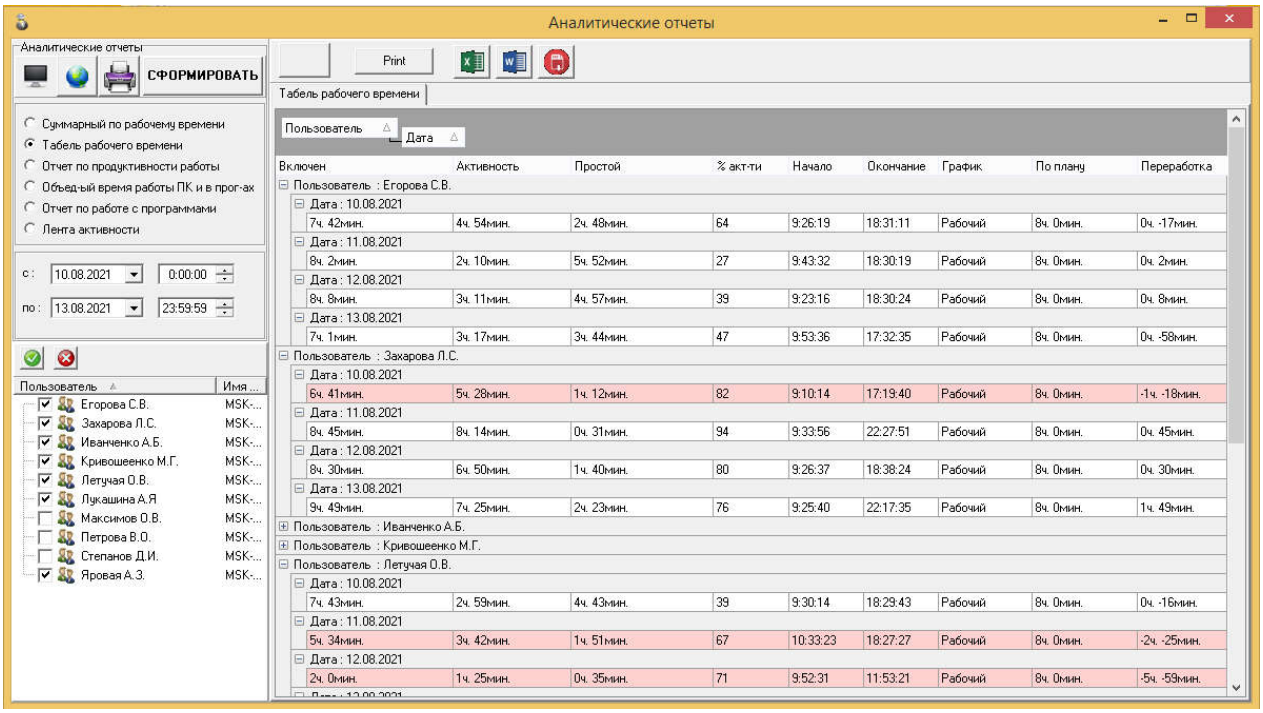
Компьютер	Включен	Активность	Простой	% акт-ти	По плану	Переработка	Прогулы	В выходные
Егорова С.В.	1д. 6ч. 55мин.	13ч. 33мин.	17ч. 22мин.	44	1д. 8ч. 0мин.	-1ч. -4мин.	0	0ч. 0мин.
Захарова Л.С.	1д. 9ч. 46мин.	1д. 3ч. 58мин.	5ч. 47мин.	83	1д. 8ч. 0мин.	1ч. 46мин.	0	0ч. 0мин.
Иванченко А.Б.	22ч. 48мин.	22ч. 29мин.	0ч. 19мин.	99	1д. 8ч. 0мин.	-9ч. -11мин.	0	0ч. 0мин.
Кривошеенко М.Г.	1д. 3ч. 14мин.	17ч. 32мин.	9ч. 41мин.	64	1д. 8ч. 0мин.	-4ч. -45мин.	0	0ч. 0мин.
Летучая О.В.	15ч. 18мин.	8ч. 7мин.	7ч. 10мин.	53	1д. 8ч. 0мин.	-16ч. -41мин.	1	0ч. 0мин.
Лукашина А.Я	1д. 10ч. 1мин.	19ч. 16мин.	14ч. 45мин.	57	1д. 8ч. 0мин.	2ч. 1мин.	0	0ч. 0мин.
Яровая А.З.	1д. 11ч. 6мин.	1д. 10ч. 48мин.	0ч. 18мин.	99	1д. 8ч. 0мин.	3ч. 6мин.	0	0ч. 0мин.

Щелкнув дважды на интересующем сотруднике в интерактивной форме отчета, можно перейти в детальный отчет-табель.

6.12.2 Табель рабочего времени.

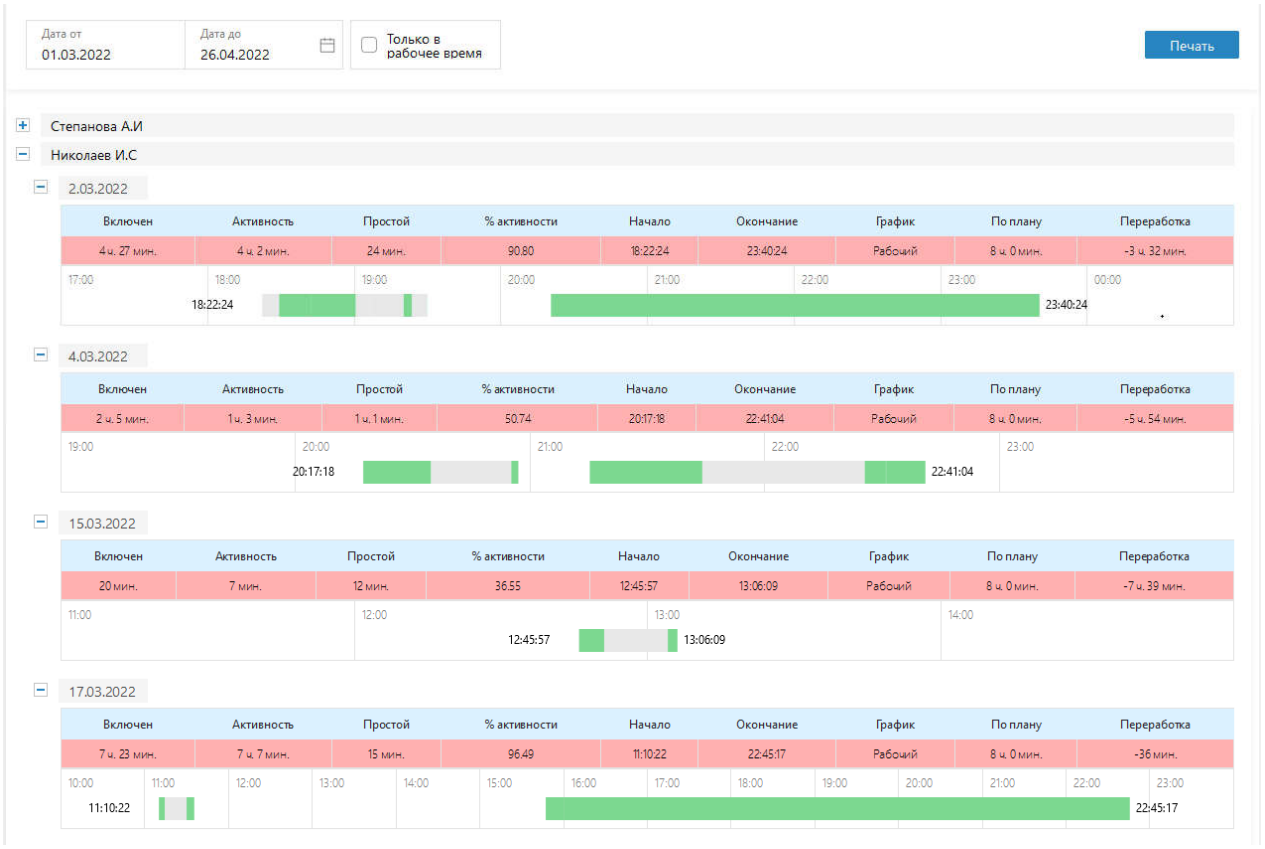
Строится по конкретному сотруднику и содержит, с разбивкой по дням, за каждый день построения отчета:

- количество отработанных часов
- кол-во часов активной работы (время работы минус простой)
- процент активности
- время начала рабочего дня (фактическое)
- время окончания рабочего дня (фактическое)
- продолжительность рабочего дня по графику
- рабочий ли это день по графику
- количество часов переработки или недоработки.



Цветом выделены те дни, когда сотрудник недоработал (количество отработанного времени менее положенного по графику) или когда был совершен прогул.

В веб версии, у данного отчета также имеется графическая отрисовка рабочего дня с периодами активности и простоя.

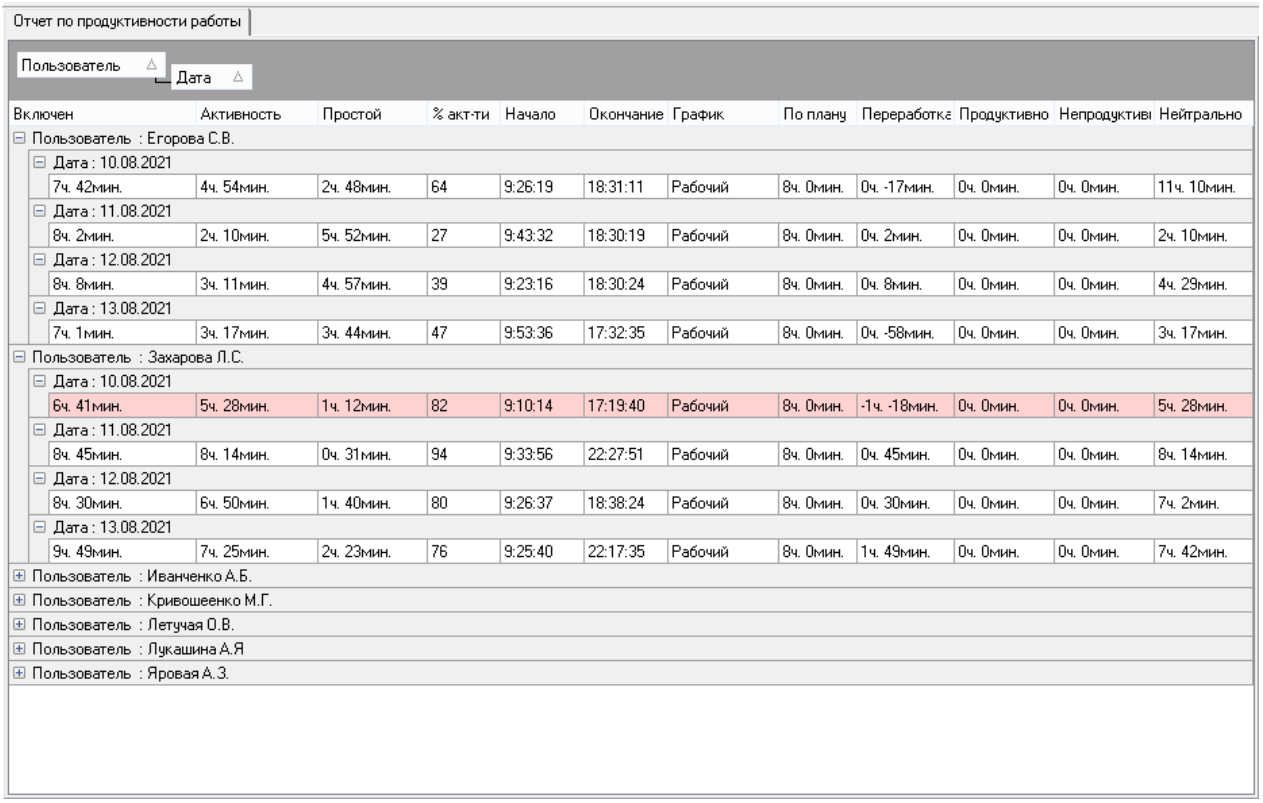


6.12.3 Отчет по продуктивности работы.

Этот отчет можно построить как самостоятельно по выбранным сотрудникам, так и можно перейти на него из суммарного отчета по рабочему времени. Для этого достаточно щелкнуть правой клавишей мыши по интересующему сотруднику и выбрать в выпадающем меню вариант.

Данный отчет содержит те же данные, что и Табель (предыдущий отчет) плюс к этому, количество часов Продуктивной работы, кол-во часов Непродуктивной работы и кол-во часов нейтральной работы. Строится он по конкретному сотруднику с разбивкой информации за каждый день построения отчета.

Продуктивности, непродуктивность, нейтральность считается для приложений и сайтов, в которых работал сотрудник на основе профиля продуктивности. Профиль продуктивности может быть задан как для всего функционального отдела, так и для конкретного сотрудника свой.



