SoftControl

SClient 5.0.18

Руководство пользователя

Уважаемый пользователь!

Safe'N'Sec Corporation благодарит Вас за то, что выбрали продукт SoftControl SClient. Специалисты компании постарались, чтобы наше программное обеспечение отвечало самым высоким требованиям в области защиты информации и в то же время было простым и удобным в работе. Мы надеемся, что SoftControl SClient будет Вам полезен.

Почтовый адрес:
127106, Россия, Москва
Ботаническая ул., дом 10Д строение 1
Safe'N'Sec Corporation
Телефон:
+7 (495) 967-14-51
Факс:
+ 7 (495) 967-14-52
Электронная почта:
Общие вопросы и предложения: support@safensoft.com
Коммерческие вопросы: sales@safensoft.com
Веб-сайт компании: http://www.safensoft.com

Содержание

1. Введение

1.1 Назначение

SoftControl SClient (далее по тексту – SoftControl SysWatch) предназначен для защиты от несанкционированного доступа к информационным ресурсам серверов, функционирующих под управлением ОС семейства Microsoft® Windows®.

1.2 Возможности

SoftControl SysWatch является проактивным средством защиты, относящимся к классу систем предотвращения вторжений Host Intrusion Prevention System (HIPS). SoftControl SysWatch анализирует активность приложений и блокирует опасные действия, которые могут привести к неработоспособности системы или порче/потере конфиденциальной информации пользователя, обеспечивает защиту от различных видов вредоносного ПО, уязвимостей "нулевого дня" и других действий злоумышленников.

SoftControl SysWatch предоставляет следующие основные возможности:

- **Проактивная защита** на базе запатентованной технологии контроля приложений V.I.P.O. (Valid Inside-Permitted Operations):
  - динамический контроль целостности – обнаружение попыток несанкционированного запуска приложений и блокировка их запуска до того, как приложение может нанести вред системе;
  - динамическая "песочница" – запуск потенциально опасного ПО в ограниченной изолированной среде;
  - динамический контроль ресурсов – контроль доступа к файловой системе, ключам и значениям ключей реестра, внешним устройствам (USB-накопители, CD/DVD-диски, LPT- и COM-порты) и сетевым ресурсам (функции брандмауэра) на уровне приложений.
- **Автоматическая настройка** (сбор профиля системы): профилирование защищаемой системы с целью дальнейшего контроля целостности ее исходного состояния.
- **Выбор режимов обработки событий безопасности**:
  - классический (ручной) режим, позволяющий пользователю самому формировать политику активности, принимая решения по запуску и блокировке приложений вручную;

  - экспертный (автоматический) режим, в котором программа автоматически принимает решения относительно запуска и блокировки приложений на основе текущей политики активности и заданных настроек обработки.
- **Гибкая настройка правил активности**:
  - возможность задания частных правил для отдельных приложений;
  - возможность задания исключений по доступу к файловой системе, реестру и USB-накопителям ("белый список" USB-накопителей);
  - возможность задания временных интервалов действия правил доступа к файловой системе, реестру, сетевым ресурсам и USB-накопителям;
  - возможность задания учетных записей пользователей, на которые распространяется действие правил доступа к файловой системе, реестру, сетевым ресурсам и USB-накопителям.
- **Хранение истории активности приложений**:
  - возможность просмотра истории активности отдельных приложений;
  - возможность сохранения резервных копий файлов, измененных выбранным приложением, для их последующего восстановления в случае необходимости.
- **Антивирусная защита**: инструменты для антивирусной проверки системы и обезвреживания известного вредоносного ПО (вирусы, троянские программы, черви, программы-шпионы и т.д.) с использованием актуальных баз сигнатур.
- **Регистрация событий безопасности и статусов программы в отчеты**: сохранение детализированной информации о работе программы в файлы текстовых отчетов и WMI.
- **Самозащита программы**:
  - возможность установки парольной защиты интерфейса и удаления программы;
  - возможность выключения внешнего доступа к системной службе.
- **Сохранение и восстановление настроек программы**: возможность сохранения резервной копии настроек программы для их последующего восстановления в случае необходимости.
- **Возможность удаленного управления**: в случае применения программы в составе с программным продуктом SoftControl Service Center, возможно удаленное централизованное управление экземплярами программы, настройка и мониторинг состояния защиты на узлах ЛВС с помощью средств администрирования.

1.3 Условные обозначения и термины

1.3.1 Обозначения

Условные обозначения, применяемые в данном документе, приведены в табл. 1.

Таблица 1. Условные обозначения

Пример обозначения	Описание
	Важная информация.
Условие	Условие выполнения, примечание, пример.
Обновить	– заголовки и сокращения; – названия экранных кнопок, ссылок, пунктов меню, других элементов программного интерфейса.
Политика контроля	– термины (определения); – имена файлов и других объектов; – тексты сообщений, выводимых пользователю.
`C:\Program Files\SoftControl`	Пути к файлам, каталогам, ключам системного реестра.
`%windir%\system32\msiexec.exe /i`	Фрагменты программного кода, командных и конфигурационных файлов.
<каталог установки SoftControl SysWatch	Поля для замены функциональных названий фактическими значениями.
Приложение 8	Ссылки на внутренние ресурсы (разделы документа) с указанием номера страницы или на внешние ресурсы (URL-адреса).

1.3.2 Сокращения

В данном документе употребляются без расшифровки следующие сокращения:

- **ГИП** – графический интерфейс пользователя;
- **ЛВС** – локальная вычислительная сеть;
- **ОЗУ** – оперативное запоминающее устройство;
- **ОС** – операционная система;
- **ПО** – программное обеспечение;
- **УС** – устройство самообслуживания;
- **ЦП** – центральный процессор;
- **ЭЦП** – электронная цифровая подпись.

1.3.3 Глоссарий

Таблица 2. Глоссарий

Термин	Пояснение
Проактивная защита	Комплекс мер по предотвращению вредоносных воздействий, основанный на превентивных технологиях.

Превентивные технологии	Передовые технологии защиты данных, в основе которых лежит анализ активности на компьютере пользователя: действий любых приложений, служб операционной системы, действий пользователя, активности извне и т.д. В отличие от реактивных технологий, на которых построены такие средства защиты, как антивирусы и персональные сетевые экраны, превентивные технологии анализируют не код объекта, а отслеживают потенциально опасные действия, выполняемые им. Следовательно, инструменты проактивной защиты не требуют наличия и постоянного обновления баз вредоносного кода, что является необходимым для традиционных средств защиты.
Реактивные (сигнатурные) технологии	Метод работы антивирусного программного обеспечения и систем обнаружения вторжений, при котором программа в процессе анализа объекта обращается к базе данных известных вирусов и проверяет соответствие какого-либо участка кода просматриваемого объекта известному коду (сигнатуре) вируса в базе данных.
Политика контроля	Целостный набор **правил контроля активности**.
Правило контроля активности	Набор условий, определяющих действие приложения и реакцию на него SoftControl SysWatch.
Профиль системы	База данных, хранящаяся локально на **клиентском хосте** и содержащая контрольные суммы **исполняемых модулей**. Профиль системы создается в результате автоматической настройки SoftControl SysWatch (операция сбора профиля).
Приложение в профиле	Приложение, контрольная сумма которого есть в **профиле системы**.
Отслеживаемое приложение	Приложение, факт запуска которого SoftControl SysWatch обнаружил на **клиентском хосте** в процессе работы с момента установки.
Доверенное приложение	**Отслеживаемое приложение** из **доверенной зоны выполнения**.
Ограниченное приложение	**Отслеживаемое приложение** из **ограниченной зоны выполнения**.
Запрещенное приложение	**Отслеживаемое приложение** из **запрещенной зоны выполнения**. SoftControl SysWatch запрещает запуск таких приложений на клиентском хосте.
Зона выполнения (доверенная, ограниченная, запрещенная)	Отдельная **политика контроля**, применяемая к подмножеству **отслеживаемых приложений**. Всего на каждом **клиентском хосте** имеется 3 зоны выполнения: доверенная, ограниченная, запрещенная. Любое **отслеживаемое приложение** принадлежит к одной из этих трех зон выполнения.
Инсталлятор	Приложение, которое SoftControl SysWatch эвристически определил как программу, предназначенную для установки других программ, или которое пользователь пометил как инсталлятор. Инсталлятор имеет особые привилегии по запуску (см. ниже "Режим обновления ПО").
Режим обновления ПО	Режим запуска приложения, при котором происходит помещение в профиль системы самого приложения и всех созданных или измененных им PE-файлов. Дочерние процессы данного приложения наследуют режим обновления ПО.
V.I.P.O. (Valid Inside Permitted Operations)	Учетная запись пользователя с ограниченными правами (ограниченный набор системных привилегий, отсутствие доступа к системным объектам). Служит для организации "песочницы" при запуске приложений и обеспечивает дополнительную защиту от потенциальных вредоносных воздействий приложений, которым нельзя полностью доверять. Запуск с использованием учетной записи V.I.P.O. можно устанавливать только для **ограниченных**

	приложений.
PE-файл	Исполняемый файл в формате PE (Portable Executable). Данный формат используется в операционных системах семейства Microsoft® Windows® для исполняемых файлов (EXE), динамических библиотек (DLL) и некоторых других типов файлов.
Клиентский хост	Средство вычислительной техники (рабочая станция, сервер, терминал самообслуживания), на котором установлен SoftControl SysWatch.

2. Принцип работы SoftControl SysWatch

SoftControl SysWatch поддерживает два механизма защиты – профиль системы и политика контроля. Задача профиля – сохранение первоначальной целостности ОС и всех ее компонентов, включая ПО, установленное пользователем. Политика контроля представляет собой набор правил контроля активности и определяет действия приложений и реакцию SoftControl SysWatch на эти действия. Политика контроля позволяет разграничивать доступ к ресурсам системы.

Профиль системы (автоматическая настройка [46]) создается при первом запуске SoftControl SysWatch. По умолчанию предполагается, что компьютер, на который устанавливается SoftControl SysWatch, не содержит вредоносного ПО. Все приложения, которые уже были установлены на компьютере, заносятся в профиль системы.

Правила контроля активности определяют зоны выполнения приложений [62] (доверенная, ограниченная, запрещенная). После сбора профиля всем приложениям в нем назначается доверенная зона.

Детальная настройка SoftControl SysWatch [52], в том числе выбор режима обработки инцидентов безопасности (ручной [59] или автоматический [58]), и задание правил контроля активности [72] осуществляется пользователем после сбора профиля.

Профиль работает следующим образом (см. схему ниже [57]). При попытке запуска какого-либо приложения SoftControl SysWatch проверяет, находится ли оно в профиле системы. Если приложение в профиле, его запуск происходит согласно заданным правилам контроля активности [72]. Приложения из запрещенной зоны блокируются. Если приложения нет в профиле, оно считается потенциально опасным, и дальнейшие действия зависят от выбранных настроек.

Для инсталляторов выполнятся проверка на наличие действительной ЭЦП. Запуск инсталляторов с действительной ЭЦП разрешается. Для подписанных инсталляторов возможна дополнительная проверка сертификата ЭЦП на наличие в белом списке сертификатов [70], определяемом пользователем.

Действия при запуске неподписанного инсталлятора или инсталлятора с недействительной ЭЦП аналогичны действиям при запуске приложения, не внесенного в профиль системы. Запуск инсталляторов и выполнение скриптов ограничиваются в следующих случаях:

- отсутствие у инсталлятора/скрипта ЭЦП;
- наличие ЭЦП, срок действия сертификата которой истек, при отсутствии подписанной метки времени;
- наличие ЭЦП неизвестного производителя, либо производителя, чья ЭЦП была украдена злоумышленником;
- отсутствие сертификата ЭЦП в белом списке сертификатов.

В каждом из указанных случаев существует риск заражения вредоносным ПО и нарушения целостности программного окружения защищаемой системы.

Политика контроля работает следующим образом. Для незапрещенных приложений (доверенная и ограниченная зоны) действуют заданные по умолчанию и общие в пределах каждой зоны правила доступа к файловой системе, системному реестру и внешним устройствам, по сетевой активности, привилегиям процессов и межпроцессному взаимодействию. Кроме того, каждому приложению могут быть назначены частные правила [69]. Все правила контроля активности [72], действующие для данной зоны, распространяются и на инсталляторы.

Приложениям из ограниченной зоны можно назначить [68] специальную учетную запись «V.I.P.O.» с ограниченными правами. Данная учетная запись:

- имеет ограниченный набор системных привилегий;
- не имеет доступа к системным ресурсам в соответствии с политиками ОС (так как является гостевой учетной записью);
- не дает возможность загружать библиотеки без ЭЦП, которых нет в профиле.

Запуск приложений под учетной записью «V.I.P.O.» обеспечивает дополнительную защиту системы от потенциальных вредоносных воздействий.

3. Требования к аппаратному и программному обеспечению

3.1 Системные требования SoftControl SysWatch

Таблица 3. Минимальные системные требования

ОС	Частота ЦП	Объем ОЗУ	Объем свободного пространства на жестком диске
Клиентские операционные системы:			150 МБ + дополнительно от 120 МБ для хранения антивирусных баз
Microsoft® Windows® XP (SP2 и выше) *32-разрядная*	800 МГц	512 МБ	
Microsoft® Windows® XP (SP2) *64-разрядная*	800 МГц	512 МБ	
Microsoft® Windows® XP Embedded (SP2 и выше)	800 МГц	256 МБ	
Microsoft® Windows® Embedded for Point of Service 1.0	800 МГц	256 МБ	
Microsoft® Windows® 7 (SP1) *32-разрядная*	1 ГГц	1 ГБ	
Microsoft® Windows® 7 (SP1) *64-разрядная*	1 ГГц	2 ГБ	
Microsoft® Windows® 8 *32-разрядная*	1 ГГц	1 ГБ	
Microsoft® Windows® 8 *64-разрядная*	1 ГГц	2 ГБ	
Microsoft® Windows® 8.1 *32-разрядная*	1 ГГц	1 ГБ	
Microsoft® Windows® 8.1 *64-разрядная*	1 ГГц	2 ГБ	
Microsoft® Windows® 10 *32-разрядная*	1 ГГц	1 ГБ	
Microsoft® Windows® 10 *64-разрядная*	1 ГГц	2 ГБ	
Серверные операционные системы:			
Microsoft® Windows® Server 2003 (SP2) *32-разрядная*	800 МГц	512 МБ	
Microsoft® Windows® Server 2003 (SP2) *64-разрядная*	800 МГц	512 МБ	
Microsoft® Windows® Server 2008 R2 *64-разрядная*	1,4 ГГц	512 МБ	
Microsoft® Windows® Server 2012 *64-разрядная*	1,4 ГГц	512 МБ	
Microsoft® Windows® Server 2012 R2 *64-разрядная*	1,4 ГГц	512 МБ	
Microsoft® Windows® Server 2016 *64-разрядная*	1,4 ГГц	512 МБ	
Microsoft® Windows® Server 2016 *64-разрядная* (для варианта установки «Сервер с рабочим столом»)	1,4 ГГц	2 ГБ	

Примечание: поддерживаются все популярные платформы под управлением указанных ОС.

Дополнительные требования:

- Visual C++ 2008 SP1 Redistributable Package при установке SoftControl SysWatch на Windows XP.
- Для Windows 7 и Windows Server 2008 R2: обновление KB3033929 или любое его замещающее (поддержка алгоритма хэширования SHA-256 при проверке цифровой подписи).

4. Установка и настройка SoftControl SysWatch

SoftControl SysWatch может быть установлен на клиентские хосты как локально [14], так и одним из удаленных централизованных [18] способов. Выбор подходящего способа установки зависит от конкретных условий применения и определяется на основе таких критериев, как количество конечных точек, организация сети, политика безопасности и других особенностей среды развертывания.

В данном разделе также приведена информация по регистрации SoftControl SysWatch на сервере [33] SoftControl Service Center.

4.1 Локальная установка

Данный метод предполагает локальную установку экземпляра приложения на каждый клиентский хост.

Возможны следующие варианты локальной установки SoftControl SysWatch:

- в обычном режиме (с использованием интерфейса пользователя) [14];
- в тихом режиме [17];
- в тихом режиме с применением конфигурационного файла [18].

4.1.1 Установка в обычном режиме

1) Запустите установочный пакет *SysWatch.msi*.
2) В окне **Установка SoftControl SysWatch** нажмите на кнопку **Далее** (рис. Запуск программы установки [14]).

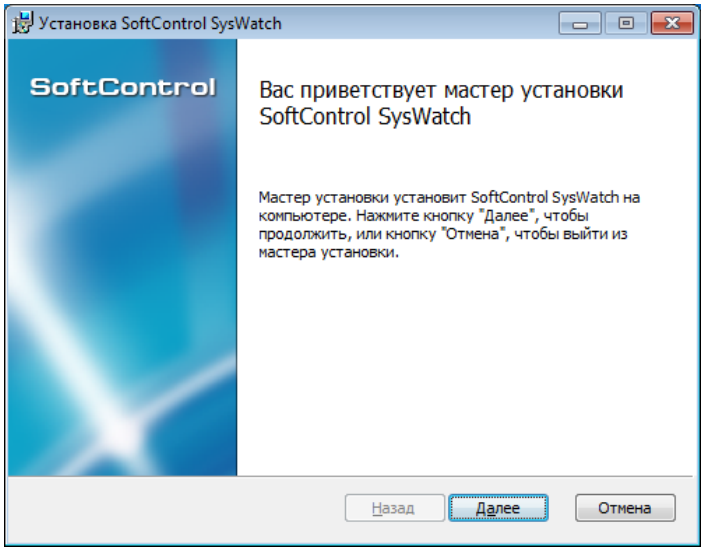

Рисунок 1. Запуск программы установки

3) В случае вашего согласия, выберите параметр **Я принимаю условия лицензионного соглашения** и нажмите на кнопку **Далее** (рис. Лицензионное соглашение 15).

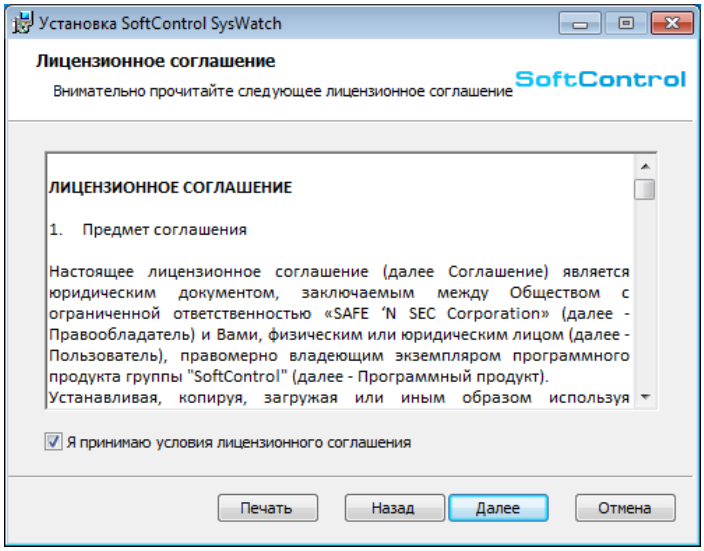

Рисунок 2. Лицензионное соглашение

4) Выберите каталог для установки SoftControl SysWatch (с помощью кнопки **Изменить**) и нажмите на кнопку **Далее** (рис. Путь установки 15).

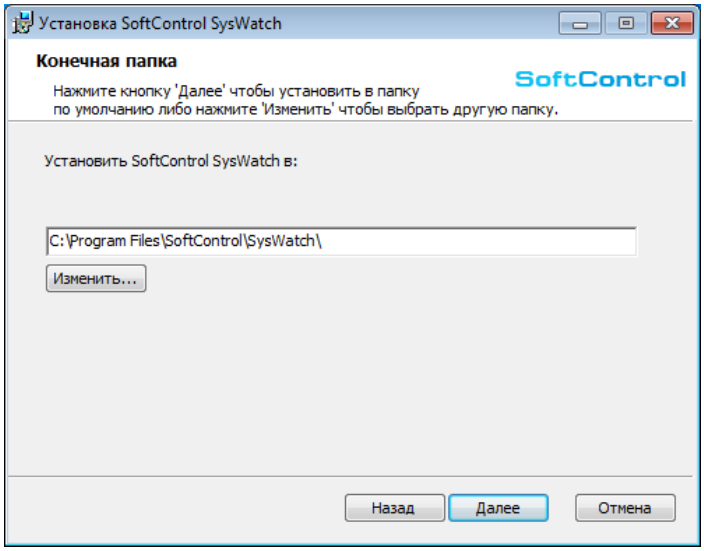

Рисунок 3. Путь установки

5) По умолчанию после установки SoftControl SysWatch начинает сбор профиля системы (рис. Включение сбора профиля 15). Так как этот процесс занимает некоторое время, вы можете снять флажок **Включить сбор профиля после установки** и запустить сбор профиля позже (см. раздел Запуск по требованию 49).

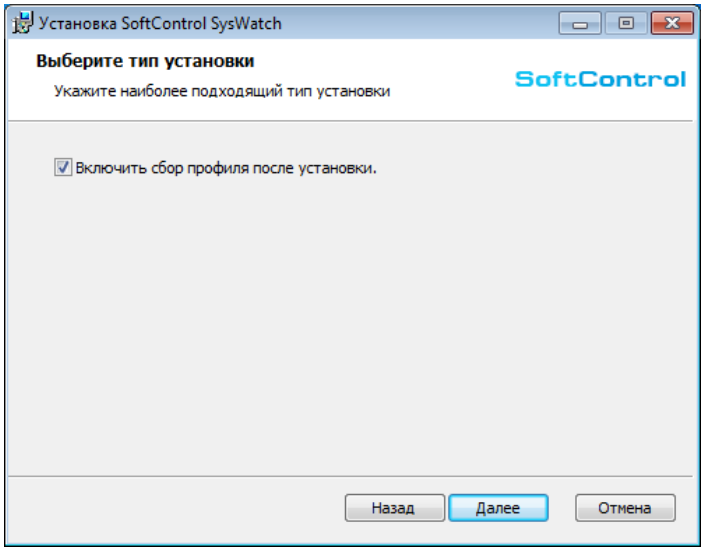

Рисунок 4. Включение сбора профиля

6) Нажмите на кнопку **Установить** (рис. Готовность к установке 16).

