Центр Управления Vba32 с Web-интерфейсом

Описание применения

ВирусБлокАда

Версия документации: 1.2 (май 2010)

ОДО «ВирусБлокАда»
220088, РБ, Минск, ул. Смоленская, 15 — 803б
телефон: (+375 17) 294-84-29 (коммерческий отдел)
телефон: (+375 17) 290-59-29 (технический отдел)
E-mail: support@anti-virus.by
WWW: www.anti-virus.by

Разработчики оставляют за собой право вносить в программу изменения, не отраженные в данной версии документации. Последнюю версию документации можно найти на сайте разработчика:

http://www.anti-virus.by/

Содержание

1. Введение

Центр Управления Vba32 с web-интерфейсом – продукт компании «ВирусБлокАда», позволяющий организовать централизованное управление и сбор статистики о работе антивирусного комплекса Vba32 на рабочих станциях в сети.

Этот продукт является основой организации корпоративной системы антивирусной защиты, как для среднего и малого бизнеса, так и для крупных предприятий с множеством территориально распределенных отделений.

Центр Управления Vba32 представляет собой клиент-серверное приложение, состоящее из управляющей части, базы данных, web-интерфейса (устанавливаются на сервере антивирусной защиты), и клиентской части — Агента удаленного администрирования, входящего в состав антивирусного комплекса Vba32.

Возможности Центра Управления Vba32:

- **управление** антивирусным комплексом Vba32 на рабочих станциях, в том числе: настройка компонентов комплекса, избирательное включение / отключение компонентов комплекса;
- **сбор информации** о ключевых событиях комплекса Vba32 на рабочих станциях, в том числе: обнаружение вредоносного ПО и произведенные с ними действия; включение / выключение компонент комплекса; статус обновления комплекса и другие события;
- **запуск проверки** рабочей станции на вирусы Сканером Vba32;
- **постоянный мониторинг состояния** компонентов антивирусного комплекса Vba32 на рабочих станциях, возможность получения отчета о состоянии компонентов на рабочей станции в сети;
- **получение информации** о последнем успешном обновлении, последнем инфицировании, версии установленного антивирусного комплекса Vba32 на рабочей станции;
- **представление статистической информации** о работе централизованной системы антивирусной защиты в виде отчетов, таблиц, графиков и диаграмм;
- **получение дополнительной информации** о рабочей станции – частота процессора, объем ОЗУ, имя активного пользователя;
- **получение списка процессов** с полными путями к исполняемым модулям;
- **запуск командной строки** на рабочей станции;
- **организация иерархической системы** Центров Управления Vba32;
- **уведомление ответственных лиц** о произошедших событиях посредством электронной почты, jabber или сетевых сообщений;
- **управление модулем защиты устройств**, что позволяет настраивать доступ к определенным USB-носителям;
- **автоматическое управление настройками** антивирусного комплекса Vba32 на рабочих станциях в сети с помощью задания политик безопасности.

Особенности Центра Управления Vba32:

- **web-интерфейс,** благодаря которому возможна одновременная работа с Центром Управления из любой точки сети;
- **отсутствие необходимости устанавливать** на рабочем месте оператора какое-либо программное обеспечение – достаточно лишь наличие Интернет-браузера (полностью поддерживаются наиболее популярные версии);

- **гибко настраиваемый** интерфейс – возможность применения «шаблонов», «тем», изменения языка;
- **возможность создания** собственной цветовой схемы отображения событий, собственных фильтров по таблицам, собственных задач;
- **индивидуальные настройки** web-интерфейса для каждого пользователя;
- **экспорт** таблицы событий в Microsoft Excel;
- **импорт / экспорт настроек** пользователя в XML-файл.

2. Условия применения

2.1 Аппаратные требования

Центр Управления Vba32 представляет собой серверное приложение, состоящее из нескольких сервисов. Предполагается круглосуточная работа компонентов Центра Управления Vba32 – это обеспечит максимальную актуальность информации и оперативность реагирования на угрозы в сети. По этой причине рекомендуется установить Центр Управления Vba32 на компьютер, функционирующий круглосуточно.

Для нормального функционирования продукта необходим компьютер платформы IBM PC с конфигурацией не хуже чем:

- Процессор: Pentium III 1000 МГц;
- 1 Гб ОЗУ;
- 200 Мбайт свободного места на жестком диске для самой программы и до 1.5 Гбайт – для базы данных;
- Сетевая карта 100 Мбит.

2.2 Программные требования

Для установки и использования Центра Управления Vba32 необходим компьютер со следующим установленным программным обеспечением:

- Операционная система (ОС) Windows Server 2003 SP1 или выше, Windows Server 2008 SP1, 32- и 64-битные (только для серверных) версии ОС;
- Система управления базами данных (СУБД) Microsoft SQL Server 2000 SP4 или выше, MSDE 2000a;
- Веб-сервер Internet Information Services (IIS) 5, IIS 6, IIS 7;
- Microsoft .NET Framework 2.0 (для Windows Server 2003).

Для работы с web-интерфейсом Центра Управления рекомендуется один из следующих браузеров:

- Microsoft Internet Explorer версий 7, 8;
- Mozilla Firefox 3.

Корректная работа всех компонентов программы в других браузерах не гарантируется.

2.3 Требования к персоналу

Для успешного администрирования Центра Управления Vba32 необходимо обладать следующими знаниями и умениями:

- Знание основ функционирования ОС семейства Windows NT;
- Умение работать со службами Windows, системным журналом, файловой системой NTFS;
- Знание основ сетевого взаимодействия, стека протоколов TCP/IP;
- Знание основ функционирования электронной почты;
- Базовые знания по администрированию Internet Information Services;
- Знания по администрированию Microsoft SQL Server;
- Опыт работы с антивирусным комплексом Vba32.

3. Работа с Центром Управления

В основе функционирования Центра Управления Vba32 лежат две сущности: события и задачи.

Компьютеры, охваченные антивирусной защитой, отображаются в Центре Управления как зарегистрированные. Агенты зарегистрированных компьютеров присылают сообщения о ключевых событиях, произошедших на рабочих станциях – 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 антивирусной защиты – например, настроить компоненты антивирусного комплекса Vba32, включить или отключить их, запустить проверку на вредоносные программы – компьютеру можно выдать одну из задач, с возможностью проследить статус их выполнения.

Центр Управления предоставляет также множество дополнительных возможностей – получение подробной информации о рабочей станции и состоянии антивирусной 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 комплекса Vba32 – не более 1 минуты.

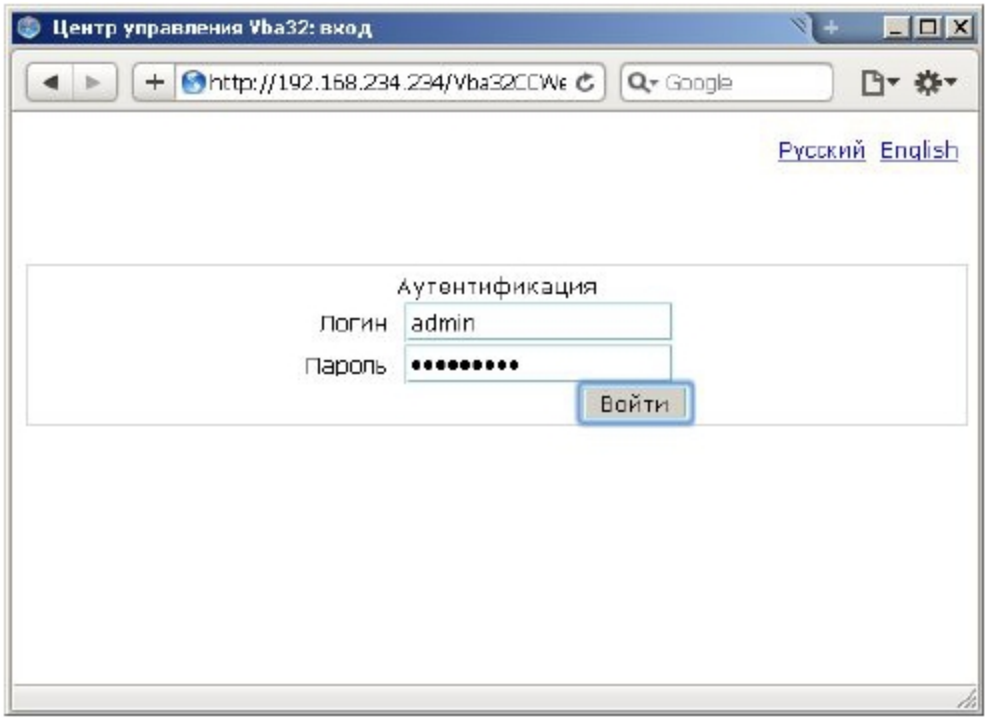
3.1 Начало работы с Центром Управления

Основным органом управления Центром Управления Vba32 является web-интерфейс. Чтобы открыть его, запустите Ваш Интернет-браузер и наберите в адресной строке следующее:

http://server/Vba32CCWebConsole/

Вместо **server** подставьте реальное имя компьютера, на котором установлена серверная часть Центра Управления Vba32.

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

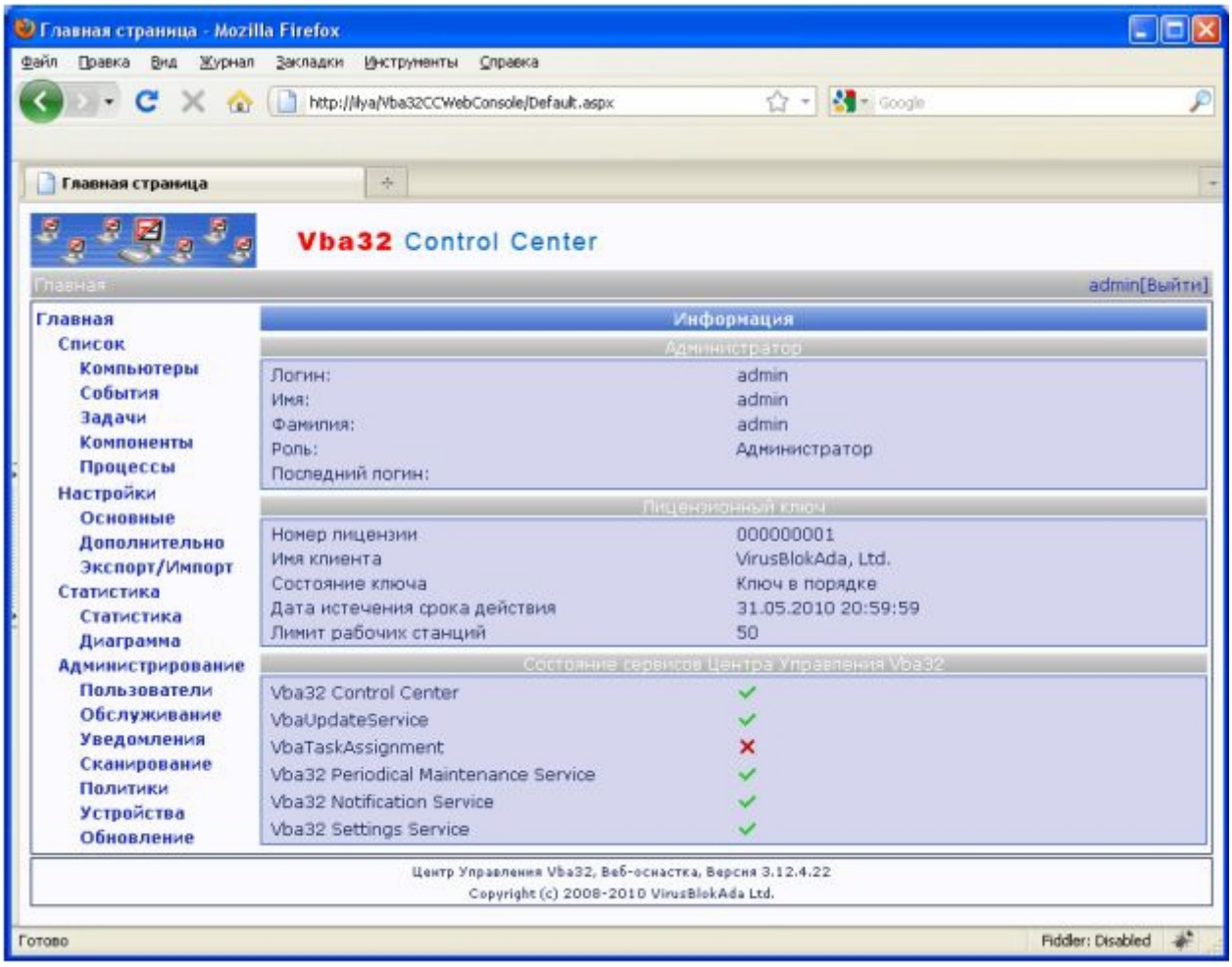


В процессе установки Центра Управления Vba32 создается пользователь со следующими реквизитами:

Имя пользователя: **admin**

Пароль: **1234qwer!**

Вы можете использовать эти реквизиты для первого входа в Центр Управления Vba32. После первого успешного входа Вы попадете на заглавную страницу web-интерфейса.



На главной странице отображены данные о текущем пользователе web-интерфейса, состоянии лицензионного ключа и состоянии сервисов Центра Управления Vba32.

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

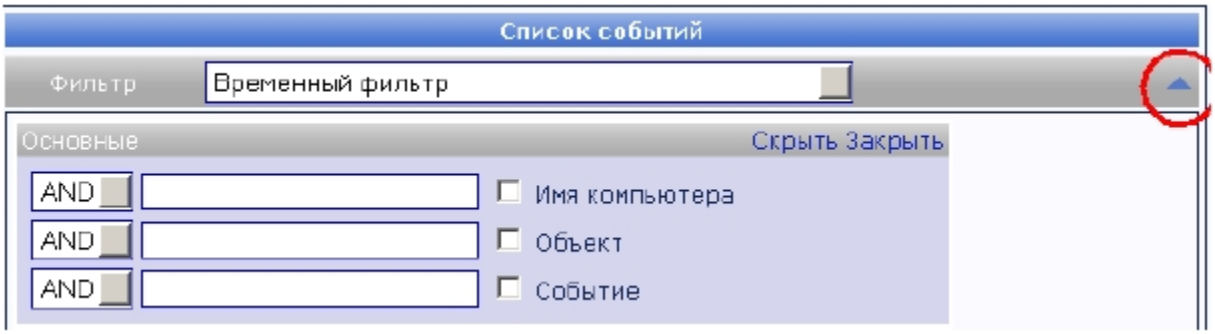
Рекомендуется сразу же сменить пароль учетной записи admin (см. пункт «Изменение личной информации и пароля»), а также завести новых пользователей (см. пункт «Создание пользователя») для работы с web-интерфейсом Центра Управления Vba32.

3.2 Работа со списками

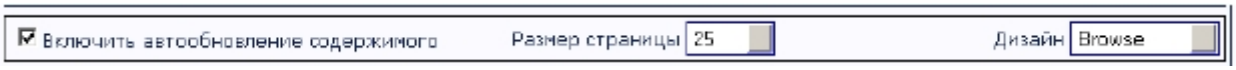
В Центре Управления Vba32 пользователю предоставлено пять списков – Компьютеры, События, Задачи, Компоненты, Процессы. Чтобы начать работу с любым из списков, надо в меню «Список» нажать на соответствующую ссылку.

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.



Под панелью фильтров расположена дополнительная панель управления, позволяющая управлять размером страницы, автоматическим обновлением, а также состоянием панели фильтров (подробнее см. раздел «Работа с табличными данными»).

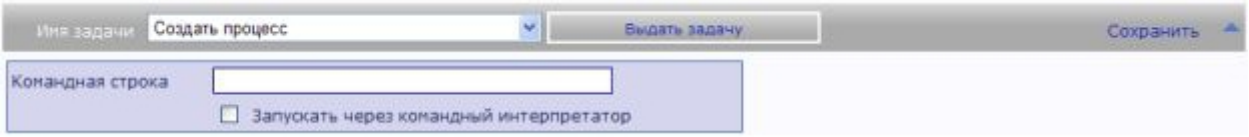


Выпадающий список «Дизайн» определяет состояние панели фильтров. Его использование подробно описано ниже (пункт «Управление панелью фильтров»).

Для списка «Компьютеры» снизу от таблицы находится панель задач, на которой расположены поля для установки параметров выдаваемых задач (подробнее см. раздел «Выдача задач»).

> **Примечание:** Панель задач не видна при работе в Центре Управления под учетной записью наблюдателя.

Панель задач сворачивается и разворачивается нажатием на стрелку в верхнем правом углу.