Отчет по продуктивности работы

Пользователь | Дата

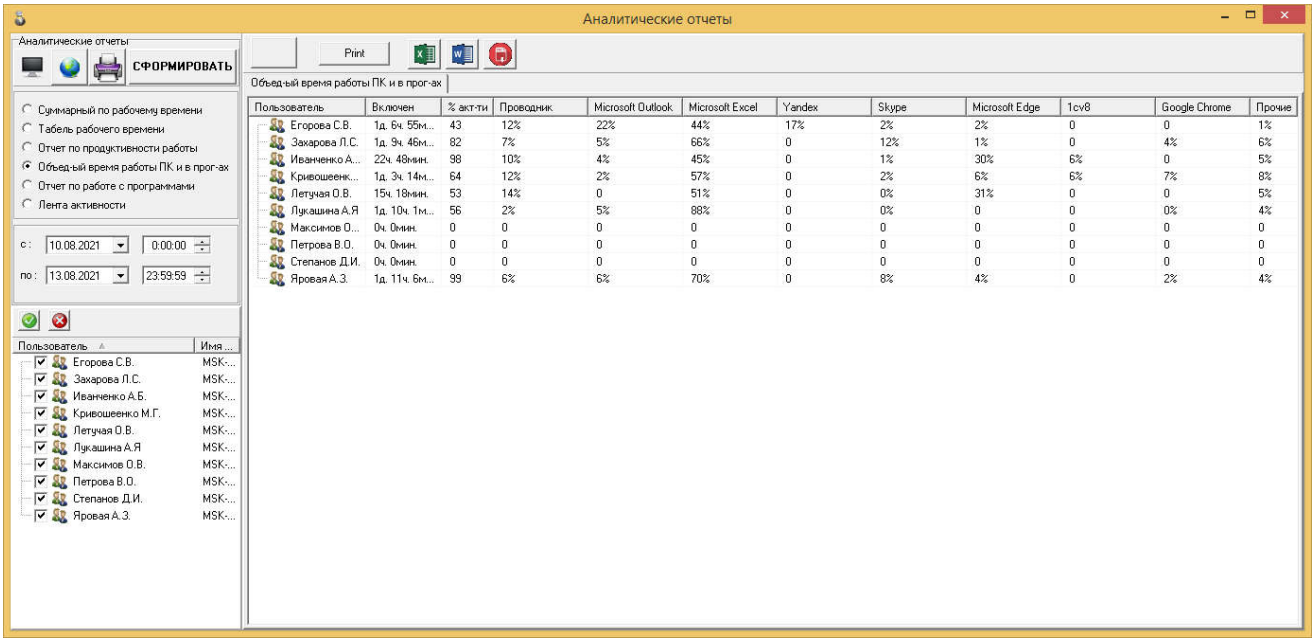
Включен	Активность	Простой	% акт-ти	Начало	Окончание	График	По плану	Переработка	Продуктивно	Непродуктиви	Нейтрально
Пользователь : Егорова С.В.											
Дата : 10.08.2021											
7ч. 42мин.	4ч. 54мин.	2ч. 48мин.	64	9:26:19	18:31:11	Рабочий	8ч. 0мин.	0ч. -17мин.	0ч. 0мин.	0ч. 0мин.	11ч. 10мин.
Дата : 11.08.2021											
8ч. 2мин.	2ч. 10мин.	5ч. 52мин.	27	9:43:32	18:30:19	Рабочий	8ч. 0мин.	0ч. 2мин.	0ч. 0мин.	0ч. 0мин.	2ч. 10мин.
Дата : 12.08.2021											
8ч. 8мин.	3ч. 11мин.	4ч. 57мин.	39	9:23:16	18:30:24	Рабочий	8ч. 0мин.	0ч. 8мин.	0ч. 0мин.	0ч. 0мин.	4ч. 29мин.
Дата : 13.08.2021											
7ч. 1мин.	3ч. 17мин.	3ч. 44мин.	47	9:53:36	17:32:35	Рабочий	8ч. 0мин.	0ч. -58мин.	0ч. 0мин.	0ч. 0мин.	3ч. 17мин.
Пользователь : Захарова Л.С.											
Дата : 10.08.2021											
6ч. 41мин.	5ч. 28мин.	1ч. 12мин.	82	9:10:14	17:19:40	Рабочий	8ч. 0мин.	-1ч. -18мин.	0ч. 0мин.	0ч. 0мин.	5ч. 28мин.
Дата : 11.08.2021											
8ч. 45мин.	8ч. 14мин.	0ч. 31мин.	94	9:33:56	22:27:51	Рабочий	8ч. 0мин.	0ч. 45мин.	0ч. 0мин.	0ч. 0мин.	8ч. 14мин.
Дата : 12.08.2021											
8ч. 30мин.	6ч. 50мин.	1ч. 40мин.	80	9:26:37	18:38:24	Рабочий	8ч. 0мин.	0ч. 30мин.	0ч. 0мин.	0ч. 0мин.	7ч. 2мин.
Дата : 13.08.2021											
9ч. 49мин.	7ч. 25мин.	2ч. 23мин.	76	9:25:40	22:17:35	Рабочий	8ч. 0мин.	1ч. 49мин.	0ч. 0мин.	0ч. 0мин.	7ч. 42мин.
Пользователь : Иванченко А.Б.											
Пользователь : Кривошеенко М.Г.											
Пользователь : Летучая О.В.											
Пользователь : Лукашина А.Я											
Пользователь : Яровая А.З.											

6.12.4 Объединенный отчет по времени работы на ПК и в программах

Строится для всех выбранных отделов или сотрудников в одной таблице и содержит:

- кол-во часов, отработанных за период построения отчета
- процент активности (какой% приходится на активность, а какой на простой)
- в отдельных столбцах процентное соотношение времени, отработанного в каждой из наиболее часто используемых программ.

Отдельные столбцы создаются для приложений, в которых совершено более 5% всей активности за период отчета. Остальные приложения, время работы которых менее 5% от общего времени работы, помещаются в категорию «Прочие».



Вариант для печати этого отчета:

Объед-ный отчет время работы ПК и приложений

с: 10.08.2021 по: 13.08.2021 23:59:59

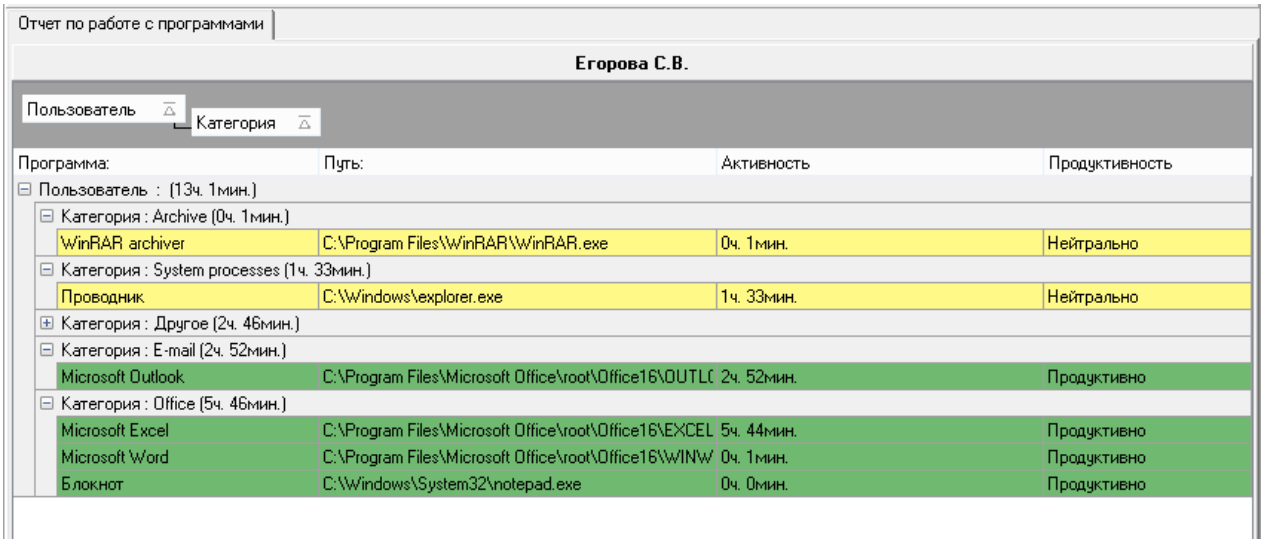
Компьютер	Включен	% акт-ти	Проводник	Microsoft Outlook	Microsoft Excel	Yandex	Skype	Microsoft Edge	1cv8	Google Chrome	Прочие
Егорова С.В.	1д. 6ч. 55мин.	43	12%	22%	44%	17%	2%	2%	0	0	1%
Захарова Л.С.	1д. 9ч. 46мин.	82	7%	5%	66%	0	12%	1%	0	4%	6%
Иванченко А.Б.	22ч. 48мин.	98	10%	4%	45%	0	1%	30%	6%	0	5%
Кривошеенко М.Г.	1д. 3ч. 14мин.	64	12%	2%	57%	0	2%	6%	6%	7%	8%
Летучая О.В.	15ч. 18мин.	53	14%	0	51%	0	0%	31%	0	0	5%
Лукашина А.Я	1д. 10ч. 1мин.	56	2%	5%	88%	0	0%	0	0	0%	4%
Максимов О.В.	0ч. 0мин.	0	0	0	0	0	0	0	0	0	0
Петрова В.О.	0ч. 0мин.	0	0	0	0	0	0	0	0	0	0
Степанов Д.И.	0ч. 0мин.	0	0	0	0	0	0	0	0	0	0
Яровая А.З.	1д. 11ч. 6мин.	99	6%	6%	70%	0	8%	4%	0	2%	4%

6.12.5 Отчет по работе с программами.

Строится для конкретного сотрудника. Содержит:

- наименование программы

- время активной работы в программе (кол-во часов и минут, в течение которых приложение было активно и при этом на компьютере не сработало событие простоя, т.е. есть события ввода от клавиатуры или мыши).
- к какой категории приложений программа относится (Офис, Браузеры, Служебные и т.д.)
- признак продуктивности: Продуктивно/непродуктивно/нейтрально. Определяется для данного сотрудника в соответствии с его профилем продуктивности.


Отчет по работе с программами

Егорова С.В.

Пользователь | Категория

Программа:	Путь:	Активность	Продуктивность
Пользователь : (13ч. 1мин.)			
Категория : Archive (0ч. 1мин.)			
WinRAR archiver	C:\Program Files\WinRAR\WinRAR.exe	0ч. 1мин.	Нейтрально
Категория : System processes (1ч. 33мин.)			
Проводник	C:\Windows\explorer.exe	1ч. 33мин.	Нейтрально
Категория : Другое (2ч. 46мин.)			
Категория : E-mail (2ч. 52мин.)			
Microsoft Outlook	C:\Program Files\Microsoft Office\root\Office16\OUTLO	2ч. 52мин.	Продуктивно
Категория : Office (5ч. 46мин.)			
Microsoft Excel	C:\Program Files\Microsoft Office\root\Office16\EXCEL	5ч. 44мин.	Продуктивно
Microsoft Word	C:\Program Files\Microsoft Office\root\Office16\WINW	0ч. 1мин.	Продуктивно
Блокнот	C:\Windows\System32\notepad.exe	0ч. 0мин.	Продуктивно

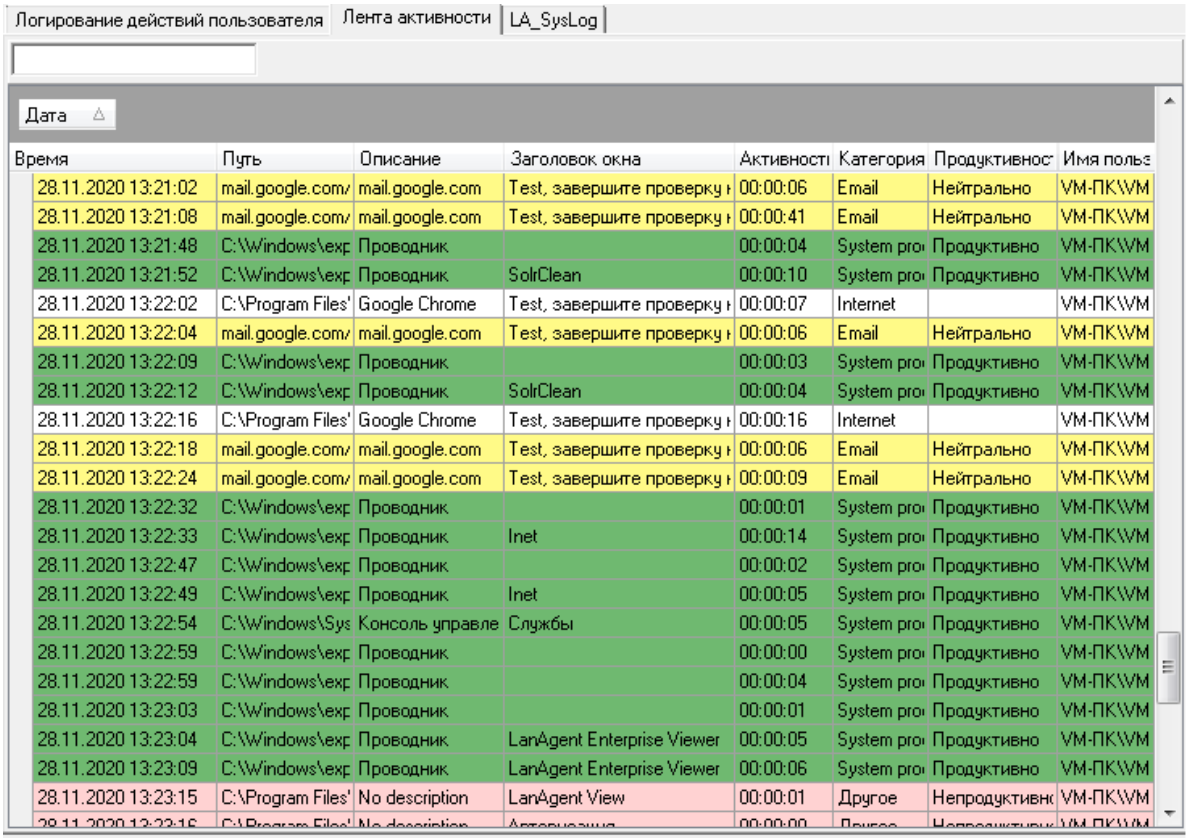
Строки этого отчета раскрашены зеленым, желтым или красным цветом в зависимости от продуктивности программы для данного сотрудника.

6.12.6 Лента активности.

Является детализацией рабочего дня и содержит в хронологическом порядке события включения/выключения компьютера, работы в программах и сайтах с указанием продолжительности. Строится для конкретного сотрудника за определенный день (если за период, то с разбивкой информации по дням).