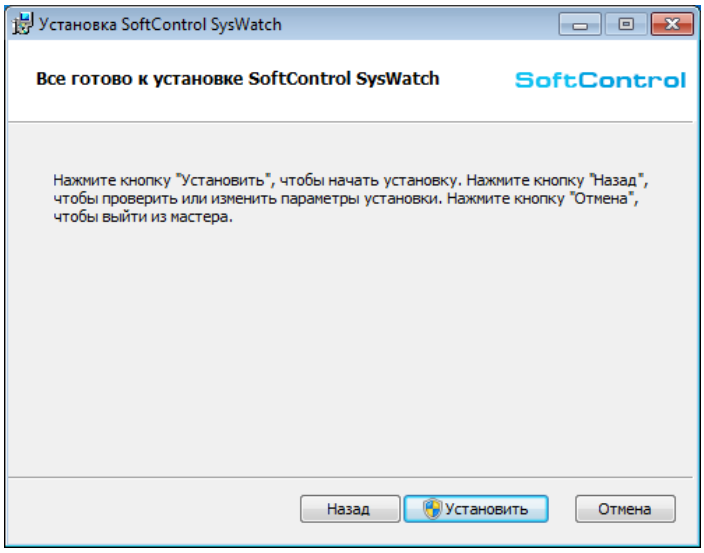

Рисунок 5. Готовность к установке

7) Дождитесь окончания процесса установки (рис. Процесс установки 16).

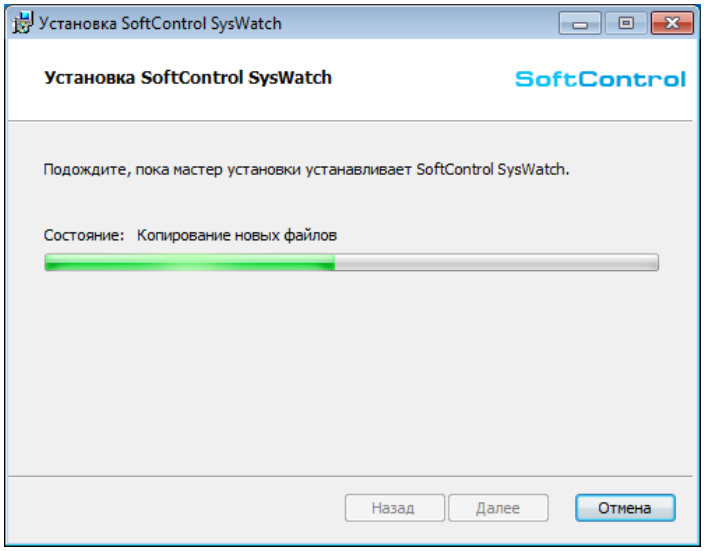

Рисунок 6. Процесс установки

8) После появления сообщения *Установка SoftControl SysWatch завершена* нажмите на кнопку **Готово** (рис. Завершение установки 17).

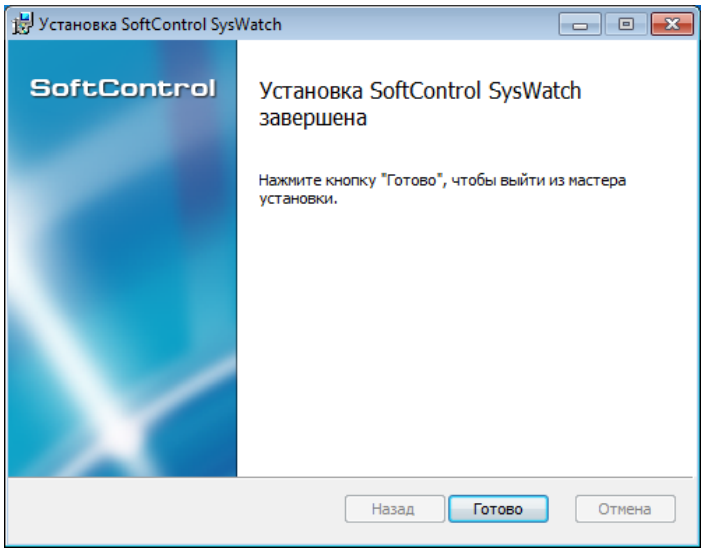

Рисунок 7. Завершение установки

4.1.2 Установка в тихом режиме

Условие: все шаги выполняются под учетной записью с правами администратора.

1) Скопируйте установочный пакет *SysWatch.msi* в каталог `C:\Temp` клиентского хоста.
2) Запустите командную строку Windows и выполните следующую команду:

```
%windir%\system32\msiexec.exe /i "C:\Temp\SysWatch.msi" /quiet
```

4.1.3 Установка в тихом режиме с применением конфигурационного файла

Условие: все шаги выполняются под учетной записью с правами администратора.

1) При тихой установке возможно применить пользовательскую конфигурацию (ранее выгруженные настройки программы[119], в примере ниже – *Storage.xmlc*) или файл настроек с параметрами подключения к управляющему серверу[43] (*ClientSettings.xmlc*) с сохранением остальной конфигурации по умолчанию. Скопируйте установочный пакет *SysWatch.msi* и необходимый конфигурационный файл в предварительно созданный каталог `C:\Temp` клиентского хоста.
2) Запустите командную строку Windows и выполните следующую команду.

   для конфигурационного файла с пользовательской конфигурацией:

   ```
   %windir%\system32\msiexec.exe /i "C:\Temp\SysWatch.msi" configfilename="C:\Temp\Storage.xmlc" /quiet
   ```

   для конфигурационного файла с параметрами подключения:

   ```
   %windir%\system32\msiexec.exe /i "C:\Temp\SysWatch.msi" tsconfig="C:\Temp\ClientSettings.xmlc" /quiet
   ```

   Примечание: в этом случае SoftControl SysWatch будет автоматически переведен в режим управления с Сервисного Центра[43] по окончании установки.

4.2 Удалённая установка

Удаленная установка SoftControl SysWatch подразумевает централизованно управляемую установку клиентских приложений на группу хостов, объединенных в одну сеть. Выбор определенного варианта установки зависит от способа организации сети, на конечных точках которой предполагается развертывание клиентских приложений (рабочая группа, домен), и используемых средств администрирования.

Возможны следующие варианты удаленной централизованной установки SoftControl SysWatch:

- через доменную групповую политику[18];
- с помощью утилиты удаленной инсталляции[28];
- сторонними средствами администрирования[33].

4.2.1 Установка через доменную групповую политику

Примечание: продемонстрировано на примере ОС Microsoft® Windows® Server 2008 R2.

1) Откройте оснастку **Server Manager** (Диспетчер сервера) из раздела **Administrative Tools** (Администрирование) меню **Start** (Пуск) в ОС контроллера домена.

2) Выберите раздел **Features** → **Group policy Management** → **Forest: <имя домена>** → **Domains** → **<имя домена>**, вызовите его контекстное меню и выберите пункт **New Organizational Unit** (рис. Создание нового подразделения домена 19).

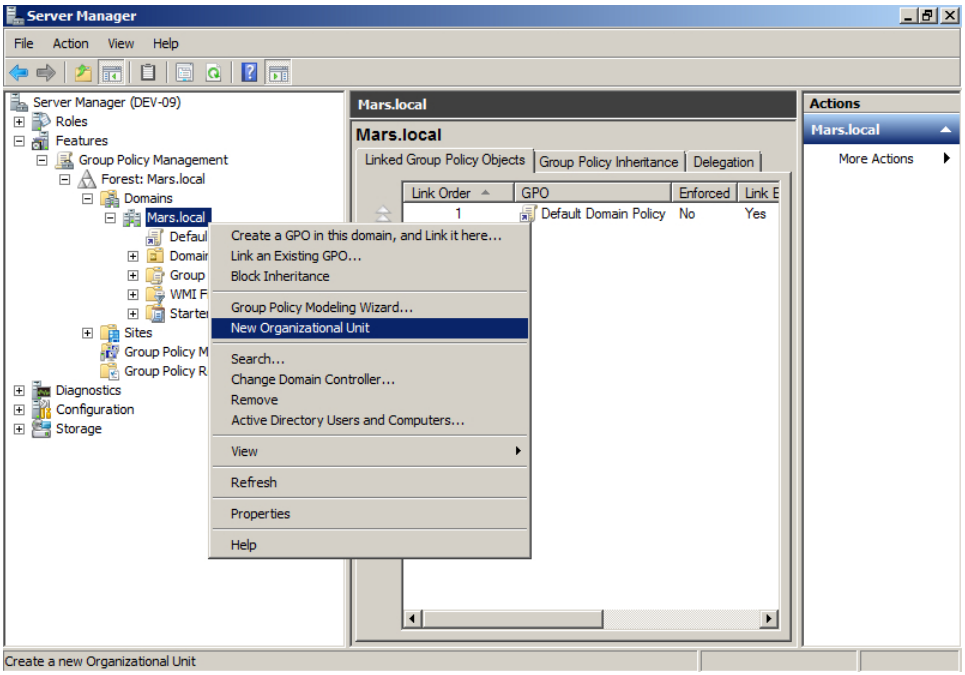

Рисунок 8. Создание нового подразделения домена

3) В диалоговом окне **New Organizational Unit** задайте имя (**Name**) нового подразделения и нажмите на кнопку **OK** (рис. Задание имени подразделения 19).

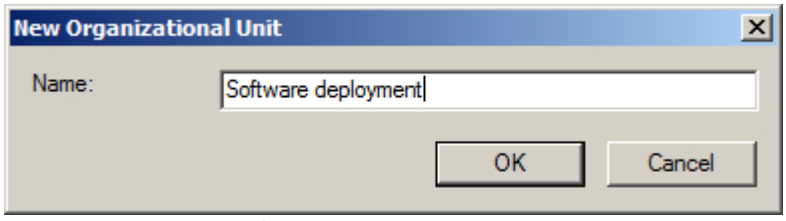

Рисунок 9. Задание имени подразделения

4) В разделе **Features** → **Group policy Management** → **Forest: <имя домена>** → **Domains** → **<имя домена>** вызовите контекстное меню созданного подразделения и выберите пункт **Create a GPO in this domain, and Link it here** (рис. Создание нового объекта групповой политики 19).

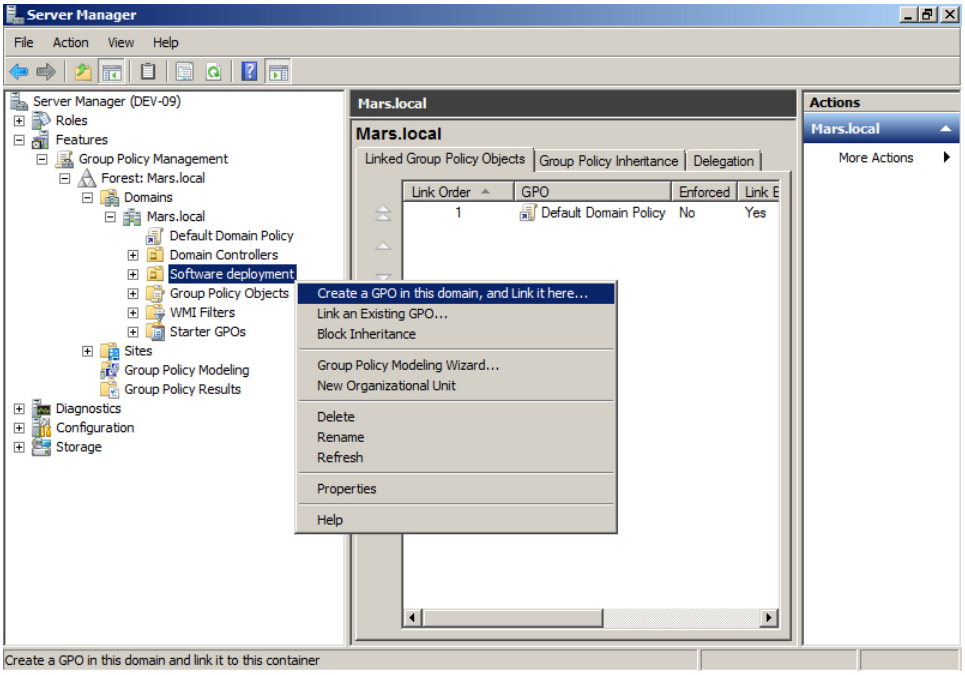

Рисунок 10. Создание нового объекта групповой политики

5) В диалоговом окне **New GPO** задайте имя (**Name**) нового объекта и начальный объект групповой политики (**Source Starter GPO**), если требуется наследовать свойства от "шаблонной" групповой политики в новом объекте, после чего нажмите на кнопку **OK** (рис. Задание имени и начального объекта групповой политики 20).

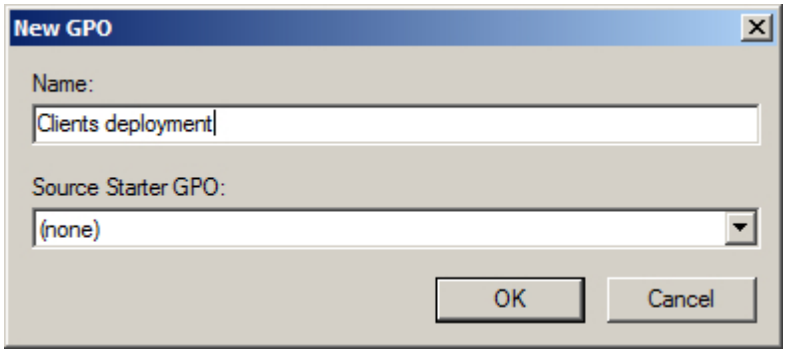

Рисунок 11. Задание имени и начального объекта групповой политики

6) Разверните созданное подразделение, вызовите контекстное меню созданного объекта групповой политики и выберите пункт **Edit** (рис. Редактирование объекта групповой политики 20).

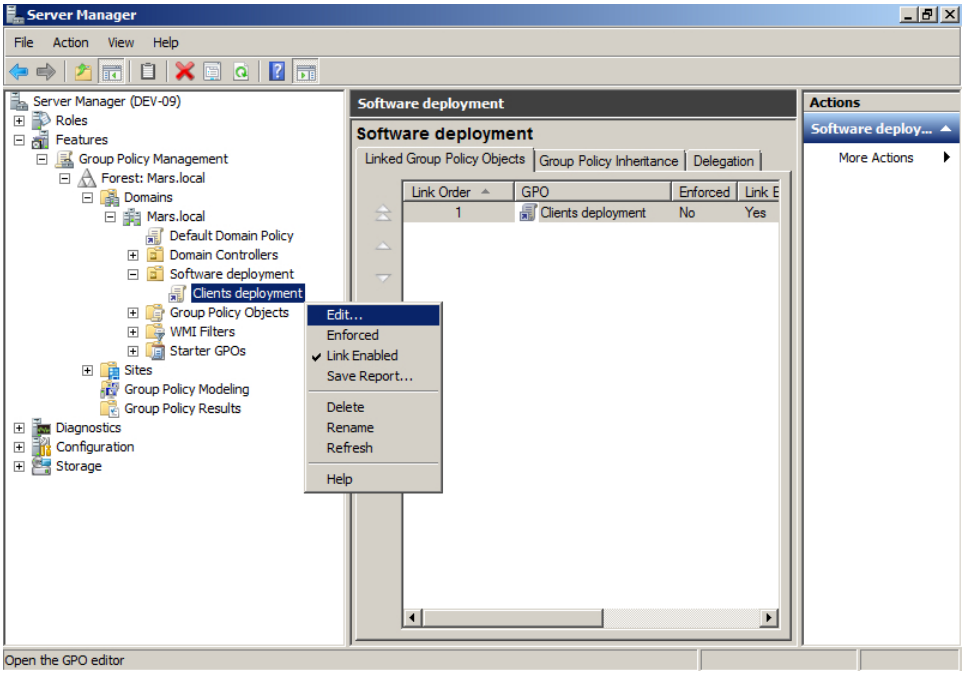

Рисунок 12. Редактирование объекта групповой политики

7) В открывшемся окне оснастки **Group Policy Management Editor** (Управление групповой политикой) выберите раздел **Computer configuration** → **Policies** → **Software Settings** → **Software installation**, вызовите его контекстное меню и выберите пункт **New** → **Package** (рис. Добавление нового пакета установки 21).

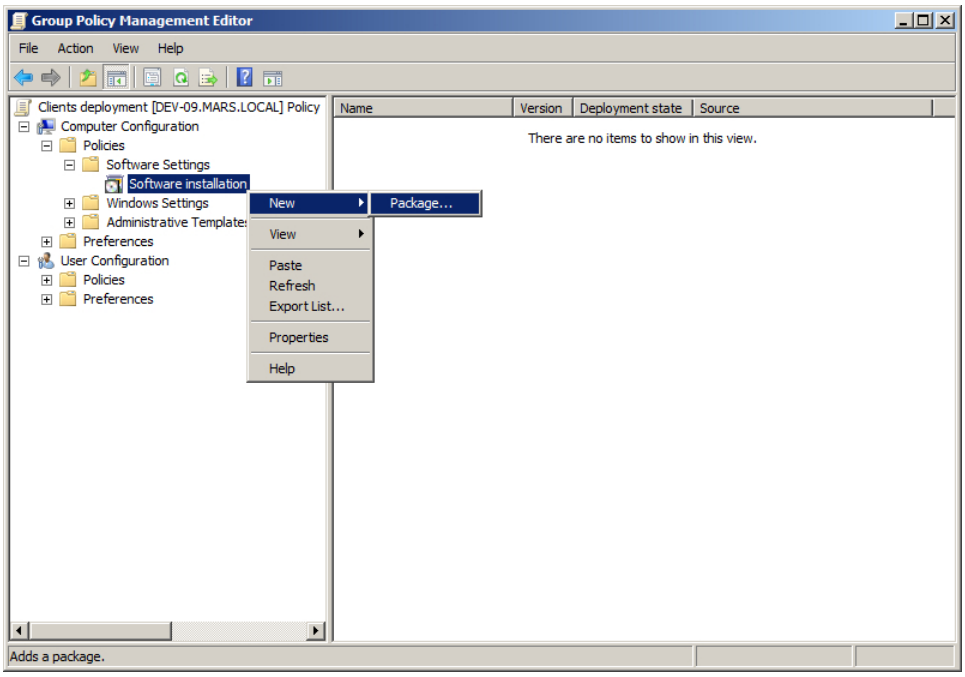

Рисунок 13. Добавление нового пакета установки

8) В открывшемся диалоговом окне выберите пакет установки *SysWatch.msi*,

расположенный на сетевом ресурсе, доступном для клиентских хостов, на которые предполагается произвести установку, и нажмите на кнопку **Open** (Открыть) (рис. Выбор пакета установки 22).

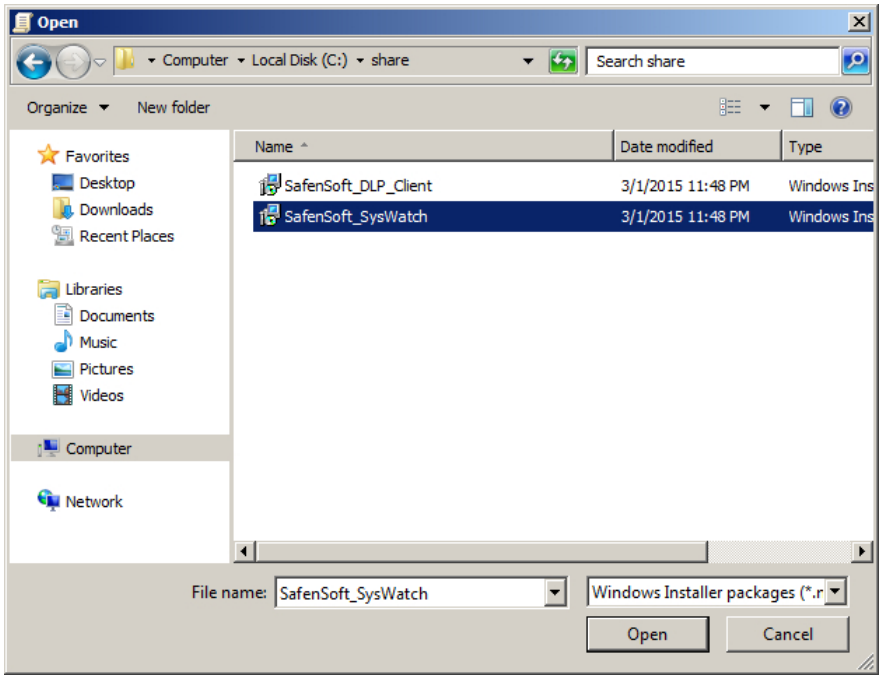

Рисунок 14. Выбор пакета установки

9) В случае появления предупреждения, дополнительно убедитесь, что выбранный пакет установки доступен удаленным клиентским хостам по сети, и нажмите на кнопку **Yes** (рис. Предупреждение при выборе местонахождения пакета установки 22).

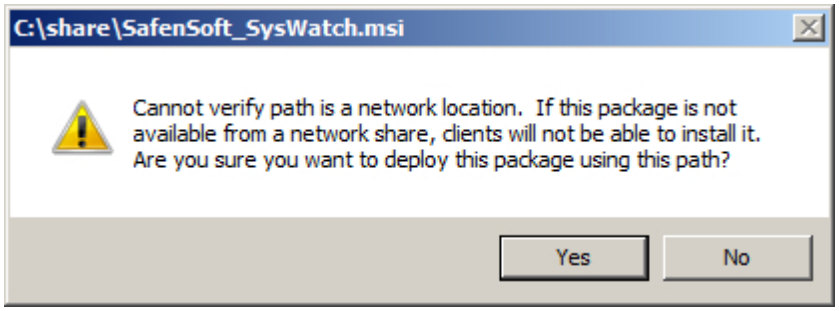

Рисунок 15. Предупреждение при выборе местонахождения пакета установки

10) В диалоговом окне **Deploy Software** выберите метод развертывания **Assigned** и нажмите на кнопку **OK** (рис. Выбор метода развертывания приложения 22).

