КОМПЛЕКС ПРОГРАММНЫЙ КАНОЭ

Руководство администратора

Версия 1.0.8

Листов 142

2019

АННОТАЦИЯ

Настоящий документ содержит руководство администратора программного комплекса КАНОЭ BY.ИАДВ.10030, который осуществляет защиту информации, обрабатываемой на ПЭВМ, от утечек, вызванных сканированием, воздействием вредоносного ПО, несанкционированным использованием внешних устройств и программ пользователем.

СОДЕРЖАНИЕ

1. СОСТАВ И НАЗНАЧЕНИЕ ПРОГРАММЫ

Программный комплекс КАНОЭ (далее – комплекс КАНОЭ) осуществляет защиту информации, обрабатываемой на ПЭВМ, от утечек, вызванных сканированием, воздействием вредоносного ПО, несанкционированным использованием пользователем внешних устройств и программ. Комплекс КАНОЭ поддерживает как локальное, так и сетевое исполнение.

В состав локального исполнения комплекса КАНОЭ входят следующие модули:

1) модуль управления доступом – предназначен для ограничения и контроля доступа пользователей к внешним устройствам;
2) модуль контроля данных – предназначен для проверки данных (в том числе поступающих и отправляемых с ПЭВМ) на наличие вредоносных программ;
3) модуль межсетевого экранирования – предназначен для контроля и фильтрации сетевых пакетов по принципу «то, что не разрешено – запрещено»;
4) модуль удаления – предназначен для удаления временных файлов;
5) модуль контроля целостности – предназначен для контроля целостности конфигурации СВТ и контроля целостности программного обеспечения;
6) модуль графического интерфейса – предназначен для отображения работы комплекса в графическом виде на экране пользователя и организации взаимодействия с ним в локальном варианте исполнения;
7) модуль «Агент» – предназначен для обеспечения взаимодействия модуля «Центр управления» с программными модулями;
8) модуль взаимодействия – предназначен для управления модулями и организации их взаимодействия между собой, контроля целостности комплекса.

Сетевой вариант исполнения комплекса КАНОЭ разработан на базе клиент-серверной архитектуры. Структура клиентской части сетевого варианта исполнения соответствует структуре локального варианта исполнения комплекса КАНОЭ. На серверной части, помимо модулей входящих в клиентскую часть устанавливается модуль «Центр Управления». Модуль «Центр Управления» – предназначен для обеспечения централизованного управления по сети программными модулями и детализированного отображения информации о событиях их работы.

Комплекс КАНОЭ обеспечивает:

1) централизованное управление всеми его программными модулями по сети;
2) контроль действий пользователя при работе с информацией на ПЭВМ;
3) защиту ПЭВМ от вредоносного ПО;

4) защиту от несанкционированного доступа к информации;
5) межсетевое экранирование (реализующее политику «то, что не разрешено - запрещено»);
6) удаление информации, не требующейся для дальнейшего использования, а также следов ее обработки – в ручном и автоматическом режимах;
7) контроль и ограничение доступа пользователей к внешним устройствам;
8) ведение аудита действий пользователя при работе с информацией и функционирования прикладного и системного ПО с возможностью просмотра и редактирования списка объектов и устройств в электронных журналах только администратором безопасности;
9) проверку данных (в т.ч. поступающих или отправляемых с ПЭВМ) на наличие вредоносных программ (в реальном масштабе времени и по запросу пользователя/администратора);
10) контроль целостности конфигурации средства вычислительной техники (СВТ) и установленного на нем программного обеспечения;
11) ведение журналов аудита доступа пользователей к информации, функционирования прикладного и системного ПО;
12) контроль целостности файлов комплекса с реализацией функции восстановления с единого центра управления в случае выявленного нарушения;
13) контроль настроек, запуска, обновления всех компонент комплекса, исключая необходимость каких-либо действий на ПЭВМ пользователей по инсталляции и настройке, кроме разрешения нештатных ситуаций;
14) контроль и управление перечнем программных процессов, функционирующих на ПЭВМ для каждого пользователя;
15) ограничение доступа пользователей к настройкам комплекса;
16) анализ обрабатываемой информации на наличие вредоносных программ в соответствии с заданными администратором условиями (либо постоянный автоматический, либо по запросу);
17) непрерывный контроль за действиями пользователя при работе с информацией (доступ, запись, чтение, копирование информации, вывод на печать), состоянием защиты системы для своевременного обнаружения нарушений политики безопасности системы и действий вредоносных программ с возможностью уведомления администратора при возникновении критических ситуаций;
18) контроль и фильтрацию проходящих через изделие сетевых пакетов (IP v.4/IP v.6) в соответствии с заданными правилами (сетевые адреса получателя и отправителя, используемый протокол передачи данных, порт)

и принятие на основе интерпретируемых правил следующих решений: не пропустить данные, пропустить данные, занести информацию в журнал аудита, уведомить пользователя/администратора;

19) регистрацию запуска клиентской части и управление работой комплекса КАНОЭ;
20) выставление приоритета на потребление ресурсов операционной системой при выполнении фоновых заданий комплекса КАНОЭ, объединение защищаемых объектов (ПЭВМ) в группы и подгруппы для применения к ним отдельных политик и заданий, контроль работы комплекса, состояния защищаемых объектов и отображение их состояния, осуществление централизованного автоматического/принудительного обновления компонент;
21) уведомление администратора о критических событиях, возникающих при работе комплекса (с возможностью выбора уровня подробности протоколирования), о регистрации события, ведении, хранении и статистической обработке отчетов о результатах работы комплекса (указанные функции должны выполняться как с отдельными защищаемыми объектами, так и с группой таких объектов одновременно);
22) просмотр и редактирование списка защищаемых объектов и устройств только администратором;
23) назначение заданий защищаемым объектам по управлению клиентской частью ПО (задания могут быть как периодические, так и разовые);
24) хранение в центральном журнале аудита событий безопасности и результатов заданий администратора;
25) контроль и ограничение доступа (доступ, запись, чтение) к следующим видам устройств:
    а) USB-устройства (flash-накопители, внешние жесткие диски, цифровые камеры и аудиоплееры, карманные компьютеры; локальные и сетевые принтеры);
    б) контроллеры беспроводных сетей (Wi-Fi, Bluetooth, IrDA);
    в) сетевые карты и модемы, дисководы, CD и DVD-приводы, накопители на жестких магнитных дисках;
    г) внешние порты LPT, COM и IEEE 1394 и другие устройства, имеющие в ОС символическое имя.

При инсталляции или обновлении комплекса автоматически определяется тип операционной системы, после чего проводится установка соответствующих компонентов комплекса.

Область применения комплекса КАНОЭ: информационные системы государственных организаций Республики Беларусь, в том числе банковской сферы.

2. УСЛОВИЯ ВЫПОЛНЕНИЯ ПРОГРАММЫ

Комплекс КАНОЭ устанавливается на ПЭВМ на базе архитектуры Intel x86 и требует наличия:

1) 32-разрядного (x86) или 64-разрядного (x64) процессора с тактовой частотой не ниже 2 ГГц;
2) не менее 2 ГБ оперативной памяти;
3) не менее 800 Мб свободного пространства на логическом диске ПЭВМ (локальный вариант исполнения, клиентская часть сетевого варианта исполнения);
4) не менее 3 Гб свободного пространства на логическом диске ПЭВМ (серверная часть сетевого варианта исполнения);
5) сетевая карта не менее 100 Мбит (сетевой вариант исполнения).

Централизованное управление комплексом КАНОЭ осуществляется посредством ЛВС.

Локальный вариант исполнения, клиентская часть сетевого варианта исполнения комплекса КАНОЭ устанавливаются и корректно функционируют на базе следующих лицензионных операционных системах семейства Windows:

1) Windows XP (32 битная версия);
2) Windows Server 2003 (64 битная версия);
3) Windows 7 (32/64 битная версия);
4) Windows 8 (32/64 битная версия);
5) Windows 8.1 (32/64 битная версия);
6) Windows 10 (32/64 битная версия);
7) Windows Server 2008R2 (64 битная версия);
8) Windows Server 2012 (64 битная версия);
9) Windows Server 2012R2 (64 битная версия).

Серверная часть сетевого варианта исполнения комплекса КАНОЭ устанавливается и корректно функционирует на базе следующих лицензионных операционных системах семейства Windows:

1) Windows Server 2008R2 (64 битная версия);
2) Windows Server 2012 (64 битная версия);
3) Windows Server 2012R2 (64 битная версия).

На операционные системы должны быть установлены все обновления, предоставляемые их разработчиком.

Установленные на ПЭВМ средства защиты информации должны быть подвергнуты процедурам подтверждения соответствия требованиям информационной безопасности, установленным в техническом регламенте

Республики Беларусь «Информационные технологии. Средства защиты информации. Информационная безопасность» (ТР 2013.027.BY), в форме сертификации или декларирования соответствия.

Кроме выше изложенного для корректной работы серверной части сетевого варианта исполнения комплекса КАНОЭ необходимо наличие и настройка следующего программного обеспечения:

1) система управления базами данных (далее - СУБД) Microsoft SQL Server 2005 Express SP4 или выше. СУБД Microsoft SQL Server 2005 Express SP4 входит в состав сетевого варианта исполнения комплекса КАНОЭ;
2) веб-сервер Internet Information Services IIS 7.5, IIS 8, IIS 8.5 (входит в состав соответствующих ОС);
3) Microsoft .NET Framework 2.0 SP2 или выше (Microsoft .NET Framework 2.0 SP2 входит в состав сетевого варианта исполнения комплекса КАНОЭ).

3. УСТАНОВКА КОМПЛЕКСА КАНОЭ

Программа установки комплекса КАНОЭ выполнена в виде стандартного мастера Windows и имеет интуитивно понятный интерфейс. Для корректной установки программного комплекса КАНОЭ рекомендуется закрыть все приложения. Антивирусные программы должны быть удалены.

Перед установкой комплекса КАНОЭ следует убедится что активированы следующие компоненты IIS и их зависимости: .Net Framework, HTTP Activation, Application Development ASP, обработка статического содержимого (Static Content).

Комплекс КАНОЭ устанавливается как в локальном, так и сетевом варианте исполнения.

Локальный и сетевой вариант исполнения комплекса КАНОЭ представлен в файле KANOE.exe.

Для корректной работы комплекса КАНОЭ требуется наличие регистрационного файла vba32.key.

3.1. Установка сетевого варианта исполнения

Для установки программы на ПЭВМ необходимо запустить на выполнение исполняемый файл KANOE.exe. Для данной установки необходимы права администратора системы.

После запуска исполняемого файла KANOE.exe выбрать тип установки (рис. 1) **Сетевая** нажать кнопку **Продолжить**, начнется установка сетевого варианта исполнения комплекса КАНОЭ (п. 3.1.1 – 3.1.11).

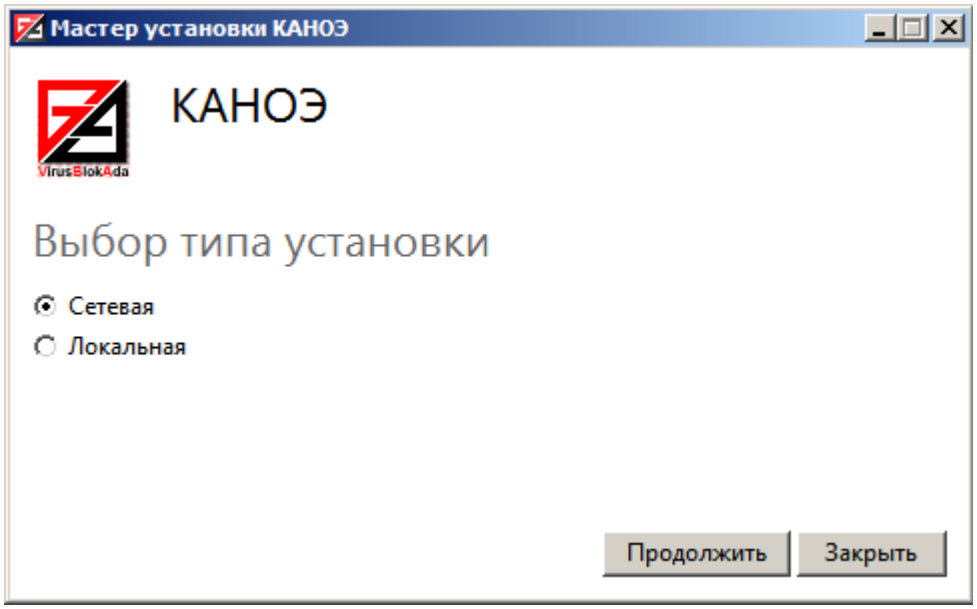

Рис. 1

3.1.1. Установка вспомогательного программного обеспечения

Окно приветствия (рис. 2) содержит рекомендации по подготовке к установке модуля «Центр Управления» (устанавливается/настраивается SQL Server, .NET Framework).

Примечания:

1. .NET Framework устанавливается в фоновом режиме, если не было обнаружено подходящей версии на ПЭВМ.

2. Microsoft SQL Server редакции Express, входящая в инсталляционный пакет комплекса КАНОЭ, имеет ограничения размера базы данных 4 ГБ.

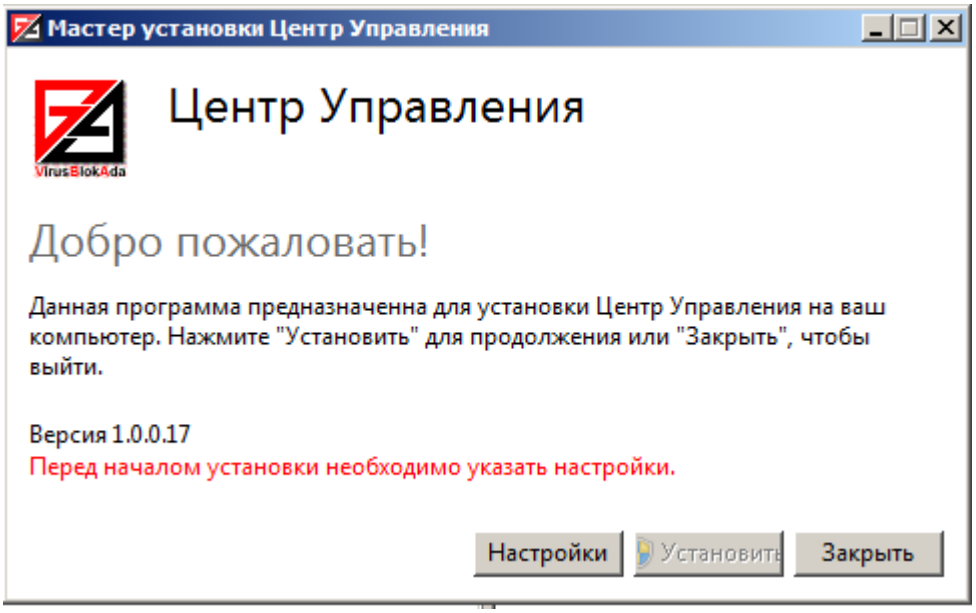

Рис. 2

Для начала установки необходимо задать настройки для Microsoft SQL Server: имя экземпляра и пароль (рис. 3).

Примечание. Пароль должен соответствовать установленной политике паролей Windows.

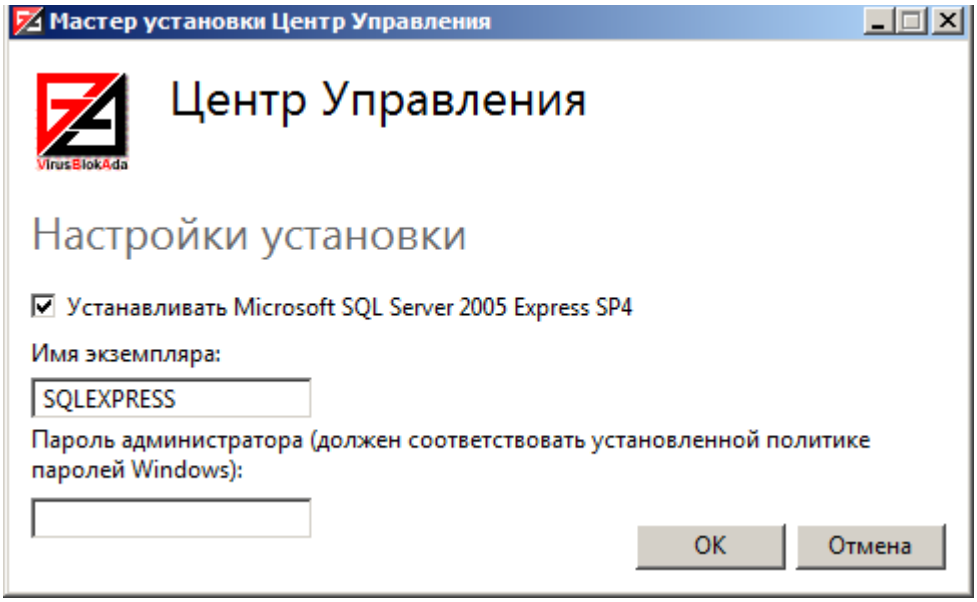

Рис. 3

После задания настроек необходимо нажать **OK**.

При заданных настройках становится доступной кнопка **Установить** (рис. 4).

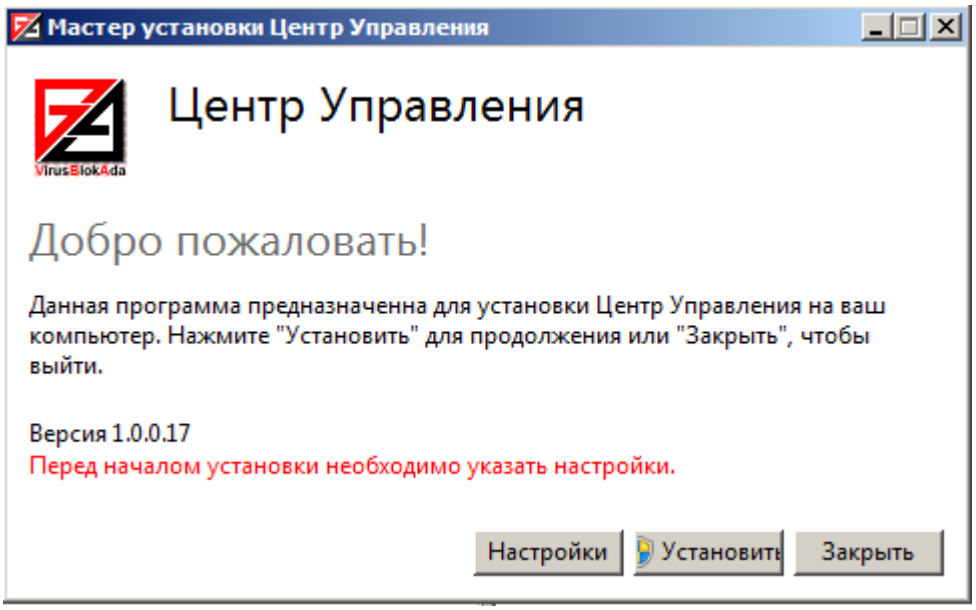

Рис. 4

Далее показан процесс установки вспомогательного программного обеспечения (рис. 5), (рис. 6).

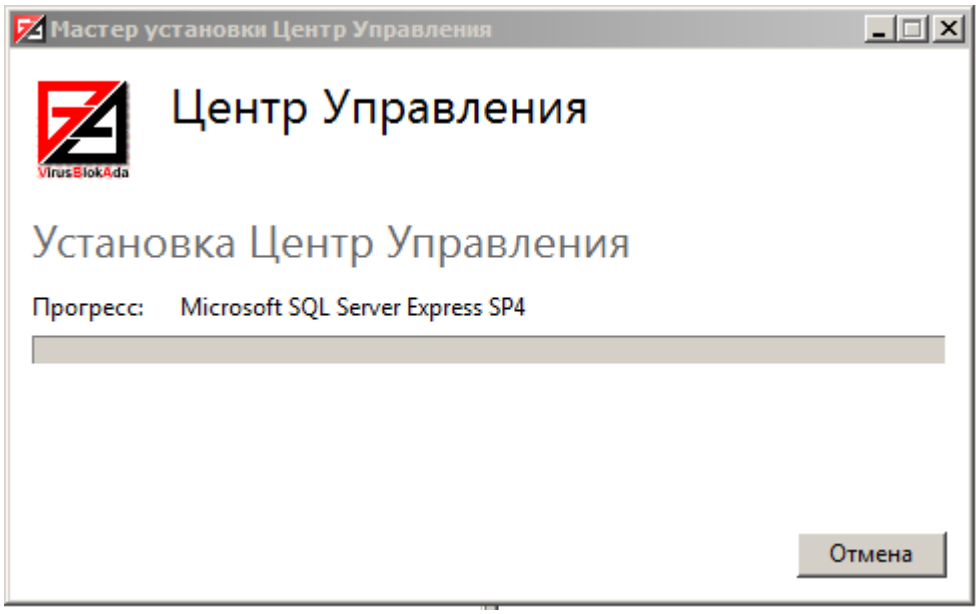

Рис. 5

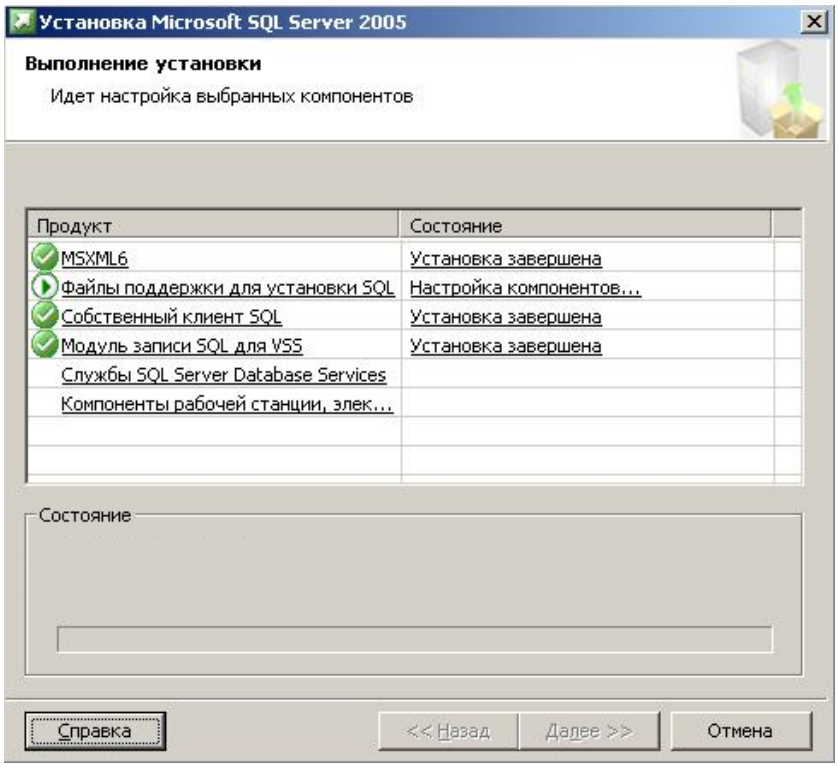

Рис. 6

3.1.2. Установка модуля «Центр Управления»

Окно приветствия программы установки модуля «Центр Управления», приведенное на рис. 7, содержит рекомендации по установке модуля «Центр Управления».

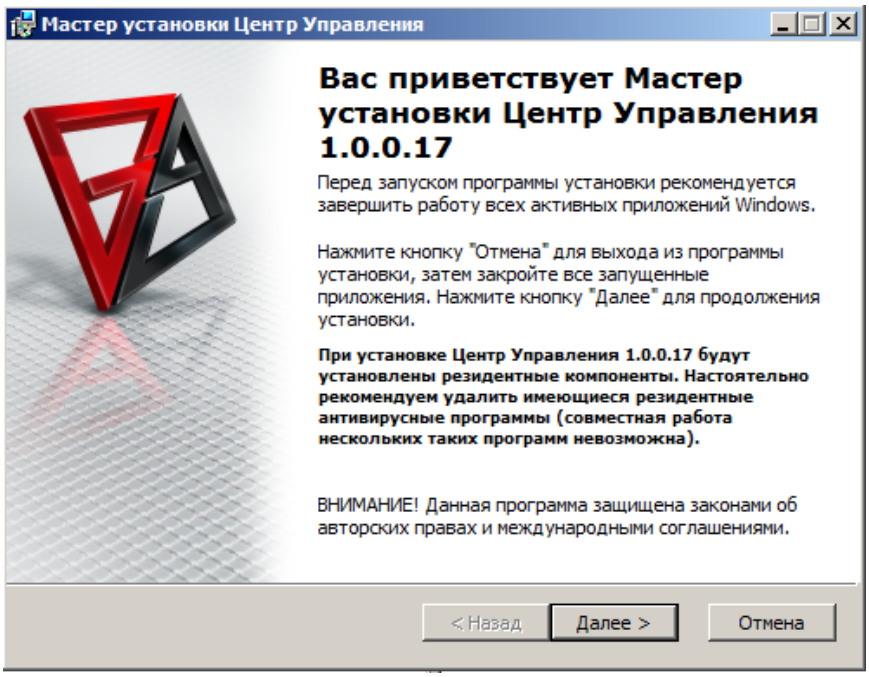

Рис. 7

Для установки модуля «Центр Управления» нажмите кнопку **Далее**.

3.1.3. Выбор регистрационного ключа

Данный шаг работы **Мастера установки** предназначен для установки регистрационного ключа, подтверждающего легальность пользования продуктом. Ключ представляет собой файл следующего вида – vba32.key.

Необходимо указать путь к регистрационному ключу. Нажмите кнопку **Обзор** (рис. 8) и в появившемся диалоге укажите путь к файлу vba32.key.

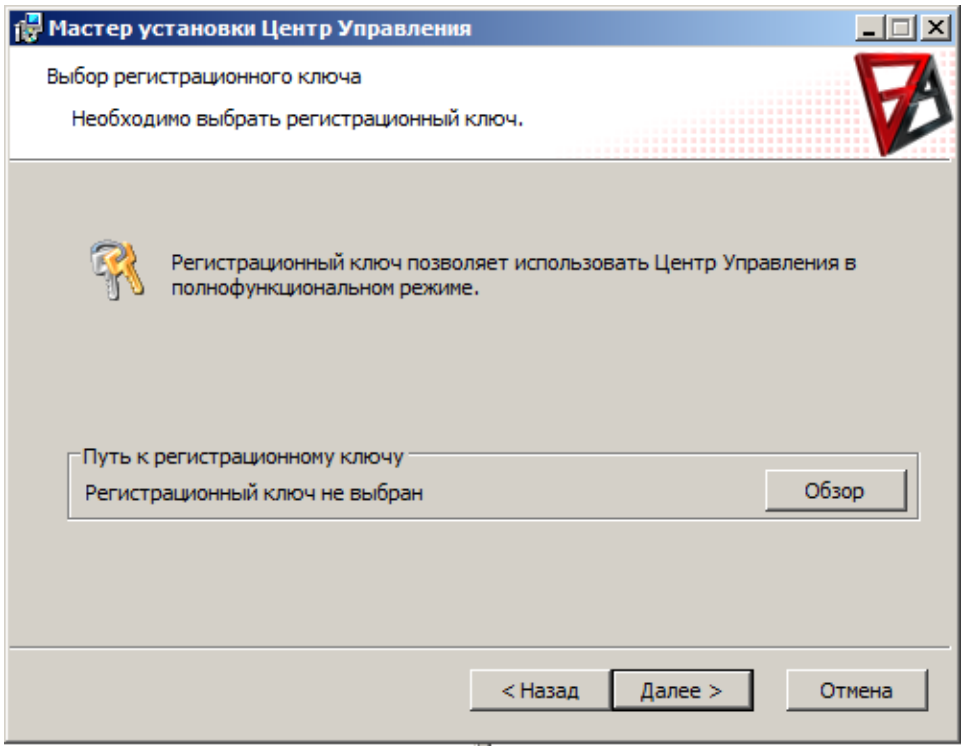

Рис. 8

Примечание. Без регистрационного ключа дальнейшая установка комплекса КАНОЭ невозможна. Необходимо обязательно указать действительный ключ комплекса КАНОЭ.

Нажмите кнопку **Далее** для продолжения установки.

3.1.4. Настройка баз данных

Модуль «Центр Управления» использует базу данных для хранения сведений об управляемых компьютерах, пришедших с них сообщений о событиях, а также пользователях web-интерфейса и их настроек.

Следующий шаг позволяет настроить базу данных пользователей. Есть возможность выбрать сервер баз данных, ввести реквизиты учетной записи для доступа к СУБД. Если в предыдущем шаге устанавливали СУБД, все настройки выставятся автоматически.

В поле **Имя сервера SQL** (рис. 9) необходимо ввести имя компьютера с установленной СУБД, которая будет в дальнейшем использоваться модулем «Центр Управления» для хранения данных о пользователях. Для получения списка всех доступных Microsoft SQL Server в сети необходимо воспользоваться кнопкой **Обновить**, затем выбрать нужный в появившемся выпадающем списке.

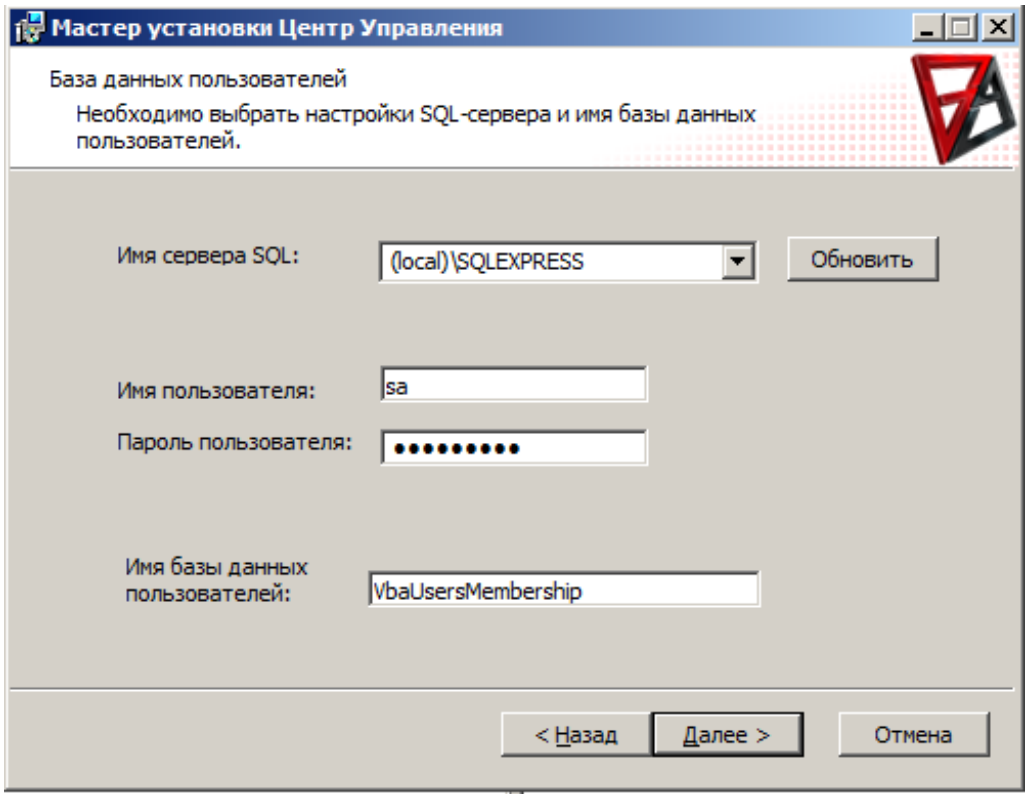

Рис. 9

В поле **Имя базы данных пользователей** необходимо указать имя базы данных, которая будет использоваться для хранения информации о пользователях web-интерфейса модуля «Центр Управления». По умолчанию указано значение VbaUsersMembership.

В случае использования уже установленной СУБД MS SQL Server, необходимо задать **имя** и **пароль пользователя** для администратора СУБД (при установке СУБД с установочного комплекта программного комплекса КАНОЭ имя пользователя и пароль автоматически заполняются данными), указанными на рис. 9.

Нажмите кнопку **Далее**, чтобы перейти к установке и настройке основной БД VbaControlCenterDB для модуля «Центр Управления».

Примечание. Размер файлов базы данных модуля «Центр Управления» может достигать гигабайта и более. Убедитесь в наличии достаточного свободного места на логическом диске, куда устанавливается база данных. При необходимости укажите пути, отличные от заданных по умолчанию.

Настройка БД VbaControlCenterDB происходит аналогично настройке БД VbaUsersMembership, которая описана выше.

Нажмите кнопку **Далее** для продолжения установки (рис. 10).

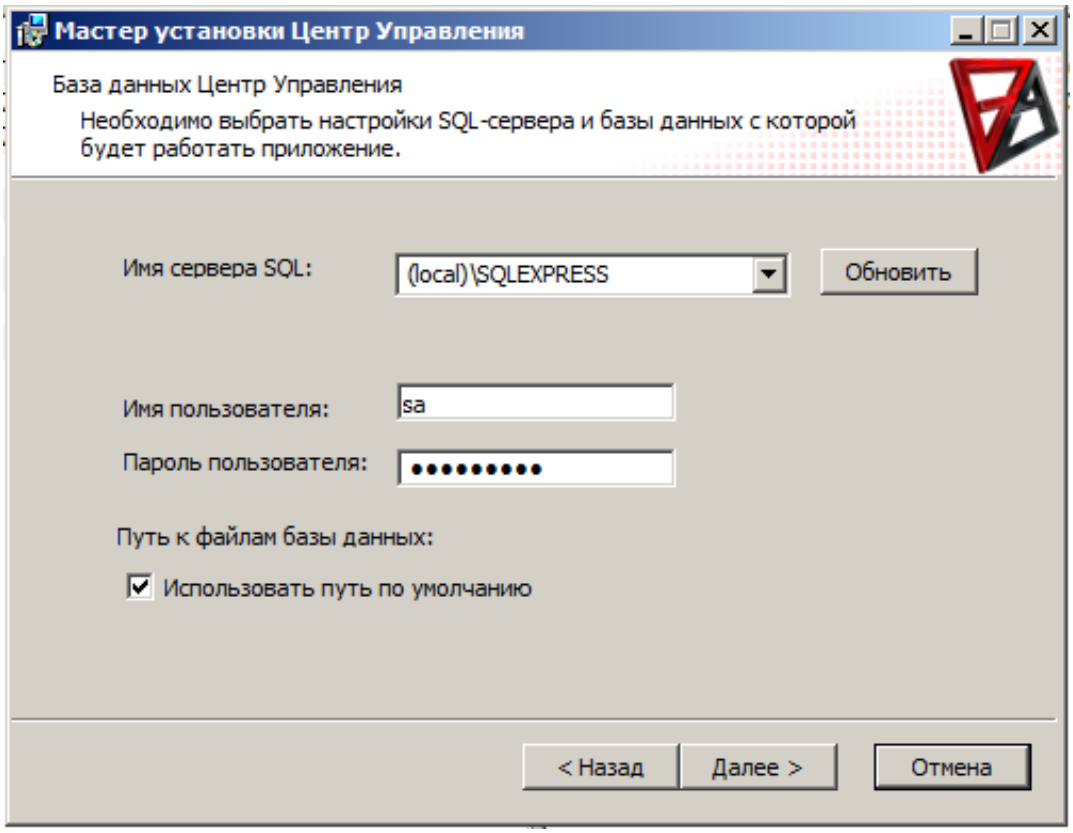

Рис. 10

3.1.5. Конфигурация адаптера

Существует 3 режима при конфигурации адаптера (рис. 11):

1) **Использовать старые настройки адаптера** – применяется в случае переустановки модуля «Центр Управления» (в данном случае, модуль «Агент» (см. п. 3.1.8) продолжит работать без перенастройки на новый модуль «Центр Управления»);
2) **Определить новые настройки** – режим по умолчанию, в котором выбирается адаптер из списка доступных адаптеров;
3) **Пропустить** - данный режим применять не рекомендуется, т.к. впоследствии нужно будет настраивать адаптер в ручном режиме.

Нажать кнопку **Далее**.

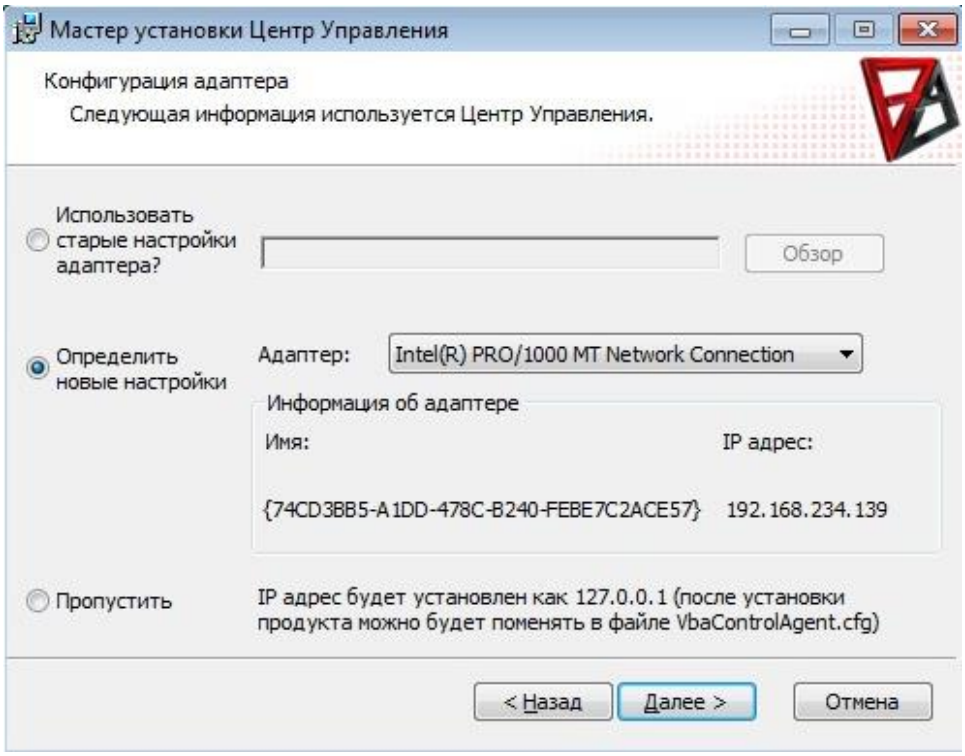

Рис. 11

3.1.6. Завершение установки модуля «Центр Управления»

Нажмите кнопку **Установить** (рис. 12) для начала установки файлов. Нажмите кнопку **Назад**, если необходимо повторно ввести данные для установки или нажмите кнопку **Отмена** для выхода из программы установки.

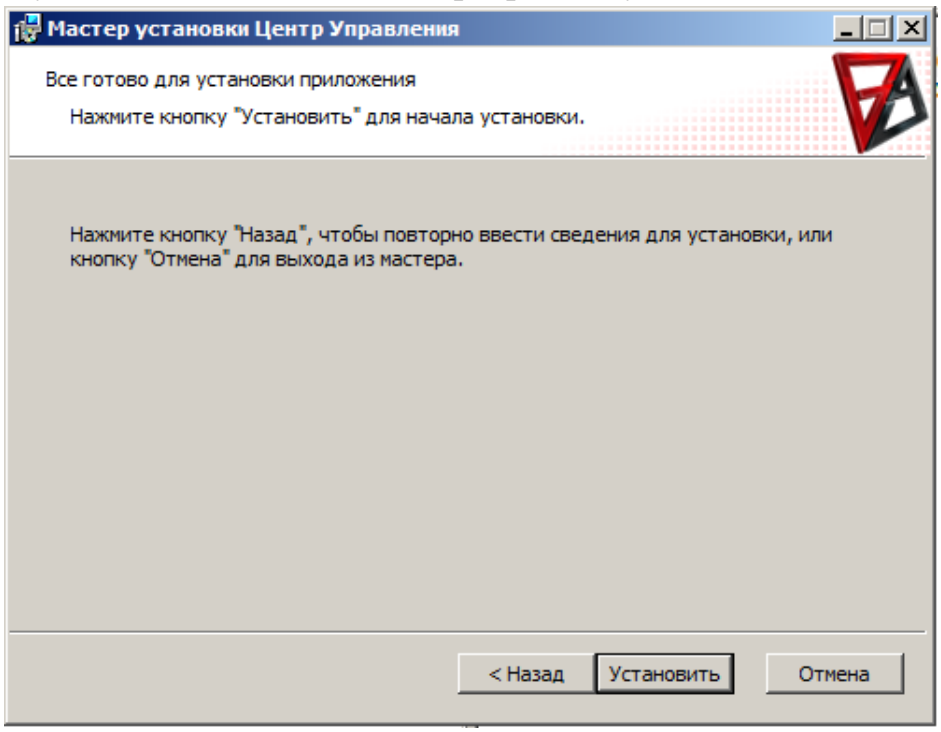

Рис. 12

Окно процесса установки (рис. 13).

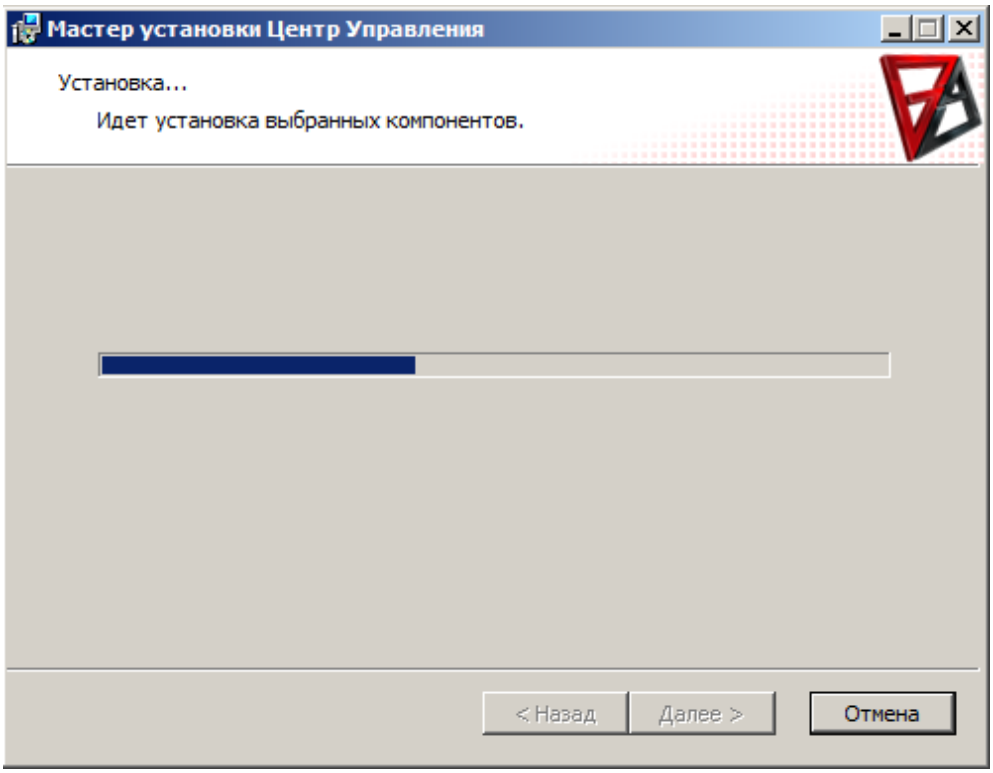

Рис. 13

3.1.7. Установка успешно завершена

При завершении установки модуля «Центр Управления» на компьютер нажмите кнопку **Готово** (рис. 14).

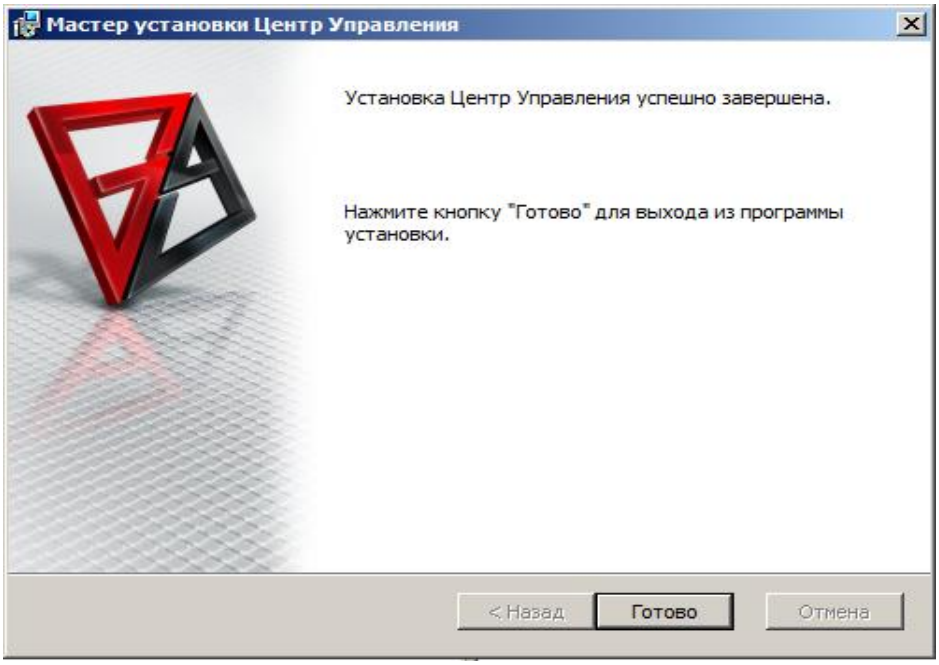

Рис. 14

Модуль «Центр Управления» успешно установлен на компьютер, для выхода из программы установки нажмите кнопку **Закрыть (**рис. 15).

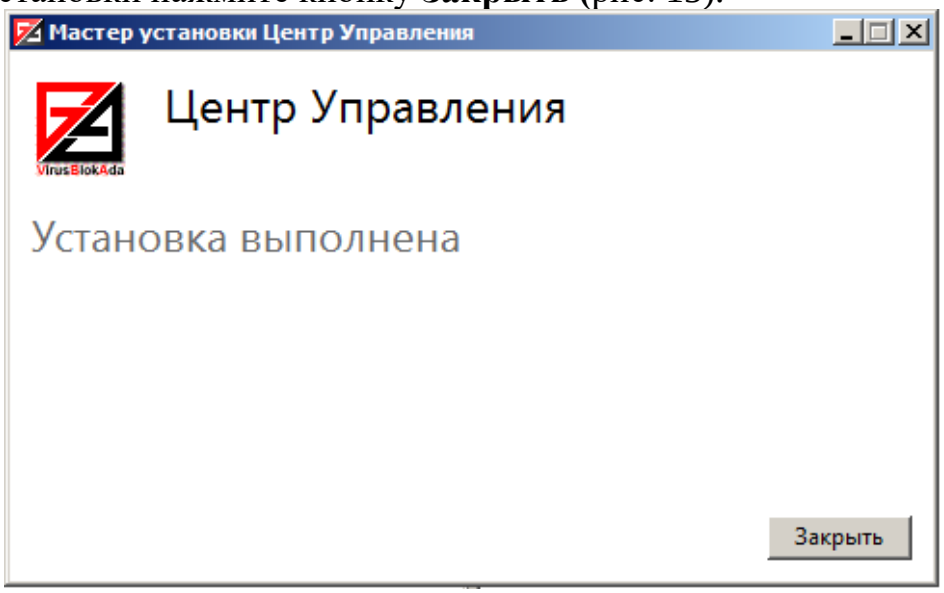

Рис. 15

Примечание. Для установки безопасного канала связи при работе с модулем «Центр Управления» настройте службу HTTPS в IIS. Настройка службы HTTPS осуществляется в соответствии с эксплуатационной документацией на IIS.

Сервисы, необходимые для работы модуля «Центр Управления», запускаются автоматически по окончанию инсталляции, если был установлен соответствующий флажок. В противном случае рекомендуется перезагрузить компьютер.

Работа компонентов продукта осуществляется в полностью автоматическом режиме. Контроль над работой необходимо осуществлять по системному журналу Windows, а также файлам отчета. Файлы отчета модуля «Центр Управления» имеют имена **Vba32CC.log, Vba32NS.exe.log, Vba32PMS.exe.log, Vba32SS.exe.log, packet_parser.log** и расположены в том каталоге, куда установлен модуль «Центр Управления».

Данные о сервере модуля «Центр Управления», а также о ключе ЭЦП, используемом для подписи пакетов, хранятся в файле **VbaControlAgent.cfg**, генерируемом в процессе инсталляции. Этот файл расположен в том каталоге, куда установили модуль «Центр Управления».

3.1.8. Установка модуля «Агент»

«КАНОЭ-клиент» взаимодействует с модулем «Центр Управления» посредством модуля «Агент». Для того чтобы получать с рабочих станций в сети информацию о работе программного комплекса «КАНОЭ», а также иметь возможность управления, необходимо подключить эти рабочие станции к модулю «Центр Управления».

«КАНОЭ-клиент» и модуль «Агент» устанавливаются на все защищаемые компьютеры, включая компьютер, на котором установлен модуль «Центр Управления».

Для обеспечения взаимодействия «КАНОЭ-клиент» с модулем «Центр Управления» посредством модуля «Агент» используются порты 17001, 17002, 17005.

Для подключения рабочих станций необходимо провести сканирование сети, установку модуля «Агент» и его привязку к модулю «Центр Управления».

3.1.9. Сканирование сети

Для успешного выполнения операции сканирования на удаленной рабочей станции должен быть доступен ресурс Admin$ с правами администратора.

Примечание. Для получения доступа к Admin$ необходимо, чтобы имелись следующие ключи со значением ”**1**” и типом **REG_DWORD** в реестре и перезагрузить операционную систему:

ОС: Windows 2003
Ветка: HKLM\System\CurrentControlSet\Services\lanmanserver\parameters
Ключ: AutoShareServer

ОС: Windows XP
Ветка: HKLM\System\CurrentControlSet\Services\lanmanserver\parameters
Ключ: AutoShareWks
ОС: Windows Vista / Server 2008 / Windows 7 / Server 2008 R2
Ветка: HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\System
Ключ: LocalAccountTokenFilterPolicy

Примечание. Перед выполнением операции сканирования на удаленной рабочей станции, работающей под управлением ОС Windows XP, необходимо в свойствах папки, на вкладке "Вид" деактивировать пункт "Использовать простой общий доступ к файлам"/"Use simple file sharing".

Для выполнения операции сканирования перейдите на страницу **Сканирование** в меню **Администрирование**. Данное меню позволяет осуществить сканирование сети (определить тип ОС, наличие агента удаленного администрирования) и подключить рабочую станцию к Центру Управления.

Необходимо:

1) задать IP диапазон для сканирования (рис. 16);

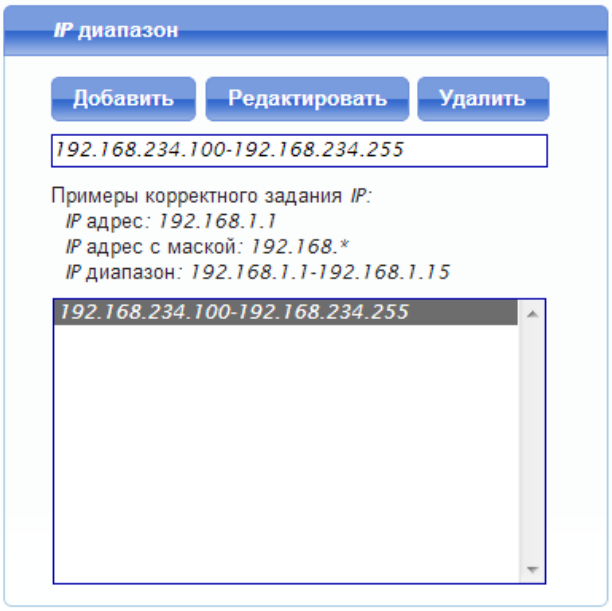

Рис. 16

Примечание. При сканировании исключаются те IP адреса, которые уже используются на странице Компьютеры. В случае, если после такого исключения список адресов на сканирование останется пустым, будет выдано соответствующее сообщение и процесс сканирования не будет начат.

2) задать реквизиты (домен либо имя локальной машины, логин и пароль администратора домена) (рис. 17);

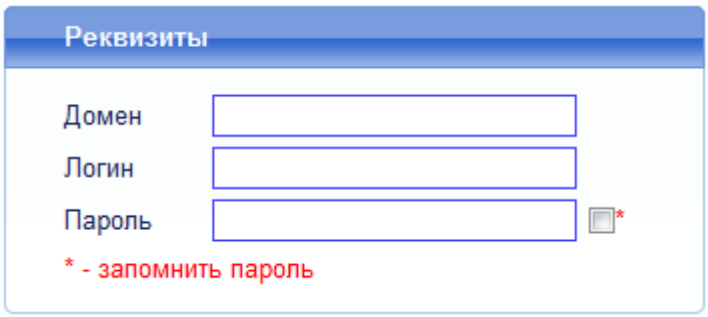

Рис. 17

3) задать дополнительные настройки (количество отправляемых пакетов, таймаут при задержке ответа от удаленной машины) (рис. 18);

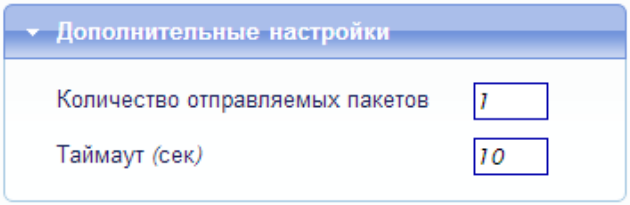

Рис. 18

4) запустить сканирование (кнопка **Старт**).

В результате получаем список, представленный на рис. 19.

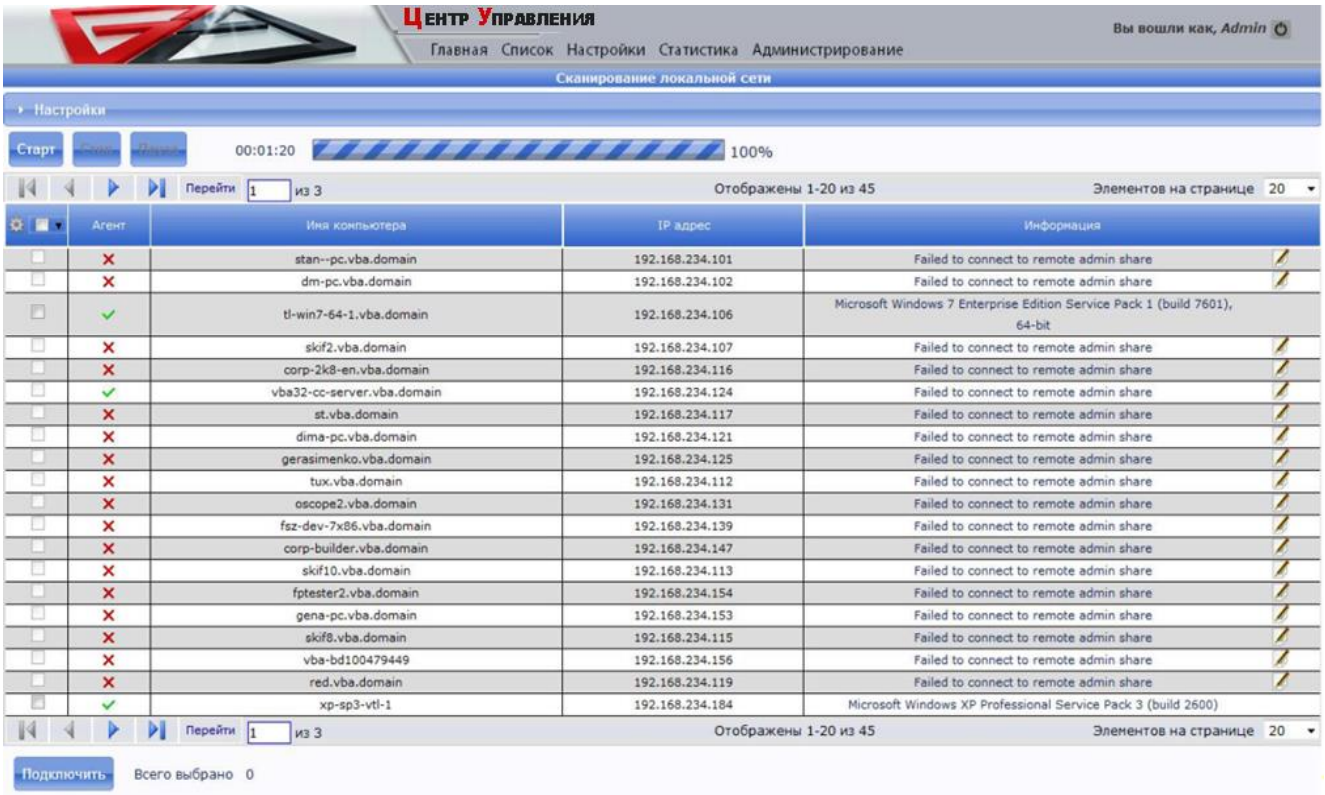

Рис. 19

Примечание. В случае, если компьютер не был обнаружен, проверьте настройки **Брандмауэра Windows** (необходимо разрешить отвечать на входящие эхо-сообщения ICMP (утилита **Ping**)).

Для устройств, в которых тип операционной системы не определился, имеется возможность добавлять комментарии (кнопка в правом углу столбца **Информация**) (рис. 19).

3.1.10. Установка модуля «Агент» и его привязка к модулю «Центр Управления»

Для установки модуля «Агент» необходимо: по завершению сканирования выбрать рабочие станции, на которые необходимо установить модуль «Агент», и нажать кнопку **Подключить** (рис. 20). В случае успешного запуска задачи, должно появиться сообщение о постановке в очередь на выполнение.

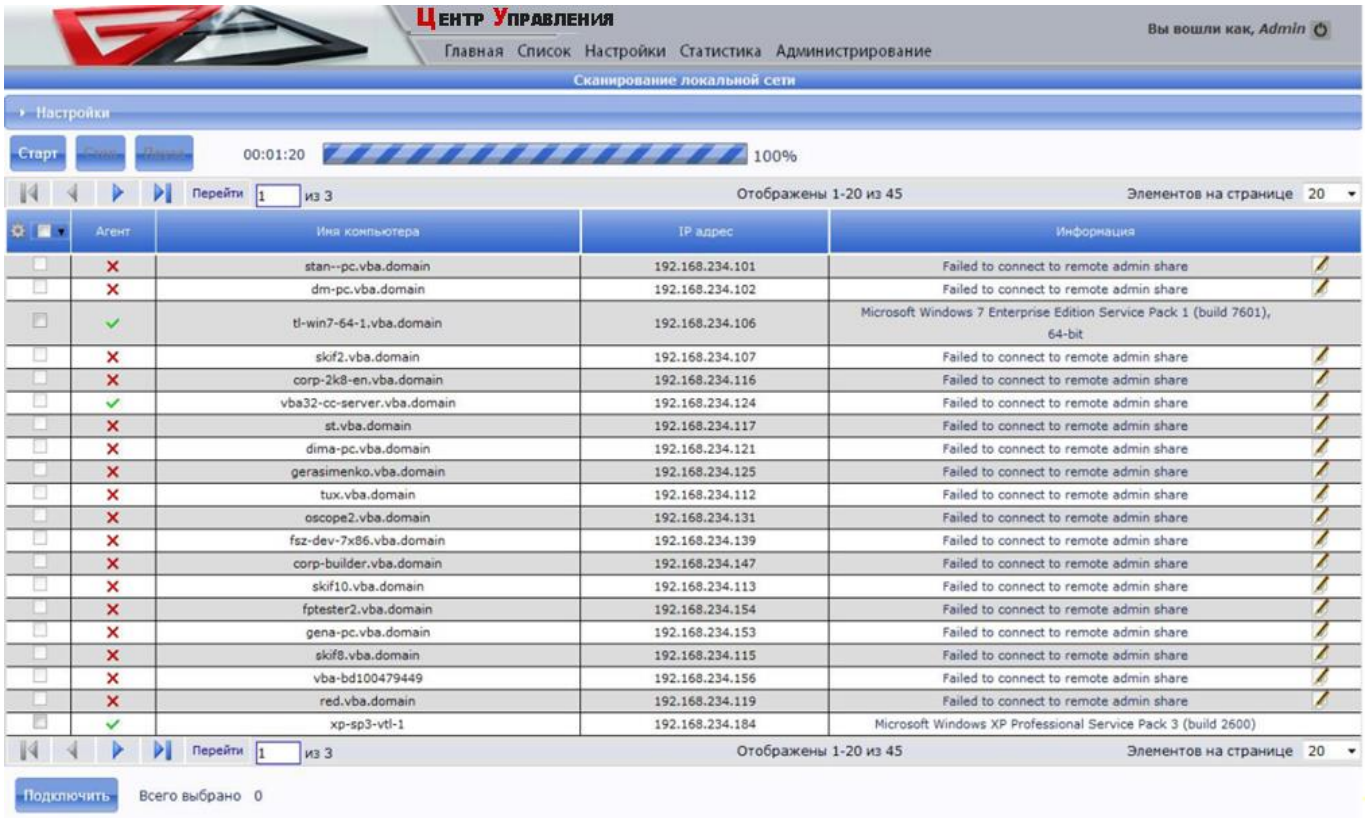

Рис. 20

Результаты установки можно просмотреть на странице **Задачи подключения** (рис. 21).