Содержит:

- время события
- путь программы или адрес сайта
- описание (название программы или домен сайта)
- заголовок окна программы или сайта
- время активности в часах-минутах-секундах
- к какой категории программ или сайтов относится (Почта, Офис и т.д.)
- признак продуктивности: продуктивно/непродуктивно/нейтрально в соответствии с профилем продуктивности сотрудника.



Логирование действий пользователя | Лента активности | LA_SysLog

Дата

Время	Путь	Описание	Заголовок окна	Активности	Категория	Продуктивнос	Имя польз
28.11.2020 13:21:02	mail.google.com/	mail.google.com	Test, завершите проверку н	00:00:06	Email	Нейтрально	VM-ПК\VM
28.11.2020 13:21:08	mail.google.com/	mail.google.com	Test, завершите проверку н	00:00:41	Email	Нейтрально	VM-ПК\VM
28.11.2020 13:21:48	C:\Windows\exp	Проводник		00:00:04	System pro	Продуктивно	VM-ПК\VM
28.11.2020 13:21:52	C:\Windows\exp	Проводник	SolrClean	00:00:10	System pro	Продуктивно	VM-ПК\VM
28.11.2020 13:22:02	C:\Program Files'	Google Chrome	Test, завершите проверку н	00:00:07	Internet		VM-ПК\VM
28.11.2020 13:22:04	mail.google.com/	mail.google.com	Test, завершите проверку н	00:00:06	Email	Нейтрально	VM-ПК\VM
28.11.2020 13:22:09	C:\Windows\exp	Проводник		00:00:03	System pro	Продуктивно	VM-ПК\VM
28.11.2020 13:22:12	C:\Windows\exp	Проводник	SolrClean	00:00:04	System pro	Продуктивно	VM-ПК\VM
28.11.2020 13:22:16	C:\Program Files'	Google Chrome	Test, завершите проверку н	00:00:16	Internet		VM-ПК\VM
28.11.2020 13:22:18	mail.google.com/	mail.google.com	Test, завершите проверку н	00:00:06	Email	Нейтрально	VM-ПК\VM
28.11.2020 13:22:24	mail.google.com/	mail.google.com	Test, завершите проверку н	00:00:09	Email	Нейтрально	VM-ПК\VM
28.11.2020 13:22:32	C:\Windows\exp	Проводник		00:00:01	System pro	Продуктивно	VM-ПК\VM
28.11.2020 13:22:33	C:\Windows\exp	Проводник	Inet	00:00:14	System pro	Продуктивно	VM-ПК\VM
28.11.2020 13:22:47	C:\Windows\exp	Проводник		00:00:02	System pro	Продуктивно	VM-ПК\VM
28.11.2020 13:22:49	C:\Windows\exp	Проводник	Inet	00:00:05	System pro	Продуктивно	VM-ПК\VM
28.11.2020 13:22:54	C:\Windows\Sys	Консоль управле	Службы	00:00:05	System pro	Продуктивно	VM-ПК\VM
28.11.2020 13:22:59	C:\Windows\exp	Проводник		00:00:00	System pro	Продуктивно	VM-ПК\VM
28.11.2020 13:22:59	C:\Windows\exp	Проводник		00:00:04	System pro	Продуктивно	VM-ПК\VM
28.11.2020 13:23:03	C:\Windows\exp	Проводник		00:00:01	System pro	Продуктивно	VM-ПК\VM
28.11.2020 13:23:04	C:\Windows\exp	Проводник	LanAgent Enterprise Viewer	00:00:05	System pro	Продуктивно	VM-ПК\VM
28.11.2020 13:23:09	C:\Windows\exp	Проводник	LanAgent Enterprise Viewer	00:00:06	System pro	Продуктивно	VM-ПК\VM
28.11.2020 13:23:15	C:\Program Files'	No description	LanAgent View	00:00:01	Другое	Непродуктивно	VM-ПК\VM

В веб версии просмотра данных, данный отчет имеет похожий вид

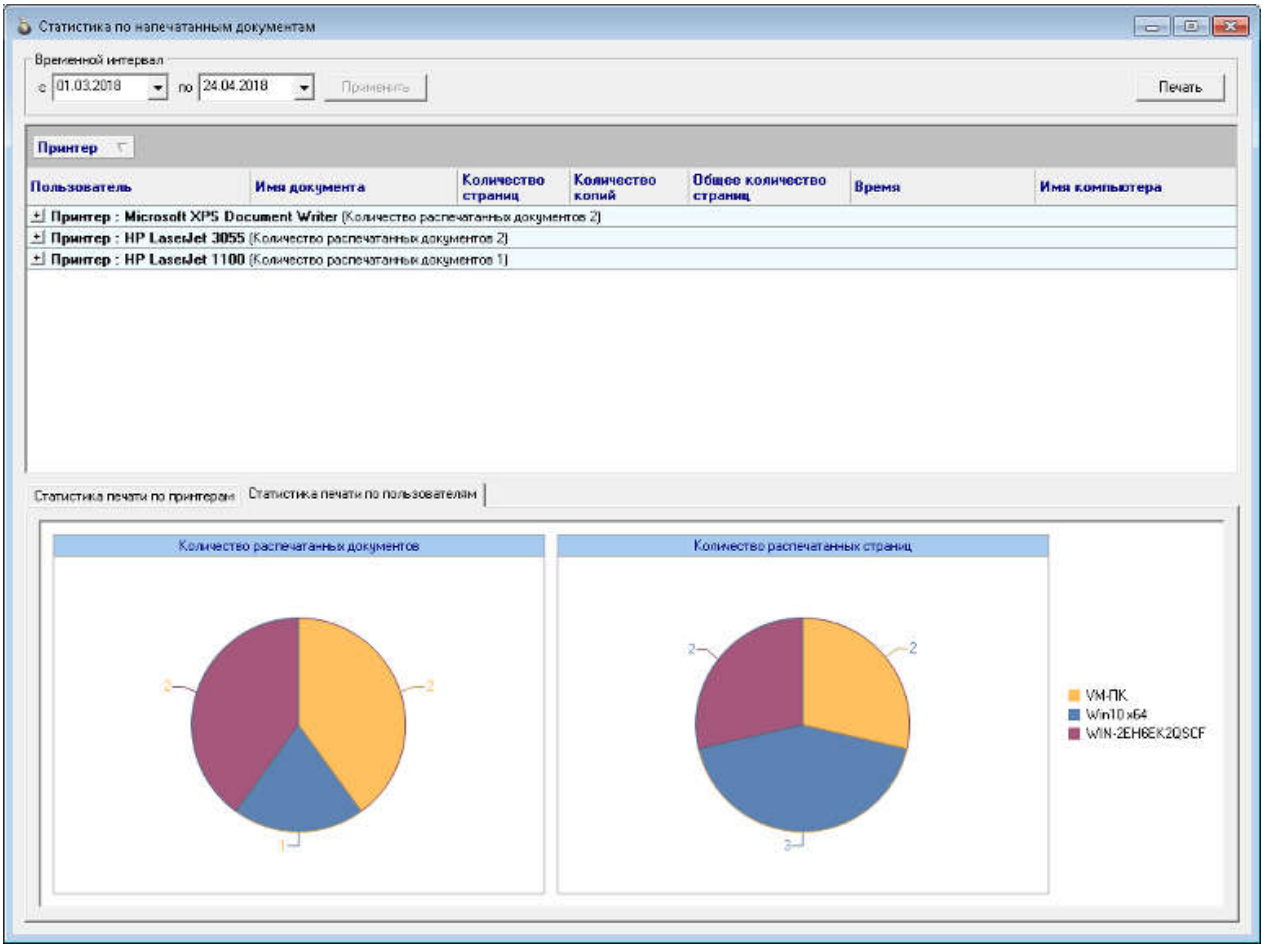
Степанов З.И.

3.07.2023

Время	Путь	Описание	Заголовок окна	Активность	Категория	Продуктивность
03.07.2023 12:55:37		Включение компьютера		0 мин		Браузер
03.07.2023 12:56:01	C:\Program Files\Google\Chrome\Application\chrome.exe	Google Chrome	frontend - Google Chrome	менее 1 мин	Internet	Браузер
03.07.2023 12:56:03	127.0.0.1/search	127.0.0.1	frontend - Google Chrome	менее 1 мин	Другое	Нейтрально
03.07.2023 12:56:15	C:\Program Files (x86)\LanAgent Enterprise Viewer\LA Enterprise View.exe	No description		менее 1 мин	LanAgent	Продуктивно
03.07.2023 12:56:16	C:\Program Files (x86)\LanAgent Enterprise Viewer\LA Enterprise View.exe	No description	LanAgent View	менее 1 мин	LanAgent	Продуктивно
03.07.2023 12:56:22	google.com/search?q=работа+в+перми+удаленно&oq=работа+в+перми&aqs=chrome.2.69i57j0i512l9.1644024148j0j15&sourceid=chrome&ie=UTF-8	google.com	Новая вкладка - Google Chrome	менее 1 мин	Поисковики	Нейтрально
03.07.2023 12:56:53	google.com/search?q=работа+в+москве+вакансии&sxsrf=AB5stBjUghRzl9SEYC7AwUcUhreUQjy1w%3A1688371003609&ei=O3-IZLTUMak3AOZ7quqAQ&oq=работа+в+москве&gs_lcp=Cgxnd3Mtd2l6LXNlcnAQARgFMgsIABCABBCxAxCDATIFCAAQgAQyCwgAEIAEELEDEIMBMgsIABCABBCxAxCDATIFCAAQgAQyBQgAEIAEMgsIABCABBCxAxCDATILCAAQgAQQsQMQgwEyBQgAEIAEMgUIABCABDoKCAAQRxDWBBCwAzoICAAQgAQQsQNKBAhBGABQ3wZY1w5guzFoAXABeACAAV2IAcQDkgEBNpgBAKABAcABAcgBCA&sclient=gws-wiz-serp	google.com	работа в перми удаленно - Поиск в Google - Google Chrome	менее 1 мин	Поисковики	Нейтрально
03.07.2023 12:57:14	C:\Program Files\Google\Chrome\Application\chrome.exe	Google Chrome	www.google.com запрашивает разрешение на:	менее 1 мин	Internet	Браузер
03.07.2023 12:57:16	C:\Program Files (x86)\LanAgent Enterprise Viewer\LA Enterprise View.exe	No description		0 мин	LanAgent	Продуктивно
03.07.2023 12:57:16	C:\Program Files (x86)\LanAgent Enterprise Viewer\LA Enterprise View.exe	No description	LanAgent View	менее 1 мин	LanAgent	Продуктивно
03.07.2023 12:57:38	C:\Program Files (x86)\LanAgent Enterprise Viewer\LA Enterprise View.exe	No description	LanAgent Enterprise Viewer	менее 1 мин	LanAgent	Продуктивно
03.07.2023 12:57:40	C:\Program Files (x86)\LanAgent Enterprise Viewer\LA Enterprise View.exe	No description	Формирование задач	менее 1 мин	LanAgent	Продуктивно
03.07.2023 12:58:00	C:\Program Files (x86)\LanAgent Enterprise Viewer\LA Enterprise View.exe	No description	LanAgent Enterprise Viewer	менее 1 мин	LanAgent	Продуктивно
			Table : [HMAIL] : C:\Program Files			

6.12.7 Отчет по печати документов на принтере

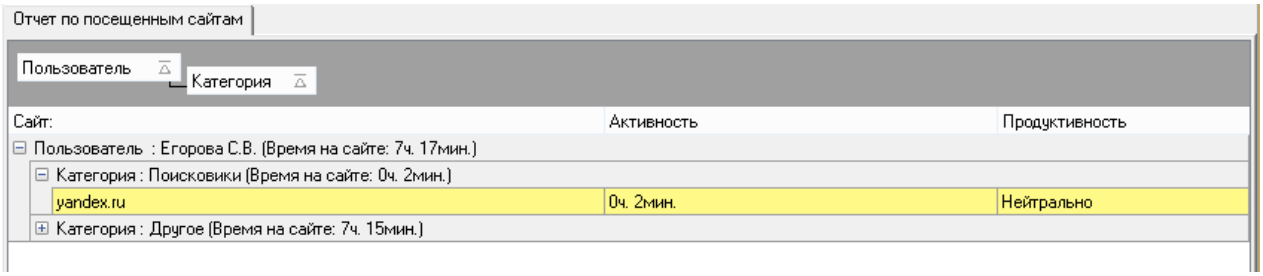
Содержит информацию по количеству страниц, напечатанных на каждом из принтеров сотрудниками. Информация может быть представлена с группировкой как по принтерам, так и по сотрудникам. Также он содержит детализацию печати по документам с указанием наименования документа.



6.12.8 Отчет по посещению сайтов.