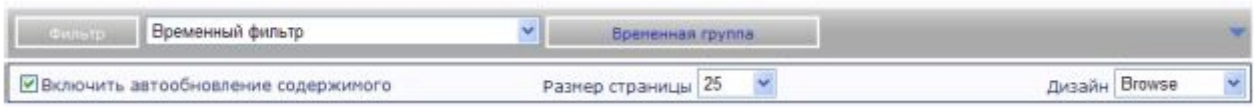
Работа с табличными данными

Данные, выбранные соответствующим фильтром, отображаются в табличном виде с разбивкой на страницы.

Чтобы изменить количество записей, выводимых на одной странице, надо выбрать на дополнительной панели управления в выпадающем списке «Размер страницы» нужное число (возможные варианты – 1, 10, 25, 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.

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



Флажком «Включить автообновление содержимого» включается асинхронное обновление данных на страницах «События» и «Задачи» (более подробно описано в пункте «Настройки автоматического асинхронного обновления содержимого»).

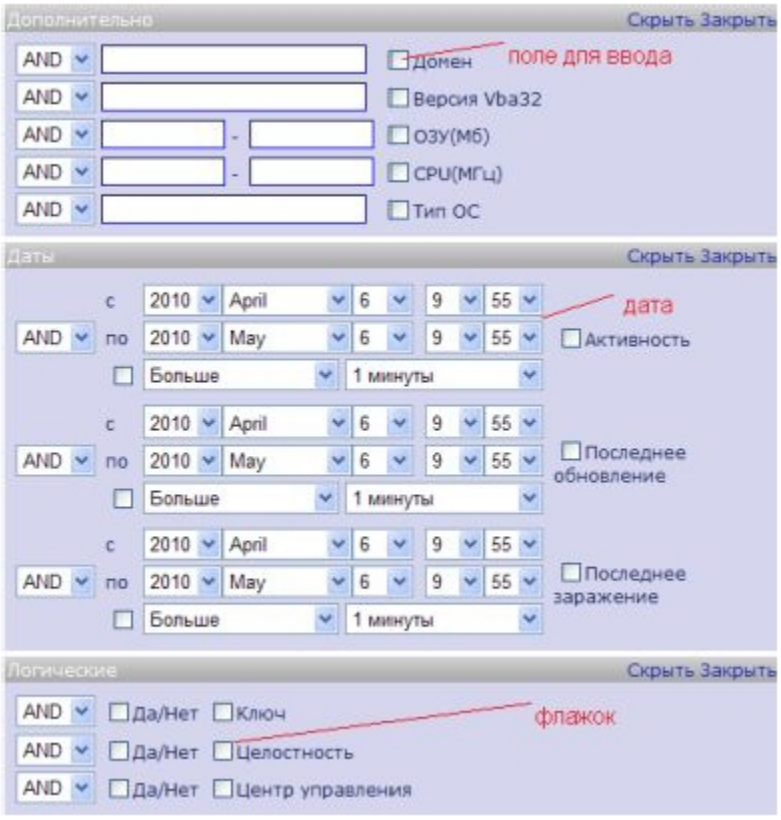
Табличные данные можно сортировать в порядке возрастания или убывания. Для этого необходимо нажать на имя в заголовке таблицы; первый раз происходит сортировка записей по возрастанию, второй раз – по убыванию.

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 Центре 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. Так как в полях бывают данные различных типов, то бывают различные контейнеры фильтров:

- Поля для ввода. Данный тип контейнеров описан ниже;
- Выпадающие списки. Данный тип позволяет выбрать одно значение из заранее предопределенного списка;
- Флажки. Данный тип контейнеров позволяет установить логическое значение (истина или ложь), которому соответствует два состояние флажка – установлен и сброшен;
- Дата. Контейнеры этого типа представляют собой специальный элемент управления, позволяющий настроить временной интервал (при помощи выпадающих списков). Значение «С» должно быть раньше, чем «По».



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.

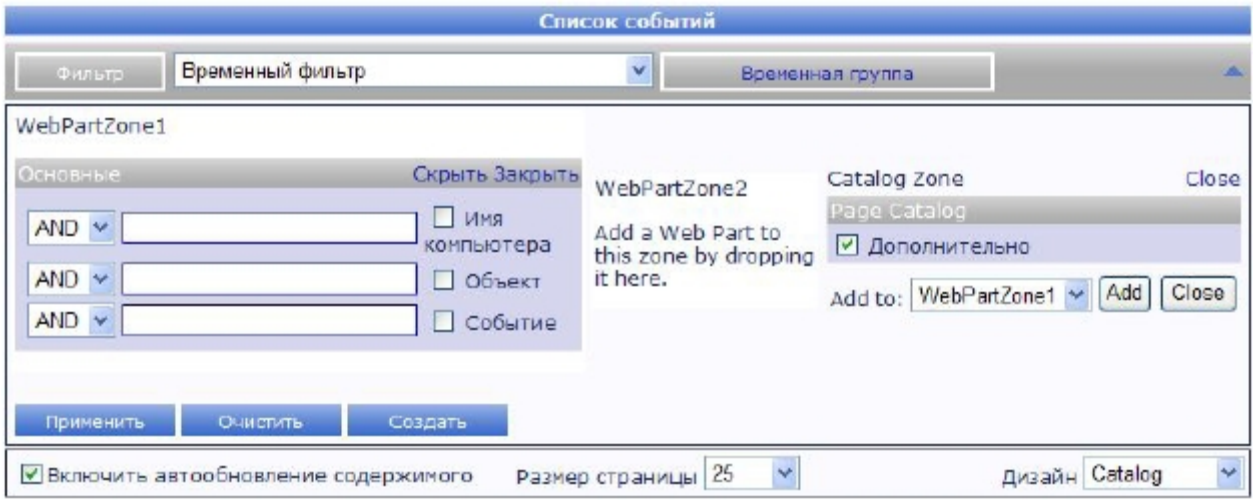
При одновременном использовании нескольких контейнеров имеется возможность указать логические отношения между несколькими параметрами. Для этого служит выпадающий список слева от контейнера, в котором можно выбрать одно из следующих значений:

- AND – заданный критерий должен, безусловно, встречаться в результирующей выборке;
- OR – заданный критерий может встречаться. Имеет смысл лишь при использовании нескольких контейнеров;
- NOT – заданный критерий не должен встречаться в выборке (не применяется вместе с OR).

Управление панелью фильтров

Контейнеры фильтра расположены на панели фильтров. Для повышения удобства работы с фильтрами контейнеры разбиты на группы (например, для событий – «Основные» и «Дополнительно»), которые можно скрыть, восстановить, закрыть и переместить. Первые три действия выполняются при нажатии соответствующих ссылок на панели группе. После нажатия на ссылку «Закрыть» выбранная группа контейнеров будет полностью убрана с исходной страницы.

Существует три режима отображения панели фильтров: просмотр (для работы), дизайн (для изменения размещения групп контейнеров) и каталог (для добавления скрытых групп). Переключение режимов осуществляется выпадающим списком «Дизайн», расположенным на дополнительной панели управления.



Режим «Просмотр» – основной режим работы с панелью фильтров. Он позволяет вводить данные в контейнеры, применять и сохранять фильтры, очищать их и т.п. Положение и порядок групп контейнеров на панели остается неизменным.

Режим «Дизайн» позволяет менять положение групп контейнеров на странице, для этого можно перетаскивать группы мышью (если перетаскивание поддерживается браузером) в подписанные зоны на панели фильтров.

Режим «Каталог» позволяет добавить скрытые при помощи ссылки «Закрыть» группы контейнеров. Для этого необходимо выбрать группу, установив флажок напротив нее, в выпадающем списке выбрать название зоны и нажать «Добавить».

Операции над фильтрами

Примечание: Некоторые операции с фильтрами можно произвести, только раскрыв панель филь тров. Для этого необходимо на жать на с трелку в правой верхней части панели филь тров.

Применение

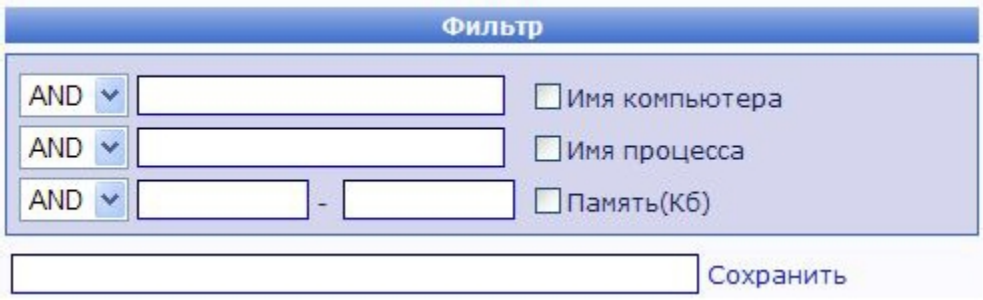
Для применения ранее сохраненного фильтра необходимо выбрать его из выпадающего списка «Фильтр» на панели фильтров.

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.

Внимание! При значительном размере базы данных м ожет потребова ться некоторое время для получения данных на сервере. В этом случае не рекомендуется пользова ться воз можность ю асинхронного обновлен ия содержимого, так как это создаст дополнительную нагрузку на сервер.

Сохранение

Настроенный пользователем фильтр можно сохранить для повторного использования. Для этого необходимо перейти на специальную страницу, нажав на ссылку «Создать» на панели фильтров. При этом все установленные значения в контейнерах, помеченных для использования в фильтре, сохраняются в соответствующих полях.



Для сохранения фильтра необходимо задать его уникальное имя в поле ввода внизу страницы и нажать на ссылку «Сохранить». В случае если такое имя есть в коллекции фильтров, будет получено сообщение об ошибке.

Внимание! Запрещается испо льзовать д ля именования пользова тельских ф иль тров на звани е встроенного временного фильтра на любом из доступных языков веб-интерфейса.

Редактирование

Чтобы отредактировать фильтр, необходимо выбрать его из выпадающего списка «Фильтр» и нажать на ссылку «Редактировать» на панели фильтров. После этого пользователь будет перенаправлен на страницу создания фильтров.

После внесения необходимых изменений необходимо нажать на ссылку «Сохранить».

Примечание: Если введенное имя фильтра отличается от исходного, то будет создан новый фильтр.

Удаление

Для удаления фильтра нужно выбрать его из выпадающего списка «Фильтр» на панели фильтров, нажать на ссылку «Удалить» на панели фильтров и в диалоге подтверждения удаления нажать «ОК».

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 (кроме элементов управления с датой) и все флажки сбрасываются. В поле выбора фильтра выставляется значение «Временный фильтр», а в таблицу выводится полный список.

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 Центре Управления.

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

Временная группа

С помощью временной группы возможно сформировать группу компьютеров и затем использовать ее на разных страницах списков. Для формирования группы используется специальное меню:

- Добавить со страницы – добавляет компьютеры в группу со страницы с текущим примененным фильтром
- Добавить со всех страниц – добавляет компьютеры в группу со всех страниц текущего примененного фильтра
- Заменить со страницы – делает то же самое, что и «добавить со страницы», но очищая предыдущий список компьютеров во временной группе
- Заменить со всех страниц – делает то же самое, что и «добавить со всех страниц», но очищая предыдущий список компьютеров во временной группе
- Применить – в зависимости от страницы списка, выводит информацию о компьютерах, имена которых занесены во временную группу
- Отмена – отключает действие кнопки «Применить».

- **Примечание:** Временная группа рассчитана на хранение порядка нескольких десятков имен компьютеров

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 «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 определенной рабочей станции, следует сделать следующее.

1. На странице списка событий в контейнере «Компьютер» ввести имя рабочей станции и отметить соответствующий фла жок справа от поля для ввода. Это укажет системе, ч то данный контейнер используется в фильтре;

2. Нажать на ссылку «Применить» на панели фильтра;

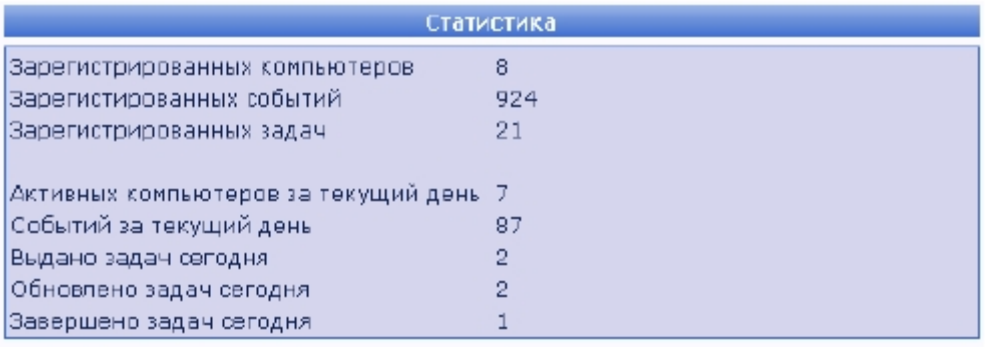
3. После отображения списка событий нажать на ссылку «Excel»;

4. В появившемся диалоговом окне указать путь и имя сохраняемому файлу и нажать кнопку «Сохранить».

Получение статистических отчетов

Статистические данные о работе антивирусной защиты в сети могут быть представлены в Центре Управления в виде статистической таблицы либо диаграмм.

Чтобы просмотреть статистические таблицы, надо в меню «Статистика» нажать на ссылку «Статистика». При этом появится страница, где в простом текстовом виде отображается информация об общем количестве зарегистрированных в системе рабочих станций, событий, задач, а также данные о работе системы антивирусной защиты в сети за сегодня.



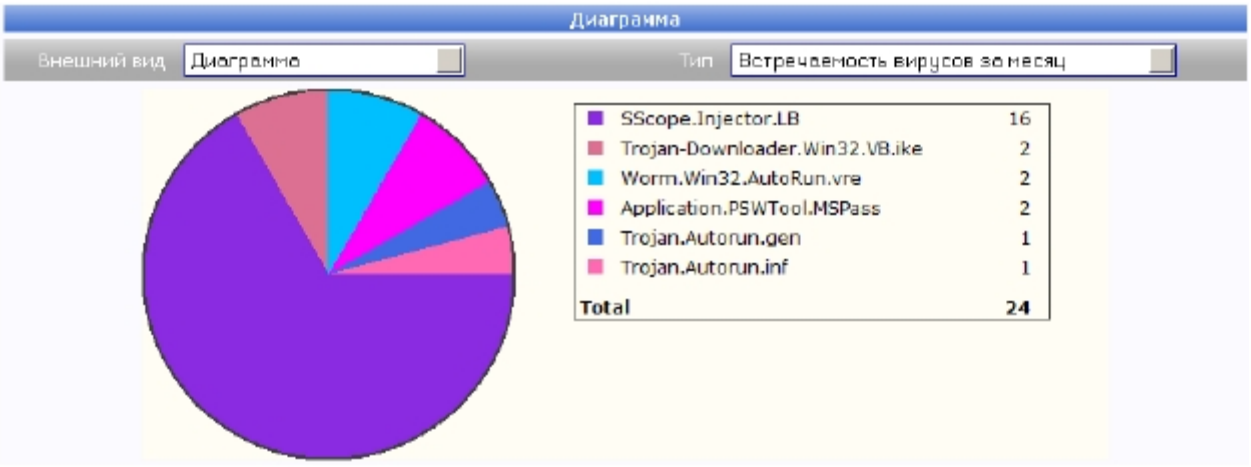
Чтобы просмотреть диаграммы, надо в меню «Статистика» нажать на ссылку «Диаграмма». На появившейся странице статистика отображается в виде гистограмм, диаграмм или таблиц, в зависимости от выбора пользователя.

Смена типа диаграмм осуществляется с помощью выпадающего списка «Внешний вид». Кроме того, доступно несколько базовых типов статистической информации:

- Количество событий;
- Количество событий за сегодня;

- Количество вирусов;
- Количество вирусов за сегодня;
- Общая встречаемость вирусов;
- Встречаемость вирусов за месяц;
- Встречаемость вирусов за сегодня.

В результате выбора одного из вышеперечисленных типов будет отображена соответствующая информация в виде диаграммы, гистограммы или таблицы в виде пар «имя рабочей станции - количество» для первых десяти записей, отсортированных по убыванию.



Кроме этого, для событий существует возможность определить собственный критерий для статистики. Для этого необходимо настроить фильтр на странице «События» и нажать на ссылку «Диаграмма», расположенную внизу таблицы рядом со ссылкой «Excel». Произойдет перенаправление на страницу «Диаграмма», при этом выпадающий список «Тип» будет скрыт, а на его месте отображено имя текущего фильтра (или ничего, если это временный фильтр).