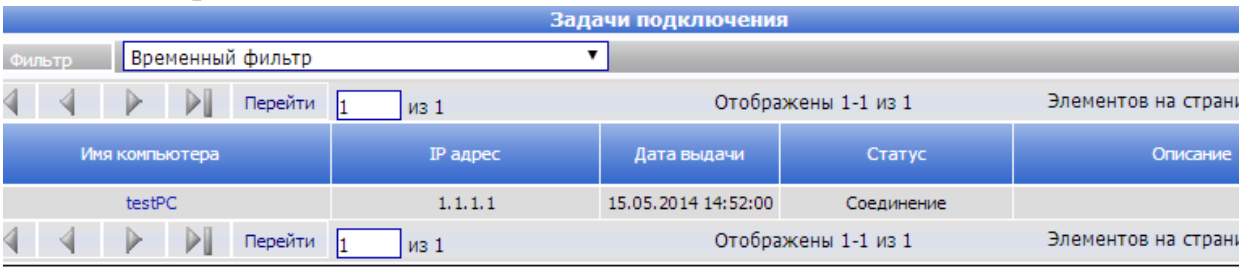

Рис. 21

Модуль «Агент» установлен тогда, когда статус будет **Успешно**.

Настройка модуля «Агент» на текущий модуль «Центр Управления» происходит автоматически после успешной установки.

Примечание. При попытке подключения рабочей станции с уже установленным модулем «Агент» данная рабочая станция помещается в таблицу **Задачи подключения** со статусом **Установлен** и выполняется разовая отправка пакета с настройками. В то время, как на рабочие станции со статусом установки модуля «Агент» **Успешно** отправка происходит периодически, до тех пор, пока эта станция не подключится к модулю «Центр Управления».

После успешной установки модуля «Агент» становится доступна установка «КАНОЭ-клиент» п. 3.1.11.

3.1.11. Установка клиентской части сетевого варианта исполнения комплекса КАНОЭ

Перед установкой сетевого варианта исполнения КАНОЭ-клиент необходимо выполнить базовую задачу **Обновить ключевой файл**.

При необходимости ввода дополнительных параметров, возможно, потребуется развернуть дополнительные настройки нажатием на треугольник справа в строке.

Данная задача (рис. 22), дает возможность установить продукты на удаленные рабочие станции. Для этого необходимо выбрать продукт из списка **Продукт** и задать **Аргументы** командной строки, при необходимости.

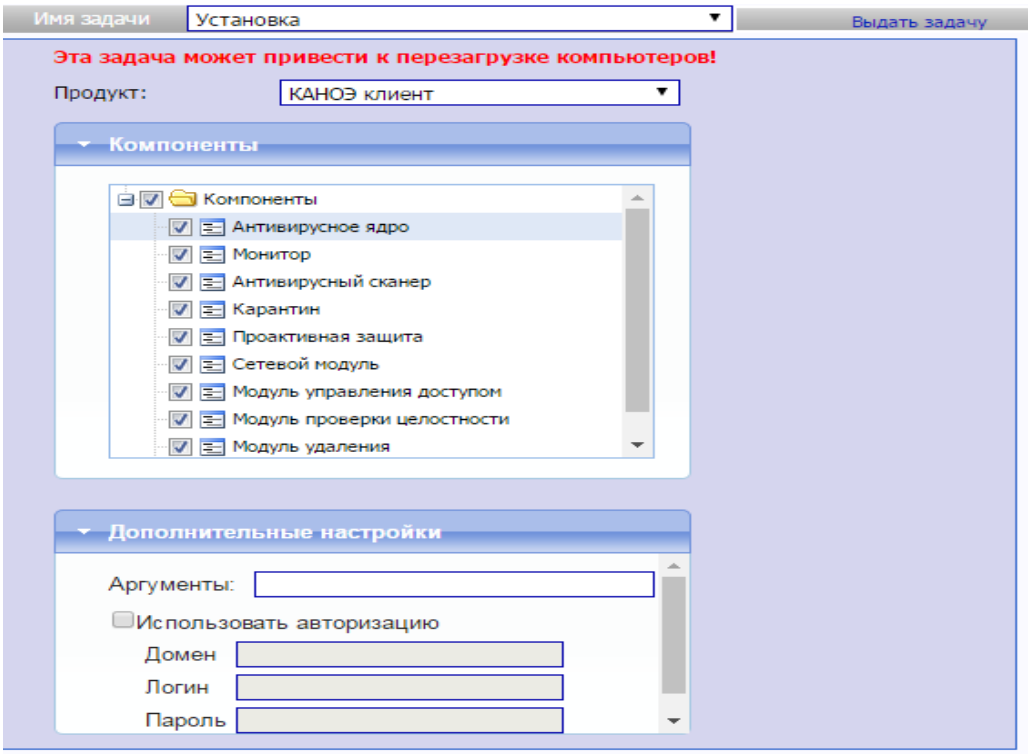

Рис. 22

3.1.12. Обновление сетевого варианта исполнения комплекса КАНОЭ

Перед началом работы следует обновить клиентскую часть сетевого варианта исполнения КАНОЭ и модуль «Центр Управления». Для этого необходимо выдать задачу **Настроить Диспетчер** (см. п. 4.10.2.1.11) для установленных комплексов, где указать путь обновления.

3.2. Установка локального варианта исполнения

Для установки программы локального варианта исполнения комплекса КАНОЭ на ПЭВМ необходимо запустить на выполнение исполняемый файл kanoe.exe. Для данной установки необходимы права администратора системы.

После запуска исполняемого файла KANOE.exe выбрать тип установки (рис. 23) **Локальная** нажать кнопку **Продолжить**, начнется установка локального варианта исполнения комплекса КАНОЭ

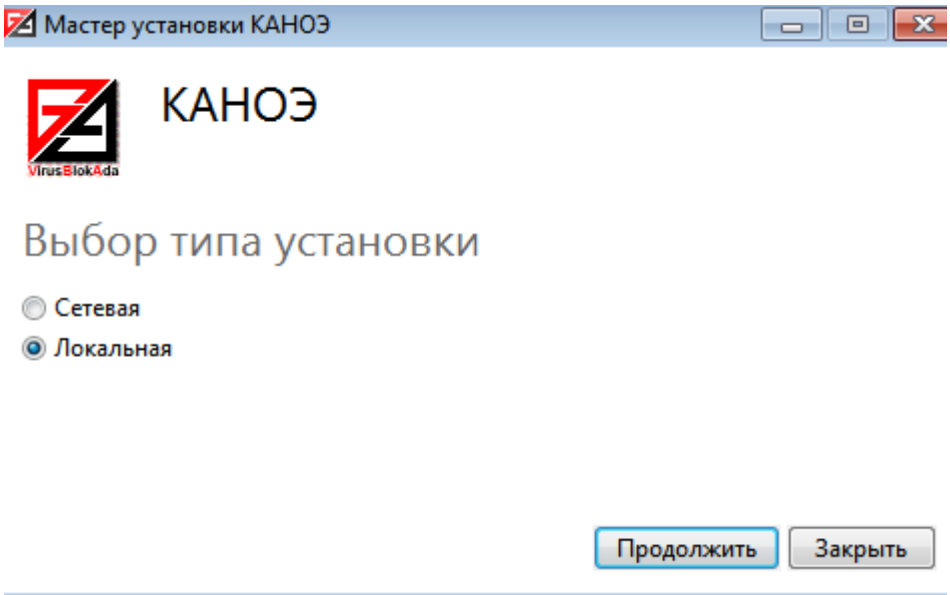

Рис. 23

Окно приветствия содержит рекомендации по подготовке к установке комплекса КАНОЭ (рис. 24).

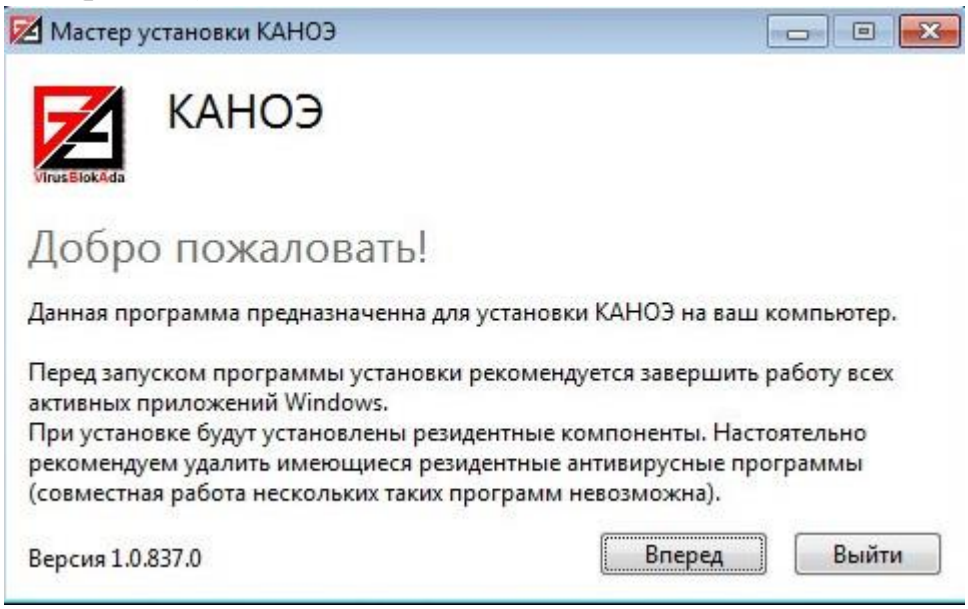

Рис. 24

На следующем этапе мастер установки предоставляет форму для установки регистрационного ключа, подтверждающего легальность пользования продуктом. Необходимо указать путь к регистрационному ключу. Нажмите кнопку **Обзор** (рис. 25) и в появившемся диалоге укажите путь к файлу vba32.key.

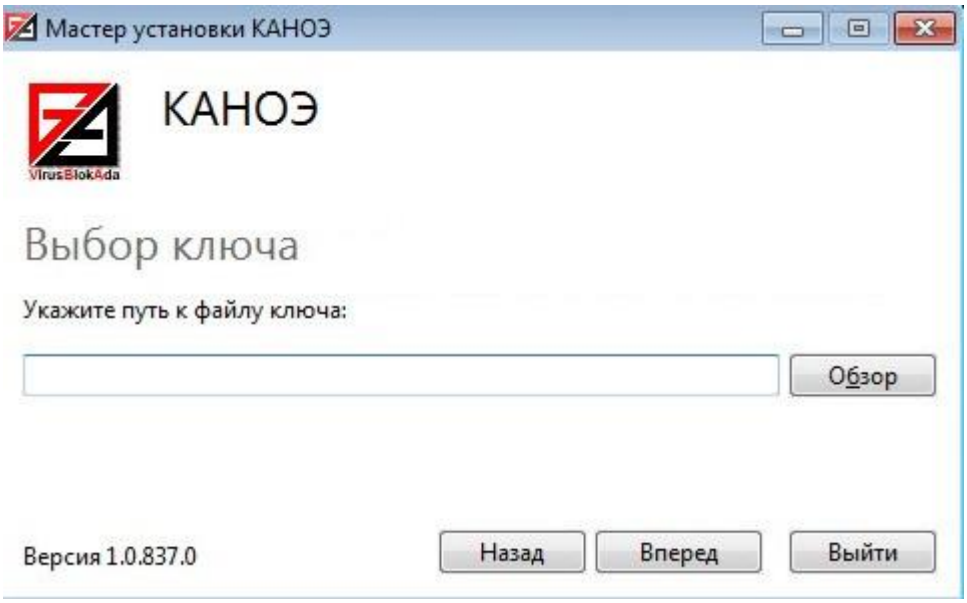

Рис. 25

Примечание. Без регистрационного ключа дальнейшая установка программы локального варианта исполнения комплекса КАНОЭ невозможна. Необходимо обязательно указать действительный ключ комплекса КАНОЭ.

Нажмите кнопку **Вперед** для продолжения установки.

Далее необходимо выбрать устанавливаемые модули и компоненты (рис. 26).

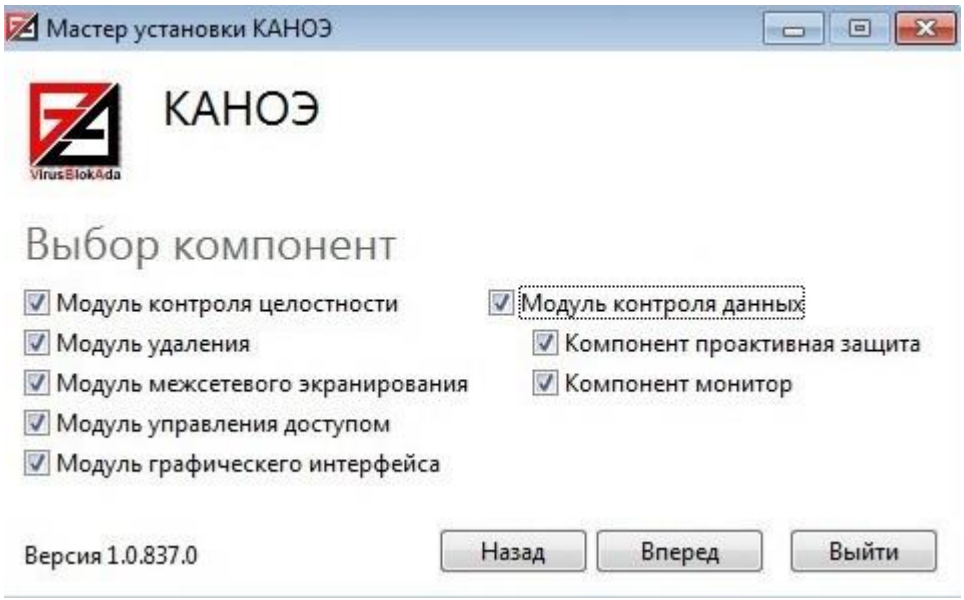

Рис. 26

Примечания:

1. Для работы компонента монитор необходим компонент проактивная защита, поэтому при выборе компонента монитор будет автоматически выбран и

компонент проактивная защита. В случае отсутствия выбора компонента проактивная защита не будет установлен и компонент монитор.

2. Компоненты проактивная защита и монитор требуют наличия модуля контроля данных. Выбор этих компонентов автоматически выбирает установку модуля контроля данных.

Нажмите кнопку **Установить** (рис. 27) для начала установки файлов. Нажмите кнопку **Назад**, если необходимо повторно ввести данные для установки или нажмите кнопку **Выйти** для выхода из программы установки.

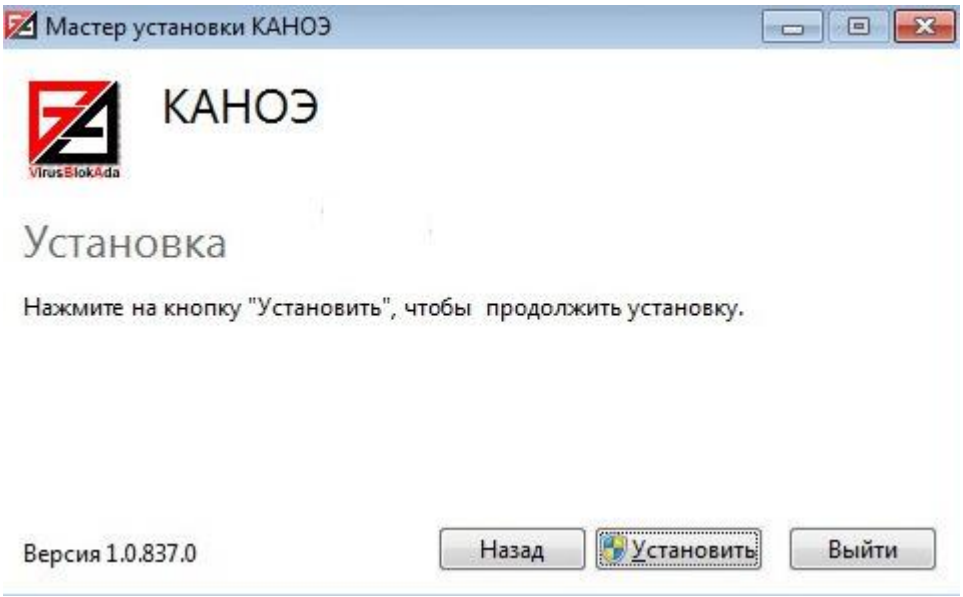

Рис. 27

Окно процесса установки (рис. **Ошибка! Источник ссылки не найден.**).

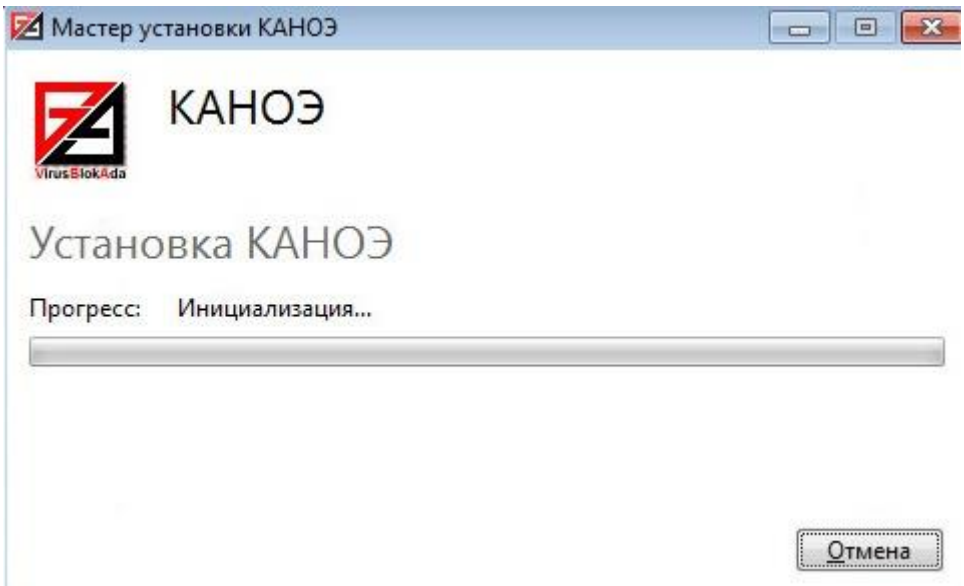

Рис. 28

При завершении установки на компьютер нажмите кнопку **Перезагрузка** (рис. 29). Для выхода из программы установки нажмите кнопку **Закрыть**.

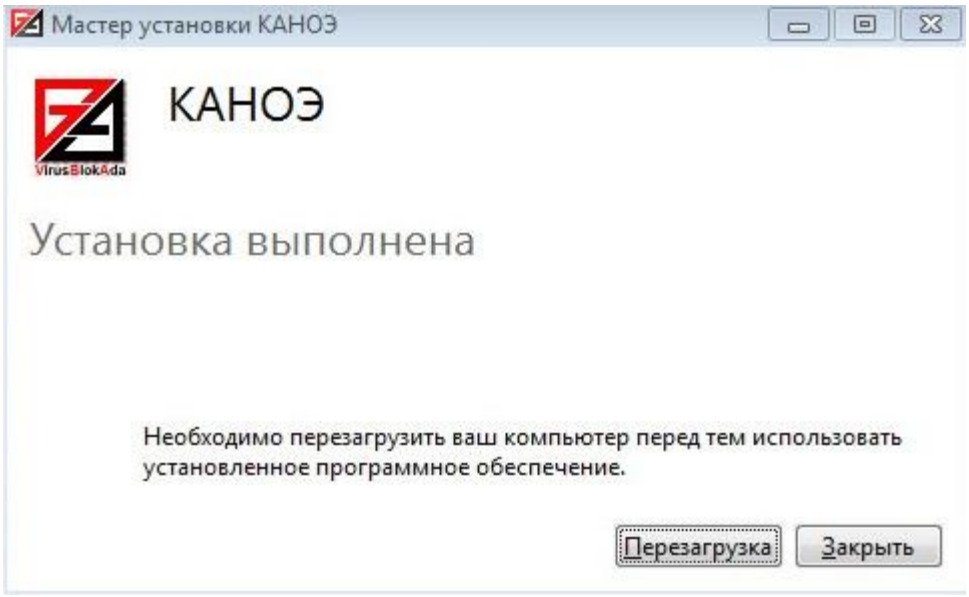
Мастер установки КАНОЭ
КАНОЭ
VirusBlokAda
Установка выполнена
Необходимо перезагрузить ваш компьютер перед тем использовать установленное программное обеспечение.
Перезагрузка
Закрыть

Рис. 29

4. ВЫПОЛНЕНИЕ ПРОГРАММЫ И СООБЩЕНИЯ ОПЕРАТОРУ

4.1. Раздел Диспетчер

Раздел **Диспетчер** комплекса КАНОЭ включает в себя вкладки:

1) Состояние;
2) Обновление;
3) Настройки;
4) Планировщик.

4.1.1. Вкладка Состояние

Вкладка **Состояние** (рис. 30) содержит информацию о состоянии комплекса КАНОЭ.

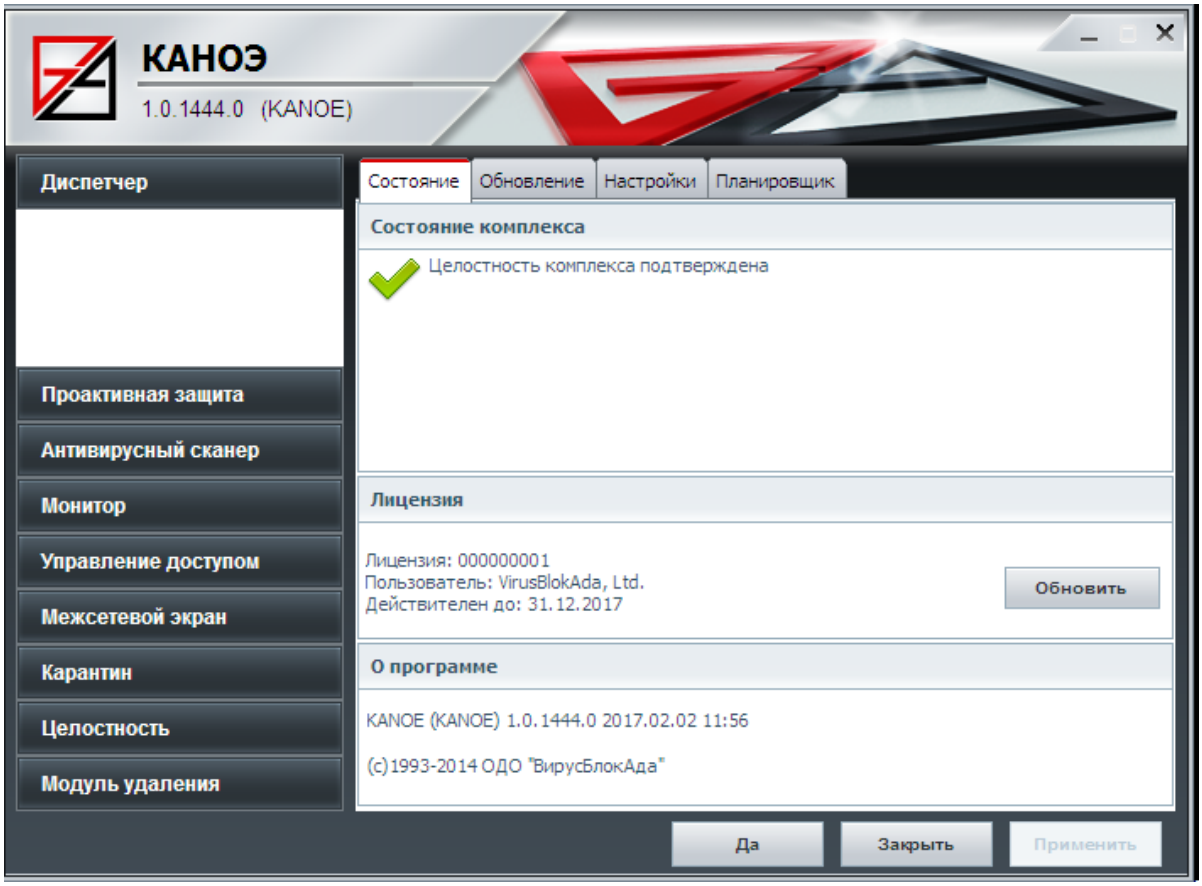

Рис. 30

4.1.2. Вкладка Обновление

Вкладка **Обновление** (рис. 31) имеет следующие параметры и возможности:

1) запуск/остановка обновления;
2) добавление, удаление и редактирование путей обновления. Возможность перемещения пути обновления вверх и вниз в соответствии с приоритетом,

установленным пользователем. Список по умолчанию содержит один путь обновления;

Примечание. Допускается выбор пути обновления с локальных дисков и ЛВС. Обновление с сетевых дисков (mapping) не поддерживается.

3) выбор использования при доступе к ресурсу обновления либо прокси-сервера, либо пользовательской учетной записи, либо и то и другое. При этом при использовании прокси-сервера потребуется настройки прокси-сервера, а при использовании пользовательской учетной записи имя пользователя и пароль.

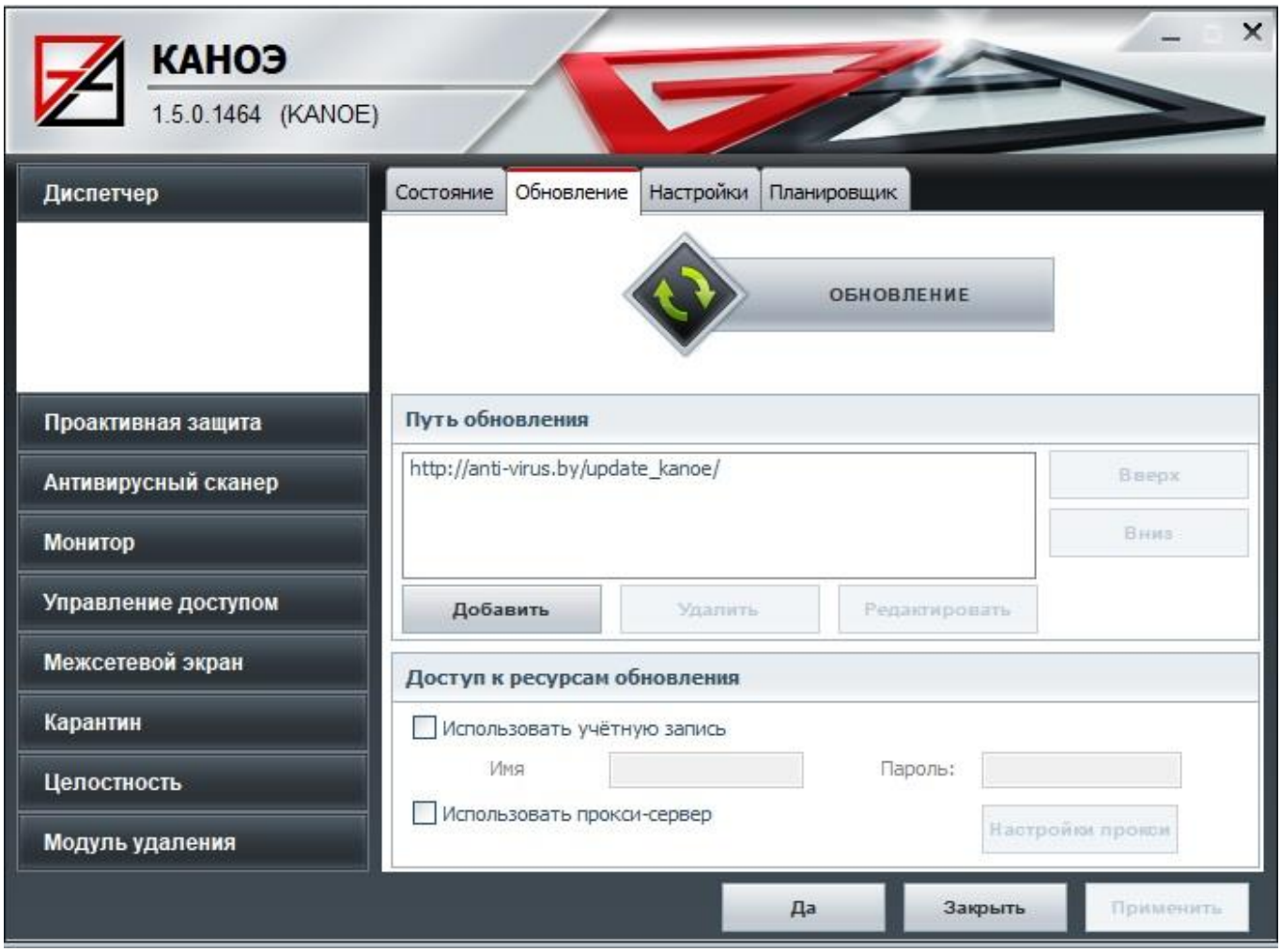

Рис. 31

В окне **Настройки прокси** (рис. 32) необходимо ввести тип прокси-сервера, адрес, порт и если вы хотите использовать авторизацию, то имя пользователя и пароль.

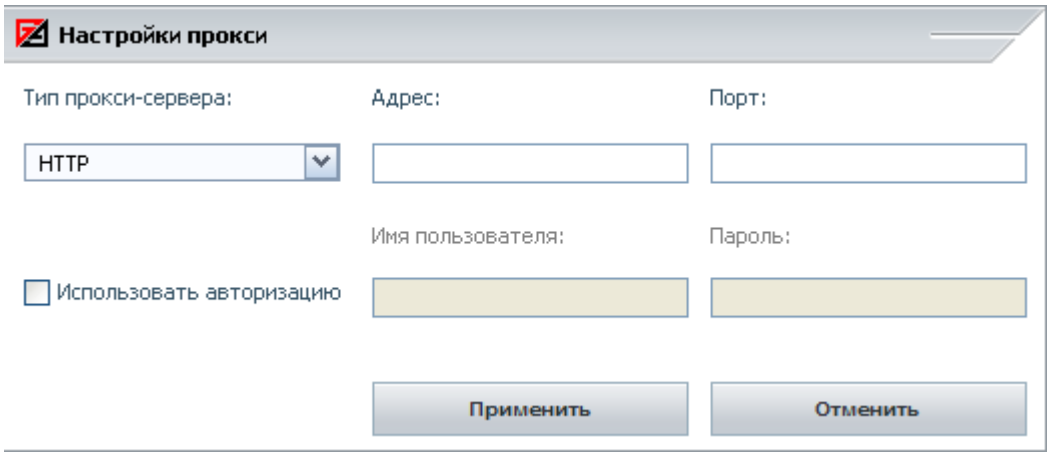

Рис. 32

4.1.3. Вкладка Настройки

Вкладка **Настройки** (рис. 33) имеет следующие параметры и возможности:

1) добавление, редактирование и удаление пользовательской парольной записи для доступа к настройкам диспетчера. При добавлении нового пользователя после нажатия на кнопку **Добавить** возникает диалог (рис. 33), который просит ввести имя пользователя и пароль (пароль вводится дважды). Введена будет лишь та запись, которая еще не присутствует в списке. При редактировании после нажатия на кнопку **Изменить** возникнет диалог с введенным именем пользователя, который просит ввести новый пароль и повторить его. При нажатии на кнопку **Удалить** выделенная запись в списке будет удалена;

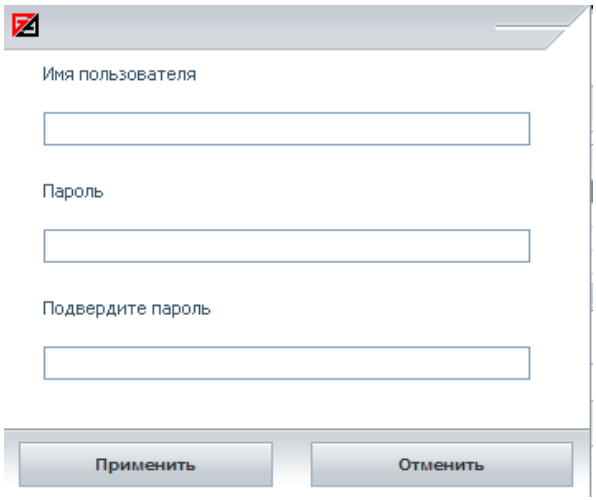

Рис. 33

2) выбор языка интерфейса: русский или английский (рис. 34).

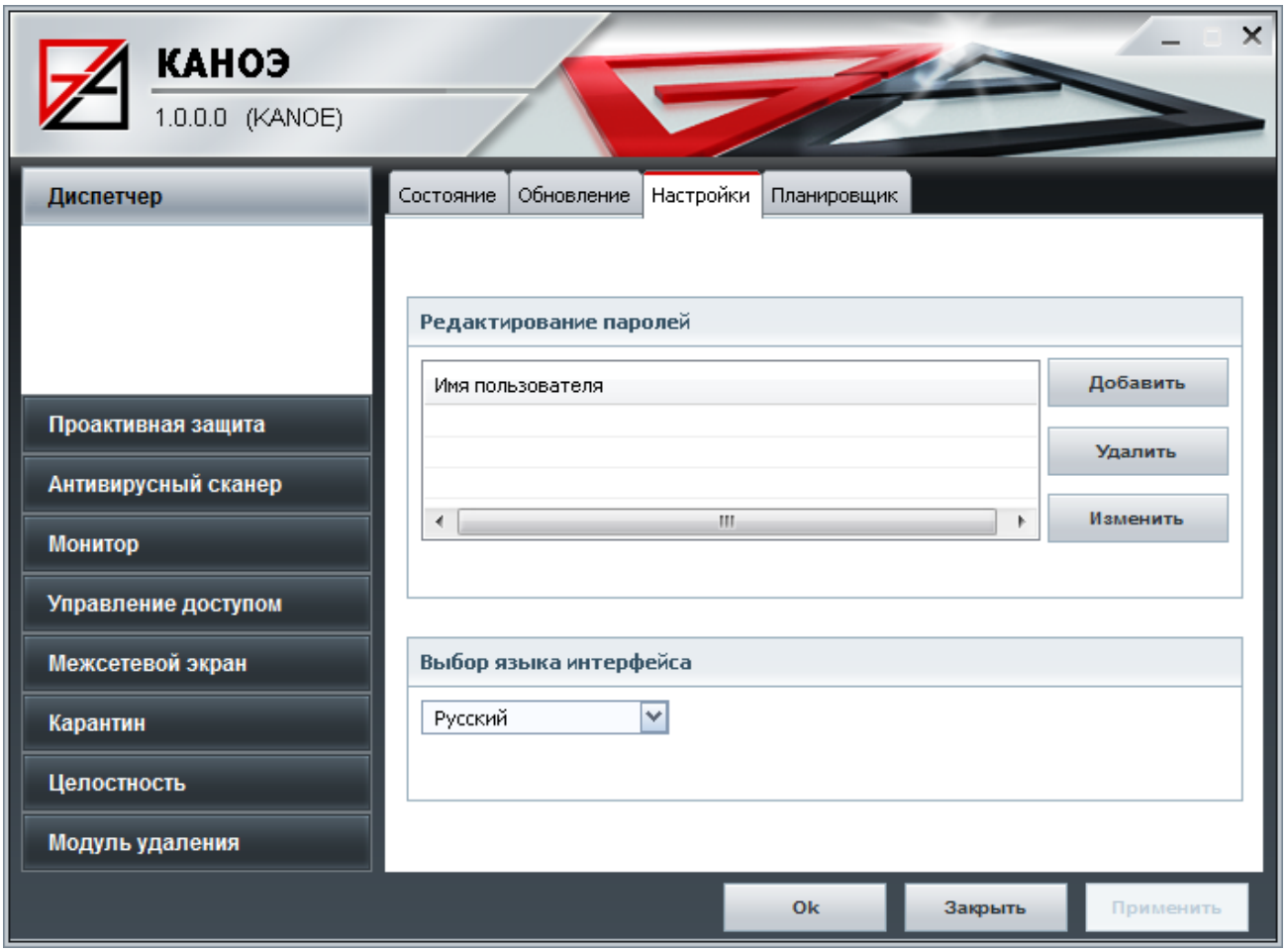

Рис. 34

4.1.4. Вкладка Планировщик

Вкладка **Планировщик** обеспечивает настройку запуска задач в фоновом режиме в указанные временные рамки (рис. 35).

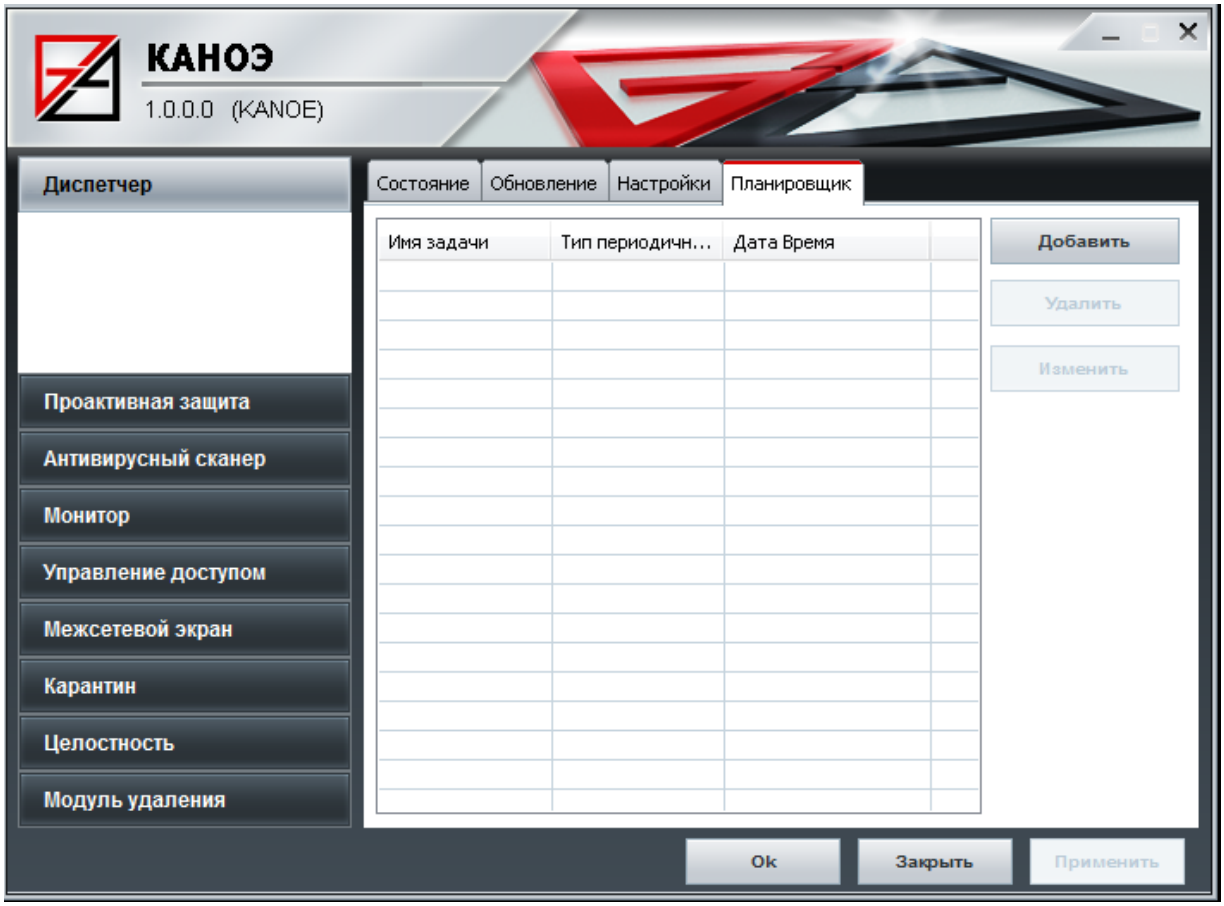

Рис. 35

Добавление стандартных операций (рис. 36) комплекса КАНОЭ производятся по нажатию кнопки **Добавить** (рис. 35).

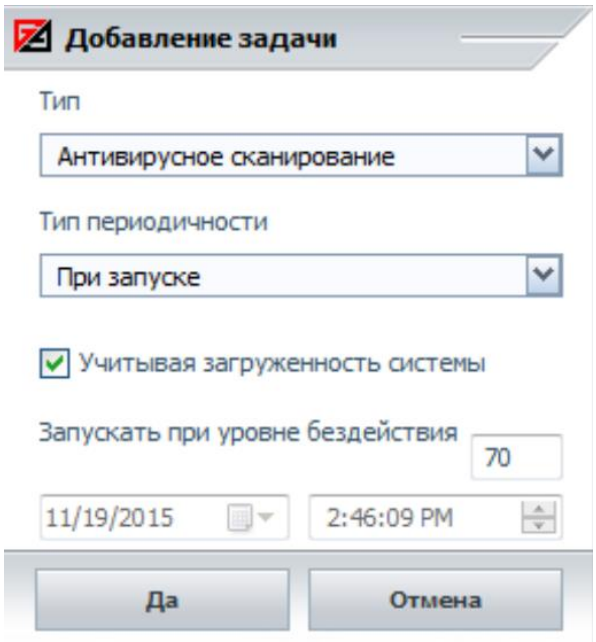

Рис. 36

Удаление стандартных операций комплекса КАНОЭ производятся по нажатию кнопки **Удалить** (рис. 35).

Изменение стандартных операций комплекса КАНОЭ производятся по нажатию кнопки **Изменить** (рис. 35).

Для принятия всех изменений нужно нажать на кнопку **Применить** (рис. 35).

4.2. Раздел Проактивная защита

Раздел **Проактивная защита** комплекса КАНОЭ (рис. 37) имеет следующие вкладки:

1) Защищаемые объекты;
2) Пользователи;
3) Аудит;
4) Принтеры
5) Журнал;
6) События журнала.

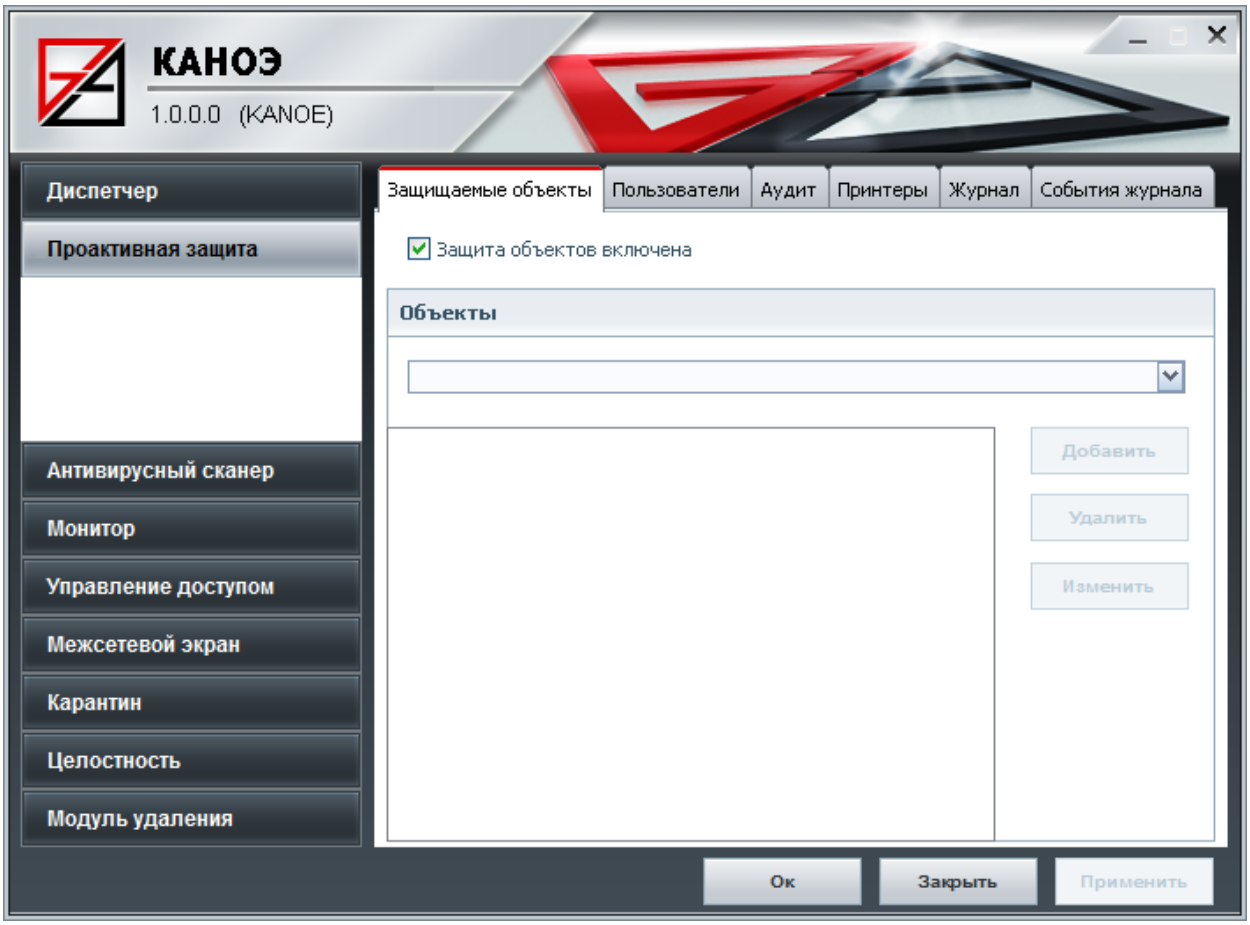

Рис. 37

4.2.1. Вкладка Защищаемые объекты

Вкладка **Защищаемые объекты** (рис. 38) имеет следующие возможности:

1) включение\выключение защиты объектов;
2) выбор типа защищаемого объекта:
   а) защищенные директории/файлы – к этим объектам имеют доступ только доверенные приложения;
   б) директории/файлы (только чтение) – к этим объектам предоставлен доступ на чтение. Доверенные приложения имеют полный доступ;
   в) исключенные директории/файлы – объекты, к которым проверка доступа игнорируется;
   г) доверенные приложения – приложения, которые имеют полный доступ к любому защищаемому объекту;
   д) защищенные приложения – приложения, которые нельзя завершить извне;
   е) защищенные ключи/значения реестра – объекты, доступ к которым имеют только доверенные приложения;
   ж) ключи/значения реестра (только чтение) – объекты, к которым предоставляется доступ только для чтения. Доверенные приложения имею полный доступ;
3) настройка защищаемых объектов выбранного типа. Блок **Объекты** содержит функционал по добавлению, удалению и изменению объектов выбранного типа.

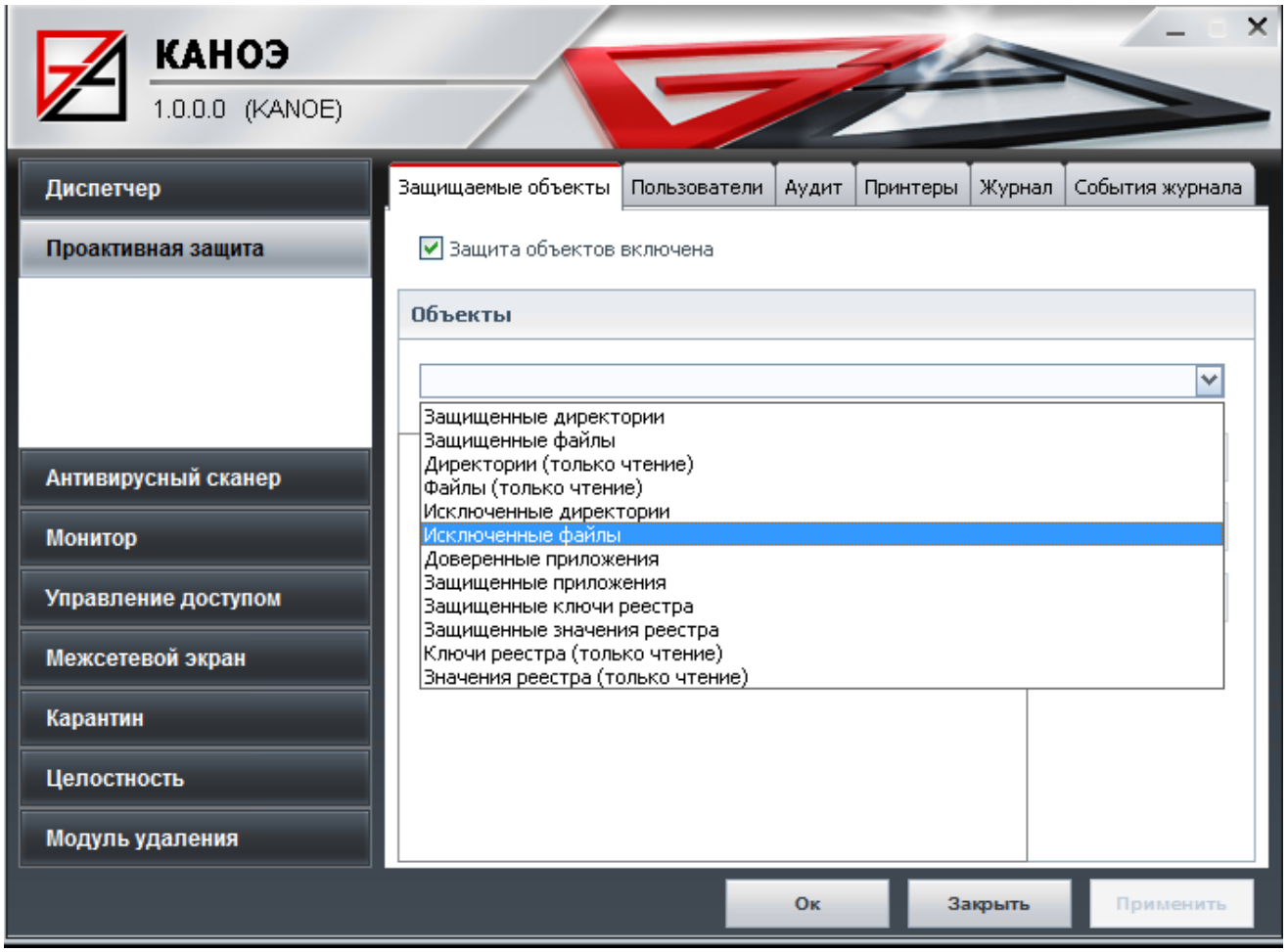

Рис. 38

4.2.2. Вкладка Пользователи

Контроль действий пользователей имеет следующие возможности (рис. 39):

1) включение\выключение контроля действий пользователей;
2) добавление пользователей для определения разрешений для них производиться в блоке **Пользователи**. Если контроль действий пользователей включен, а для пользователя нет настроек, то применяются настройки по умолчанию (<Default>). Блок **Пользователи** содержит кнопки для добавления и удаления пользователей (кнопка **Добавить** и **Удалить** соответственно). При добавлении нового пользователя ему изначально автоматически выставляются настройки по умолчанию. Настройки по умолчанию сконфигурированы таким образом, чтобы пользователь без настроек для него имел возможность войти в систему;
3) настраивать доступные объекты для каждого пользователя:
   a) директории/файлы (полный доступ), ключи реестра (полный доступ) – к этим объектам пользователь будет иметь полный доступ;

б) директории/файлы (только чтение), ключи реестра (только чтение) – к этим объектам пользователю предоставляется доступ только на чтение;

в) разрешенные приложения – список приложений, которые пользователю разрешено запускать;

г) разрешенные принтеры.

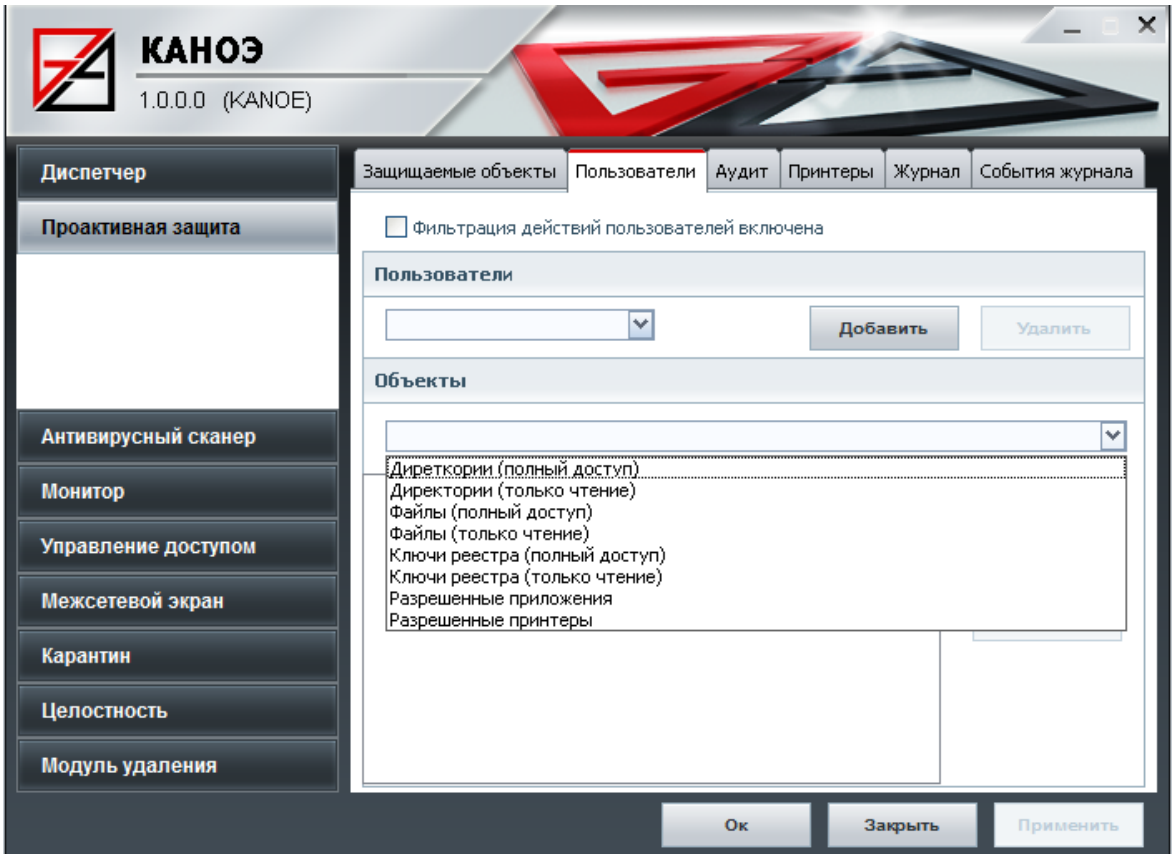

Рис. 39

Блок **Объекты** (рис. 40) содержит функционал по добавлению, удалению и редактированию доступных объектов.

Добавление объектов производится по нажатию кнопки **Добавить.**

Удаление объектов производится по нажатию кнопки **Удалить**.

Редактирование объектов производятся по нажатию кнопки **Изменить**.

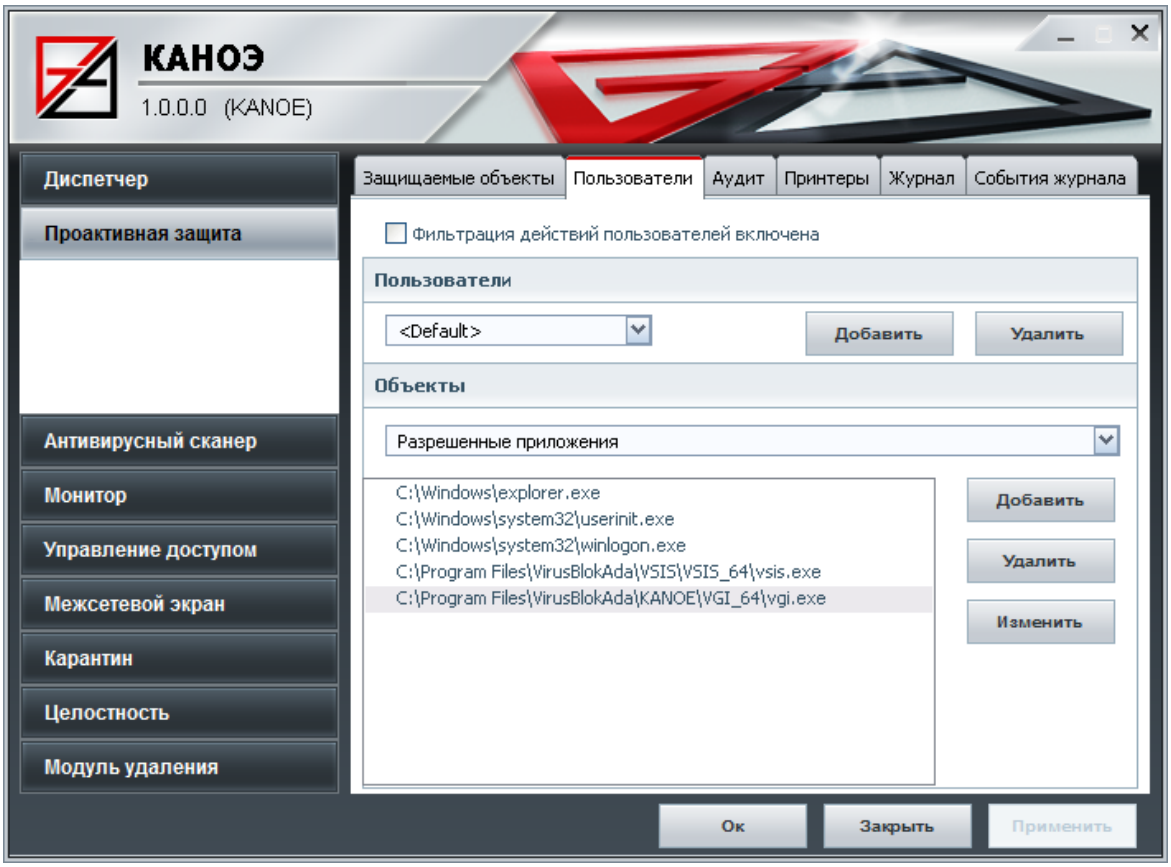

Рис. 40

4.2.3. Вкладка Аудит

Вкладка **Аудит** (рис. 41) имеет следующий функционал:

1) включение\выключение аудита;
2) возможность задавать типы файлов, для которых будет производиться аудит. Типы файлов (расширения) задаются через разделитель «.» (точка) без пробелов.

При доступе к файлам генерируются события, сохраняемые в журналах.