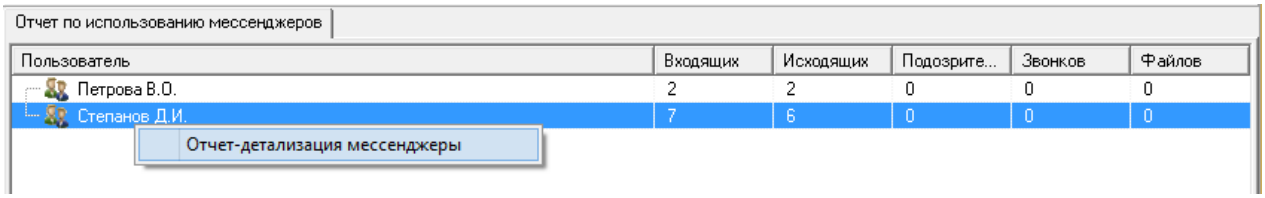
Строится для конкретного сотрудника. Содержит:

- ссылка на сайт (домен сайта)
- время, проведенное на сайте в часах-минута
- К какой категории относится данный сайт (Поиск работы, Соц сети, Развлечения, Фильмы онлайн и т.д.)
- доля времени на этом сайте по сравнению с общим временем, проведенным на сайтах, в %



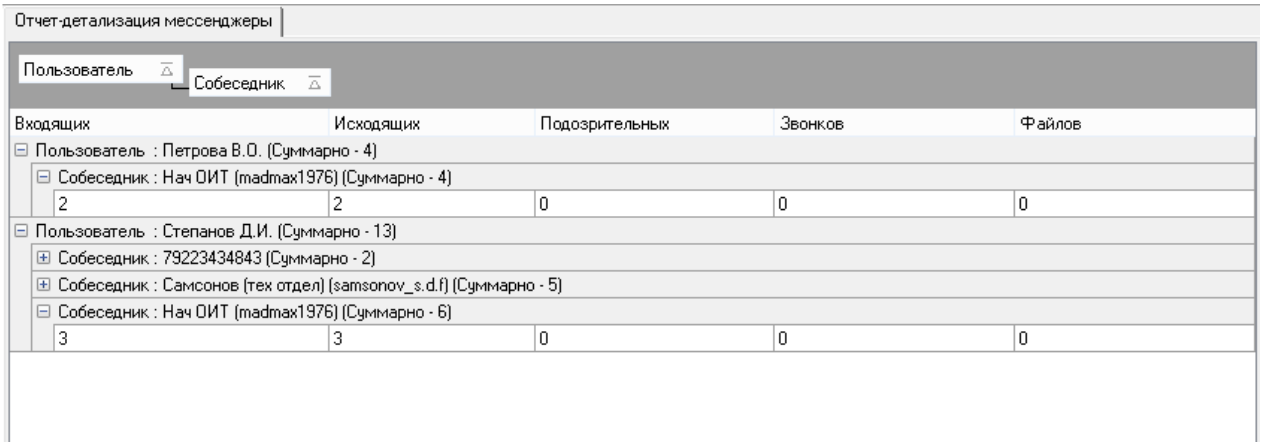
6.12.9 Отчет по переписке в мессенджерах.

И **Отчет по переписке в почте**. Строятся для выбранных отделов или конкретных сотрудников в одной таблице. Содержат статистику переписки и общения в мессенджерах или через почту соответственно.



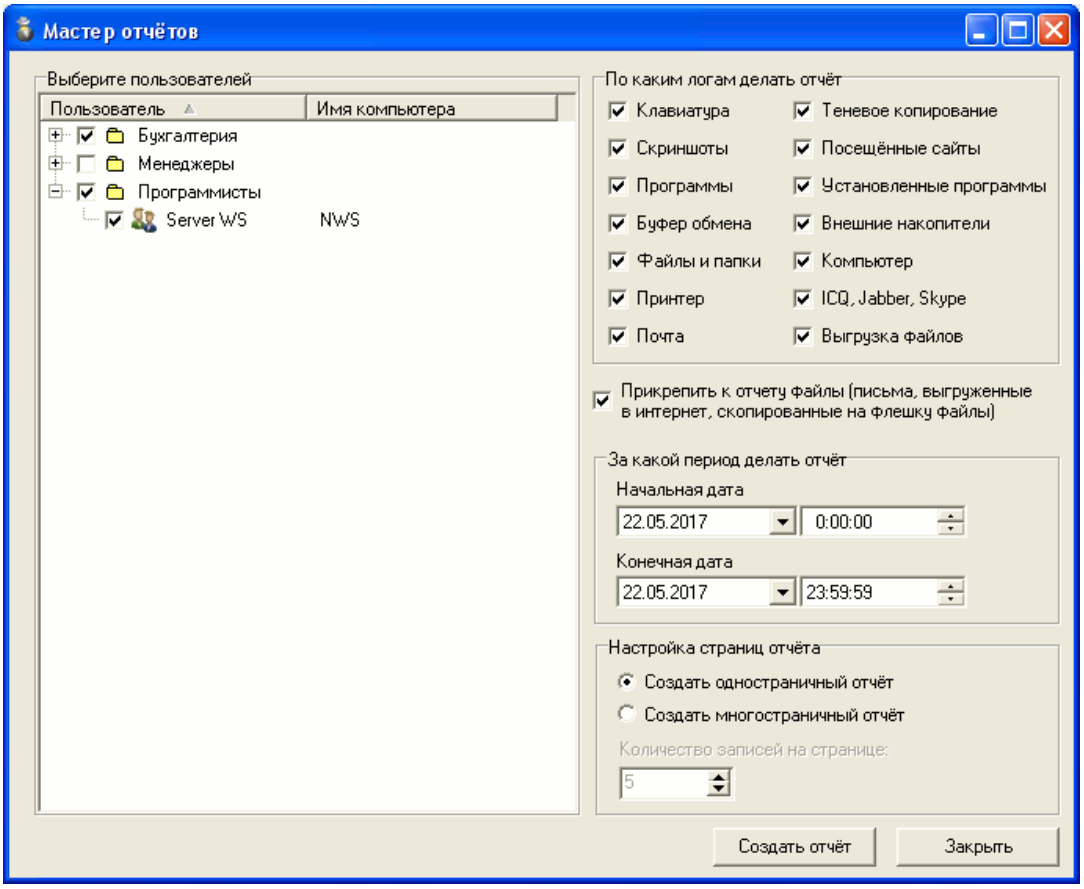
6.12.10 Отчет по переписке с детализацией по собеседникам.

Строится для конкретного сотрудника. Содержит статистику по общению в мессенджерах с группировкой ее по собеседникам.



6.13 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.

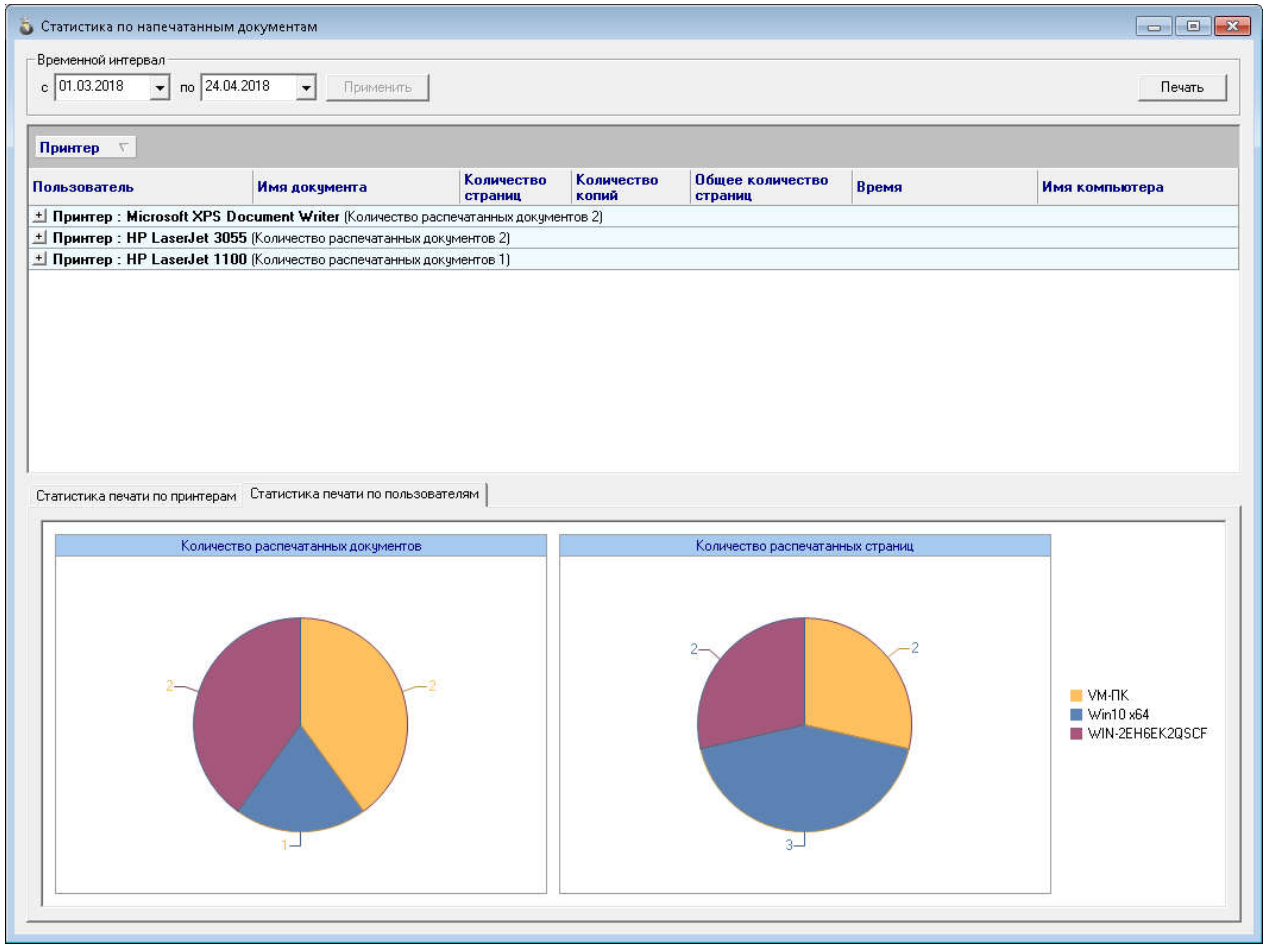
Данный отчет позволяет включить в себя также и все файлы данных: файлы писем, вложенных файлов, копии файлов, размещенных на USB накопители и т.д. Это регулируется соответствующей опцией.

Сам отчет можно создать как одностраничный html документ или многостраничный.

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

6.14 Статистика по принтерам

Данный отчет позволяет просматривать статистику по напечатанным документам по всем принтерам, используемым в компании.

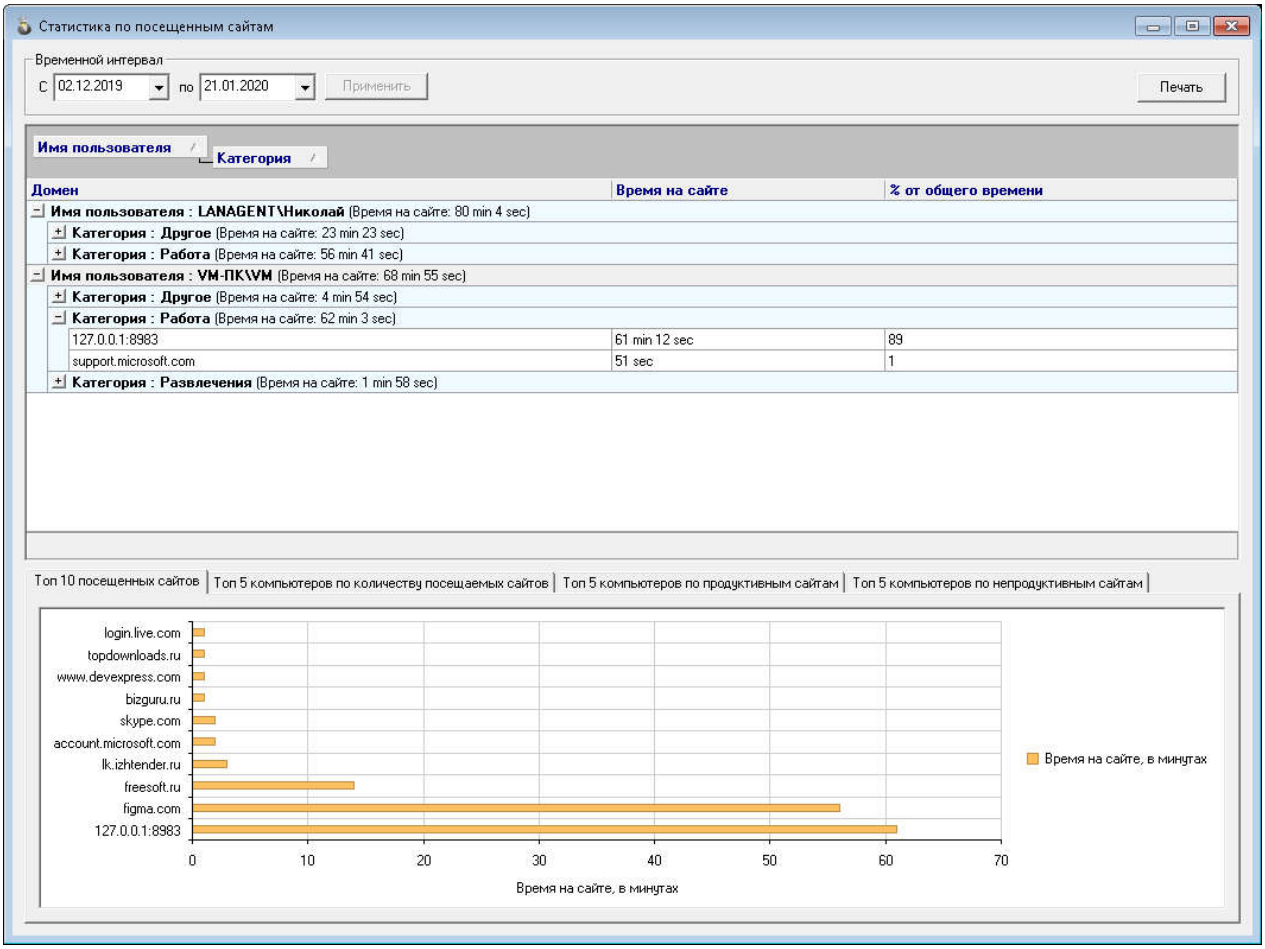


Данные отображаются по всем контролируемым компьютерам за указанный промежуток времени. При этом можно легко сгруппировать их как по принтерам и посмотреть какой из них используется больше, так и по пользователям.