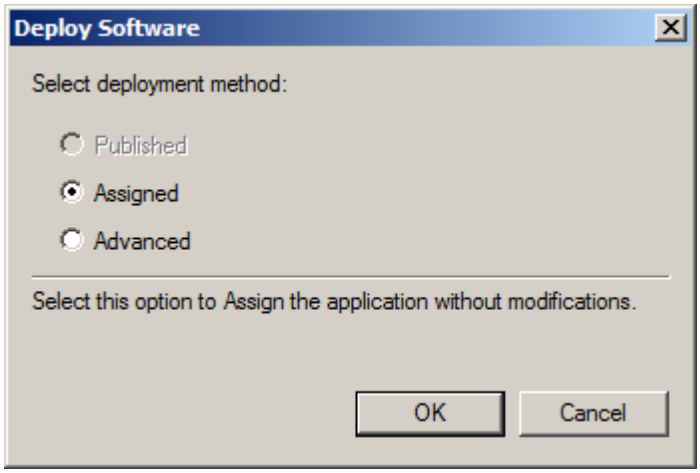

Рисунок 16. Выбор метода развёртывания приложения

11) В окне оснастки **Group Policy Management Editor** (Управление групповой политикой) выберите раздел **Computer configuration** → **Policies** → **Software Settings** → **Software installation**, вызовите его контекстное меню и выберите пункт **Properties** (рис. Изменение свойств развертывания приложений 23).

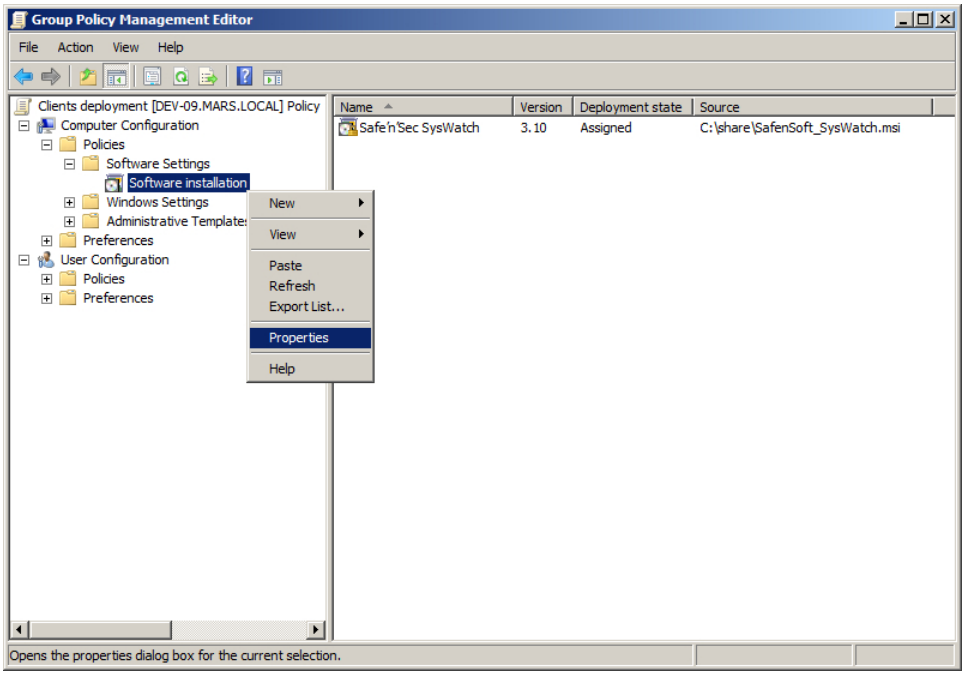

Рисунок 17. Изменение свойств развёртывания приложений

12) В появившемся окне настроек **Software installation Properties** перейдите на вкладку **Advanced**, установите флажок **Uninstall the applications when they fall out of the scope of the management**, если требуется удалять приложения, когда прекращается действие заданной групповой политики в отношении клиентских хостов, и флажок **Make 32-bit X86**

Windows Installer applications available to Win64 machines, если предполагается установка на клиентские хосты с ОС, имеющей 64-битную разрядность (рис. Свойства развертывания приложений 24). Для вступления изменений в силу нажмите на кнопку **OK**.

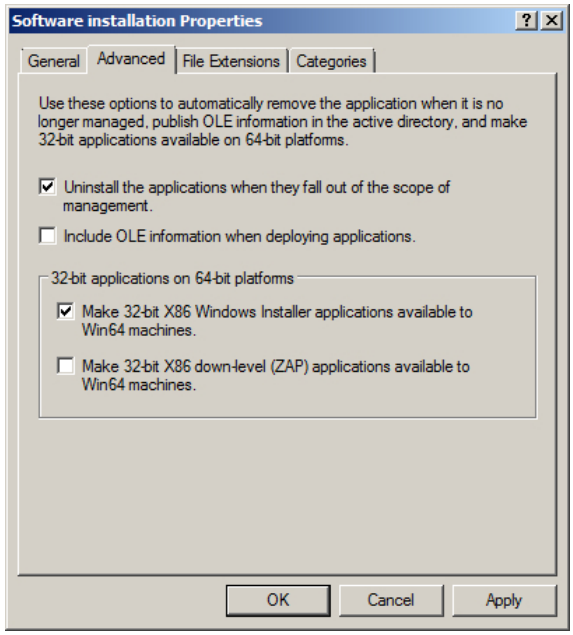

Рисунок 18. Свойства развёртывания приложений

13) В окне оснастки **Group Policy Management Editor** (Управление групповой политикой) выберите раздел **Computer configuration** → **Policies** → **Software Settings** → **Software installation**, в списке устанавливаемых приложений справа выберите требуемое приложение, вызовите контекстное меню и выберите пункт **Properties** (рис. Изменение свойств развертывания конкретного приложения 24).

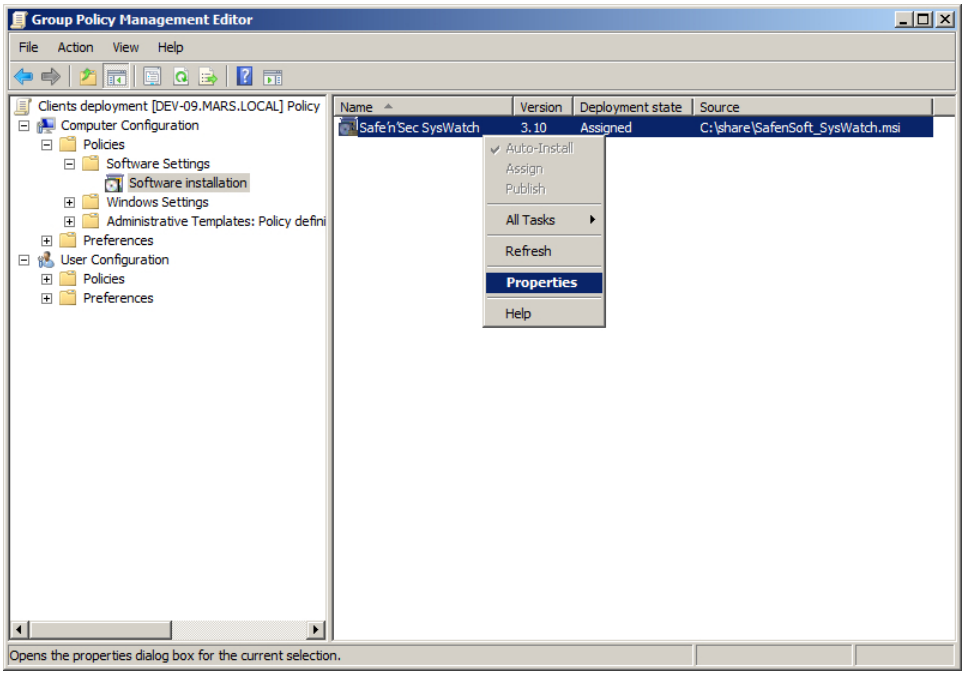

Рисунок 19. Изменение свойств развёртывания конкретного приложения

14) В появившемся окне настроек перейдите на вкладку **Deployment** и установите флажок **Uninstall this application when it falls out of the scope of management**, если требуется удалять данное приложение, когда прекращается действие заданной групповой политики в отношении клиентских хостов (рис. Свойства развертывания конкрентного приложения 25).

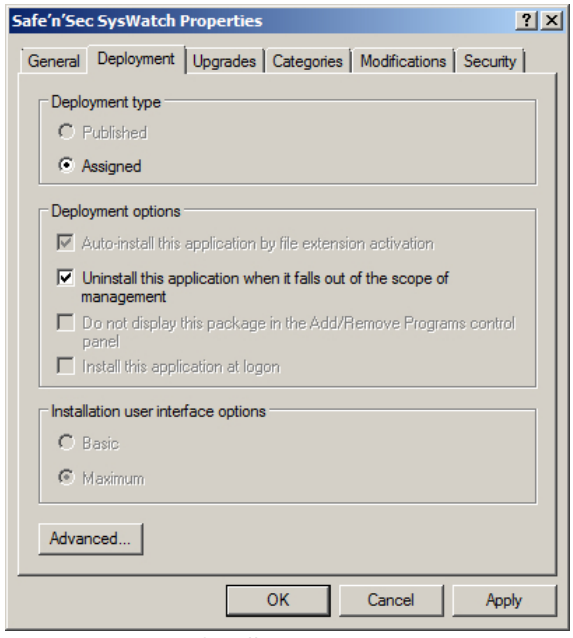

Рисунок 20. Свойства развертывания конкрентного приложения

Нажмите на кнопку **Advanced** и в окне **Advanced deployment options** установите

флажок **Make this 32-bit X86 application available to Win64 machines**, если предполагается установка на клиентские хосты с ОС, имеющей 64-битную разрядность (рис. Дополнительные свойства 26). Для вступления изменений в силу нажмите на кнопку **OK** в обоих окнах настройки.

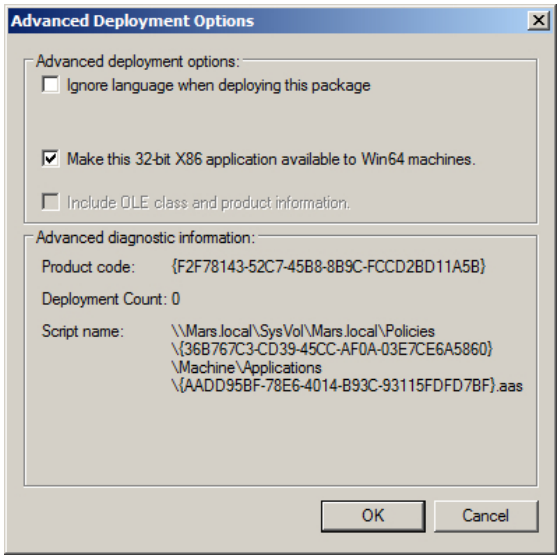

Рисунок 21. Дополнительные свойства

15) Закройте окна оснасток **Group Policy Management Editor** и **Server Manager** и откройте оснастку **Active Directory Users and Computers** (Active Directory – пользователи и компьютеры) из раздела **Administrative Tools** (Администрирование) меню **Start** (Пуск).

16) Разверните раздел **<имя домена>** и выберите раздел **Computers** (рис. Перечень хостов домена 26).

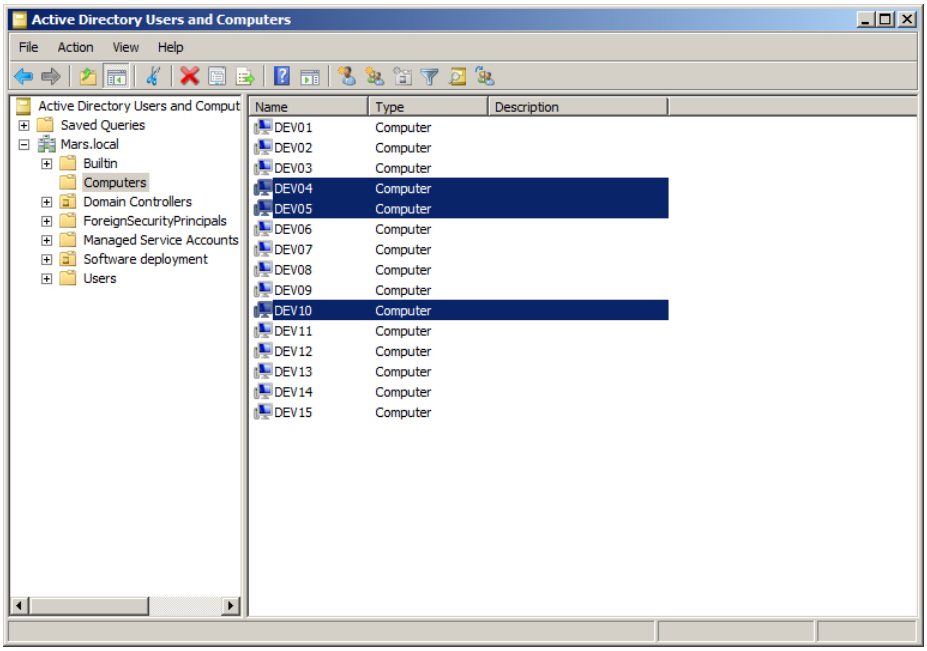

Рисунок 22. Перечень хостов домена

17) Выделите в списке хостов доменной сети те, на которые предполагается установка клиентских приложений, и переместите их в раздел **Software deployment**. В появившемся окне предупреждения выберите вариант **Yes** (рис. Предупреждение при переносе хостов в другое подразделение 27).

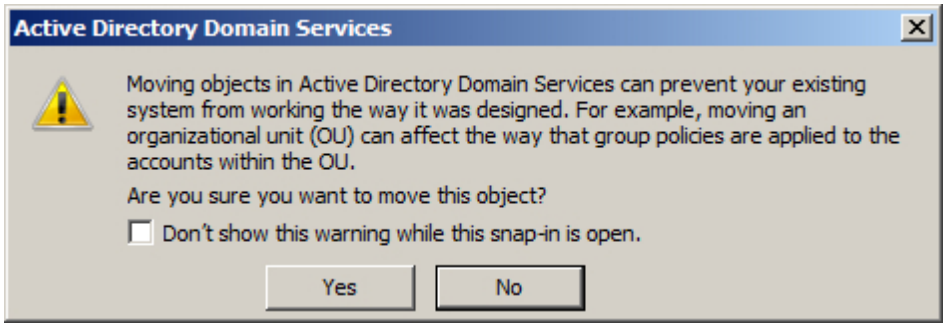

Рисунок 23. Предупреждение при переносе хостов в другое подразделение

18) Откройте раздел **Software deployment** и убедитесь, что необходимые клиентские хосты расположены в перечне компьютеров данного подразделения (рис. Перечень хостов подразделения 27).

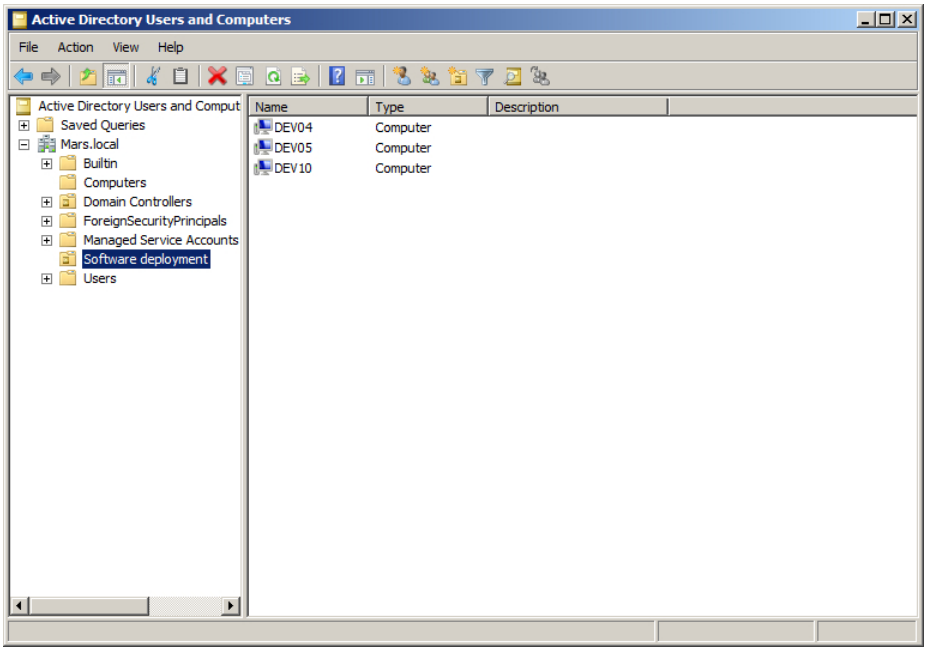

Рисунок 24. Перечень хостов подразделения

19) По истечении интервала обновления групповых политик (данный параметр зависит от настроек Active Directory) созданная политика применяется к клиентским хостам. Установка выбранных приложений будет произведена после очередного перезапуска клиентских хостов. Для мгновенного применения созданной групповой политики запустите

командную строку от имени администратора на клиентском хосте и выполните следующую команду:

```
gpupdate /force
```

По окончании выполнения команды подтвердите перезагрузку системы командой *Y* для применения обновленной групповой политики (рис. Ручное обновление групповой политики 28).

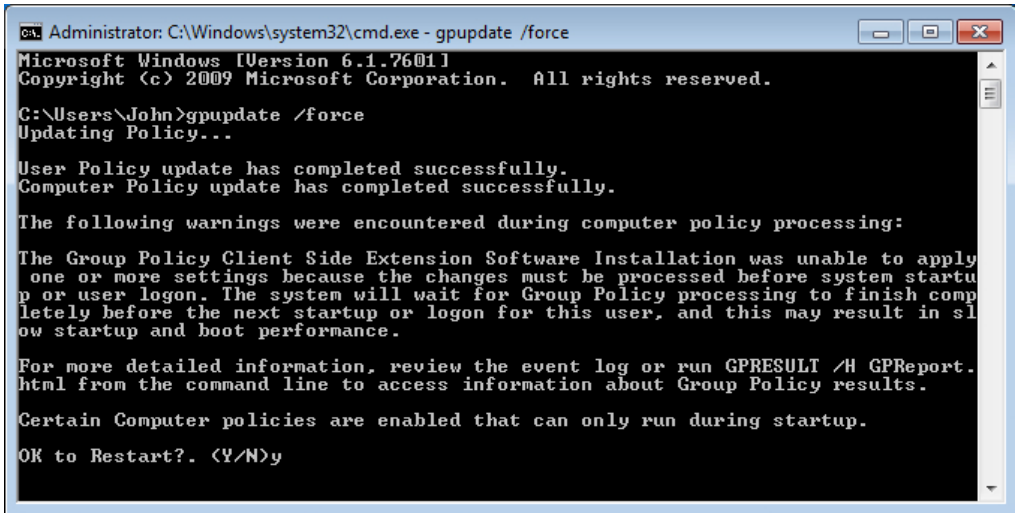

Рисунок 25. Ручное обновление групповой политики

4.2.2 Установка с помощью утилиты удалённой инсталляции

Данный способ установки рассчитан на случаи, в которых установка через групповые политики домена невозможна, например, когда сеть из защищаемых конечных точек организована в рабочую группу.

Утилита командной строки *srvrimp.exe* поставляется с SoftControl Service Center и предназначена для удаленной установки клиентских приложений Safe'N'Sec Corporation. Утилита расположена в каталоге установки компонента SoftControl Server.

Для успешной установки на удаленных хостах должны выполняться приведенные ниже условия.

Условия установки

- На сервере и удаленных конечных точках существует учетная запись пользователя с полными правами администратора, с одним и тем же логином и паролем.

- Запущены и работают службы ОС:
  1) *Удаленный реестр* (Remote Registry);
  2) *Удаленный вызов процедур* (RPC);
  3) *Локатор удаленного вызова процедур* (RPC Locator);
  4) *Инструментарий управления Windows* (Windows Management Instrumentation).
- Системная служба *Установщик Windows* (Windows Installer) не отключена и не заблокирована.
- Открыт доступ к общим ресурсам *\\host\C$*, *\\host\ADMIN$* на чтение, запись и удаление.

  Microsoft® Windows® XP, Microsoft® Windows® Server 2003:
  1) Откройте оснастку **Свойства папки** (Folder options) Панели управления Windows.
  2) Перейдите на вкладку **Вид** (View).
  3) Отключите опцию **Использовать простой общий доступ к файлам** (Use Simple File Sharing).

  Microsoft® Windows® 7, Microsoft® Windows® Server 2008, Microsoft® Windows® 8, Microsoft® Windows® Server 2012:
  1) Откройте оснастку **Параметры папок** (Folder options) Панели управления Windows.
  2) Перейдите на вкладку **Вид** (View).
  3) Отключите опцию **Использовать мастер общего доступа** (Use Sharing Wizard).
  4) Откройте оснастку **Параметры управления учетными записями пользователей** (User Account Control Settings) Панели управления Windows.
  5) Отключите контроль учетных записей, выставив ползунок с уровнем оповещения в положение **Никогда не уведомлять** (Never notify).
  6) Откройте следующий раздел системного реестра:

     `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System`
  7) В контекстном меню указанного раздела реестра выберите команду **Создать** (New) → **Параметр DWORD** (DWORD Value) и введите имя **LocalAccountTokenFilterPolicy** для созданного параметра.

8) В контекстном меню созданного параметра выберите команду **Изменить** (Modify) и в появившемся окне введите **1** в поле **Значение** (Value data), после чего нажмите на кнопку **OK**.
9) Перезагрузите систему для вступления изменений в силу.

- Включен общий доступ со следующими параметрами.