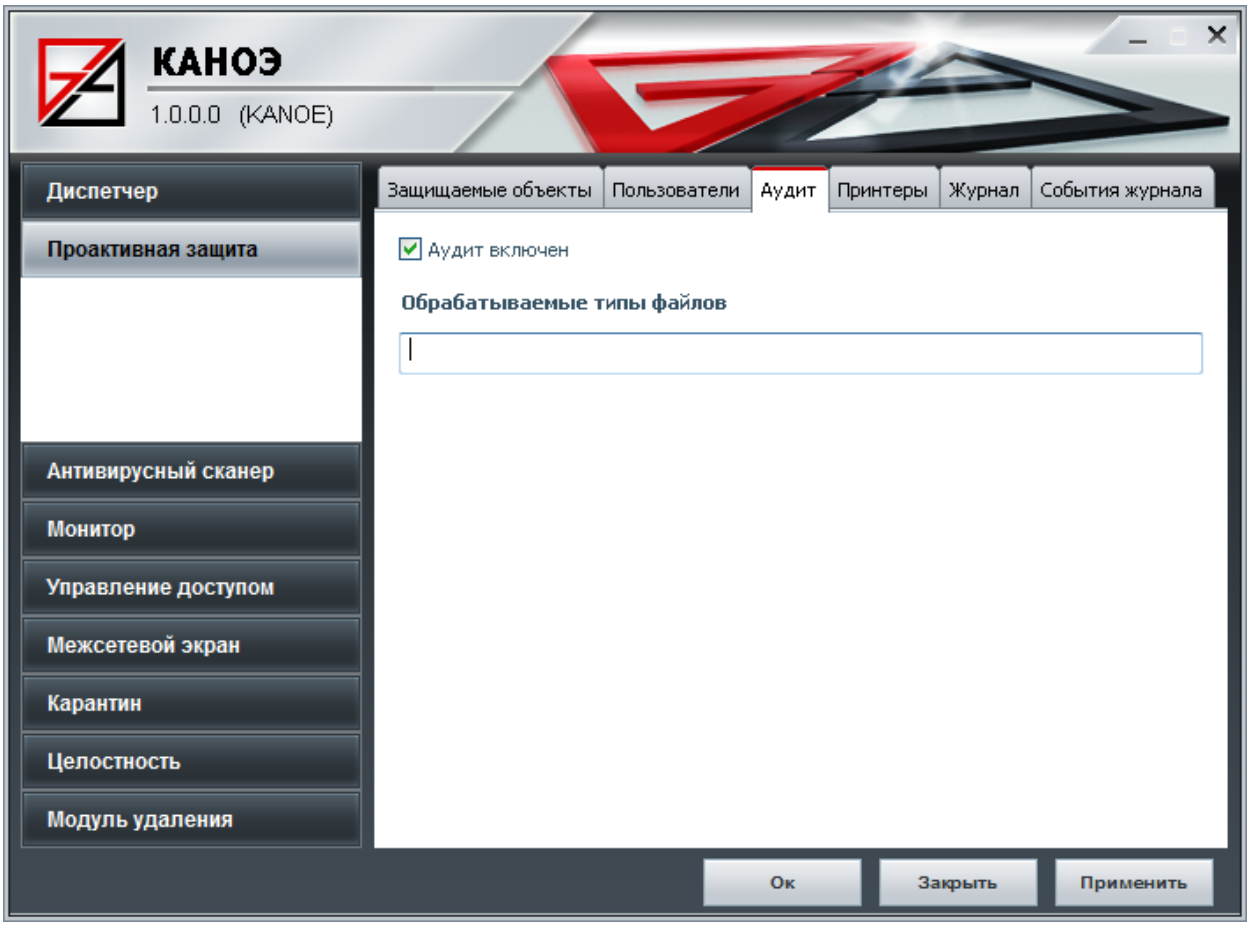

Рис. 41

4.2.4. Вкладка Принтеры

Вкладка **Принтеры** (рис. 42) предоставляет возможность контроля физически подключенных принтеров, с возможностью сохранения событий об отправлении печати документов. Блок **Доверенные принтеры** содержит функционал по добавлению, удалению и редактированию доступных объектов с помощью кнопок **Добавить**, **Удалить** и **Изменить** соответственно.

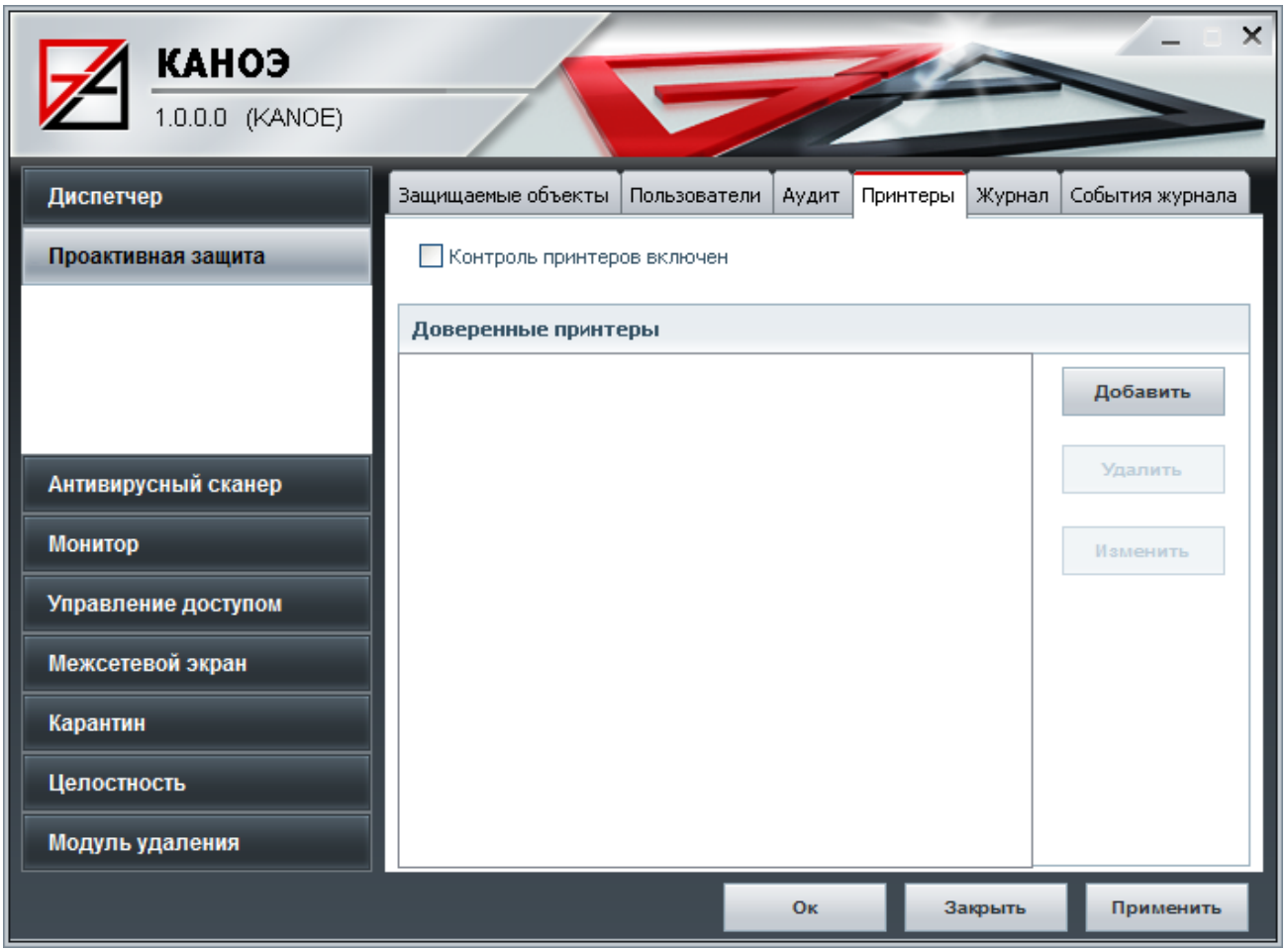

Рис. 42

4.2.5. Вкладка Журнал

Вкладка **Журнал** (рис. 43) служит для отображения событий, которые были сгенерированы модулем **Проактивная защита** и записаны в **Локальный журнал**:

1) **дата начала журнала** – задает дату, начиная с которой будет отображаться журнал;
2) **дата окончания журнала –** задает дату, на которой будет заканчиваться отображение журнала.

Примечание. Дата отображается в формате дат, выбранном на компьютере (например, мм/дд/гггг).

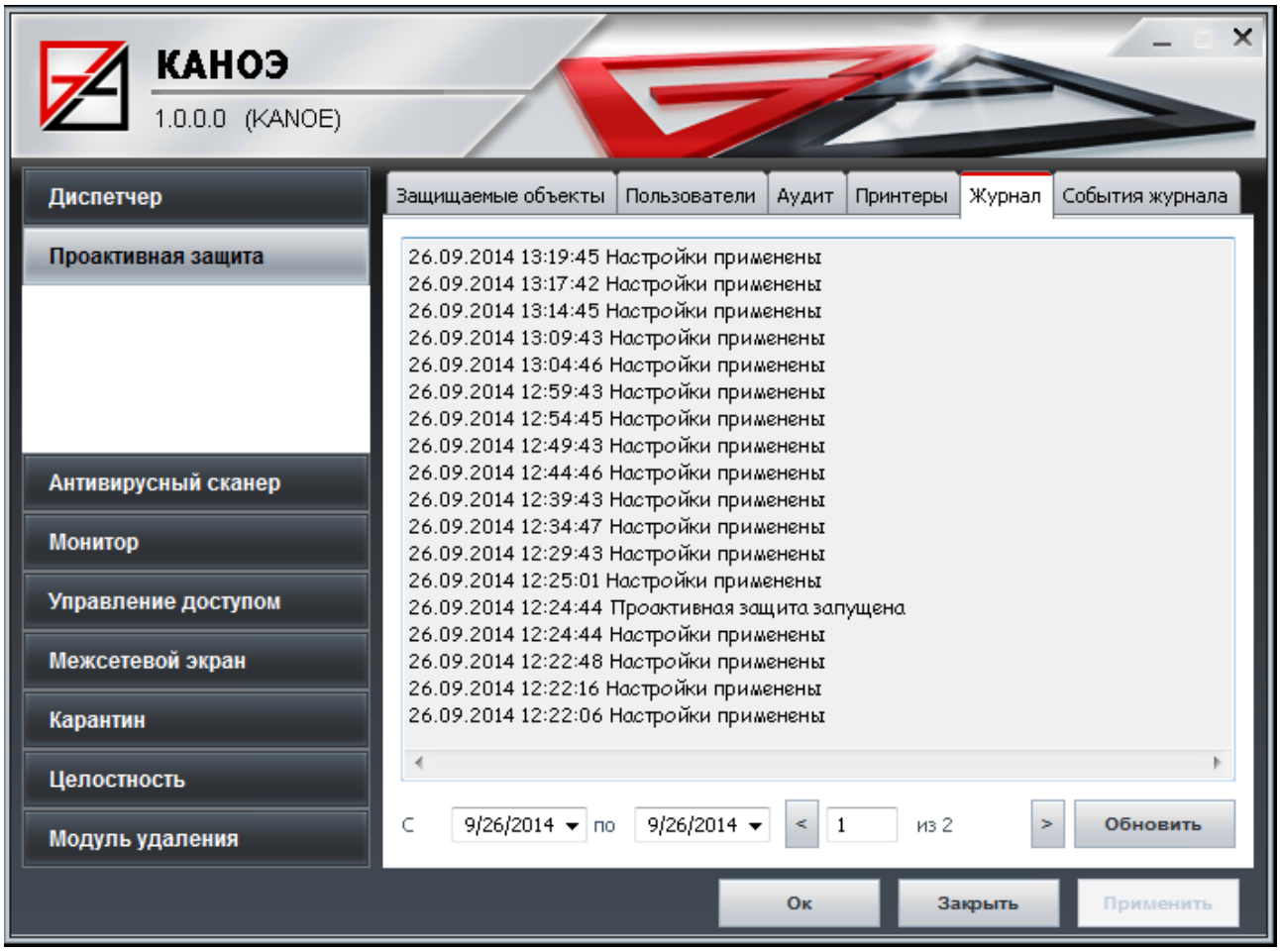

Рис. 43

Нажмите кнопку **Обновить,** чтобы отобразить журнал действий модуля **Проактивная защита** в соответствии с указанными датами.

4.2.6. Вкладка События журнала

Вкладка **События журнала** (рис. 44) служит для настройки в какой журнал будет записываться то или иное событие. Доступные журналы: **журнал ЦУ**, **локальный журнал** и **журнал Windows**.

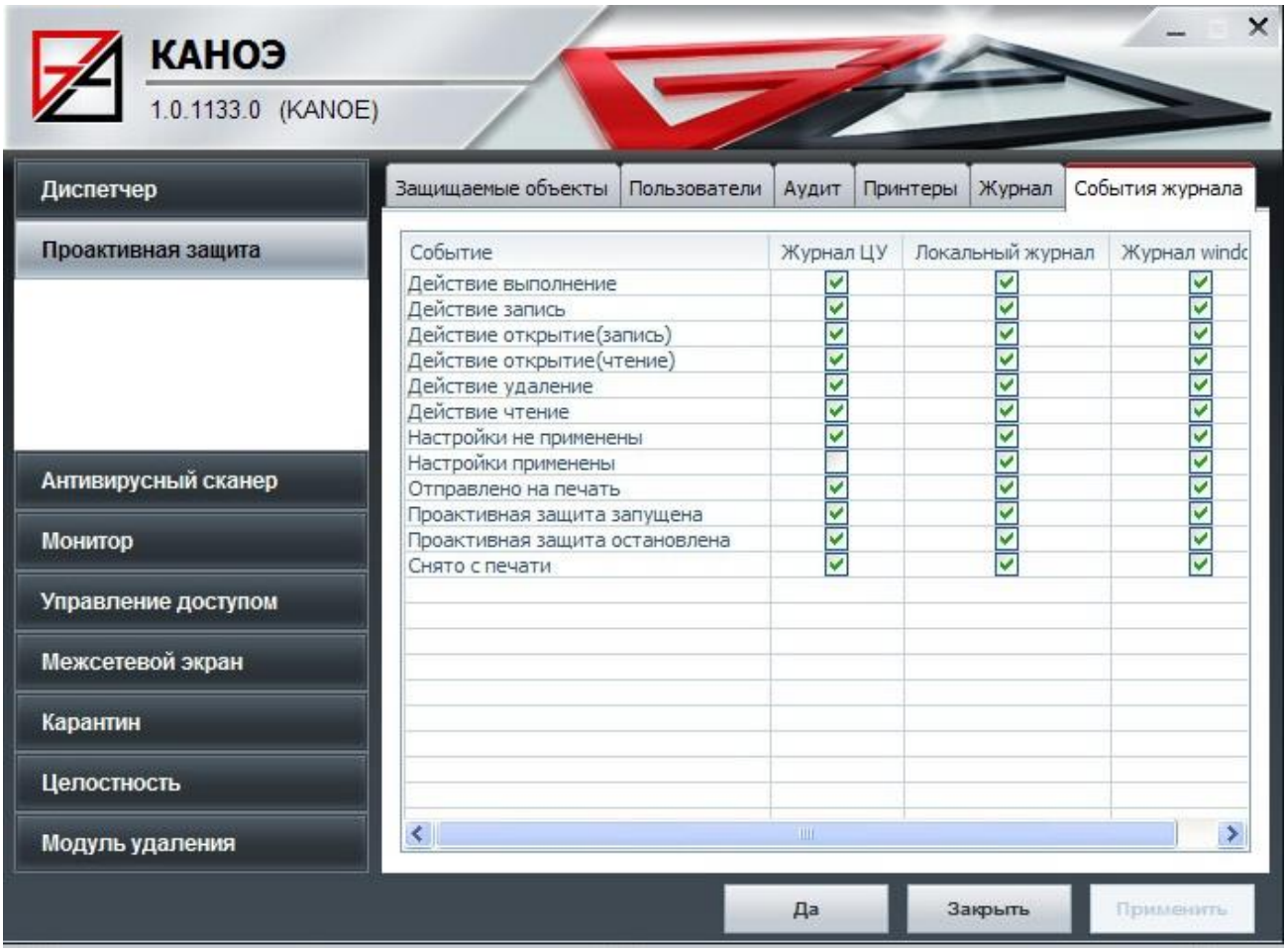

Рис. 44

4.3. Раздел Антивирусный сканер

Сканирование файлов по запросу является неотъемлемой частью полноценной антивирусной защиты.

Раздел **Антивирусный сканер** реализует антивирусную обработку по запросу пользователя.

Раздел **Антивирусный сканер** состоит из вкладок, представляющих удобные средства выбора для работы с объектами обработки.

4.3.1. Вкладка Сканирование

На вкладке **Сканирование** (рис. 45) выполняется настройка путей сканирования, производится запуск сканера. **Антивирусный сканер** позволяет обрабатывать сетевые и локальный диски, каталоги. Для того, чтобы объект был обработан, его необходимо добавить в список обработки.

Вы можете начинать процесс сканирования, нажав кнопку:

1) **Сканировать компьютер**;

2) **Запуск**.

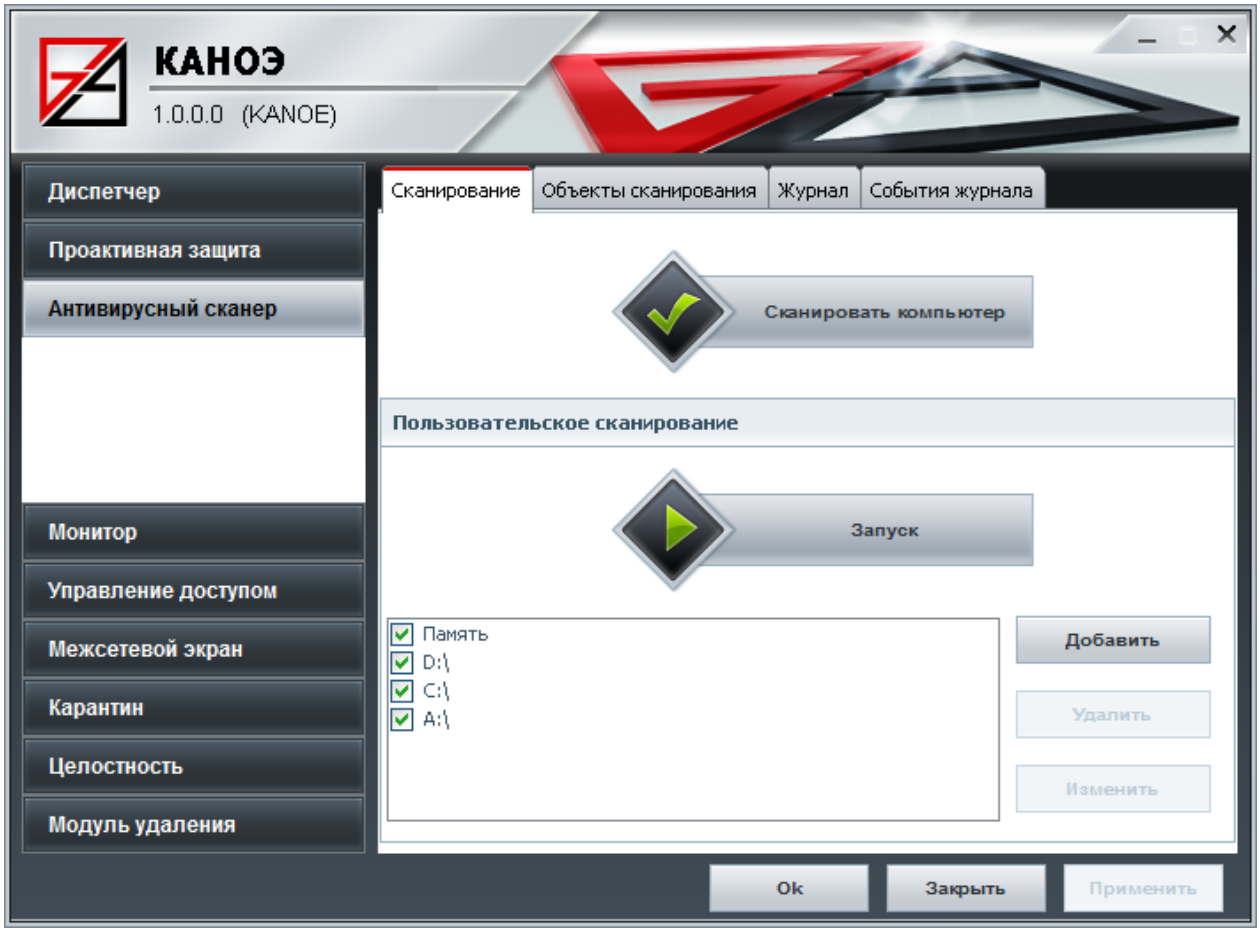

Рис. 45

4.3.1.1. Запуск сканирования путем нажатия кнопки Сканировать компьютер

При нажатии кнопки **Сканировать компьютер** запускается проверка памяти и всех выбранных дисков, процесс проверки отображается в появившемся окне **Сканирование** (рис. 46), можно запускать, приостанавливать и продолжать, а также прекращать процесс антивирусной обработки.

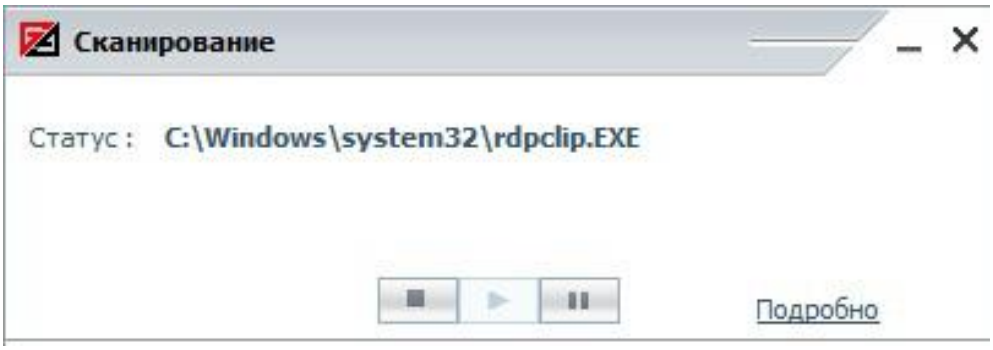

Рис. 46

Статус

Во время сканирования можно видеть текущий **Статус** сканирования. Он отображается в верхней части диалога сканирования.

Приостановление и продолжение процесса антивирусной обработки

Во время работы **Антивирусного сканера** можно приостанавливать и возобновлять процесс сканирования:

1) чтобы приостановить процесс сканирования нажмите кнопку ⏸ на диалоге сканирования;
2) чтобы возобновить процесс сканирования нажмите кнопку ▶ на диалоге сканирования.

Прекращение обработки

Чтобы прекратить процесс сканирования нажмите кнопку ■ на диалоге сканирования.

Расширенный вид

Чтобы включить расширенное отображение диалога сканирования нажмите кнопку **Подробно.** Чтобы отключить расширенное отображение нажмите кнопку **Скрыть** (рис. 47).

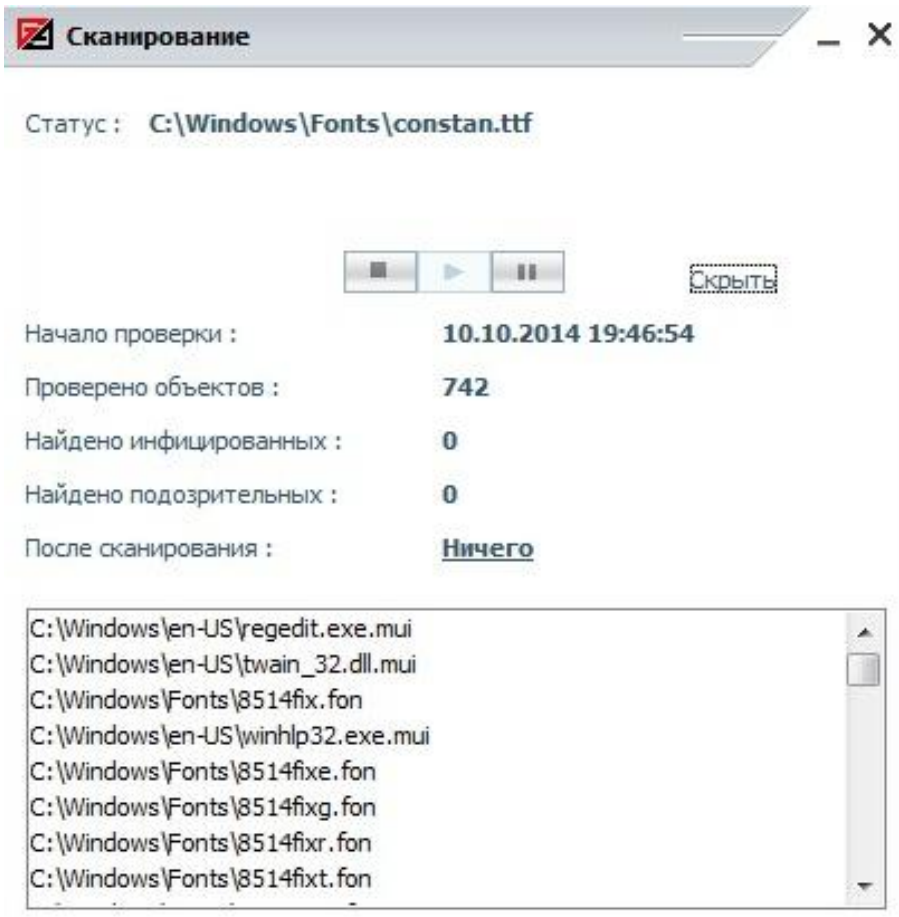

Рис. 47

Действия после остановки сканирования

Можно задать действие, которое будет совершено после окончания сканирования и выбрать один из следующих пунктов действия по завершению сканирования:

1) **Ничего** - никаких действий не производится;
2) **Закрыть** - закрывается окно сканирования, если после окончательного сканирования не обнаружены инфицированные или подозрительные объекты.

Просмотр результатов обработки

Каждый запуск процесса сканирования может сопровождаться отображением информации о ходе обработки на диалоге сканирования и ведением журналов.

Панель результатов

Панель результатов находится в нижней части окна сканирования и позволяет наблюдать за процессом обработки объектов, получить результаты сканирования в виде списка объектов.

Статистика

Диалог сканирования содержит статистику работы Сканера при последнем его запуске:

1) **Начало проверки** - показывает время начала сканирования;
2) **Проверено объектов** - показывает общее количество обработанных файлов;
3) **Найдено инфицированных** - показывает количество обнаруженных инфицированных файлов;
4) **Найдено подозрительных** - показывает количество обнаруженных подозрительных файлов.

4.3.1.2. Запуск сканирования путем нажатия кнопки Запуск

При нажатии кнопки **Запуск** запускается проверка выбранных объектов из списка обработки.

Список пользовательского сканирования состоит из 3 частей:

1) **Память** – сканирование запущенных приложений;
2) **Системные диски** – диски на локальном компьютере;
3) **Пользовательский список обработки** – диски, каталоги или файлы, добавляемые пользователем.

Для выбора уже существующего диска, каталога или файла в списке обработке установите результат выбора напротив нужного объекта.

Пользовательский список обработки формируется путем добавления объектов обработки в список путей сканирования.

Для добавления нового диска, каталога или файла в список обработки используйте кнопку **Добавить** и нажмите кнопку **Применить**.

Для удаления диска, каталога или файла из списка обработки выделите объект левой кнопкой мыши, нажмите **Удалить** и нажмите кнопку **Применить**.

Для редактирования диска, каталога или файла в списке обработки выделите объект левой кнопкой мыши, нажмите **Изменить** и нажмите кнопку **Применить**.

Примечание. Удалить системные диски из списка сканирования невозможно.

4.3.2. Вкладка Объекты сканирования

На вкладке **Объекты сканирования** (рис. 48) выполняется настройка отбора обрабатываемых **Антивирусным сканером** объектов по расширению файлов:

1) **Наборы файлов для сканирования** - позволяет задать расширения тех файлов, которые будут обрабатываться Сканером. Расширения отделяются друг от друга точкой. По умолчанию в строке задан типовой набор расширений файлов. Нажмите кнопку **По умолчанию**, чтобы восстановить начальный список расширений, в случае его изменений. Расширениями типового набора файлов являются:
   а) .COM.EXE.DLL.DRV.SYS.OV?.VXD.SCR.CPL.OCX.BPL.AX.PIF.DO? .XL?.HLP.RTF.WI?.WZ?.MSI.MSC.HT*.VB*.JS.JSE.ASP*.CGI.PHP* .?HTML.BAT.CMD.EML.NWS.MSG.XML.MSO.WPS.PPT.PUB.JPG .JPEG.ANI.INF.SWF.PDF.7Z.RAR.ZIP.GZ.BZ2.TAR.OSX.CAB;
   б) **Исключенные** - позволяет задать расширения файлов, которые необходимо исключить из обработки Сканером. Сюда можно включить некоторые маловероятные для инфицирования типы файлов.

Примечания:

1) знак вопроса «?» заменяет один любой символ при написании расширения.
2) знак звездочки «*» может быть трактован как «ни одного символа» или цепочка любых символов произвольной длины;
3) чтобы проверить все файлы, необходимо ввести в поле знак «*».

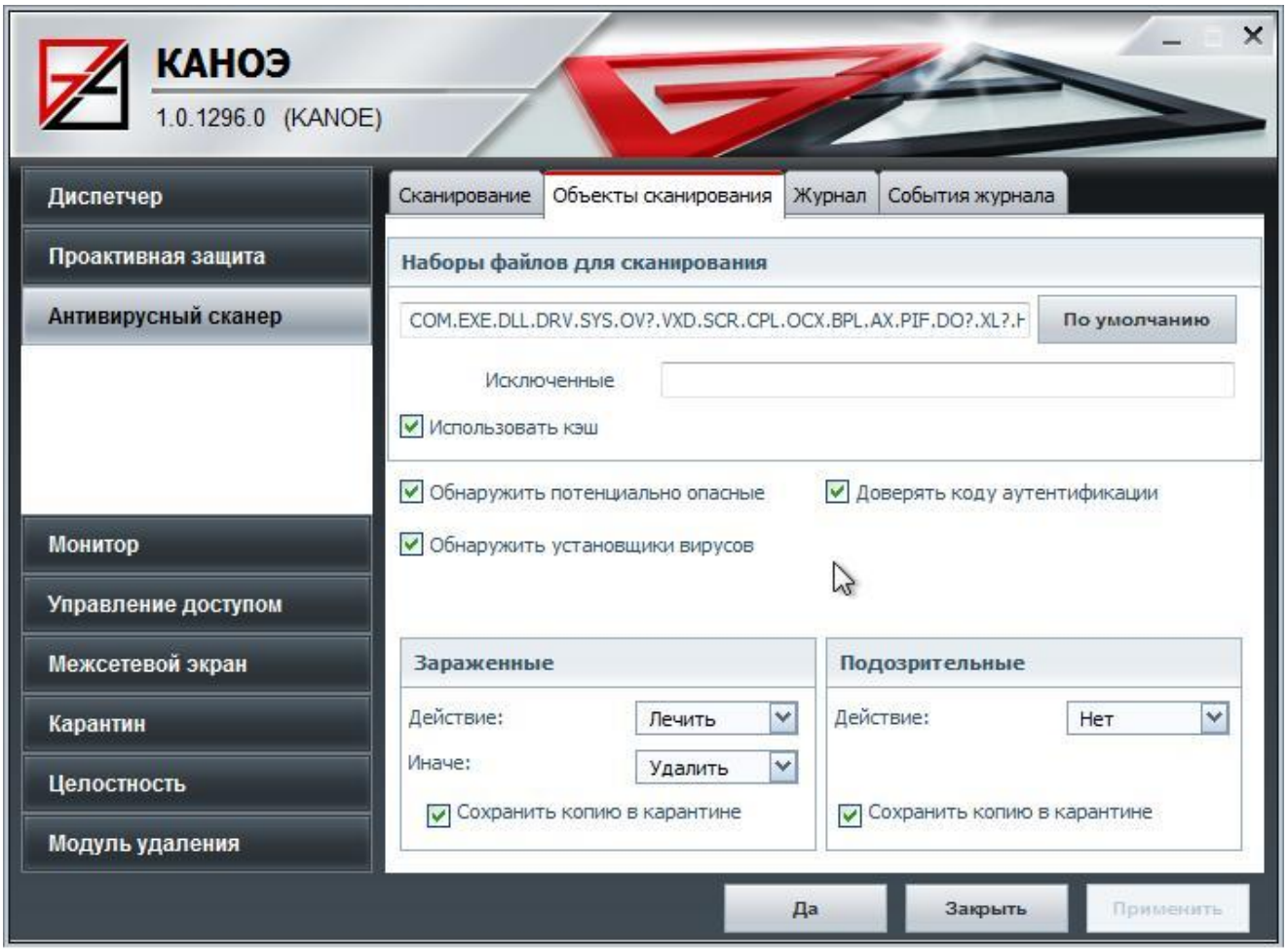

Рис. 48

2) **Использовать кэш** - разрешает использование особого алгоритма, позволяющего значительно уменьшить время обработки за счет сканирования только измененных со времени последнего сканирования файлов;
3) **Обнаружить потенциально опасные** - устанавливает дополнительный режим, при котором Сканер перестанет игнорировать потенциально опасные программы.
4) **Обнаружить установщики вирусов** - устанавливает режим, при котором Сканер детектирует инсталляторы вредоносных программ;
5) **Доверять коду аутентификации -** использование при проверке объектов технологию Microsoft Authenticode.

Далее настраиваются действия **Антивирусного сканера** при обнаружении инфицированных и подозрительных файлов:

Зараженные - позволяет выбрать в выпадающем списке действие над инфицированными файлами.

1) **Действие –** определяет действия для инфицированных объектов:
   а) **Лечить** - инфицированный файл лечится;
   б) **Удалить** - инфицированный файл удаляется из системы;

в) **Нет** - над объектом не производятся какие-либо действия;

2) **Иначе –** позволяет выбрать в выпадающем списке действие над инфицированными файлами, в случае невозможности выполнения первого действия:
   а) **Удалить** - инфицированный файл удаляется из системы;
   б) **Нет** - над объектом не производятся какие-либо действия;
3) **Сохранять копию в карантине** - включает сохранение копий инфицированных объектов в Карантин;

Подозрительные - позволяет выбрать в выпадающем списке действие над подозрительными объектами.

1) **Действие –** определяет действия для подозрительных объектов:
   а) **Удалить** - подозрительный объект удаляется;
   б) **Нет** - над объектом не производятся какие-либо действия;
2) **Сохранять копию в карантине** - включает сохранение копий подозрительных файлов в Карантин.

4.3.3. Вкладка Журнал

На вкладке **Журнал** (рис. 49) выполняется просмотр событий действий выполняемых **Антивирусным сканером**:

1) **дата начала журнала** – задает дату, начиная с которой будет отображаться журнал;
2) **дата окончания журнала** – задает дату, на которой будет заканчиваться отображение журнала.

Примечание. Дата отображается в формате дат, выбранном на компьютере (например, мм/дд/гггг).

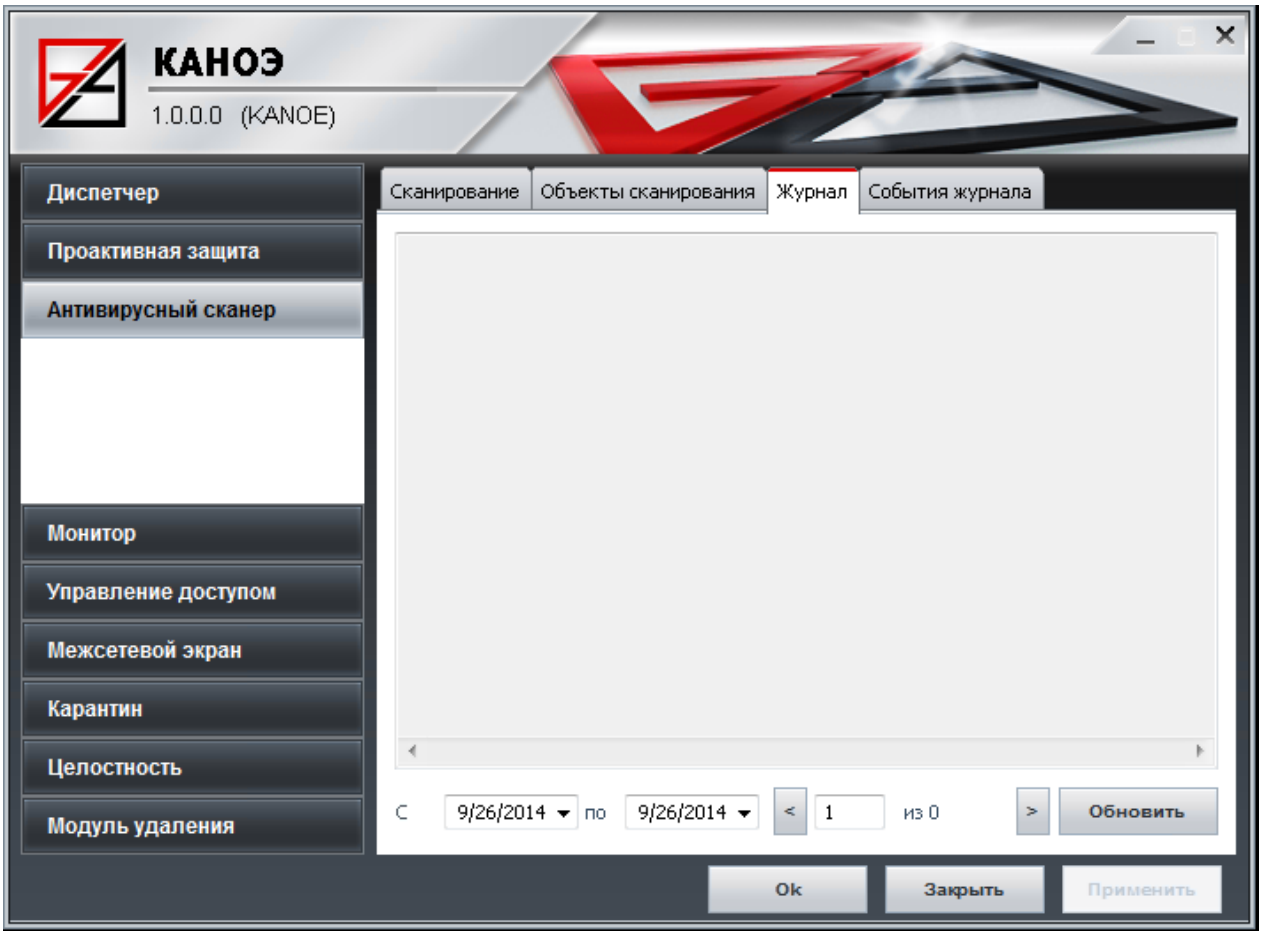

Рис. 49

Нажмите кнопку **Обновить**, чтобы отобразить журнал действий Антивирусного сканера в соответствии с указанными датами.

4.3.4. Вкладка События журнала

На вкладке **События журнала** (рис. 50) выполняется выбор событий сканирования и журналов, куда эти события будут записываться.

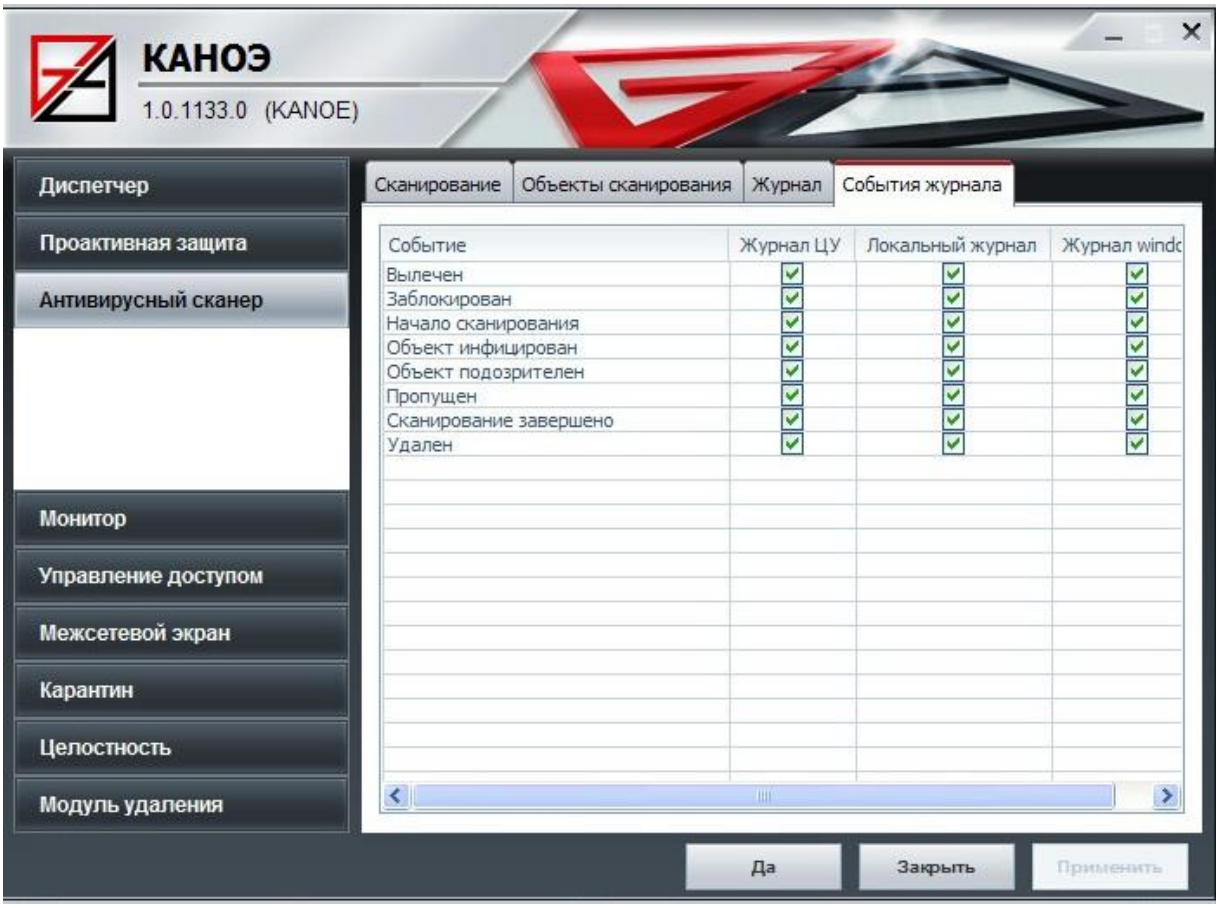

Рис. 50

Комплекс КАНОЭ предоставляет сбор сведений в следующие виды журналов:

1) **Журнал ЦУ** - события отправляются в модуль «Центр Управления». Журнал модуля «Центр Управления» (далее – журнал ЦУ);
2) **Локальный журнал** - представляет локальную базу событий, просмотр которого доступен через вкладку **Журнал**;
3) **Журнал Windows** - единый журнал событий операционной системы, хранящий события от всех приложений.

4.4. Раздел Монитор

4.4.1. Вкладка Настройки

Вкладка **Настройки** раздела **Монитор** (рис. 51) имеет следующие параметры и возможности:

1) включение\выключение **Монитора**;

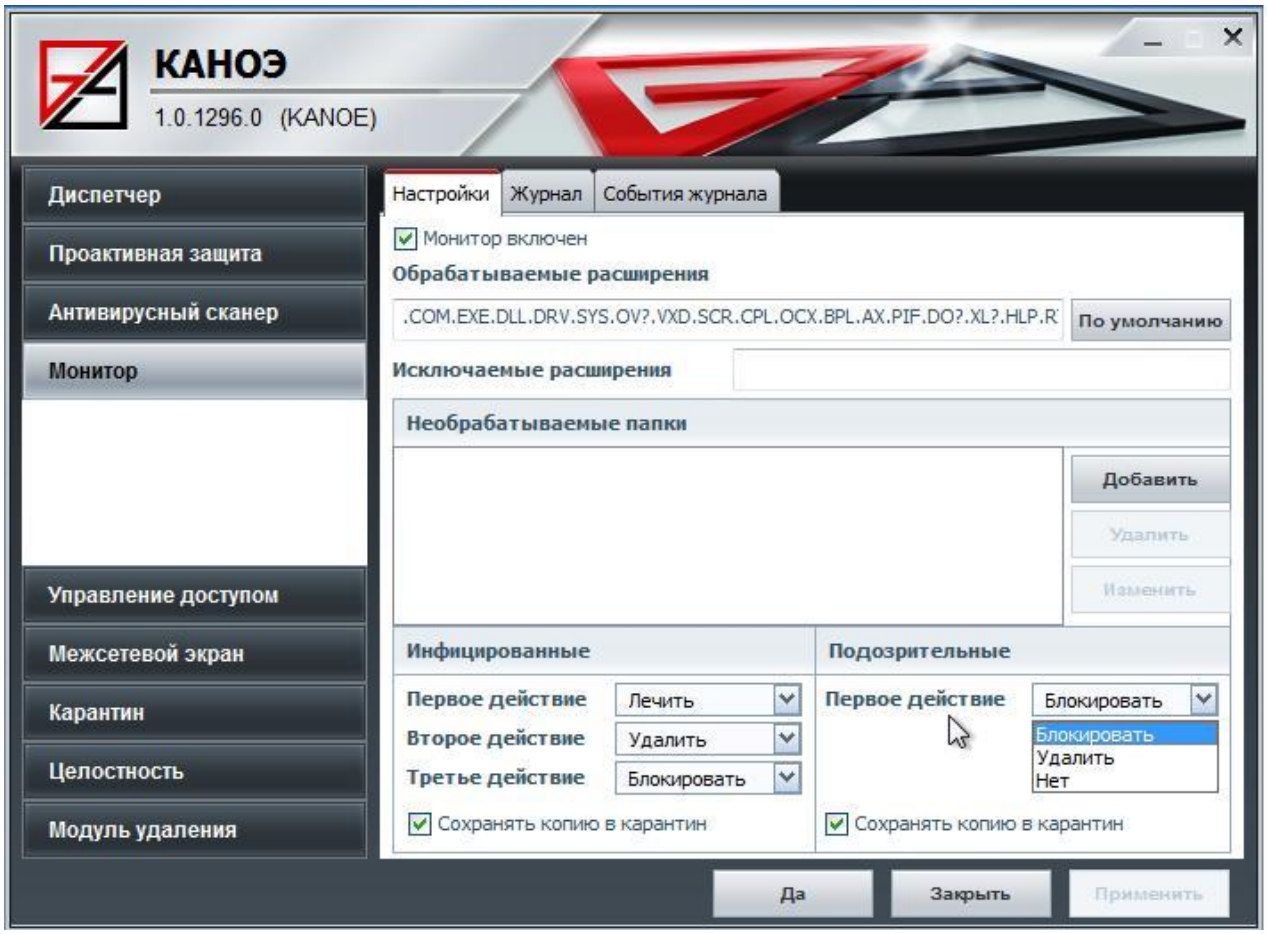

Рис. 51

2) обработка определенных типов файлов. Для этого в поле **Обрабатываемые расширения** вписываются типы файлов, которые будут обрабатываться в процессе работы **Монитора** (типовой набор файлов по умолчанию включает в себя следующие типы: .COM.EXE.DLL.DRV.SYS.OV?.VXD .SCR.CPL.OCX.BPL.AX.PIF.DO?.XL?.HLP.RTF.WI?.WZ?.MSI.MSC.HT* .VB*.JS.JSE.ASP*.CGI.PHP*.?HTML.BAT.CMD.EML.NWS.MSG.XML.MSO .WPS.PPT.PUB.JPG.JPEG.ANI.INF.SWF. PDF);
3) исключение из обработки определенных типов файлов вписываются в поле **Исключаемые расширения**;
4) исключение из обработки папок, находящиеся в списке **Необрабатываемые папки**. Блок **Необрабатываемые папки** содержит функционал по добавлению, удалению и изменению путей к папкам, которые будут исключены из обработки.
5) выбор действия над инфицированными и подозрительными объектами максимум в три этапа. Обработка происходит по следующему алгоритму: при невозможности выполнения первого действия, выполняется второе, при невозможности выполнения второго – третье. В блоке **Инфицированные** каждое из трех действий имеет четыре состояния:

а) блокировать;
б) лечить;
в) удалить;
г) нет;

В блоке **Подозрительные** действие имеет три состояния:

а) блокировать;
б) удалить;
в) нет;

6) включение/выключение сохранения копии объекта в карантин находятся в блоках **Инфицированные** и **Подозрительные**.

4.4.2. Вкладка Журнал

Вкладка **Журнал** (рис. 52) служит для отображения событий, которые были сгенерированы модулем **Монитор** и записаны в локальный журнал:

1) **дата начала журнала** – задает дату, начиная с которой будет отображаться журнал;
2) **дата окончания журнала –** задает дату, на которой будет заканчиваться отображение журнала.

Примечание. Дата отображается в формате дат выбранном на компьютере (например, мм/дд/гггг).

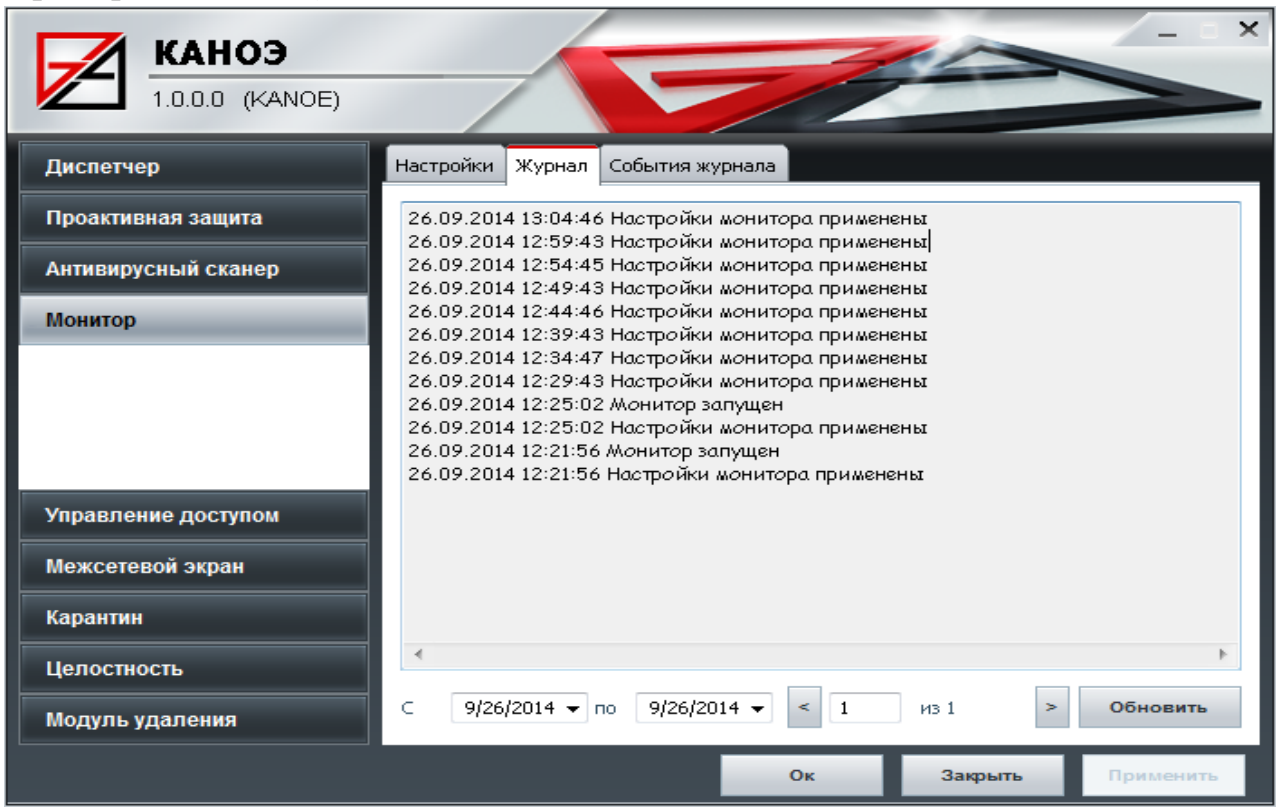

Рис. 52

Нажмите кнопку **Обновить,** чтобы отобразить журнал действий модуля Монитор в соответствии с указанными датами.

4.4.3. Вкладка События журнала

Вкладка **События журнала** (рис. 53) служит для настройки, в какой журнал будет записываться то или иное событие. Доступные журналы: **журнал ЦУ**, **локальный журнал** и **журнал Windows**.

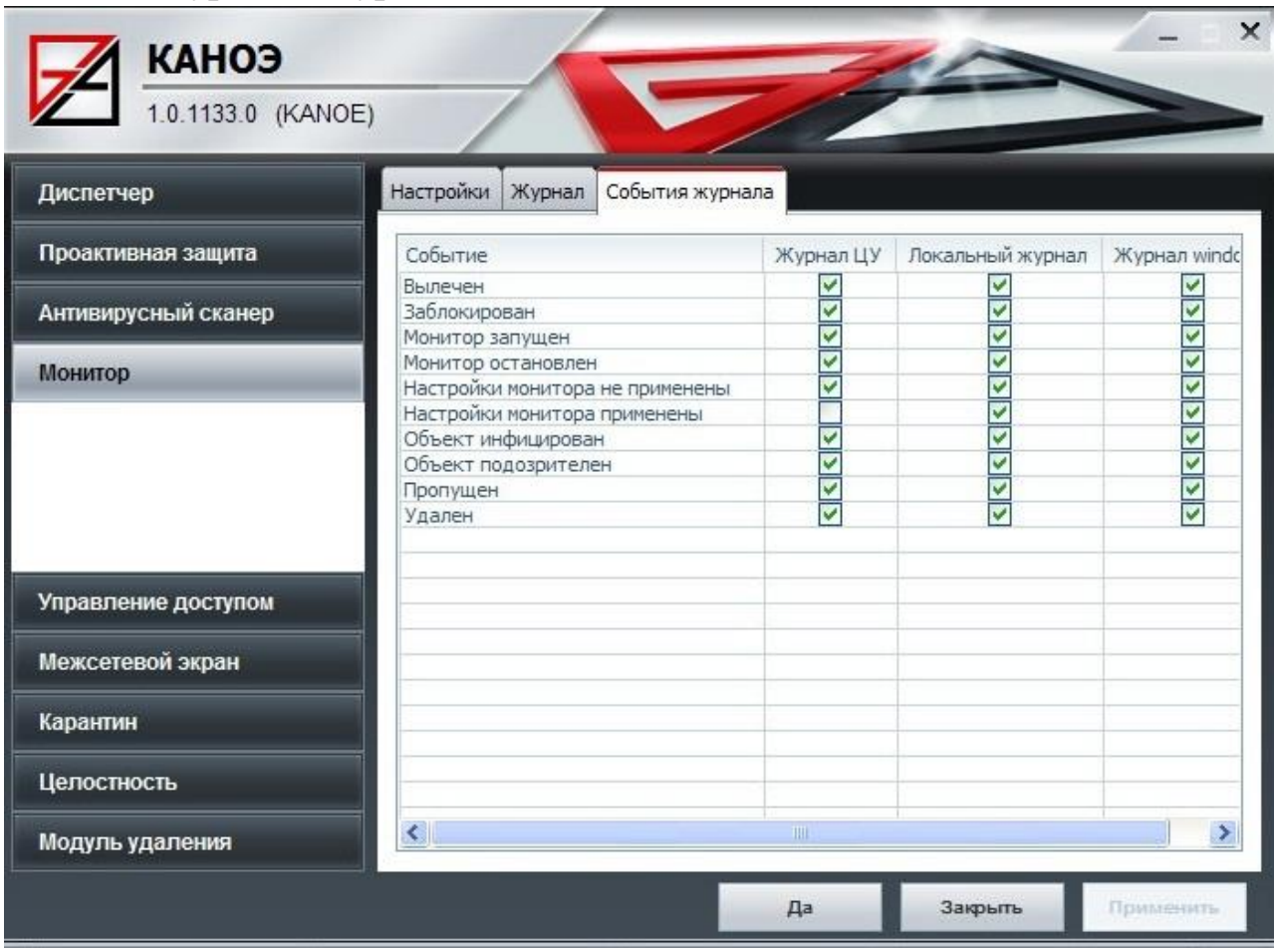

Рис. 53

4.5. Раздел Управление доступом

Раздел **Управление доступом** является компонентом комплекса и реализует контроль подключения устройств к компьютеру.

Для открытия модуля **Управление доступом** нажать кнопку **Управление доступом** на боковой панели.

4.5.1. Настройки модуля управления доступом

Настройки управления доступом позволяют выбрать устройства, классы устройства, определить действия, которые будет выполнять модуль при их подключении.

Для применения изменений настроек необходимо нажать кнопку **Применить**. Если хотите закрыть диалог и применить изменения нажмите кнопку **Ок**. Если хотите закрыть диалог и не применять настройки нажмите кнопку **Закрыть**.

4.5.2. Вкладка Классы устройств

На вкладке **Классы устройств** (рис. 54) выполняется настройка контроля доступом к определенным классам устройств. По умолчанию все классы пропускаются. Для того чтобы драйвер начал работать с классом устройств, его надо добавить в список классов.

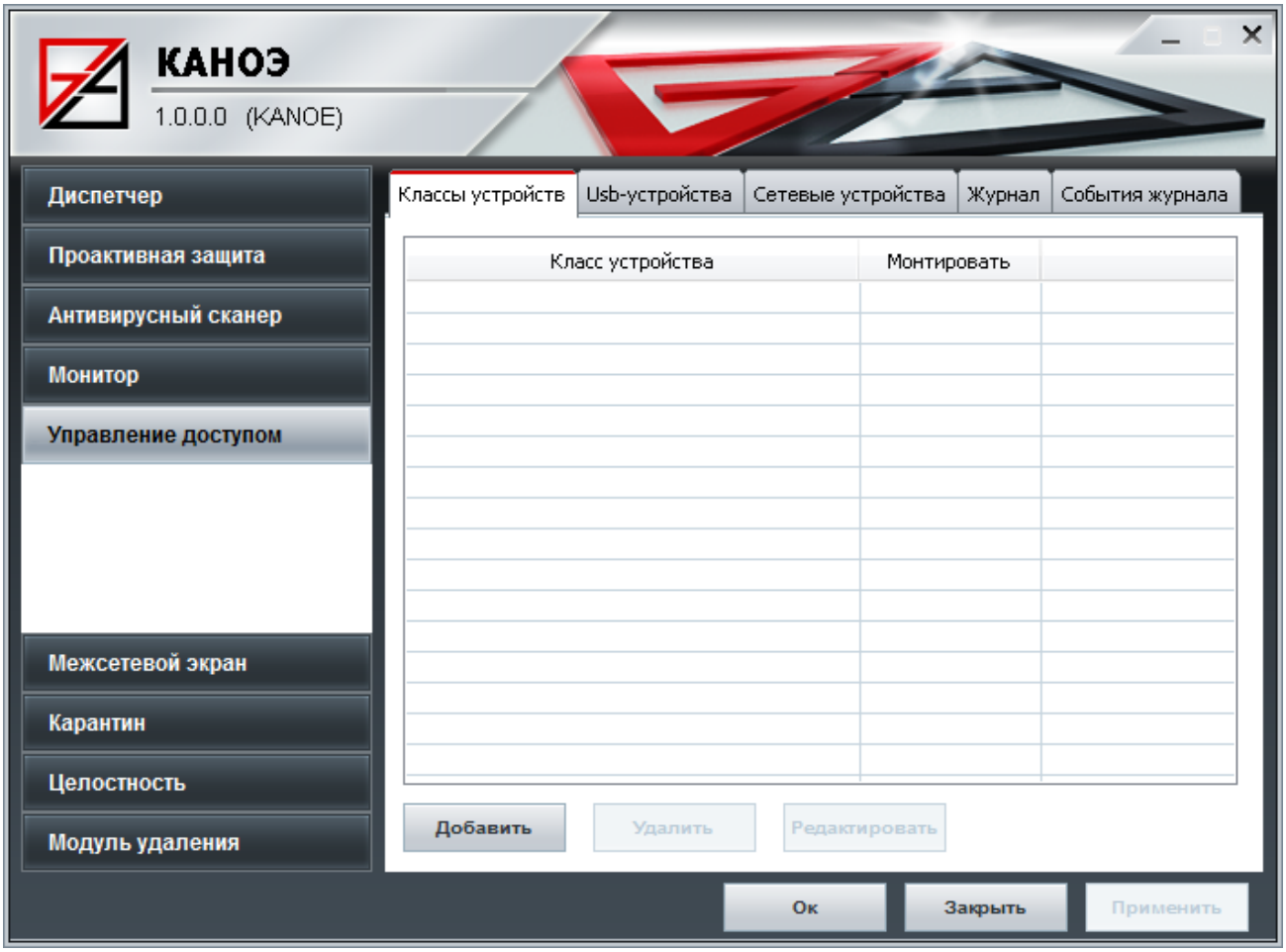

Рис. 54

Список классов состоит из двух частей:

1) **Класс устройства** – имя класса устройств, доступ к которому надо контролировать;

2) **Монтировать** – действие, которое необходимо производить с устройствами данного класса.