Отчет позволяет легко найти ответ на вопросы: кто в компании печатает больше всего, кто печатал на принтере с дорогой печатью (цветной лазерный, к примеру), как оптимизировать этот процесс.

6.15 Статистика по сайтам

Данный отчет позволяет просматривать статистику по использованию веб ресурсов.



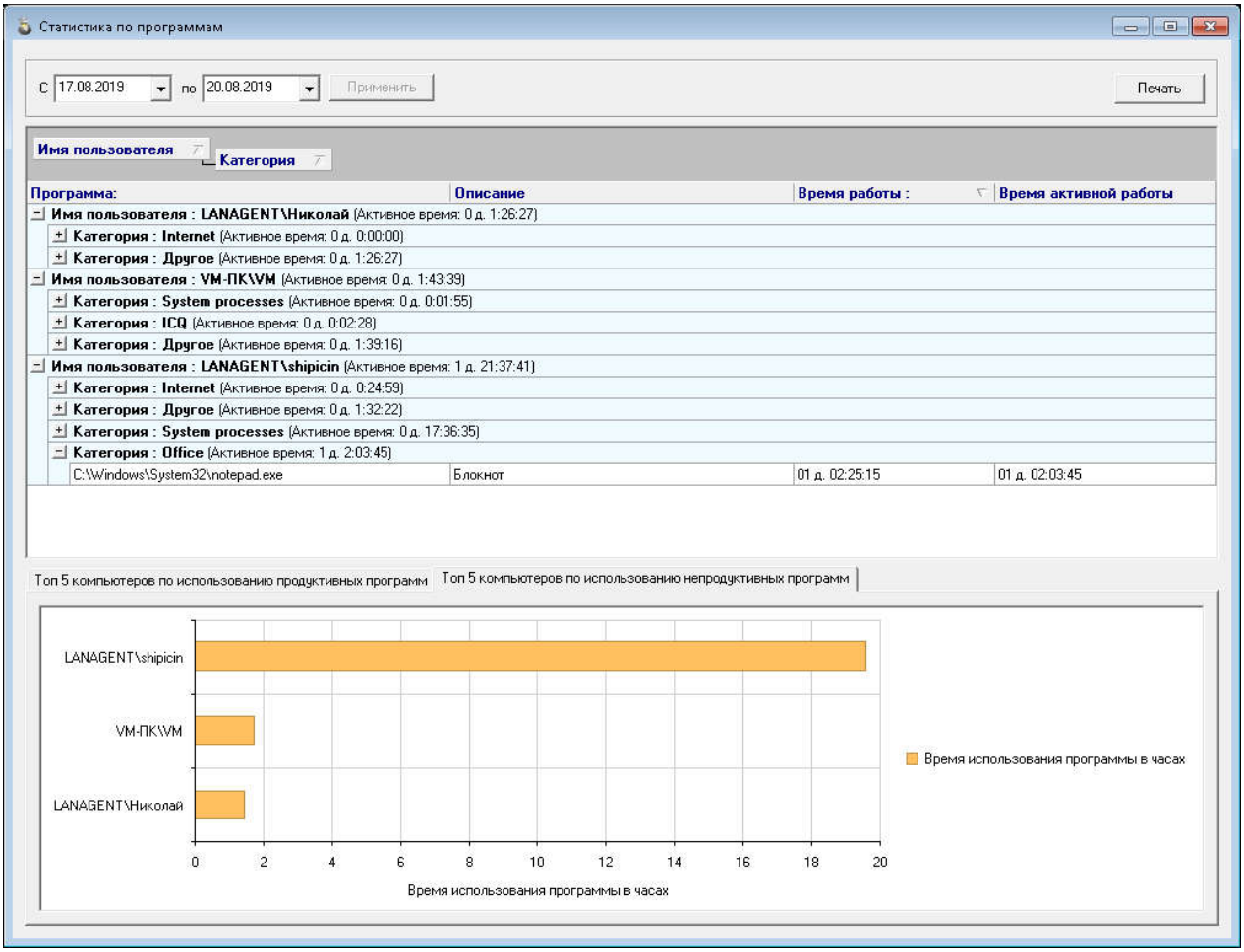
Данные отображаются по всем контролируемым компьютерам за указанный промежуток времени. При этом можно легко сгруппировать их как по пользователям, так и по категориям сайтов.

Так можно увидеть сколько времени суммарно проведено пользователем на той или иной категории сайтов.

Также статистика содержит список из 10 наиболее популярных у работников веб сайтах, список пользователей, которые проводят больше всего времени в интернет, а также список сотрудников, которые больше остальных посещают продуктивные или непродуктивные сайты.

6.16 Статистика по программам

Данный отчет позволяет просматривать статистику по использованию программ пользователями.



Данные отображаются по всем контролируемым компьютерам за указанный промежуток времени. При этом можно легко сгруппировать их как по пользователям, так и по категориям программ.

Так можно увидеть сколько времени суммарно отработали пользователем в той или иной категории программ.

Также статистика содержит список сотрудников, которые больше остальных работали в продуктивных или непродуктивные программах.

6.17 Отчеты в web интерфейсе (через браузер)

При работе через браузер, отчеты-выборки строятся непосредственно на самих вкладках данных при помощи кнопки экспорта.

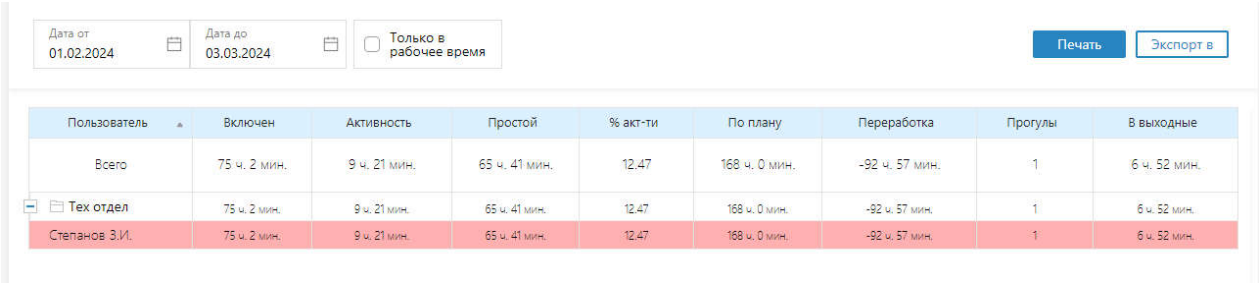
Вычисляемые отчеты в веб, так же как и в приложении вьюера, сгруппированы по трем категориям:

- отчеты по работе ПК и в программах;
- отчеты, связанные с Интернет
- отчеты по печати документов на принтере.

При этом их можно условно разделить на обобщенные (показывают суммарные данные по активности) и детализованные.

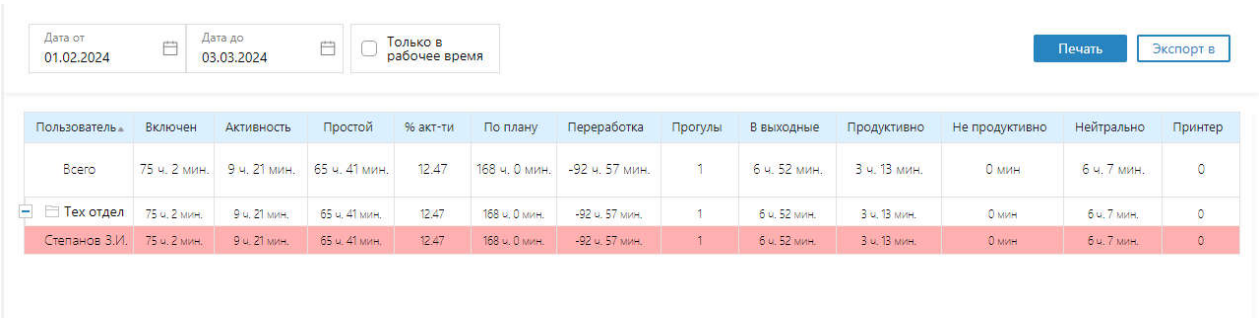
К обобщенным можно отнести «Суммарный по рабочему времени», «Тепловая карта» и «Суммарный ПК, продуктивность, принтер».

Суммарный отчет по рабочему времени содержит время работы ПК сотрудника, какая его часть приходится на активную работу и сколько – на простой. Сколько сотрудник должен был отработать по плану (в соответствии с графиком рабочего времени, выходных и отпусков), наличие прогулов, а также переработка/недоработка. В том числе, переработка в выходные дни.



Пользователь	Включен	Активность	Простой	% акт-ти	По плану	Переработка	Прогулы	В выходные
Всего	75 ч. 2 мин.	9 ч. 21 мин.	65 ч. 41 мин.	12.47	168 ч. 0 мин.	-92 ч. 57 мин.	1	6 ч. 52 мин.
Тех отдел	75 ч. 2 мин.	9 ч. 21 мин.	65 ч. 41 мин.	12.47	168 ч. 0 мин.	-92 ч. 57 мин.	1	6 ч. 52 мин.
Степанов З.И.	75 ч. 2 мин.	9 ч. 21 мин.	65 ч. 41 мин.	12.47	168 ч. 0 мин.	-92 ч. 57 мин.	1	6 ч. 52 мин.

Суммарный ПК, продуктивность, принтер содержит все те же данные, что и предыдущий отчет, но дополнительно к ним - количество часов работы в продуктивных программах и сайтах, непродуктивных и нейтральных.

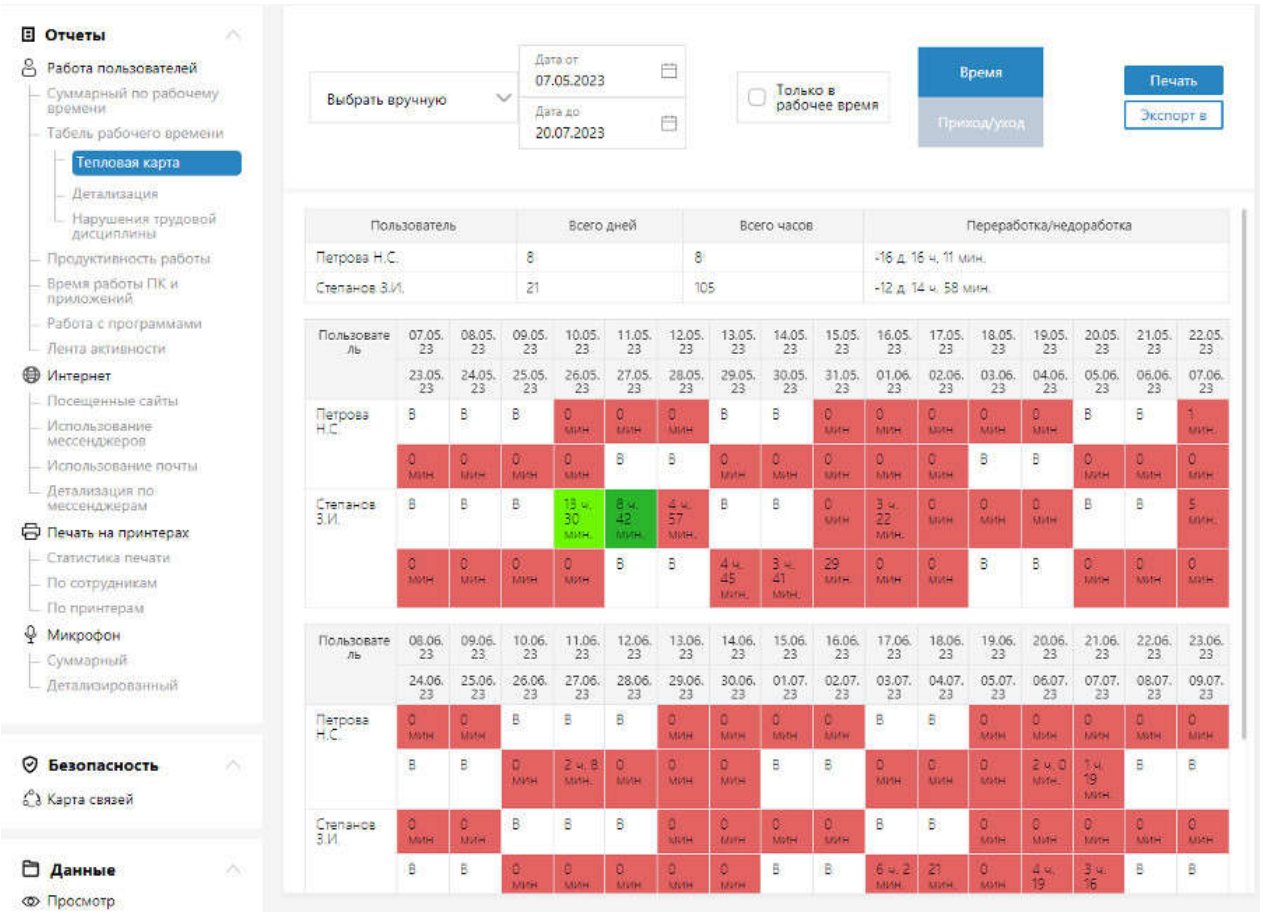


Пользователь	Включен	Активность	Простой	% акт-ти	По плану	Переработка	Прогулы	В выходные	Продуктивно	Не продуктивно	Нейтрально	Принтер
Всего	75 ч. 2 мин.	9 ч. 21 мин.	65 ч. 41 мин.	12.47	168 ч. 0 мин.	-92 ч. 57 мин.	1	6 ч. 52 мин.	3 ч. 13 мин.	0 мин	6 ч. 7 мин.	0
Тех отдел	75 ч. 2 мин.	9 ч. 21 мин.	65 ч. 41 мин.	12.47	168 ч. 0 мин.	-92 ч. 57 мин.	1	6 ч. 52 мин.	3 ч. 13 мин.	0 мин	6 ч. 7 мин.	0
Степанов З.И.	75 ч. 2 мин.	9 ч. 21 мин.	65 ч. 41 мин.	12.47	168 ч. 0 мин.	-92 ч. 57 мин.	1	6 ч. 52 мин.	3 ч. 13 мин.	0 мин	6 ч. 7 мин.	0

Тепловая карта позволяет одним взглядом оценить наличие нарушений трудовой дисциплины за период построения отчета.