Microsoft® Windows® 7, Microsoft® Windows® Server 2008:

1) Откройте **Центр управления сетями и общим доступом** (Network and Sharing Center) Панели управления Windows.
2) Убедитесь, что хост имеет следующее сетевое размещение: для рабочей группы – **Домашняя сеть** (Home network) или **Рабочая сеть** (Work network), для домена – **Доменная сеть** (Domain network). Для изменения типа сети нажмите на ссылку с названием текущего сетевого размещения.
3) Нажмите на ссылку **Изменить дополнительные параметры общего доступа** (Change advanced sharing settings) и разверните профиль для текущего сетевого размещения.
4) В разделе **Общий доступ к файлам и принтерам** (File and printer sharing) выберите опцию **Включить общий доступ к файлам и принтерам** (Turn on file and printer sharing).
5) В разделе **Подключения домашней группы** (HomeGroup Connections) выберите опцию **Использовать учетные записи пользователей и пароли для подключения к другим компьютерам** (Use user accounts and passwords to connect to other computers).
6) Нажмите на кнопку **Сохранить изменения** (Save changes).

Microsoft® Windows® 8, Microsoft® Windows® Server 2012:

1) Выполните двойное нажатие левой кнопкой мыши на значке сети в области уведомлений.
2) Нажмите правой кнопкой мыши на имени сети в появившемся списке справа и выберите пункт **Включение и отключение общего доступа** (Turn sharing on or off).
3) Выберите вариант **Да, включить общий доступ и подключение к устройствам** (Yes, turn on sharing and connect to devices).
4) Откройте **Центр управления сетями и общим доступом** (Network and

Sharing Center) Панели управления Windows.

5) Нажмите на ссылку **Изменить дополнительные параметры общего доступа** (Change advanced sharing settings) и разверните сетевой профиль **Частная** (Private).
6) В разделе **Общий доступ к файлам и принтерам** (File and printer sharing) выберите опцию **Включить общий доступ к файлам и принтерам** (Turn on file and printer sharing).
7) В разделе **Подключения домашней группы** (HomeGroup Connections) выберите опцию **Использовать учетные записи пользователей и пароли для подключения к другим компьютерам** (Use user accounts and passwords to connect to other computers).
8) Нажмите на кнопку **Сохранить изменения** (Save changes).

- При включенном брандмауэре Windows разрешено входящее сетевое подключение к службе **Общий доступ к файлам и принтерам** (File and Printer Sharing).

  Microsoft® Windows® XP, Microsoft® Windows® Server 2003:

  1) Откройте брандмауэр Windows.
  2) Выберите вкладку **Исключения** (Exceptions).
  3) Добавьте в исключения (установите флажок у правила) **Общий доступ к файлам и принтерам** (File and Printer Sharing).

  Microsoft® Windows® 7, Microsoft® Windows® Server 2008, Microsoft® Windows® 8, Microsoft® Windows® Server 2012:

  1) Откройте брандмауэр Windows.
  2) Откройте **Дополнительные параметры** (Advanced settings).
  3) Выберите **Правила для входящих подключений** (Inbound Rules).
  4) Включите правило **Общий доступ к файлам и принтерам (входящий трафик SMB)** (File and Printer Sharing (SMB-In)) для профиля той сети, в которой находится хост.

- В оснастке **Администрирование** (Administrative Tools) → **Локальная политика безопасности** (Local Security Policy) Панели управления Windows выставлены следующие параметры: **Локальные политики** (Local Policies) → **Параметры безопасности** (Security Options) → **Сетевой доступ: модель совместного доступа и безопасности для локальных учетных записей** (Network access:

Sharing and security model for local accounts) → **Обычная - локальные пользователи удостоверяются как они сами** (Classic - local users authenticate as themselves).

Параметры запуска утилиты

Параметры, принимаемые утилитой удаленной инсталляции, описаны в табл. 4.

Таблица 4. Опции srvrimp

Параметр	Описание
-h	Краткая справка по принимаемым параметрам.
-i	Перевод в режим установки. Требует задания обязательных ключей и их значений, описанных ниже.
--login=<имя>	Имя пользователя, имеющего права администратора на удаленном хосте.
--password=<пароль>	Пароль пользователя, имеющего права администратора на удаленном хосте.
--client="<путь к установщику>"	Путь к пакету установки SoftControl SysWatch. Если файл расположен в каталоге, откуда вызывается утилита, допускается указывать только имя файла (без кавычек).
--config="<путь к файлу конфигурации>"	Путь к конфигурационному файлу настроек соединения с управляющим сервером. Требуется для автоматической подачи запроса на регистрацию 33 на сервере SoftControl Server после окончания установки. Если файл расположен в каталоге, откуда вызывается утилита, допускается указывать только имя файла (без кавычек).
--hostnames=<имя 1> <имя 2>...<имя N>	Список имен удаленных хостов, на которые требуется произвести установку, разделенных пробелами.

Допускается также запуск утилиты без указания имен ключей, расположив значения в следующем порядке:

```
srvrimp -i <имя> <пароль> "<путь к установщику>" "<путь к файлу конфигурации>" <имя 1> <имя 2>...<имя N>
```

Если требуется установить клиентский компонент в том числе и на сервер, то утилита должна быть вызвана из командной строки Windows, запущенной с правами администратора.

В случае успешной установки, утилита отображает сообщение *Installation successfully completed on host <имя хоста>*.

4.2.3 Установка сторонними средствами администрирования

Для удаленной установки SoftControl SysWatch могут применяться сторонние системы управления IT-инфраструктурой, например, Microsoft® System Center Configuration Manager (далее – MS SCCM). Методика установки в данном случае определяется, исходя из конкретной системы и принятыми в ней способами распространения пакетов инсталляции.

4.3 Регистрация на сервере

SoftControl SysWatch является клиентским компонентом и способен работать как автономно, так и в режиме удаленного управления с SoftControl Service Center («Сервисного Центра»). Чтобы подключить SoftControl SysWatch к Сервисному Центру, необходимо зарегистрировать его на сервере SoftControl Server. Для этого выполните следующие действия:

1) Переведите SoftControl SysWatch в режим удаленного управления [43] в настройках программы.
2) Примените зашифрованный конфигурационный файл [43] с настройками подключения к серверу.
3) Подтвердите регистрацию в консоли управления SoftControl Admin Console на вкладке **Клиенты** (см. документ «Руководство администратора SoftControl Service Center»).

5. Локальная работа с SoftControl SysWatch

В данном разделе приведены инструкции по локальной работе с основными функциями SoftControl SysWatch.

5.1 Интерфейс SoftControl SysWatch

Графический интерфейс пользователя (ГИП) SoftControl SysWatch составляют следующие основные элементы:

- Значок в области уведомлений [35] (поз. 1 на рис. ниже [34]);
- Контекстное меню [35] (поз. 2 на рис. ниже [34]);
- Панель управления [36] (поз. 3 на рис. ниже [34]).

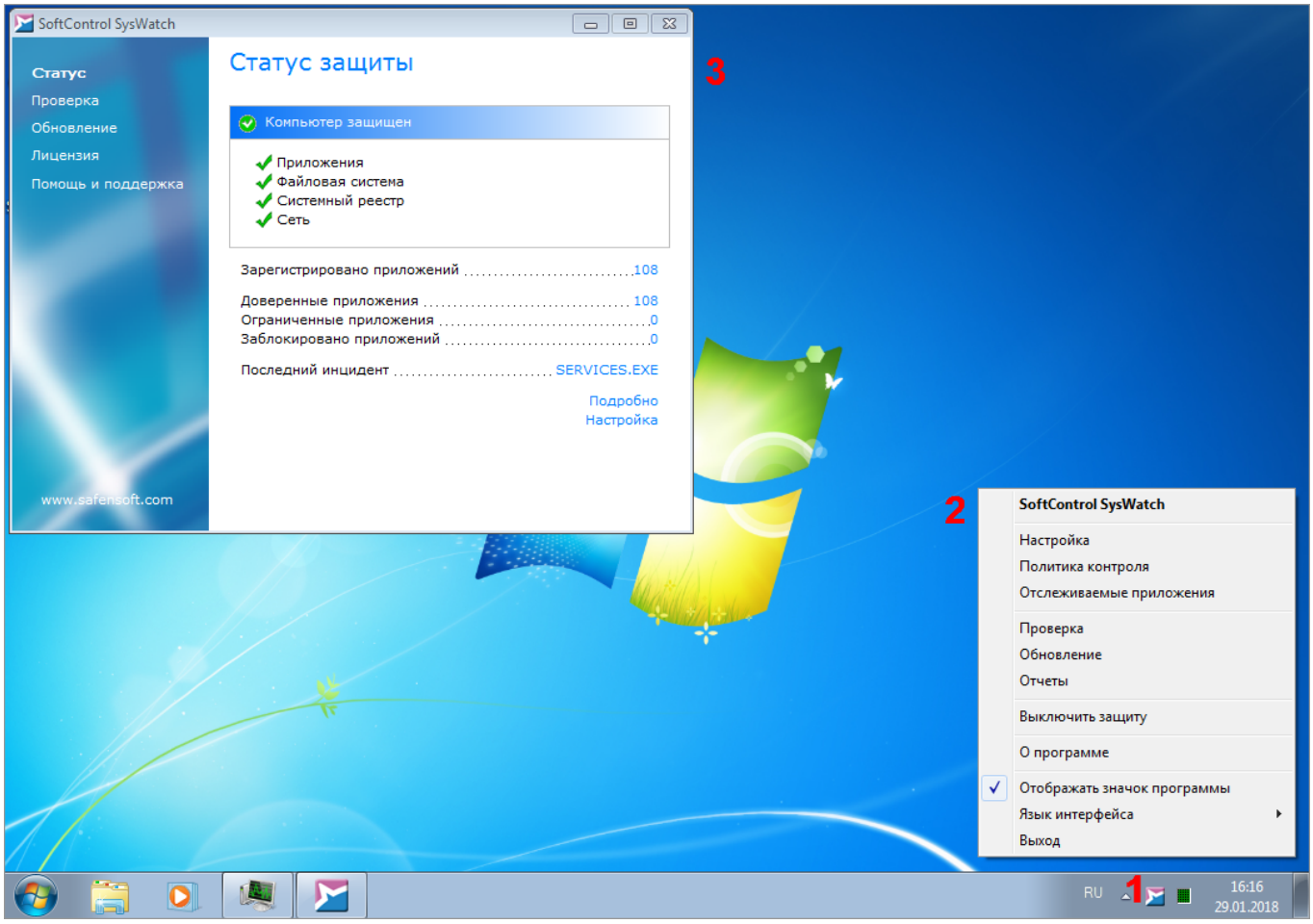

Рисунок 26. Элементы интерфейса программы

5.1.1 Значок в области уведомлений

После установки SoftControl SysWatch его значок появляется в области уведомлений панели задач Microsoft® Windows®.

Значок является индикатором работы приложения. Он отражает состояние защиты, а также показывает ряд основных действий, выполняемых приложением (табл. 5).

Таблица 5. Состояния программы

Значок	Состояние программы
	Защита включена (активна защита как минимум одной области контроля).
	Защита выключена.
	Выполняется автоматическая настройка/антивирусное сканирование.
	Выполняется обновление программных модулей и/или антивирусных баз.

Также значок обеспечивает доступ к остальным элементам ГИП приложения – контекстному меню [35] и панели управления [36]:

- чтобы открыть контекстное меню, нажмите правой кнопкой мыши по значку приложения;
- чтобы открыть панель управления, дважды нажмите левой кнопкой мыши по значку приложения.

5.1.2 Контекстное меню

Контекстное меню SoftControl SysWatch содержит пункты, обеспечивающие быстрый доступ к основным настройкам и командам программы. Внешний вид меню показан на рис. Контекстное меню SoftControl SysWatch [35], описание пунктов – в табл. 6.

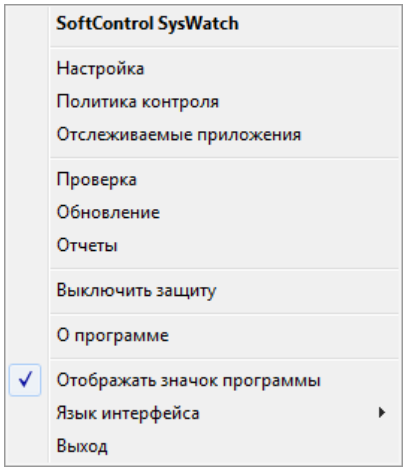

Рисунок 27. Контекстное меню SoftControl SysWatch

Таблица 6. Описание пунктов контекстного меню SoftControl SysWatch

Пункт меню	Действие
SoftControl SysWatch	Перейти на вкладку **Статус** панели управления программы.
Настройка	Перейти в раздел просмотра и настройки параметров программы.
Политика контроля	Перейти на вкладку **Области контроля** окна **Политика контроля** для просмотра и изменения прав доступа приложений к ресурсам и устройствам компьютера, а также правил сетевой активности.
Отслеживаемые приложения	Перейти на вкладку **Отслеживаемые приложения** окна **Политика контроля** для просмотра и изменения свойств контроля активности приложений.
Проверка	Перейти на вкладку **Проверка** панели управления программы.
Обновление	Перейти на вкладку **Обновление** панели управления программы.
Отчеты	Открыть каталог хранения отчетов программы.
Включить/выключить защиту	Изменить статус активности защиты.
О программе	Открыть окно с информацией о SoftControl SysWatch.
Отображать значок программы	Включить/выключить отображение значка программы в области уведомлений.
Язык интерфейса	Изменить язык интерфейса программы.
Выход	Выгрузить ГИП программы (при выборе данного пункта меню модуль интерфейса SoftControl SysWatch будет выгружен из ОЗУ, без завершения работы модуля защиты).

5.1.3 Панель управления

Панель управления является главным окном SoftControl SysWatch и состоит из вкладок **Статус**, **Проверка**, **Обновление**, **Лицензия**, **Помощь и поддержка**.

На вкладке **Статус** отображается текущий статус защиты (рис. Вкладка "Статус" 36). Детальное описание работы с вкладкой приведено в разделе Детальная настройка SoftControl SysWatch 52.

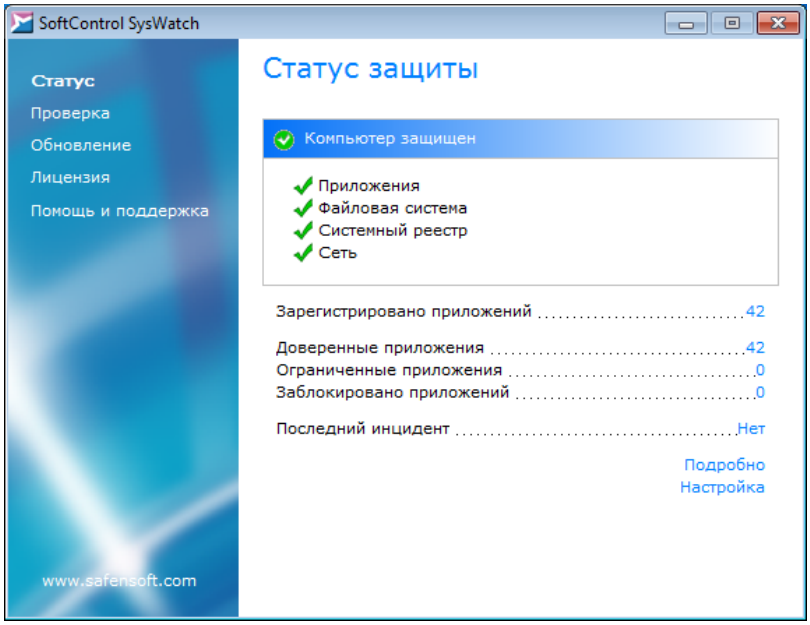

Рисунок 28. Вкладка "Статус"

На вкладке **Проверка** расположено дерево объектов для антивирусной проверки по требованию (рис. Вкладка "Проверка" 37). Подробная информация приведена в разделе Антивирусное сканирование 98.

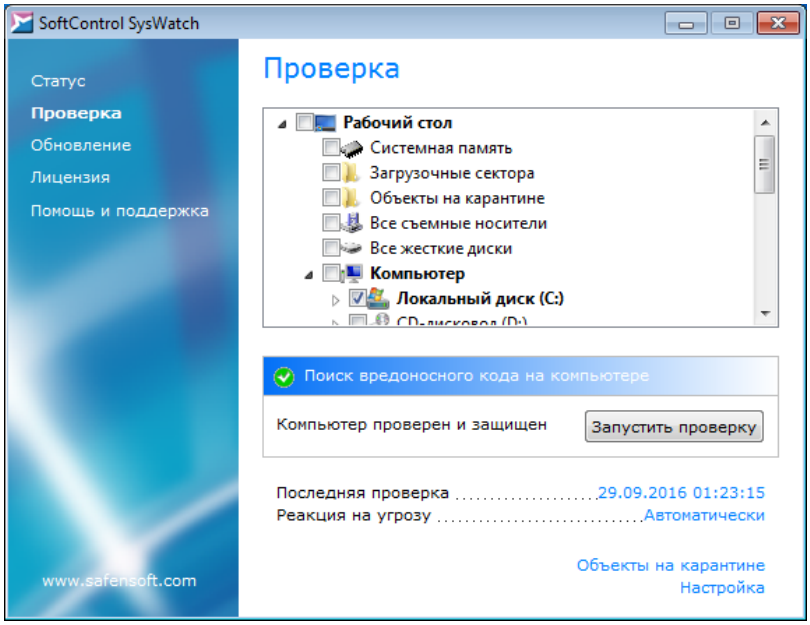

Рисунок 29. Вкладка "Проверка"

На вкладке **Обновление** находится информация по наличию обновлений программных модулей и антивирусных баз 122 (рис. Вкладка "Обновление" 37).

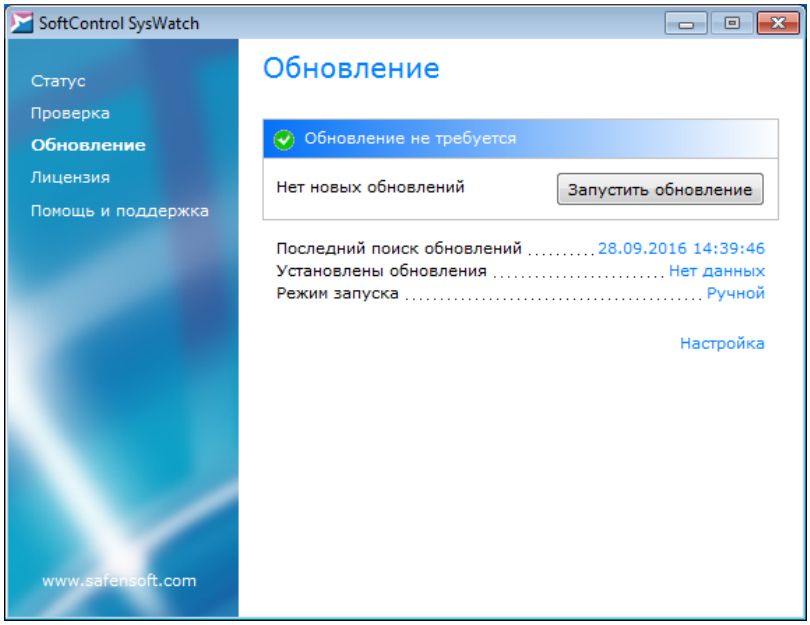

Рисунок 30. Вкладка "Обновление"

Вкладка **Лицензия** содержит данные по используемому лицензионному ключу[45] и компонентам программы (рис. Вкладка "Лицензия"[38]).

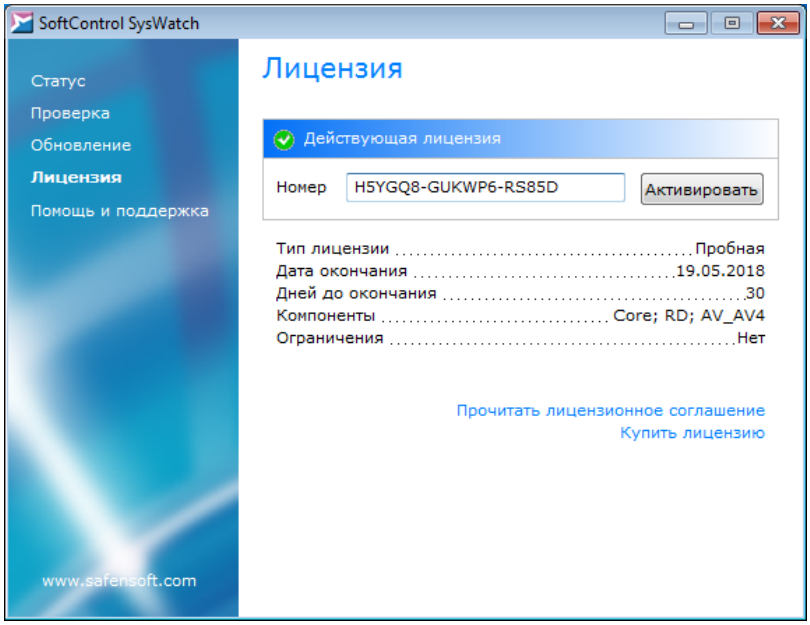

Рисунок 31. Вкладка "Лицензия"

На вкладке **Помощь и поддержка** указан номер версии установленного SoftControl SysWatch и информация об ОС. На данной вкладке по ссылке **Открыть Справку** доступна электронная справка программы, а также приведены ссылки на сайт компании для связи с технической поддержкой[141]. Внешний вид вкладки представлен на рис. Вкладка "Помощь и поддержка"[38].

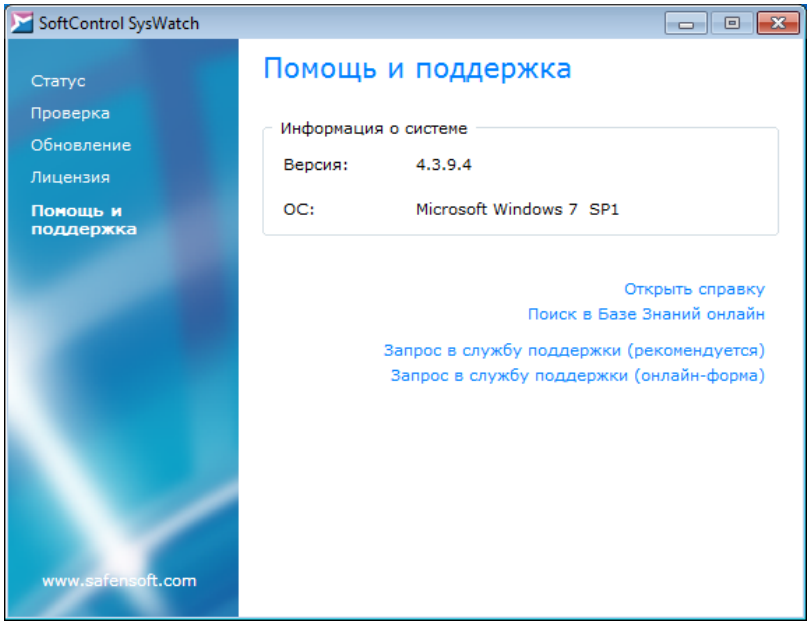

Рисунок 32. Вкладка "Помощь и поддержка"

5.1.4 Настройка интерфейса и оповещений

Настройка интерфейса

Для настройки параметров ГИП SoftControl SysWatch в настройках программы выберите раздел **Параметры** → **Вид** (рис. Настройка интерфейса 39).