Пример.

Отобразить статистику о найденных вирусах за определенный интервал времени.

1. На странице со списком событий ввести в контейнере «Событие» имя события обнаружения вируса - vba32.virus.found и отметить соответс твующий ф лажок справа от поля для ввода. Это укажет системе, что данный контейнер используется в фильтре;

2. Сконфигурировать контейнер «Дата». В нем необходимо выставить начало и конец временного интервала, за который необходимо выбрать события;

3. Нажать на ссылку «Применить» на панели фильтра;

4. После отображения списка событий нажать на ссылку «Диаграмма».

3.3 Выдача задач

Задача – определенные программные действия, выполняемые клиентской частью Центра Управления на локальном компьютере по указанию управляющей части. Задачи выдаются с web-интерфейса Центра Управления Vba32.

Внимание! Работа с задачам и (выдача, сохранение) недоступна при рабо те в Центре Управления под учетной записью с правами наблюдателя.

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

- Создать процесс;
- Передать файл;
- Запустить сканер;
- Получить информацию о системе;
- Получить список процессов;
- Получить состояние компонентов;
- Настроить Vba32 Диспетчер;
- Настроить Vba32 Монитор;
- Настроить Vba32 Карантин;
- Настроить Vba32 Проактивная защита
- Восстановить файл из карантина
- Установить пароль.
- Настроить защиту устройств
- Запросить политику

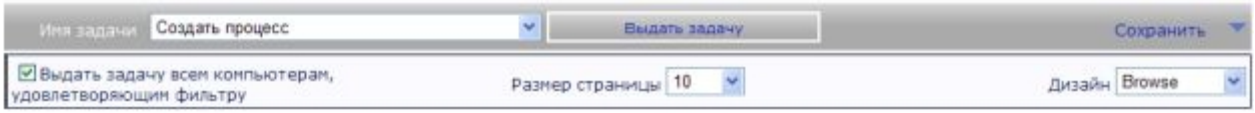
Пользовательские задачи создаются на основе базовых путем задания всех или части параметров. Далее пользовательская задача сохраняется в базе данных под задаваемым именем, и появляется возможность ее быстрой выдачи путем выбора из списка задач.

Выдача задач

Выдача задач осуществляется на странице «Компьютеры».

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».

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



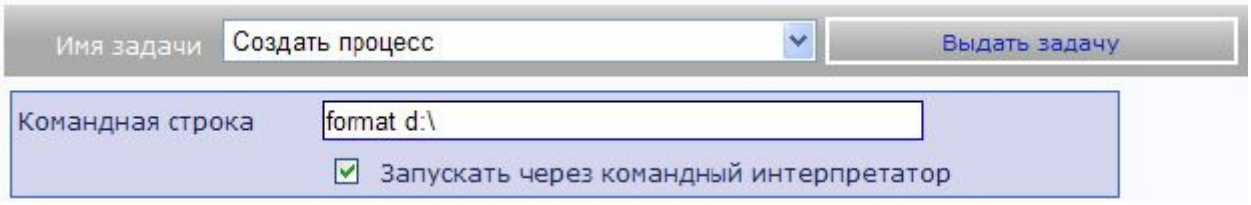
В случае успешного выполнения операции над панелью задач будет отображено сообщение о том, что данная задача была выдана. После этого в списке задач на странице «Задачи» для каждой рабочей станции появится запись о выданной задаче со статусом «Выдача».

Базовые задачи

Создать процесс

Данная задача предназначена для создания процесса на клиентской рабочей станции с возможностью указания параметров командной строки.

В поле «Командная строка» необходимо ввести полный путь к запускаемому процессу и, при необходимости, параметры командной строки.



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

Внимание! Максима льное количество одновременно вы полняю щихся задач «Создать процесс» на любой из рабочих ста нций - 10. При попытке запустить 11ю, ей будет присвоен ста тус «Завершена с ошибкой».

Передать файл

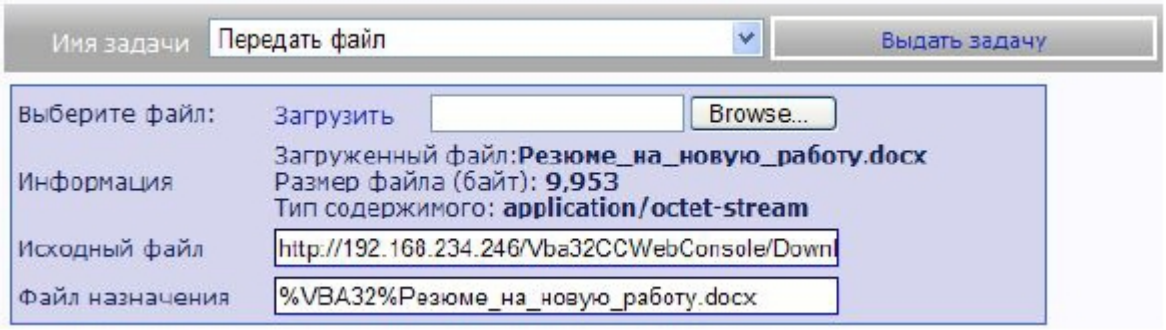
Данная задача предназначена для передачи файла на клиентскую рабочую станцию.

Сначала нужный файл нужно загрузить на сервер. Для этого необходимо нажать на кнопку «Обзор», в стандартном диалоге выбрать файл для передачи и нажать на ссылку «Загрузить».

Внимание! 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.

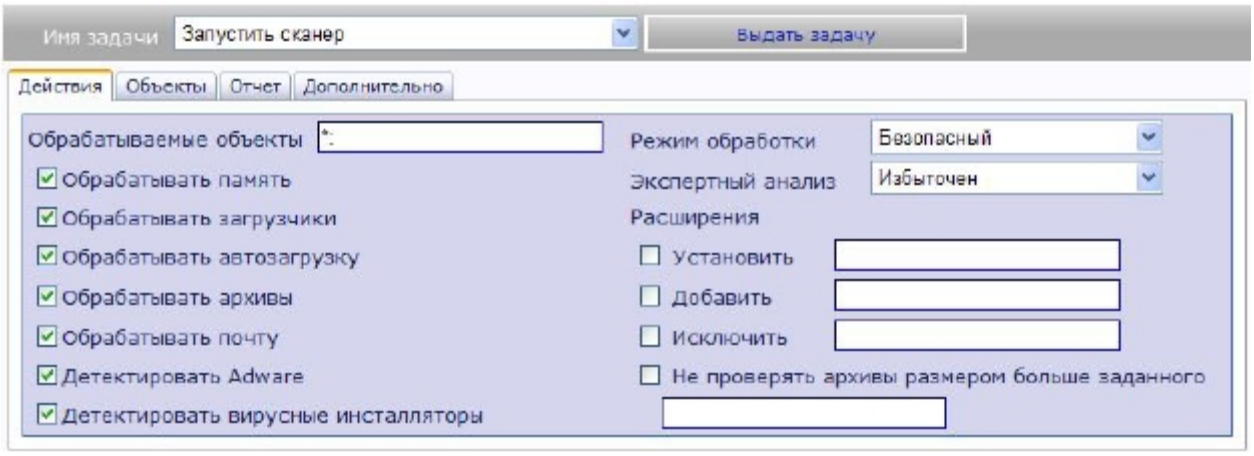


В поле «Файл назначения» необходимо ввести полный путь, куда Агент должен поместить файл после скачивания. В этом поле можно использовать переменные окружения (%WINDIR%, %VBA32% и т.п.), которые будут раскрываться на клиентском компьютере.

Примечание: Если до нажатия на ссылку «Загрузить» данное поле было пустым, то в него автоматически подставляется строка вида «%VBA32%имя_исходного_файла».

Запустить сканер

Данная задача запускает сканер с установленными параметрами. На вкладках «Объекты», «Действия», «Отчет», «Дополнительно» задаются параметры, которые соответствуют параметрам консольного сканера Vba32.



На клиентском компьютере при выдаче данной задачи запускается консольный сканер Vba32 в скрытом режиме.

Получить информацию о системе

Данная задача дает команду Агенту немедленно отослать информацию о системе, а также целостности антивируса и актуальности ключевого файла на клиентском компьютере.

У задачи нет параметров.

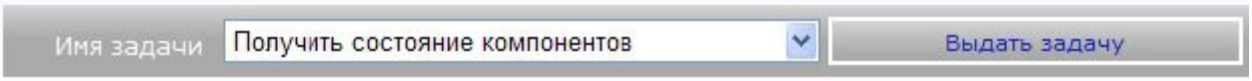
Получить список процессов

Данная задача дает команду Агенту немедленно отослать список процессов, выполняющихся на клиентской машине.

У задачи нет параметров.

Получить состояние компонентов

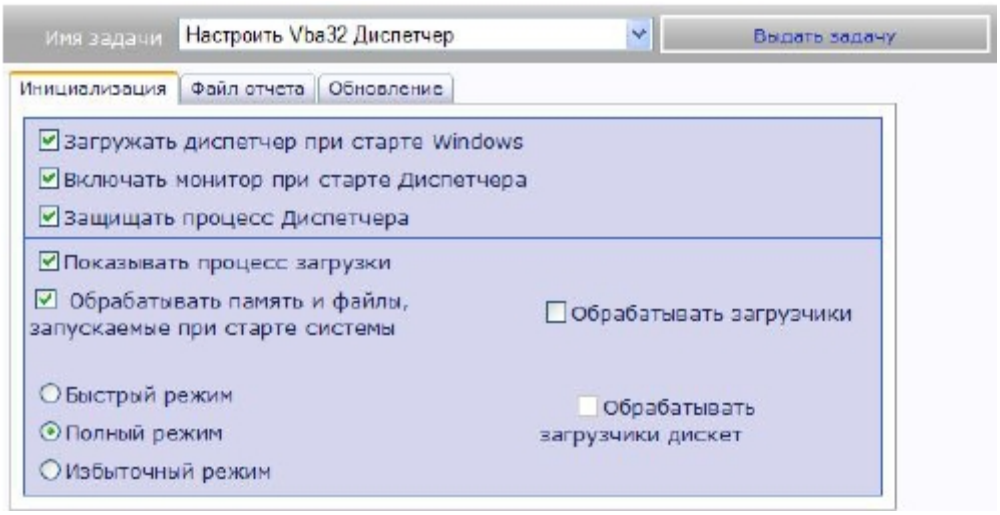
Данная задача дает команду Агенту немедленно отослать состояние компонентов антивируса.



У задачи нет параметров.

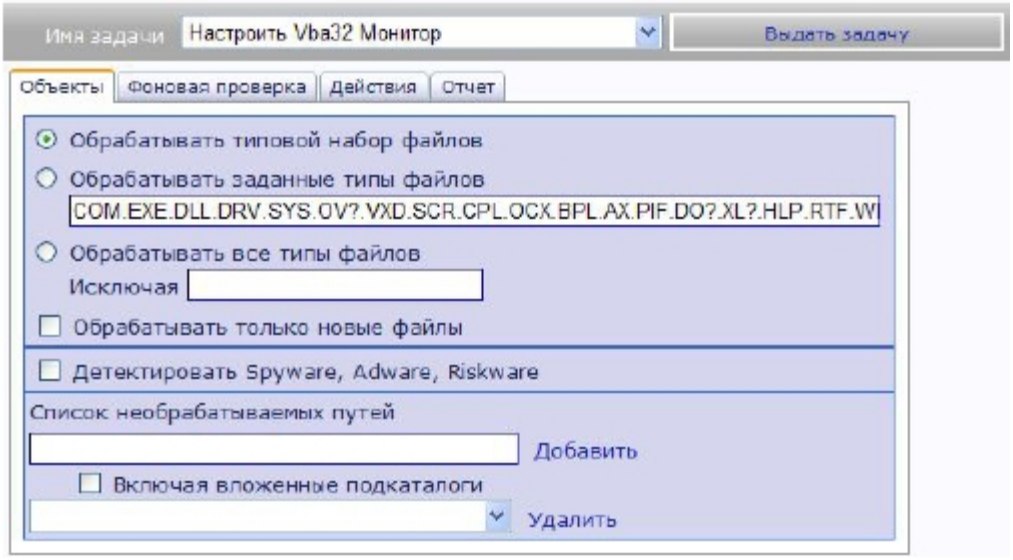
Настроить Vba32 Диспетчер

Данная задача дает возможность настроить Диспетчер. На вкладках «Инициализация», «Файл отчета», «Обновление» задаются параметры, которые соответствуют настройкам Диспетчера Vba32.



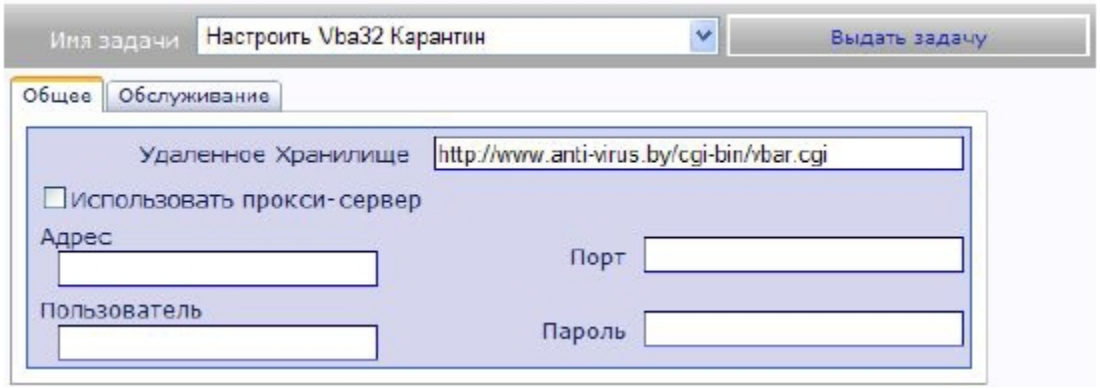
Настроить Vba32 Монитор

Данная задача дает возможность настроить Монитор. На вкладках «Объекты», «Фоновая проверка», «Действия», «Отчет» задаются параметры, которые соответствуют настройкам Монитора Vba32.



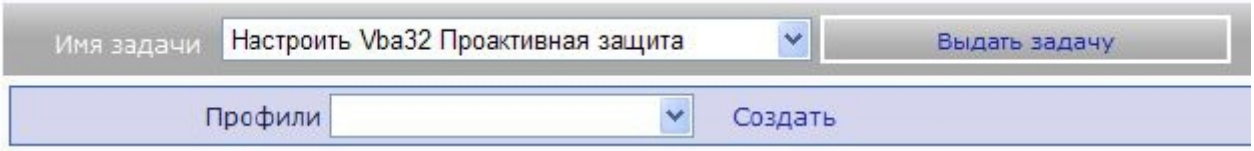
Настроить Vba32 Карантин

Данная задача дает возможность настроить Карантин. На вкладках «Общее», «Обслуживание»1 задаются параметры, которые соответствуют настройкам Карантина Vba32.

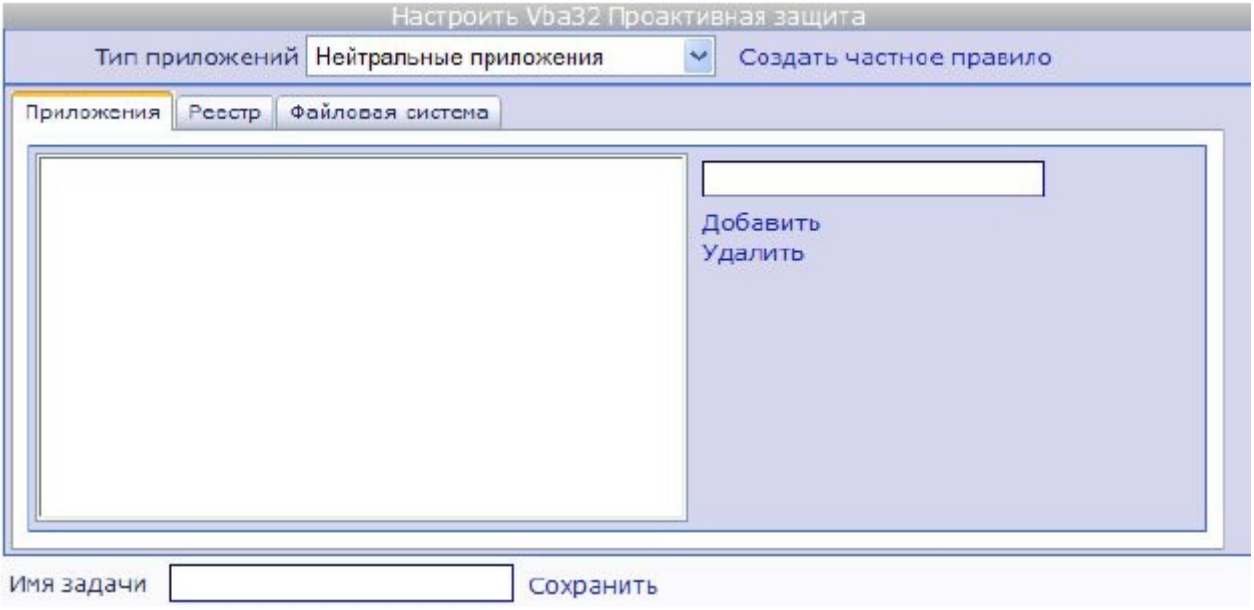


Настроить Vba32 Проактивная защита

Данная задача дает возможность настроить модуль проактивной защиты. Для настройки необходимо выбрать профиль из списка и выдать задачу.