Для каждого из дней сделана подкраска цветом. При отсутствии нарушений – цвет зеленый. При наличии опозданий, ранних уходов, недоработке или прогулах, происходит изменение цвета от зеленого к красному.

Таким образом, можно определить за какой из дней стоит посмотреть более детальную информацию.

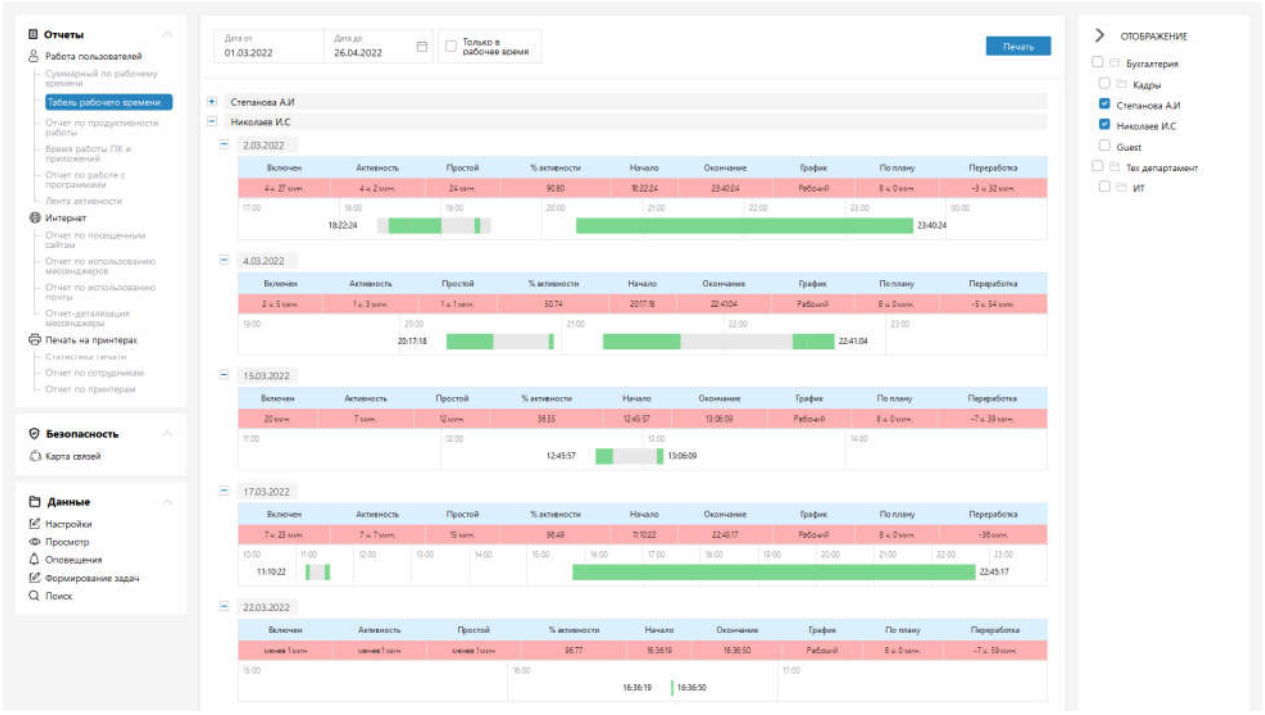


.

Через меню, открываемое по правой клавише мыши на нужной строке отчета, можно перейти к детализованному отчету.

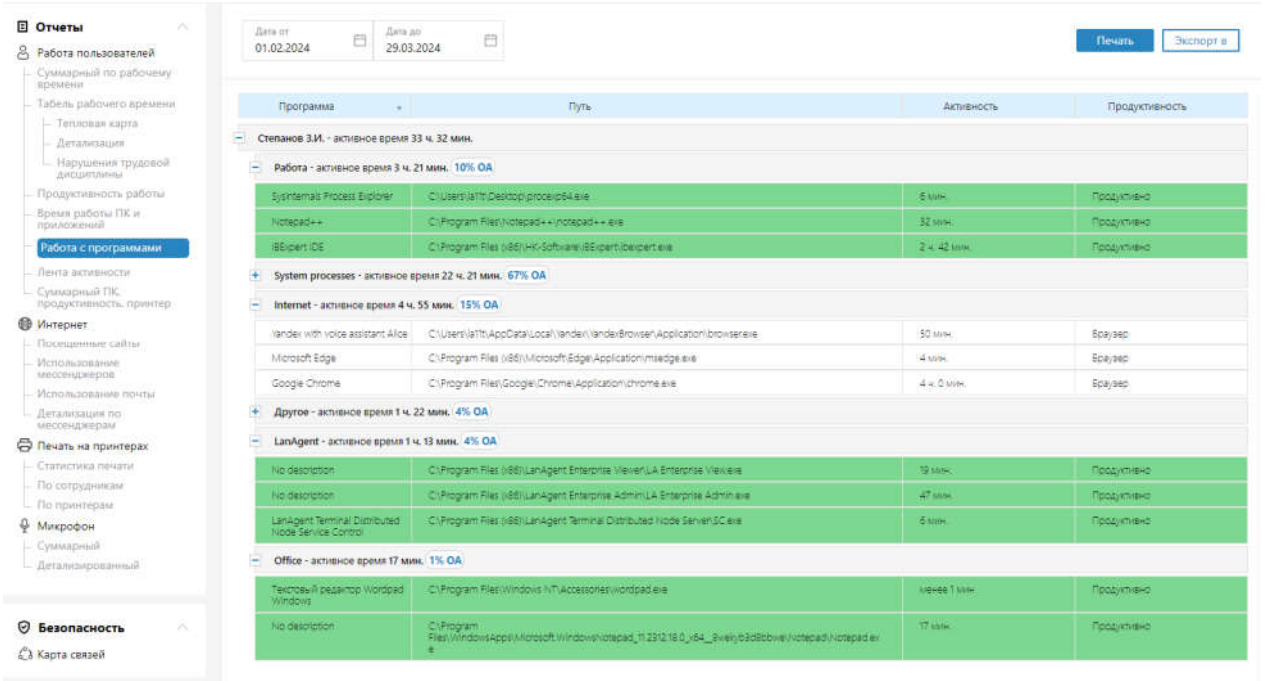
К детализованным отчетам можно отнести **Табель рабочего времени – «Детализация»**, отчет «**Продуктивность работы**», «**Время работы ПК и приложений**», «**Работа с программами**», «**Посещенные сайты**» и т.д.

Детализация табеля рабочего времени содержит информацию по времени работы ПК за каждый из дней, а также графическое отображение активности работы сотрудника. По нему видно время начала работы, завершения, периоды активности и простоя.



Отчет «**Продуктивность работы»**, дополнительно к детализации табеля содержит информацию по соотношению продуктивной, непродуктивной и нейтральный работы, с отрисовкой периодов такой активности на линии времени.

Отчет по работе с программами и **Посещенные сайты** покажут время активной работы пользователя в каждой из категорий программ и конкретных приложениях.



«**Время работы ПК и приложений**» покажет наиболее часто используемые сотрудником приложения. Также с его помощью можно определить время работы в конкретном приложении для всех выбранных пользователей.

Каждый из отчетов имеет как интерактивный вид, так и вариант для печати.

Интерактивный формат отчета позволяет в один клик переходить из общих отчетов в детализацию информации по конкретному сотруднику и возвращаться обратно к общему виду.

Отчет может быть отсортирован и сгруппирован по любому из столбцов. Также можно применять фильтрацию по конкретному значению.

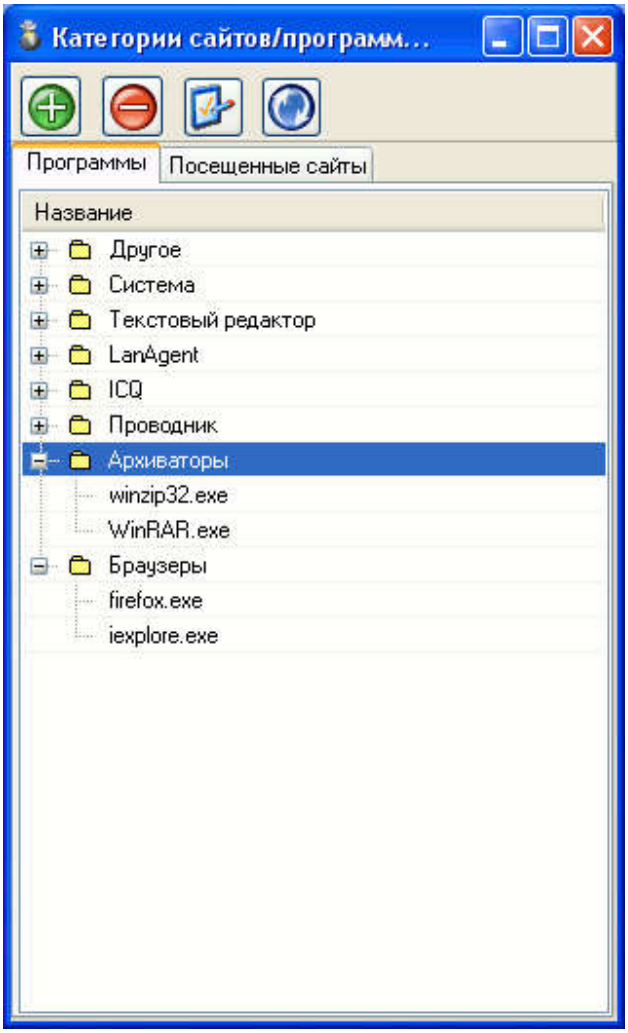
Например, можно отчет по использованию программ сгруппировать по продуктивности. Тогда отдельно будут показаны продуктивные, непродуктивные и нейтральные программы, используемые сотрудником.

Либо, задать фильтр и увидеть всех работников, использовавших 1С и просмотреть сколько времени они в этом приложении провели.

Также, в один клик можно экспортировать отчет в PDF, Excel или Word документ.

6.18 Категории программ/сайтов

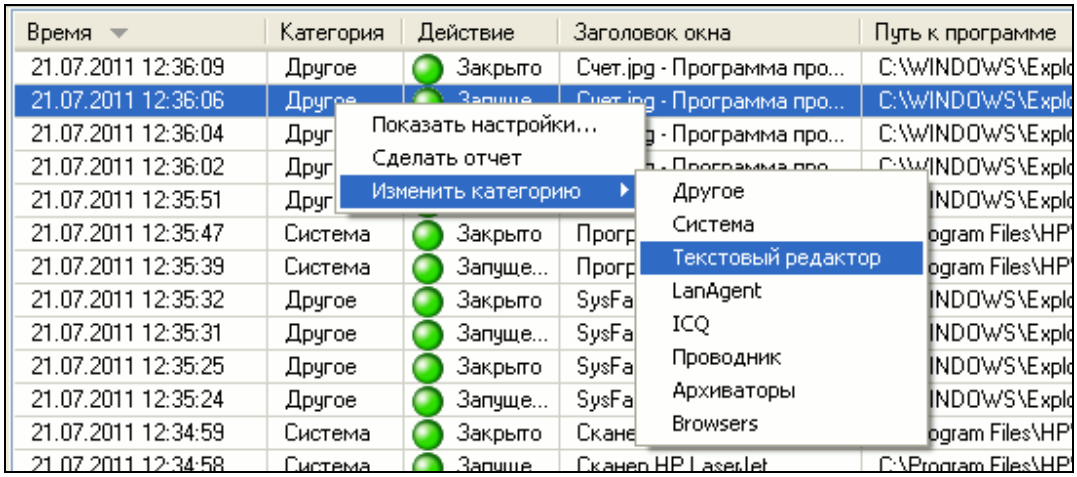
В LanAgent имеется возможность распределить все программы, запускаемые на пользовательских компьютерах, и все посещаемые сайты по категориям. Например: "Развлечение" или "Офисные программы". Категория будет отображаться при просмотре логов работы с программами и посещения веб-сайтов, Также можно формировать 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.

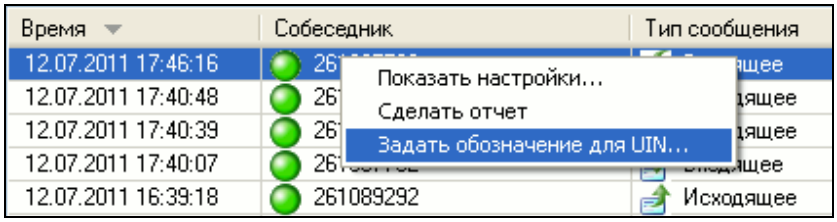
Для создания новой категории, нажмите кнопку  Перемещение программ из одной категории в другую осуществляется обычным "перетаскиванием".

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.

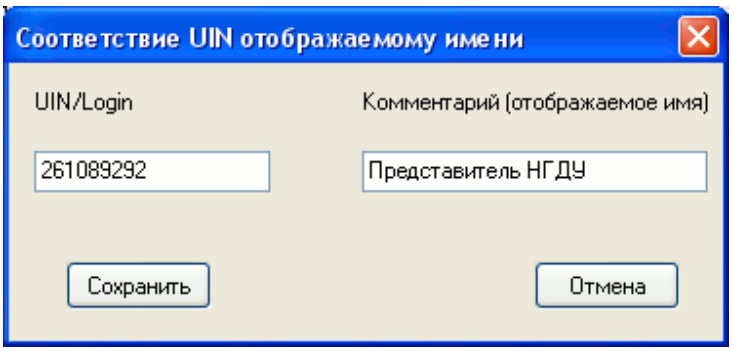


6.19 Комментарии для UIN/логинов

Для более удобного разбора переписки в мессенджерах, в LanAgent есть возможность задать комментарий (описание) для конкретного логина пользователя. 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...".