Выберите необходимый язык интерфейса в выпадающем списке **Выбор языка**:

- **English** (английский);
- **Русский**.

Установите флажок **Показывать значок программы в области уведомлений** для отображения значка 35.

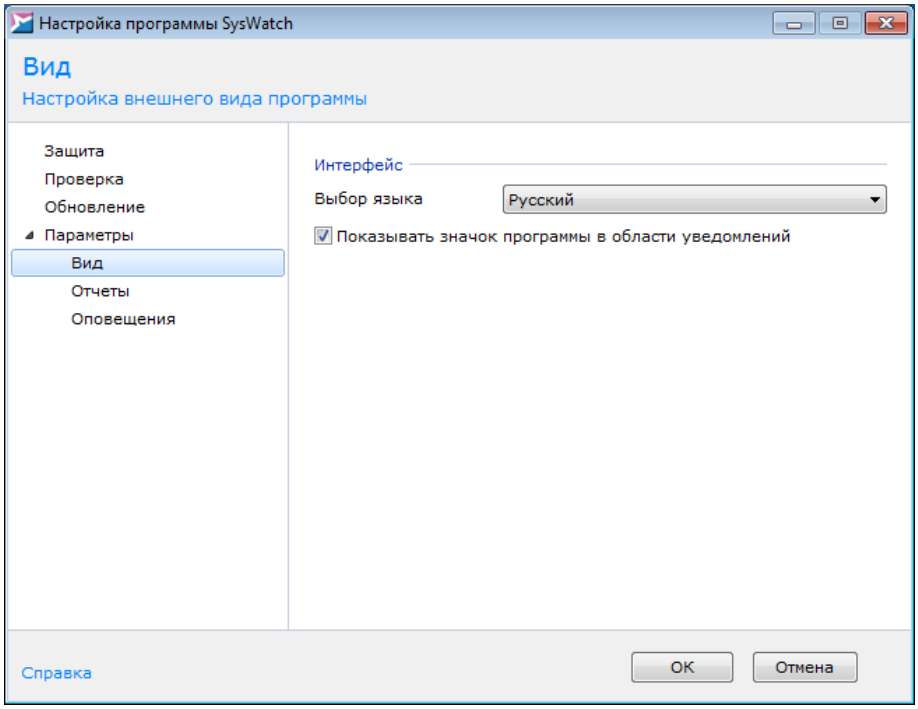

Рисунок 33. Настройка интерфейса

Настройка локальных оповещений

Для настройки параметров оповещения пользователя SoftControl SysWatch о событиях безопасности и состоянии программы в настройках программы выберите раздел **Параметры** → **Оповещения** (рис. Настройка оповещений 40).

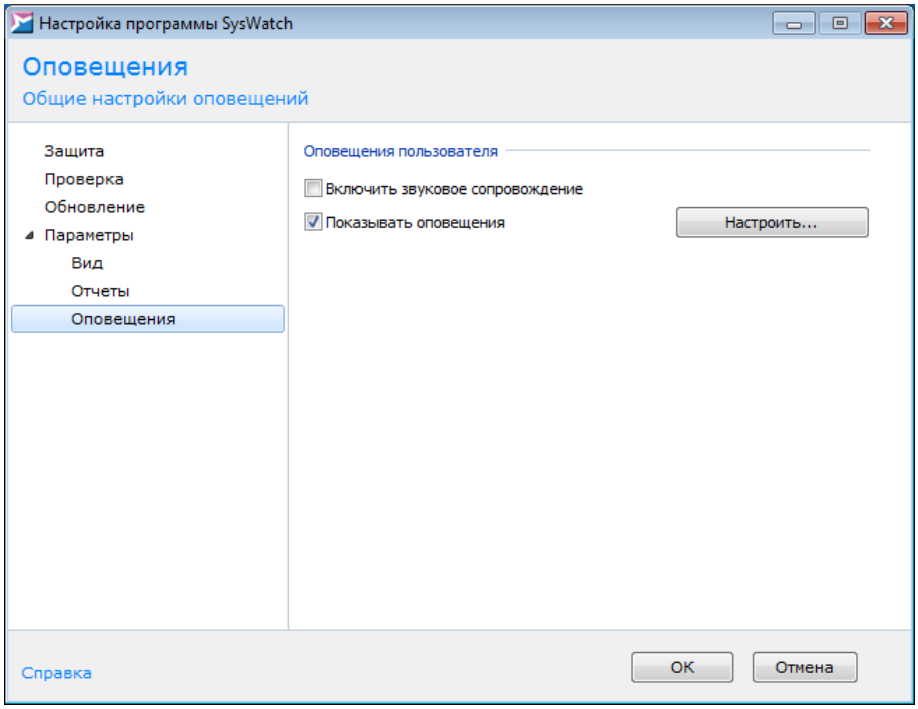

Рисунок 34. Настройка оповещений

Для включения звуковых оповещений программы установите флажок **Включить звуковое сопровождение**.

Для включения текстовых и графических оповещений установите флажок **Показывать оповещения** и нажмите на кнопку **Настроить**. В окне **Настройка режима оповещений** установите флажки у требуемых событий (рис. Настройка типов событий для оповещения 41):

- **Статус защиты**;
- **Обновление программы**;
- **Проверка компьютера**;
- **Отчеты**;
- **Лицензия**;
- **Установка (удаление) программ**;
- **Блокирование модулей программы**;
- **Ограничение приложений**.

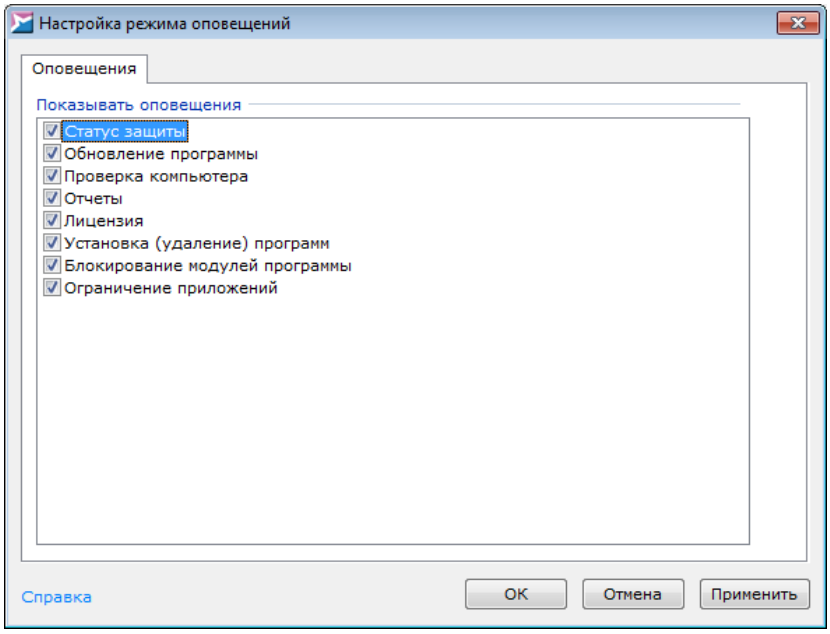

Рисунок 35. Настройка типов событий для оповещения

Для вступления изменений в силу нажмите на кнопку **OK**.

5.2 Режимы управления

Возможны следующие варианты управления работой SoftControl SysWatch:

- Автономный режим [42];
- Удаленное управление с сервера [43].

Чтобы установить необходимый режим, откройте настройки программы, перейдите в раздел **Параметры** и выберите требуемый вариант в области **Удаленное управление** (рис. Настройки параметров программы [42]). Для вступления изменений в силу нажмите на кнопку **OK**.

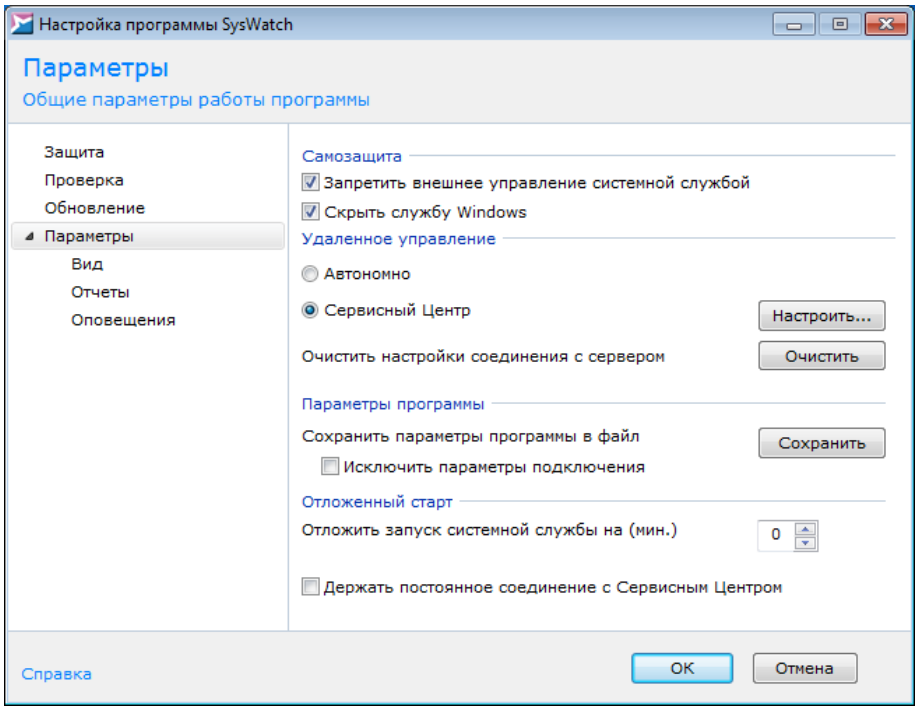

Рисунок 36. Настройки параметров программы

5.2.1 Автономный режим

При автономном режиме управления SoftControl SysWatch настройка программы, запуск задач и обработка событий безопасности производится локально с помощью ГИП SoftControl SysWatch.

Для установки режима выберите вариант **Автономно** в настройках программы (рис. Настройки параметров программы [42]).

5.2.2 Удалённое управление с сервера

При удаленном режиме управления SoftControl SysWatch с помощью средств администрирования программного продукта SoftControl Service Center настройка программы, запуск задач и мониторинг состояния защиты производится администратором удаленно. Подробное описание процесса удаленного управления приведено в документе «Руководство администратора SoftControl Service Center».

Для установки режима выберите вариант **Сервисный Центр** в настройках программы (рис. Настройки параметров программы 42) и нажмите на кнопку **Настроить**, чтобы открыть окно с подробными настройками подключения к серверу (рис. Параметры подключения к серверу 43).

Для применения клиентских настроек, заданных на сервере, выполните следующее:

1) Скопируйте файл *ClientSettings.xmlc* (см. документ «Руководство администратора SoftControl Service Center») на жесткий диск клиентского хоста.
2) Нажмите на кнопку **Обзор** в окне **Настройки SoftControl Server** (рис. Параметры подключения к серверу 43).
3) В появившемся окне выберите ранее скопированный файл *ClientSettings.xmlc* и нажмите на кнопку **Открыть**.

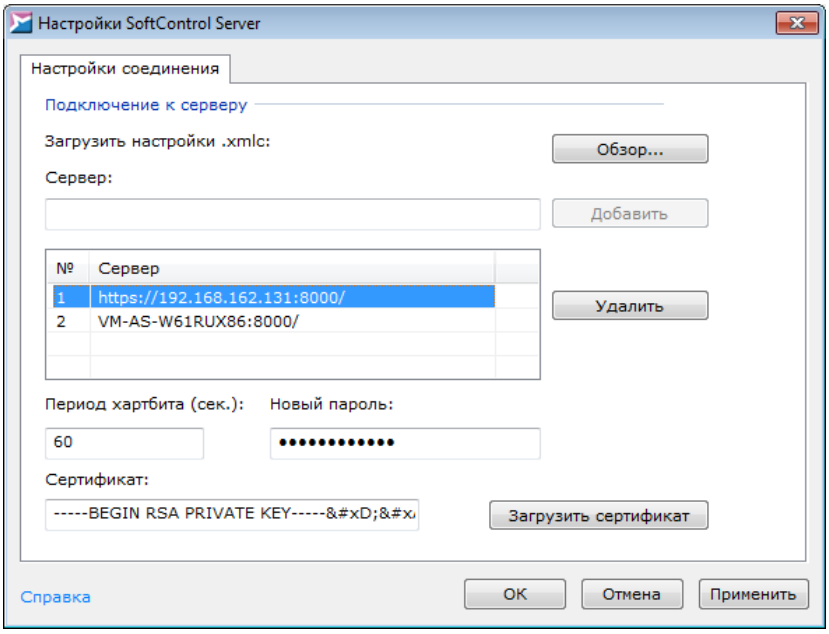

Рисунок 37. Параметры подключения к серверу

Сразу по окончании применения файла настроек SoftControl SysWatch отправляет первый запрос на сервер, в окне **Настройки SoftControl Server** отображается принятая

конфигурация (рис. Параметры подключения к серверу[43]).

В области **Подключение к серверу** расположен список адресов, по которым SoftControl SysWatch осуществляет подключение к управляющему серверу. Список задается администратором удаленно из консоли управления SoftControl Admin Console. Список также может быть изменен вручную через интерфейс SoftControl SysWatch. Для добавления адреса в список введите полную адресную строку вида

https://<IP-адрес или имя сервера>:<порт подключения к серверу>/

в поле **Сервер** и нажмите на кнопку **Добавить**. Для удаления адреса из списка выберите его и нажмите на кнопку **Удалить**. В списке должен находиться по меньшей мере один адрес, поэтому удаление единственного адреса невозможно.

В нижней части области **Подключение к серверу** расположены остальные параметры подключения:

- **Период харбита (сек.)** – интервал между обращениями SoftControl SysWatch к управляющему серверу (в секундах).
- **Новый пароль** – пароль для аутентификации SoftControl SysWatch с указанным ниже сертификатом на управляющем сервере.
- **Сертификат** – строковое представление сертификата, используемого для установления безопасного соединения между SoftControl SysWatch и управляющим сервером.

Все параметры могут быть изменены вручную в соответствующих полях. Для замены сертификата без изменения остальных настроек нажмите на кнопку **Загрузить сертификат**, в открывшемся окне выберите файл сертификата с расширением *.pem* и нажмите на кнопку **Открыть**.

Если требуется выполнить локальное отсоединение SoftControl SysWatch от текущего сервера, перейдите в настройки программы и в разделе **Параметры** нажмите на кнопку **Очистить** (рис. Настройки параметров программы[42]). В окне с предупреждением выберите вариант **Да** (рис. Предупреждение при очистке параметров подключения к серверу[44]).

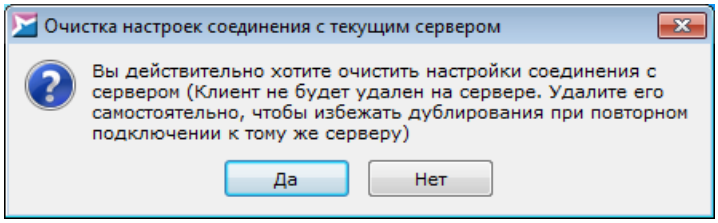

Рисунок 38. Предупреждение при очистке параметров подключения к серверу

После очистки настроек SoftControl SysWatch автоматически переключается в автономный режим работы. Чтобы избежать дублирования клиентских компонентов при повторном подключении к тому же серверу, администратору необходимо удалить данный клиентский компонент с сервера из консоли управления SoftControl Admin Console.

5.3 Активация лицензионного ключа

Возможность использования SoftControl SysWatch определяется наличием лицензионного ключа. Лицензия дает право использовать компоненты программы со дня активации ключа:

- SoftControl SysWatch Core (Core) – базовый компонент проактивной защиты SoftControl SysWatch
- Anti_virus (AV-AV4) – дополнительный компонент поиска вирусов, троянских программ и других вредоносных объектов (сканер Avira).

Типы лицензий SoftControl SysWatch описаны в табл. 7.

Таблица 7. Типы лицензий

Лицензия	Описание
Пробная	Лицензионный ключ для пробного использования программы. Срок действия – 30 дней. Примечание: может быть использован на одном компьютере только один раз. Продление и повторное использование ключа невозможно.
Коммерческая	Лицензионный ключ для полноценного использования программы. Свойства лицензии и используемые дополнительные компоненты определяются конкретными лицензионными ключами.

Для локальной активации лицензионного ключа перейдите на вкладку **Лицензия** панели управления [36] SoftControl SysWatch, введите ключ в поле **Номер** и нажмите на кнопку **Активировать**. В случае успешной активации отображается статус *Действующая лицензия*.

За 30 дней, 2 недели до истечения срока, а также в течение последней недели действия ключа приложение уведомляет об этом пользователя. В указанные дни на экран выводится

соответствующее сообщение. По окончании срока действия ключа на вкладке **Лицензия** отображается статус *Лицензия закончилась*. После этого отключается возможность обновления программных модулей и антивирусных баз[122]. Кроме того, запрещается установка msi-пакетов, если включен контроль активности приложений (выставлена галочка **Приложения** в разделе **Защита** настроек программы, см. рис. Настройки общих параметров защиты[46]). В остальном функциональность SoftControl SysWatch сохраняется.

Через два месяца после истечения срока действия ключа каждый час поверх всех окон выводится сообщение о том, что лицензия истекла. Сообщение отображается в течение 10 секунд.

Чтобы использовать новые функции программы и последние разработки в области превентивных технологий, рекомендуется продлевать лицензию программы.

5.4 Автоматическая настройка (сбор профиля)

Автоматическая настройка, или сбор профиля, является важным этапом в обеспечении проактивной защиты программного окружения системы. Сбор профиля запускается автоматически по окончании установки SoftControl SysWatch, за исключением случаев, когда снят флажок **Включить сбор профиля после установки** (см. рис. Включение сбора профиля[15]). Предполагается, что перед началом сбора профиля система не содержит вредоносных объектов. По этой причине первоначальный сбор профиля по умолчанию осуществляется с включенной опцией антивирусного сканирования[46] для надежного обеспечения указанного условия. Если объект не инфицирован, то рассчитывается его контрольная сумма и добавляется в профиль. Объектами являются файлы формата PE (переносимые исполняемые файлы).

Перед началом сбора профиля по требованию[49] выполните настройку его параметров[46].

5.4.1 Опции сбора профиля

Для настройки параметров сбора профиля откройте раздел **Защита** настроек программы, в области **Режим защиты** нажмите на кнопку **Настроить** (рис. Настройки общих параметров защиты[46]).

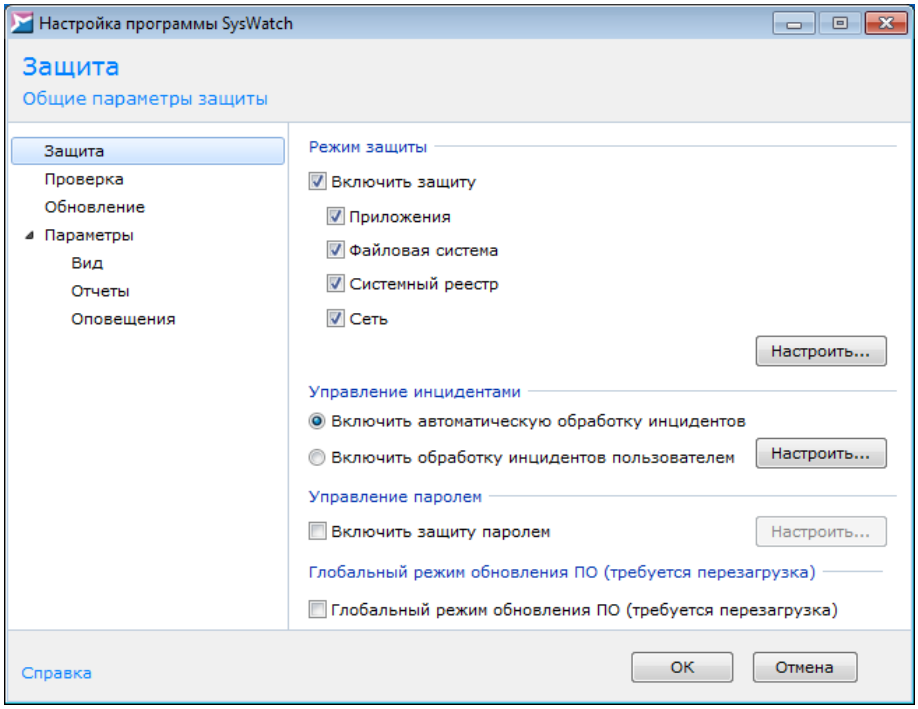

Рисунок 39. Настройки общих параметров защиты

В окне **Настройка режима защиты** на вкладке **Профиль системы** нажмите на ссылку **Настройка** (рис. Окно сбора профиля [47]).

В области **Состояние компьютера** (рис. Настройки сбора профиля [48]) возможен выбор двух вариантов автоматической настройки:

- **Требуется проверка**

  При выборе данной опции будет производиться полная автоматическая настройка, включающая в себя антивирусное сканирование. Рекомендуется проводить проверку в процессе автоматической настройки в случае, когда в системе не установлено антивирусное ПО и возможны уязвимости в области безопасности.