Для добавления нового класса в список:

1) нажмите кнопку **Добавить**;
2) в появившемся диалоге выберите класс и действие, которое необходимо производить над устройствами данного класса. Доступные действия над классами устройств:

   а) **Пропустить** – подключать устройства без ограничений;

   б) **Блокировать** – блокировать подключение устройства;

   в) **Блокировать запись** – подключить устройство, но блокировать запись на него;
3) после выбора в диалоге класса и действия над ним, нажмите кнопку **Ок**.

Нажмите кнопку **Отмена**, если вы передумали добавлять класс в список.

Для удаления класса из списка выделите класс в списке левой кнопкой мыши и нажмите кнопку **Удалить**.

Для редактирования уже добавленного класса в списке:

1) выделите класс в списке левой кнопкой мыши и нажмите кнопку **Редактировать**;
2) в появившемся диалоге выберите класс и действие, которое необходимо производить над устройствами данного класса;
3) после выбора в диалоге класса и действия над ним, нажмите кнопку **Ок**. Нажмите кнопку **Отмена**, если вы передумали редактировать класс в списке.

Примечание. После изменения настроек в списке классов устройств необходима перезагрузка компьютера.

4.5.3. Вкладка Usb-устройства

На вкладке **Usb-устройств** (рис. 55) выполняется настройка контроля доступом к usb-устройствам. Настройки разбиты на две части:

1) контроль доступом определенных usb-устройств;
2) контроль доступом над классами usb-устройств.

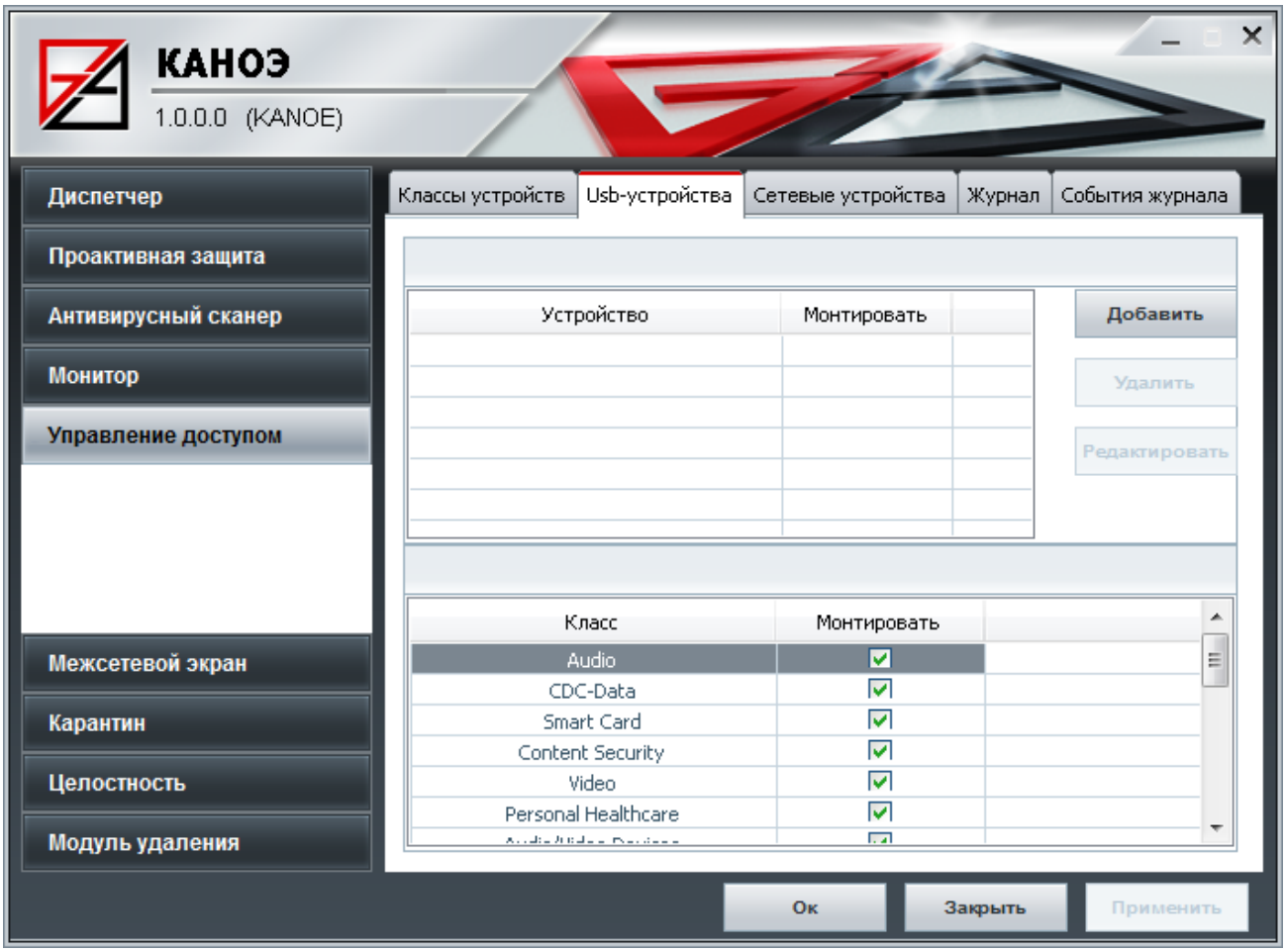

Рис. 55

Приоритетными являются настройки контроля доступом определенных usb-устройств, если подключаемого устройства нет в этих настройках, то применяются настройки контроля доступом над классами usb-устройств.

Чтобы устройство/класс было смонтировано необходимо, поставить галочку напротив соответствующего устройства/класса, иначе оно будет заблокировано.

Для добавления определенного устройства:

1) нажмите кнопку **Добавить**;
2) в появившемся диалоге, выберите устройство и действия из выпадающих списков. Возможные действия над устройствами и классами usb-устройств:
   а) **Блокировать** – запретить подключение устройства;
   б) **Блокировать запись** – запретить запись на устройства;
   в) **Пропустить** – разрешить подключение устройства.
3) после выбора в диалоге устройства, нажмите кнопку **Ок**. Нажмите кнопку **Отмена**, если вы передумали добавлять устройство.

Примечание. По умолчанию все USB-накопители, имеющие в ОС символическое имя, при монтировании файловой системы блокируются на запись. Чтобы разрешить данному устройству операцию записи, необходимо добавить его с помощью действия **Пропустить**.

4.5.4. Вкладка Сетевые устройства

На вкладке **Сетевые устройства** возможно настроить контроль используемых сетевых устройств (рис. 56). Вкладка **Сетевые устройства** состоит из двух частей:

1) **Сетевое устройство** – сетевое устройство, доступ к которому контролируется;
2) **Монтировать** – действие, которое необходимо производить с сетевым устройством.

При выборе действия с сетевым устройством **Монтировать**, необходимо выбрать действие **Контролировать сетевые устройства**.

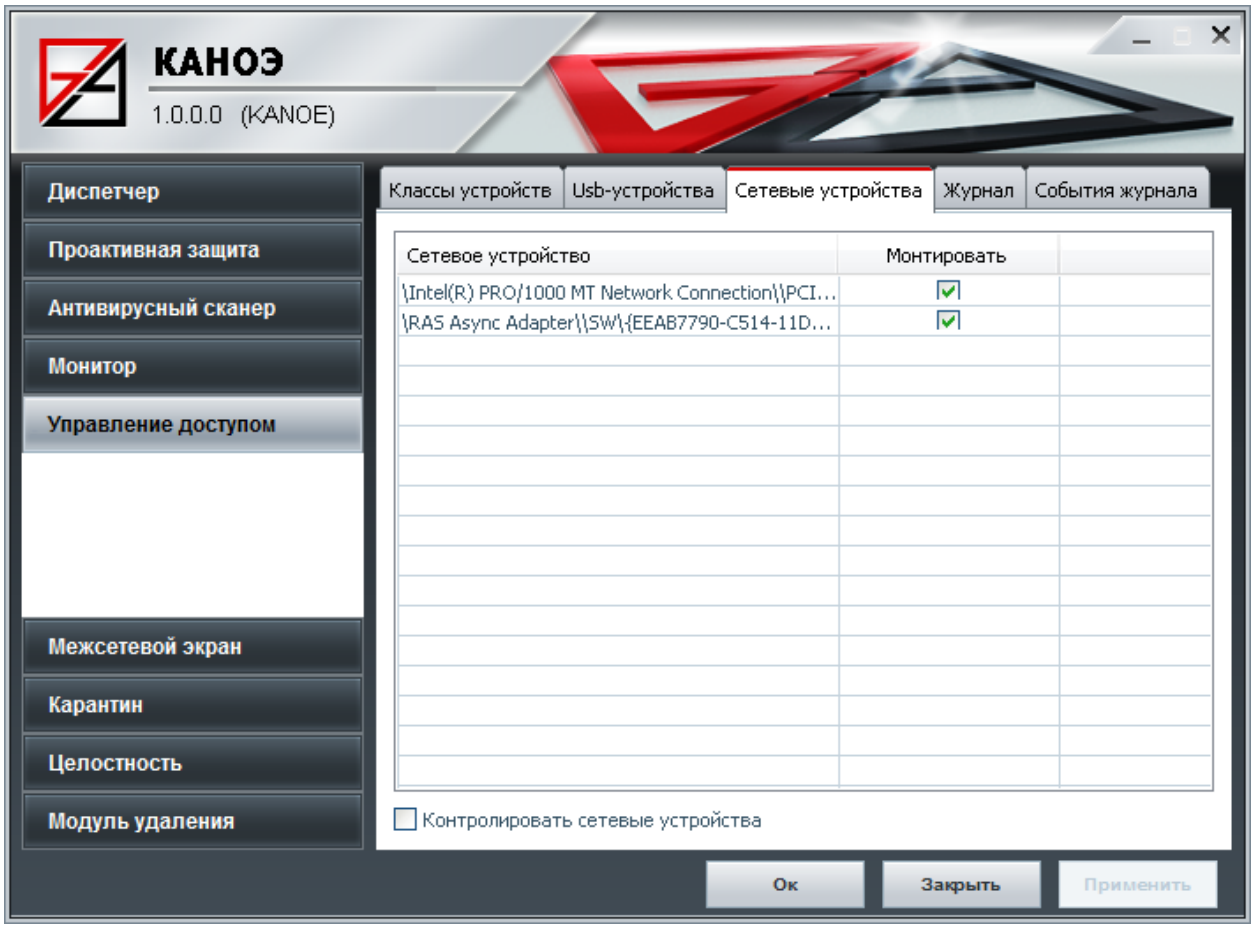

Рис. 56

4.5.5. Вкладка Журнал

На вкладке **Журнал** (рис. 57) выполняется просмотр действий, выполняемых модулем управления доступом, действий:

1) **дата начала журнала** – задает дату, начиная с которой будет отображаться журнал;
2) **дата окончания журнала** – задает дату, на которой будет заканчиваться отображение журнала.

Примечание. Дата отображается в формате дат, выбранном на компьютере (например, мм/дд/гггг).

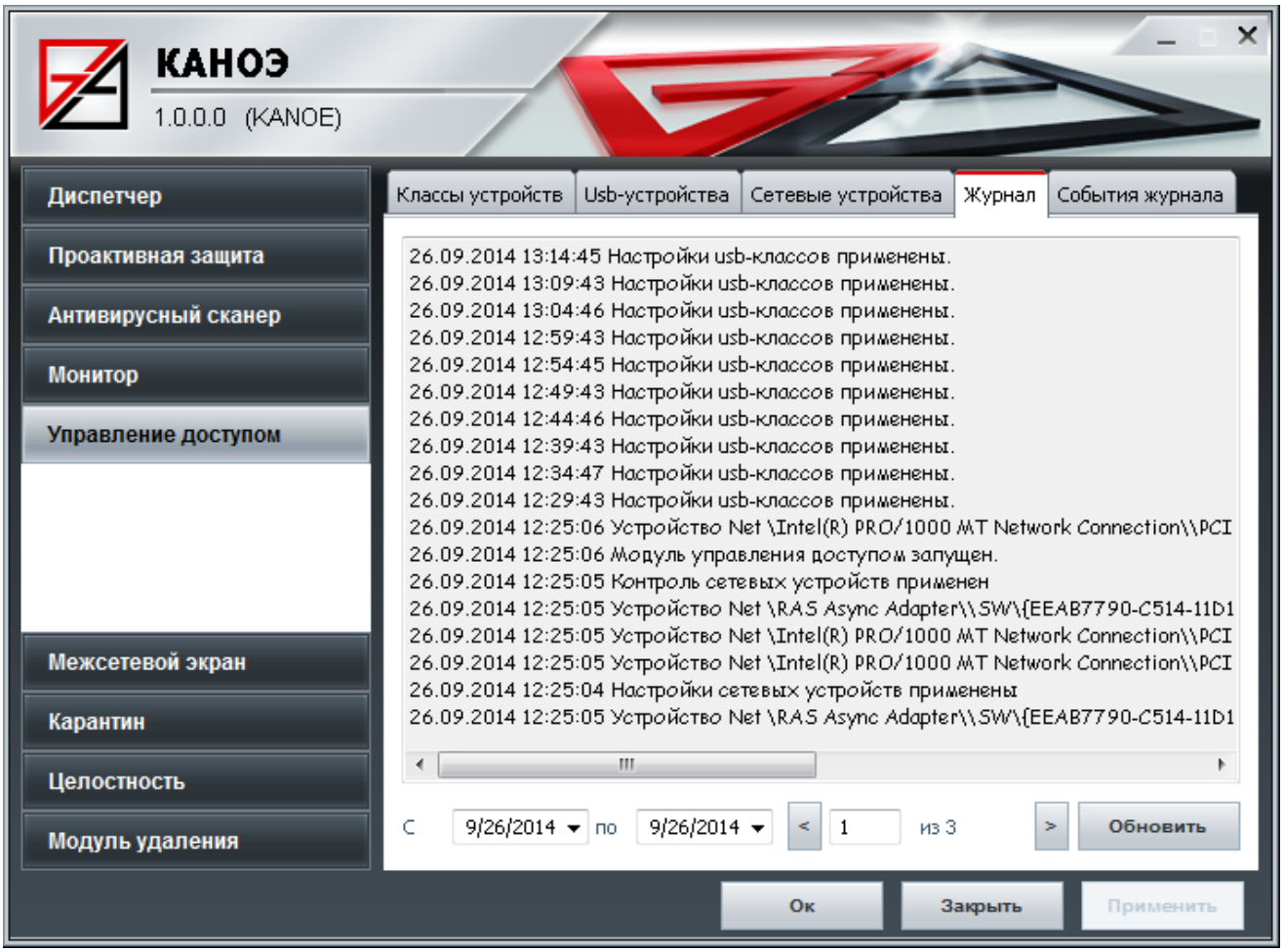

Рис. 57

Нажмите кнопку **Обновить,** чтобы отобразить журнал действий модуля управления доступом в соответствии с указанными датами.

Для копирования из **Журнала** интересующих данных:

1) выделите мышкой интересующие данные;
2) после нажатия правой кнопки мыши, выберите в контекстном меню действие **Копировать**.

4.5.6. Вкладка События журнала

На вкладке **События журнала** (рис. 58) выполняется выбор событий управления доступом и журналов, куда эти события будут записываться.

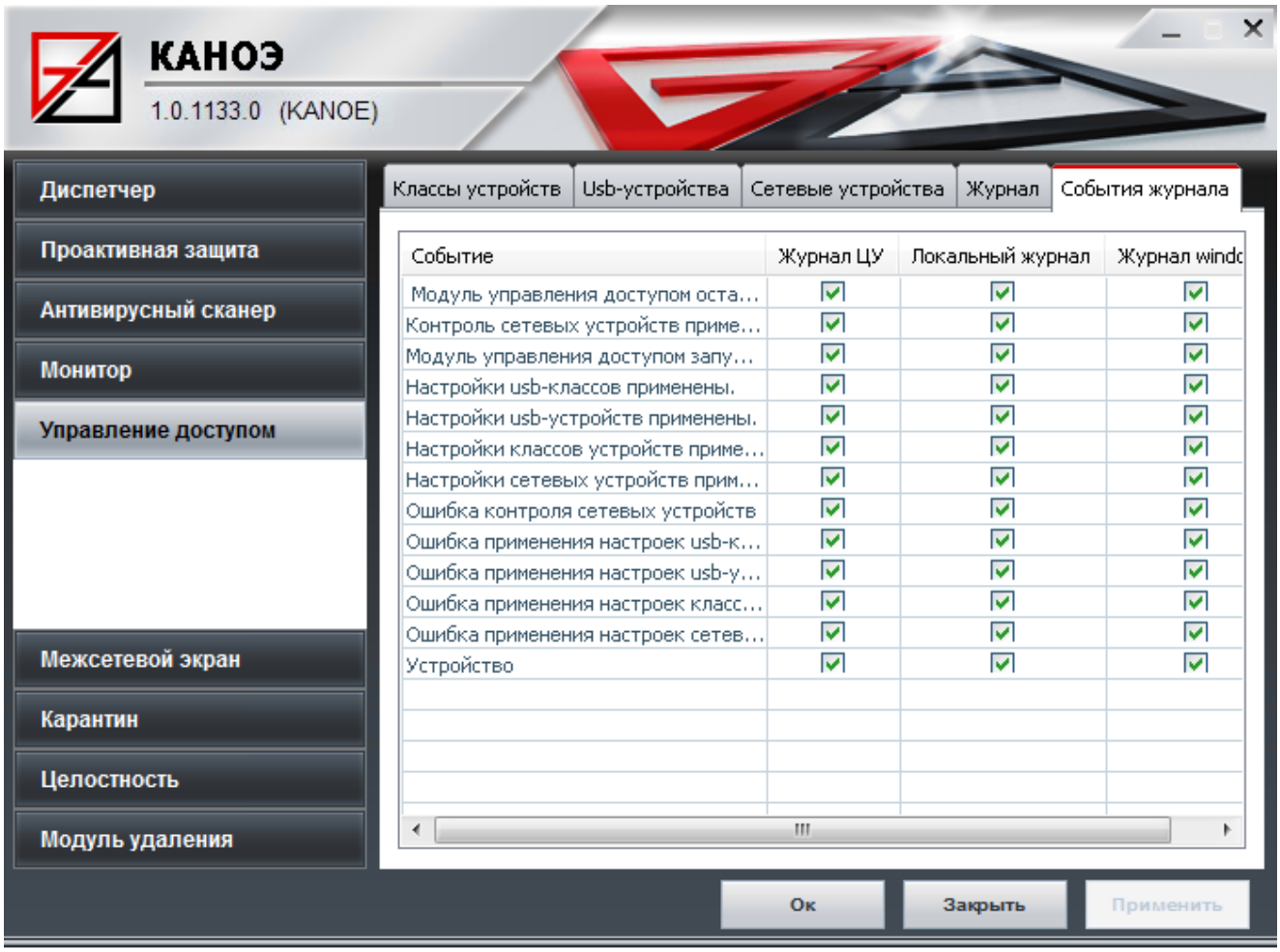

Рис. 58

4.6. Раздел Межсетевой экран

Раздел **Межсетевой экран** (рис. 59) имеет следующий функционал:

1) включение\выключение межсетевого экрана;
2) выбор типа сети, в которой находиться компьютер: открытая, частная доменная или закрытая. В зависимости от этого устанавливаются правила, чтобы обеспечить работоспособность сетевых компонентов компьютера в соответствии с выбранным типом сети;

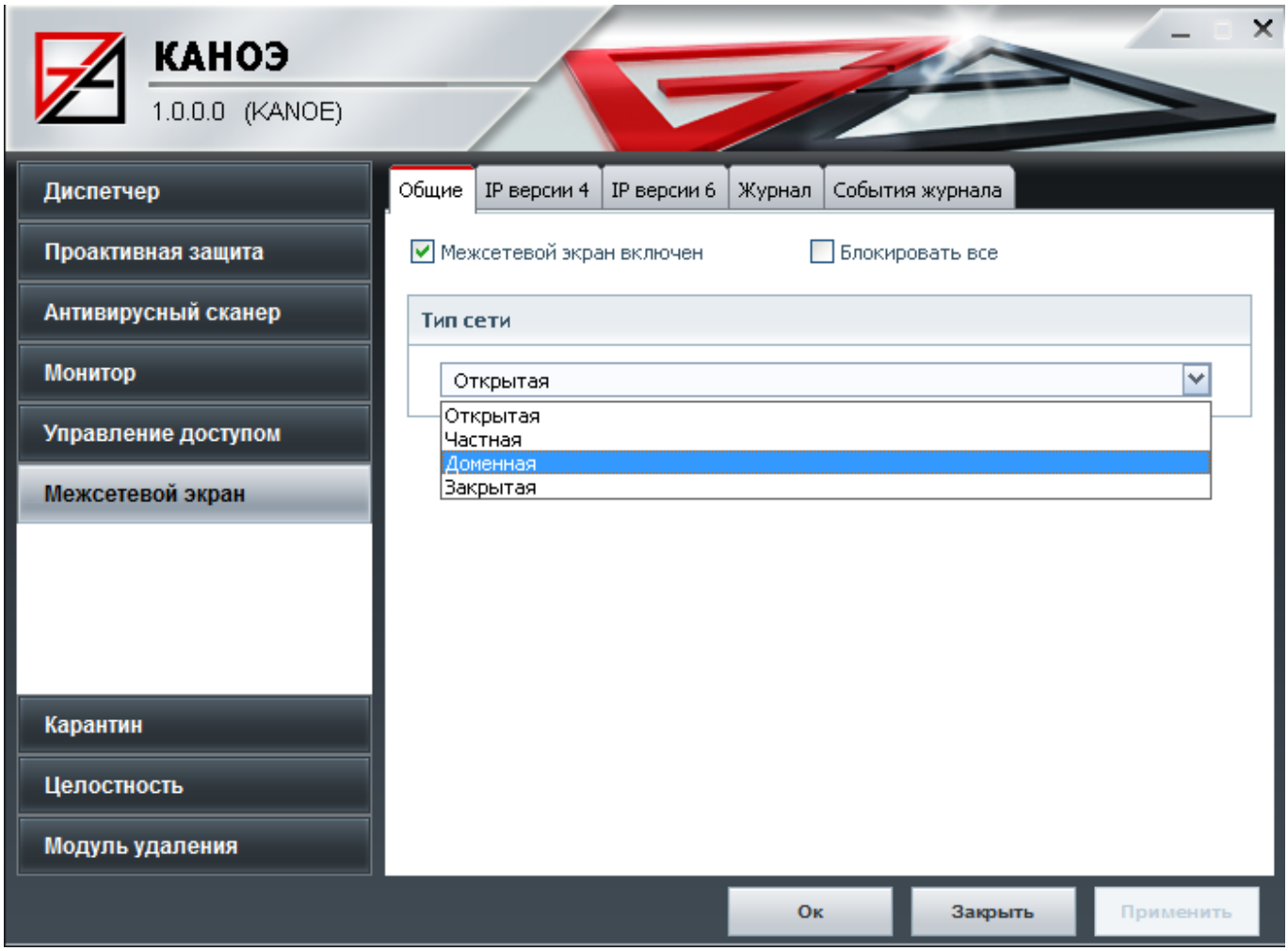

Рис. 59

3) добавление, изменение и удаление правил отдельно для протоколов Ip версии 4 и Ip версии 6, нажав соответствующую вкладку. Так же присутствует возможность делать правило активным или нет, и изменять порядок проверки пакета по правилам. Проверка по правилам осуществляется «сверху вниз» до первого правила, под которое попал сетевой пакет. Если пакет не попал ни под одно правило, то применяется действие по умолчанию **Отклонить**.

4.6.1. Вкладка Ip версии 4

Вкладка **Ip версии 4** (рис. 60) служит для отображения правил фильтрации пакетов IP версии 4 и их редактирования: добавления, изменения и удаления.

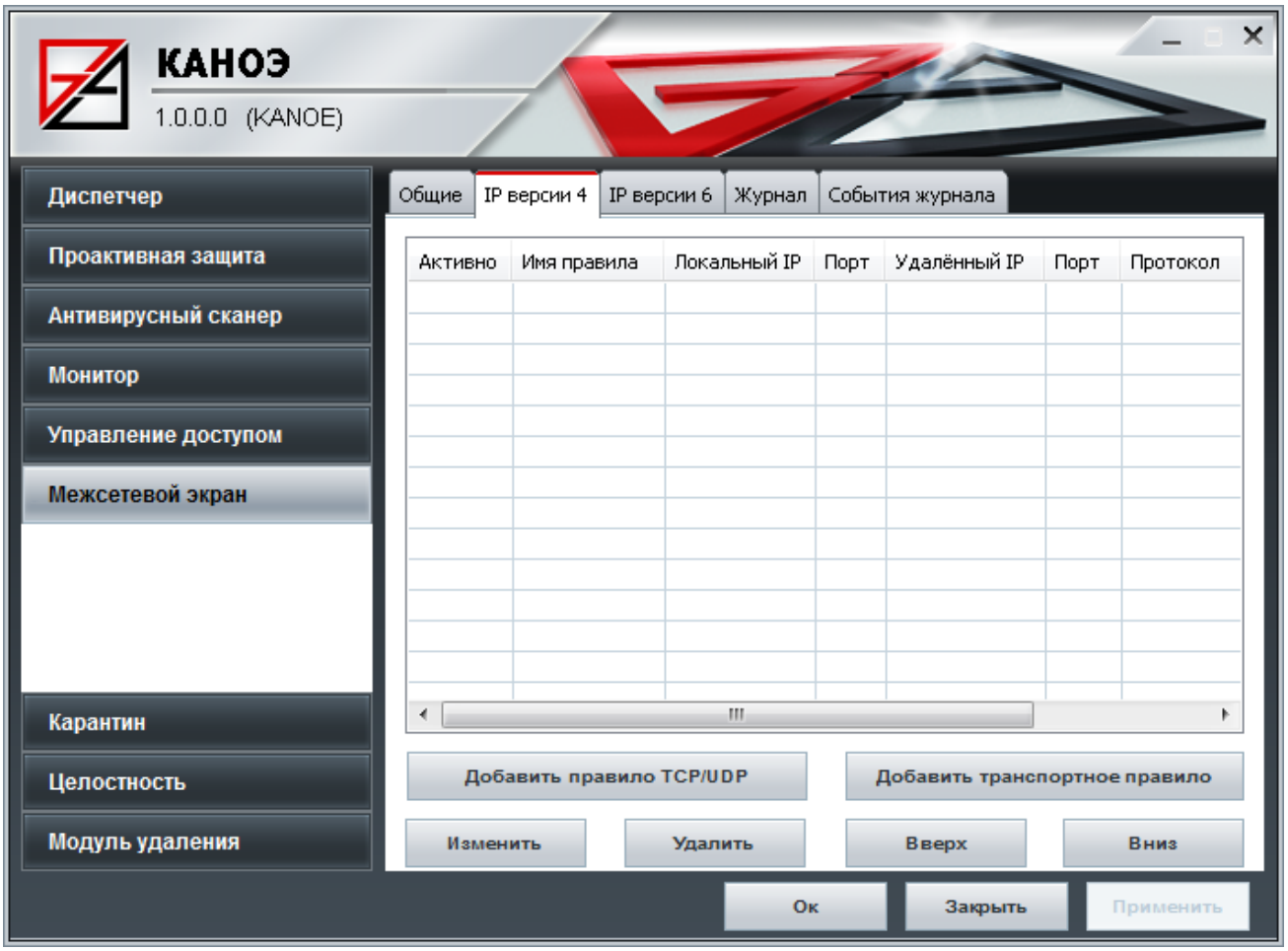

Рис. 60

Для добавления правил используются две кнопки: **Добавить правило TCP/UDP** (рис. 61) и **Добавить транспортное правило** (рис. 62). Разница лишь в том, что для TCP/UDP необходимо задать порт, а для остальных транспортных протоколов это не обязательно.

При добавлении правила необходимо указать имя правила, локальный и удаленный IP адрес и порт, протокол передачи данных, и действие над пакетами, которые попадут под это правило. Возможны следующие действия над пакетами:

- **Запретить все**;
- **Позволить отправить**;
- **Позволить отправить и получить**;
- **Позволить получить**.

IP адреса задаются четырьмя десятичными числами разделенными точками. Диапазон значений каждой составляющей от 0 до 255. Поддерживается несколько способов задания адресов ip v4. Можно указать определенный адрес (например: 10.144.90.11). Если значение в каком-нибудь байте охватывает весь диапазон (т.е. от 0 до 255), то можно вместо промежутка 0-255 написать *. Таким образом, задания адресов «10.144.0-255.11-66» и «10.144.*.11-66» идентичны. Если каждый из

четырех байтов охватывает весь диапазон, то вместо адреса «*.*.*.*» можно задать просто «*». Это означает, что под правило попадает весь диапазон ip адресов.

Порт задается в виде десятичного числа. Диапазон значений от 0 до 65535. Можно указать диапазон портов через тире (например: 25-80). Можно указать звездочку (*) – это будет означать, что правило распространяется на весь диапазон портов. Если несколько определенных, то разделитель «,» (запятая).

При создании TCP/UDP правила необходимо выбрать протокол из предложенного списка: **TCP** или **UDP**.

При создании транспортного правила протокол задается путем выбора из списка, предложенных протоколов. Существует возможность дополнительно указать протоколы, путем ввода их числового значения в поле **Другие протоколы**. Если несколько протоколов, то разделитель «,» (запятой).

Если при решении об отправке или отклонении сетевого пакета было принято правило с включенным аудитом, то информация об этом пакете сохраняется в **Журнал**.

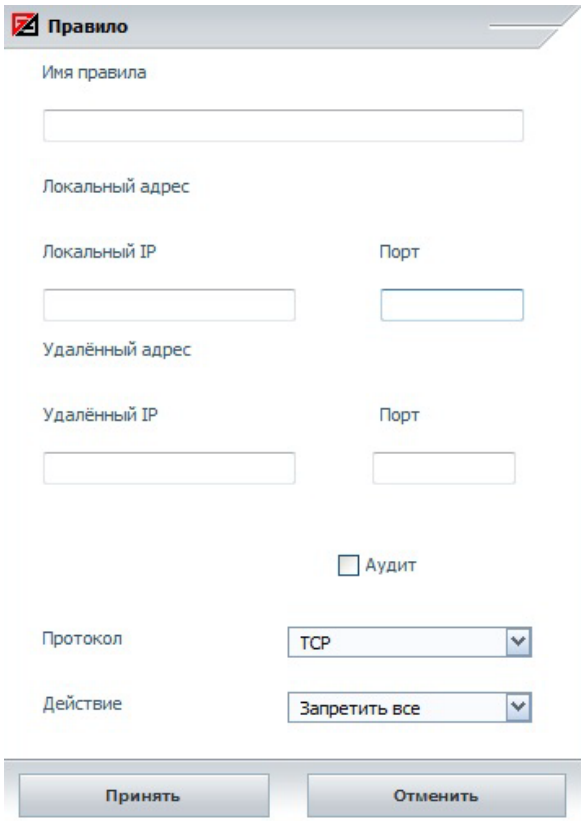

Рис. 61

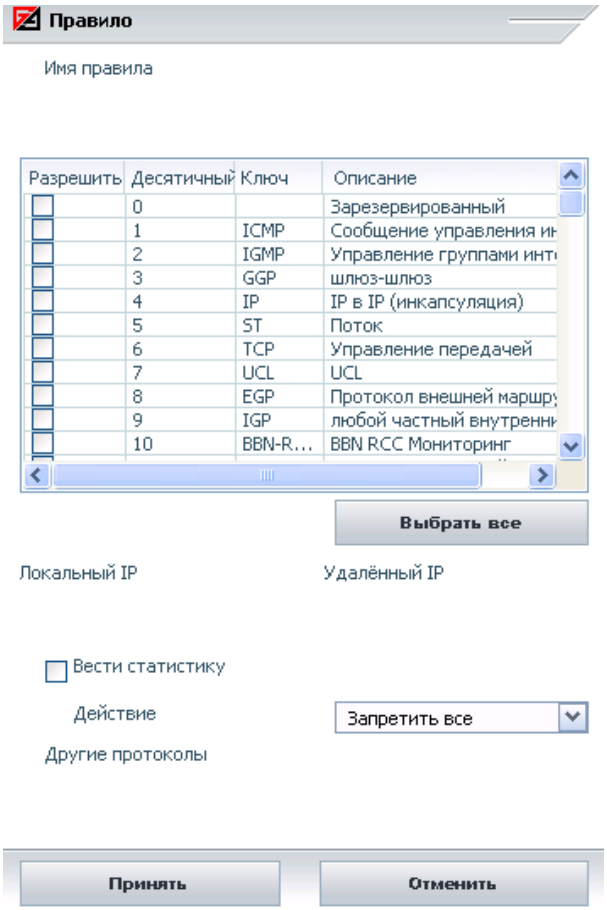

Рис. 62

4.6.2. Вкладка Ip версии 6

Вкладка **Ip версии 6** (рис. 63) служит для отображения правил фильтрации пакетов IP версии 6 и их редактирования: добавления, изменения и удаления. Вкладка **Ip версии 6** аналогична вкладке **Ip версии 4** за исключения формата задания IP адреса.

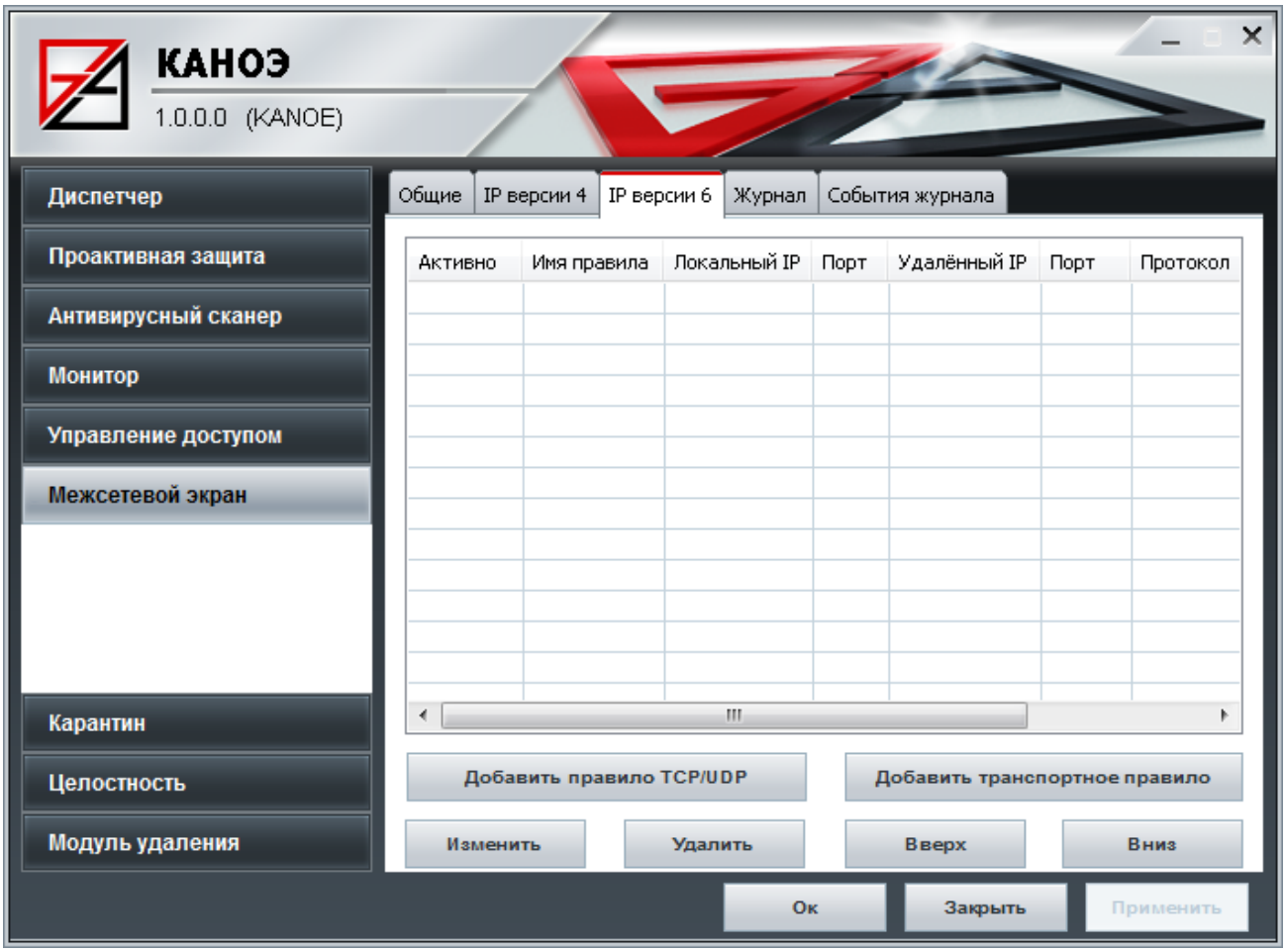

Рис. 63

IP адреса задаются восемью шестнадцатеричными числами, разделенными двоеточием. Диапазон каждой составляющей от 0 до FFFF. Для адресов ip v6, так же как и для ip v4, поддерживается формат задания в виде диапазона в любой из составляющей адреса. Вместо диапазона от 0 до FFFF то можно указать просто звездочку (*). Если каждая составляющая равна *, то вместо адреса «*:*:*:*:*:*:*:*» можно задать «*».

Также для ip v6 поддерживается общий формат задания адресов.

1) если элемент адреса начинается с нуля, но при этом не равен нулю, то нули вначале можно опустить;
   Пример: адрес FF43:0000:0000:0000:0462:B1A2:0079:1235 идентичен FF43:0000:0000:0000:462:B1A2:79:1235;
2) если в адресе встречается несколько подряд идущих нулевых элементов, то их можно опустить, заменив двоеточием;
   Пример: адрес FF43:0000:0000:0000:462:B1A2:79:1235 идентичен FF43::462:B1A2:79:1235.

Примечание. Данный алгоритм действий можно сделать только для одной группы подряд идущих нулевых элементов. То есть адрес

FF43:0000:0000:0000:462:0000:0000:1235 нельзя записать в виде FF43::462::1235. Можно либо так FF43::462:0000:0000:1235, либо FF43:0000:0000:0000:462::1235.

4.6.3. Вкладка Журнал

Вкладка **Журнал** служит (рис. 64) для отображения событий, которые были сгенерированы модулем **Межсетевой экран** и записаны в **Локальный журнал**:

1) **дата начала журнала** – задает дату, начиная с которой будет отображаться журнал;
2) **дата окончания журнала –** задает дату, на которой будет заканчиваться отображение журнала.

Примечание. Дата отображается в формате дат, выбранном на компьютере (например, мм/дд/гггг).

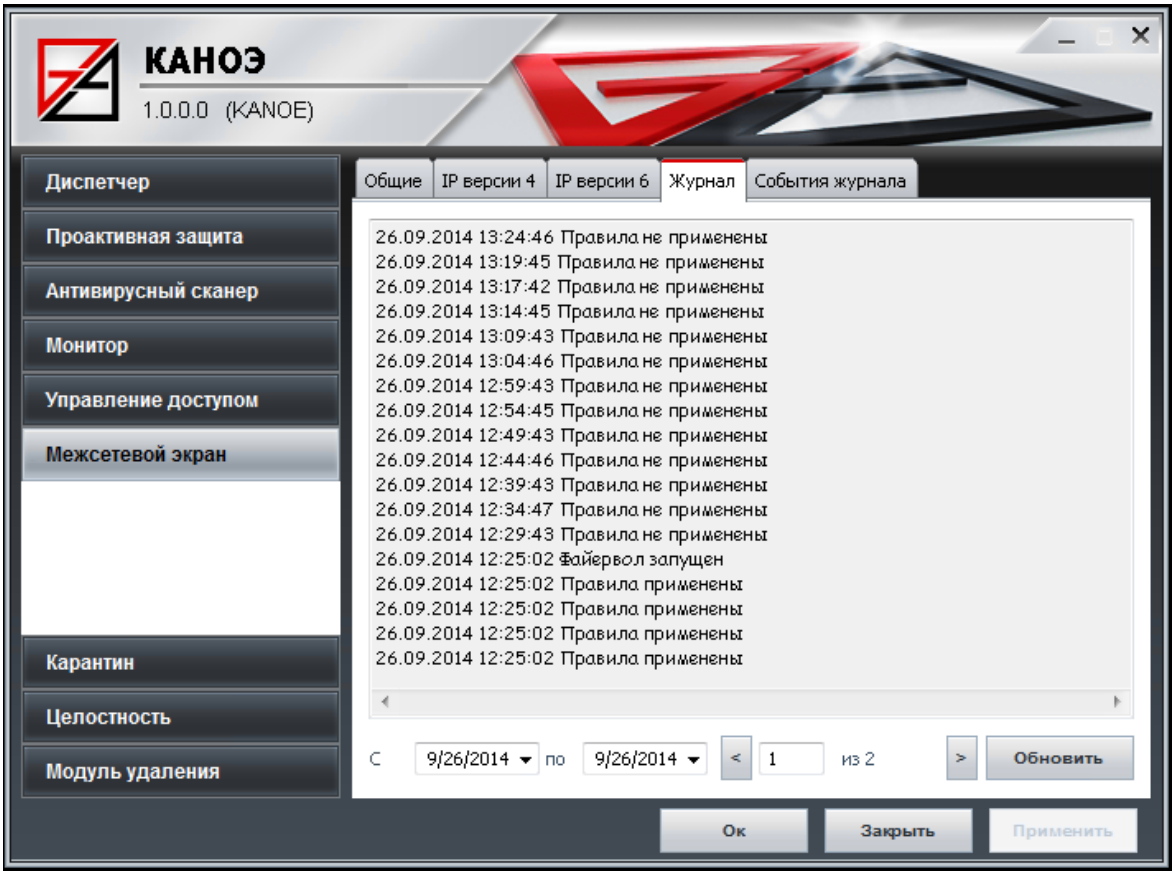

Рис. 64

Нажмите кнопку **Обновить,** чтобы отобразить журнал действий модуля **Межсетевой экран** в соответствии с указанными датами.

4.6.4. Вкладка События журнала

Вкладка **События журнала** (рис. 65) служит для настройки в какой журнал будет записываться то или иное событие. Доступные журналы: **журнал ЦУ**, **локальный журнал** и **журнал Windows**.

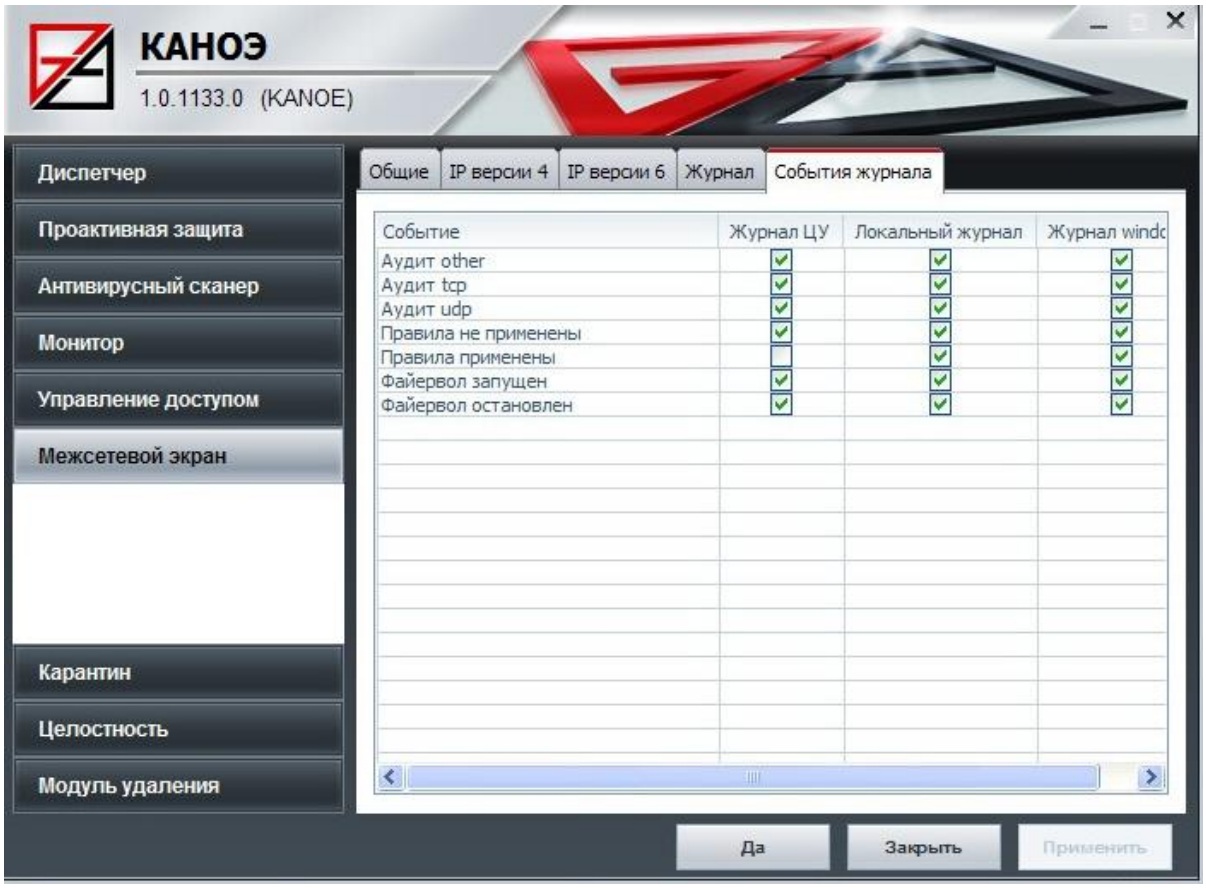

Рис. 65

4.7. Раздел Карантин

Раздел **Карантин** предназначен для хранения инфицированных объектов, обнаруженных антивирусной проверкой.

4.7.1. Вкладка Информация об объектах

Вкладка **Информация об объектах** (рис. 66) предоставляет список объектов, попавших в карантин при антивирусной проверке. Доступны возможности удаления и восстановления объектов с использованием кнопок **Восстановить** и **Удалить** соответственно.

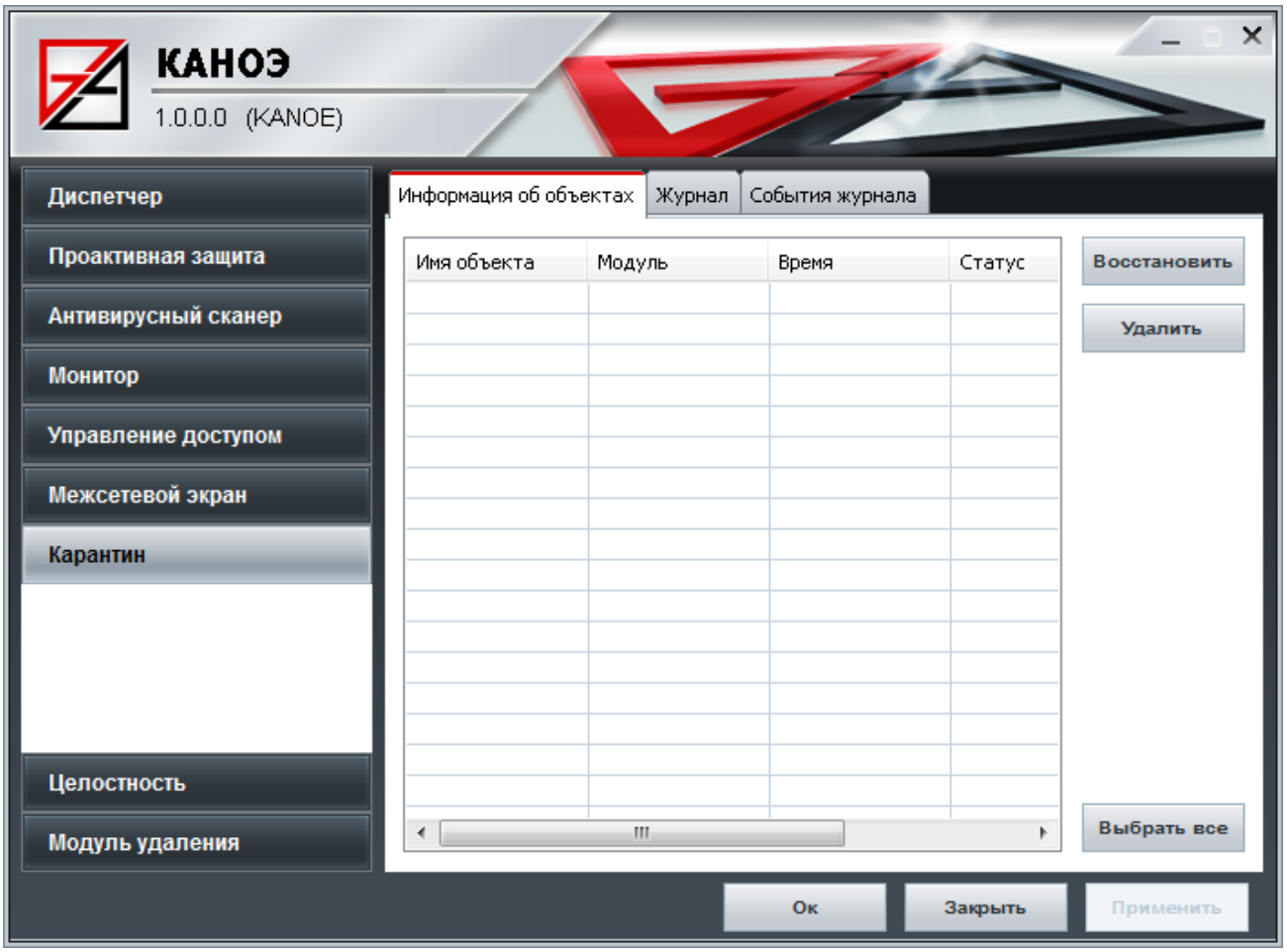

Рис. 66

4.7.2. Вкладка Журнал

Вкладка **Журнал** (рис. 67) служит для отображения событий, которые были сгенерированы **Модулем контроля данных** и записаны в **Локальный журнал**:

1) **дата начала журнала** – задает дату, начиная с которой будет отображаться журнал;
2) **дата окончания журнала –** задает дату, на которой будет заканчиваться отображение журнала.

Примечание. Дата отображается в формате дат, выбранном на компьютере (например, мм/дд/гггг).

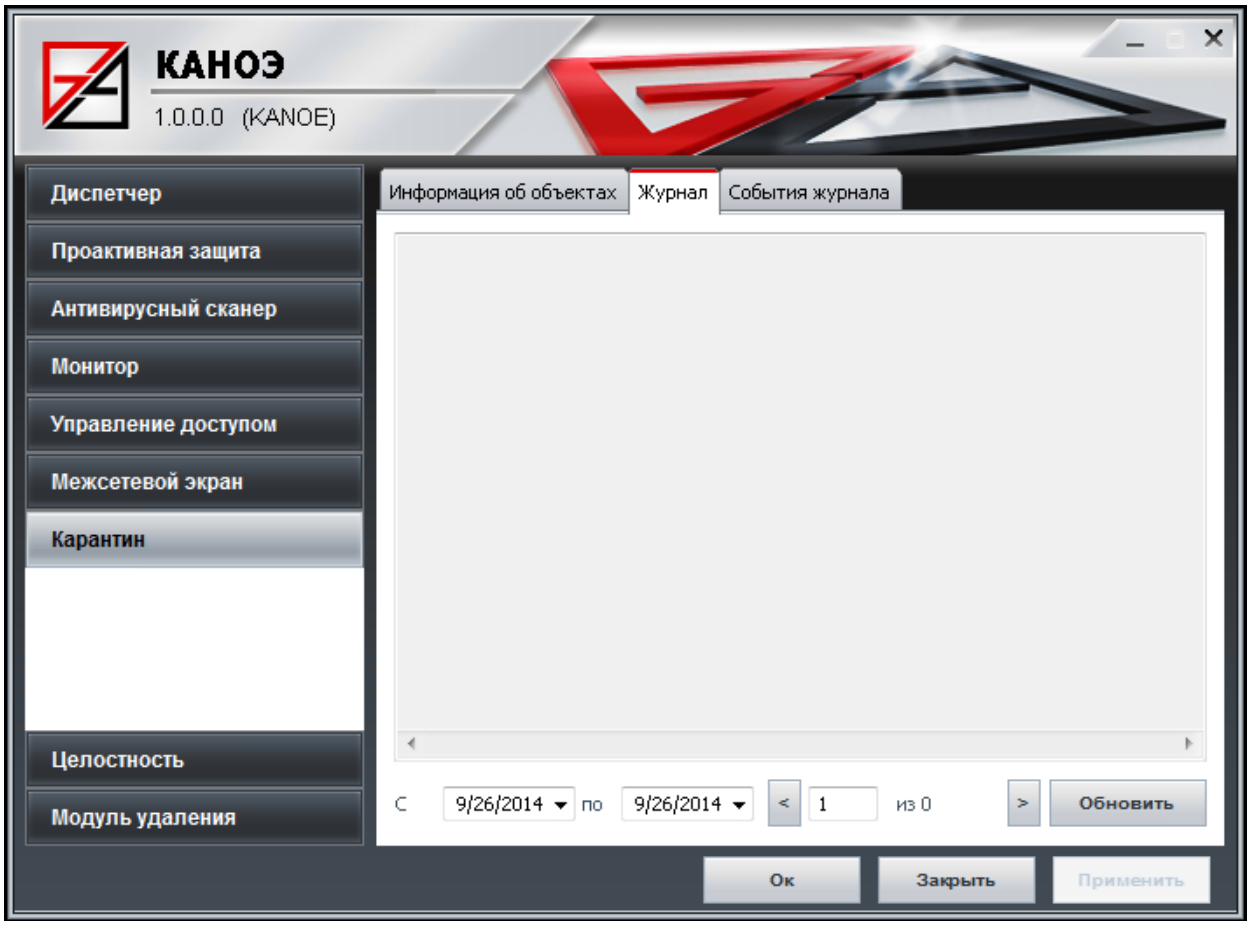

Рис. 67

Нажмите кнопку **Обновить,** чтобы отобразить журнал действий **Модуля контроля данных** в соответствии с указанными датами.

4.7.3. Вкладка События журнала

Вкладка **События журнала** (рис. 68) служит для настройки, в какой журнал будет записываться то или иное событие. Доступные журналы: **журнал ЦУ**, **локальный журнал** и **журнал Windows**.

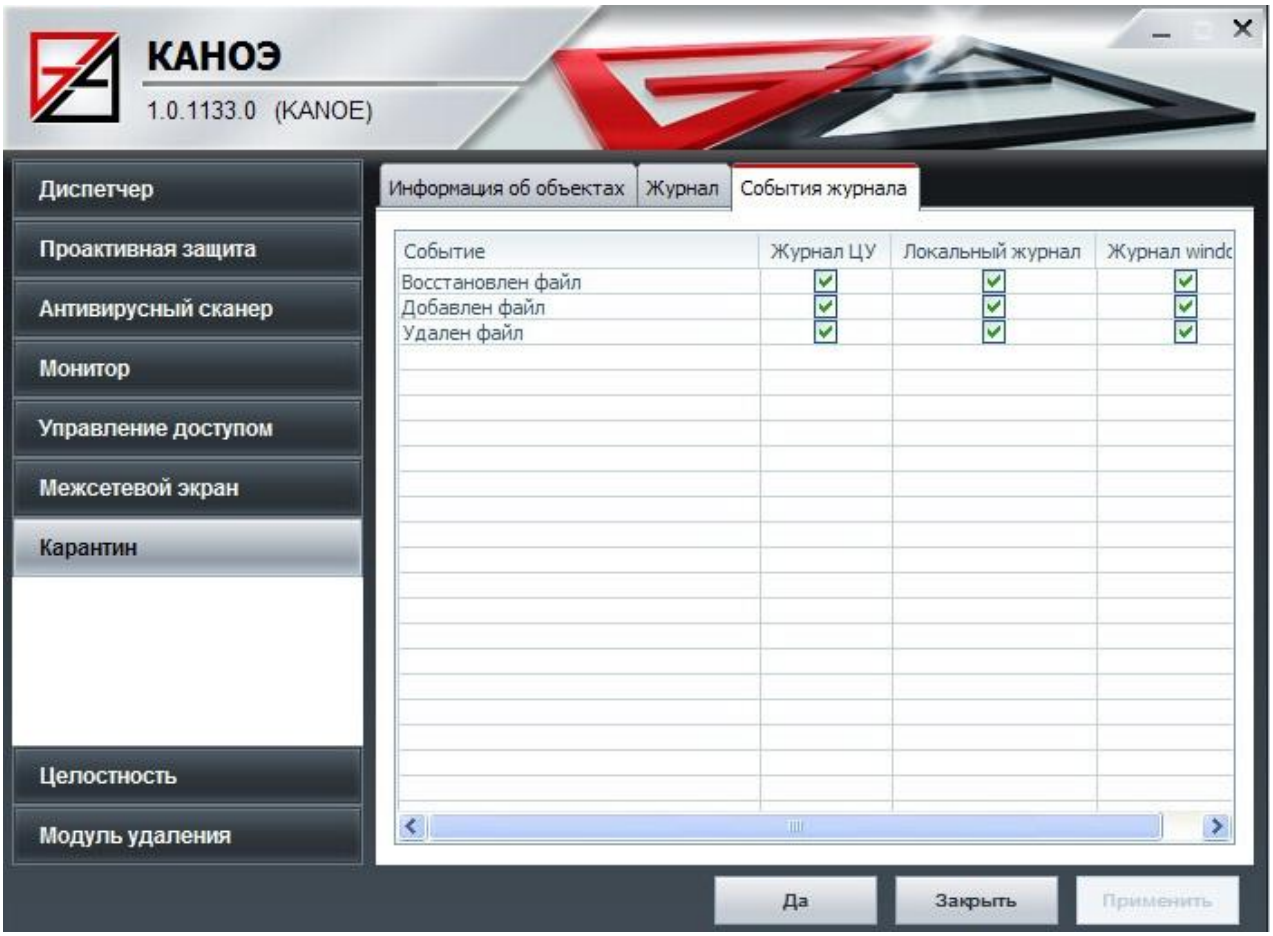

Рис. 68

4.8. Раздел Целостность

Раздел **Целостность** включает в себя вкладки:

1) Файлы;
2) Реестр и устройства;
3) Журнал;
4) События журнала.