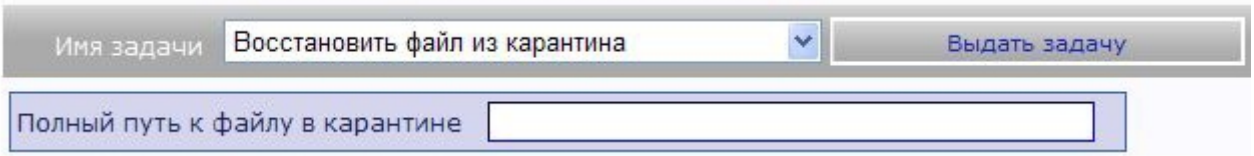


Для создания профиля необходимо нажать кнопку «Создать». После этого появится страница, на которой осуществляется полная настройка профиля.



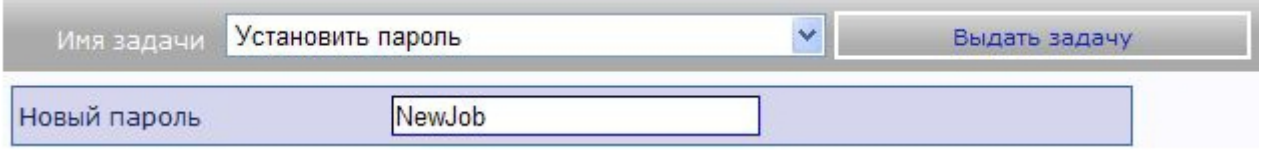
Восстановить файл из карантина

Данная задача позволяет восстановить файл из карантина. Для этого необходимо указать полный путь файла в карантине. Эта информация может быть получена из соответствующего события *vba32.virus.suspict*.



Установить пароль

Данная задача дает возможность установить пароль на Диспетчер Vba32 (аналогично нажатию кнопки «Пароль» на вкладке «Общее» Диспетчера). В поле «Новый пароль» необходимо ввести новый пароль для изменения настроек и режимов Диспетчера.



Настроить защиту устройств

Данная задача позволяет настроить модуль защиты устройств:

Доступны три режима:

- Выключить –выключает модуль.
- Включить – включает модуль.
- Регистрировать события – включает модуль с ограниченной функциональностью, которая позволяет только регистрировать события.

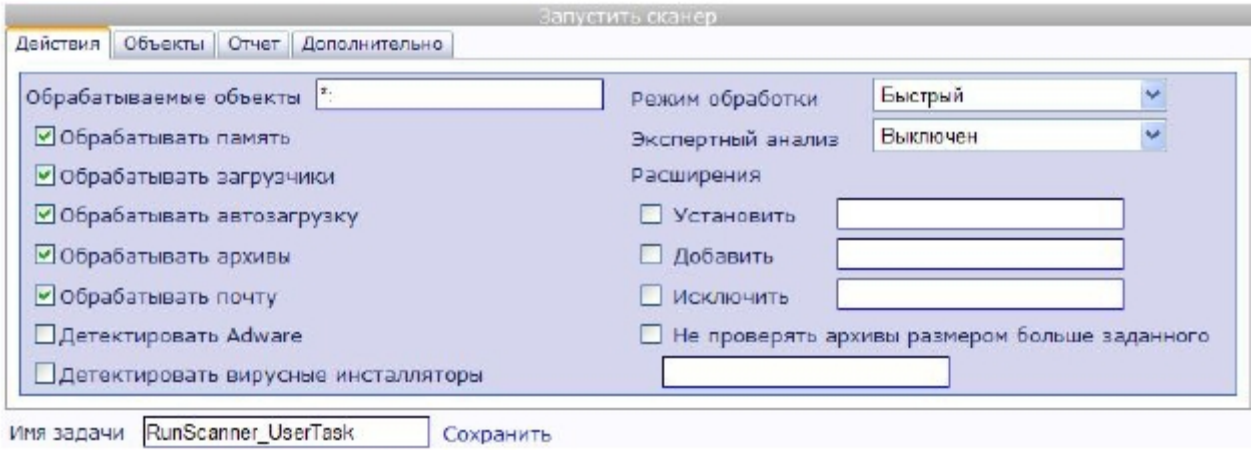
Запросить политику

Данная задача заставляет удаленный агент администрирования обратиться за политикой на сервер ЦУ и применить ее после получения.

У задачи нет параметров.

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».



Внимание! Не льзя сохранять задачи без параметров. Запрещено давать пользовате льским задачам имя как у любой из базовых задач (на любом из поддерживаемых языков).

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. Настройка Центра Управления

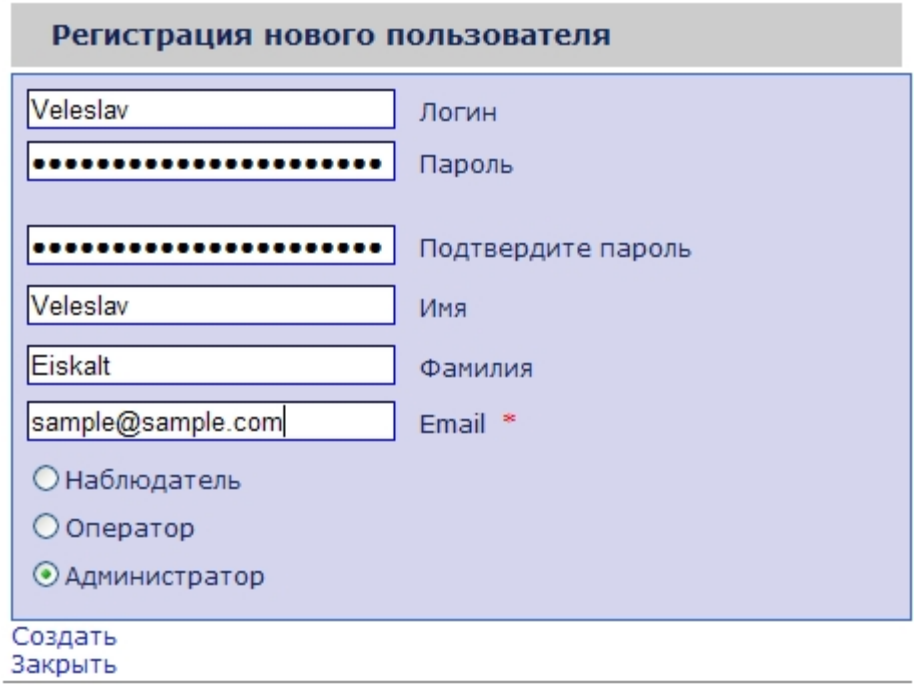
4.1 Управление учетными записями

Центр Управления Vba32 требует авторизации для просмотра любой из своих страниц. Чтобы иметь возможность войти в систему, надо завести учетную запись. Центр Управления может поддерживать 128 учетных записей пользователей. Количество пользователей, одновременно работающих с Центром Управления, ограничено аппаратными ресурсами сервера антивирусной защиты.

Создание учетной записи пользователя

Внимание! Создание, редактирование, удаление пользователя може т быть произведено тольк о при работе в Центре Управления под учетной записью с правами администратора.

Для создания учетной записи пользователя, надо нажать в меню «Администрирование» ссылку «Пользователи», затем – «Создать пользователя». Появится форма регистрации пользователя.



Необходимо заполнить следующие поля:

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

Внизу формы находится выбор роли пользователя. Существуют три роли:

- Наблюдатель – позволяет просматривать списки компьютеров, событий, компонентов и процессов, а также статистику;
- 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;

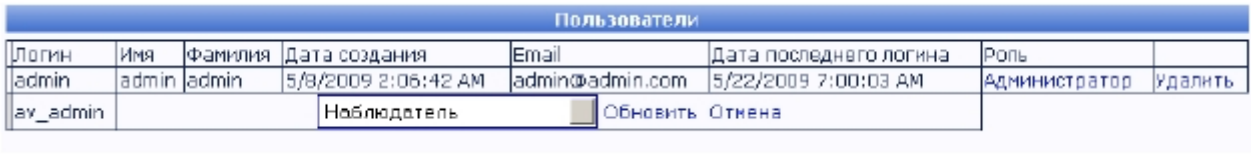
- Администратор – позволяет, помимо всех возможностей оператора, изменять настройки обслуживания базы данных (страница «Обслуживание»), уведомлений (страница «Уведомления»), самообновления (страница «Обновление). Кроме того, администратор может создавать пользователей и управлять ими (страницы «Регистрация» 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 красной звездочкой.

Изменение роли пользователя

Внимание! Создание, редактирование, удаление пользователя може т быть произведено тольк о при работе в Центре Управления под учетной записью с правами администратора.

Для изменения роли пользователя необходимо открыть список пользователей, для этого в меню «Администрирование» нажать ссылку «Пользователи». В списке напротив учетной записи, у которой надо изменить роль, нажать на ссылку, указывающую его текущую роль.



Появится выпадающий список, в котором надо выбрать новую роль пользователя, после чего нажать ссылку «Обновить». Для отмены действия можно нажать ссылку «Отмена». Результаты изменения можно сразу увидеть в списке пользователей.

Подробнее о ролях пользователей можно прочитать в разделе «Создание учетной записи».

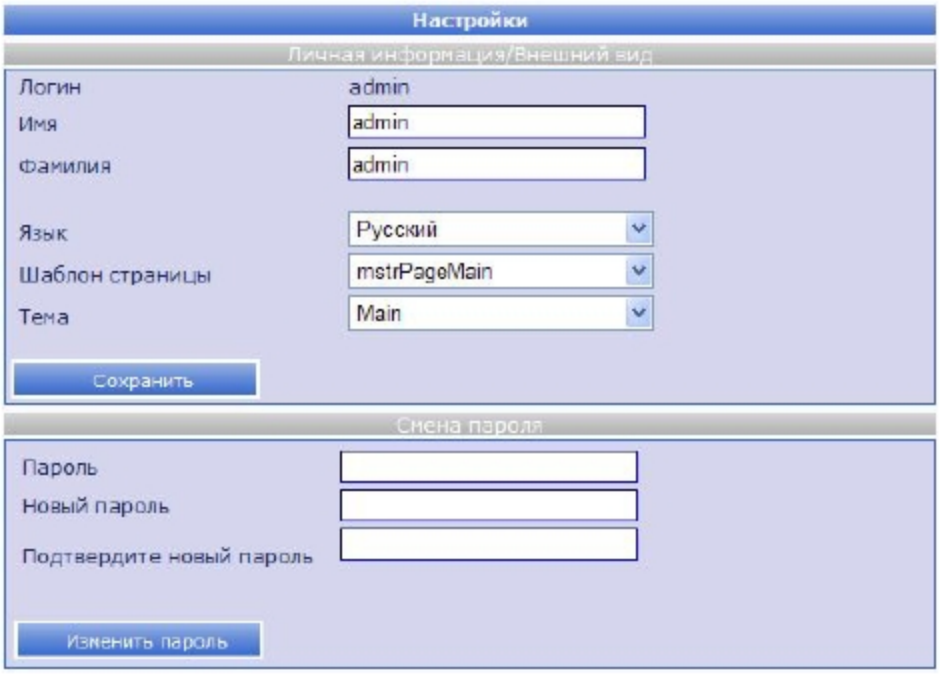
Удаление учетной записи

Внимание! Создание, редактирован ие, удаление уче тной записи может быть прои зведено только при работе в Центре Управления под учетной записью с правами администратора.

Для удаления учетной записи необходимо открыть список пользователей, для этого в меню «Администрирование» нажать ссылку «Пользователи». В списке напротив нужной учетной записи нажать на ссылку «Удалить», подтвердить свои действия.

Изменение личной информации и пароля

Web-интерфейс Центра Управления предоставляет возможность пользователю изменять свою личную информацию и пароль. Для этого необходимо в меню «Настройки» нажать на ссылку «Основные», появится страница настроек.



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 новую учетную запись 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.

4.2 Настройка графического интерфейса

Web-интерфейс Центра Управления Vba32 является гибко настраиваемым под пожелания пользователя, поддерживает различные шаблоны оформления, цветовые схемы и темы.

Большинство настроек применяются только для текущего пользователя; если данная настройка распространяется на всех пользователей, об этом будет упомянуто отдельно.

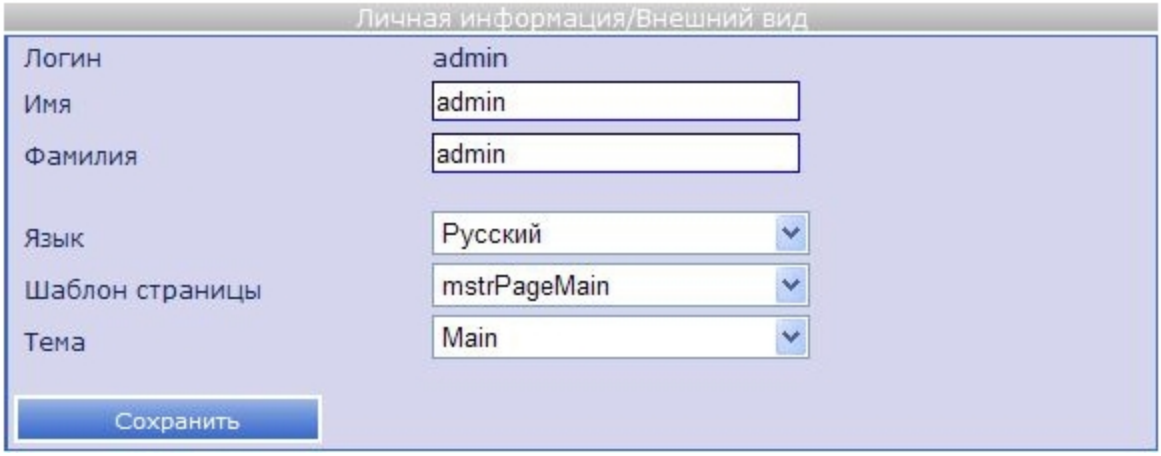
Настройки внешнего вида сохраняются и действуют при последующих входах в Центр Управления.

Настройка шаблона оформления

Существует несколько вариантов оформления и взаимного расположения элементов на страницах Центра 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».



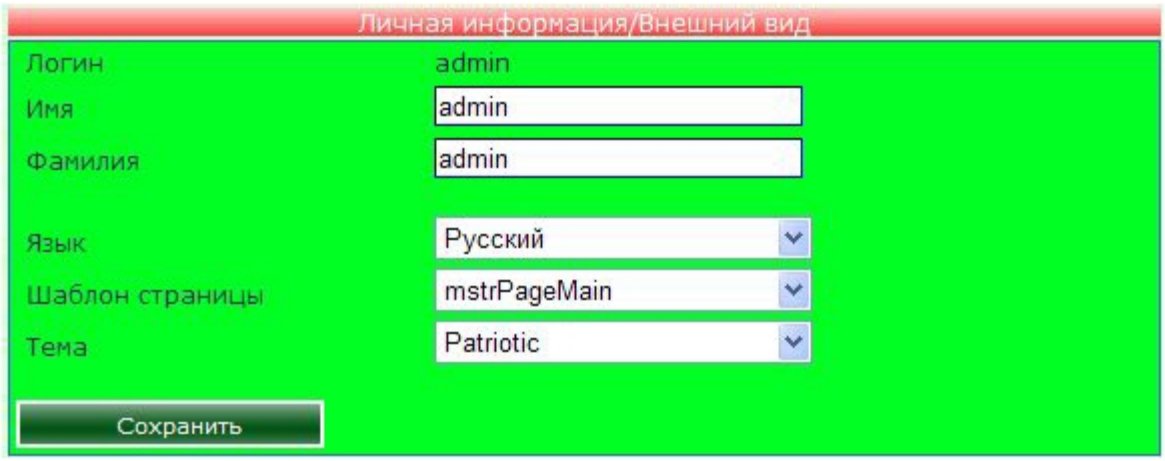
После выбора необходимого шаблона надо нажать на ссылку «Сохранить». Настройки применяются немедленно.