- **Чистый, проверка не требуется**

  В случае выбора данной опции автоматическая настройка будет производиться без антивирусного сканирования.

При полной автоматической настройке затрачивается больше системных ресурсов и времени, чем при автоматической настройке без антивирусного сканирования.

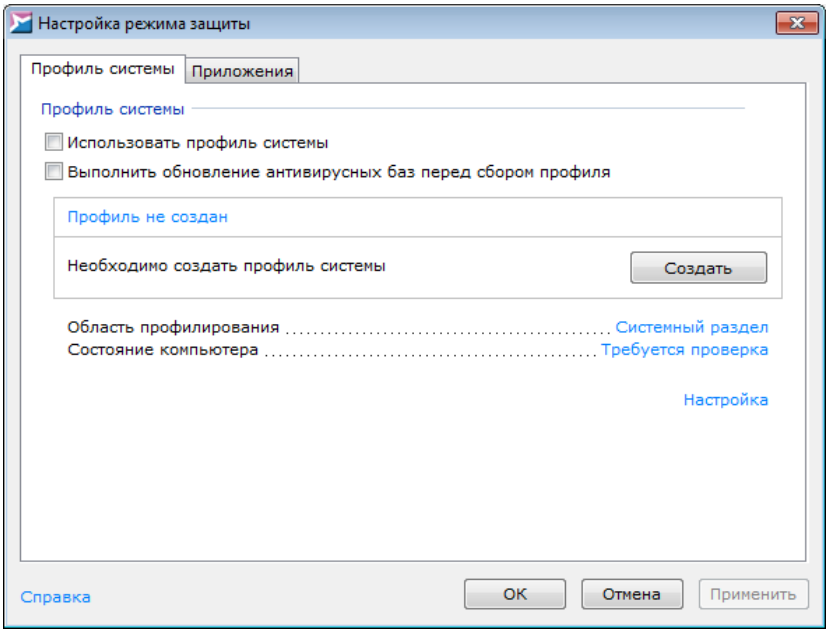

Рисунок 40. Окно сбора профиля

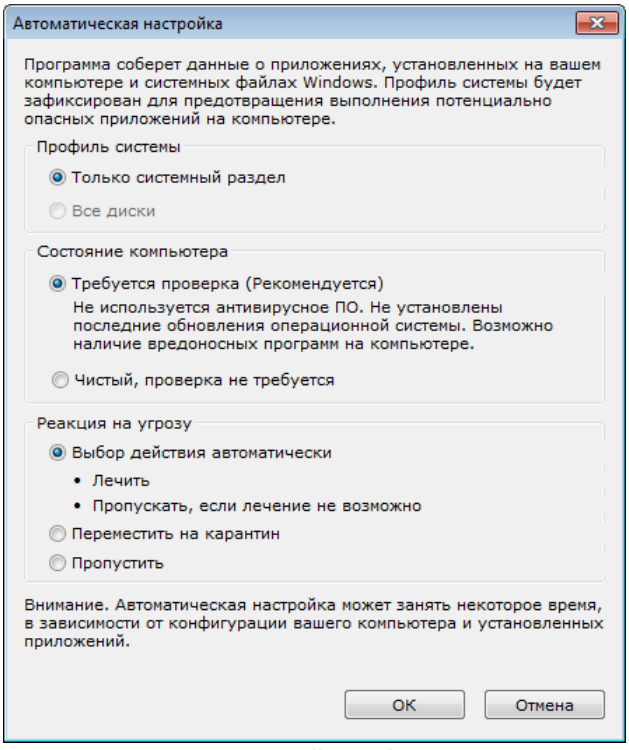

Рисунок 41. Настройки сбора профиля

В области **Реакция на угрозу** (доступна только при выборе полной автоматической настройки) возможны следующие варианты действий при обнаружении угроз в процессе антивирусного сканирования:

- **Выбор действия автоматически**:
  - **Лечить**

Обезвредить зараженный объект.

- **Пропускать, если лечение невозможно**

Не выполнять каких-либо действий над зараженным объектом, если обезвредить его не удается.

○ **Переместить на карантин**

Переместить зараженный объект в специальный каталог и запретить его выполнение.

○ **Пропустить**

Не выполнять каких-либо действий над зараженным объектом.

5.4.2 Запуск по требованию

Запуск сбора профиля

Для начала сбора профиля в окне **Настройка режима защиты** на вкладке **Профиль системы** нажмите на кнопку **Создать** (рис. Окно сбора профиля 47).

Во время автоматической настройки нежелательно выполнять установку ПО в системе.

Если необходимо прервать сбор профиля, нажмите на кнопку **Остановить** (рис. Процесс сбора профиля 49).

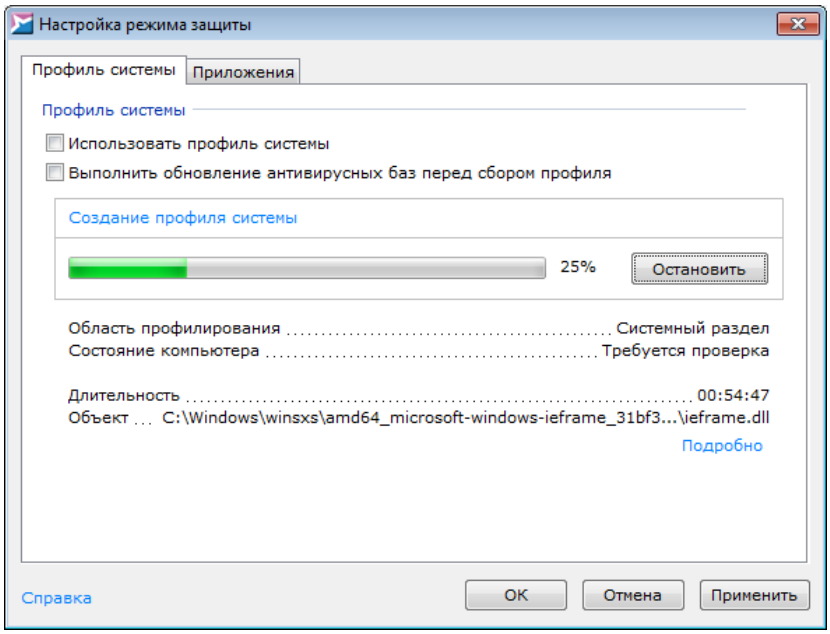

Рисунок 42. Процесс сбора профиля

В диалоговом окне выберите, сохранять ли накопленную информацию о файлах для

использования при продолжении сбора профиля (рис. Выбор режима прерывания сбора профиля [50]). При выборе варианта **Да** вы сможете продолжить сбор профиля с того места, где он был прерван.

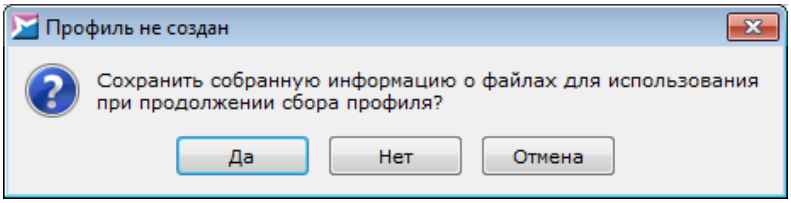

Рисунок 43. Выбор режима прерывания сбора профиля

Если работа системной службы *safensec.exe* была каким-либо образом завершена в процессе сбора профиля, то после ее повторного запуска профиль продолжит собираться автоматически. Если сбор профиля был остановлен пользователем с помощью соответствующей кнопки, то после повторного запуска системной службы *safensec.exe* профиль собираться не будет. В этом случае для продолжения автоматической настройки необходимо запустить ее вручную.

По окончании процесса автоматической настройки отображается статус *Профиль создан* и автоматически устанавливается флажок **Использовать профиль системы** – программа переходит в штатный режим работы.

Не рекомендуется снимать флажок **Использовать профиль системы**, так как в этом случае перестает работать контроль исполняемых файлов PE.

Обновление профиля системы

В случае необходимости (например, если было развернуто большое число ПО без использования программ установки или когда защита SoftControl SysWatch была отключена) можно обновить профиль системы.

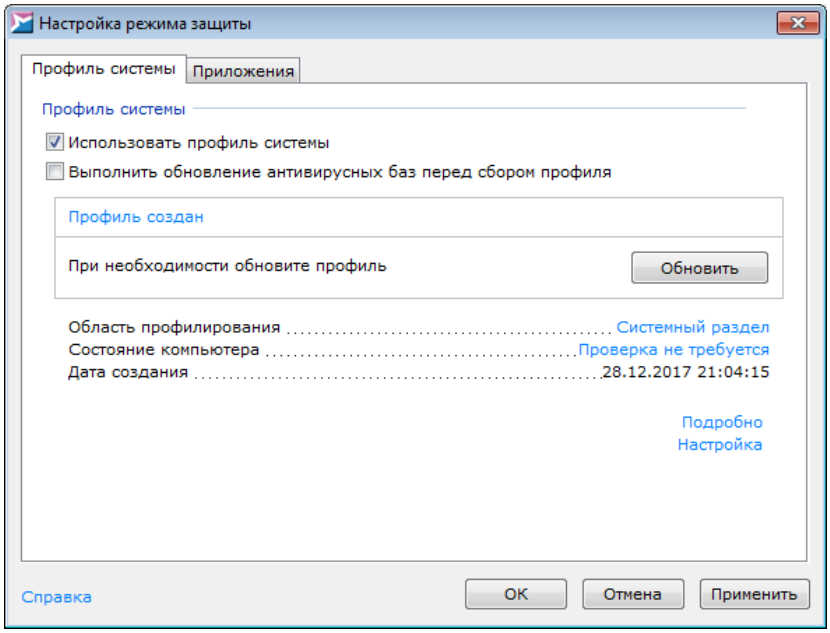

Рисунок 44. Запуск обновления профиля

При этом полный сбор профиля не производится, собираются данные только о тех приложениях, которые не включены в профиль на момент начала его обновления. Для выполнения операции в окне **Настройка режима защиты** на вкладке **Профиль системы** нажмите на кнопку **Обновить** (рис. Запуск обновления профиля 50).

Добавление отдельных файлов в профиль

Если требуется добавить только определенный файл или каталог с файлами в профиль системы, в окне **Настройка режима защиты** на вкладке **Профиль системы** нажмите на строку **Область профилирования** (рис. Запуск обновления профиля 50), выберите соответствующий вариант (**Добавить файл** или **Добавить папку**), укажите необходимые файлы и нажмите на кнопку **Открыть**. После того, как в строке **Область профилирования** отобразится путь к требуемому файлу или каталогу, нажмите на кнопку **Обновить**.

Просмотр отчёта о сборе профиля

Для просмотра подробного отчета о проведенном сборе профиля нажмите на ссылку **Подробно** (рис. Запуск обновления профиля 50).

5.5 Детальная настройка SoftControl SysWatch

По классификации SoftControl SysWatch виды событий, представляющих угрозу безопасности программной среды (инциденты), подразделяются на следующие основные категории:

- Запуск приложения не в профиле.
- Запуск неподписанного инсталлятора.
- Нарушение политики контроля.

Возможные действия для каждой категории инцидентов перечислены в табл. 8.

Таблица 8. Возможные действия при инцидентах

Инцидент	Действия
Запуск приложения не в профиле 59	• **Выполнить в ограниченном режиме** Выполнение приложения в изолированной среде ("песочнице") под учетной записью пользователя «V.I.P.O.» с ограниченными привилегиями. При этом добавления в профиль системы не происходит, а приложение помещается в ограниченную зону. Приложение может загружать дочерние модули, которые также не войдут в профиль системы. Даже если такое приложение является вредоносным и выполнит установку каких-либо дополнительных компонентов, то их последующая загрузка будет предотвращена. • **Выполнить в ограниченном режиме после проверки** Запуск приложения в ограниченном режиме, если при антивирусном сканировании приложения не найдено вредоносного кода. В обратном случае запуск будет заблокирован. • **Выполнить в режиме обновления ПО** Выполнение приложения под текущей учетной записью без ограничений. При этом приложение и все его дочерние модули помещаются в профиль системы и доверенную зону. • **Выполнить в режиме обновления ПО после проверки** Запуск приложения в режиме обновления ПО, если при антивирусном сканировании приложения не найдено вредоносного кода. В обратном случае запуск будет заблокирован. • **Заблокировать** (по умолчанию) Блокировка запуска приложения.
Запуск неподписанного инсталлятора 61	• **Установить** Выполнение инсталлятора под текущей учетной записью без ограничений. При этом после установки приложение и все его дочерние модули помещаются в профиль системы и доверенную зону. • **Установить после проверки** Запуск инсталлятора в режиме обновления ПО, если при антивирусном сканировании установщика не найдено вредоносного кода. В обратном случае запуск будет заблокирован. • **Установить в ограниченном режиме** Выполнение инсталлятора в изолированной среде ("песочнице") под учетной записью пользователя «V.I.P.O.» с ограниченными привилегиями. При этом добавления в профиль системы не происходит.

Инцидент	Действия
	• **Установить в ограниченном режиме после проверки** Запуск инсталлятора в ограниченном режиме, если при антивирусном сканировании инсталлятора не найдено вредоносного кода. В обратном случае запуск будет заблокирован. • **Заблокировать** (по умолчанию) Блокировка запуска инсталлятора.
Нарушение политики контроля [72]	• **Разрешить** Разрешение приложению выполнить действие, совпадающее с условиями правила заданной политики контроля, однократно/на сессию. • **Разрешить после проверки** Разрешение приложению выполнить действие, совпадающее с условиями правила заданной политики контроля, однократно/на сессию, если при антивирусном сканировании приложения не найдено вредоносного кода. В обратном случае действие будет запрещено. • **Запретить** Запрет приложению выполнить действие, совпадающее с условиями правила заданной политики контроля, однократно/на сессию. • **Запретить и завершить приложение** Запрет приложению выполнить действие, совпадающее с условиями правила заданной политики контроля, и последующее завершение приложения, однократно/на сессию.

На вкладке **Статус** панели управления [36] программы отображается текущий статус защиты и список областей отслеживания. Также на вкладке приводится статистика по общему количеству зарегистрированных SoftControl SysWatch приложений в системе, статистика по количеству приложений в каждой из зон выполнения [62], а также имя приложения, вызвавшего последний по времени инцидент. По умолчанию устанавливается отслеживание по всем областям защиты, при этом отображается статус *Компьютер защищен*. Отключение и включение отслеживания по каждой области осуществляется нажатием левой кнопки мыши по названию области; при этом общий статус защиты изменяется на *Неполная защита компьютера*, если отключено отслеживание хотя бы по одной области, и на *Компьютер не защищен*, если отключено отслеживание по всем областям. Данные возможности также дублируются в настройках программы в разделе **Защита** (рис. Настройки общих параметров защиты [53]). Отслеживание активности приложений включено, когда отмечена область защиты **Приложения**.

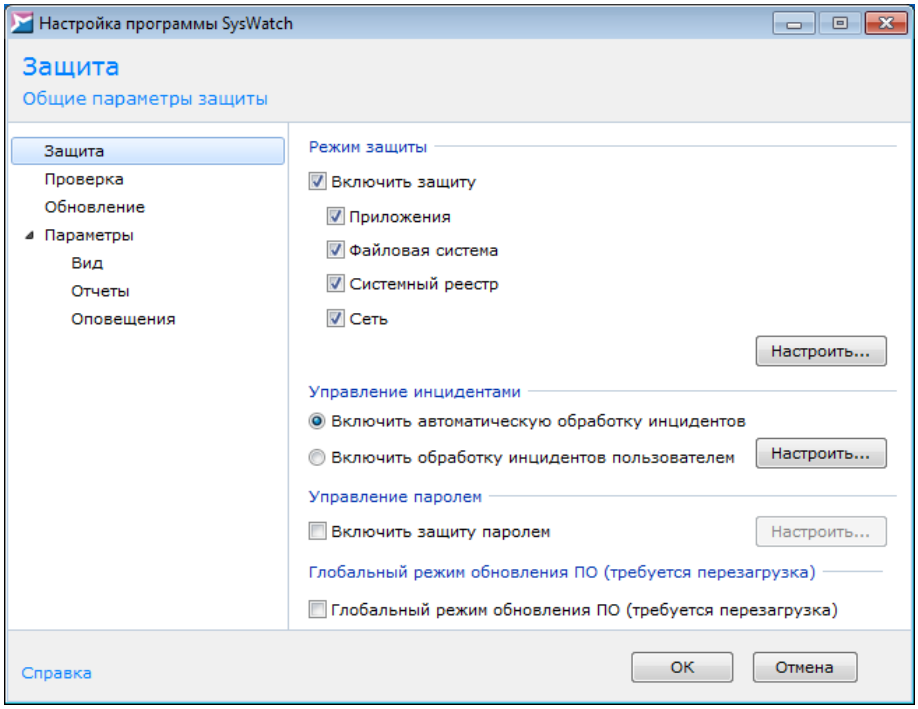

Рисунок 45. Настройки общих параметров защиты

Ниже приведена детальная информация по настройке отслеживания активности приложений:

- опции отслеживания активности [54];
- обработка инцидентов запуска приложений [57];
- зоны выполнения приложений [62];
- свойства отдельных приложений [65];
- белый список сертификатов [70].

5.5.1 Опции отслеживания активности

Для изменения дополнительных опций отслеживания активности откройте раздел **Защита** настроек программы, в области **Режим защиты** нажмите на кнопку **Настроить** (рис. Настройки общих параметров защиты [53]) и в окне **Настройка режима защиты** перейдите на вкладку **Приложения** (рис. Опции контроля активности [56]).

В области **Приложения** расположены следующие опции:

- **Сохранять историю активности неотслеживаемых приложений и инсталляторов**:

  Автоматическое включение опции записи истории активности [68] при первом запуске приложения, отсутствующего в профиле, или инсталлятора без ЭЦП.

❑ **Запретить выполнение скриптов**:

Блокировка выполнения недоверенных скриптов интерпретаторами (кроме скриптов, подписанных ЭЦП из белого списка сертификатов[70]). Запрещаются следующие процессы:

- wscript.exe (Microsoft ® Windows Based Script Host);
- cscript.exe (Microsoft ® Console Based Script Host);
- java.exe (Java™ Platform SE binary);
- javaw.exe (Java™ Platform SE binary);
- javaws.exe (Java™ Web Start Launcher).

Для запрета запуска определенных процессов рекомендуется создавать соответствующие Правила политики контроля[72].

❑ **Включить контроль dll-модулей (требуется перезагрузка)**:

Контроль целостности динамически подключаемых библиотек (DLL), используемых исполняемыми компонентами.

Контроль запуска dll-модулей работает следующим образом. При попытке загрузить dll-библиотеку SoftControl SysWatch проверяет, подписана ли она ЭЦП. Если библиотека подписана и Windows признает ЭЦП действительной, то загрузка библиотеки разрешается (даже если ее нет в профиле). Если у библиотеки отсутствует ЭЦП, SoftControl SysWatch проверяет, есть ли данная библиотека в профиле. Если есть, запуск разрешается; если нет – отклоняется.

Примечание: не поддерживается запрет на запуск библиотек, в которых отсутствует точка входа (библиотек, содержащих только ресурсы, без исполняемого кода).

❑ **Запретить всем, кроме инсталляторов, модификацию исполняемых файлов PE**:

Запрет изменения исполняемых файлов (exe, dll и т.п.) всеми приложениями, кроме работающих в режиме обновления ПО. Позволяет снизить риски нарушения целостности системы.

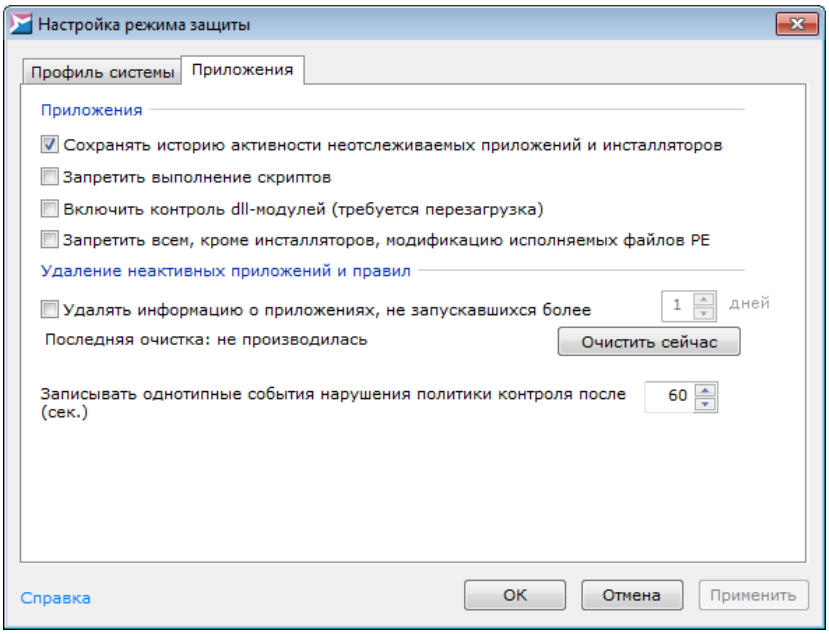

Рисунок 46. Опции контроля активности

В области **Удаление неактивных приложений и правил** установите флажок **Удалять информацию о приложениях, не запускавшихся более** и выберите количество дней, если требуется удалять из базы данных SoftControl SysWatch записи о неактивных приложениях, удовлетворяющих заданному условию. Чтобы произвести очистку немедленно, нажмите на кнопку **Очистить сейчас**. Чтобы собирать историю активности приложений, выставите галочку **Хранить историю активности приложений** (см. рисунок ниже 68).

Чтобы изменить интервал, после которого однотипные события нарушения политики контроля начнут записываться в журнал, задайте требуемое значение в секундах в поле **Записывать однотипные события нарушения политики контроля после (сек.)** (по умолчанию 60 секунд). События нарушения политики контроля считаются *однотипными* и не вносятся в файл отчета, если одновременно выполняются следующие условия:

- у событий совпадают:
  - тип активности;
  - программы-источники инцидентов;
  - контролируемые объекты;
  - идентификаторы (PID) процессов;
- время, прошедшее с момента добавления предыдущего события, меньше заданного значения.