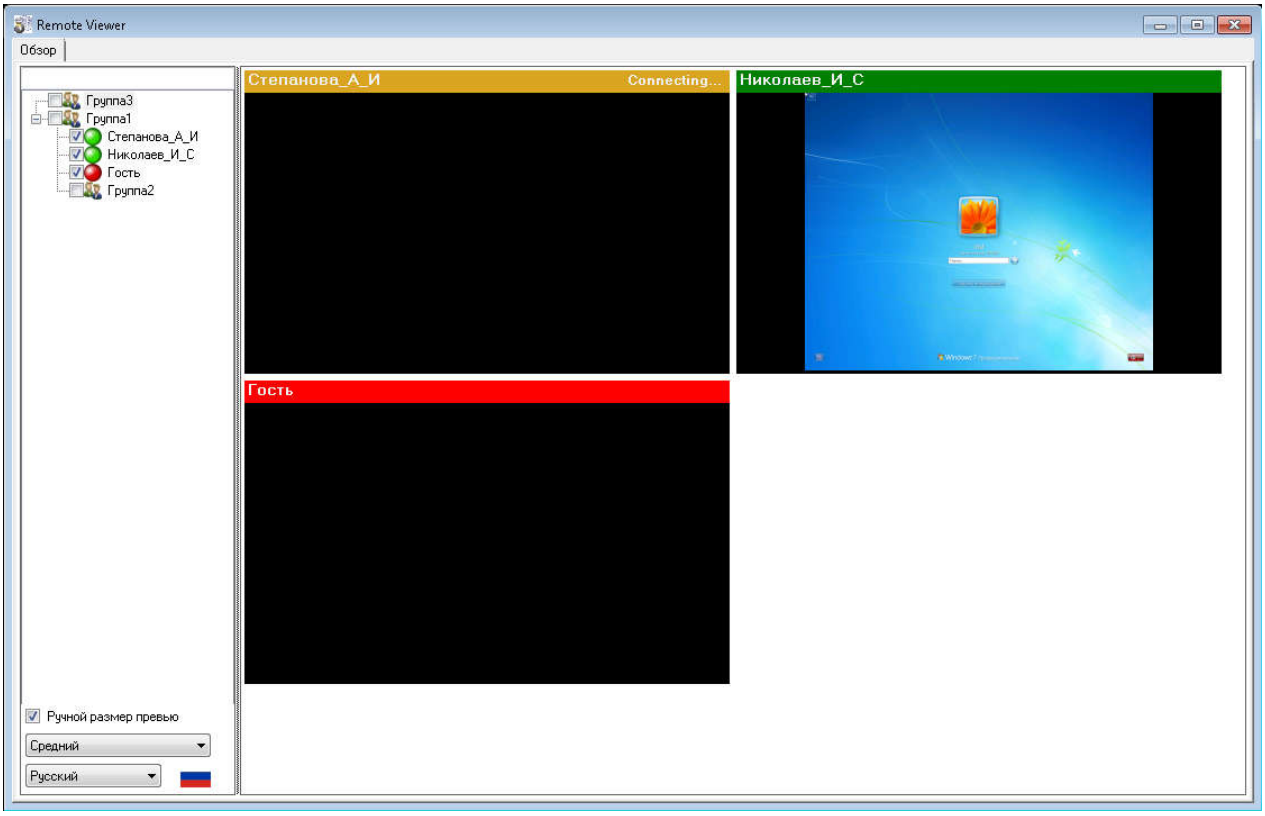


При этом откроется следующее окно. Задайте в нем комментарий и нажмите кнопку Сохранить.



6.20 Просмотр экранов контролируемых компьютеров в реальном времени

Для запуска просмотра экрана контролируемого компьютера Online, нажмите кнопку «Просмотр Online» в панели инструментов. Тогда откроется окно превью. Выберите в списке компьютеры, экраны которых надо отобразить.

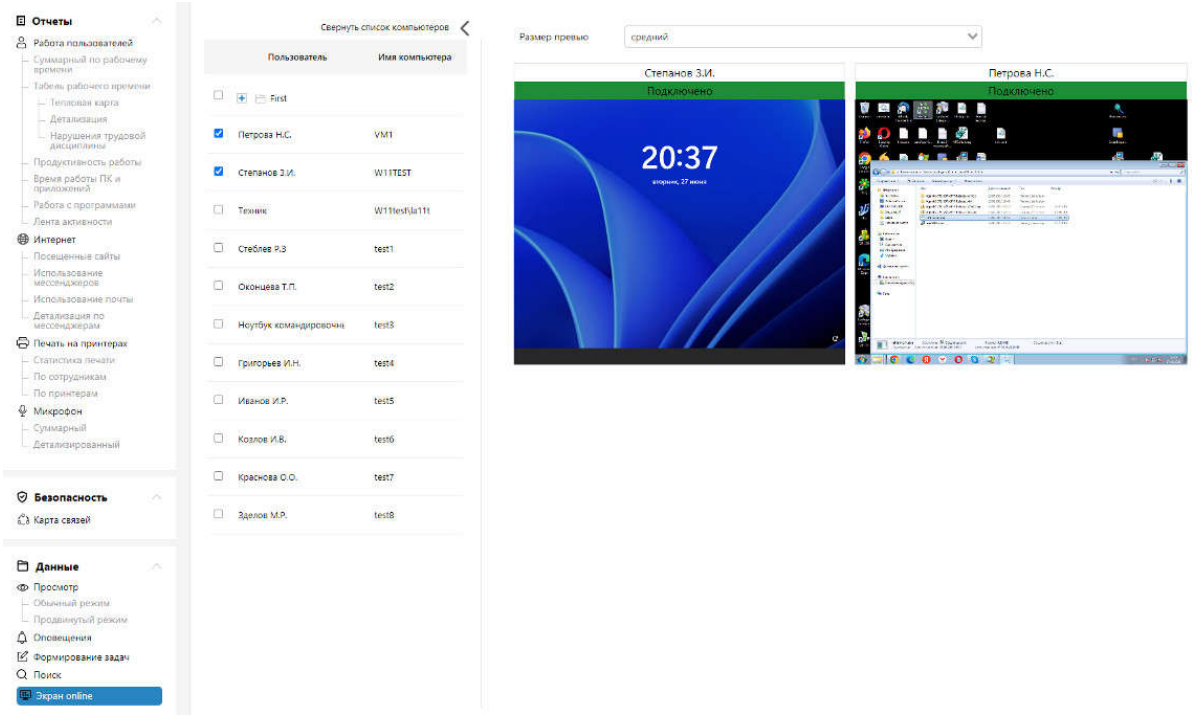


Есть возможность изменить размер отображаемых экранов. Для этого установите в левой нижней части окна галочку «Ручной размер превью» и выберите нужный размер.

Щелкнув дважды на интересующем экране превью, его можно открыть в отдельном окне в большем масштабе. Там же есть возможность и взять управление контролируемым компьютером.

Чтобы сразу из окна LanAgent Viewer открыть на просмотр экран нужного компьютера, щелкните на интересующем компьютере правой клавишей мыши и выберите в выпадающем меню для него пункт «Просмотреть экран монитора Online…».

При работе в веб интерфейсе (через браузер), выберите пункт Экран online в боковом меню.



В остальном, управление аналогично тому, как сделано в приложении Viewer.

7 Работа с LanAgent Sheduler (планировщиком отчетов)

Интерфейс программы LanAgent Sheduler имеет следующий вид:

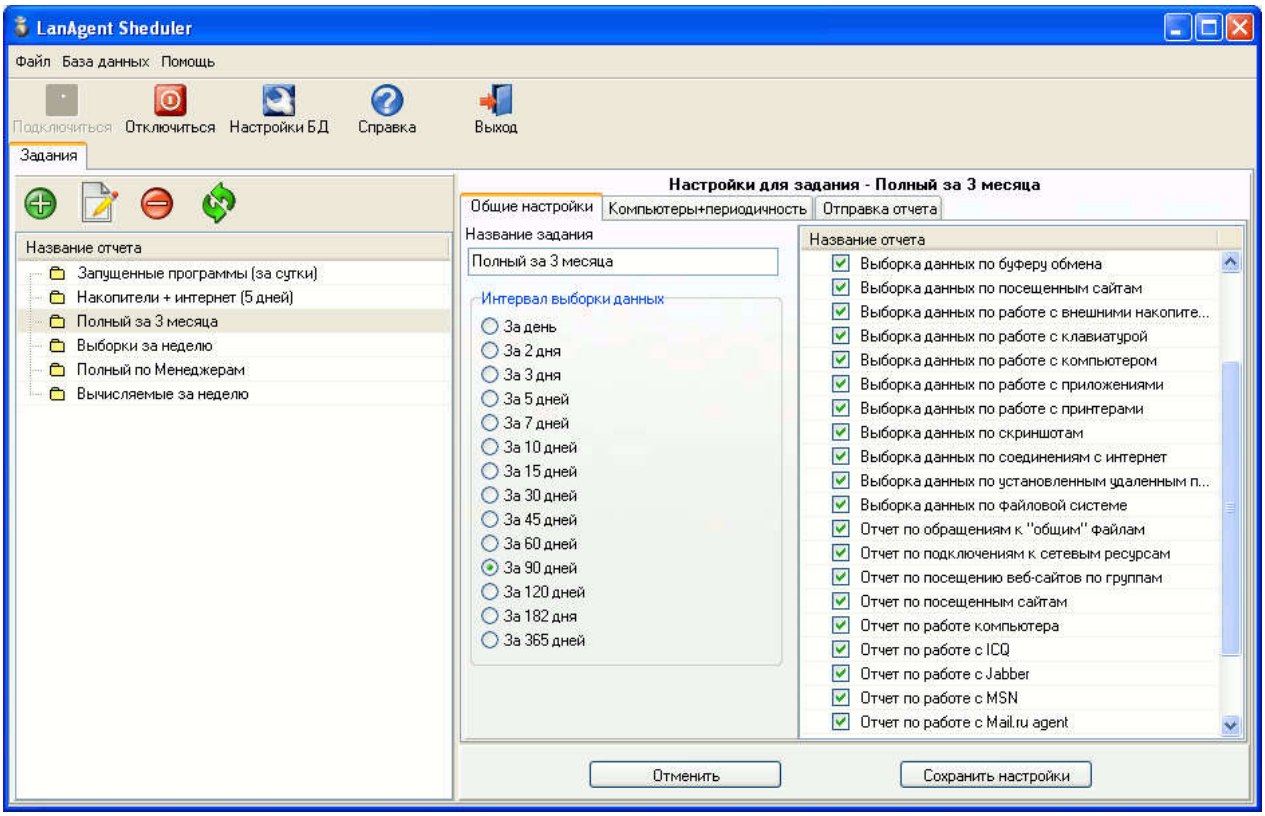
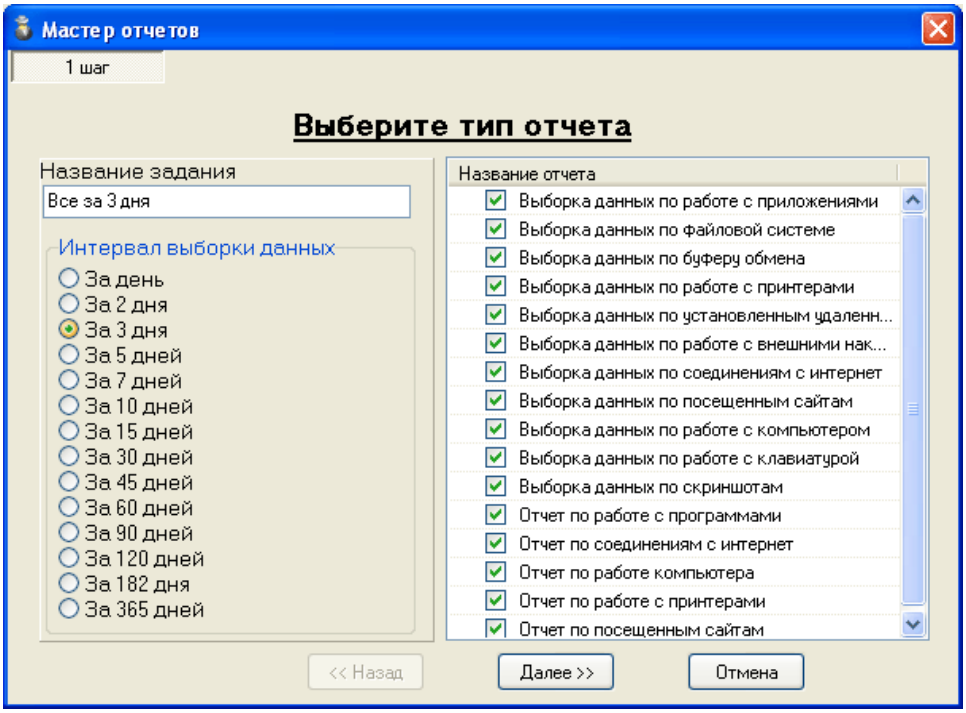