Настройка темы оформления

Центр Управления Vba32 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».

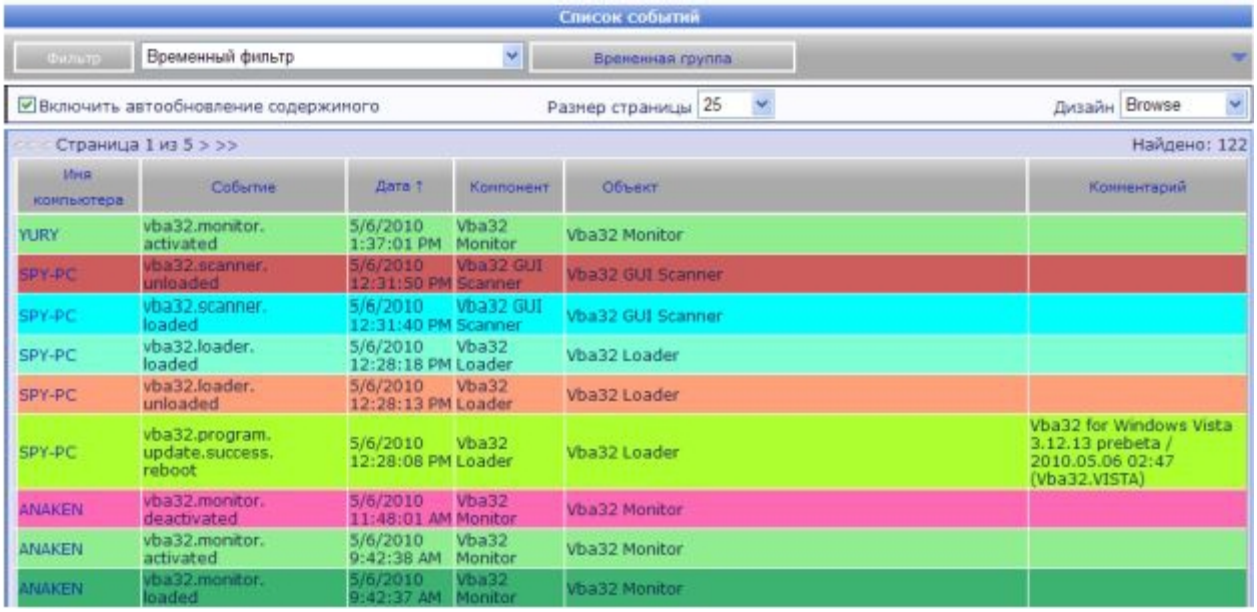


После выбора необходимой цветовой темы надо нажать на ссылку «Сохранить». Настройки применяются немедленно.

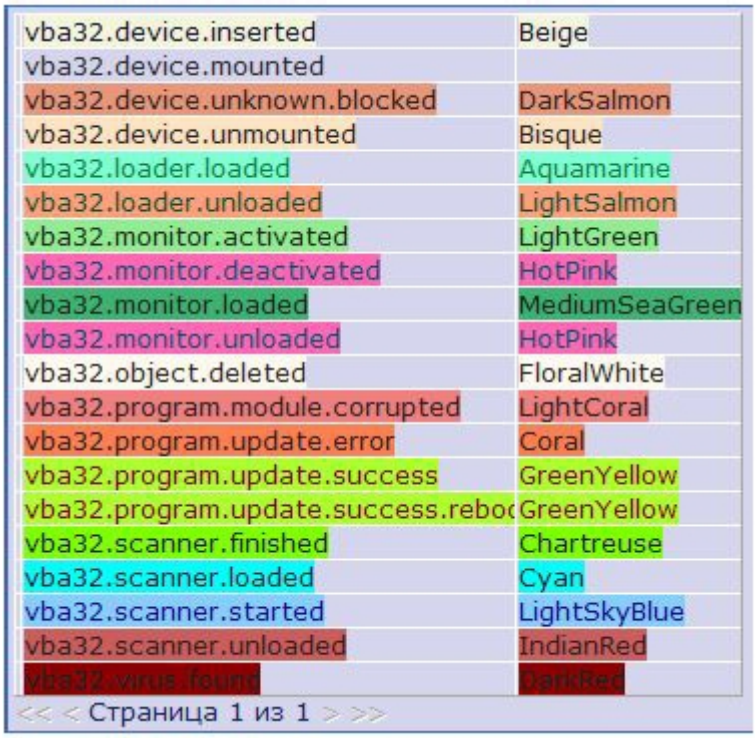
Настройка цветового оформления событий

> **Примечание:** Данная настройка действует для всех пользователей Центра Управления.

Центр Управления Vba32 позволяет применять цветовую раскраску для различных типов событий, отображаемых на странице «Список событий».

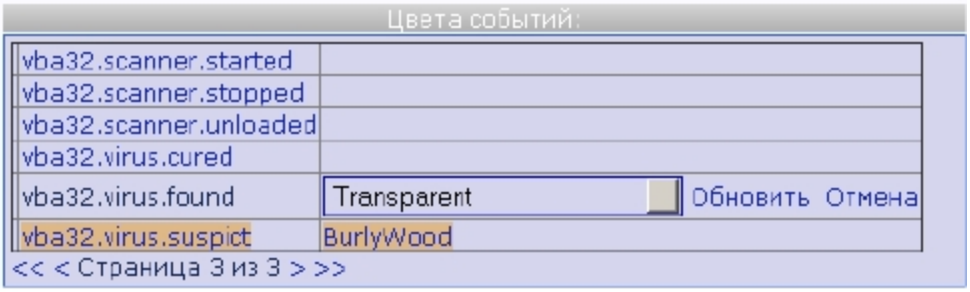


Цветовая схема событий настраивается на форме «Цвета событий» страницы «Настройки». Для ее открытия надо в меню «Настройки» нажать на ссылку «Дополнительно» и перейти на вкладку «Цвета событий».



Список типов 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 надо нажать на его название, в появившемся выпадающем списке выбрать нужный цвет и нажать «Обновить».



Настройки применяются немедленно, результаты можно увидеть на странице «Список событий».

Настройка цветового оформления таблицы компьютеров

Центр Управления Vba32 позволяет выделять отдельные компьютеры в списке компьютеров различными цветами, в зависимости от полученной информации. Для этого необходимо в меню «Настройки» нажать на ссылку «Дополнительно» и перейти на вкладку «Настройка цветов».

Механизм задания цветовой палитры следующий:

Последняя активность, *последнее обновление* – сначала задается более ранний интервал, затем - более поздний.

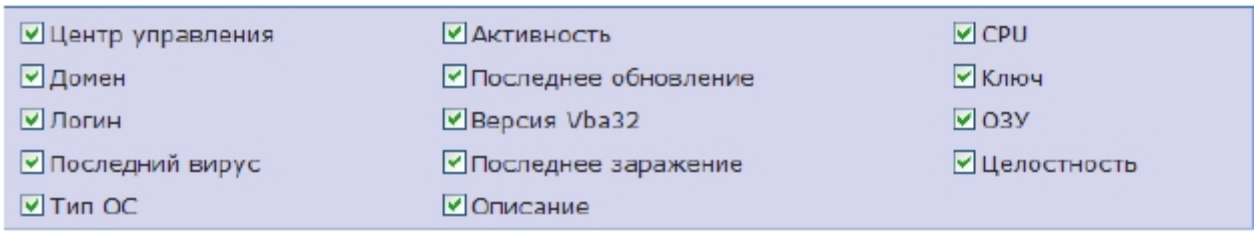
Последнее заражение – сначала задается более поздний интервал, затем - более ранний.

В зависимости от положения в списке параметров и истинности/ложности заданных условий, будет применен соответствующий цвет. Более высокое положение в списке имеет более высокий приоритет.

Настройка отображения столбцов в списке компьютеров

Центр Управления Vba32 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» и выбрать вкладку «Отображать столбцы в списке компьютеров». Поля, которые должны отображаться в списке компьютеров, необходимо отметить флажками.



Для применения настроек необходимо нажать на ссылку «Сохранить».

Настройки автоматического асинхронного обновления содержимого

При просмотре табличных списков при помощи web-интерфейса для получения наиболее актуальных данных надо принудительно обновлять страницу в браузере. 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.

Внимание! Автоматическое обнов ление содержимого со здает 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».

4.3 Настройка уведомлений

Центр Управления Vba32 предоставляет возможность уведомления уполномоченных лиц при регистрации того или иного события. Существуют три типа уведомлений:

- по электронной почте;
- по jabber;
- при помощи net send.

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

Примечание: Рекомендуется для уведомлений использовать локаль ные сервера: почтовый и jabber.

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

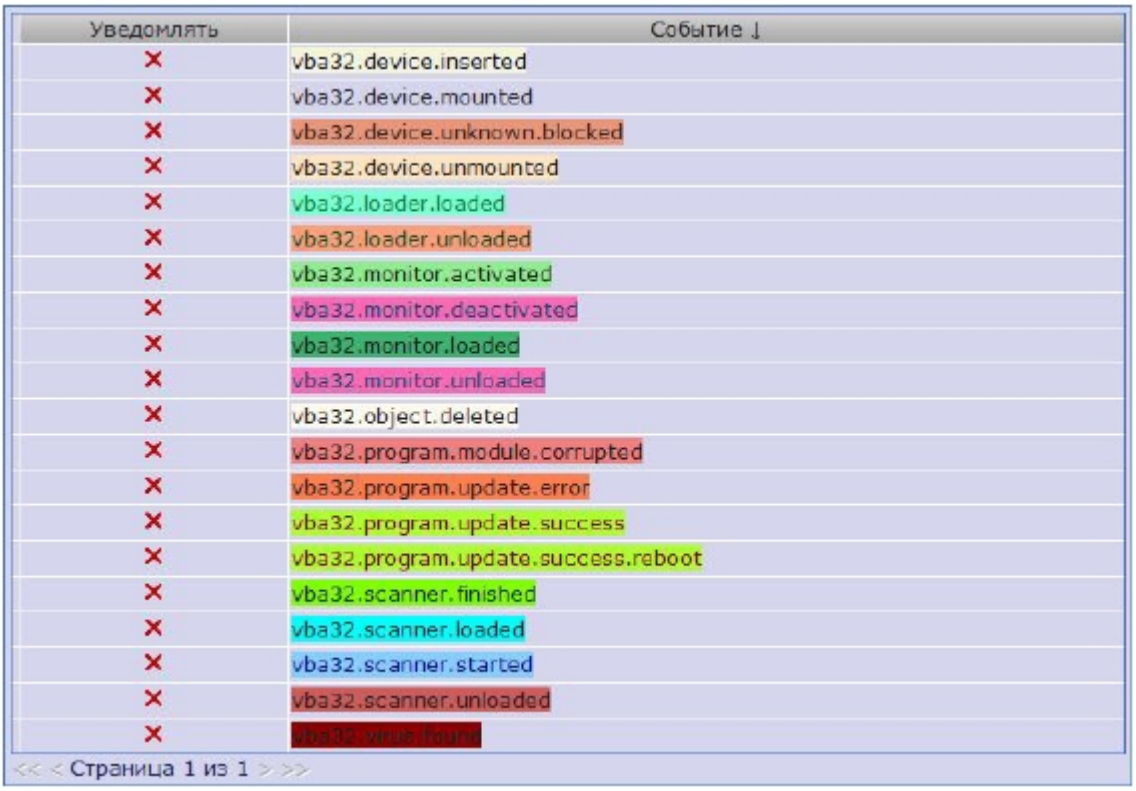
Внимание! Данные настро йки могут быть прои зведены только при работе в Центре Управления под учетной записью с правами администратора.

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

Выбор события, для которого будет производиться настройка уведомлений

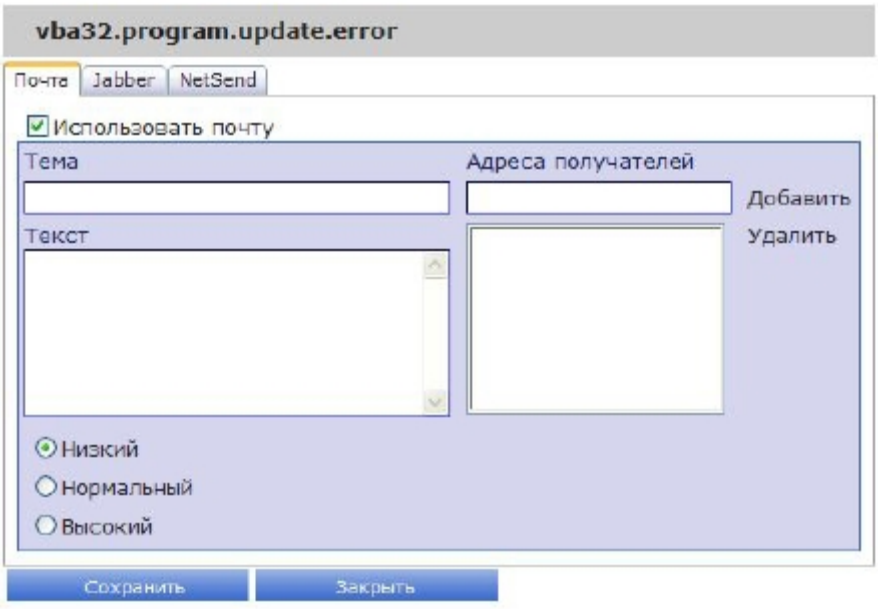
На вкладке «Зарегистрированные события» выводится многостраничный список событий, зарегистрированных в системе. Перемещение по страницам происходит по стандартному алгоритму: ссылки > и < показывают следующую и предыдущую страницы соответственно, << и >> - первую и последнюю.

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 птичка – уведомления будут отправлены. Для изменения настройки надо нажать на иконку, и та изменится на противоположную.



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 нажать на имя этого события. После этого появится всплывающее окно.



Настройка уведомлений по электронной почте

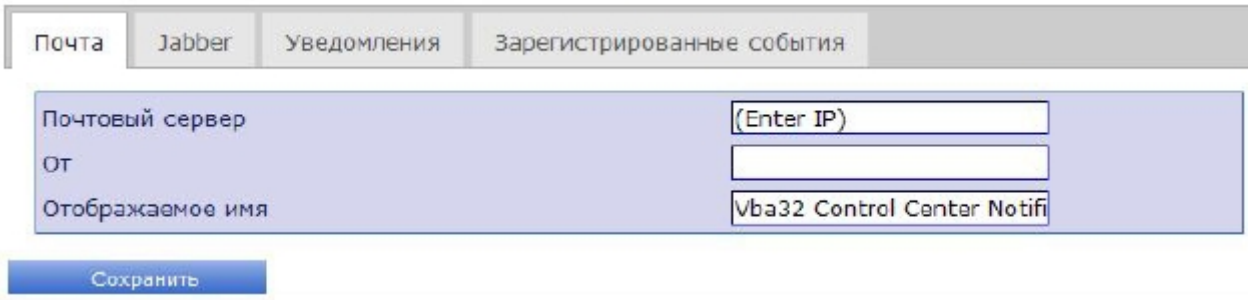
Чтобы иметь возможность отправлять уведомления по электронной почте, необходимо указать почтовый сервер. Для этого служит форма «Настройки почты» страницы «Настройки сервиса уведомлений».

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

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

Внимание! Некотор ые поч тов ые сервера требуют ука зать реа льно су ществующий почтов ый ящик.

В поле «Отображаемое имя» необходимо ввести имя, которое будет отображаться в почтовом клиенте вместо адреса электронной почты, указанного 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 справа от списка событий нажать на ссылку «Почта».

Для включения почтового уведомления для данного события надо отметить флажок «Использовать почту».

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».