При этом в файл отчета добавляется информация о том, сколько однотипных событий было пропущено.

В SoftControl SysWatch реализован глобальный режим обновления ПО для поддержки выполнения многошаговых программ установки. При включении данного режима все приложения запускаются как инсталлятор и добавляются в профиль (режим обучения). Кроме того, в профиль добавляются все изменения в исполняемых файлах PE. Для включения режима установите флажок у опции **Глобальный режим обновления ПО (рекомендуется перезагрузка)** в разделе **Защита** настроек программы (рис. Настройки общих параметров защиты 53) и перезагрузите систему. Также управление глобальным режимом обновления ПО возможно в тихом режиме с помощью дополнительной утилиты changetpsmode 120.

> Во избежание добавления в профиль вредоносного ПО опцию **Глобальный режим обновления ПО** рекомендуется использовать только на "чистых" системах, все ПО для которых устанавливалось с "золотого" образа.

Для отключения режима снимите флажок и перезагрузите систему.

5.5.2 Обработка инцидентов запуска приложений

Общая схема реагирования на инциденты запуска приложений, отсутствующих в профиле, представлена на рисунке ниже 57.

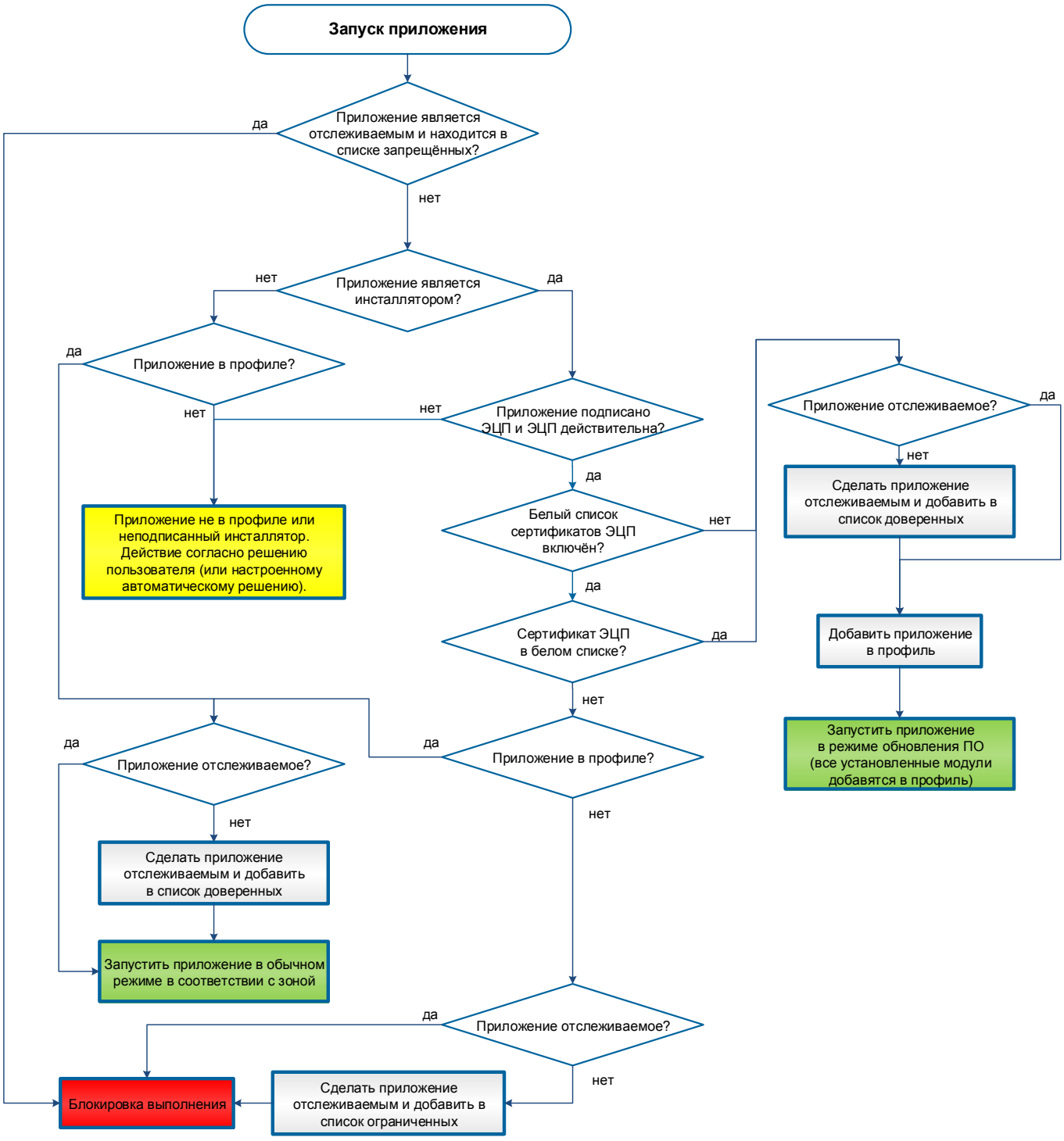

Рисунок 47. Общая схема обработки запуска приложений, отсутствующих в профиле

Окончательное *решение* (рис. выше 57) выбирается в зависимости от режима управления инцидентами:

- **Автоматический**

Решение принимается SoftControl SysWatch исходя из параметров обработки инцидентов, без обращения к пользователю. Для установки данного режима и изменения его параметров откройте раздел **Защита** настроек программы, установите переключатель **Управление инцидентами** в положение **Включить автоматическую обработку инцидентов** и нажмите на кнопку **Настроить** (рис. Настройки общих параметров защиты 53). В окне **Управление инцидентами** (рис. Настройка реакции на инциденты 59) в **Списке инцидентов** выберите требуемый тип события и в выпадающем меню **Решение** установите действие, которое будет производиться SoftControl SysWatch при наступлении данного события.

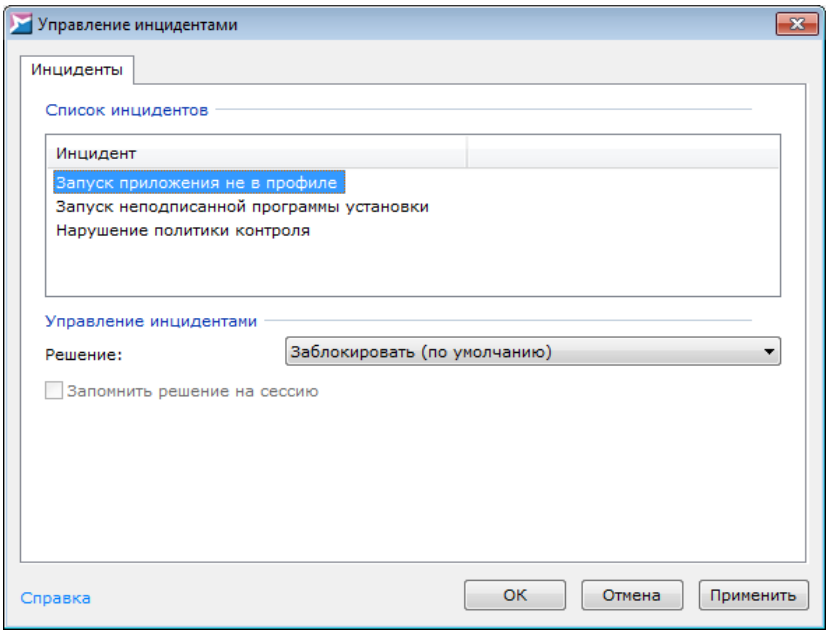

Рисунок 48. Настройка реакции на инциденты

Полный перечень инцидентов и возможных реакций на них приведен в табл. 8 выше 52. Для подтверждения выбранных установок нажмите на кнопку **OK**.

- **Ручной**

Решение принимается SoftControl SysWatch исходя из выбора пользователя, отметившего требуемый вариант в диалоговом окне. Для установки данного режима откройте раздел **Защита** настроек программы, установите переключатель **Управление инцидентами** в положение **Включить обработку инцидентов пользователем** и нажмите на кнопку **OK** (рис. Настройки общих параметров защиты 53).

Запуск приложения не в профиле

Окно предупреждения, отображаемое SoftControl SysWatch при запуске приложения не в профиле, показано на рис. Окно предупреждения для приложения не в профиле [60].

Окно **Предупреждение - SoftControl SysWatch** состоит из 2 частей:

- Область описания приложения. В данном блоке приводится информация о приложении не в профиле: имя, изготовитель, результат антивирусной проверки [98] (можно проверить приложение перед принятием решения, нажав на ссылку **Проверить объект** и выбрав в контекстном меню вариант **Запустить проверку**).
- Область выбора действия. В блоке выбора действия отображаются возможные действия при запуске приложения не в профиле:
  - → **Выполнить**
    - **однократно запустить в ограниченной зоне** – выполнить приложение в изолированной среде ("песочнице") под учетной записью пользователя «V.I.P.O.» с ограниченными привилегиями;
    - **запустить в режиме обновления ПО** – выполнить приложение и добавить в профиль системы.

Рекомендуется выбирать это действие только в случае, если вы уверены, что данное приложение не нанесет вреда системе.

→ **Запретить** – заблокировать выполнение приложения.

Рекомендуется выбирать это действие, если происхождение приложения неизвестно или его запуск не санкционирован пользователем.

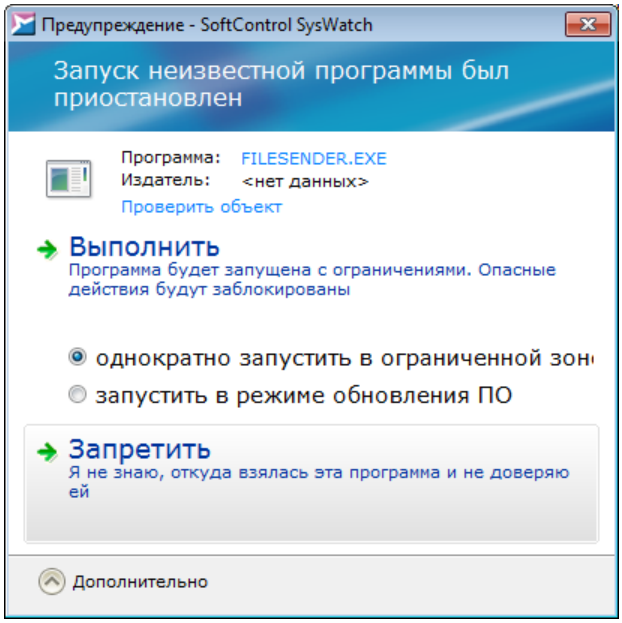

Рисунок 49. Окно предупреждения для приложения не в профиле

Если в течение 5 минут действие не будет выбрано, SoftControl SysWatch заблокирует запуск приложения и закроет окно предупреждения.

Запуск неподписанного инсталлятора

Окно предупреждения, отображаемое SoftControl SysWatch при запуске неподписанного инсталлятора, показано на рис. Окно предупреждения для неподписанного инсталлятора [61].

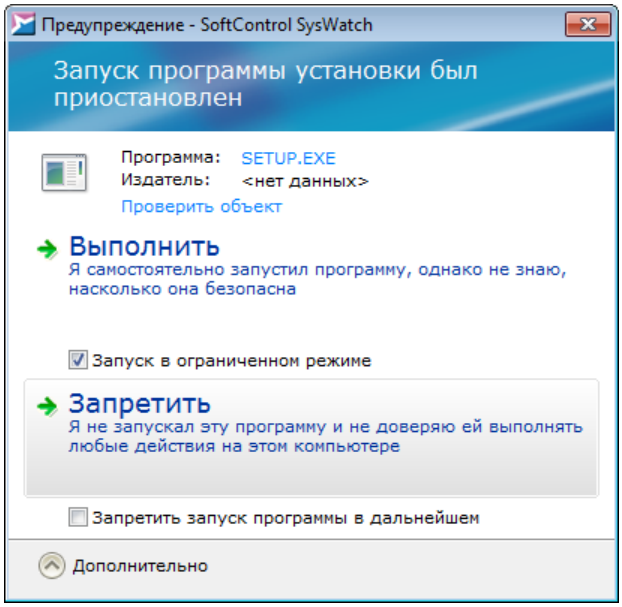

Рисунок 50. Окно предупреждения для неподписанного инсталлятора

Окно **Предупреждение - SoftControl SysWatch** состоит из 2 частей:

- Область описания инсталлятора. В данном блоке приводится информация о неподписанном инсталляторе: имя, изготовитель, результат антивирусной проверки [98] (можно проверить инсталлятор перед принятием решения, нажав на ссылку **Проверить объект** и выбрав в контекстном меню вариант **Запустить проверку**).
- Область выбора действия. В блоке выбора действия отображаются возможные действия при запуске неподписанного инсталлятора:

  → **Выполнить** – Запустить инсталлятор и добавить его и все установленные модули в профиль системы;

Рекомендуется выбирать это действие, если уверены, что данный инсталлятор не нанесет вреда системе.

  ❑ **запуск в ограниченном режиме** – запустить инсталлятор в изолированной среде ("песочнице") под учетной записью пользователя «V.I.P.O.» с ограниченными правами, без добавления установленных модулей в профиль системы.

  → **Запретить** – заблокировать выполнение инсталлятора.

Рекомендуется выбирать это действие, если происхождение программы установки неизвестно или ее запуск не санкционирован пользователем.

Если в течение 5 минут действие не будет выбрано, SoftControl SysWatch заблокирует запуск инсталлятора и закроет окно предупреждения.

5.5.3 Зоны выполнения приложений

Чтобы просмотреть и изменить текущее распределение приложений по зонам выполнения, выберите пункт **Отслеживаемые приложения** контекстного меню [35] SoftControl SysWatch. В окне **Политика контроля** на вкладке **Отслеживаемые приложения** содержатся все отслеживаемые приложения, то есть зарегистрированные SoftControl SysWatch с момента установки программы (рис. Процессы и приложения [62]).

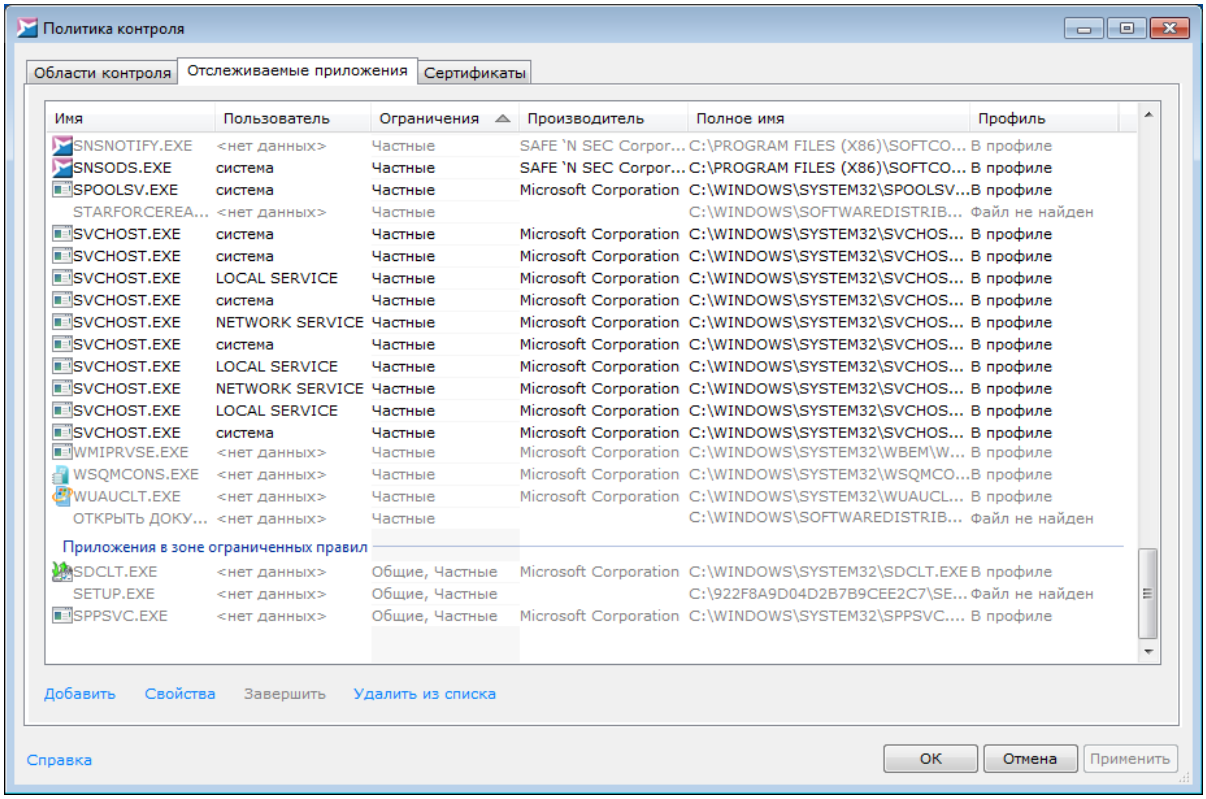

Рисунок 51. Отслеживаемые приложения

Каждое приложение (процесс) расположено в одной из зон выполнения и имеет следующие параметры:

- **Имя** – имя исполняемого файла приложения.
- **Пользователь** – учетная запись пользователя, под которой запускается приложение.
- **Ограничения** – набор ограничений и разрешений, которые действуют при выполнении приложения:
  - **Частные** – действуют для отдельного приложения.
  - **Общие** – действуют для всех приложений в зоне выполнения.
  - **Запрет выполнения** – выполнение приложения запрещено.
- **Производитель** – изготовитель приложения.
- **Полное имя** – полный путь к исполняемому файлу приложения.
- **Авторские права** – информация об обладателе авторских прав на приложение.
- **Описание** – краткое описание основной функции.
- **Версия файла** – полная версия исполняемого файла приложения.
- **Версия** – версия приложения (продукта).

- **Рабочее название** – рабочее наименование от изготовителя приложения.
- **Название** – наименование приложения.
- **Продукт** – программный продукт, в который входит приложение.
- **Идентификатор** – идентификатор приложения в системе.
- **Статус** – состояние приложения:
  - **Выполняется** – активный процесс, приложение выполняется в данный момент (имя обозначено черным цветом);
  - неактивный процесс, приложение не выполняется в данный момент (имя обозначено серым цветом).
- **Удалить при перезагрузке** – индикатор необходимости удаления исполняемого файла приложения после перезагрузки системы:
  - **Нет** – файл приложения не будет удален после перезагрузки;
  - **Да** – файл приложения будет удален после перезагрузки.
- **Профиль** – индикатор нахождения контрольной суммы приложения в профиле системы:
  - **В профиле**;
  - **Не в профиле**;
  - **Профиль отключен**;
  - **Профиль не собран**;
  - **Файл не найден**.

Возможные действия в списке приложений:

Добавление/удаление приложения из списка

Если приложение отсутствует в списке, можно добавить его вручную, нажав на ссылку **Добавить** и указав путь к приложению. Обратное действие совершается с помощью ссылки **Удалить из списка** (либо клавишей **Delete**). Если данное приложение не включено в профиль системы, то для того, чтобы оно запускалось с требуемыми привилегиями, необходимо добавить его в профиль 64.

Добавление/удаление приложения из профиля системы

Если требуется переместить приложение в профиль системы или удалить его без

обновления всего профиля [50], вызовите контекстное меню нажатием правой кнопки мыши на требуемом приложении и выберите необходимый вариант:

- **Добавить в профиль**;
- **Удалить из профиля**.

Данная возможность доступна, только если одновременно выставлены флажки **Использовать профиль системы** (рис. Окно сбора профиля [47]) и **Приложения** в области **Режим защиты** (рис. Настройки общих параметров защиты [46]).

Изменение зоны выполнения приложения

Для перемещения приложения между зонами выполнения вызовите контекстное меню нажатием правой кнопки мыши на требуемом приложении и выберите один из вариантов (в зависимости от текущей зоны выполнения):

- **Запретить выполнение приложения**;
- **Удалить приложение из доверенных**;
- **Разрешить выполнение приложения**;
- **Сделать приложение доверенным**.

Завершение процесса

Если приложение запущено в текущий момент, можно прервать выполнение процесса, выбрав требуемое приложение в списке и нажав ссылку **Завершить**. Для того чтобы **Удалить файл приложения при перезагрузке**, вызовите контекстное меню и выберите одноименный пункт.

5.5.4 Свойства отдельных приложений

SoftControl SysWatch позволяет задавать не только общие правила контроля активности для всех приложений, но и работать со свойствами отдельных приложений, включая задание частных правил. Для этого выберите пункт **Свойства приложения** в контекстном меню приложения на вкладке Процессы и приложения [62].

Просмотр подробной информации о приложении

Для просмотра подробной информации об отдельном приложении перейдите на вкладку **Общие** окна **Свойства приложения** (рис. Общая информация о приложении

66).

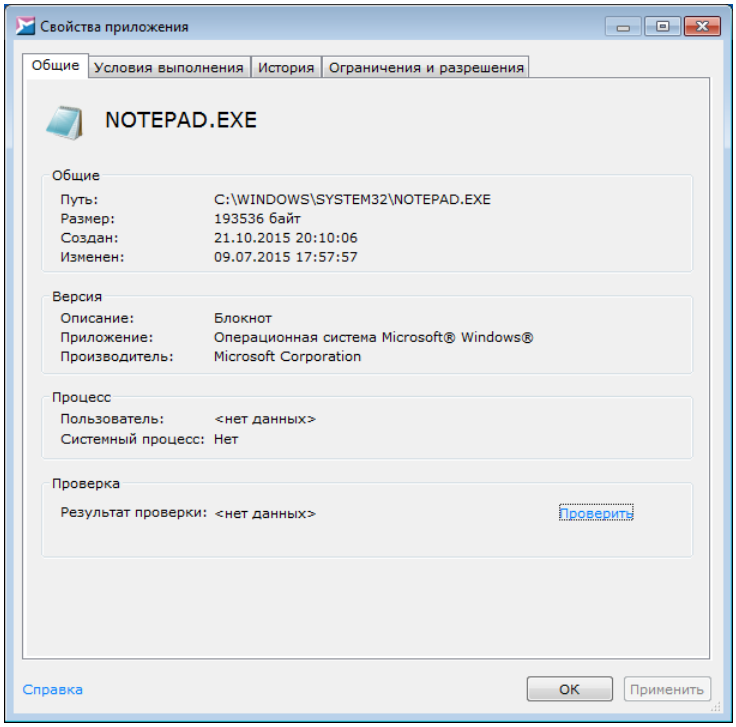

Рисунок 52. Общая информация о приложении

Для антивирусной проверки исполняемого файла приложения нажмите на ссылку **Проверить** и выберите в контекстном меню вариант **Запустить проверку**.