4.8.1. Вкладка Файлы

Вкладка **Файлы** (рис. 69) имеет следующие параметры и возможности:

1) возможность добавления, изменения и удаления путей (рис. 70) и шаблонов файлов, целостность которых необходимо контролировать. При добавлении нового пути и шаблона после нажатия на кнопку **Добавить** возникает модальный диалог, который просит ввести путь и шаблон файла. Диалог не позволяет ввести некорректный путь или шаблон, а также путь, который уже добавлен (появиться сообщение об ошибке), путь можно выбирать при помощи специального диалога, появляющегося по нажатию на кнопку. При

изменении записи можно изменить только шаблон к заданному пути ... . При нажатии на кнопку **Удалить** выделенная запись в списке будет удалена;

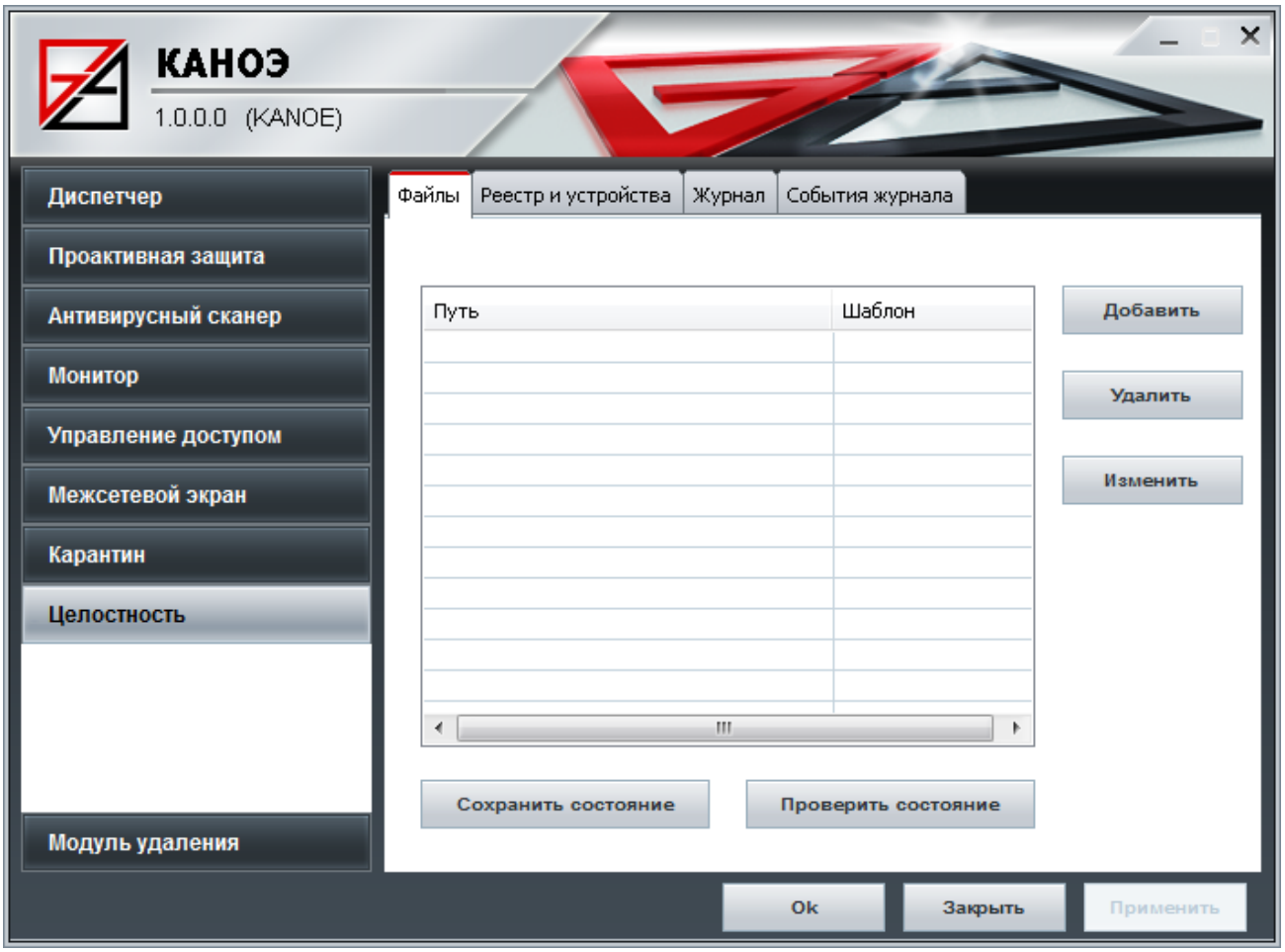

Рис. 69

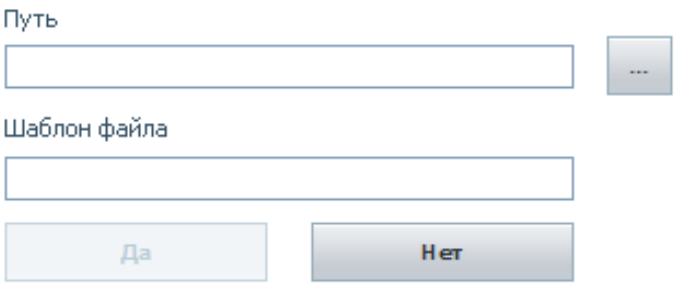

Рис. 70

2) проверка состояния и сохранение состояния файлов по указанным путям, удовлетворяющих заданным шаблонам.

4.8.2. Вкладка Реестр и устройства

Вкладка **Реестр и устройства** (рис. 71) имеет следующие параметры и возможности:

1) возможность добавления, изменения и удаления путей реестра, целостность которых необходимо контролировать. При добавлении нового пути после нажатия на кнопку **Добавить** возникает модальный диалог, который просит ввести путь реестра. Диалог не позволяет ввести пустой путь. При изменении возникнет модальный диалог с текущим путем реестра, который необходимо изменить. При нажатии на кнопку **Удалить** выделенная запись в списке будет удалена;

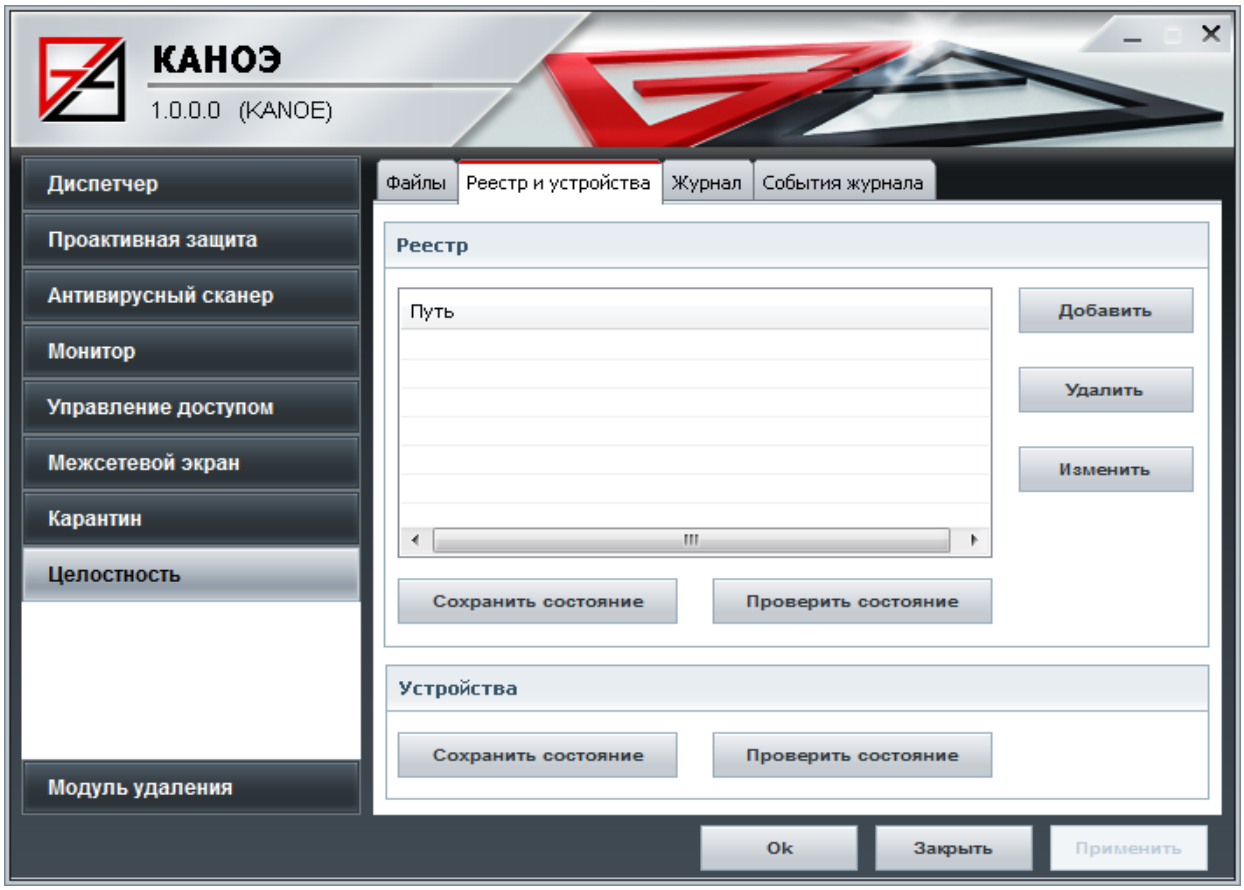

Рис. 71

2) проверка состояния и сохранение состояния указанных путей реестра (рис. 72);

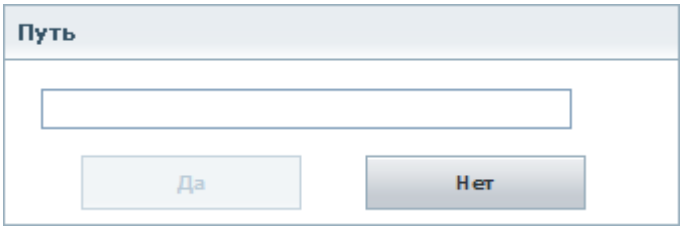

Рис. 72

3) проверка состояния и сохранение состояния **Устройства**.

Для принятия всех изменений нужно нажать на кнопку **Применить**.

4.8.3. Вкладка Журнал

Вкладка **Журнал** (рис. 73) служит для отображения событий, которые были сгенерированы **Модулем контроля целостности** и записаны в **Локальный журнал**:

1) **дата начала журнала** – задает дату, начиная с которой будет отображаться журнал;
2) **дата окончания журнала –** задает дату, на которой будет заканчиваться отображение журнала.

Примечание. Дата отображается в формате дат, выбранном на компьютере (например, мм/дд/гггг).

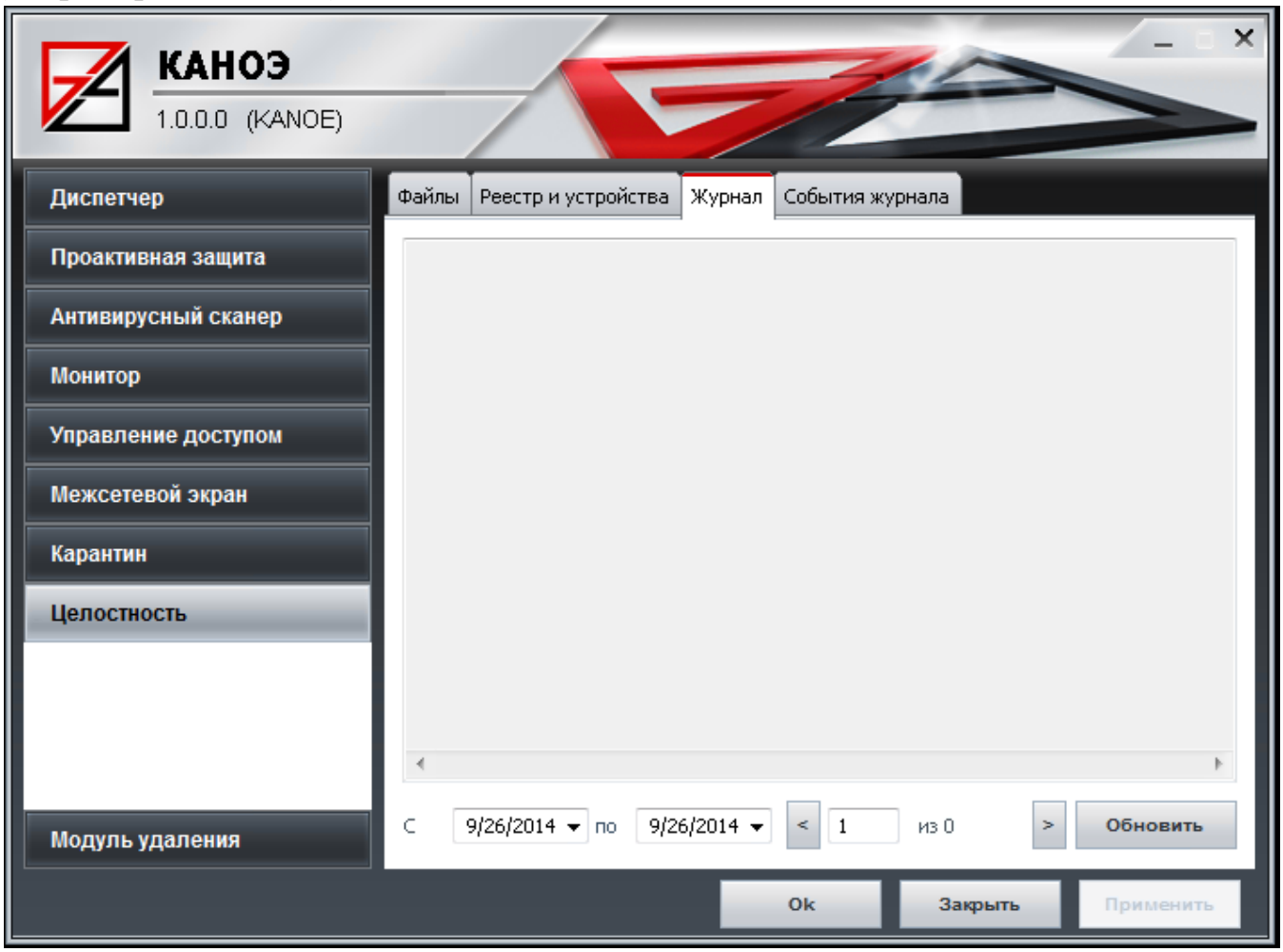

Рис. 73

Нажмите кнопку **Обновить,** чтобы отобразить журнал действий **Модуля контроля целостности** в соответствии с указанными датами.

4.8.4. Вкладка События журнала

Вкладка **События журнала** (рис. 74) служит для настройки, в какой журнал будет записываться то или иное событие. Доступные журналы: **журнал ЦУ**, **локальный журнал** и **журнал Windows**.

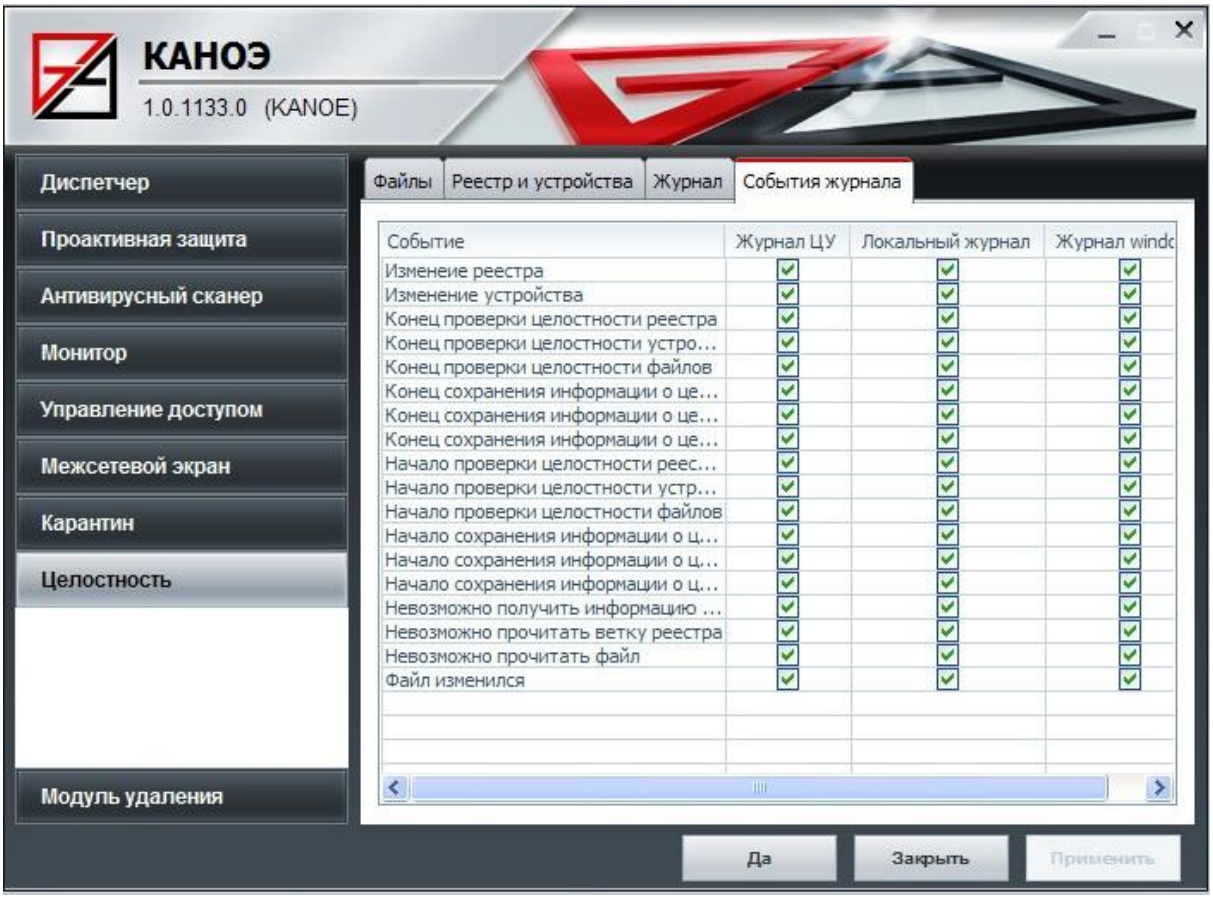

Рис. 74

4.9. Раздел Модуль удаления

4.9.1. Вкладка Настройки

Модуль удаления (рис. 75) имеет следующие функционал – безопасное удаление объектов по задаваемым шаблонам.

Все доступные шаблоны содержаться в списке **Имя шаблона**. Справа от него расположен функционал для добавления, изменения и удаления шаблона. При выборе шаблона в нижнем списке **Путь, Маска** отобразятся его параметры. Смысл их таков: в этой директории и во всех вложенных в нее будут удалены файлы, которые удовлетворяют маске. Справа от списка **Путь, Маска** расположен функционал для добавления, изменения и удаления параметров шаблона.

Для того чтобы начать процесс очистки по шаблонам, необходимо нажать кнопку **Очистить**, предварительно отметив галочкой по каким шаблонам производить очистку.

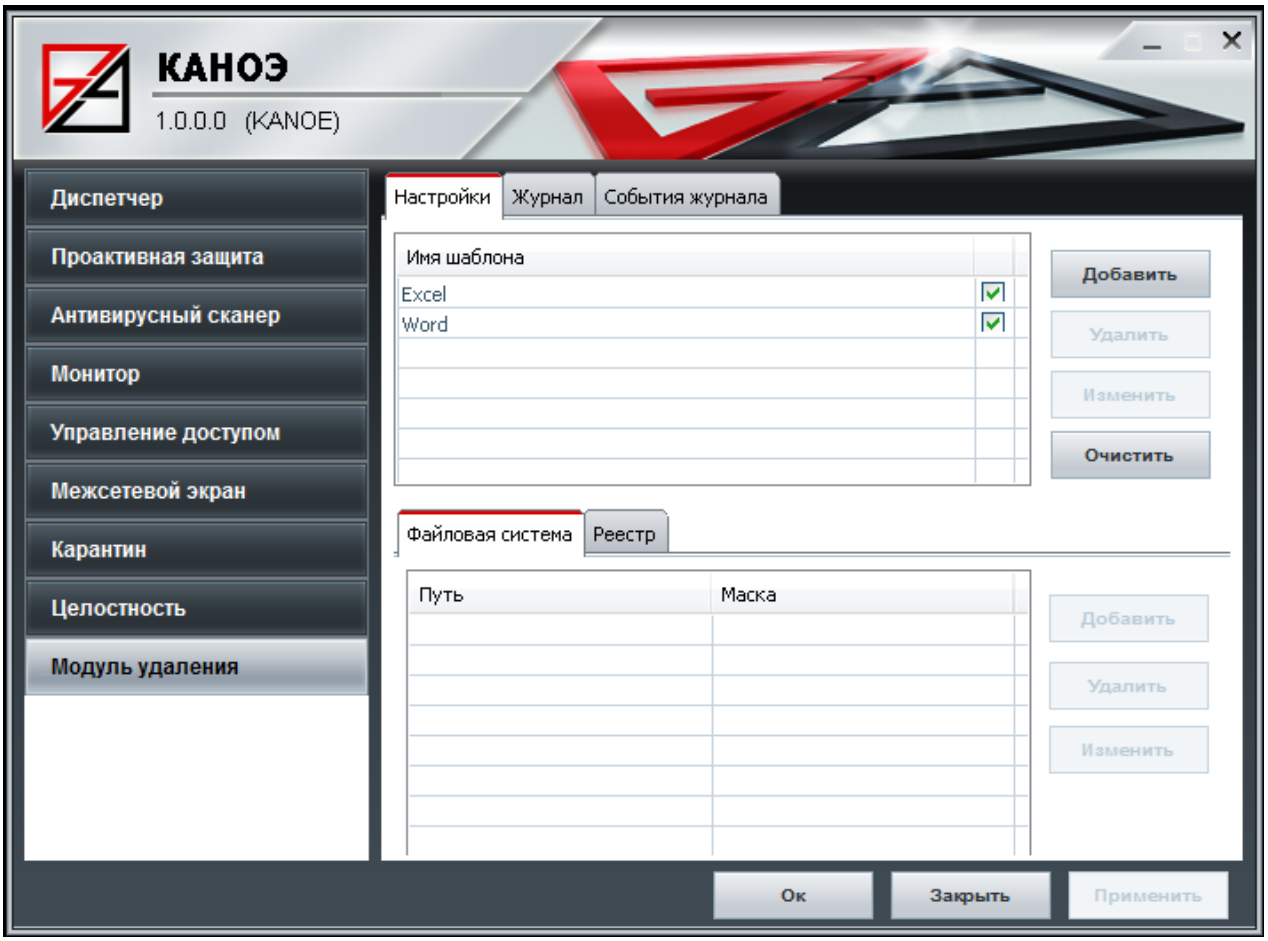

Рис. 75

4.9.2. Вкладка Журнал

Вкладка **Журнал** (рис. 76) служит для отображения событий, которые были сгенерированы **Модулем удаления** и записаны в **Локальный журнал**:

1) **дата начала журнала** – задает дату, начиная с которой будет отображаться журнал;
2) **дата окончания журнала –** задает дату, на которой будет заканчиваться отображение журнала.

Примечание. Дата отображается в формате дат, выбранном на компьютере (например, мм/дд/гггг).

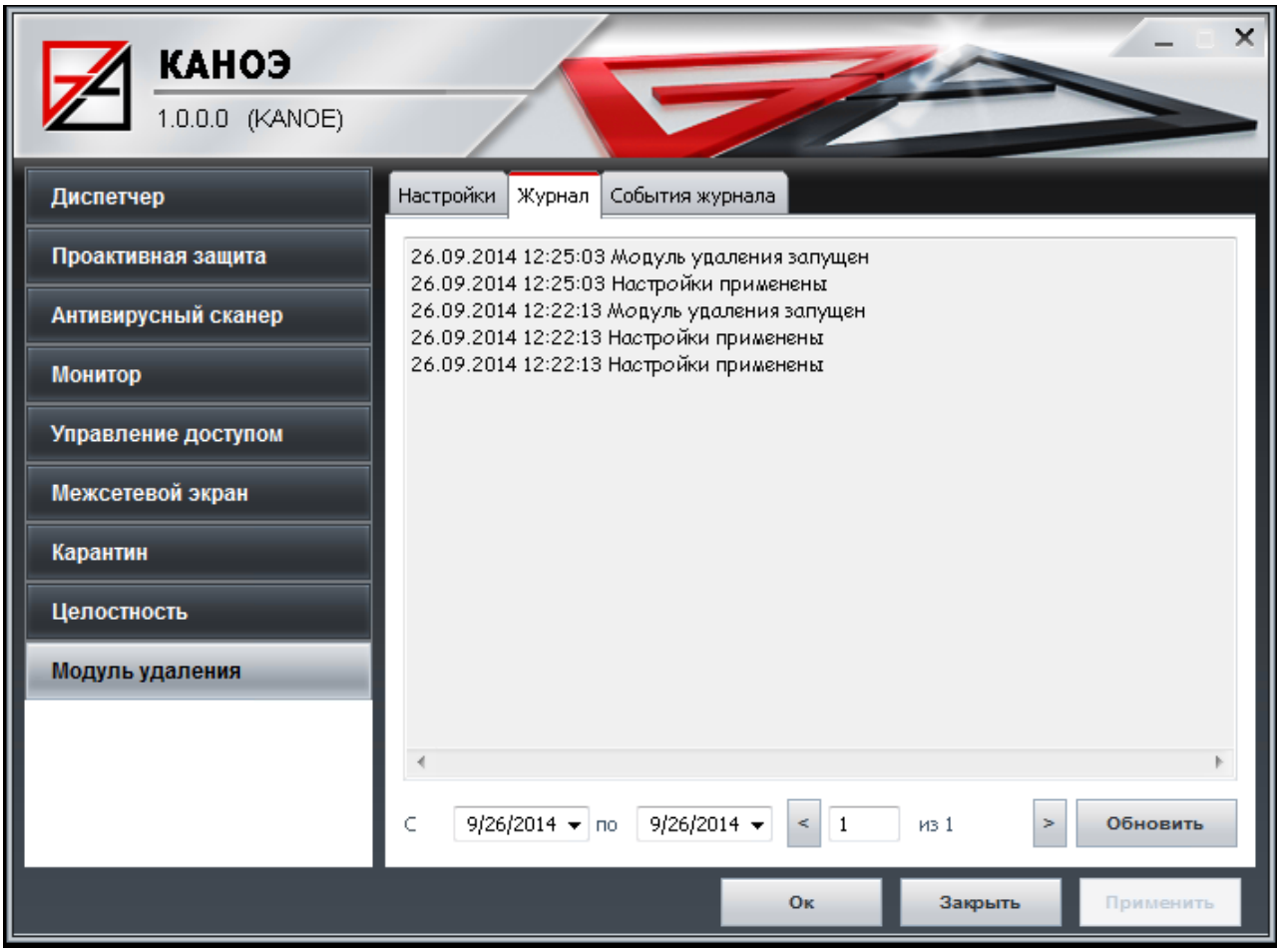

Рис. 76

Нажмите кнопку **Обновить,** чтобы отобразить журнал действий **Модуля удаления** в соответствии с указанными датами.

4.9.3. Вкладка События журнала

Вкладка **События журнала** (рис. 77) служит для настройки, в какой журнал будет записываться то или иное событие. Доступные журналы: **журнал ЦУ**, **локальный журнал** и **журнал Windows**.

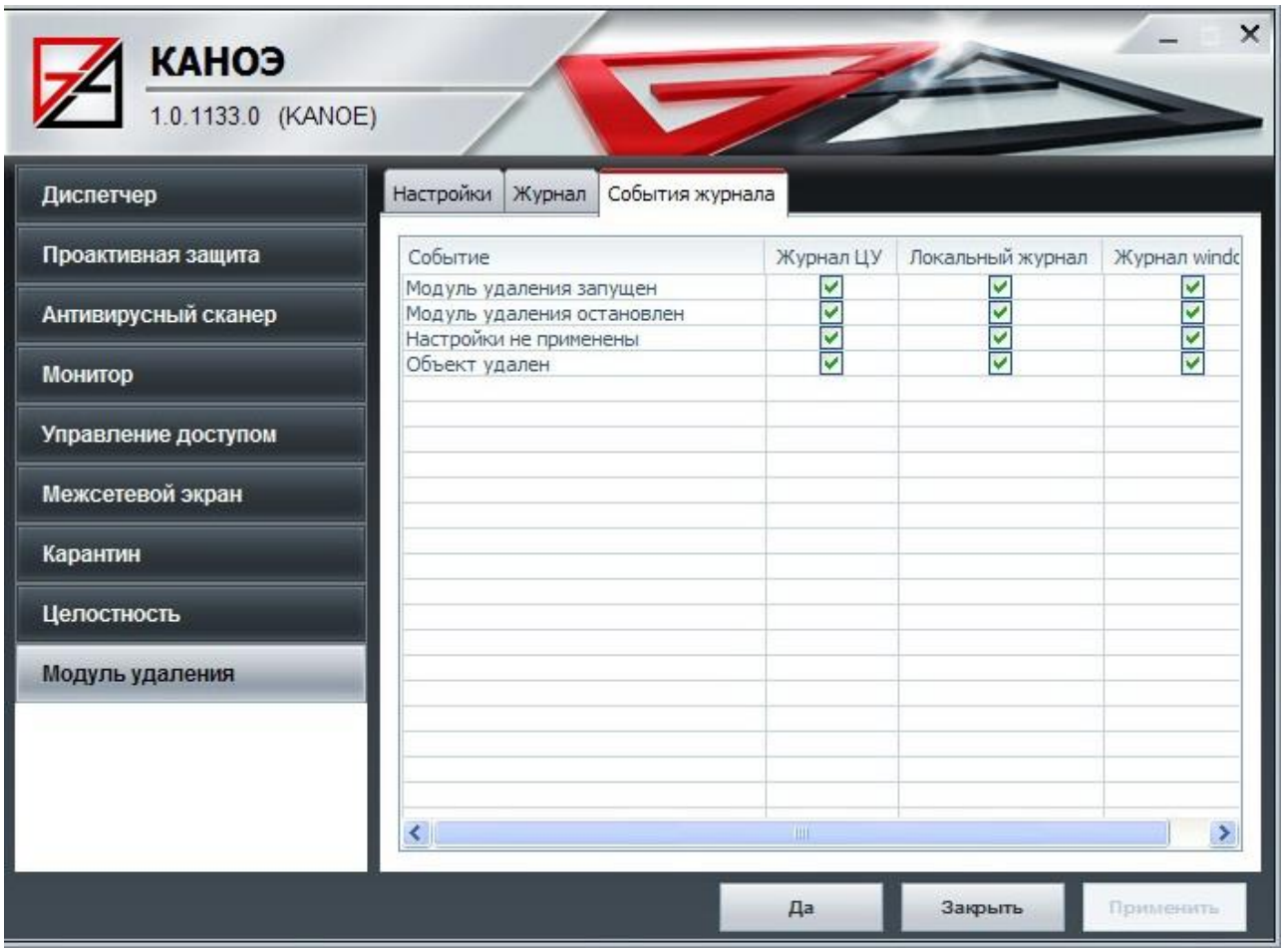

Рис. 77

4.10. Начало работы с модулем «Центр Управления»

В основу функционирования модуля «Центр Управления» заложены две сущности: события и задачи.

Компьютеры, на которых обеспечивается защита, отображаются в модуле «Центр Управления» как зарегистрированные. Модули «Агент» зарегистрированных компьютеров присылают сообщения о ключевых событиях, произошедших на компьютерах – включении/выключении антивирусной защиты, обновлении, обнаружении вредоносной программы и т.п. Все сообщения сохраняются в общем списке событий; есть возможность настроить уведомления администратора при регистрации события какого-либо типа.

В случае если необходимо предпринять какие-либо меры по администрированию защиты – например, настроить компоненты антивирусного комплекса, включить или отключить их, запустить проверку на вредоносные программы – компьютеру можно выдать одну из задач, с возможностью проследить статус их выполнения.

Модуль «Центр Управления» предоставляет также множество дополнительных возможностей — получение подробной информации о рабочей станции и состоянии защиты на ней.

Оперативность получения сообщения о событии – не более 1 минуты с момента наступления события. Оперативность получения информации об изменении состояния ключевых компонентов антивирусного сканера комплекса КАНОЭ – не более 1 минуты.

Основным органом управления модуля «Центр Управления» является web-интерфейс. Чтобы открыть его, необходимо воспользоваться соответствующим ярлыком, который был создан при установке модуля «Центр Управления», либо запустить Интернет-браузер и набрать в адресной строке:

http://server/VBA32CCWebConsole/

Вместо **server** подставьте реальное имя компьютера, на котором установлена серверная часть модуля «Центр Управления».

Откроется страница аутентификации (рис. 78). Чтобы получить доступ к web-интерфейсу, необходимо ввести имя пользователя и пароль.

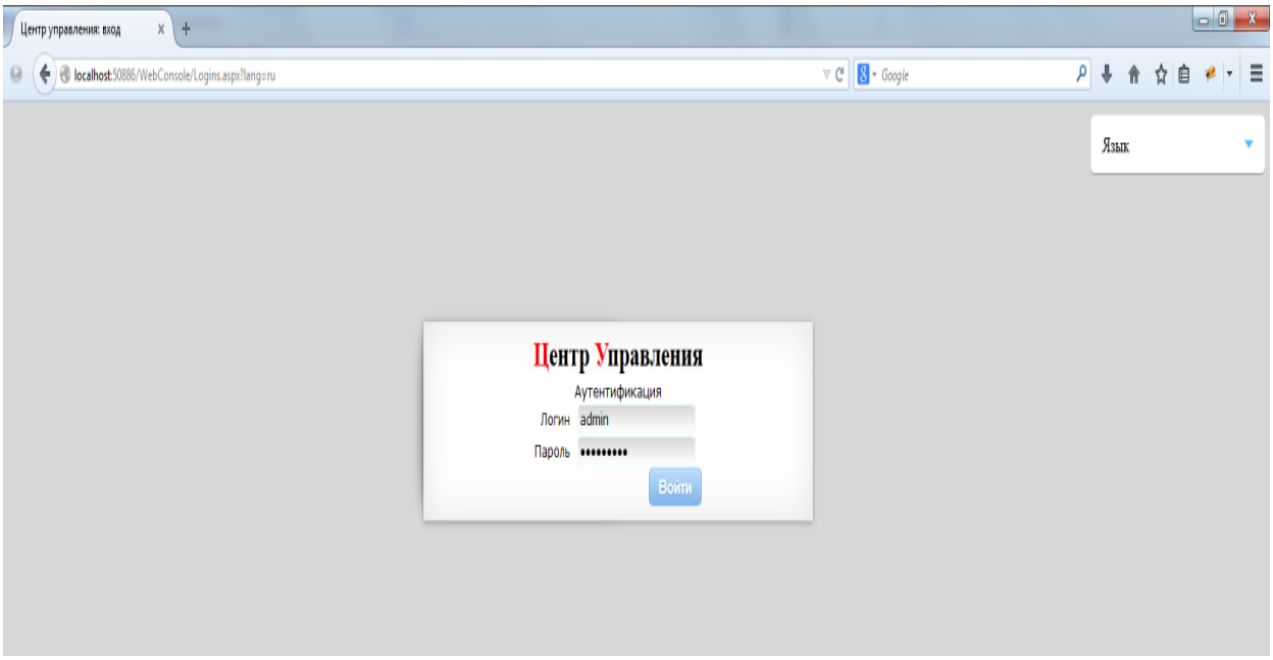

Рис. 78

В процессе установки модуля «Центр Управления» создается пользователь со следующими реквизитами:

Имя пользователя: **admin**

Пароль: 1234qwer!

Вы можете использовать эти реквизиты для первого входа в модуль «Центр Управления». После первого входа открывается заглавная страница web-интерфейса (рис. 79).

Примечание. Для корректной работы в браузерах Internet Explorer необходимо добавить сайт в список доверенных и/или локальных сайтов (Меню **Сервис → Безопасность**).

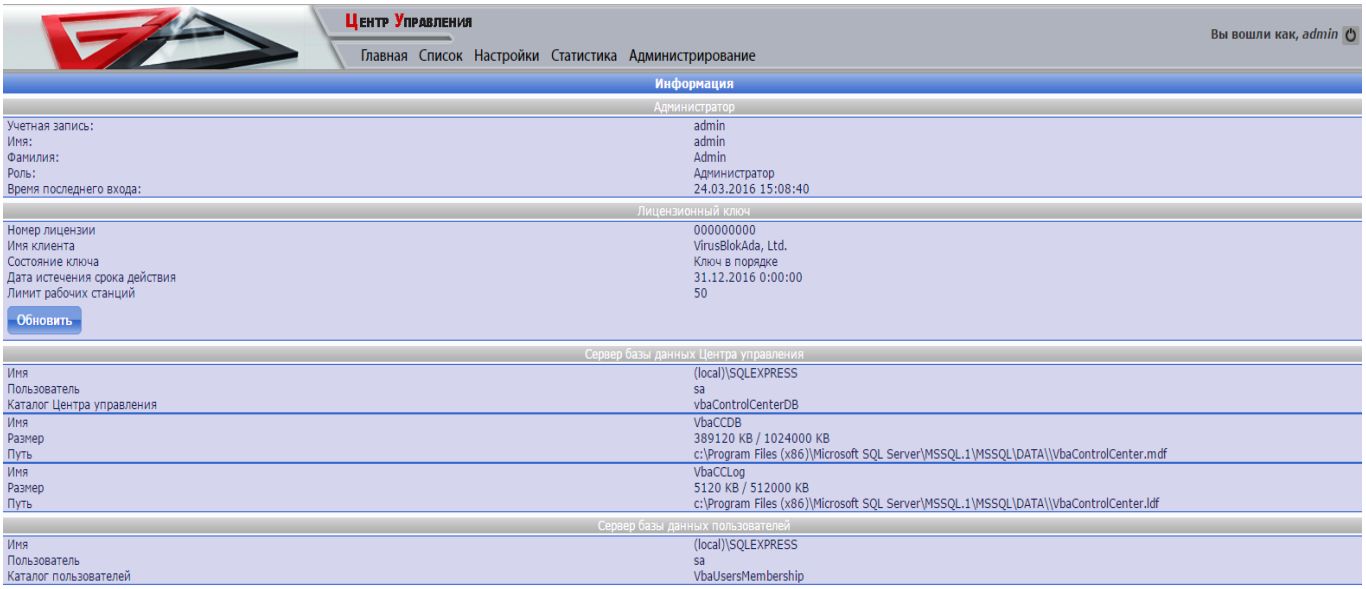

Рис. 79

На главной странице отображены данные о текущем пользователе web-интерфейса, лицензионном ключе, используемой базе данных и состоянии сервисов модуля «Центр Управления».

Примечание. После успешного открытия страницы рекомендуется сохранить ее адрес в закладках Избранного Интернет-браузера.

Рекомендуется сразу же сменить пароль учетной записи admin (см. п. 4.11.1.4), а также завести новых пользователей (см. п. 4.11.1.1) для работы с web-интерфейсом модуля «Центр Управления».

При 20 минутном отсутствии активности пользователя в web-интерфейсе происходит автоматическое завершение сеанса. На страницах с автоматическим обновлением содержимого автоматическое завершение сеанса не происходит.

4.10.1. Работа со списками

В Центре Управления пользователю предоставлен список – Компьютеры, Группы, События, Задачи, Задачи подключения, Компоненты, Процессы. Чтобы начать работу с любым из списков, надо в меню **Список** (рис. 80) нажать на соответствующую ссылку.

Списки представлены в виде таблиц. Основные принципы работы с ними одинаковы. Над таблицами находится панель фильтров, которая в обычном состоянии свернута. Чтобы развернуть ее, необходимо нажать на стрелку в правой верхней части панели. На данной панели находятся поля настройки фильтра (тип и

количество полей разные для разных списков). Чтобы свернуть панель, надо еще раз нажать на стрелку, обведенную кругом (рис. 80).

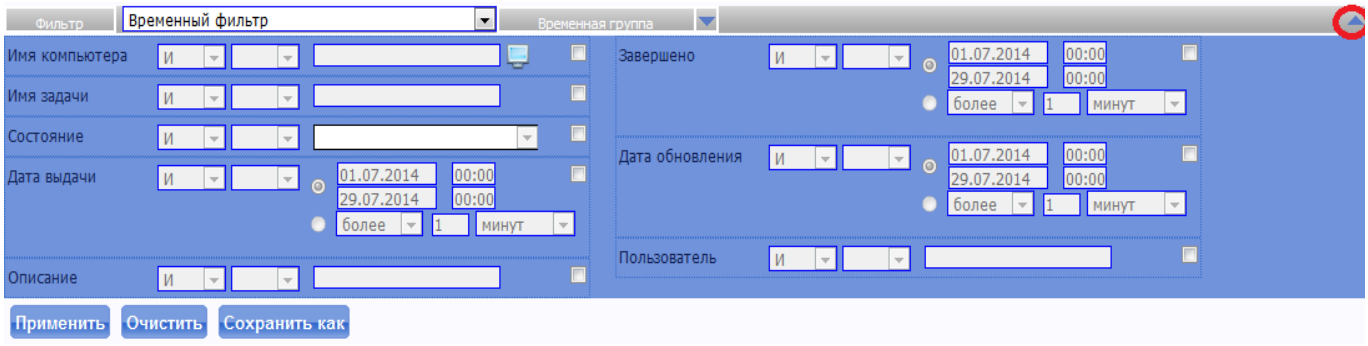

Рис. 80

4.10.1.1. Работа с табличными данными

Данные, выбранные соответствующим фильтром, отображаются в табличном виде с разбивкой на страницы (рис. 81).

Чтобы изменить количество записей, выводимых на одной странице, надо выбрать в выпадающем списке **Элементов на странице** нужное число (возможные варианты – 10, 20, 50, 100). Настройка применяется немедленно.

Для перехода по страницам служит специальный элемент управления с 4 ссылками, информацией о текущей странице и общем количестве страниц (Страница X из XX) при выбранном размере страницы. Перемещение по страницам происходит по стандартному алгоритму: ссылки > и < показывают следующую и предыдущую страницы соответственно, |< и >| - первую и последнюю. Также доступен переход на произвольную страницу: для этого необходимо ввести номер нужной страницы в текстовое поле и нажать кнопку **Перейти.**

В правом верхнем углу таблицы выводится информация о количестве записей, удовлетворяющих выбранному фильтру.

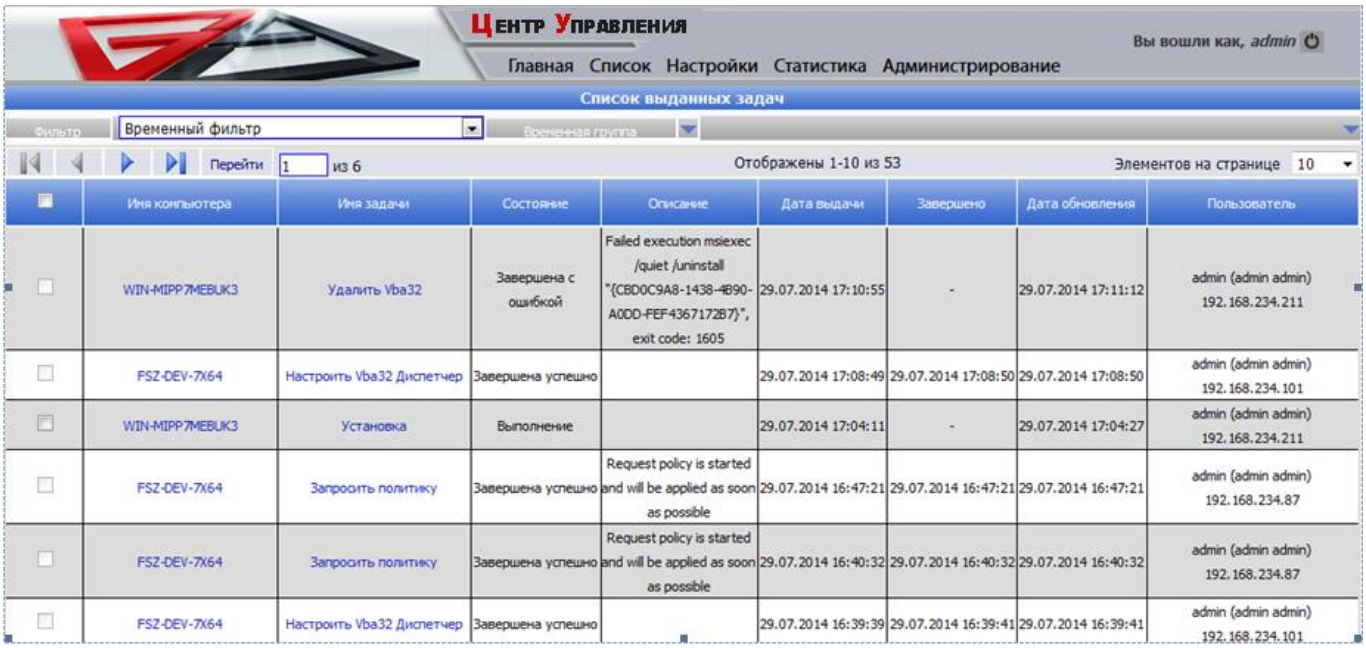

Рис. 81

Флажком **Включить автообновление содержимого** включается асинхронное обновление данных на страницах **События**, **Задачи подключения** и **Задачи**.

Табличные данные можно сортировать в порядке возрастания или убывания. Для этого необходимо нажать на имя в заголовке таблицы; первый раз происходит сортировка записей по возрастанию, второй раз – по убыванию.

4.10.1.2. Фильтрация

Одной из основных операций, выполняемых при просмотре списка, является поиск каких-либо данных – например, отчета по определенному компьютеру, событий о заражениях за определенный период и т.п. В модуле «Центр Управления» данная возможность реализована при помощи гибко настраиваемых фильтров, которые можно сохранить для дальнейшего повторного использования.

Для каждого из списков существует возможность отфильтровать данные по любому из полей (рис. 82). Так как в полях бывают данные различных типов, то бывают различные контейнеры фильтров:

1) поля для ввода. Данный тип контейнеров описан ниже;
2) выпадающие списки. Данный тип позволяет выбрать одно значение из заранее предопределенного списка;
3) флажки. Данный тип контейнеров позволяет установить логическое значение (истина или ложь), которому соответствует два состояние флажка – установлен и сброшен;
4) дата. Контейнеры этого типа представляют собой специальный элемент управления, позволяющий настроить временной интервал (при помощи выпадающих списков). Значение **С** должно быть раньше, чем **По**.

5) специализированные поля для ввода (для выбора компьютеров и IP адресов). Позволяют делать выбор более интуитивно понятным, через визуальные компоненты.

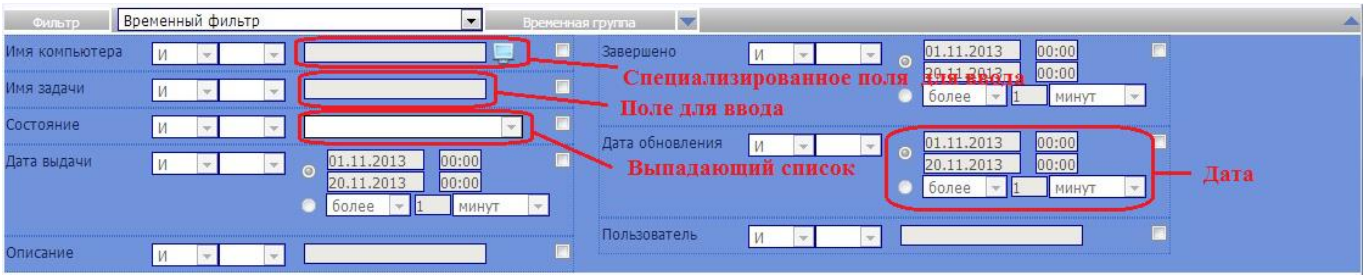

Рис. 82

Поля для ввода предполагают получение от пользователя некоторой текстовой информации. В зависимости от типа данных, используемого в соответствующем поле таблицы, различают строковые и численные контейнеры.

Строковые контейнеры разрешают ввод русских и английских символов, цифр, знаков препинания. В данных контейнерах можно использовать символы подстановки: «_» (нижнее подчеркивание, без кавычек – один любой символ) и «*» (звездочка, без кавычек – любое количество любых символов). Кроме того, возможно задавать составное значение контейнера, разделяя отдельные значения символом &:

Arg1[&Arg2]…[&ArgN], где Arg1, Arg2, … – допустимые значения параметра.

Числовые контейнеры позволяют определить интервал допустимых значений параметра. Формат ввода следующий:

Arg1-Arg2, где Arg1, Arg2 – целые неотрицательные числа, причем Arg1 не должен быть больше Arg2.

Чтобы указать, что тот или иной контейнер задействован в данном фильтре, необходимо установить флажок напротив его названия. Если этого не сделать, то данные, указанные в контейнере, не будут добавлены к фильтру.

При одновременном использовании нескольких контейнеров имеется возможность указать логические отношения между несколькими параметрами. Для этого служат выпадающие списки слева от контейнера, в котором можно выбрать комбинацию из следующих значений:

1) «И» (заданный критерий должен, встречаться в результирующей выборке);
2) «ИЛИ» (заданный критерий может встречаться. Имеет смысл лишь при использовании нескольких контейнеров);
3) «НЕ» (заданный критерий не должен встречаться в выборке).

4.10.1.3. Операции над фильтрами

Примечание. Некоторые операции с фильтрами можно произвести, только раскрыв панель фильтров. Для этого необходимо нажать на стрелку в правой верхней части панели фильтров.

4.10.1.3.1. Применение

Для применения ранее сохраненного фильтра необходимо выбрать его из выпадающего списка **Фильтр** на панели фильтров.

Чтобы настроить и применить временный фильтр (подробнее см. пункт **Временный фильтр**), необходимо заполнить требуемые контейнеры, включить их использование, установив флажки справа, и нажать на ссылку **Применить** на панели фильтров. Если данные введены верно, то в таблице будут отображены полученные данные.

Примечание. При значительном размере базы данных может потребоваться некоторое время для получения данных на сервере. В этом случае не рекомендуется пользоваться возможностью асинхронного обновления содержимого, так как это создаст дополнительную нагрузку на сервер.

4.10.1.3.2. Сохранение

Настроенный пользователем фильтр можно сохранить для повторного использования. Для этого необходимо нажать на кнопку **Сохранить как** на панели фильтров.

Для сохранения фильтра необходимо задать его уникальное имя в поле ввода во всплывающем диалоге и нажать на кнопку **Сохранить**. В случае если такое имя есть в коллекции фильтров, будет получен запрос на подтверждение его перезаписи.

Примечание. Запрещается использовать для именования пользовательских фильтров название встроенного временного фильтра на любом из доступных языков веб-интерфейса.

4.10.1.3.3. Редактирование

Чтобы отредактировать фильтр, необходимо выбрать его из выпадающего списка **Фильтр**.

После внесения необходимых изменений необходимо нажать на кнопку **Сохранить**.

4.10.1.3.4. Удаление

Для удаления фильтра нужно выбрать его из выпадающего списка **Фильтр** на панели фильтров, нажать на ссылку **Удалить** Очистить на панели фильтров и в диалоге подтверждения удаления нажать **Да**.

4.10.1.3.5. Очистка

Если к списку применен какой-либо фильтр, а необходимо получить полный список, то надо отменить действие фильтра. Для этого надо нажать на ссылку **Очистить** на панели фильтров. При этом все контейнеры очищаются и все флажки сбрасываются. В поле выбора фильтра выставляется значение **Временный фильтр**, а в таблицу выводится полный список.

4.10.1.3.6. Временный фильтр

Временным фильтром является любой не сохраненный пользователем фильтр. Он установлен по умолчанию в выпадающем списке **Фильтр**. По умолчанию данный фильтр пустой и не производит никакой фильтрации; все изменения, которые пользователь внесет в настройки данного фильтра, будут утеряны при завершении сессии работы в модуле «Центр Управления».

Временным фильтром удобно пользоваться для получения выборки, которая, скорее всего, повторно использована не будет. В противном случае рекомендуется создать и сохранить пользовательский фильтр.

4.10.1.4. Экспорт данных в Excel

Данные, выбранные с помощью фильтра и отображенные на странице списков, можно экспортировать в документ Microsoft Excel (рабочую книгу). Для этого необходимо нажать на ссылку **Экспорт данных в Excel**, расположенную в правом углу сразу под таблицей. После нажатия появится стандартный диалог сохранения файла. Все данные, удовлетворяющие текущему фильтру, будут экспортированы в документ Excel (независимо настроек размера страницы и номера текущей страницы).

Пример. Чтобы экспортировать в Excel все события с определенного компьютера, следует сделать следующее:

1) на странице списка событий в контейнере **Компьютер** ввести имя рабочей станции и отметить соответствующий флажок справа от поля для ввода. Это укажет системе, что данный контейнер используется в фильтре;
2) нажать на ссылку **Применить** на панели фильтра;

3) после отображения списка событий нажать на ссылку **Экспорт данных в Excel**;
4) в появившемся диалоговом окне указать путь и имя сохраняемому файлу и нажать кнопку **Сохранить**.

4.10.1.5. Получение статистических отчетов

Статистические данные могут быть представлены в модуле «Центр Управления» в виде статистической таблицы либо диаграмм.

Чтобы просмотреть статистические таблицы, надо в меню **Статистика** нажать на ссылку **Статистика** (рис. 83), где в доступном текстовом виде отображается информация об общем количестве зарегистрированных в системе компьютеров, событий, задач, а также данные о работе системы антивирусной защиты в сети за сегодня (например).

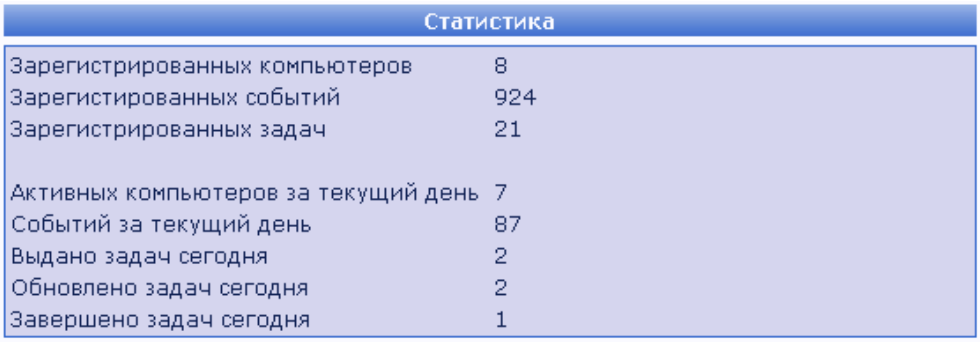

Рис. 83

Чтобы просмотреть диаграммы, надо в меню **Статистика** нажать на ссылку **Диаграмма**. На появившейся странице статистика отображается в виде гистограмм, круговых диаграмм и графиков в зависимости от выбора пользователя (рис. 84).

Чтобы развернуть фильтр диаграмм необходимо нажать на  в правой части строки.

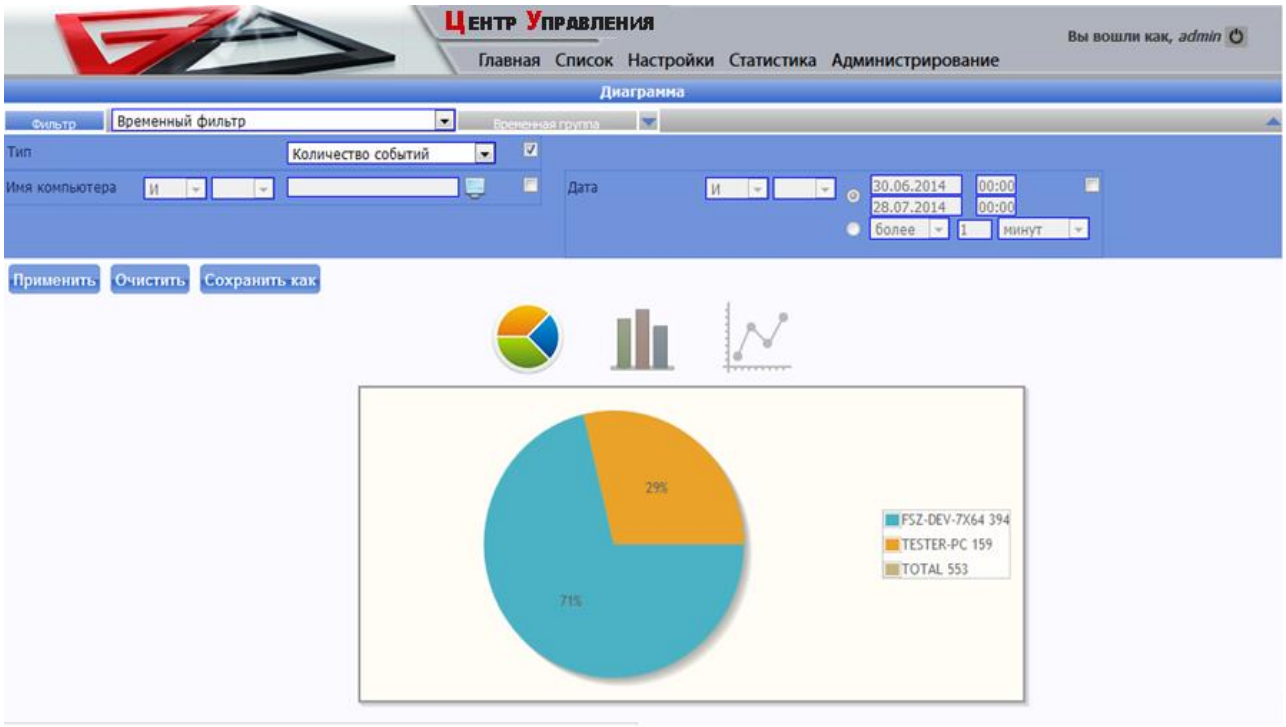

Рис. 84

Типы диаграмм выбираются путем нажатия на соответствующий значок под панелью с фильтрами. Кроме того, доступно несколько базовых типов статистической информации:

1) количество событий;
2) количество вирусов;
3) общая встречаемость вирусов.

В результате выбора одного из вышеперечисленных типов будет отображена соответствующая информация. Остальные критерии выборки задаются с помощью фильтра.

4.10.2. Выдача задач

Задача – определенные программные действия, выполняемые клиентской частью модуля «Центр Управления» на локальном компьютере по указанию управляющей части. Задачи выдаются с web-интерфейса модуля «Центр Управления».

Примечание. Работа с задачами (выдача, сохранение) недоступна при работе с модулем «Центр Управления» под учетной записью с правами наблюдателя.

Различают базовые и пользовательские задачи. Базовые задачи – это набор задач, заложенный на этапе разработки модуля «Центр Управления», и предоставляющий основу функционирования механизма задач. Существуют следующие базовые задачи:

1) создать процесс;

2) передать файл;
3) запустить сканер;
4) получить информацию о системе;
5) получить список процессов;
6) получить состояние компонентов;
7) установка;
8) удаление;
9) изменить настройки агента;
10) сконфигурировать агент;
11) отсоединить агент;
12) настроить «Диспетчер»;
13) настроить «Монитор»;
14) настроить «Сканер»;
15) настроить «Карантин»;
16) настроить «Проактивная защита»;
17) настроить «Планировщик»;
18) настроить «Межсетевой экран»;
19) настроить «Проверка целостности»;
20) настроить «Удаление файлов»;
21) «Удаление файлов»: очистить;
22) сохранение/проверка целостности;
23) запросить политику;
24) монитор-включен;
25) монитор-выключен;
26) обновить комплекс и базы;
27) обновить ключевой файл.

Пользовательские задачи создаются на основе базовых путем задания всех или части параметров. Далее пользовательская задача сохраняется в базе данных под задаваемым именем, и появляется возможность ее быстрой выдачи путем выбора из списка задач. Выдача задач осуществляется в меню **Список** на странице **Компьютеры** (рис. 85).

Сначала необходимо пометить в таблице флажками те компьютеры, которым необходимо выдать задачу. Существует возможность выдать задачу одному компьютеру, группе или всем компьютерам одновременно. Для выбора всех компьютеров, отображенных на текущей странице, можно воспользоваться кнопкой «+» в шапке таблицы. Для выдачи задачи всем компьютерам, удовлетворяющим текущему фильтру (независимо от их наличия на текущей странице), необходимо

установить флажок **Выдать задачу всем компьютерам, удовлетворяющим фильтру**.