Настройка уведомлений по jabber

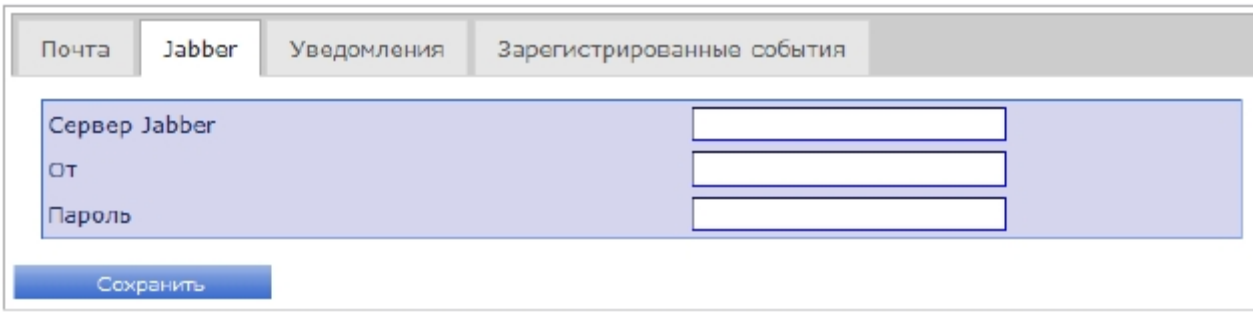
Чтобы иметь возможность отправлять уведомления по jabber, необходимо указать сервер и учетную запись jabber. Для этого служит вкладка «Настройки Jabber» страницы «Настройки сервиса уведомлений».

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).

В поле «От» надо ввести JID (идентификатор учетной записи), от имени которого будут рассылаться письма. Данную учетную запись необходимо заранее зарегистрировать, используя сервисы Вашего 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 справа от списка событий нажать на ссылку «Jabber».

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».

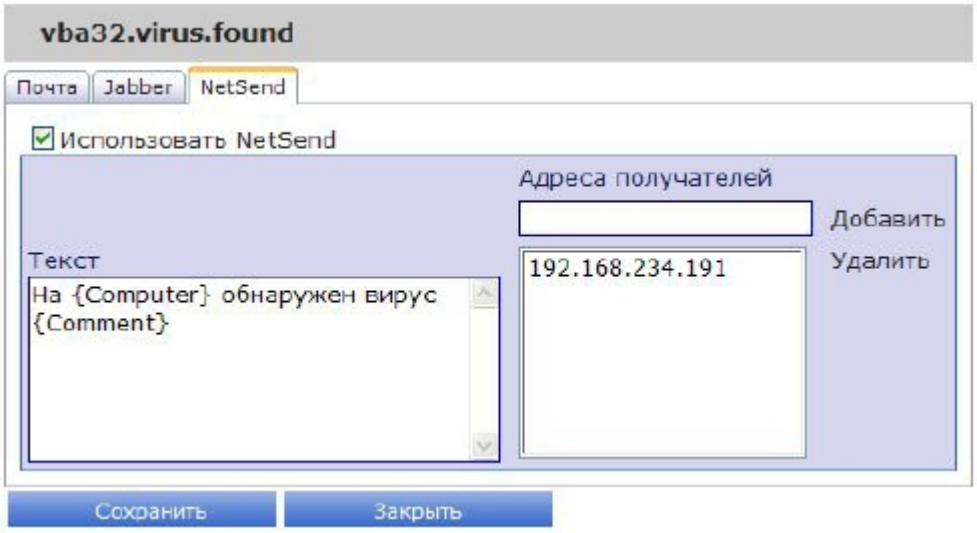
В поле «Текст» надо ввести текст уведомления, при этом можно использовать подстановочные макросы (подробнее описано в пункте «Подстановочные макросы в теме и тексте уведомления»).

Для применения настроек необходимо нажать на ссылку «Сохранить».

Настройка уведомлений при помощи net send

> **Внимание!** Для корректн ой работы уведомлений net send на сервере и компьютере получате ля должна быть запущена служ ба «Служба сооб щен ий». Данная функцио нальность 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 справа от списка событий нажать на ссылку «NetSend».



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».

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:

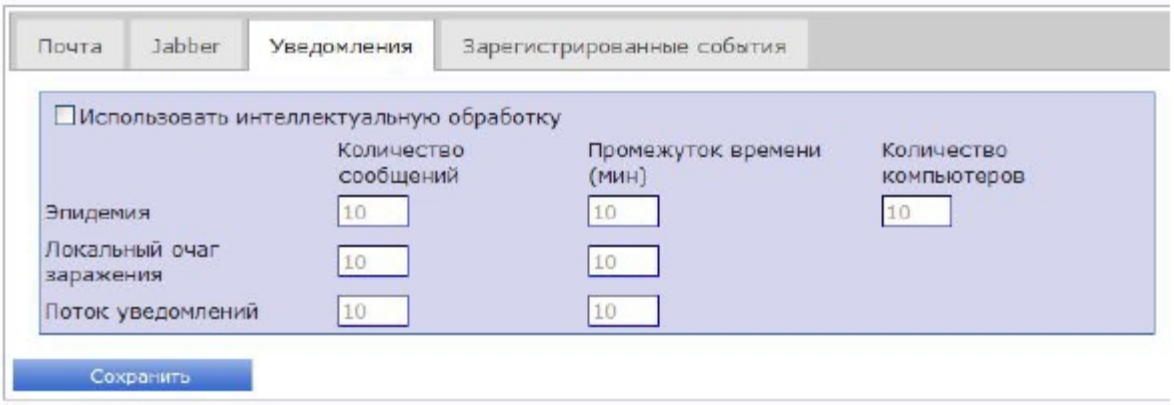
- {Computer} – имя компьютера, на котором произошло событие;
- {IPAddress} – IP-адрес компьютера, на котором произошло событие;
- {EventName} – имя произошедшего события;
- {EventTime} – дата и время наступления события;
- {Component} – компонент, сгенерировавший событие;
- {Object} – объект, с которым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

Например, уведомление об обнаружении вируса может иметь следующий вид:

ВНИМАНИЕ! На компьютере {Computer} обнаружен вирус {Comment} в {Object} ({Component})

4.4 Интеллектуальная обработка потока событий

Центр Управления предоставляет возможность управлять потоком уведомлений о наступлении какого-то события. Для этого служит вкладка «Уведомления» одноименной страницы.



Для включения механизма контроля необходимо установить флажок «Использовать интеллектуальную обработку» и задать необходимые настройки.

- *Эпидемия* – настройки, позволяющие определить массовое заражение одной вредоносной программой несколькими рабочими станциями. Генерируется одно специальное сообщение – vba32.cc.GlobalEpidemy. Событие о нахождении этого вируса перестает посылаться в течение заданного периода.
- *Локальный очаг заражения* – настройки, позволяющие определить локальный источник заражения. Учитываются разные типы вредоносных программ. Генерируется одно специальное сообщение – vba32.cc.LocalHearth. Событие о нахождении вируса на зараженной рабочей станции перестает посылаться в течение заданного периода.
- *Поток уведомлений* – позволяет предотвратить массовую рассылку других типов сообщений.

4.5 Настройка обслуживания базы данных

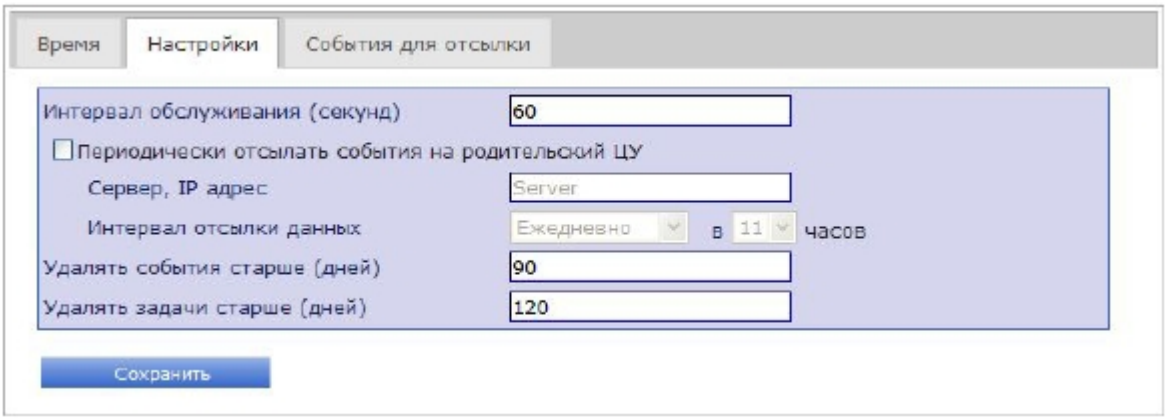
Хранилищем данных Центра Управления Vba32 является его база данных. С течением времени база может значительно увеличиться в размерах, снижая эффективность работы Центра Управления.

Внимание! Необходимо следить за размером базы данных Центра Управления. Чем больше ее размер, тем больше требования к аппара тным ресурсам сервера баз данных. Настоя тель но рекомендуется периодически делать резервные копии базы данных.

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

Внимание! Данные настро йки могут быть прои зведены только при работе в Центре Управления под учетной записью с правами администратора.

Для настройки обслуживания базы данных необходимо в меню «Администрирование» нажать ссылку «Обслуживание». На форме «Настройки» ввести в поле «Удалять события старше (дней)» количество дней, по истечению которых события будут удалены из базы данных.



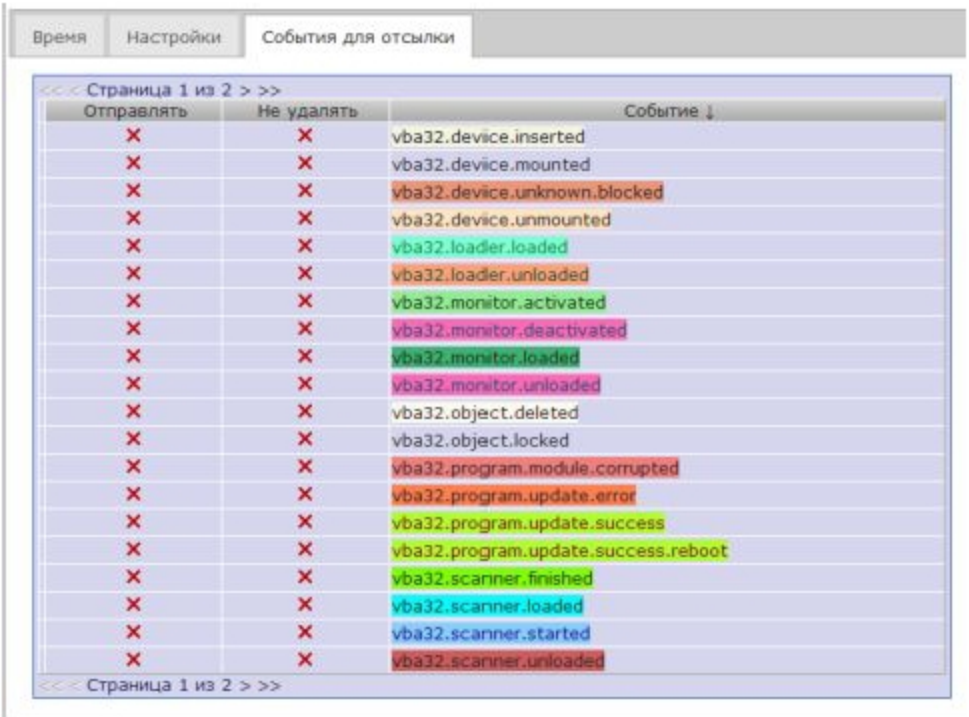
Помимо очистки базы данных от устаревших событий, сервис периодического обслуживания также выставляет выданным задачам статус «Таймаут выполнения», если в течение минуты не было ответа от Агента; выполняющимся задачам – статус «Таймаут выполнения», если задача не завершилась в течение 2 часов.

На этой же форме можно настроить период, по истечении которого сервис производит проверку базы данных 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 базы данных, производится на этой же странице «Установки для сервиса периодического обслуживания». На форме «События для отсылки» выводится многостраничный список событий, зарегистрированных в системе. Перемещение по страницам происходит по стандартному алгоритму: ссылки > и < показывают следующую и предыдущую страницы соответственно, << и >> - первую и последнюю.

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



Изменения вступают в силу немедленно.

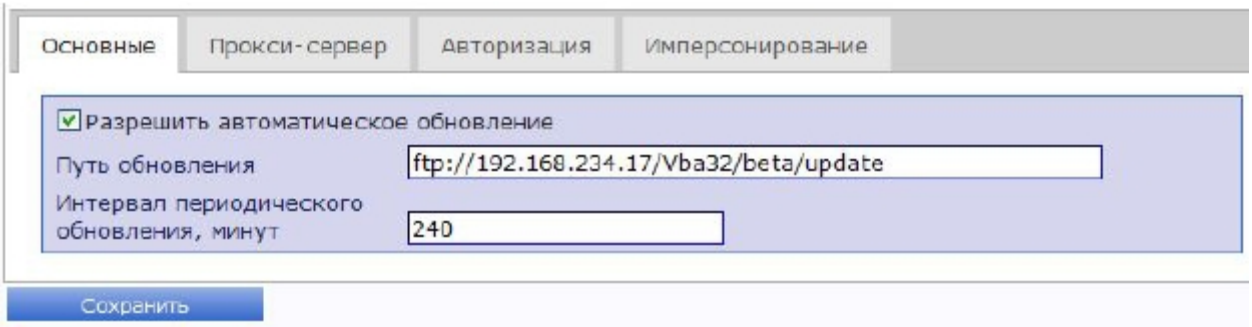
4.6 Настройка самообновления

Центр Управления Vba32 обладает возможностью самообновления и обновления своих компонентов стандартным для продуктов компании «ВирусБлокАда» образом.

При самообновлении с локального ресурса обновлений, созданного Центром Обновлений Vba32, необходимо убедиться, что в настройках ЦО включена синхронизация комплектации VBA32AAW.

Внимание! Данные настро йки могут быть прои зведены только при работе в Центре Управления под учетной записью с правами администратора.

Для изменения настроек самообновления надо в меню «Администрирование» нажать на ссылку «Обновление».



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», «Использовать имперсонирование».

Для применения настроек необходимо нажать на ссылку «Сохранить».

Обновление из сетевого каталога

Сервис обновлений, входящий в состав Центра 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 Центр Управления, и компьютер, с которого производится обновление, входят в один домен, необходимо установить флажок «Использовать имперсонирование» и ввести имя доменного пользователя и пароль в соответствующие поля формы «Обновление».

Внимание! Данный пользователь должен име ть право чтения из сетевого каталога обнов лений. Как правило, достаточно ввести реквизиты своего доменного пользователя.

В случае если обновление проводится с компьютера, принадлежащего рабочей группе, необходимо установить флажок «Использовать авторизацию» и ввести имя пользователя и пароль для доступа в соответствующие поля формы «Обновление».

В любом случае, необходимо ввести путь к сетевому каталогу обновлений в поле «Путь обновления».

Для применения настроек необходимо нажать на ссылку «Сохранить».

Обновление с ftp/http-сервера

Если обновление производится с ftp или http сервера, доступ к которому осуществляется через прокси, то необходимо установить флажок «Использовать прокси-сервер» 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 (при необходимости отметив флажок «NTLM-авторизация»).

Если ftp-сервер требует авторизации, необходимо установить флажок «Использовать имперсонирование» и ввести имя пользователя и пароль для доступа в соответствующие поля формы.

В любом случае, необходимо ввести путь к сетевому каталогу обновлений в поле «Путь обновления».

Для применения настроек необходимо нажать на ссылку «Сохранить».

4.7 Экспорт и импорт пользовательских настроек

Центр Управления Vba32 предоставляет возможность сохранения всех или части пользовательских настроек (фильтров по спискам, созданных задач) в файл. Такая возможность может потребоваться, например, при переустановке Центра Управления или необходимости создать нового пользователя с такими же настройками, как у уже существующего.

> **Примечание:** Настройки графического интерфейса не экспортируются.

Экспорт настроек в файл

Для сохранения настроек учетной записи 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, событий, компонентов, процессов, 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:** Фа йл с настройкам и будет сохранен на клиентском компью тере – том, где web-интерфейс открыт в браузере.

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 на странице «Экспорт/Импорт» ввести в поле ввода путь к файлу с настройками (или воспользоваться стандартным диалогом выбора файлов, нажав на кнопку «Обзор»), после чего нажать на ссылку «Импорт».

Удаление всех пользовательских настроек

Чтобы удалить некоторые из пользовательских настроек (фильтры компьютеров, событий, компонентов, процессов, задач, пользовательские задачи), необходимо на

странице «Экспорт/Импорт» отметить флажками соответствующие пункты и нажать на ссылку «Удалить».

4.8 Организация многоуровневой иерархической системы Центров Управления Vba32

В случае если Ваша организация состоит из значительного количества подразделений, распределенных территориально и имеющих связь с центральным офисом по выделенной линии, зачастую оптимальным решением может стать установка самостоятельных Центров Управления в отделениях. В таком случае администратор антивирусной защиты, ответственный за всю организацию, должен быть осведомлен о состоянии защиты на каждой рабочей станции и сервере, в том числе и в отделениях. Центр Управления Vba32 предлагает решение для данного вопроса – возможность отсылки определенных событий вышестоящему по иерархии Центру Управления. В случае если необходимо получить возможность управления рабочими станциями какого-либо из подчиненных Центров Управления, достаточно зайти на web-интерфейс этого подчиненного ЦУ.