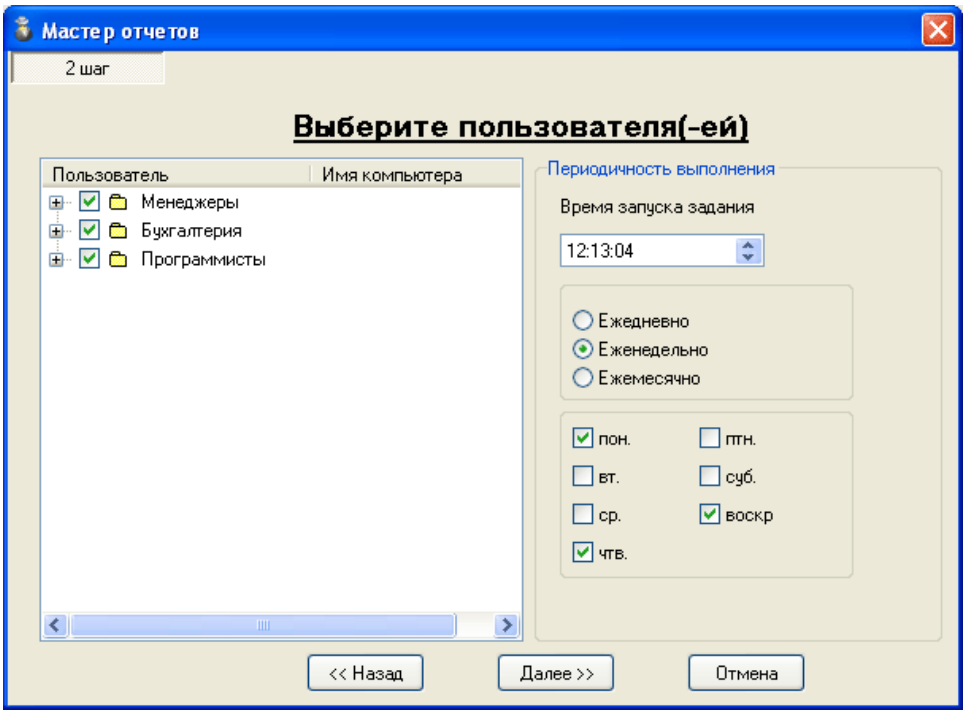
Рис. 7.1 – Главное окно программы

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

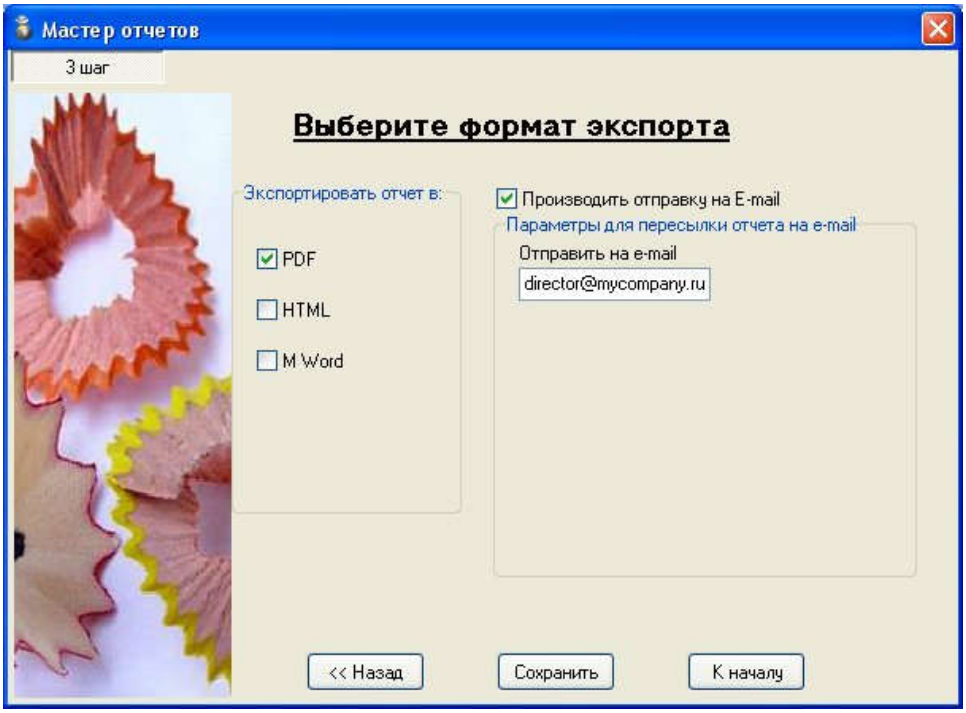
Для создания нового – воспользуйтесь кнопкой  панели инструментов. При этом откроется следующий диалог добавления:



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



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



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

8 Удаление программы

Если возникла необходимость произвести удаление программы, например при переходе на следующую версию программы, то это производится отдельно для серверной части, программ Admin, Viewer, Sheduler. Удаление агентов с контролируемых компьютеров можно произвести как вручную (при помощи файла инсталляции), так через встроенные средства LanAgent Admin.

8.1 Удаление Серверной части, Admin, View, Sheduler

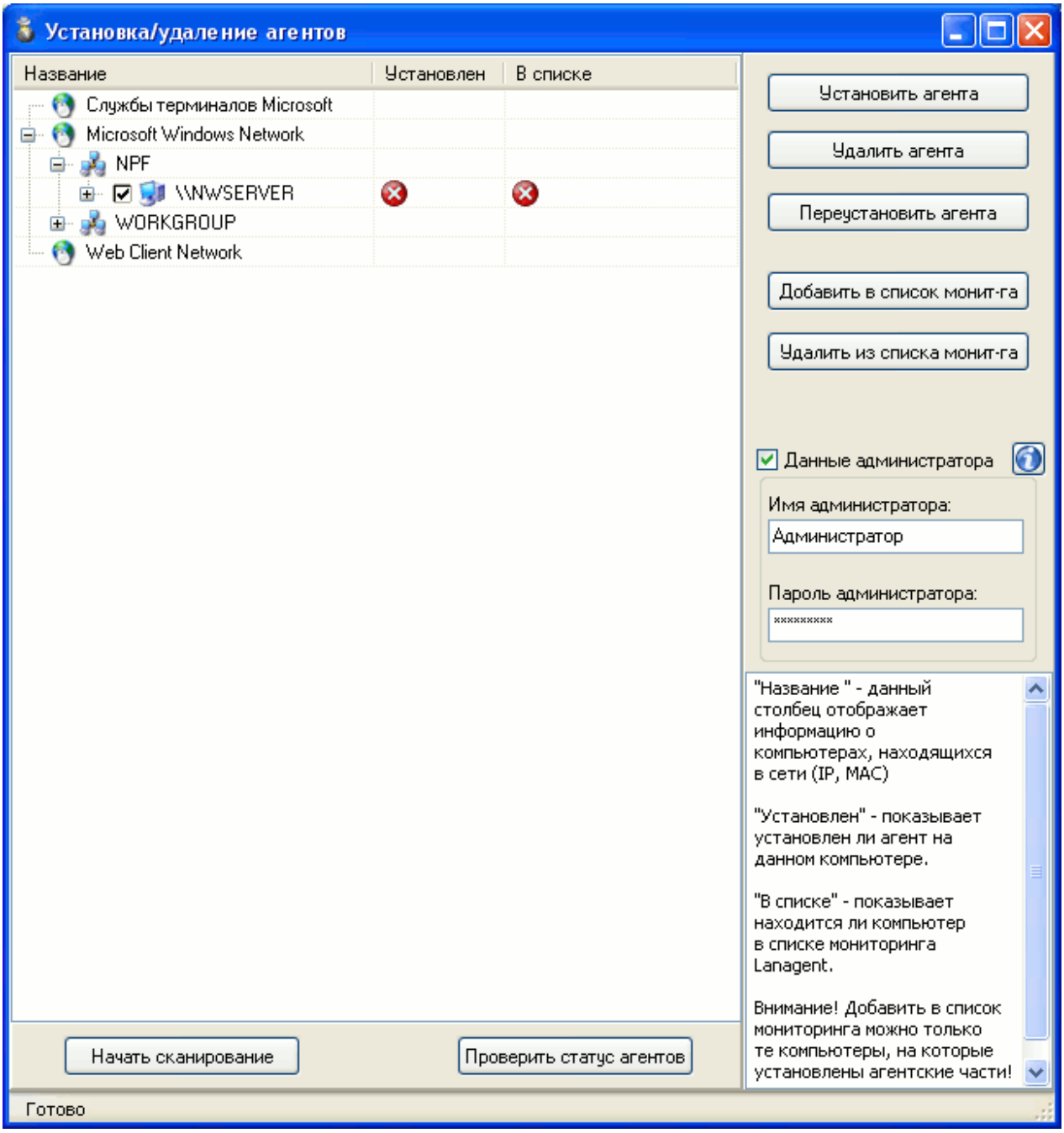
Для удаления любой из перечисленных в заголовке программ, можно использовать стандартные средства Windows, также как и для любого другого приложения. Для этого в "Панели управления" ("Control Panel") выбрать пункт "Установка и удаление программ" ("Add and remove programs"), выберите в списке соответствующую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

8.2 Удаление агентов

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

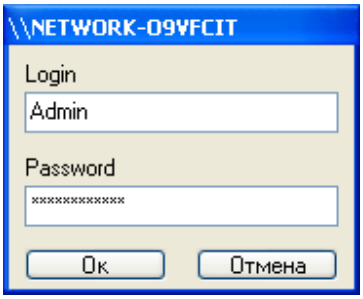
Удаленное удаление агентов

Для этого воспользуйтесь диалогом установки/удаления агентов, который вызывается в **LanAgent Admin** 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**". 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 3.3.3.

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**.

9 Техническая поддержка

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

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

9.1 Типичные действия

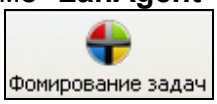
1 Добавление компьютера в список мониторинга

Данная возможность реализуется в программе **LanAgent Admin**. 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

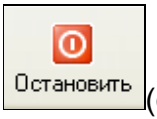
Данная возможность реализуется в программе **LanAgent Admin**. Для удаления определенного компьютера из списка мониторинга, необходимо встать на строку, соответствующую данному компьютеру в списке и нажать кнопку "Удалить"  панели инструментов LanAgent Admin или выбрать соответствующий пункт "Удалить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

3. Запуск или остановка мониторинга на нужном компьютере

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

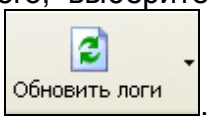
панели инструментов. В открывшемся окне выберите требуемые компьютеры и щелкните на кнопке "Запустить" 

(если хотите

запустить мониторинг) или "Остановить" 

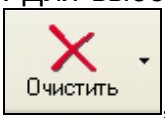
(если хотите его остановить). Процесс отработки задания будет отображаться в правой части окна.

4. Обновление логов

Данное действие, также как и запуск/останов мониторинга осуществляются через диалог формирования задач программы LanAgent View. Запустите его, выберите требуемые компьютеры, а затем нажмите кнопку "Обновить логи" 

. Процесс отработки задания будет отображаться в правой части окна.

5. Очистка логов

В программе LanAgent имеется возможность очистки выбранной категории логов (например "Программы") для выбранного пользователя; очистки всех логов для выбранного пользователя; очистка всех логов для всех пользователей. Для выбора любого из этих вариантов можно воспользоваться кнопкой "Очистить" 

, а можно выбрать соответствующий пункт в меню "Управление". **Внимание!** Производить очистку логов могут только пользователи, имеющие соответствующие права.

6. Сбросить статус опасности компьютера до "зеленого"

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

9.2 Часто задаваемые вопросы

1. Как просмотреть снимки экранов мониторов (скриншоты)?

Выберите 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 и Linux.

Для Windows поддерживаются следующие версии:

- Windows XP (ограниченный функционал)
- Windows Server 2003/2008/2012/2016/2019
- Windows Vista (ограниченный функционал)
- Windows 7/8/8.1/10/11

3. Каковы системные требования программы LanAgent?

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

Серверная часть.

Минимальные требования:

- Операционная система: Windows 2008/20122016/2019, 7/8/8.1/10/11.
- Процессор с частотой не менее 1,4 Ггц.
- 512 МБ оперативной памяти.
- 300 МБ свободного места на диске.
- Открытые порты 47658, 7657, 3050 и 6587 TCP/IP на компьютере с сервером LanAgent (если используется фаервол, то надо в нем их открыть).

Рекомендуемые требования:

- Операционная система: Windows 2008/20122016/2019, 7/8/8.1/10/11.
- Процессор с 2-4 ядрами с частотой ядра 3 Ггц и выше.
- От 4 ГБ оперативной памяти.
- 15 ГБ свободного места на диске (зависит от количества компьютеров и настроек программы).
- Открытые порты 47658, 7657, 3050 и 6587 TCP/IP на компьютере с сервером LanAgent (если используется фаервол, то надо в нем их открыть).

Пользовательская часть (агент).

Минимальные требования:

- Операционная система: Windows XP/2003/2008/2012/Vista/7/8/8.1/10/11.
- Процессор с частотой от 1,4 Ггц и выше.
- 512 МБ оперативной памяти.
- 300 МБ свободного места на диске.
- Открытые порты 47658 и 7657 TCP/IP на компьютере с агентом (если используется фаервол, то надо в нем их открыть).

Рекомендуемые требования:

- Операционная система: Windows 7/8/8.1/10/11.
- Процессор с частотой 2 Ггц и выше.
- 1 ГБ оперативной памяти.
- 300 МБ свободного места на диске.
- Открытые порты 47658 и 7657 TCP/IP на компьютере с агентом (если используется фаервол, то надо в нем их открыть).

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

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 серверной 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 серверной 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.

Также убедитесь, что в используемом фаерволе и брандмауере Windows открыт для обмена порт 47658 tcp/ip. Также можно полностью внести в исключение входящего сетевого трафика процесс агента syswow64\lasys\svchost.exe (это для 64 битной ОС, для 32 битной – system32\lasys\svchost.exe). Он отвечает за сетевой обмен между следящим модулем LanAgent и сервером LanAgent.

7. Как установить срок хранения логов в базе?

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