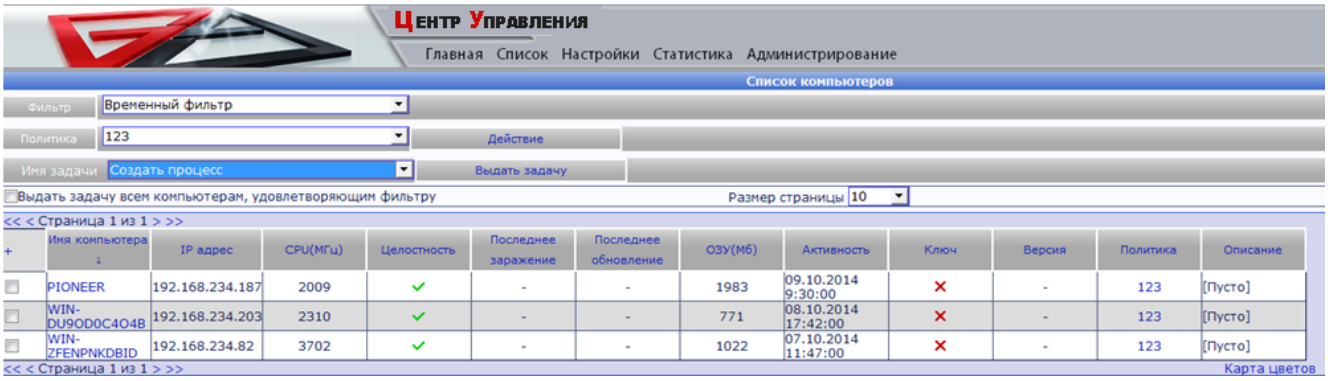

Рис. 85

Затем надо выбрать задачу в выпадающем списке **Имя задачи** (рис. 86), задать при необходимости параметры ее выполнения (для этого может понадобиться развернуть список, нажав на стрелку справа) и нажать на кнопку **Выдать задачу**.

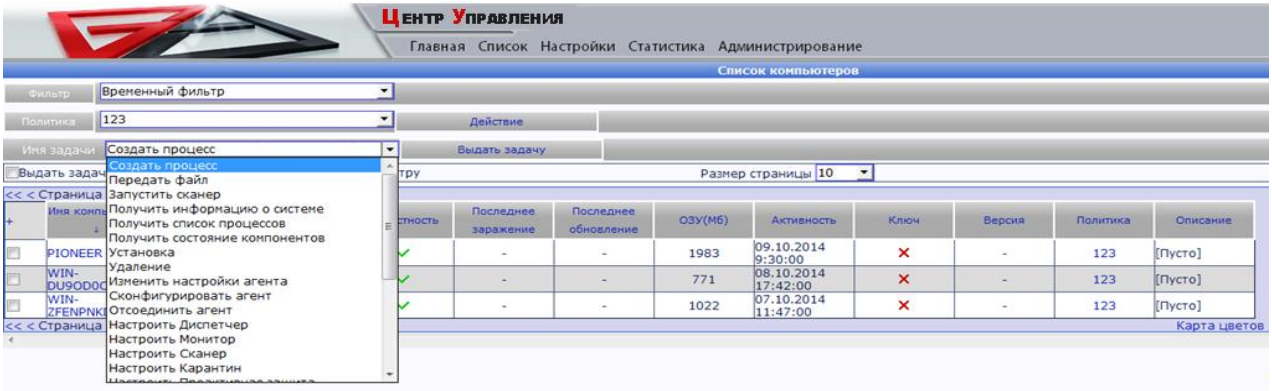

Рис. 86

В случае успешного выполнения операции над списком задач будет отображено сообщение о том, что данная задача была выдана. После этого в списке задач на странице **Задачи** для каждой рабочей станции появится запись о выданной задаче.

4.10.2.1. Базовые задачи

4.10.2.1.1. Создать процесс

Данная задача предназначена для создания процесса на клиентском компьютере с возможностью указания параметров командной строки.

При необходимости ввода дополнительных параметров возможно потребуется развернуть дополнительные настройки нажатием на треугольник справа в строке.

В поле **Командная строка** (рис. 87) необходимо ввести полный путь к запускаемому процессу и, при необходимости, параметры командной строки.

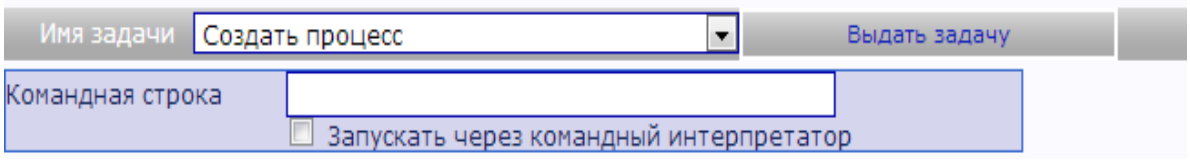

Рис. 87

При установке флажка **Запускать через командный интерпретатор** появляется возможность использовать команды командного интерпретатора, например, copy, md и другие.

Примечание. Максимальное количество одновременно выполняющихся задач **Создать процесс** на любой из рабочих станций - десять. При попытке запустить одиннадцатую, ей будет присвоен статус **Завершена с ошибкой**.

4.10.2.1.2. Передать файл

При необходимости ввода дополнительных параметров возможно потребуется развернуть дополнительные настройки нажатием на треугольник справа в строке.

Данная задача предназначена для передачи файла на клиентскую рабочую станцию.

Сначала нужный файл нужно загрузить на сервер. Для этого необходимо нажать на кнопку **Обзор** (рис. 88) в стандартном диалоге выбрать файл для передачи и нажать на ссылку **Загрузить**.

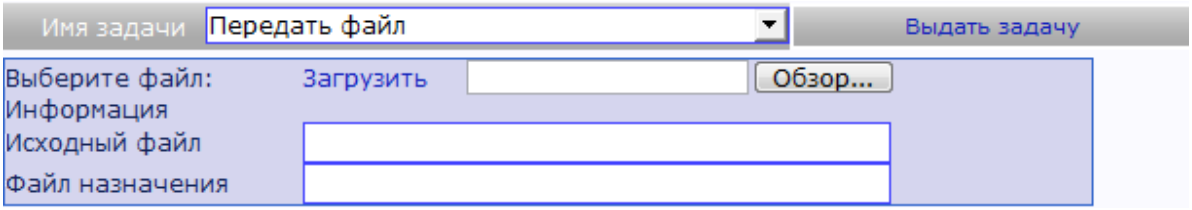

Рис. 88

Примечание. Размер загружаемого файла не должен превышать 2.097.151 Кб.

После загрузки в поле **Информация** появится информация о загруженном файле.

Поле **Исходный файл** будет автоматически заполнено путем для скачивания файла **Агентом**. Все файлы закачиваются в подкаталог **Downloads** web-консоли, при этом им присваивается уникальное имя без расширения.

В поле **Файл назначения** необходимо ввести полный путь, куда модуль «Агент» должен поместить файл после скачивания. В этом поле можно использовать переменные окружения (%WINDIR% и т.п.), которые будут раскрываться на клиентском компьютере.

Примечание. Если до нажатия на ссылку **Загрузить** данное поле было пустым, то в него автоматически подставляется строка вида: **%WINDIR%\Temp\имя_исходного_файла**.

4.10.2.1.3. Запустить сканер

При необходимости ввода дополнительных параметров возможно потребуется развернуть дополнительные настройки нажатием на треугольник справа в строке.

Данная задача запускает сканер. В списке **Пути сканирования** (рис. 89) задаются пути для сканирования, а также, определяется необходимость сканировать память.

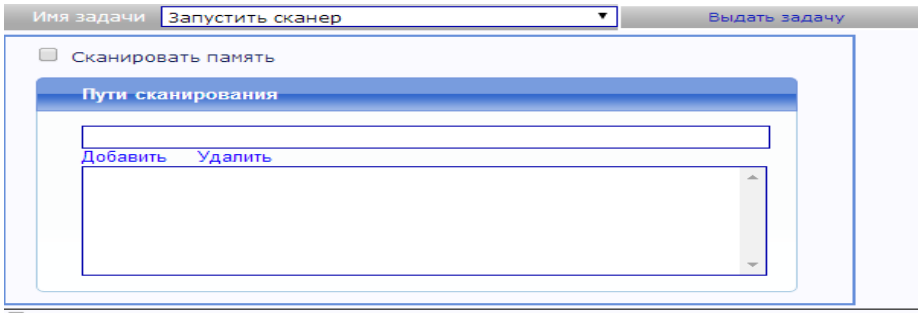

Рис. 89

4.10.2.1.4. Получить информацию о системе

Данная задача дает команду модулю «Агент» немедленно отослать информацию о системе, а также целостности антивируса на клиентском компьютере.

У задачи нет параметров.

4.10.2.1.5. Получить список процессов

Данная задача дает команду модулю «Агент» немедленно отослать список процессов, выполняющихся на клиентском компьютере.

У задачи нет параметров.

4.10.2.1.6. Получить состояние компонентов

Данная задача дает команду модулю «Агент» немедленно отослать состояние компонентов антивируса.

У задачи нет параметров.

4.10.2.1.7. Удаление

При необходимости ввода дополнительных параметров возможно потребуется развернуть дополнительные настройки нажатием на треугольник справа в строке.

Данная задача (рис. 90), позволяет удалить продукты на рабочих станциях. Для этого необходимо выбрать продукт из выпадающего списка **Продукт**.

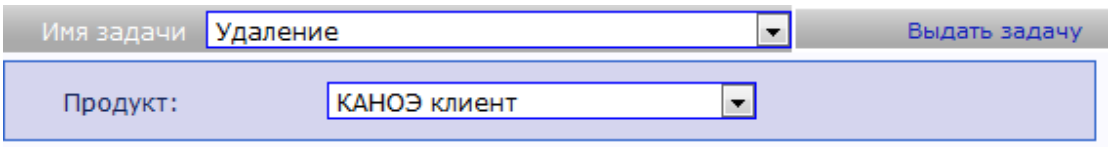

Рис. 90

4.10.2.1.8. Изменить настройки агента

При необходимости ввода дополнительных параметров возможно потребуется развернуть дополнительные настройки нажатием на треугольник справа в строке.

Данная задача (рис. 91), дает возможность настроить интервал опроса агента.

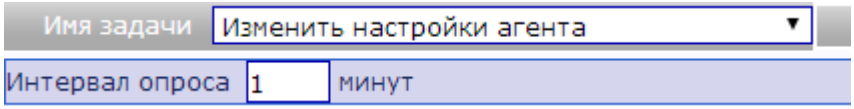

Рис.91

4.10.2.1.9. Сконфигурировать агент

Данная задача (рис. 92), дает возможность сконфигурировать модуль «Агент» на другой модуль «Центр Управления» (данный модуль «Центр Управления» продолжает управлять модулем «Агент»). Для настройки необходимо выбрать файл VbaControlAgent.cfg другого модуля «Центр Управления».

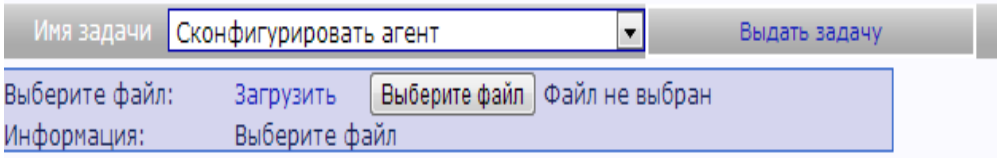

Рис. 92

4.10.2.1.10. Отсоединить агент

Данная задача дает команду модулю «Агент» отсоединиться от данного модуля «Центр Управления».

Примечание. Управление данным модулем «Центр Управления» будет потеряно.

У задачи нет параметров.

4.10.2.1.11. Настроить Диспетчер

Для доступа к детальным настройкам необходимо нажать на треугольник в правой части строки **Имя задачи**. Данная задача (рис. 93), дает возможность настроить **Диспетчер**. На вкладках **Основные**, **Прокси-сервер**, **Авторизация**,

Пароль задаются параметры, которые соответствуют настройкам Диспетчера (см. п. 4.1.2). Вкладки **Основные, Прокси-сервер**, **Авторизация** в модуле «Центр Управления» соответствует вкладке **Обновление** в «КАНОЭ-клиент». Вкладка **Пароль** позволяет добавить, удалить или редактировать пользователей.

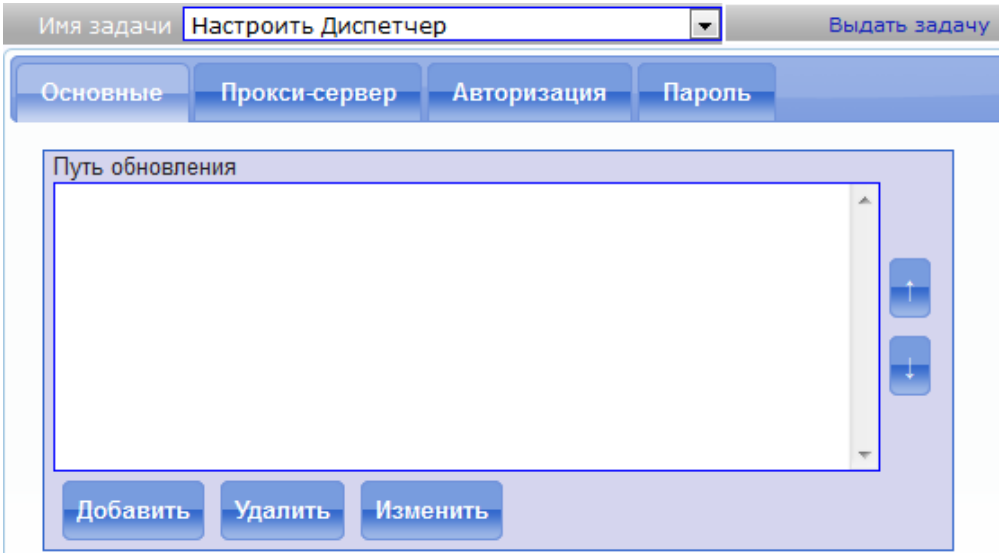

Рис. 93

4.10.2.1.12. Настроить Монитор

Данная задача (рис. 94) дает возможность настроить **Монитор**. На вкладках **Объекты**, **События журнала** задаются параметры, которые соответствуют настройкам Монитора (см. п. 4.4.1, п. 4.4.3). Вкладка **Объекты** в модуле «Центр Управления» соответствует вкладке **Настройки** в «КАНОЭ-клиент».

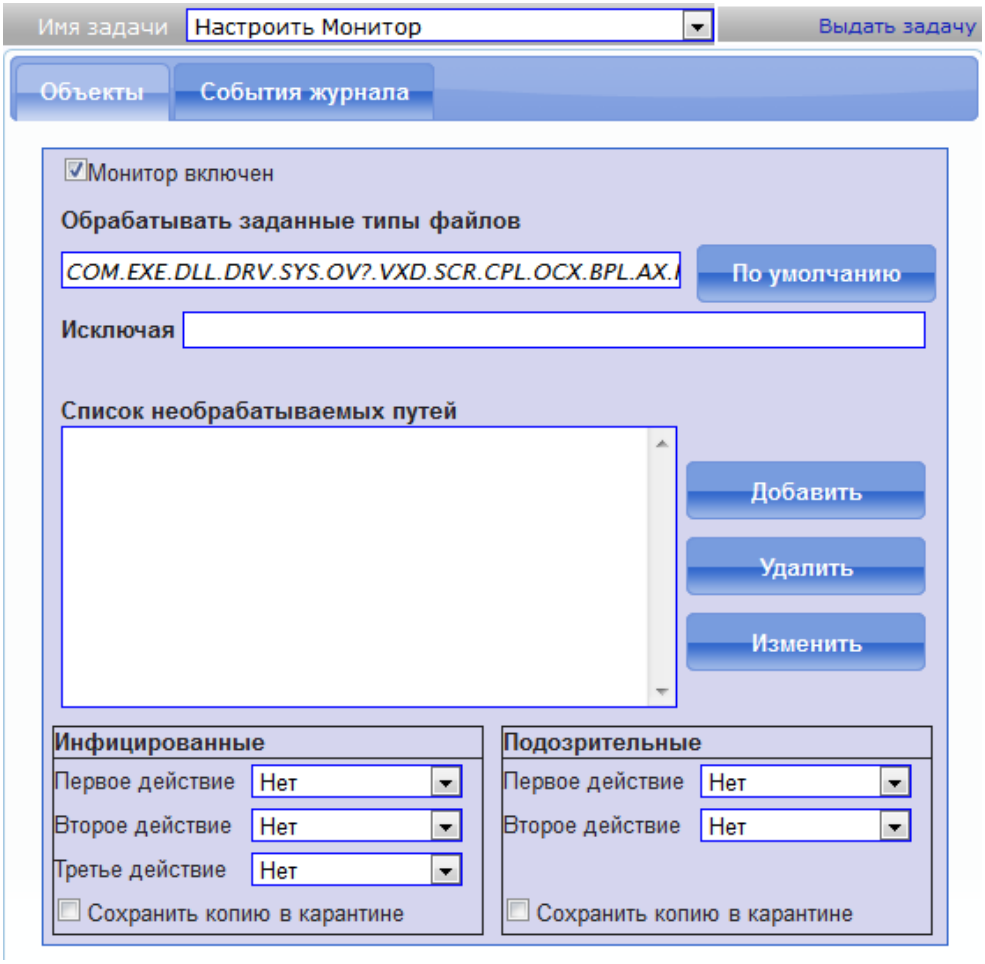

Рис. 94

4.10.2.1.13. Настроить Сканер

Данная задача (рис. 95) дает возможность настроить **Сканер**. На вкладках **Объекты сканирования**, **События журнала** задаются параметры, которые соответствуют настройкам Сканера (см. п. 4.3.2, п. 4.3.4).

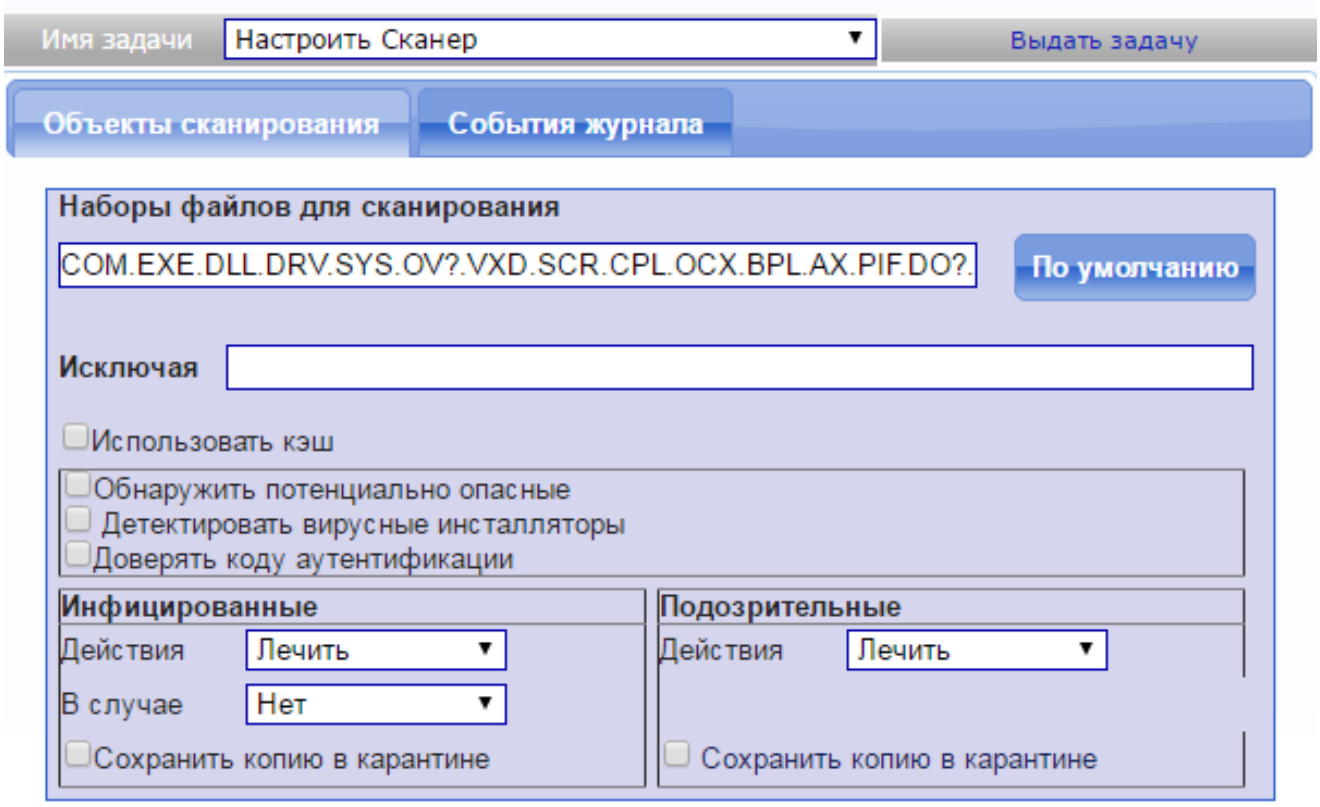

Рис. 95

4.10.2.1.14. Настроить Карантин

Данная задача (рис. 96) дает возможность настроить **Карантин**. Вкладка **События журнала** служит для настройки, в какой журнал будет записано то или иное событие. Доступные журналы: **журнал Windows**, **локальный журнал** и **журнал ЦУ**.

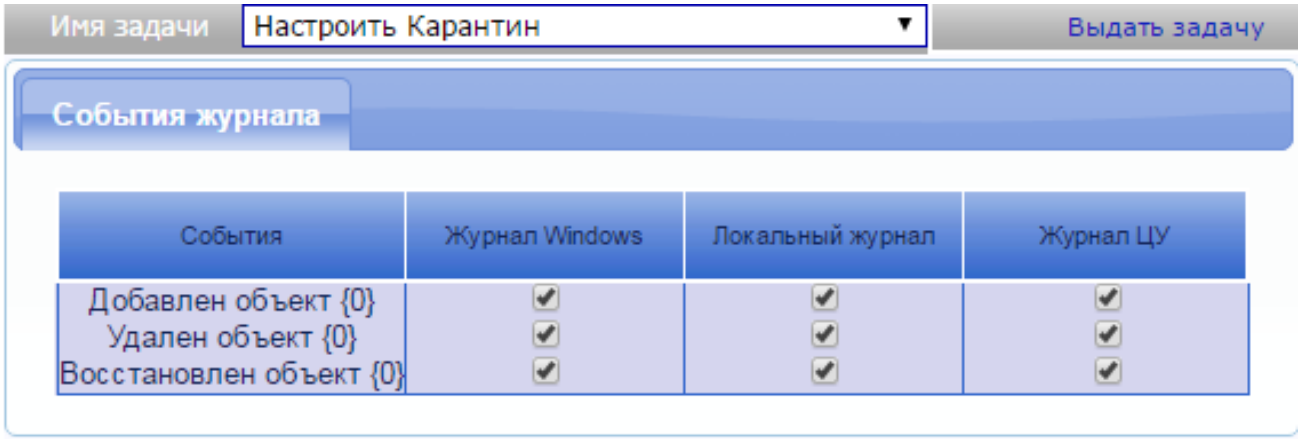

Рис. 96

4.10.2.1.15. Настроить Проактивная защита

Данная задача (рис. 97) дает возможность настроить **Проактивную защиту**. На вкладках **Общие**, **Пользователи, Принтеры, Аудит, События журнала** задаются параметры, которые соответствуют настройкам **Проактивной защите** (см. п. 4.2.1 – п. 4.2.4 и п. 4.2.6). Вкладка **Общие** в модуле «Центр Управления» соответствует вкладке **Защищаемые объекты** в «КАНОЭ-клиент».

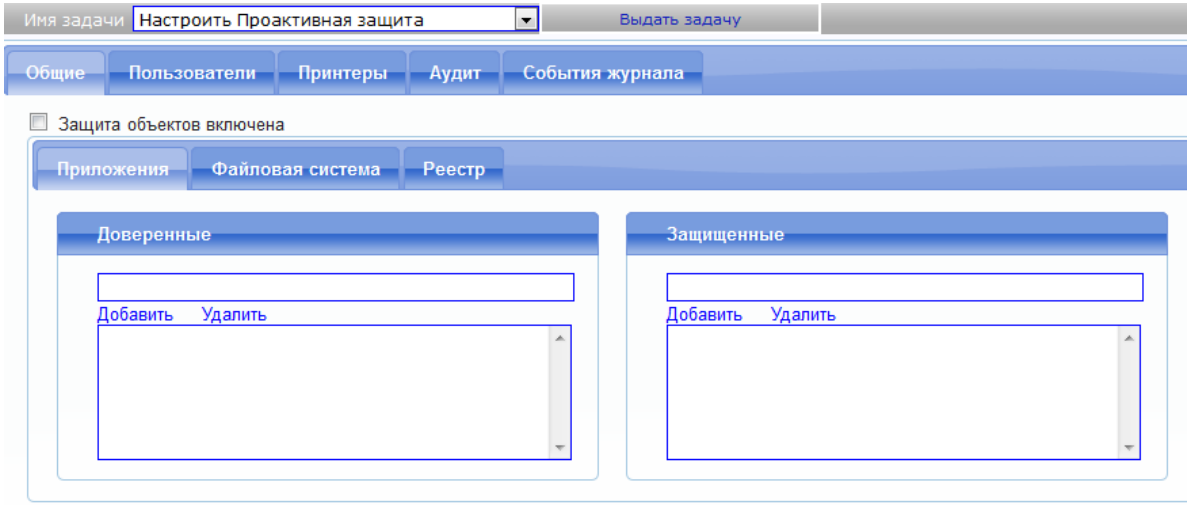

Рис. 97

4.10.2.1.16. Настроить Планировщик

Данная задача дает возможность настроить **Планировщик** (рис. 98). Вкладка **Планировщик** обеспечивает настройку запуска задач в фоновом режиме с указанной периодичностью.

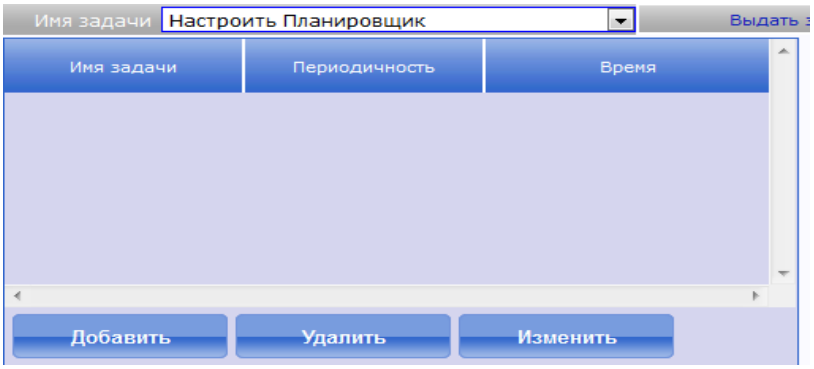

Рис. 98

4.10.2.1.17. Настроить Межсетевой экран

Данная задача дает возможность настроить **Межсетевой экран** (рис. 99). На вкладках **Общие**, **IP v4, IP v6, События журнала** задаются параметры, которые соответствуют настройкам **Межсетевого экрана** (см. п. 4.6.1, п. 4.6.2 и п. 4.6.4).

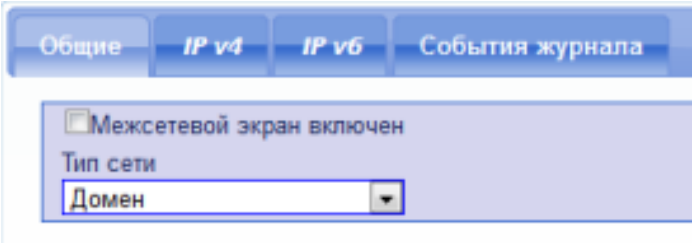

Рис. 99

4.10.2.1.18. Настроить Проверка целостности

Данная задача дает возможность настроить **Проверку целостности** (рис. 100). На вкладках **Файлы**, **Реестр, События журнала** задаются параметры, которые соответствуют настройкам **Проверки целостности** (см. п. 4.8.1, п. 4.8.2 и п. 4.8.4).

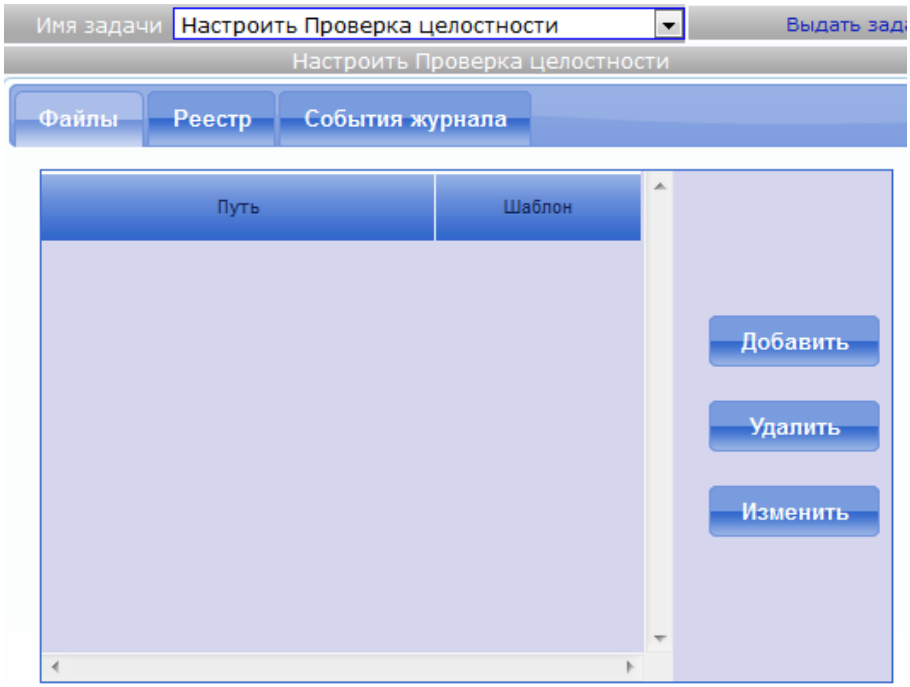

Рис. 100

4.10.2.1.19. Настроить Удаление файлов

Данная задача дает возможность настроить **Удаление файлов** (рис. 101). На вкладках **Файлы**, **События журнала** задаются параметры, которые соответствуют настройкам **Модуля удаления** (см. п. 4.9.1, п. 4.9.3).

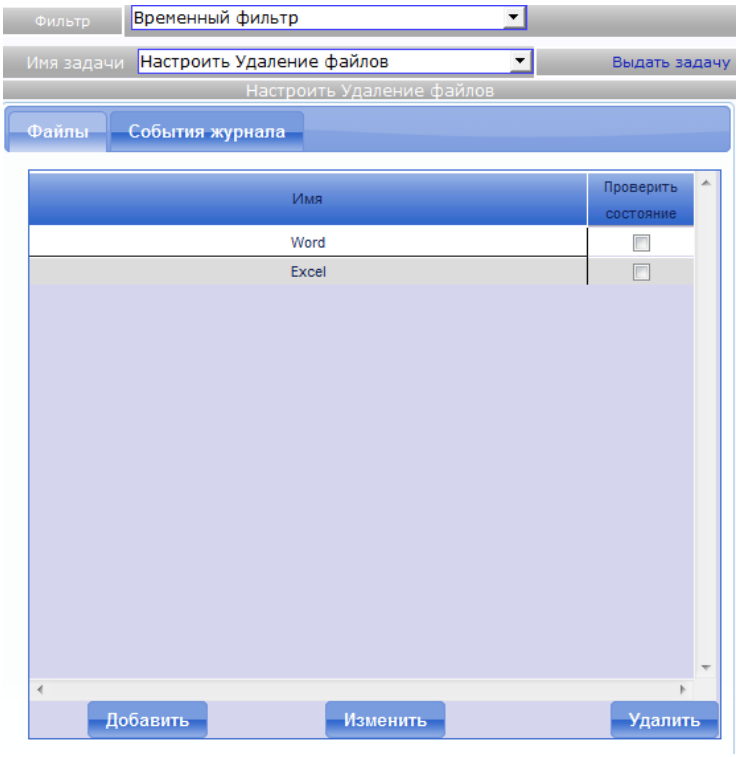

Рис. 101

4.10.2.1.20. Удаление файлов: очистить

Данная задача дает команду модулю удаления файлов на очистку жесткого диска компьютера.

У задачи нет параметров.

4.10.2.1.21. Сохранение/проверка целостности

Данная задача позволяет сохранить текущее состояние и проверить целостность относительно этого состояния (рис. 102).

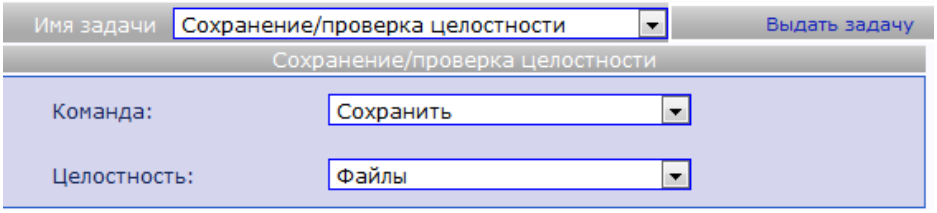

Рис. 102

4.10.2.1.22. Запросить политику

Данная задача дает команду модулю «Агент» немедленно запросить политику.

У задачи нет параметров.

4.10.2.1.23. Монитор-включить

Данная задача позволяет быстро произвести включение монитора без настройки дополнительных параметров.

У задачи нет параметров.

4.10.2.1.24. Монитор-выключить

Данная задача позволяет быстро произвести выключение монитора без настройки дополнительных параметров.

У задачи нет параметров.

4.10.2.1.25. Обновить комплекс и базы

Данная задача дает возможность обновить комплекс и базы.

У задачи нет параметров.

4.10.2.1.26. Обновить ключевой файл

Данная задача дает возможность передать ключевой файл на удаленные рабочие станции для корректной установки и последующей работы КАНОЭ-клиента (рис. 103).

Для передачи файла необходимо выбрать нужный файл нажатием на кнопку **Выберите файл**. В появившемся диалоговом окне указать ключевой файл и подтвердить данное действие. После успешно проделанной процедуры рядом с кнопкой **Выберите файл** появится название данного файла Далее необходимо нажать на ссылку **Загрузить**, а затем выдать задачу.

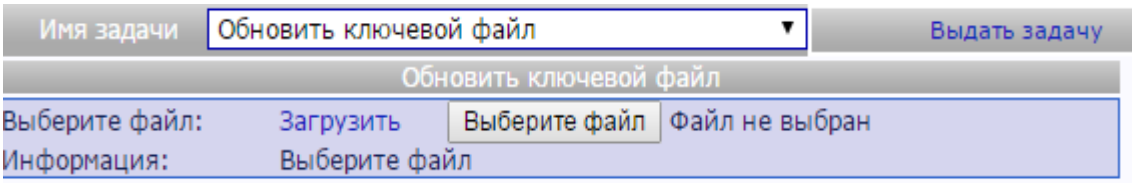

Рис. 103

4.10.2.2. Создание пользовательской задачи

Для создания пользовательской задачи необходимо выбрать в выпадающем списке **Имя задачи** нужный базовый тип задачи и нажать на ссылку **Сохранить** справа от списка. После этого на странице **Создание задачи** необходимо задать ее параметры, ввести в поле **Имя задачи** уникальное имя (если задача создавалась не на основе ранее сохраненной) и нажать **Сохранить**.

Примечание. Нельзя сохранять задачи без параметров. Запрещено давать пользовательским задачам имя как у любой из базовых задач (на любом из поддерживаемых языков).

4.10.2.3. Удаление пользовательской задачи

Чтобы удалить пользовательскую задачу, необходимо выбрать ее в выпадающем списке **Имя задачи**, нажать на ссылку **Удалить** справа от списка, после чего подтвердить операцию.

4.10.3. Информация о рабочей станции

Для перехода на страницу с информацией о рабочей станции необходимо кликнуть левой кнопкой мыши на имя нужной рабочей станции на любой из страниц **Список** (например, **Компьютеры**).

4.10.3.1. Общая информация

На вкладке **Компьютер** отображается основная информация для данной рабочей станции (рис. 104): имя компьютера, последний логин, IP адрес, версия комплекса и другое.

Также на данной вкладке имеется возможность задать собственное описание. Для этого необходимо ввести текст описания в соответствующую форму и нажать на ссылку **Сохранить**.

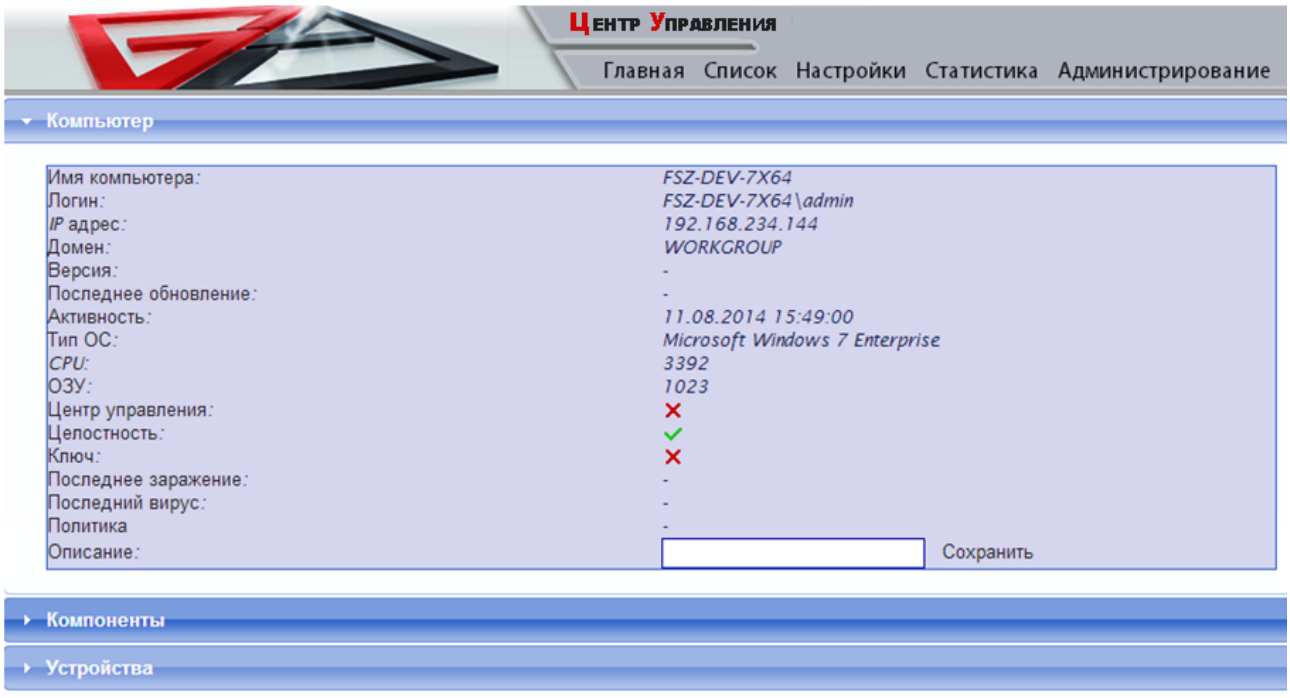

Рис. 104

4.10.3.2. Информация о компонентах комплекса

На вкладке **Компоненты** есть возможность ознакомиться с состоянием компонентов антивирусного комплекса на данной рабочей станции (рис. 105). Слева от названия компонента располагается картинка, описывающая его состояние:

1) «-» - компонент не установлен;
2) (красный цвет) - компонент выключен;
3) (зеленый цвет) - компонент включен.

Примечание. При невозможности определить состояние компонента, картинка отсутствует.

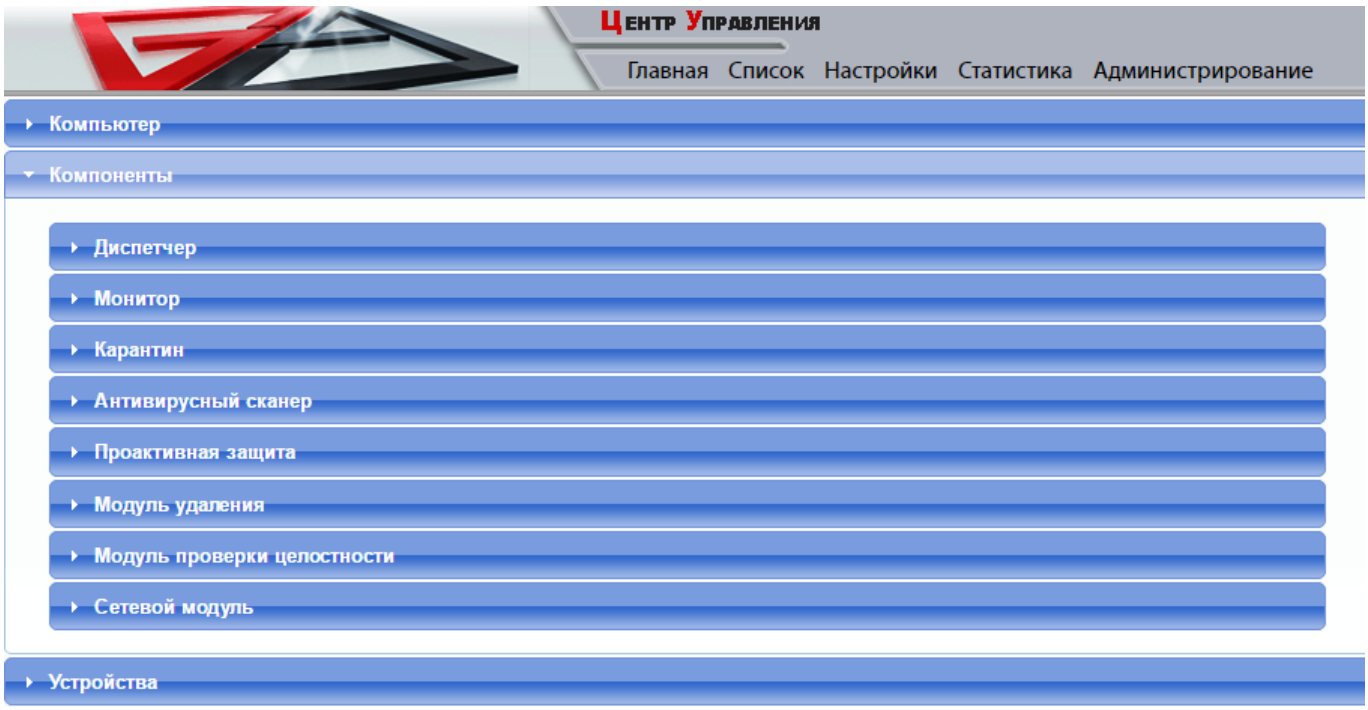

Рис. 105

4.10.3.3. Информация об устройствах

На вкладке **Устройства** есть возможность посмотреть, какие устройства назначены данной рабочей станции (рис. 106), а также произвести необходимые действия с этими устройствами.

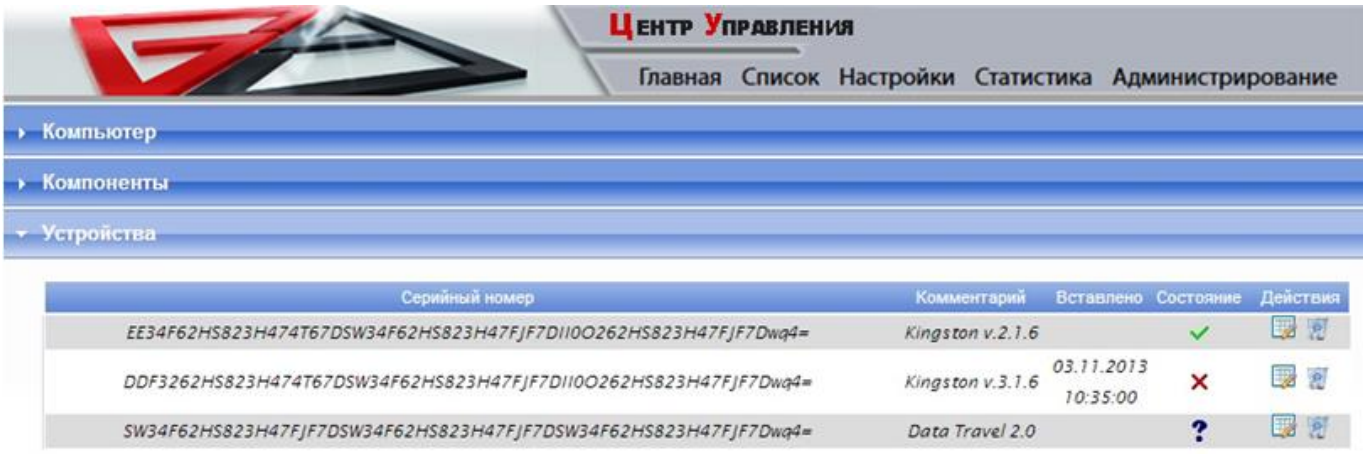

Рис. 106

4.11. Настройка модуля «Центр Управления»

4.11.1. Управление пользователями

Модуль «Центр Управления» требует авторизации для просмотра любой из своих страниц. Чтобы иметь возможность войти в систему, надо завести учетную запись. Модуль «Центр Управления» может поддерживать 128 учетных записей пользователей. Количество пользователей, одновременно работающих с модулем «Центр Управления», ограничено аппаратными ресурсами сервера антивирусной защиты.

4.11.1.1. Создание пользователя

Примечание. Создание, редактирование, удаление пользователя может быть произведено только при работе в модуле «Центр Управления» под учетной записью с правами администратора.

Для создания пользователя, надо перейти на страницу **Пользователи** раздела **Администрирование** и нажать кнопку **Создать пользователя**, появится форма регистрации пользователя (рис. 107).

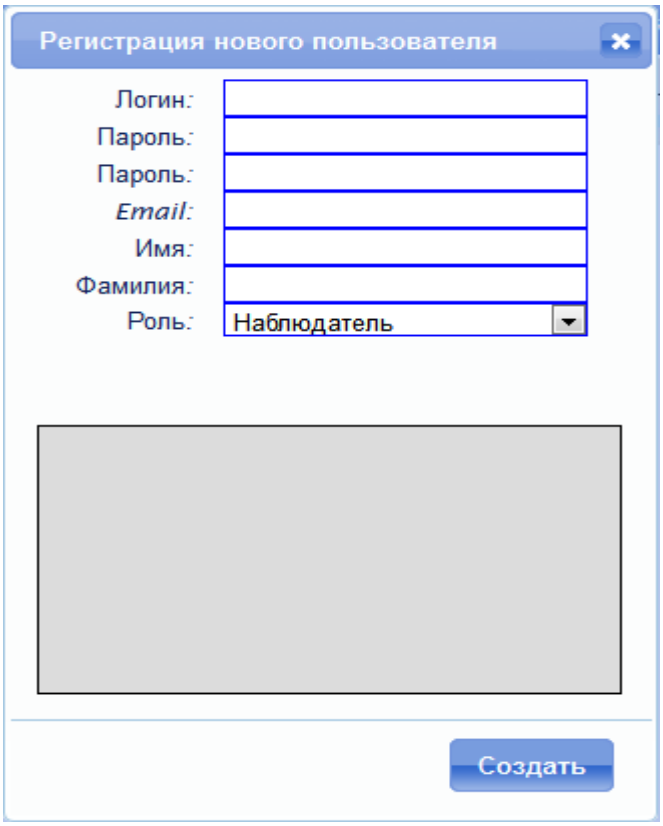

Рис. 107

Необходимо заполнить следующие поля:

1) Логин – имя учетной записи;
2) Пароль – необходимо ввести пароль учетной записи, длиной не менее 7 символов, не менее одного специального символа (не буква и не цифра);
3) Подтвердите пароль – повторно ввести пароль для исключения ошибок;
4) Имя, Фамилия, Email – данные о пользователе.

Роль пользователя. Существуют три роли:

1) Наблюдатель – позволяет просматривать списки компьютеров, событий, компонентов и процессов, а также статистику;
2) Оператор – дополнительно позволяет выдавать задачи на странице **Компьютеры** и просматривать их состояние с возможностью отмены на странице **Задачи**. Для выдачи задач становится видимой соответствующая панель внизу списка компьютеров;
3) Администратор – позволяет, помимо всех возможностей оператора, изменять настройки обслуживания базы данных (страница **Обслуживание**), уведомлений (страница **Уведомления**), самообновления (страница **Обновление**). Кроме того, администратор может создавать пользователей и управлять ими (страницы **Регистрация** и **Пользователи**), а также менять глобальную расцветку событий для страницы **События**.

После заполнения формы создания пользователя необходимо нажать на ссылку **Создать**. Если все было сделано правильно, появится надпись **Новый аккаунт был успешно создан**. В противном случае все незаполненные поля будут выделены красным цветом.

4.11.1.2. Изменение роли пользователя

Примечание. Создание, редактирование, удаление пользователя может быть произведено только при работе в модуле «Центр Управления» под учетной записью с правами администратора.

Для изменения роли пользователя необходимо открыть список пользователей (рис. 108) и нажать на кнопку редактирования  , которая находится с правой стороны строки с нужным пользователем. Во всплывающем диалоге сделать необходимые изменения и нажать кнопку **Редактировать**. Результаты изменения можно сразу увидеть в списке пользователей.

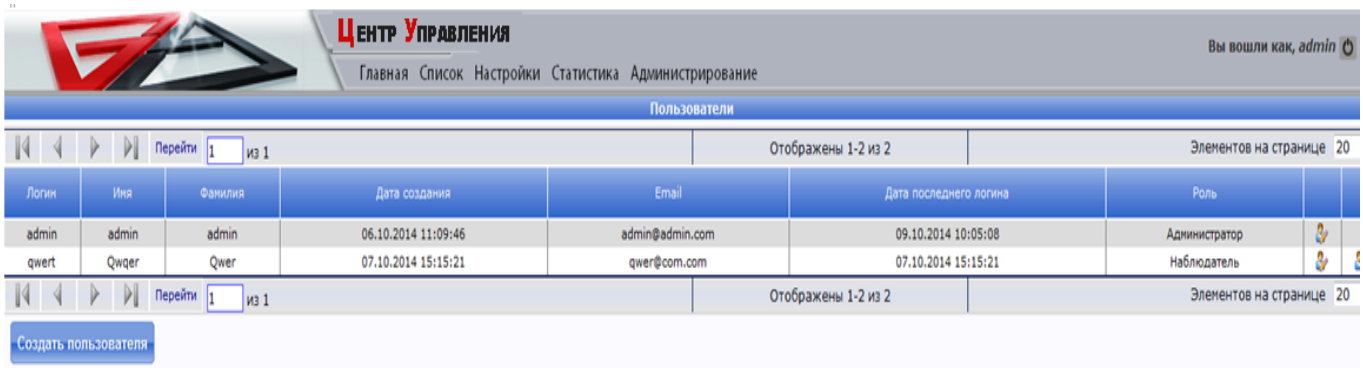

Рис. 108

4.11.1.3. Удаление пользователя

Создание, редактирование, удаление пользователя может быть произведено только при работе в модуле «Центр Управления» под учетной записью с правами администратора.

Для удаления пользователя необходимо нажать на кнопку удаления, которая располагается рядом с кнопкой редактирования (см. п. 4.11.1.2).

4.11.1.4. Изменение личной информации и пароля

Web-интерфейс модуля «Центр Управления» предоставляет возможность пользователю изменять свою личную информацию и пароль. Для этого необходимо в меню **Настройки** нажать на ссылку **Основные**, появится страница настроек (рис. 109).

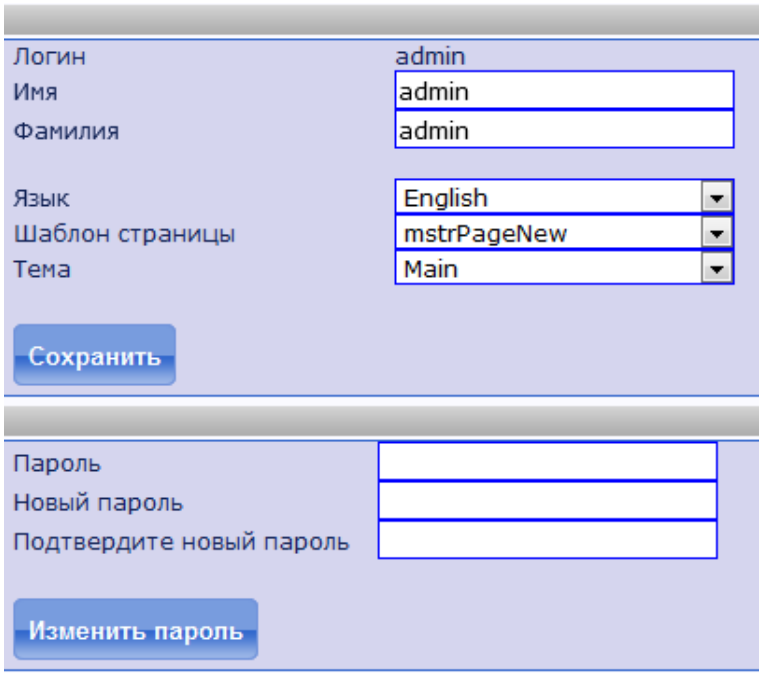

Рис. 109

Для изменения имени и фамилии надо внести соответствующие данные в поля **Имя** и **Фамилия** и нажать на ссылку **Сохранить**.

Примечание. Логин и адрес электронной почты после регистрации изменить нельзя. Вместо этого надо создать нового пользователя с новым логином.

Для изменения пароля надо заполнить форму **Смена пароля**, введя в поле **Пароль** текущий пароль, а в поля **Новый пароль** и **Подтвердите новый пароль** - новый пароль. После заполнения надо нажать ссылку **Изменить пароль**.

Примечание. Изменение личных данных и пароля других пользователей невозможно.

4.11.2. Настройка внешнего вида

Web-интерфейс модуля «Центр Управления» является гибко настраиваемым, поддерживает различные шаблоны оформления, цветовые схемы и темы.

Настройки цветов событий распространяются на всех пользователей, а все остальные настройки внешнего вида – для текущего пользователя.

Настройки внешнего вида сохраняются и действуют при последующих обращениях к модулю «Центр Управления».

4.11.2.1. Настройка шаблона оформления

Существует два варианта оформления и взаимного расположения элементов на страницах модуля «Центр Управления». Один из них с блоком навигации слева, другой – сверху.

Для выбора шаблона оформления необходимо открыть страницу основных настроек, для этого в меню **Настройки** нажать на ссылку **Основные**.

Шаблон оформления задается в выпадающем списке **Шаблон страницы**.

После выбора необходимого шаблона надо нажать на ссылку **Сохранить**. Настройки применяются немедленно.

4.11.2.2. Настройка темы оформления

Модуль «Центр Управления» поддерживает смену тем оформления страниц – набора цветовых решений.

Для выбора темы оформления необходимо открыть страницу основных настроек, для этого в меню **Настройки** нажать на ссылку **Основные**.

Тема задается в выпадающем списке **Тема**.

После выбора необходимой цветовой темы надо нажать на ссылку **Сохранить**. Настройки применяются немедленно.

4.11.2.3. Настройка цветового оформления событий

Примечание. Данная настройка действует для всех пользователей модуля «Центр Управления».

Модуль «Центр Управления» позволяет применять цветовую раскраску для различных типов событий, отображаемых на странице **События** в меню **Список событий** (рис. 110).

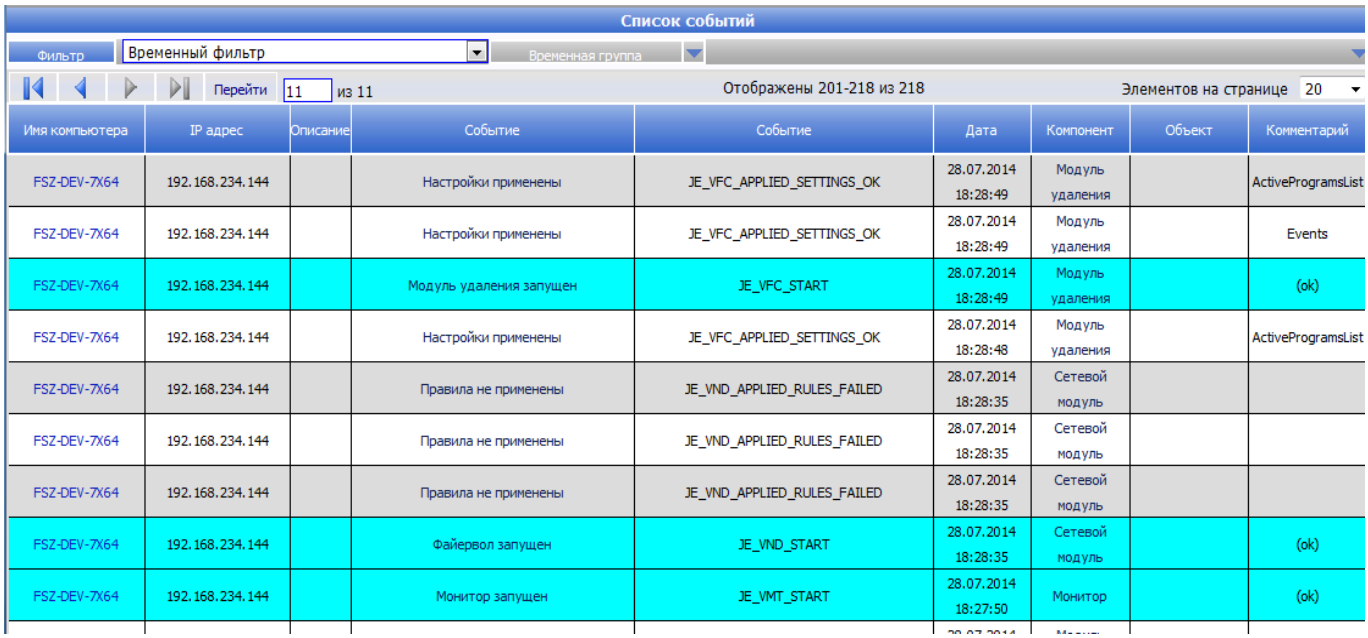

Рис. 110

Для изменения цветовой схемы событий надо в меню **Настройки** нажать на ссылку **Дополнительно**, на открывшейся форме выбрать **Цвета событий** (рис. 111).

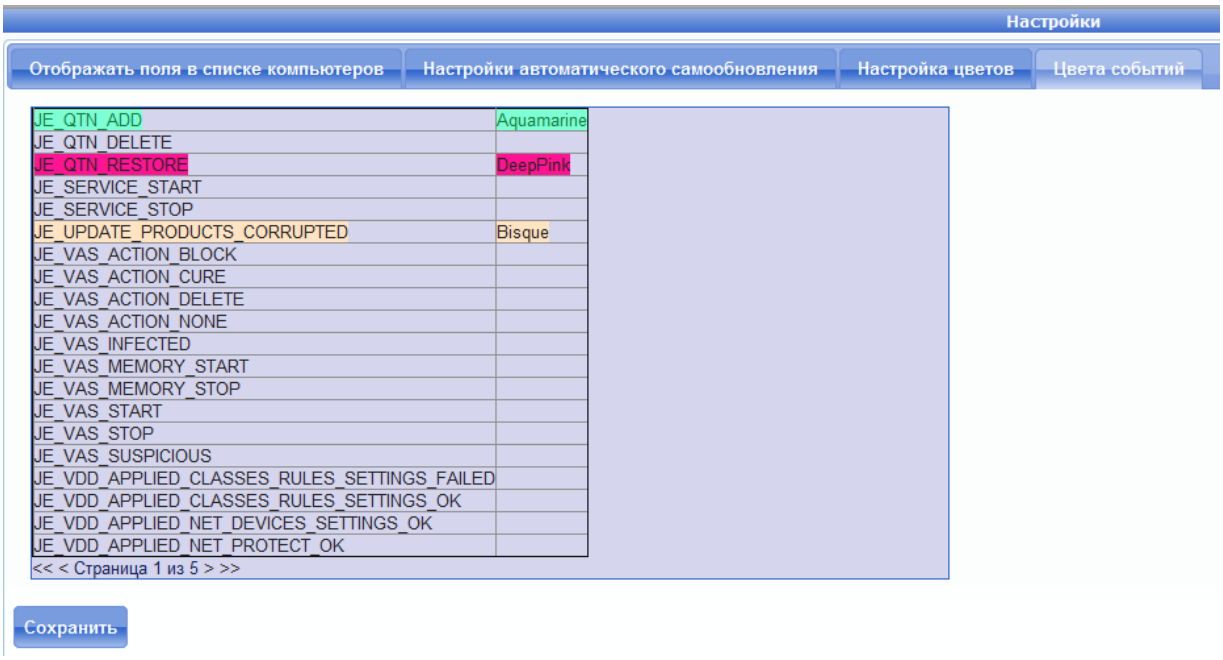

Рис. 111

Список **Цветов событий**, зарегистрированных в системе, выводится в виде многостраничной таблицы. Перемещение по страницам происходит по стандартному алгоритму: ссылки > и < показывают следующую и предыдущую страницы соответственно, << и >> - первую и последнюю.