Любой Центр Управления может стать дочерним, для этого надо включить периодическую отсылку событий на родительский ЦУ.

Настройка подчиненных Центров Управления

Внимание! Данные настро йки могут быть прои зведены только при работе в Центре Управления под учетной записью с правами администратора.

Для настройки отсылки событий надо в меню «Администрирование» нажать на ссылку «Обслуживание».

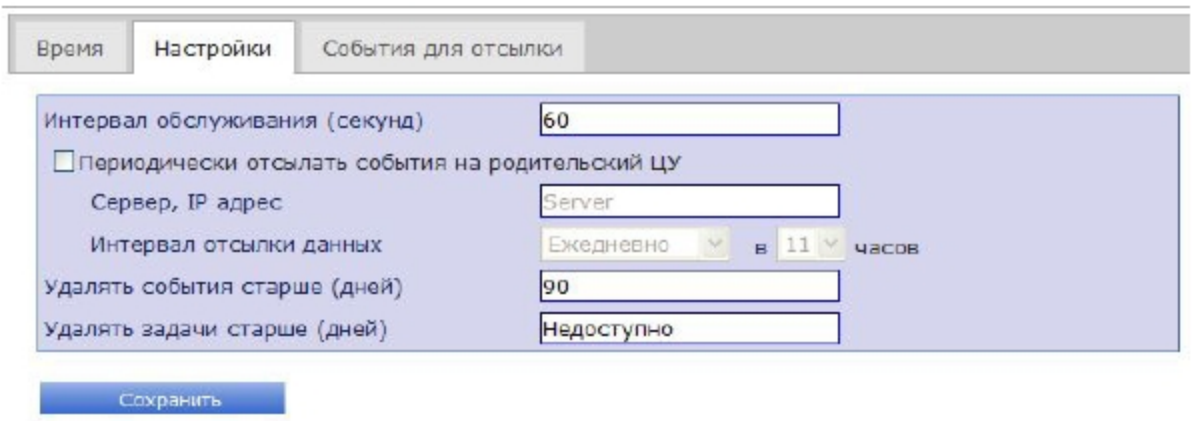
Чтобы включить отсылку, надо отметить флажок «Периодически отсылать события на родительский ЦУ», после чего ввести данные о родительском Центре Управления: имя или IP-адрес в поле «Сервер», в выпадающих списках «Интервал отсылки данных» выбрать периодичность отсылки. Для выключения отсылки достаточно снять флажок «Периодически отсылать события на родительский ЦУ».

Для применения настроек необходимо нажать на ссылку «Сохранить».

Центр Управления предоставляет возможность выбрать определенные типы событий, которые будут отсылаться на родительский. Как правило, целесообразно отсылать критичные события – обнаружение вредоносной программы и т.п.

Настройка событий, которые будут отсылаться на родительский Центр Управления, производится на этой же странице «Установки для сервиса периодического обслуживания». На форме «События для отсылки» выводится многостраничный список событий, зарегистрированных в системе. Перемещение по страницам происходит по стандартному алгоритму: ссылки > и < показывают следующую и предыдущую страницы соответственно, << и >> - первую и последнюю.

Слева от имени события, в колонке «Отправлять» в виде иконки представлена настройка – будут ли соответствующие события отосланы на родительский Центр Управления. Если в этой колонке стоит птичка – событие будет отправлено. Для изменения настройки надо нажать на иконку, и та изменится на противоположную.



Изменения вступают в силу немедленно.

Настройка родительского Центра Управления

На родительском Центре Управления не требуется делать никаких настроек.

Отображение событий от подчиненных Центров Управления

События от подчиненного Центра Управления будут выводиться в общем списке событий (страница «События»). Поле «Имя компьютера» будет содержать имя дочернего Центра Управления, который зарегистрировал данное событие. В поле «Объект» будет указано, на какой именно рабочей станции из подразделения произошло данное событие.

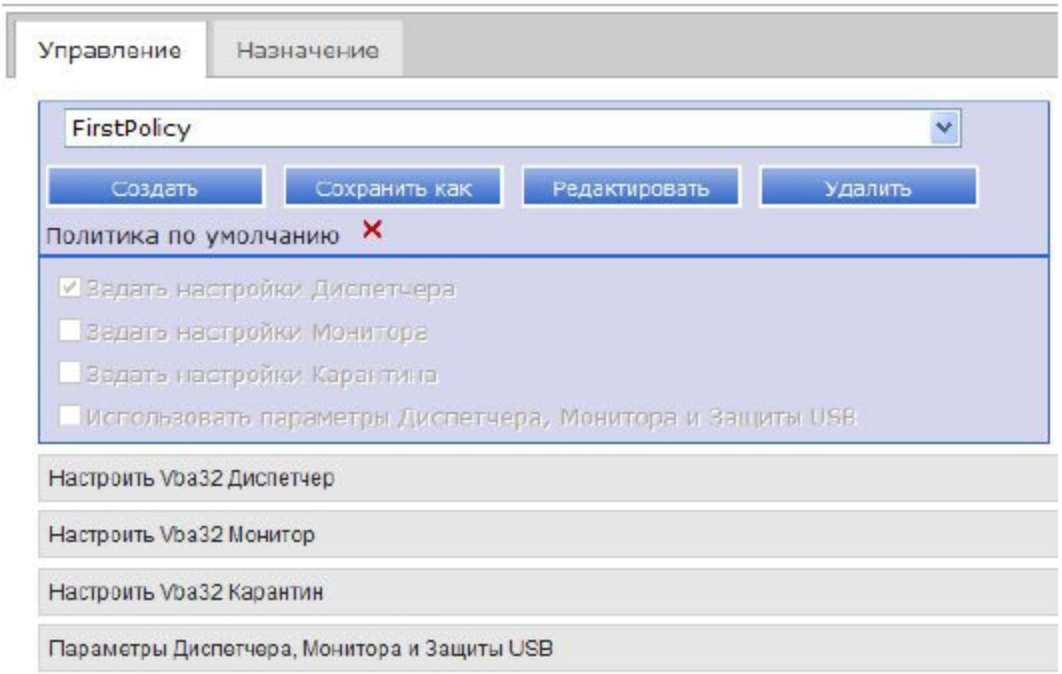
Подчиненный Центр Управления будет зарегистрирован в списке компьютеров на родительском, при этом поле «Центр Управления» будет отмечено птичкой.

5. Использование политик антивирусного комплекса

Политики антивирусного комплекса предназначены для принудительной установки на рабочей станции определенных настроек антивирусного комплекса Vba32. Доступна настройка следующих компонентов:

- Vba32 Диспетчер
- Vba32 Монитор
- Vba32 Карантин

Кроме того, возможно управление состоянием загрузки Диспетчера, состояниями Монитора и защиты USB.



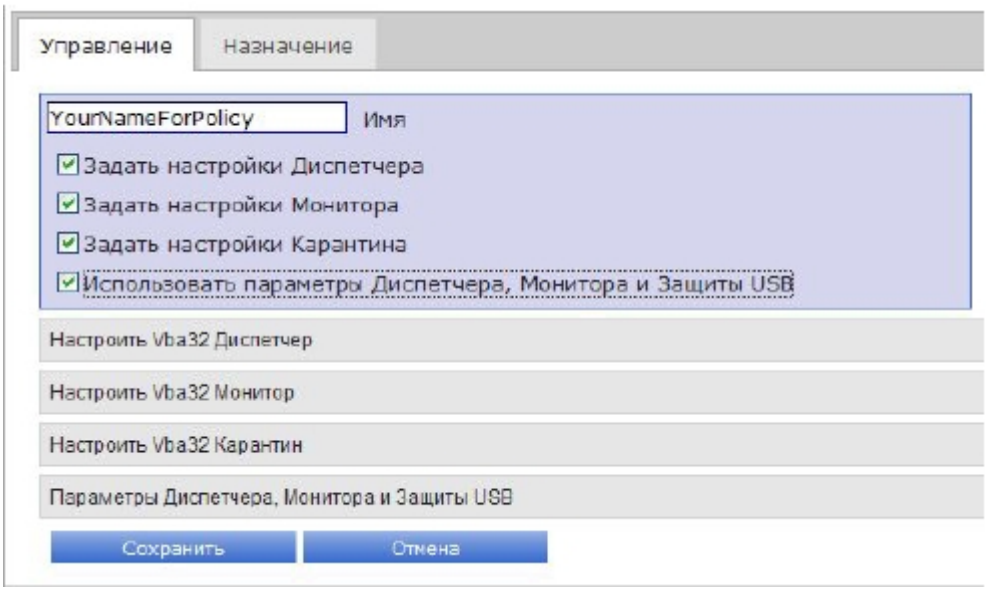
5.1 Создание политики

Для создания политики антивирусного комплекса необходимо перейти на страницу «Настройки политики», затем на вкладку «Создание политики». На данной вкладке задаются параметры новой политики. В поле для ввода «Имя» задается уникальное имя создаваемой политики.

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

- Настроить Vba32 Диспетчер
- Настроить Vba32 Монитор
- Настроить Vba32 Карантин
- Параметры запуска Диспетчера, Монитора и Защиты USB

Параметры политик задаются аналогично параметрам задач на странице списка компьютеров.



Параметры запуска Диспетчера и Монитора служат для возможности загружать/выгружать Диспетчер и включать/выключать Монитор.

Внимание!

Не допускается создавать пустую политику, т.е. нео бходимо вы брать один из доступ ных параметров.

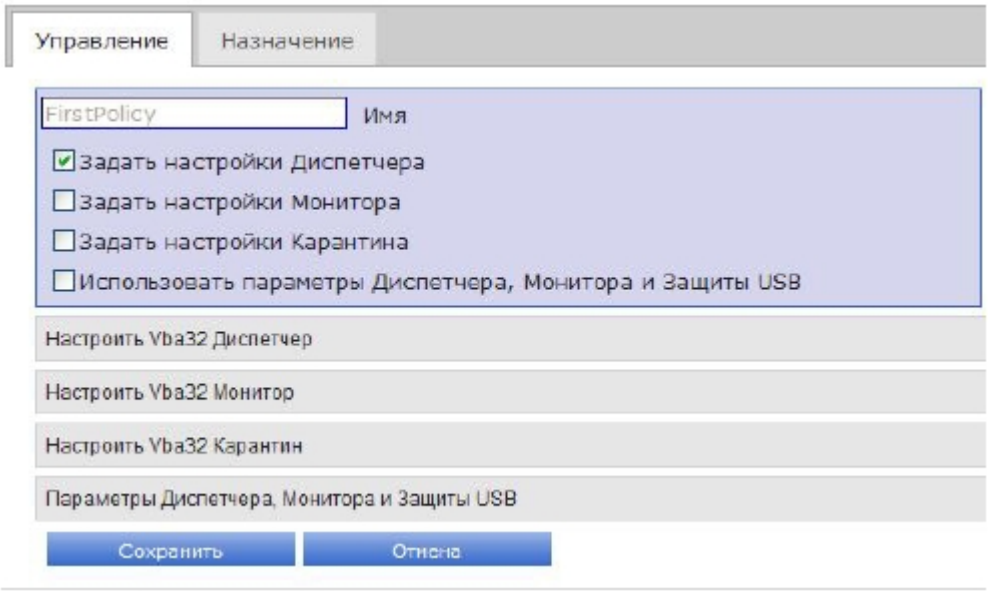
Не допускается создавать политику с существующим именем.

Не допускается создавать политику с настройками, не удовлетворяющим настройкам соответствующих используемых задач.

При выбранной нас тройке не загружать Диспетчер состояние Монитора не должно учитываться.

5.2 Редактирование политики

Чтобы изменить параметры используемой политики необходимо выбрать ее в выпадающем списке политик на странице списка компьютеров нажать кнопку «Редактировать», которая доступна в соответствующей выпадающей панели. После этого будет осуществлен переход на страницу «Настройки политики», где на вкладке «Создание политики» будет представлены настройки данной политики. При этом запрещено редактирование имени данной политики.



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

5.3 Удаление политики

Чтобы удалить используемую политику необходимо выбрать ее в выпадающем списке политик на странице списка компьютеров и нажать кнопку удалить, которая доступна в соответствующей выпадающей панели.

Все компьютеры, которые использовали эту политику, перестанут ее использовать

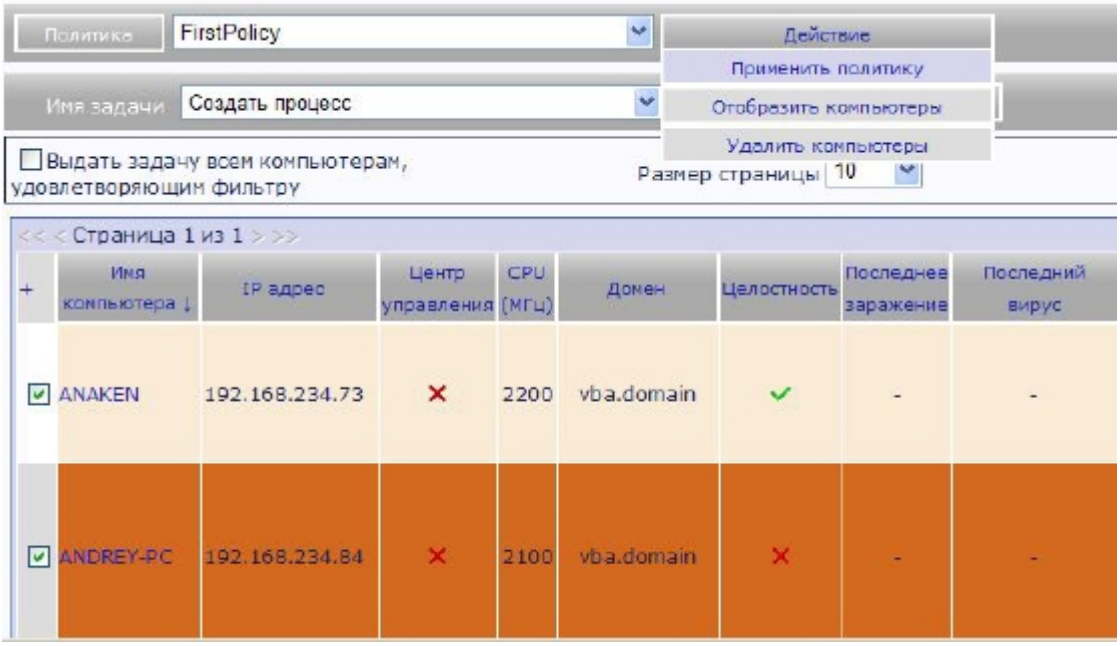
5.4 Назначение политики

Назначить политику определенному компьютеру или группе компьютеров можно двумя способами

- С помощью страницы списка компьютеров
- С помощью вкладки «Назначение политики» на странице «Настройки политики»

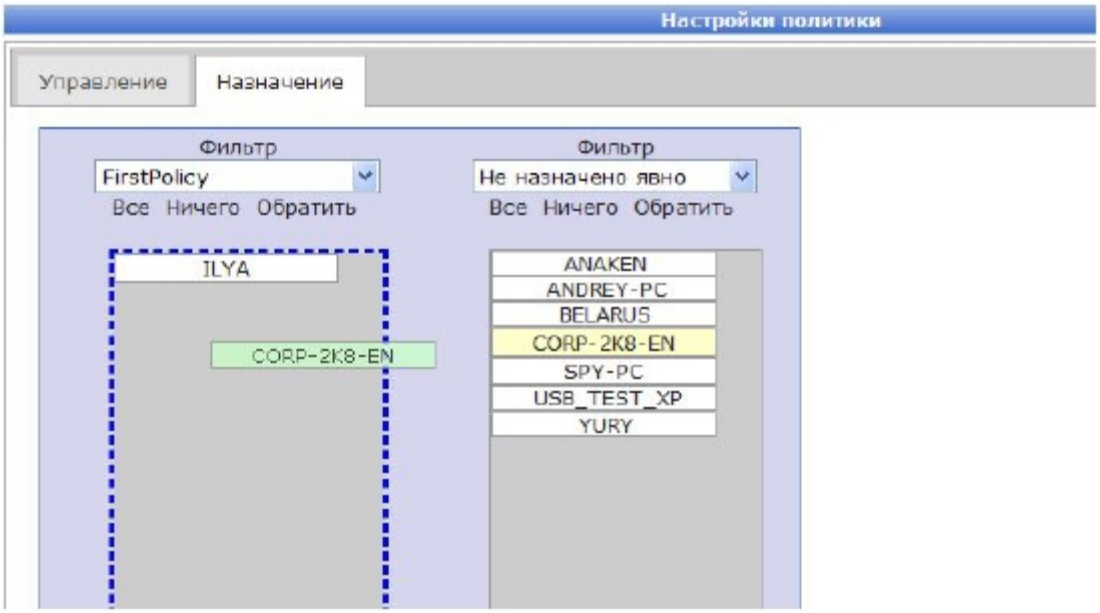
Для назначения политики на странице списка компьютеров необходимо выполнить следующие шаги:

- Выбрать ранее созданную политику из выпадающего списка политик
- Отметить отдельные компьютеры, отметив их флажками либо отметить все, используя флажок «Выдать задачу всем компьютерам, удовлетворяющим фильтру»
- Выбрать из меню «Действие» напротив имени политики пункт «Применить политику»



Для назначения политики на вкладке «Назначение политики» можно проделать следующие действия:

- Выбрать слева группу, в которой находится целевой компьютер.
- Выбрать справа необходимую политику
- Перетащить компьютер из левой группы в правую



То же самое актуально, если инвертировать расположение целевого компьютера и политики.

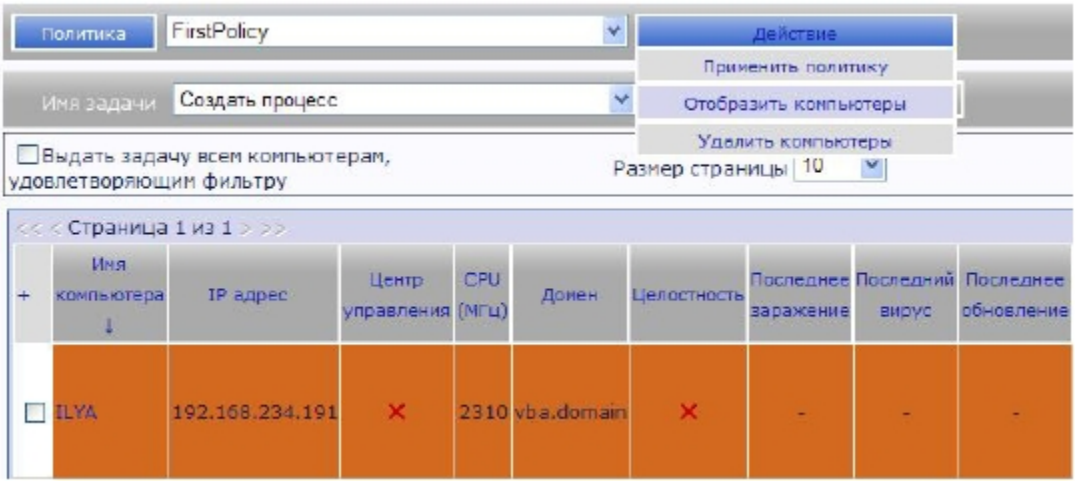
При необходимости для поиска в группе можно использовать пэйджинг

Первая группа предназначена для отображен ия компьютеров, которым не назначена ни одна из политик

Перенос компьютера из одинаковых групп не несет собой каких-либо изменений

5.5 Просмотр назначенных политик

На странице списка компьютеров можно просмотреть политики и назначенные им компьютеры. Для этого необходимо выбрать политику из выпадающего списка и в меню «Действие» выбрать пункт «Отобразить компьютеры». После этого на странице отобразиться стандартная таблица со списком компьютеров, для которых назначена данная политика.

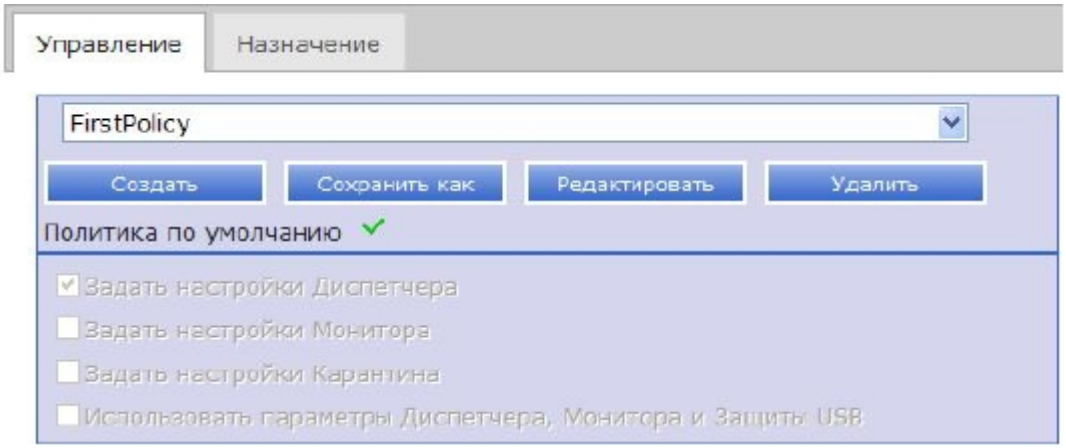


5.6 Использование политики по умолчанию

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 проделать сделать следующие шаги:

- Создать политику
- Выбрать ее на странице списка компьютеров
- На выпадающей панели политик нажать на кнопку «Политика по умолчанию»



После этого все компьютеры, которым явно не была назначена ни одна из политик, получат данную политику.

Чтобы просмотреть, какая политика является политикой по умолчанию, можно воспользоваться страницей «Политики». На вкладке «Назначение политик» в строке «Политика по умолчанию» отображается необходимая информация.

Политика по умолчанию может быть только одна

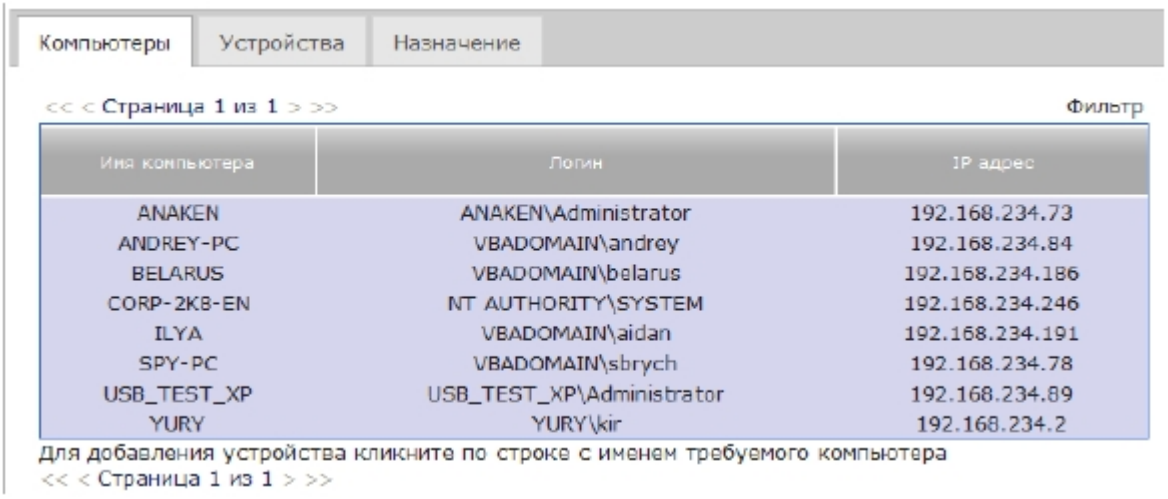
6. Управление доступом к съемным носителям

Центр управления позволяет конфигурировать специализированный драйвер управления съёмными носителями, который является частью антивирусного комплекса Vba32. Конфигурирование осуществляется на странице «Устройства».

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

6.1 Вкладка «Компьютеры»

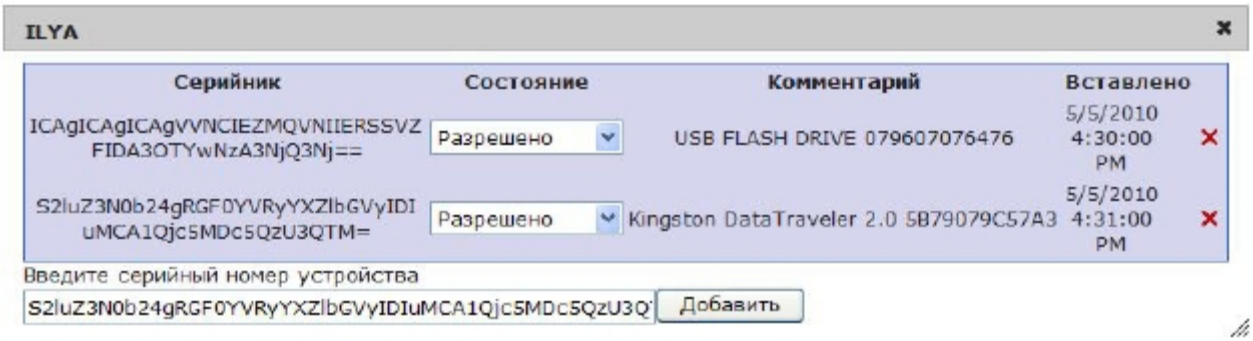
Вкладка «Компьютеры» предназначена для просмотра, добавления и изменения состояния устройств, используемых определенным компьютером. Для этого необходимо выбрать нужный компьютер в таблице щелкнуть на его имени. После этого появится диалоговое окно, в котором будет доступен список устройств, их состояний и панель добавления нового устройства.



Добавление нового устройства к компьютеру

Чтобы добавить новое устройство к компьютеру, проделайте следующее:

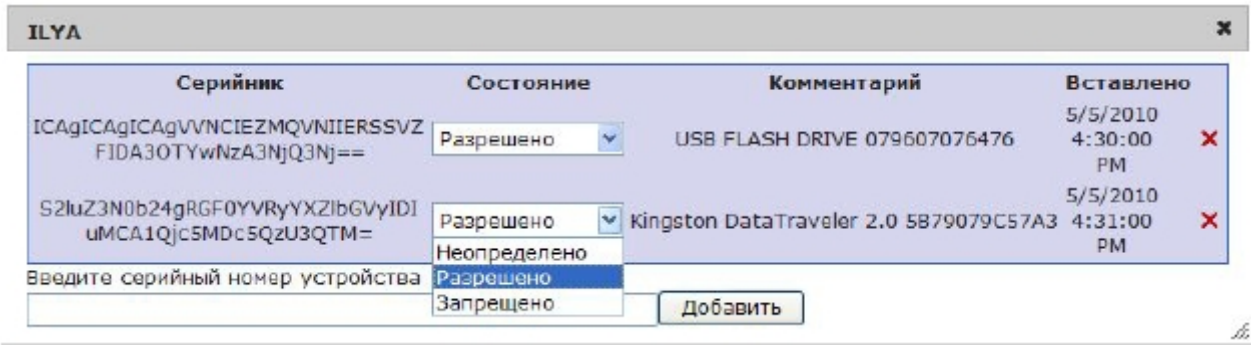
- Выберите нужный компьютер
- В появившемся диалоге введите в поле для ввода серийный номер устройства
- Нажмите кнопку «Добавить»



Если устройства не было в базе данных устройств, оно будет создано

Изменение статуса устройства компьютера

Чтобы изменить действие, выполняющееся над устройством, нужно щелкнуть на его текущем состоянии и выбрать из выпадающего списка нужное.



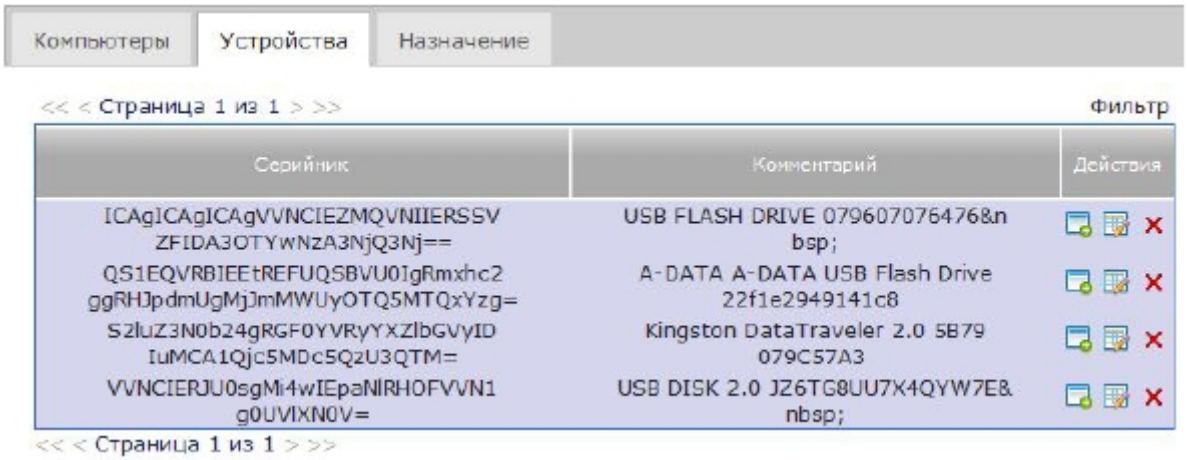
Удаление определенного устройства компьютера

Для удаления устройства компьютера необходимо нажать на ✕ напротив соответствующего устройства.

> Сама информация об устройстве не удаляется из базы данных

6.2 Вкладка «Устройства»

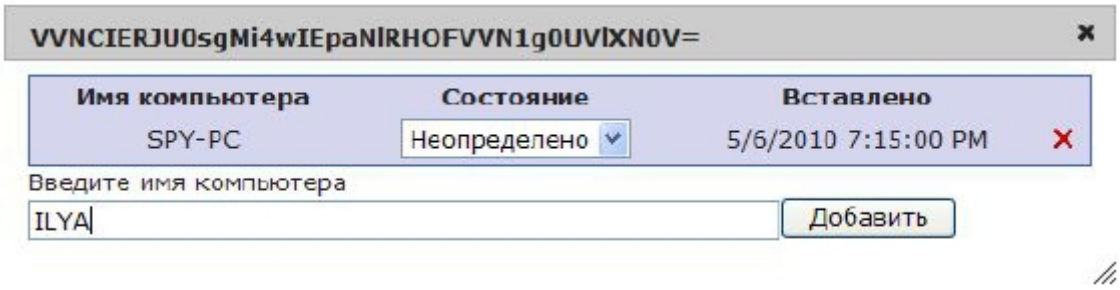
Вкладка «Устройства» предназначена для назначения определенному устройству компьютеров и действий над этим устройством.



Добавление компьютера к устройству

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

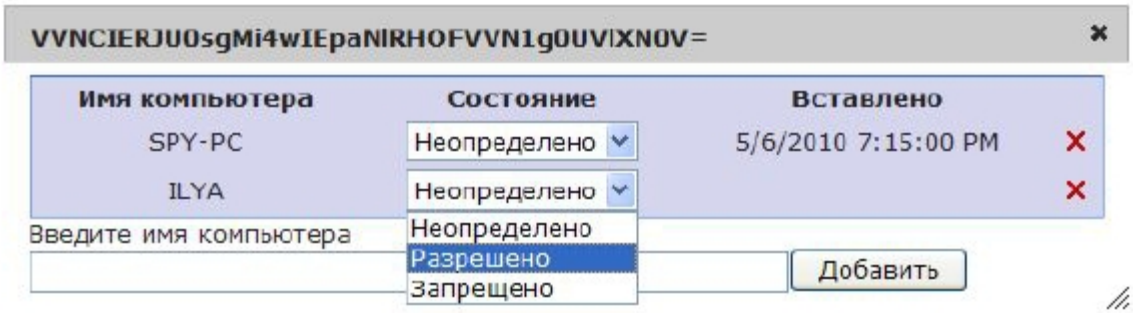
- Выбрать устройство
- В появившемся диалоге ввести имя существующего компьютера
- Нажать кнопку «Добавить»



В случае если такого компьютера не существует в базе данных, никаких измене ний не произойдет

Изменение статуса устройства компьютера

Чтобы изменить действие, выполняющееся над устройством, нужно щелкнуть на его текущем состоянии и выбрать из выпадающего списка нужное.



Удаление определенного компьютера устройства

Для удаления компьютера из списка в устройстве необходимо нажать на напротив соответствующего компьютера.

Сам компьютер удален из базы не будет

Добавление комментария к устройству

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

6.3 Вкладка «Назначение»

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

- Выбрать компьютер и устройство в таблице

- Нажать на кнопку ✓для разрешения или ✗ для блокировки

После выбора действия компьютер должен исчезнуть из списка

Для обновления таблиц на других вкладках рекомендуется обновить страницу