Для изменения цвета того или иного события (рис. 112), надо нажать на его название, в появившемся выпадающем списке выбрать нужный цвет и нажать **Обновить**.

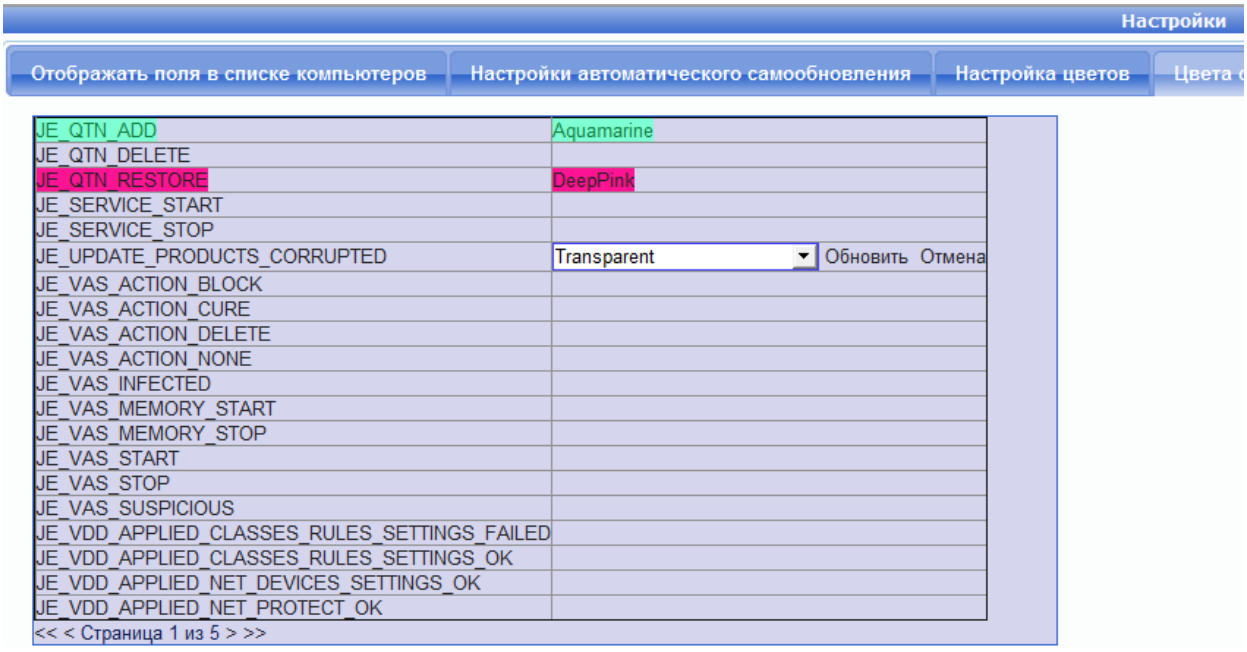

Рис. 112

Настройки применяются немедленно, результаты можно увидеть в меню **Список** на странице **События**.

4.11.2.4. Настройка отображения столбцов в списке компьютеров

Модуль «Центр Управления» предоставляет возможность включать/выключать отображение столбцов в списке компьютеров.

Для выбора столбцов, которые будут отображаться в списке компьютеров, необходимо в меню **Настройки** нажать на ссылку **Дополнительно**. Поля (рис. 113), которые должны отображаться в списке компьютеров, необходимо отметить флажками.

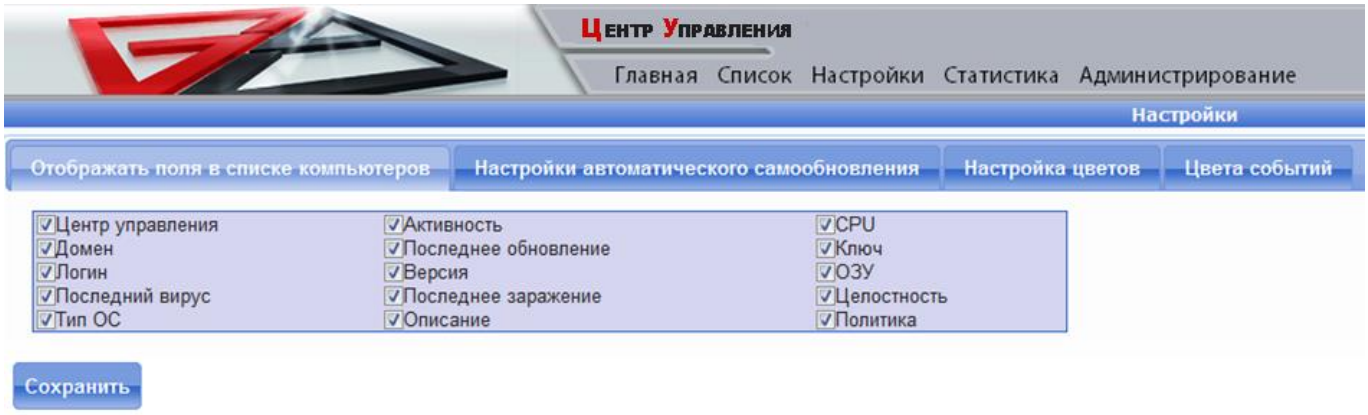

Рис. 113

Для применения настроек необходимо нажать на ссылку **Сохранить**.

4.11.2.5. Настройки автоматического асинхронного обновления содержимого

При просмотре табличных списков при помощи web-интерфейса для получения наиболее актуальных данных надо принудительно обновлять страницу в браузере. Модуль «Центр Управления» поддерживает автоматическое обновление содержимого таблиц через определенный интервал без необходимости обновления всей страницы (для этого используется технология асинхронных java-скриптов).

Примечание. Данная возможность внедрена только для двух наиболее часто обновляемых списков: событий и задач.

Чтобы включить асинхронное обновление содержимого, необходимо на странице с соответствующим списком отметить флажок **Включить автообновление содержимого**. Настройка применяется немедленно и сохраняется для данного пользователя.

Для настройки интервалов обновления необходимо в меню **Настройки** нажать на ссылку **Дополнительно**. Интервалы задаются на форме **Настройки автоматического обновления содержимого** в полях для ввода **События** и **Задачи**, отдельно для каждого из списков.

Примечание. Автоматическое обновление содержимого создает дополнительную нагрузку как на сервер баз данных, так и на браузер. Не рекомендуется сильно снижать интервал обновления.

Для применения настроек необходимо нажать на ссылку **Сохранить**.

4.11.3. Настройка уведомлений

Модуль «Центр Управления» предоставляет возможность уведомления уполномоченных лиц при регистрации того или иного события. Существуют три типа уведомлений:

1) по электронной почте;
2) по jabber;
3) при помощи net send.

Первые два типа уведомлений требуют наличия сервера, предоставляющего соответствующую услугу.

Примечание. Рекомендуется для уведомлений использовать локальные сервера: почтовый и jabber.

Для каждого из зарегистрированных типов событий можно назначить индивидуальные настройки уведомлений – адресатов, текст и т.п.

Примечание. Данные настройки могут быть произведены только при работе в модуле «Центр Управления» под учетной записью с правами администратора.

Для изменения настроек уведомлений надо в меню **Администрирование** нажать на ссылку **Уведомления**.

Для включения событий, зарегистрированных в системе, надо отметить флажок **Использовать интеллектуальную обработку** (рис. 114).

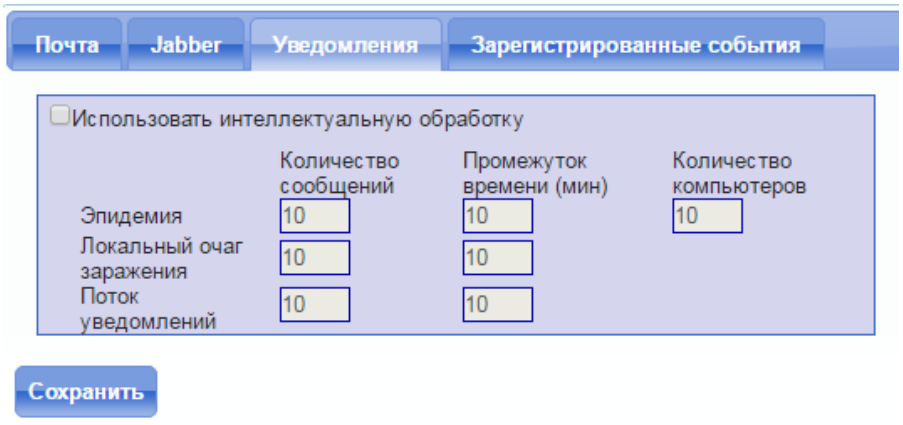

Рис. 114

На вкладке **Уведомления** (рис. 114) представлены события, которые наступают при определенных условиях:

1) эпидемия – пришло заданное количество событий об обнаружении заражения за определенное время с определенного количества компьютеров;

2) локальный очаг заражения – пришло заданное количество событий об обнаружении заражения за определенное время с одного компьютера:

3) поток уведомлений – пришло заданное количество событий за определенное время с одного компьютера.

Для применения настроек необходимо нажать на ссылку **Сохранить.**

4.11.3.1. Выбор события, для которого будет производиться настройка уведомлений

На вкладке **Зарегистрированные события**, представленной на рис. 115, выводится многостраничный список событий, зарегистрированных в системе.

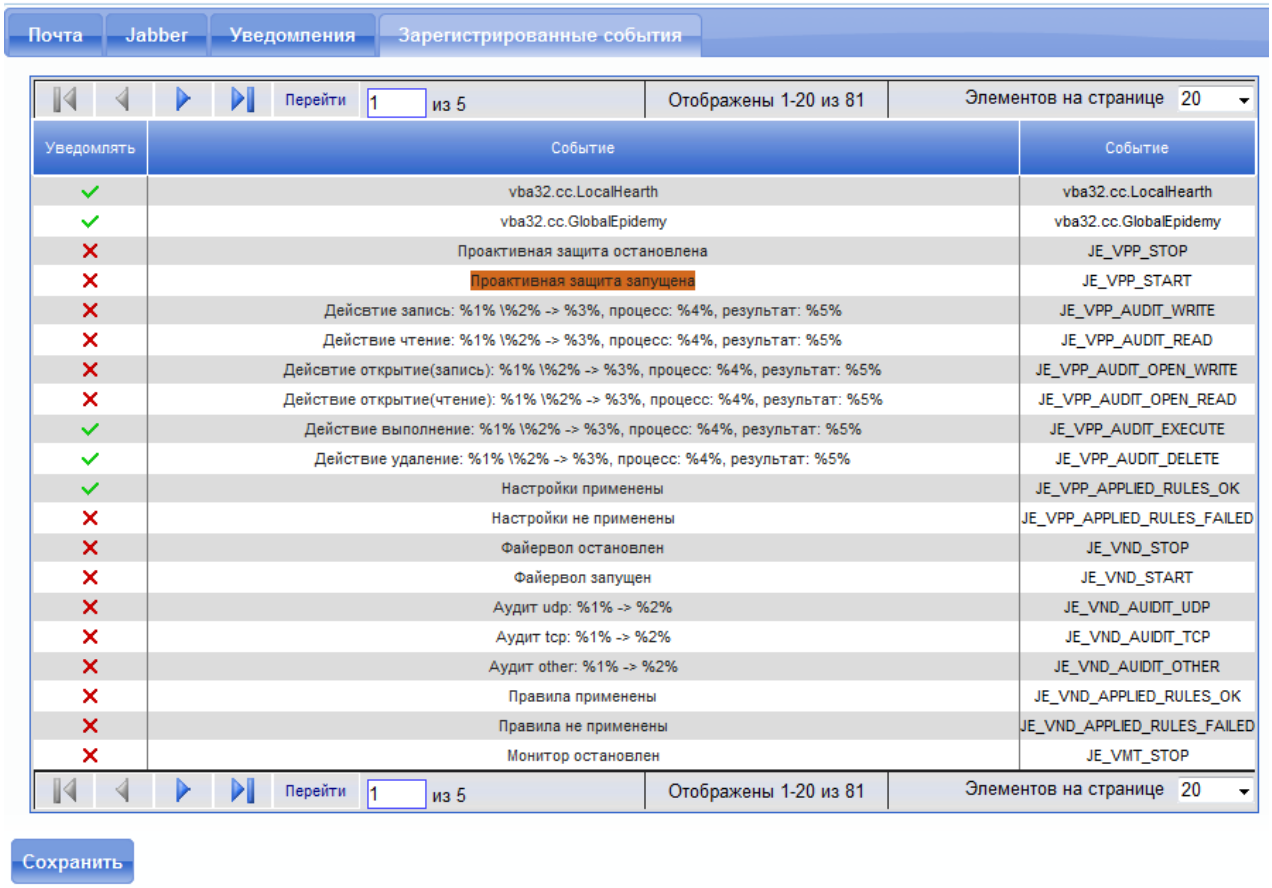

Рис. 115

Слева от имени события, в колонке **Уведомлять** в виде иконки представлена настройка – будут ли при регистрации соответствующих событий рассылаться уведомления. Если в этой колонке стоит знак выбора – уведомления будут отправлены. Для изменения настройки надо нажать на иконку, и знак выбора изменится на .

Установив настройку **Уведомлять**, надо включить необходимые типы уведомлений для данного события и сделать необходимые настройки.

Для настройки уведомлений индивидуально для каждого события, надо в списке (рис. 116), нажать на имя этого события – справа от списка форма автоматически получит заголовок в виде имени этого события.

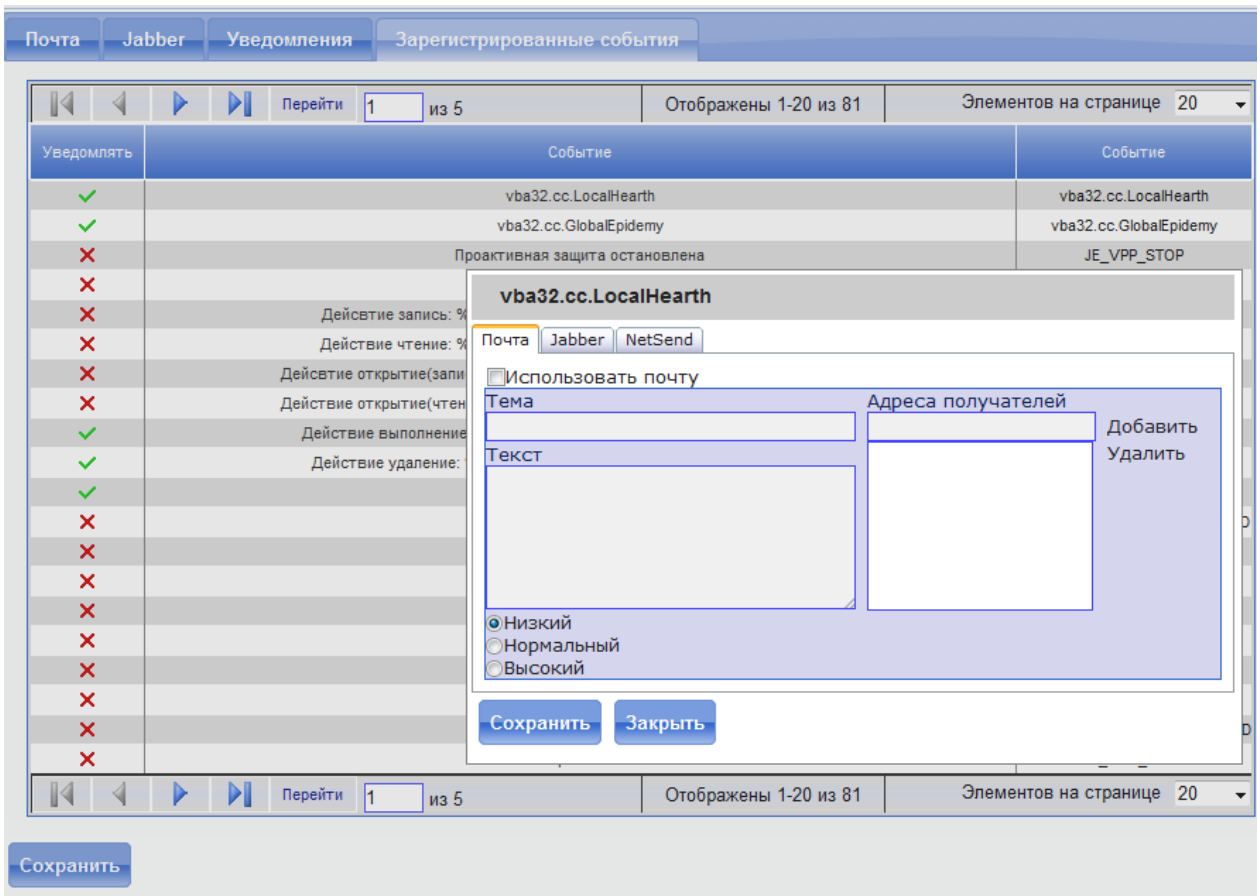

Рис. 116

4.11.3.2. Настройка уведомлений по электронной почте

Чтобы иметь возможность отправлять уведомления по электронной почте, необходимо указать почтовый сервер. Для этого служит форма **Почта** (рис. 117) страницы **Настройки сервиса уведомлений**.

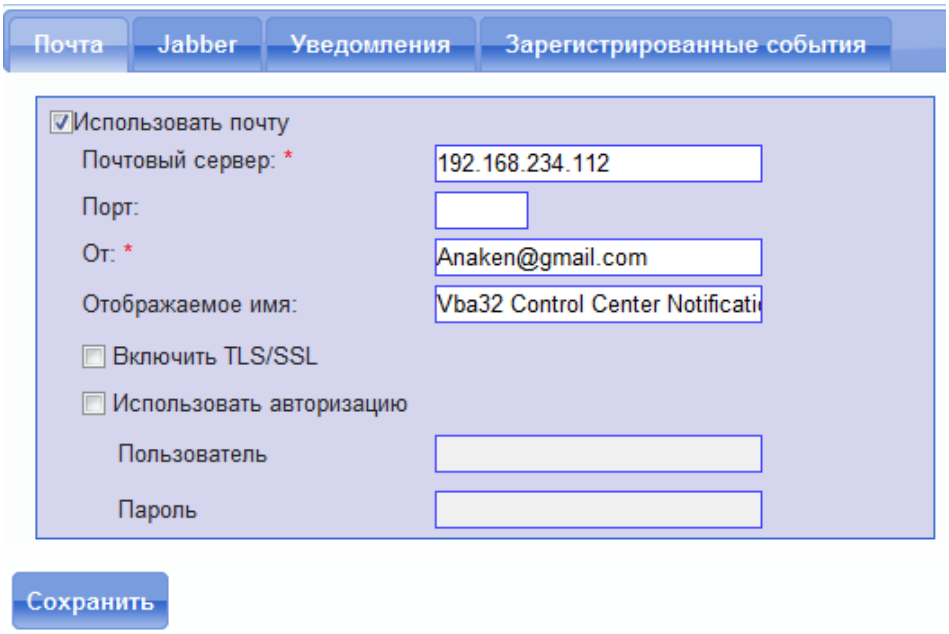

Рис. 117

В поле **Почтовый сервер** необходимо ввести IP-адрес сервера, который будет использован для отправки писем. Как правило, стоит использовать локальный почтовый сервер организации.

В поле **От** надо ввести имя почтового ящика, от которого будут рассылаться письма.

Примечание. Некоторые почтовые сервера требуют указать реально существующий почтовый ящик.

В поле **Отображаемое имя** необходимо ввести имя, которое будет отображаться в почтовом клиенте вместо адреса электронной почты, указанного в поле **От**.

При необходимости задать данные для авторизации на почтовом сервере, Порт и включить TLS/SSL.

Для применения настроек необходимо нажать на ссылку **Сохранить**.

Для настройки содержимого и получателей уведомления необходимо выбрать событие (описано в пункте **Выбор события, для которого будет производиться настройка уведомлений**), и в форме справа от списка событий нажать на ссылку **Почта**.

Для включения почтового уведомления для данного события надо отметить флажок **Использовать почту**, представленный на рис. 118.

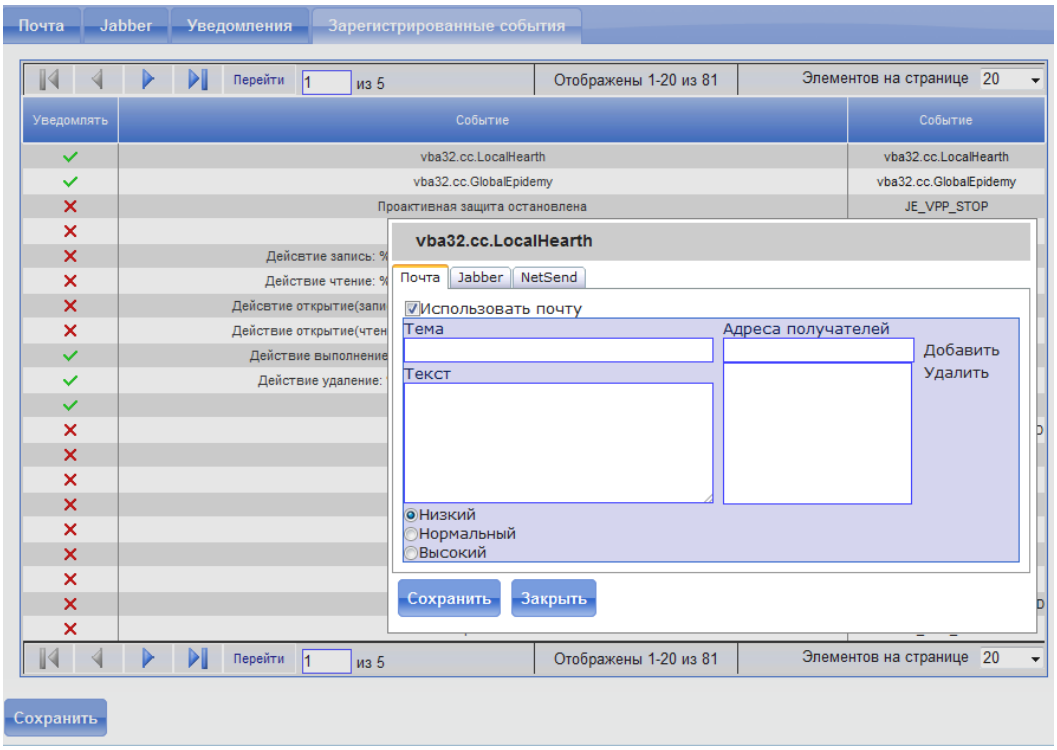

Рис. 118

Чтобы добавить адресата уведомления, надо ввести адрес его электронной почты в поле **Адреса получателей** и нажать ссылку **Добавить**. В списке должен добавиться введенный адрес. Для удаления адресата надо выделить его в списке и нажать ссылку **Удалить**.

В поля **Тема** и **Текст** надо ввести тему и текст почтового уведомления соответственно, при этом можно использовать подстановочные макросы (подробнее описано в пункте **Подстановочные макросы в теме и тексте уведомления**).

Переключателем внизу страницы можно установить важность сообщения.

Для применения настроек необходимо нажать на ссылку **Сохранить**.

4.11.3.3. Настройка уведомлений по jabber

Чтобы иметь возможность отправлять уведомления по jabber, необходимо указать сервер и учетную запись jabber. Для этого служит форма **Настройки Jabber** (рис. 119) страницы **Настройки сервиса уведомлений**.

В поле **Сервер Jabber** необходимо ввести имя сервера, который будет использован для отправки сообщений.

Примечание. Можно использовать внешние серверы, например, jabber.ru или jabber.org. Однако рекомендуется установить сервер jabber локально (например, ejabberd).

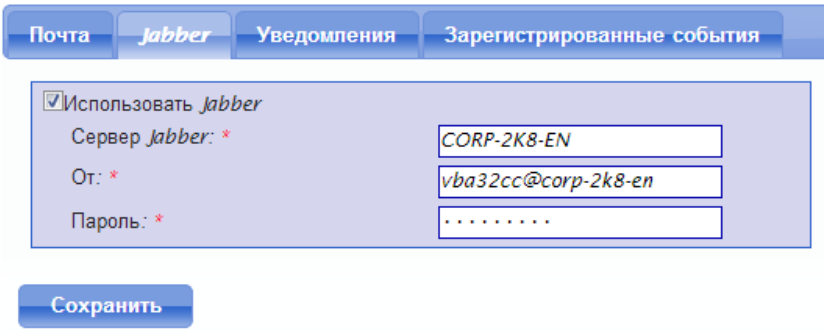

Рис. 119

В поле **От** надо ввести идентификатор учетной записи JID, от имени которого будут рассылаться письма. Данную учетную запись необходимо заранее зарегистрировать, используя сервисы сервера.

В поле **Пароль** необходимо ввести пароль для учетной записи, указанной в поле **От**.

Для применения настроек необходимо нажать на ссылку **Сохранить**.

Для настройки содержимого и получателей уведомления необходимо выбрать событие (описано в пункте **Выбор события, для которого будет производиться настройка уведомлений**), и в форме (рис. 120) справа от списка событий нажать на ссылку **Jabber**.

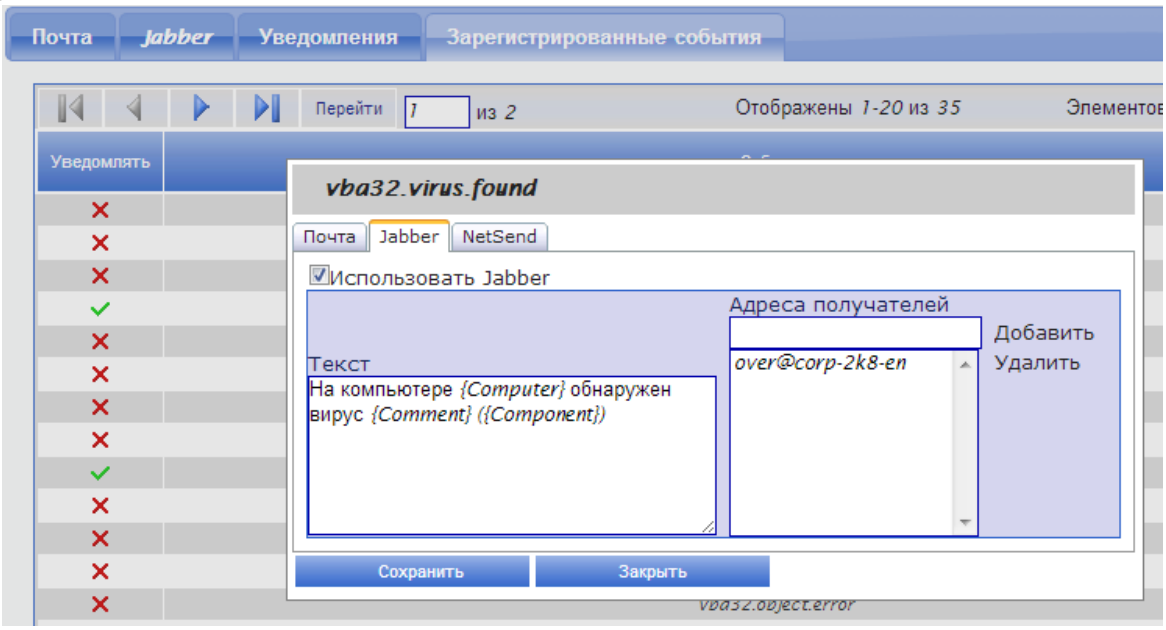

Рис. 120

Для включения jabber-уведомления для данного события надо отметить флажок **Использовать Jabber**.

Чтобы добавить адресата уведомления, надо ввести его учетную запись (JID) в поле **Адреса получателей** и нажать ссылку **Добавить**. В списке должен добавиться введенный адрес. Для удаления адресата надо выделить его в списке и нажать ссылку **Удалить**.

В поле **Текст** надо ввести текст уведомления, при этом можно использовать подстановочные макросы (подробнее описано в пункте **Подстановочные макросы в теме и тексте уведомления**).

Для применения настроек необходимо нажать на ссылку **Сохранить**.

4.11.3.4. Настройка уведомлений при помощи net send

Примечание. Для корректной работы уведомлений **net send** на сервере и компьютере получателя должна быть запущена служба **Служба сообщений**. Данная функциональность не поддерживается ОС Windows Vista.

Для настройки содержимого и получателей уведомления необходимо выбрать событие (описано в пункте **Выбор события, для которого будет производиться настройка уведомлений**), и в форме (рис. 121) справа от списка событий нажать на ссылку **NetSend**.

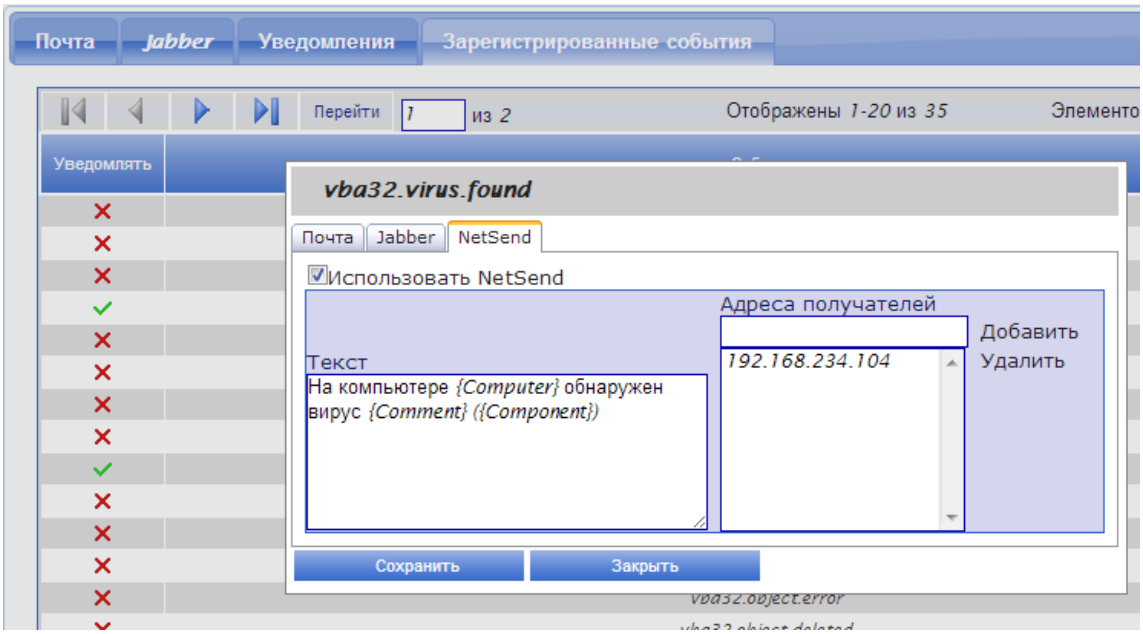

Рис. 121

Для включения уведомления по **net send** для данного события надо отметить флажок **Использовать NetSend**.

Чтобы добавить адресата уведомления, надо ввести имя или IP-адрес его компьютера в поле **Адреса получателей** и нажать ссылку **Добавить**. В списке должен добавиться введенный адрес. Для удаления адресата надо выделить его в списке и нажать ссылку **Удалить**.

В поле **Текст** надо ввести текст уведомления, при этом можно использовать подстановочные макросы (подробнее описано в пункте **Подстановочные макросы в теме и тексте уведомления**).

Для применения настроек необходимо нажать на ссылку **Сохранить**.

4.11.3.5. Подстановочные макросы в теме и тексте уведомления

При формировании текста и/или темы уведомления можно использовать подстановочные макросы, значения которых будут подставляться из конкретного события.

Существуют следующие макросы:

1) {Computer} – имя компьютера, на котором произошло событие;
2) {IPAddress} – IP-адрес компьютера, на котором произошло событие;
3) {EventName} – имя произошедшего события;
4) {EventTime} – дата и время наступления события;
5) {Component} – компонент, сгенерировавший событие;
6) {Object} – объект, с которым произошло событие;
7) {Comment} – комментарий к событию.

Например, уведомление об обнаружении вируса может иметь следующий вид:

Примечание. На компьютере {Computer} обнаружен вирус {Comment} в {Object} ({Component})

4.11.4. Настройка обслуживания БД

Хранилищем данных модуля «Центр Управления» является его БД. С течением времени база может значительно увеличиться в размерах, снижая эффективность работы модуля «Центр Управления».

Примечание. Необходимо следить за размером БД модуля «Центр Управления». Чем больше ее размер, тем больше требования к аппаратным ресурсам сервера БД. Настоятельно рекомендуется периодически делать резервные копии БД.

Данные об устаревших событиях можно удалить из БД. Очистка БД от событий производится сервисом периодического обслуживания в автоматическом режиме. Кроме того, имеется возможность настроить модуль «Центр Управления» таким образом, чтобы события определенных типов никогда не удалялись из БД (например, события об обнаруженных вредоносных программах или другие критические события).

Примечание. Данные настройки могут быть произведены только при работе в модуле «Центр Управления» под учетной записью с правами администратора.

Для настройки обслуживания БД необходимо в меню **Администрирование** нажать ссылку **Обслуживание**. На вкладке **Настройки** (рис. 122) ввести в поле **Удалять события старше (дней)** количество дней, по истечению которых события будут удалены из БД, в поле **Удалять задачи старше (дней)** количество дней, по истечению которых задачи будут удалены из БД, в поле **Удалять компьютеры с активностью старше (дней)** количество дней, по истечению которых события на

компьютерах будут удалены из БД. Значение, установленное в поле **Кол-во неудачных попыток входа,** задает максимальное допустимое число неудачных попыток входа в модуль «Центр Управления».

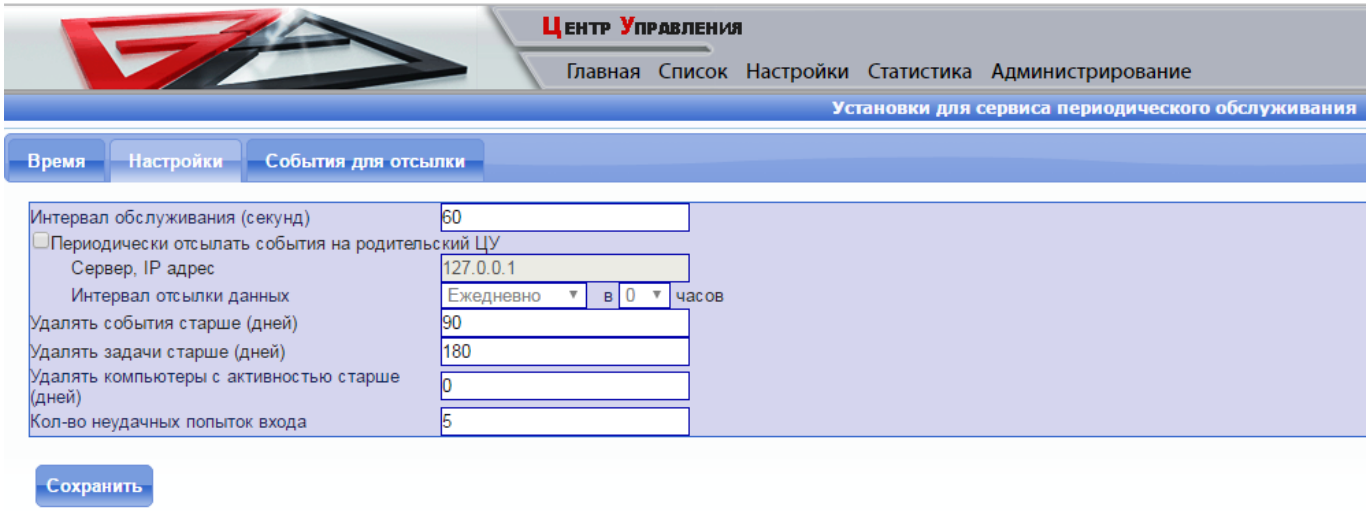

Рис. 122

На этой же форме можно настроить период, по истечении которого сервис производит проверку БД на предмет очистки событий и обновления состояния задач. Для этого надо ввести в поле **Интервал обслуживания (секунд)** новое значение периода.

Для применения настроек необходимо нажать на ссылку **Сохранить**.

Настройка событий, которые никогда не будут удалены из БД, производится на этой же странице **Установки для сервиса периодического обслуживания**. На вкладке **События для отсылки** (рис. 123) выводится многостраничный список событий, зарегистрированных в системе.

Слева от имени события, в колонке **Не удалять** в виде иконки представлена настройка – будут ли соответствующие события оставаться в БД независимо от времени их регистрации. Если в этой колонке стоит результат выбора – событие не будет удалено из БД при ее периодическом обслуживании. Для изменения настройки надо нажать на иконку, и та изменится на противоположную.

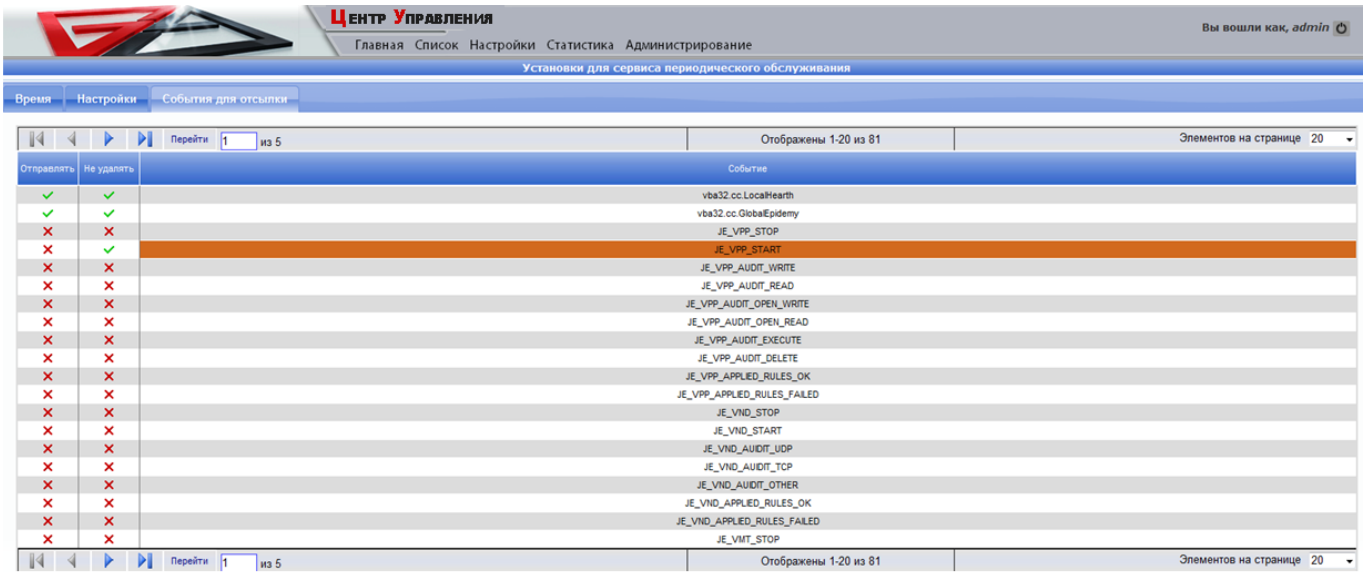

Рис. 123

Изменения вступают в силу немедленно.

4.11.5. Настройка обновления

Модуль «Центр Управления» обладает возможностью обновления компонентов стандартным образом.

Примечание. Данные настройки могут быть произведены только при работе в модуле «Центр Управления» под учетной записью с правами администратора.

Для изменения настроек обновления надо в меню **Администрирование** нажать на ссылку **Обновление** (рис. 124).

Сам процесс обновления инициируется нажатием на кнопку **Обновить**, статус обновления отображается на этой же странице. В случае необходимости отмены обновления нажать кнопку **Отмена**.

Примечание. Обновление с сетевых дисков (mapping) не поддерживается.

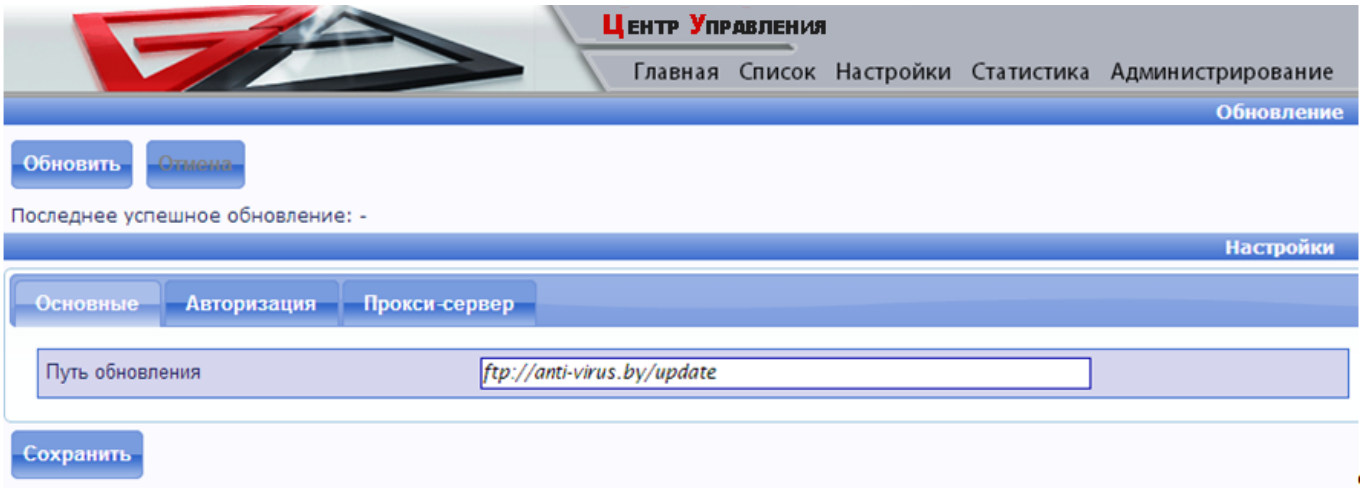

Рис. 124

4.11.5.1. Обновление из локального каталога

В случае если обновление производится из локального каталога, необходимо ввести путь к этому каталогу в поле **Путь обновления** и снять флажки **Использовать прокси-сервер**, **Использовать авторизацию** на соответствующих вкладках (рис. 125, 126). Для применения настроек необходимо нажать на ссылку **Сохранить**.

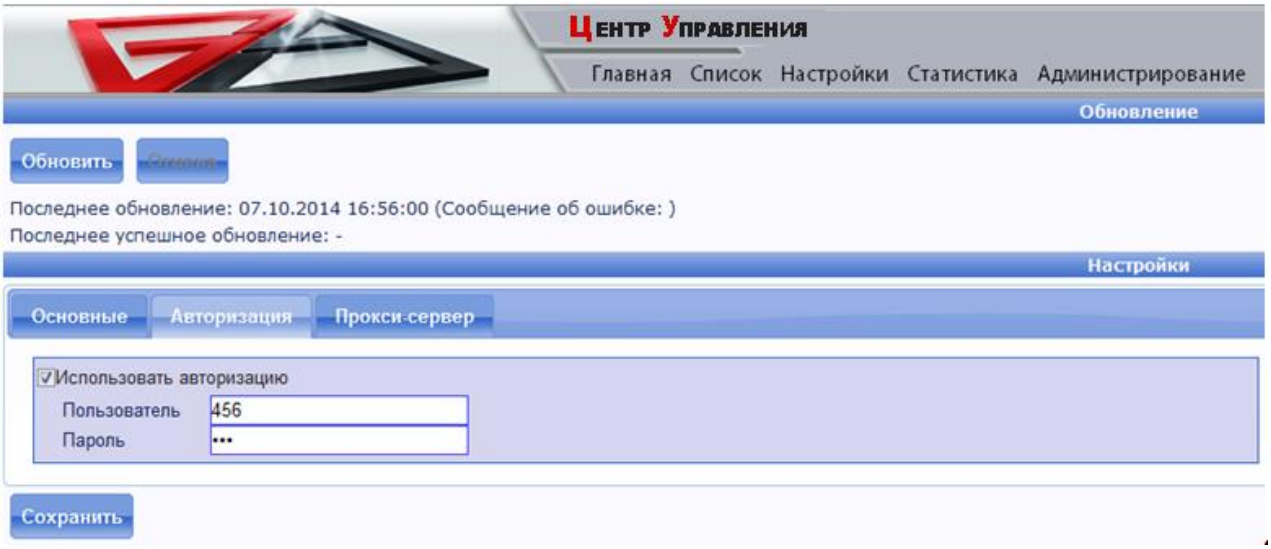

Рис. 125

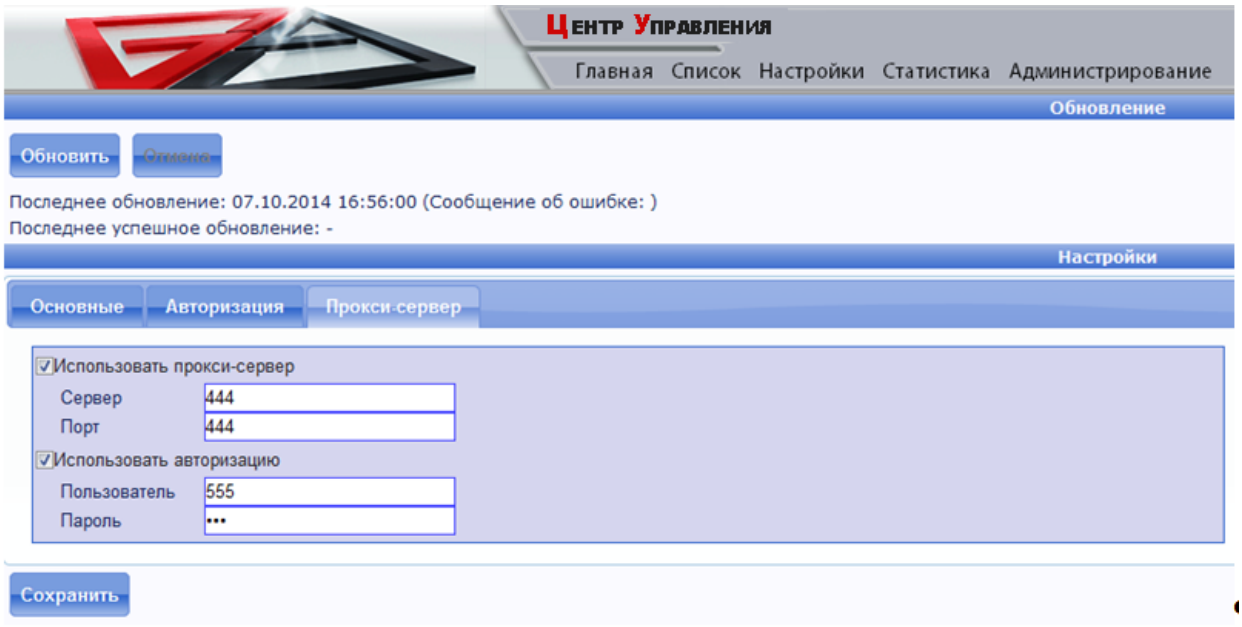

Рис. 126

4.11.5.2. Обновление из сетевого каталога

Сервис обновлений, входящий в состав модуля «Центр Управления», работает от учетной записи LOCAL_SYSTEM и не имеет никаких прав для доступа по сети,

поэтому обновление из сетевого каталога требует ввода дополнительных настроек авторизации.

В случае если компьютер, на котором установлен модуль «Центр Управления», и компьютер, с которого производится обновление, входят в один домен, необходимо установить флажок **Использовать авторизацию** и ввести имя доменного пользователя и пароль в соответствующие поля вкладки **Авторизация**.

Примечание. Данный пользователь должен иметь право чтения из сетевого каталога обновлений. Как правило, достаточно ввести реквизиты своего доменного пользователя.

Для применения настроек необходимо нажать на ссылку **Сохранить**.

4.11.5.3. Обновление по ftp/http с использованием прокси-сервера

Если обновление производится с ftp или http сервера, доступ к которому осуществляется через прокси, то необходимо установить флажок **Использовать прокси-сервер** на соответствующей вкладке и ввести данные о прокси в поля **Сервер** и **Порт** формы. Если прокси-сервер требует авторизации, необходимо установить флажок **Использовать авторизацию** и ввести данные о пользователе прокси в соответствующие поля.

Для применения настроек необходимо нажать на ссылку **Сохранить**.

4.11.6. Экспорт и импорт пользовательских настроек

Модуль «Центр Управления» предоставляет возможность сохранения всех или части пользовательских настроек (фильтров по спискам, созданных задач) в файл. Такая возможность может потребоваться, например, при переустановке модуля «Центр Управления» или необходимости создать нового пользователя с такими же настройками, как у уже существующего.

Примечание. Настройки внешнего вида не экспортируются.

4.11.6.1. Экспорт настроек в файл

Для сохранения настроек текущего пользователя в файл надо в меню **Настройки** нажать на ссылку **Экспорт/Импорт**. На появившейся форме надо флажками выбрать те части настроек, которые необходимо экспортировать (фильтры компьютеров, фильтры событий, фильтры компонентов, фильтры процессов, фильтры для задач подключения, фильтры задач, пользовательские задачи) и нажать на ссылку **Экспорт**. В появившемся окне надо выбрать путь, по которому будет сохранен файл с настройками, и нажать на кнопку **Сохранить**.

Имя файла с настройками, предлагаемое по умолчанию, - VBA32CC_settings_*login*.xml, где вместо *login* подставляется реальное имя учетной записи пользователя.

Примечание. Файл с настройками будет сохранен на клиентском компьютере, где web-интерфейс открыт в браузере.

4.11.6.2. Импорт настроек

Чтобы импортировать настройки, необходимо иметь файл с экспортированными настройками, полученный в ходе выполнения предыдущего пункта.

Для импорта всех настроек, сохраненных в данный файл, необходимо в меню **Настройки** на странице **Экспорт/Импорт** ввести в поле ввода путь к файлу с настройками (или воспользоваться стандартным диалогом выбора файлов, нажав на кнопку **Обзор**). Выбрать те части настроек, которые необходимо импортировать, после чего нажать на ссылку **Импорт**.

4.11.6.3. Удаление всех пользовательских настроек

Чтобы удалить некоторые из пользовательских настроек (фильтры компьютеров, фильтры событий, фильтры компонентов, фильтры процессов, фильтры задач, фильтры для задач подключения, пользовательские задачи), необходимо на странице **Экспорт/Импорт** отметить флажками соответствующие пункты и нажать на ссылку **Удалить**.

4.12. Использование групп

Для удобства работы и сокращения затраченного времени на однотипные действия в модуль «Центр Управления» была добавлена поддержка групп.

Поддерживаются вложенные группы (максимальная глубина вложенности равна 5).

4.12.1. Формирование групп

Формирование групп происходит на странице **Группы** в меню **Администрирование** (рис. 127).

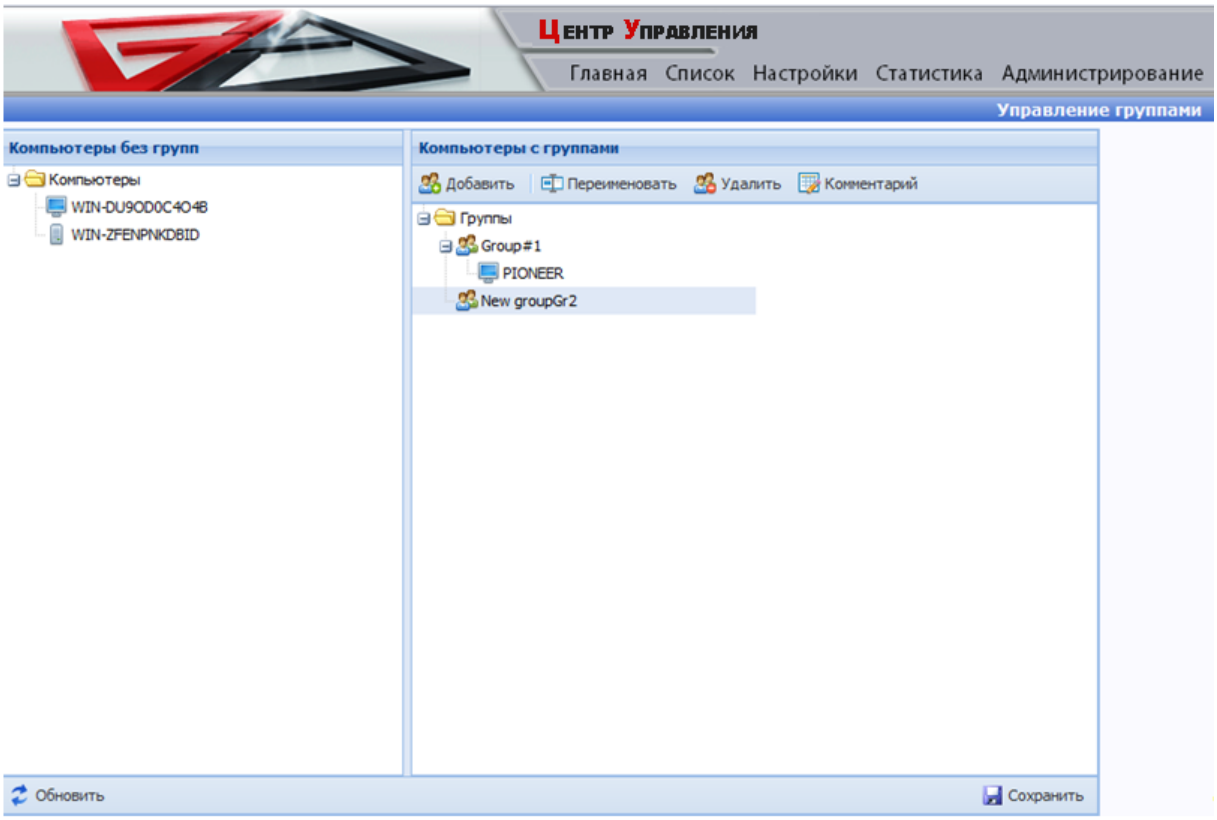

Рис. 127

Администрирование групп производится в правой панели: доступны операции добавления, удаления, переименования группы и добавление комментария (все эти действия доступны в панели инструментов либо в контекстном меню группы).

Для назначения компьютера в группу необходимо сделать следующие действия:

1) создать группу;
2) выбрать в левой панели компьютер;
3) перетащить иконку с компьютером в папку с именем нужной группы в правой панели;
4) после завершения формирования групп нажать **Сохранить** (рис. 128).

Рис. 128

Примечание. Рабочие станции и сервера отображаются с помощью различных иконок. При наведении на иконку компьютера можно получить более подробную информацию о нем.

Если необходимо отменить последние действия, нажмите **Обновить** до нажатия кнопки **Сохранить**.

Компьютер может находиться только в одной группе.

4.12.2. Выдача задач группам компьютеров

Выдача задач группам компьютеров производится на странице **Группы** раздела **Список**.

Задачи группам выдаются так же, как и компьютерам на странице **Компьютеры** (см. п. 4.10.2). Результат выполнения задачи находится на странице **Задачи**.

4.13. Использование политик антивирусного комплекса

Политики антивирусного комплекса предназначены для принудительной установки на рабочей станции определенных настроек антивирусного комплекса.

Доступна настройка следующих разделов:

1) Диспетчер;
2) Монитор;
3) Карантин;
4) События журнала модуля управления доступом.

4.13.1. Создание политики

Для создания политики антивирусного комплекса необходимо перейти на страницу **Политики** в меню **Администрирование**, затем нажать на кнопку **Создать**. В поле для ввода **Имя** задается уникальное имя создаваемой политики.

Выбор необходимых флажков позволяет задействовать специфические настройки разделов антивирусного комплекса, доступных в политике. Их настройка осуществляется во вкладках:

1) Настроить Диспетчер;
2) Настроить Монитор;
3) Настроить Сканер;
4) Настроить Карантин
5) Параметры Диспетчера, Монитора и Защиты USB;
6) Настроить Проактивная защита;
7) Настроить Планировщик;
8) Настроить Межсетевой экран;
9) Настроить Проверка целостности;
10) Настроить Удаление файлов;
11) События журнала.

Пример вкладки **Настроить Диспетчер** приведен на рисунке 129.

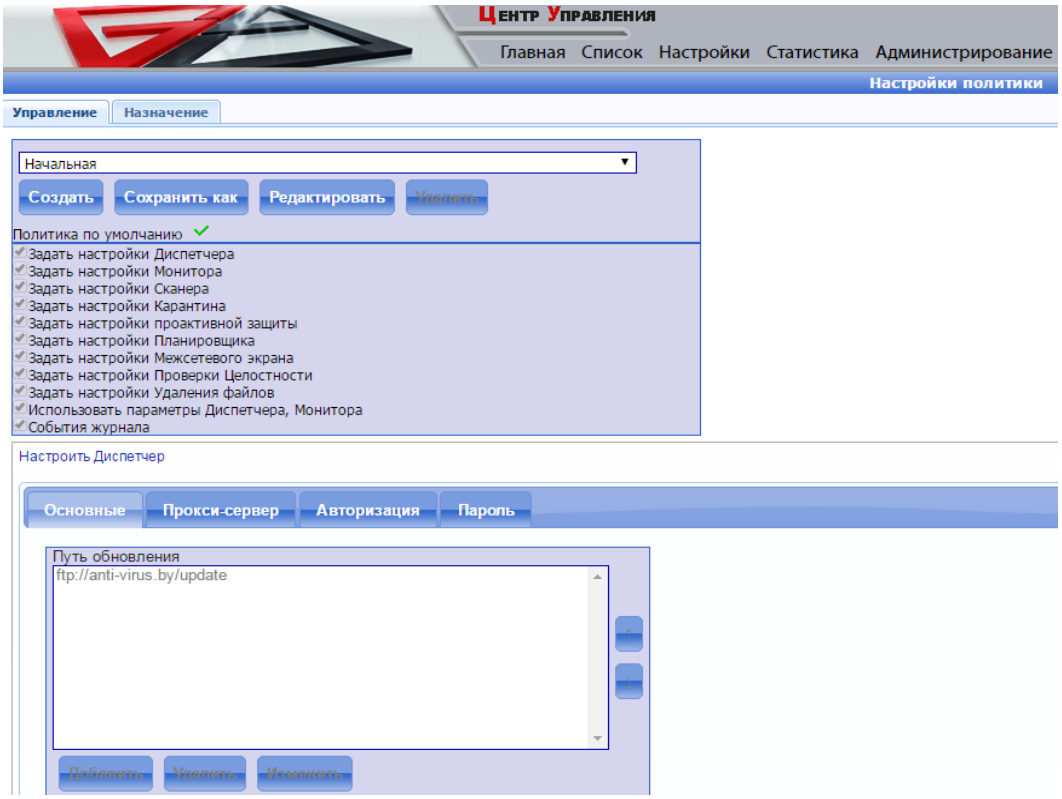

Рис. 129

Пример вкладки **Настроить Монитор** приведен на рисунке 130.

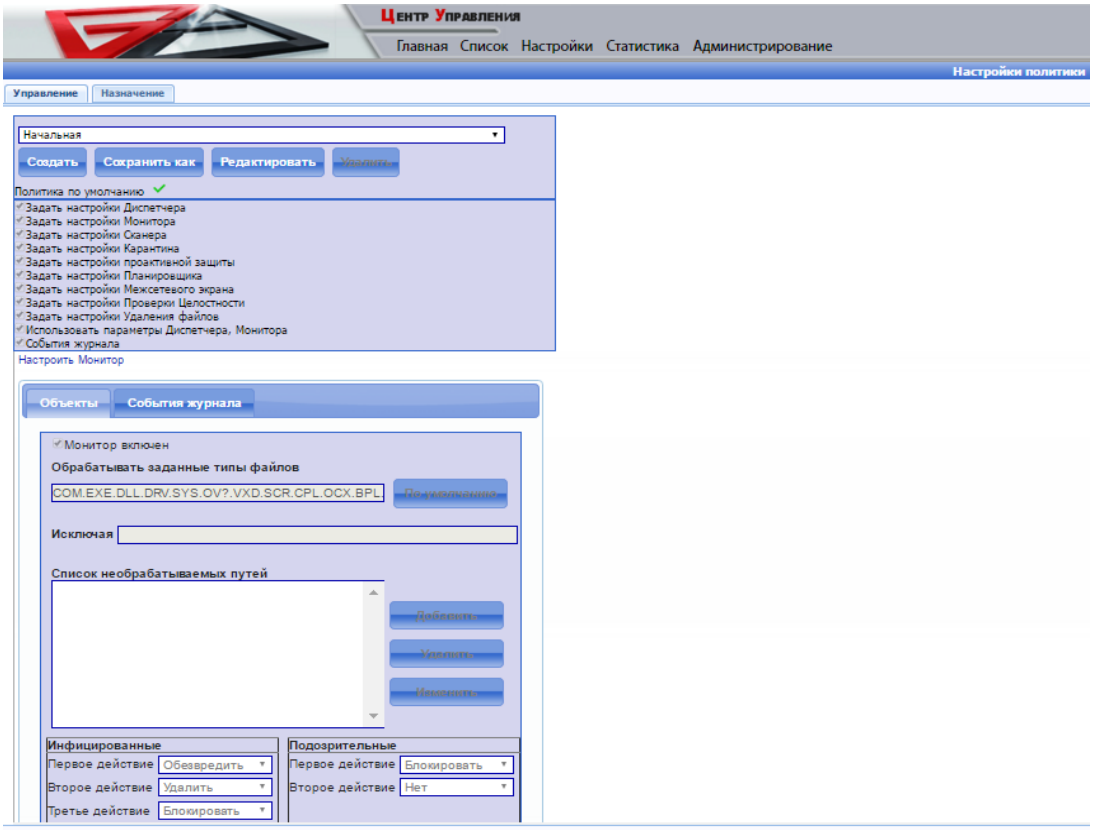

Рис. 130

Пример вкладки **Настроить Карантин** приведен на рисунке 131.

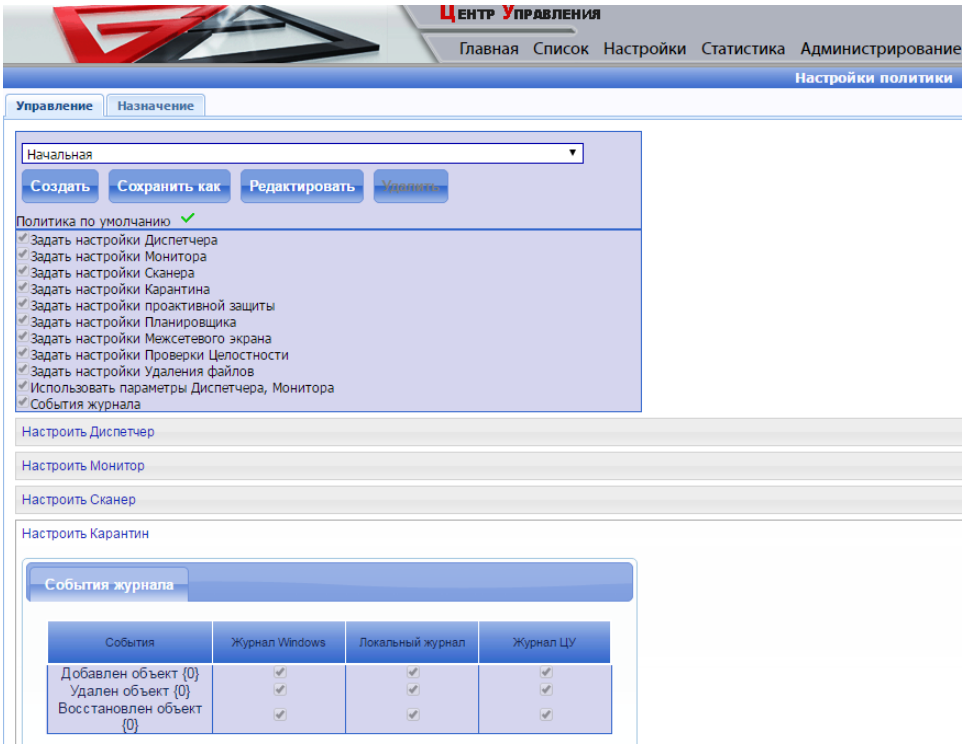

Рис. 131

Пример вкладки **Параметры Диспетчера, монитора и защиты USB** приведен на рисунке 132.

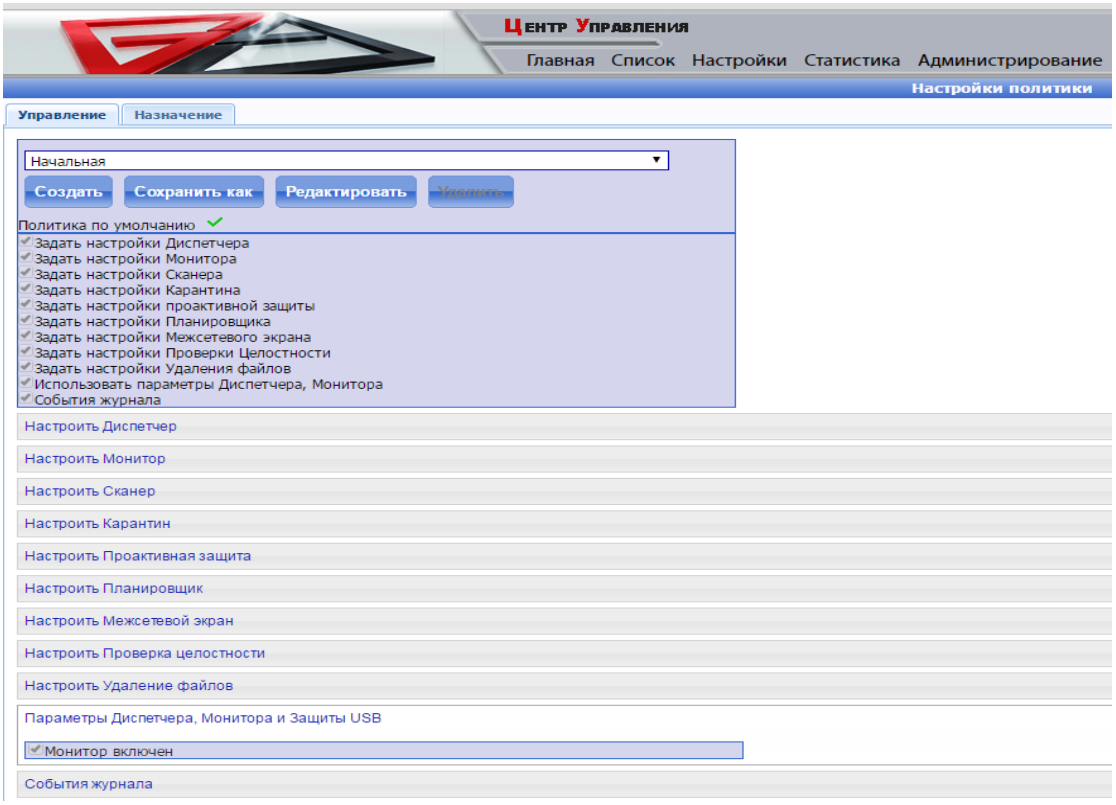

Рис. 132

Пример вкладки **Настроить Сканер** приведен на рисунке 133.

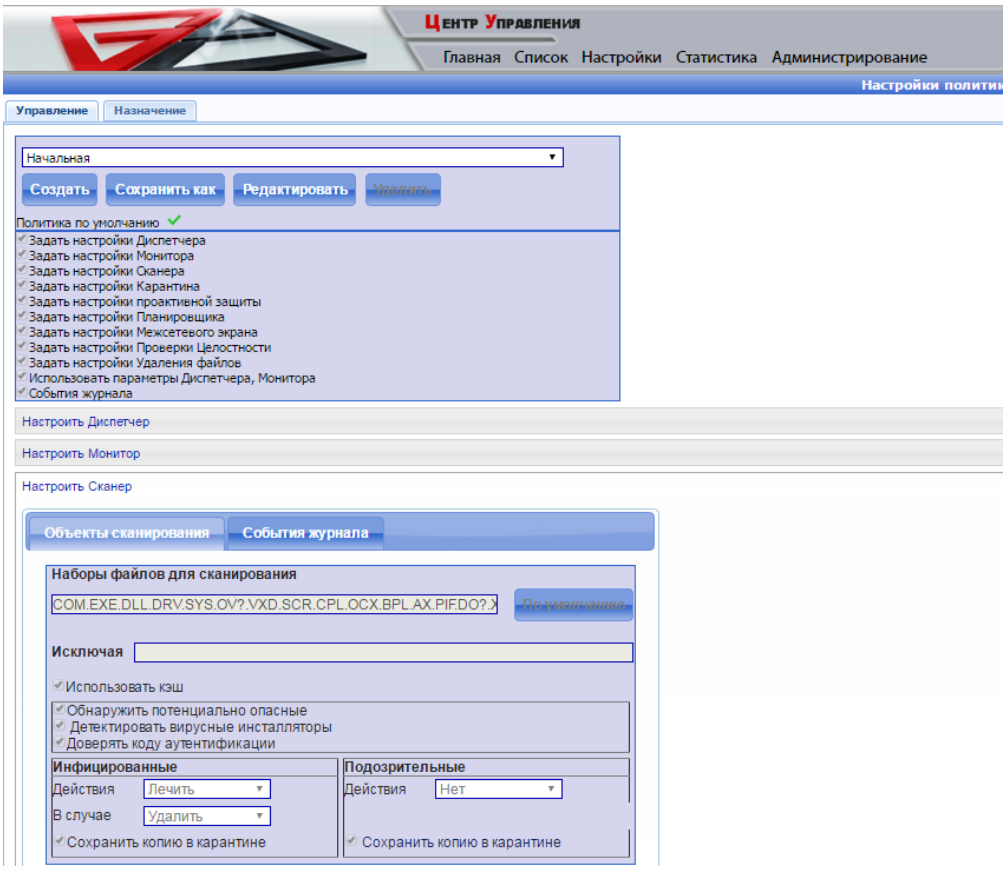

Рис. 133

Пример вкладки **Настроить проактивная защита** приведен на рисунке 134.

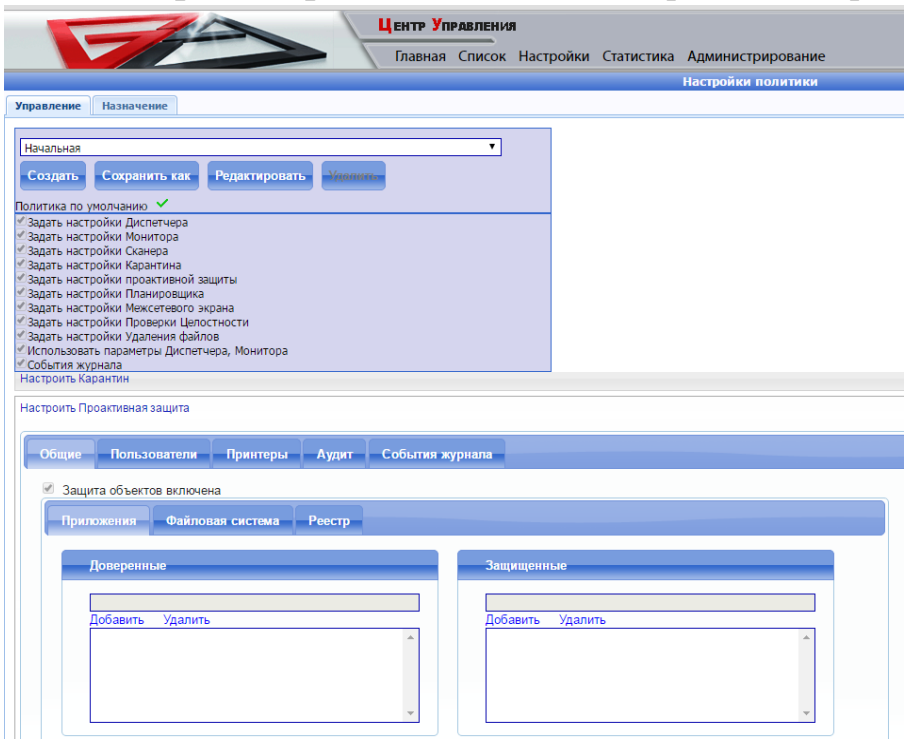

Рис. 134

Пример вкладки **Настроить Планировщик** приведен на рисунке 135.

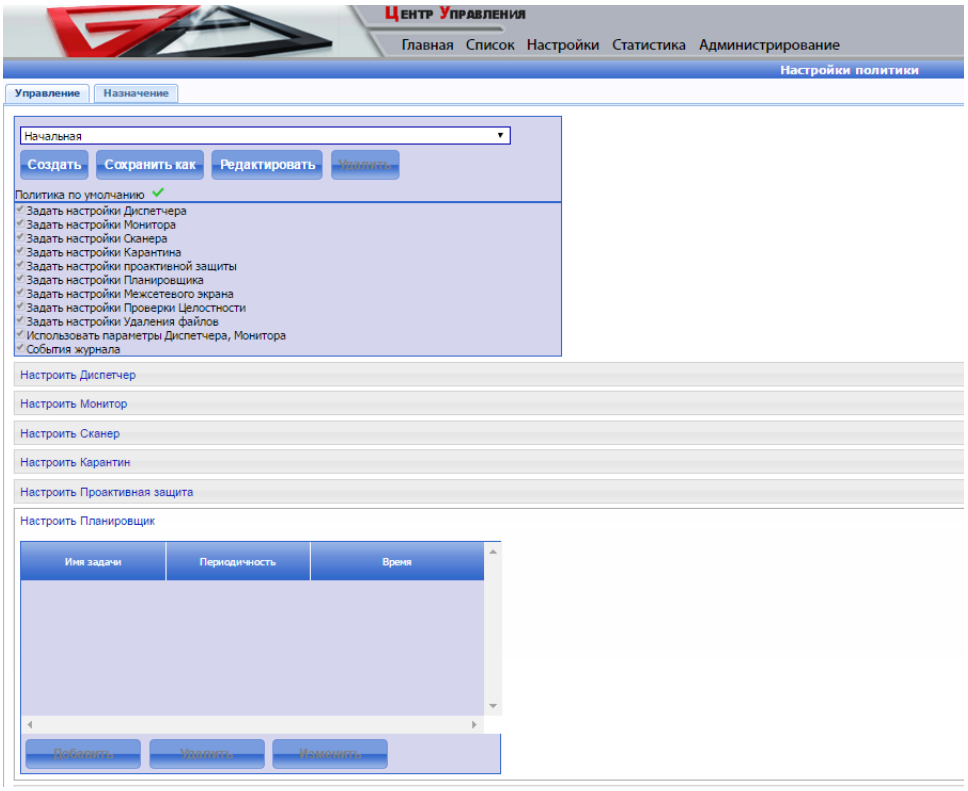

Рис. 135

Пример вкладки **Настроить Межсетевой экран** приведен на рисунке 136.

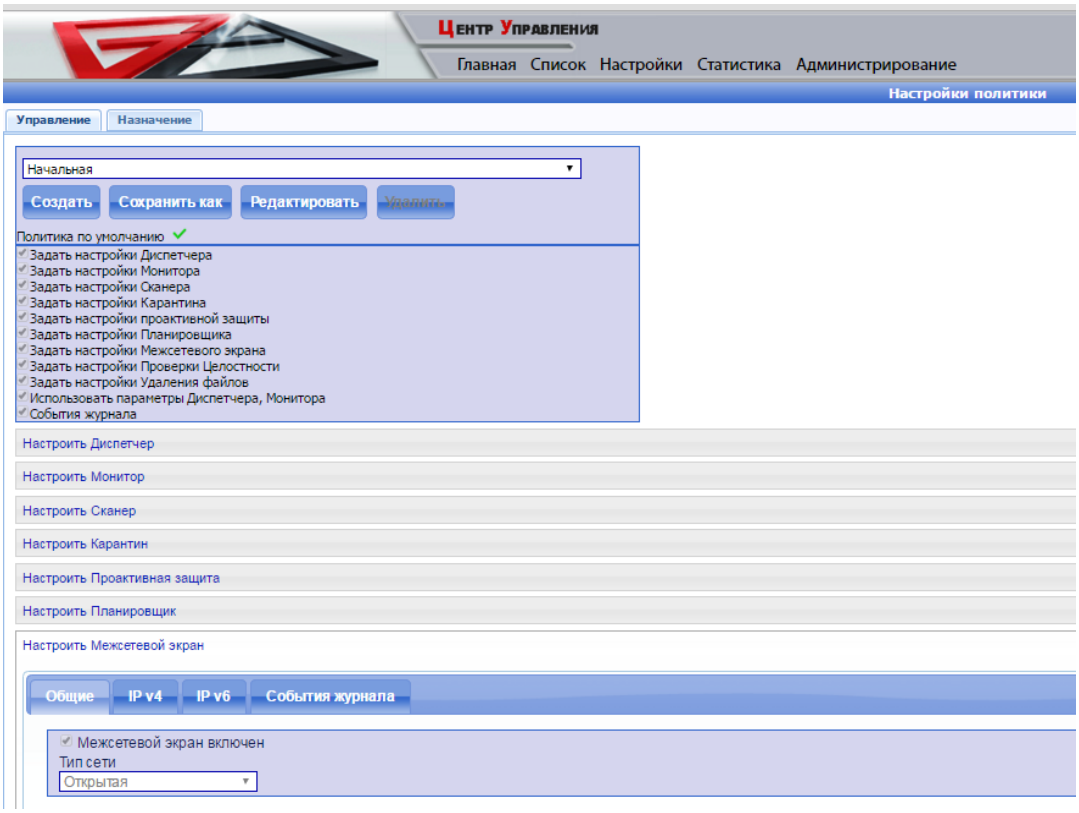

Рис. 136

Пример вкладки Настроить Проверка целостности приведен на рисунке 137.

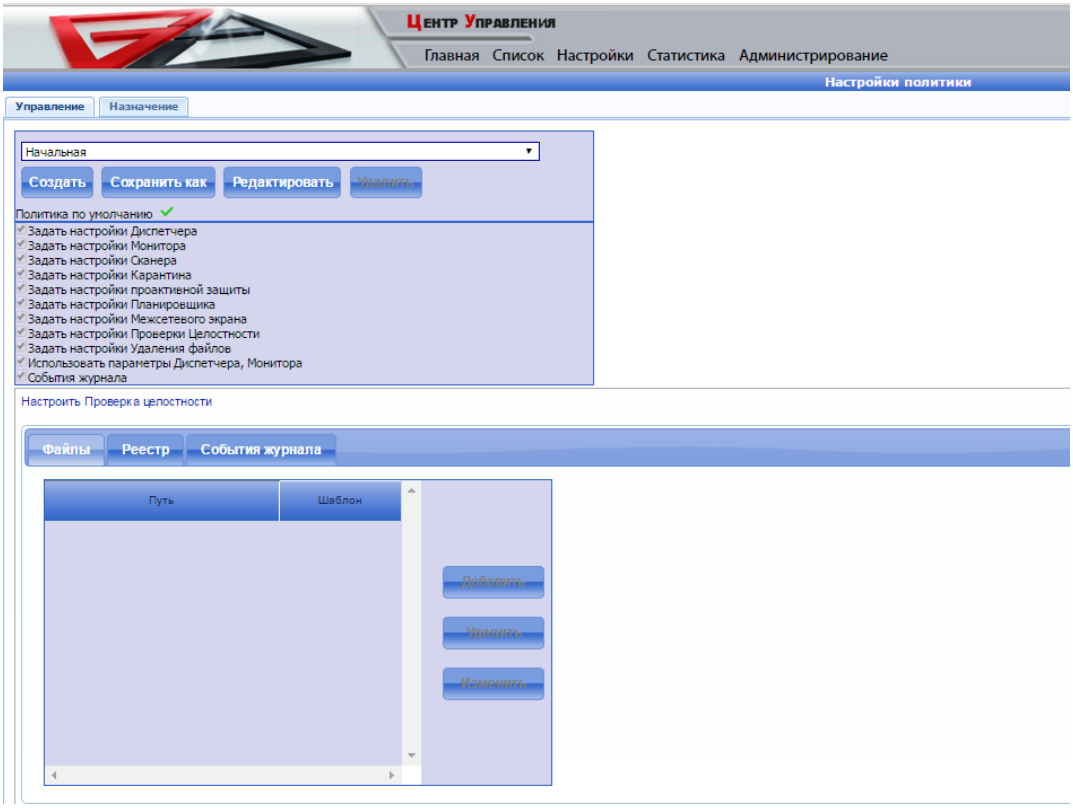

Рис. 137

Пример вкладки **Настроить Удаление файлов** приведен на рисунке 138.

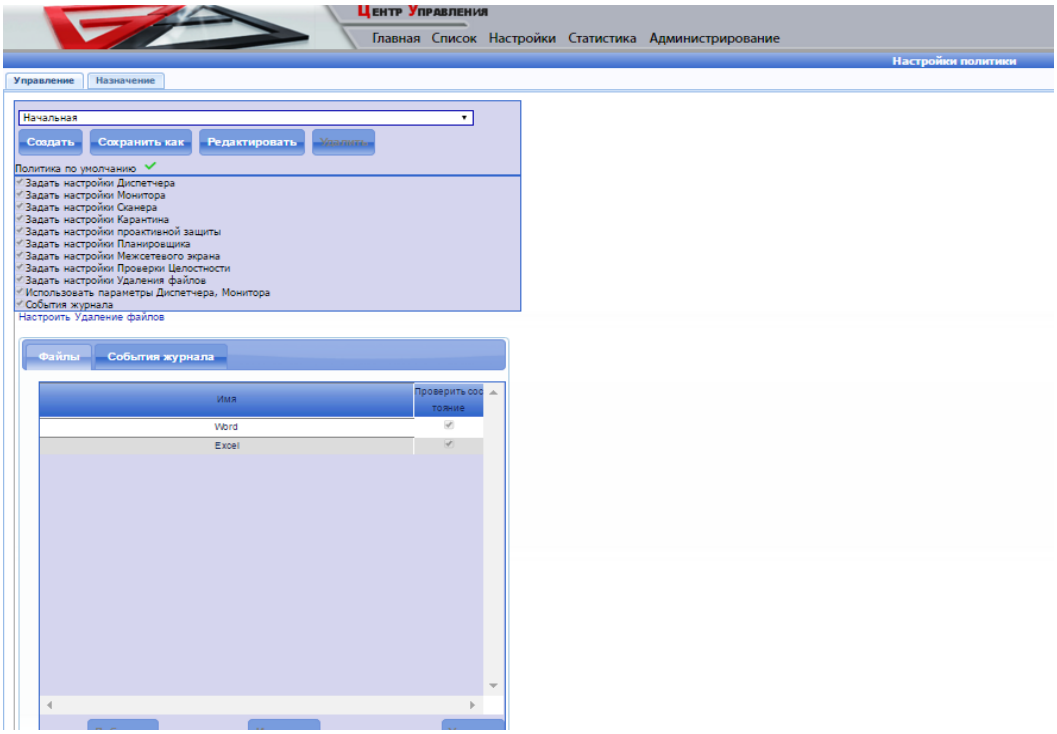

Рис. 138

Пример вкладки **События журнала** приведен на рисунке 139.

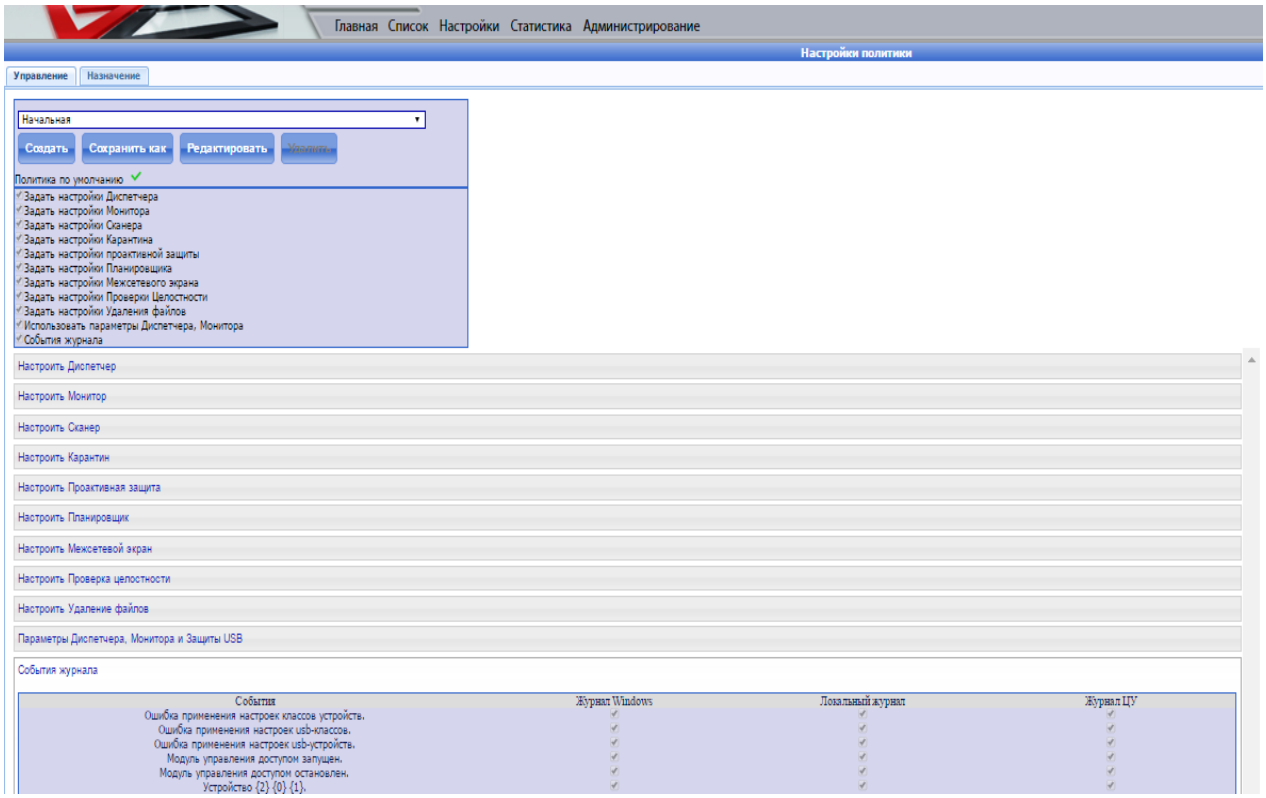

Рис. 139

Примечание. Не допускается создавать пустую политику, т.е. необходимо выбрать один из доступных параметров. Не допускается создавать политику с существующим именем.

4.13.2. Редактирование политики

Чтобы изменить параметры используемой политики необходимо выбрать ее в выпадающем списке политик на странице **Политики** в меню **Администрирование** и нажать кнопку **Редактировать**, которая доступна на вкладке **Управление**. После этого будет осуществлен переход на страницу **Настройки политики**, где на вкладке **Управление** будет представлены настройки данной политики. При этом запрещено редактирование имени данной политики.

Примечание. На редактирование политики накладываются те же ограничения, что и на создание.

4.13.3. Удаление политики

Чтобы удалить используемую политику необходимо выбрать ее в выпадающем списке политик на странице списка компьютеров и нажать кнопку **Удалить**, которая доступна на вкладке **Управление**.

Примечание. Все компьютеры, которые использовали эту политику, перестанут ее использовать.

4.13.4. Назначение политики

Назначить политику определенному компьютеру или группе компьютеров можно двумя способами:

1) с помощью страницы **Компьютеры** в меню **Список** (рис. 140);
2) с помощью вкладки **Назначение** на странице **Политики** в меню **Администрирование** (рис. 141).

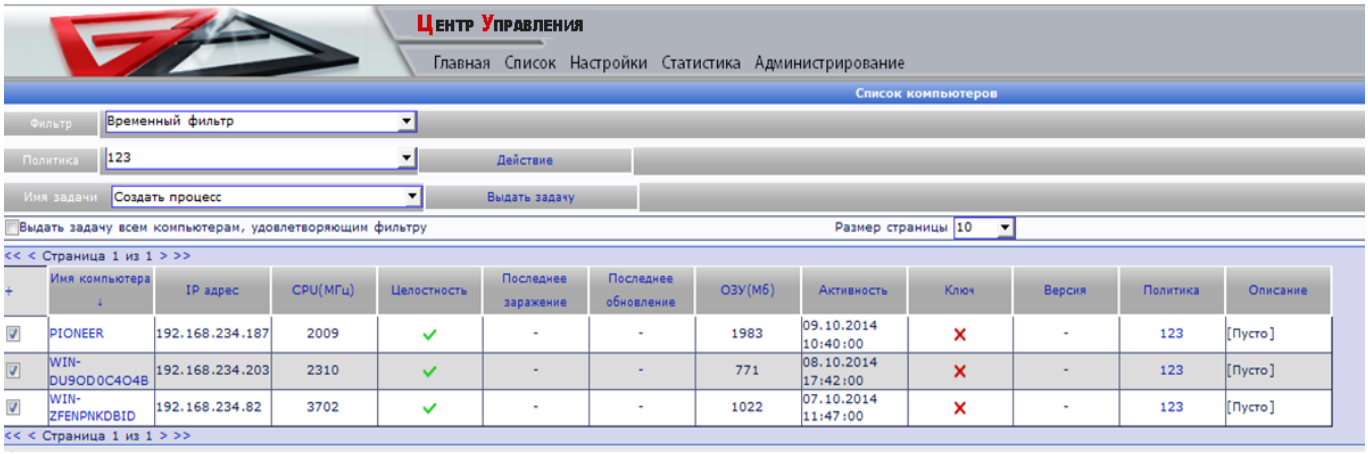

Рис. 140

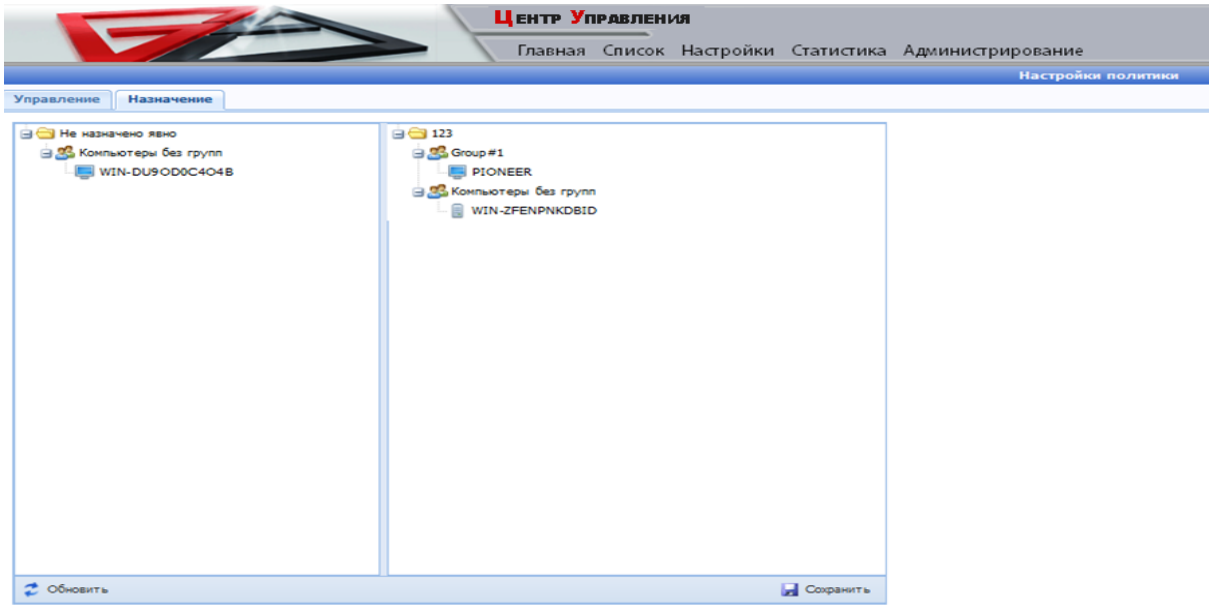

Рис. 141

Для назначения политики на странице **Компьютеры** в меню **Список** необходимо выполнить следующие шаги:

1) выбрать ранее созданную политику из выпадающего списка политик;
2) отметить отдельные компьютеры, отметив их флажками либо отметить все, используя флажок **Выдать задачу всем компьютерам, удовлетворяющим фильтру**;
3) выбрать из меню **Действие** напротив имени политики пункт **Применить политику**.

Для назначения политики на вкладке **Назначение** страницы **Политики** в меню **Администрирование** необходимо выполнить следующие действия:

1) выбрать в левой панели группу или компьютер;
2) перетащить группу/компьютер в папку с именем нужной политики в правой панели;
3) после завершения формирования политик нажать кнопку **Сохранить** (рис. 142).

Рис. 142

Примечание. Группы, компьютеры (рабочие станции) и сервера отображаются с помощью различных иконок. При наведении на иконку объекта можно получить более подробную информацию об объекте.

Если необходимо отменить последние действия, нажмите кнопку **Обновить** до нажатия кнопки **Сохранить**.

4.13.5. Просмотр назначенных политик

На странице на странице **Компьютеры** в меню **Список** можно просмотреть политики и назначенные им компьютеры. Для этого необходимо выбрать политику из выпадающего списка **Политика** и в меню **Действие** выбрать пункт **Отобразить компьютеры** (рис. 143). После этого на странице отобразиться стандартная таблица со списком компьютеров, для которых назначена данная политика. Чтобы отменить действие фильтра, нужно нажать на кнопку **Политика**, которая находится слева от выпадающего списка с именами политик.

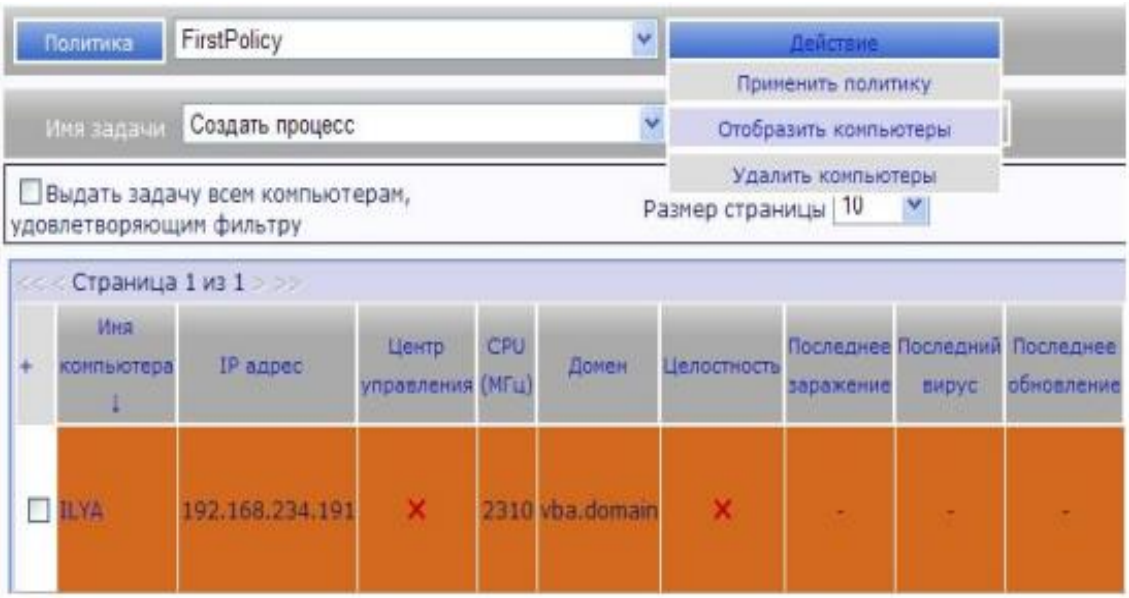

Рис. 143

4.13.6. Использование политики по умолчанию

Для более быстрого использования механизма политик, предусмотрена возможность задания политики по умолчанию. Политика по умолчанию – это та политика, которая будет выполняться на компьютерах, которым не назначена ни одна из других политик.

Для того чтобы политика стала политикой по умолчанию, необходимо выполнить следующие шаги (рис. 144):

1) создать политику либо выбрать существующую политику;
2) на вкладке **Управление** нажать стилизованную иконку ✕ справа от строки **Политика по умолчанию**. Она изменится на ✓.

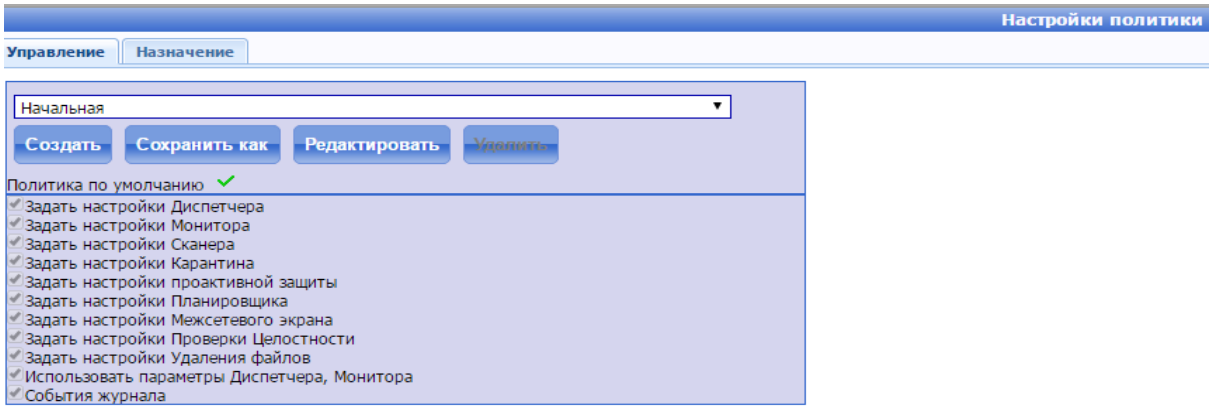

Рис. 144

После этого все группы и компьютеры, которым не была назначена ни одна из политик, получат данную политику. Чтобы просмотреть, какая политика является политикой по умолчанию, можно воспользоваться страницей **Политики** в меню **Администрирование**. На вкладке **Назначение политик** в левой панели содержатся все группы и компьютеры, для которых действует политика по умолчанию.

Примечание. Политика по умолчанию может быть только одна.

3.3. Управление доступом к съемным носителям

Модуль «Центр Управления» позволяет конфигурировать специализированный драйвер управления съёмными носителями, который является частью комплекса КАНОЭ. Конфигурирование осуществляется на странице **Устройства** в меню **Администрирование**.

Основная задача управления доступом к съёмным носителям заключается в назначении определенного действия драйвера управления по отношению к конкретному съемному носителю. То есть администратор модуля «Центр Управления» определяет поведение драйвера управления на конкретной рабочей станции. При этом для каждого компьютера задаются свои настройки действия над определенным носителем (устройства).

4.13.7. Вкладка Группы

Вкладка **Группы** в меню **Администрирование** (рис. 145) предназначена для просмотра, добавления и изменения состояния устройств, используемых определенным компьютером. Для этого необходимо выбрать нужный компьютер (группу) и щелкнуть по его имени (кнопке **Устройства**, находящейся справа в строке имени группы). После этого появится диалоговое окно (рис. 146), в котором будет доступен список устройств, их состояний и дополнительная информация; форма для добавления нового устройства.

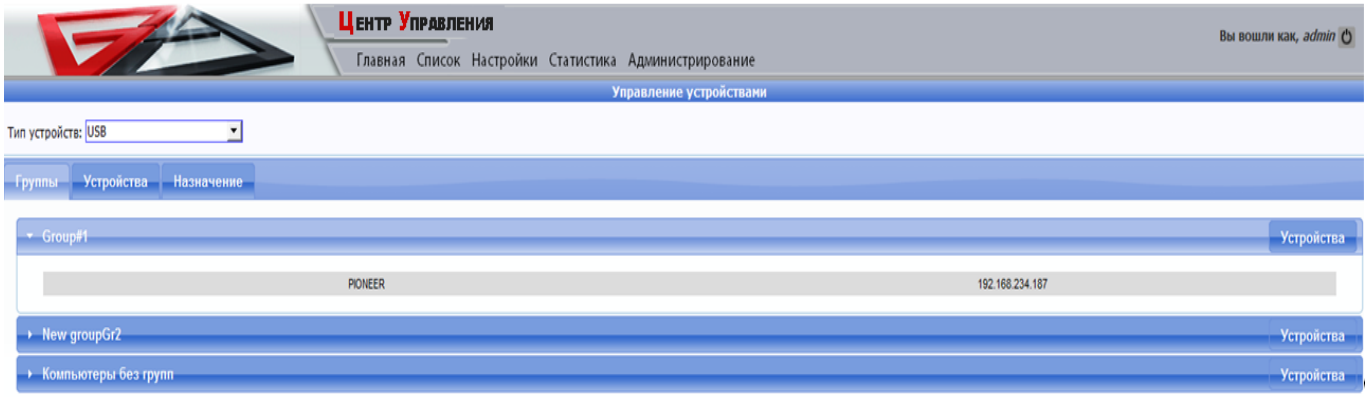

Рис. 145

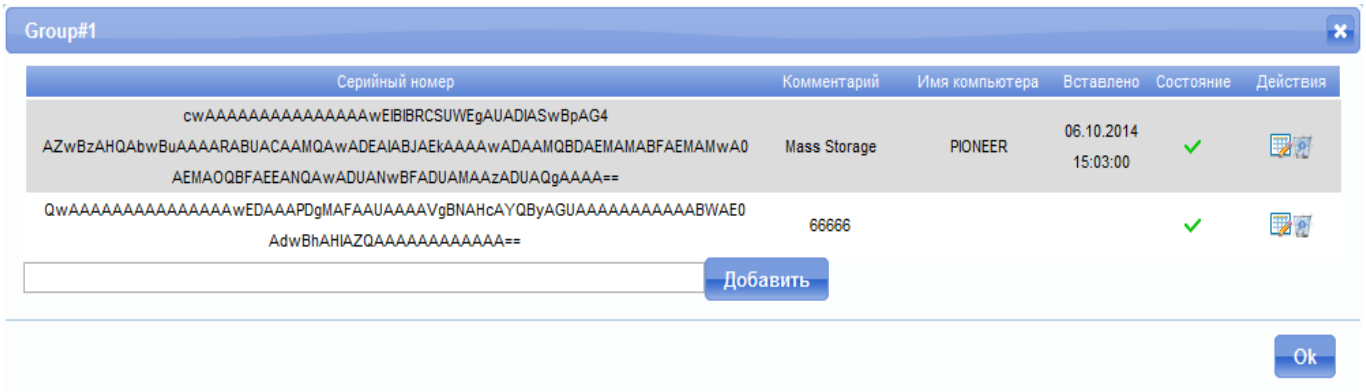

Рис. 146

Добавление нового устройства к компьютеру

Чтобы добавить новое устройство к компьютеру (группе), проделайте следующее:

1) выберите нужный компьютер (группу);
2) нажмите на кнопку **Устройства** справа в строке имени группы в появившемся диалоге введите серийный номер устройства в поле для ввода;
3) нажмите кнопку **Добавить** (рис. 146).

Изменение статуса устройства компьютера

Чтобы изменить режим работы устройства, нужно щелкнуть на его текущем состоянии (рис. 146). После каждого нажатия происходит смена режима (состояния).

Поддерживаются следующие режимы:

1) - запрещено, устройство запрещено к использованию;
2) - разрешено, устройство разрешено к использованию;
3) - неопределено, по устройству еще не принято решение (данный режим выставляется автоматически самим модулем «Центр Управления при первом определении устройства и недоступен для выставления в ручном режиме);
4) - запрещена запись.

Удаление определенного устройства компьютера

Для удаления устройства компьютера необходимо нажать на напротив соответствующего устройства.

Примечание. Сама информация об устройстве не удаляется из базы данных.

Изменение комментария устройства

Для изменения комментария устройства необходимо нажать на напротив соответствующего устройства и задать новый комментарий.

4.13.8. Вкладка Устройства

Вкладка **Устройства** (рис. 147) предназначена для назначения определенному устройству компьютеров и действий над этим устройством.

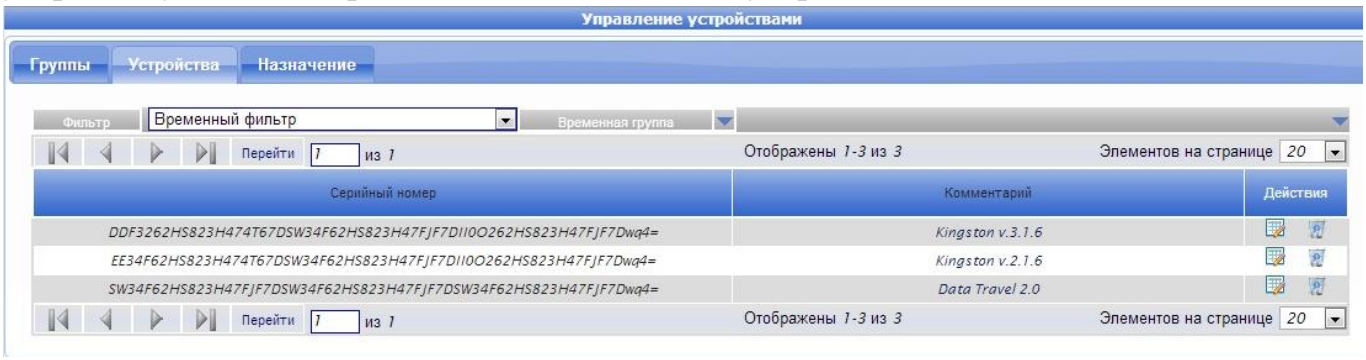

Рис. 147

Добавление компьютера к устройству

Для того чтобы на этой вкладке определить действия компьютера над нужным устройством, необходимо выполнить следующее:

1) выбрать устройство (кликнуть на серийном номере устройства);
2) в появившемся диалоге нажать кнопку **Добавить**;
3) в появившемся диалоге отметить нужные имена компьютеров (групп);
4) нажать кнопку **Добавить**.

Изменение статуса, удаление устройства

Данные действия осуществляются аналогично действиям, описанным для вкладки **Группы**.

Изменение комментария к устройству

Чтобы изменить комментарий к устройству необходимо щелкнуть мышкой на кнопке напротив нужного устройства и, в появившемся диалоге, ввести текст нового комментария.

4.13.9. Вкладка Назначение

Вкладка **Назначение** служит для назначения действий **Разрешить** и **Блокировать** для неопределенных устройств в компьютере. Для этого необходимо проделать следующее:

1) выбрать компьютер и устройство в таблице.
2) нажать на кнопку ✓ для разрешения или ✕ для блокировки (рис. 148).

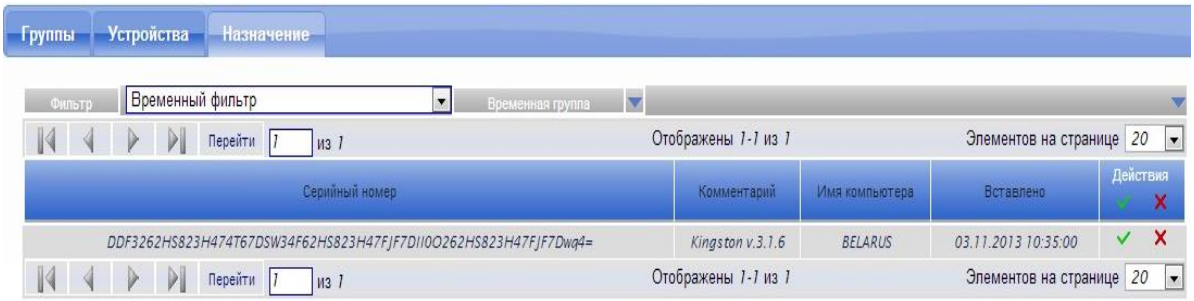

Рис. 148

Примечание. После выбора действия серийный номер устройства должен исчезнуть из списка.

Для обновления таблиц на других вкладках рекомендуется обновить страницу.

4.14. Управление доступом к классам устройств

Модуль «Центр Управления» позволяет конфигурировать специализированный драйвер управления классами устройств, который является частью антивирусного комплекса. Конфигурирование осуществляется на странице **Классы устройств** в меню **Администрирование**.

Основная задача управления доступом к классам устройств заключается в назначении определенного действия драйвера управления по отношению к конкретному классу устройств. То есть администратор модуля «Центр Управления» определяет поведение драйвера управления на конкретной рабочей станции. При этом для каждого компьютера задаются свои настройки действия над определенным классом.

4.14.1. Вкладка Группы

Вкладка **Группы** (рис. 149) предназначена для просмотра, добавления и изменения состояния классов устройств, используемых определенным

компьютером. Для этого необходимо выбрать нужный компьютер (группу) и щелкнуть по его имени (или кнопке **Классы устройств**, находящейся справа в строке имени группы). После этого появится диалоговое окно (рис. 149), в котором будет доступен список классов устройств, их состояний и дополнительной информации; форма для добавления нового класса.

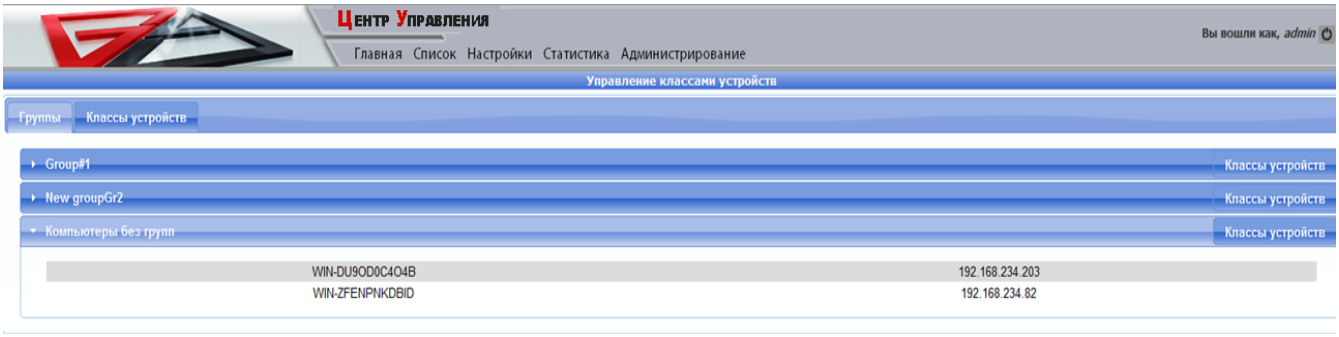

Рис. 149

Добавление нового класса к компьютеру

Чтобы добавить новый класс к компьютеру (группе), проделайте следующее:

1) нажмите на имя компьютера в группе или воспользуйтесь кнопкой **Классы устройств** справа от имени группы;
2) в появившемся диалоге введите в поле ввода UID введите буквенно-цифровой идентификатор устройства, имеющегося на компьютере;
3) нажмите кнопку **Добавить** (рис. 150).

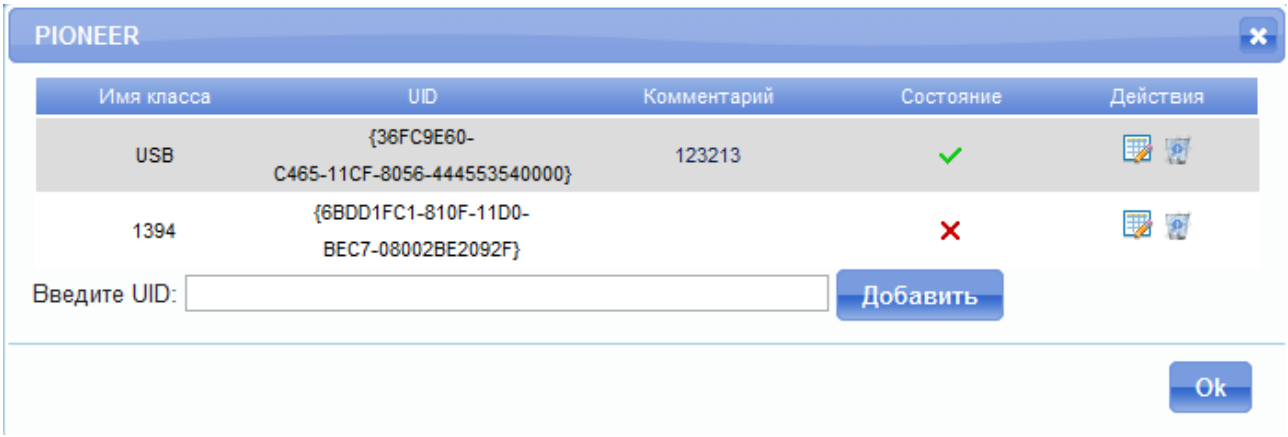

Рис. 150

Изменение состояния класса устройства компьютера

Чтобы изменить режим, выполняющийся над классами, нужно щелкнуть на его текущем состоянии (рис. 150). После каждого нажатия происходит смена режима (состояния).

Поддерживаются следующие режимы:

1) ✗ - запрещено, класс запрещен к использованию;
2) ✓ - разрешено, класс разрешен к использованию;

3)  - запрещена запись, класс может производить только чтение.

Примечание: Режим запрета записи не поддерживается классами USB.

Удаление определенного класса устройств компьютера

Для удаления класса устройств необходимо нажать на  напротив соответствующего класса. В последствии, к данному классу на данном компьютере будет применен режим по умолчанию.

Примечание. Сама информация о классе не удаляется из базы данных.

Изменение комментария класса устройств

Для изменения комментария необходимо нажать на  напротив соответствующего класса и задать новый комментарий.

4.14.2. Вкладка Классы устройств

Вкладка **Классы устройств** (рис. 151) предназначена для назначения определенному классу устройств компьютеров и действий над этим классом.

Примечание. Классы USB выделены комментарием **USB class** и порядковым номером вместо UID.

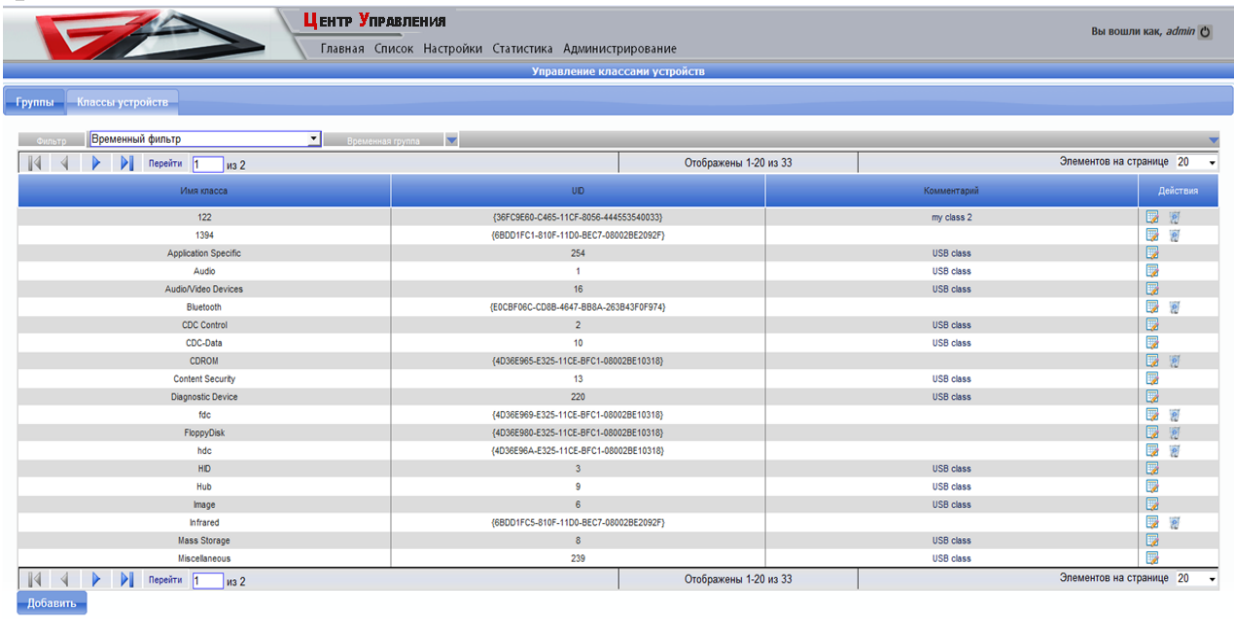

Рис. 151

Добавление нового класса устройств

Для того чтобы добавить новый класс, необходимо выполнить следующее:

1) нажать кнопку **Добавить** (рис. 151);
2) в появившимся диалоговом окне (рис. 152) заполнить необходимые поля и нажать кнопку **Ок**.

Некорректное добавление новых классов устройств и их назначение компьютерам могут привести к нестабильной работе компьютеров.

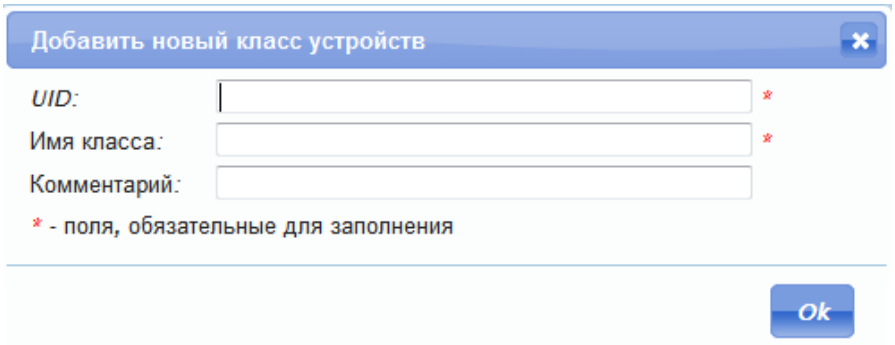

Рис. 152

Добавление компьютера к классу

Для того чтобы на этой вкладке определить действия компьютера над нужным классом, необходимо выполнить следующее:

1) выбрать класс устройства (кликнуть по имени класса или его UID);
2) в появившемся диалоге нажать кнопку **Добавить**;
3) в появившемся диалоге отметить нужные имена компьютеров (групп);
4) нажать кнопку **Добавить**;
5) закрыть аналог.

Изменение статуса, удаление класса

Данные действия осуществляются аналогично действиям, описанным для вкладки **Группы**.

Добавление комментария к классу

Чтобы добавить комментарий необходимо щелкнуть мышкой на кнопке напротив нужного класса и, в появившемся диалоге, ввести текст нового комментария.

ПЕРЕЧЕНЬ СОКРАЩЕНИЙ

БД – база данных;
ЛВС – локальная вычислительная сеть;
ОС – операционная система;
ПО – программное обеспечение;
ПЭВМ – персональная электронная вычислительная машина;
СВТ – средство вычислительной техники;
СУБД – система управления базами данных;
ЭЦП – электронно-цифровая подпись.