Задание условий выполнения

Для просмотра текущих условий выполнения приложения и их изменения перейдите на вкладку **Условия выполнения** окна **Свойства приложения** (рис. Условия выполнения приложения: доверенные 66 и Условия выполнения приложения: ограниченные 67).

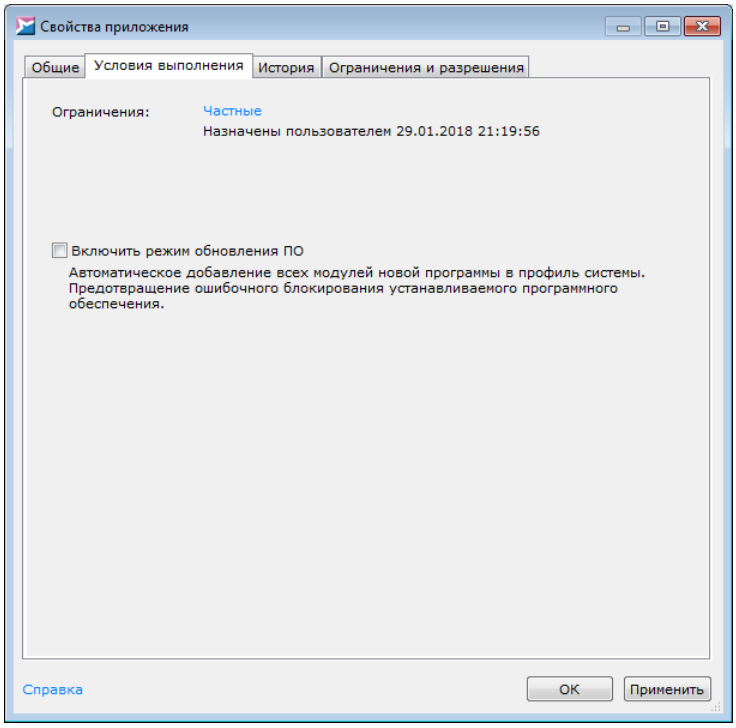

Рисунок 53. Условия выполнения приложения: доверенные

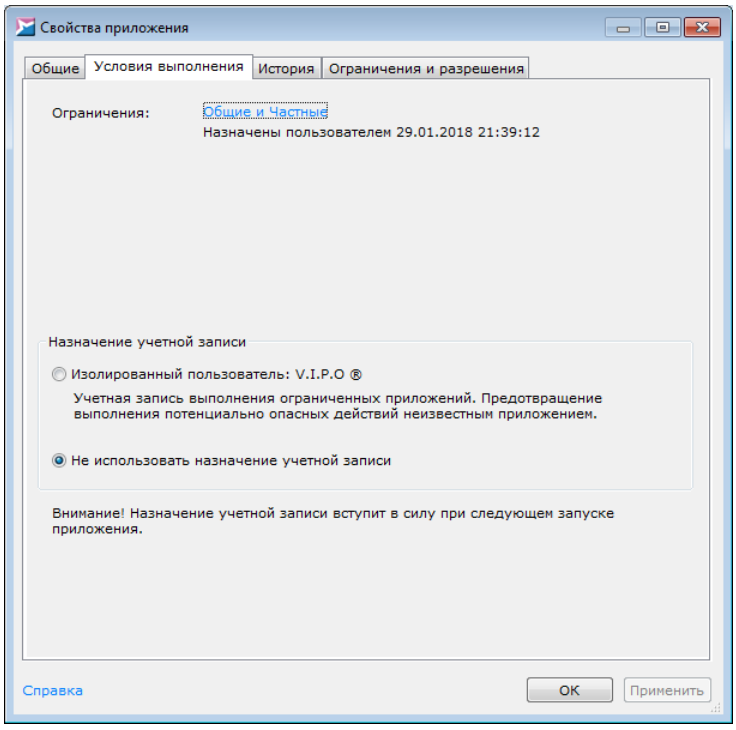

Рисунок 54. Условия выполнения приложения: ограниченные

На данной вкладке указаны категории **Ограничений** для данного приложения, изменить которые можно нажатием на них и выбором одного из вариантов в контекстном меню (в зависимости от текущей зоны выполнения):

- **Запретить выполнение приложения**;
- **Удалить приложение из доверенных**;
- **Разрешить выполнение приложения**;
- **Сделать приложение доверенным**.

При выборе опции **Включить режим обновления ПО** происходит включение всех модулей программы в профиль системы. Для включения опции установите соответствующий флажок. Опция доступна только для доверенных приложений.

Переключатель **Назначение учетной записи** отвечает за выбор учетной записи пользователя, под которой должно осуществляться выполнение приложения (только для ограниченных приложений):

- **Не использовать назначение учетной записи**: запуск приложения под текущей учетной записью;
- **Изолированный пользователь V.I.P.O. ®**: запуск приложения из ограниченной зоны под учетной записью пользователя «V.I.P.O.» с ограниченными правами.

Сохранение истории активности приложения

Для просмотра истории активности приложения при доступе к файловым ресурсам и системному реестру перейдите на вкладку **История** окна **Свойства приложения** (рис. История активности приложения 68).

Установите флажок **Хранить историю активности приложений** для включения функции хранения истории. Для обновления информации на вкладке **История** нажмите на ссылку **Обновить**.

Установите флажок **Создавать резервные копии объектов для последующего восстановления**, если необходимо сохранять резервные копии модифицированных приложением объектов. Для восстановления объекта к предыдущему состоянию выберите в списке событие по его изменению и нажмите на ссылку **Восстановить**.

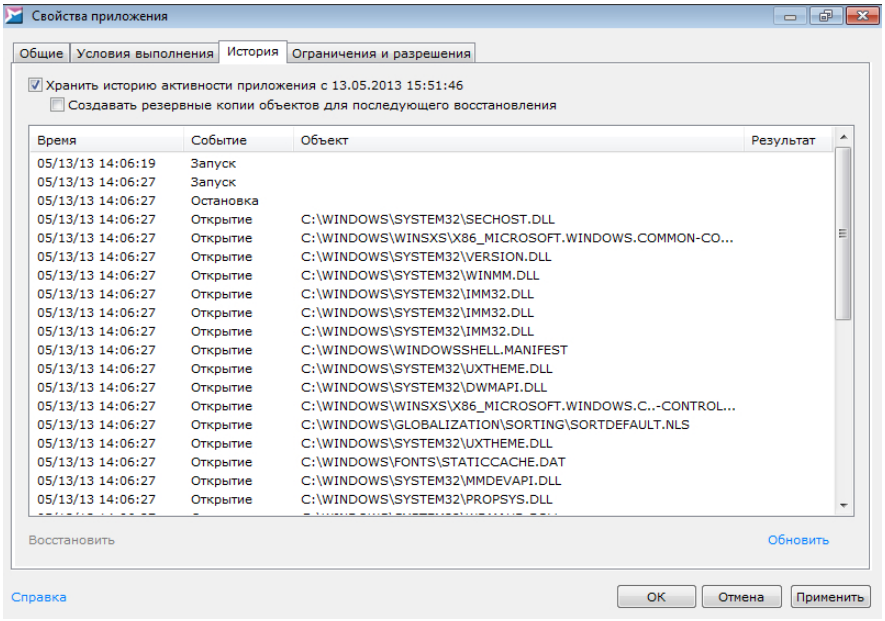

Рисунок 55. История активности приложения

Задание частных правил

Для задания частных правил перейдите на вкладку **Ограничения и разрешения** окна **Свойства приложения** (рис. Частные правила приложения 69) и выберите одну из областей контроля в выпадающем списке:

- **Файловая система**;
- **Системный реестр**;
- **Сеть**;
- **Привилегии процессов**.

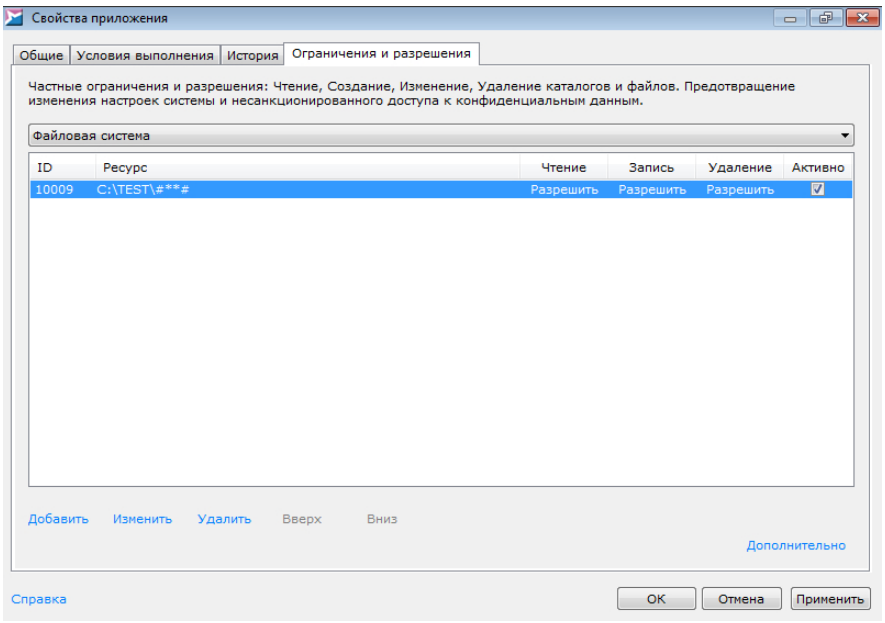

Рисунок 56. Частные правила приложения

Действия на данной вкладке аналогичны действиям при задании общих настроек:

- прав доступа приложений к файловой системе [72];
- прав доступа приложений к системному реестру [78];
- правил сетевой активности приложений [88];
- привилегий процессов [93].

Отличие от общих правил контроля состоит в отсутствии необходимости выбирать область применяемости – частное правило действует только для выбранного приложения. Приоритет выполнения частных ограничений выше, чем у общих, – сначала проверяются ограничения приложения, затем общие ограничения. Чтобы посмотреть общие правила, действующие для зоны выполнения, в которой находится приложение, выберите области контроля **Файловая система (общие)**, **Системный реестр (общие)** или **Сеть (общие)**.

В поставку SoftControl SysWatch может входить стандартный набор частных ограничений, который создан специалистами компании в результате анализа действий данного приложения.

Для вступления изменений в силу нажмите на кнопку **OK** или **Применить**.

5.5.5 Белый список сертификатов

Чтобы включить контроль по белому списку сертификатов, выполните следующие действия:

1) Выберите пункт **Отслеживаемые приложения** контекстного меню [35] SoftControl SysWatch и в окне **Политика контроля** перейдите на вкладку **Сертификаты** (рис. Белый список сертификатов [70]).

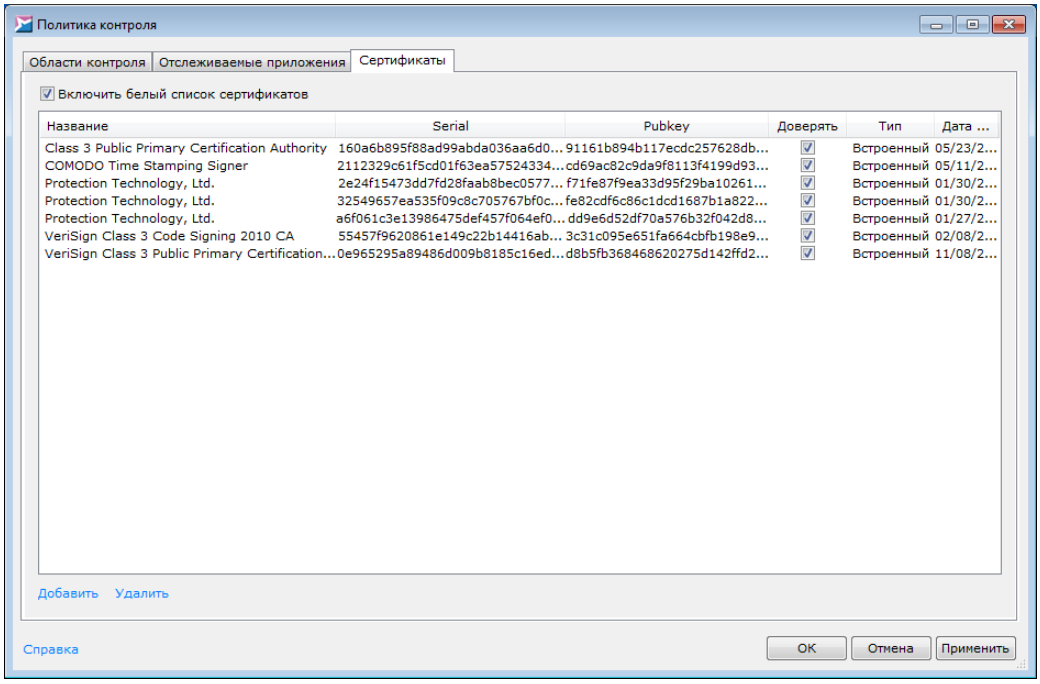

Рисунок 57. Белый список сертификатов

2) Установите флажок **Включить белый список сертификатов** для активации белого списка.
3) На вкладке **Сертификаты** приведен перечень сертификатов и их параметры. По умолчанию SoftControl SysWatch содержит базовый список сертификатов доверенных производителей, в том числе три сертификата Protection Technology, Ltd.

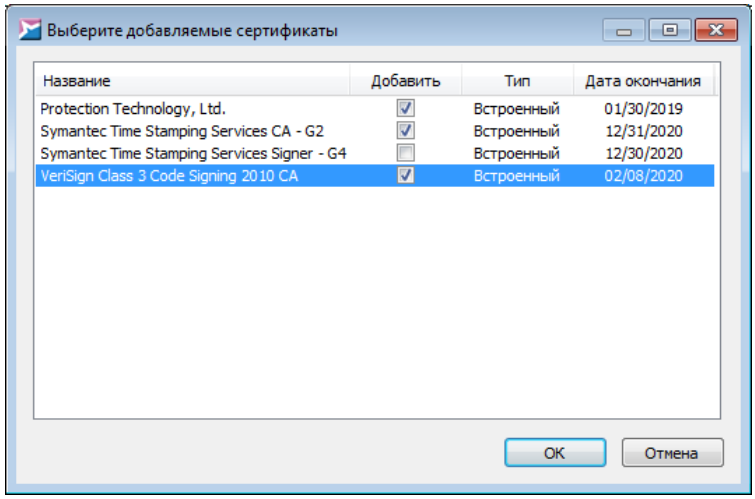

Рисунок 58. Выбор сертификатов для добавления

Чтобы добавить новый сертификат в список, нажмите на ссылку **Добавить** и укажите приложение, инсталлятор или скрипт, подписанные ЭЦП, сертификат которой требуется включить в перечень, после чего нажмите на кнопку **Открыть**. В

появившемся окне со списком сертификатов ЭЦП установите флажки в столбце **Добавить** для требуемых сертификатов и нажмите на кнопку **OK** (рис. Выбор сертификатов для добавления [71]).

4) Установите флажок в столбце **Доверять** для добавленных сертификатов (рис. Белый список сертификатов [70]).
5) Если необходимо исключить сертификат из перечня доверенных без его удаления, сбросьте флажок в столбце **Доверять**. Для полного удаления сертификата из списка выберите его и нажмите на ссылку **Удалить** (рис. Белый список сертификатов [70]).
6) Для вступления изменений в силу нажмите на кнопку **OK** или **Применить** (рис. Белый список сертификатов [70]).

Если приложение подписано несколькими ЭЦП, и в белом списке находится сертификат хотя бы одной из них, то запуск приложения разрешается. Данная возможность поддерживается для ОС, начиная с Windows 8.

5.5.6 Правила контроля активности

На вкладке **Статус** панели управления [36] программы отображается текущий статус защиты и список областей контроля. Политика контроля SoftControl SysWatch по доступу приложений к ресурсам системы активна, когда включены области **Файловая система**, **Системный реестр** и/или **Сеть**.

Ниже приведена детальная информация по настройке политики контроля:

- доступа к файловой системе [72];
- доступа к системному реестру [78];
- доступа к устройствам и портам [84];
- сетевой активности [88];
- привилегий процессов [93];
- взаимодействия процессов [96].

5.5.6.1 Настройка прав доступа к файловой системе

Область контроля **Файловая система** позволяет создавать правила доступа приложений к объектам файловой системы:

- Чтение файла или каталога;
- Запись в файл или каталог (создание/изменение файла или каталога);
- Удаление файла или каталога.

Для просмотра и изменения политики контроля файловой системы выберите пункт **Политика контроля** контекстного меню [35] SoftControl SysWatch; в окне **Политика контроля** на вкладке **Области контроля** выберите в выпадающем списке раздел **Файловая система** (рис. Политика контроля файловой системы [73]).

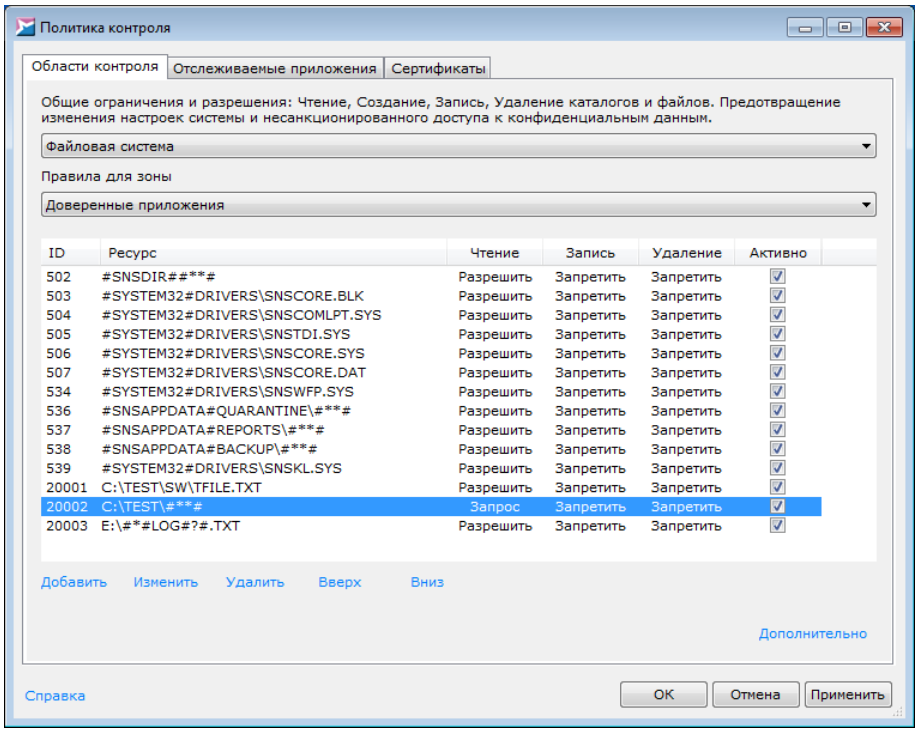

Рисунок 59. Политика контроля файловой системы

Правила разделены по спискам для приложений из следующих зон выполнения:

- **Доверенные приложения**;
- **Ограниченные приложения**.

Для переключения между списками выберите соответствующую категорию в выпадающем списке **Правила для зоны**.

Каждое правило представляет собой запись в линейном списке и имеет свой уникальный идентификатор **ID**. Объекты применения указываются в столбце **Ресурс**, права доступа к ним – в столбцах **Чтение**, **Запись** и **Удаление**. Включение и выключение правила управляется флажком в столбце **Активно**.

Если несколько правил имеют пересекающиеся области действия, то приоритет выполнения

в таком случае имеет правило, расположенное в списке наиболее низко. Положение правила в списке изменяется с помощью ссылок **Вверх** и **Вниз**.

Пример: правило с **ID** 20002, показанное на рис. Политика контроля файловой системы [73], перекрывает действие правила с **ID** 20001, т.к. расположено ниже его по списку.

Синтаксис правила

Строка в столбце **Ресурс** представляет собой путь до объекта или объектов применения правила. В данной строке могут использоваться маски – инструмент задания правил для группы объектов файловой системы. Например, с помощью масок можно создать правило для каталога и всех объектов внутри него или правило для определенных типов (расширений) файлов. Ниже приведен синтаксис масок:

#*# – заменяет любое количество символов, кроме символа '\' (в случае размещения в конце строки распространяется только на файлы корневой директории);

##** – заменяет любое количество символов (в случае размещения в конце строки распространяется на файлы корневой директории, поддиректории и файлы поддиректорий);

#?# – заменяет ровно 1 любой символ.

Пример: на рис. Политика контроля файловой системы [73] показано правило с **ID** 20003 (*E:\#*#log#?#.txt*), действующее на следующие объекты – текстовые файлы в корневой директории локального жесткого диска *E*, имеющие в своем имени последовательность букв *log*, любое количество произвольных символов до нее и один произвольный символ после нее.

Создание правила

Чтобы создать правило, нажмите на ссылку **Добавить**.

В окне **Ресурс файловой системы** нажмите на кнопку **...** для выбора объекта из проводника или вручную введите путь до него в поле **Файл или каталог** (рис. Создание правила для объекта файловой системы [75]). Обратите внимание, что система воспринимает пробелы в пути к ресурсу. Если в тексте правила стоит пробел, а в названии файла его нет – правило не будет работать. В заданных правилах пробелы отображаются в виде точки.

Вы можете указывать как папки на локальном жестком диске, так и сетевые папки. При создании правила для сетевых папок путь указывается в виде \\<*имя_сервера*> \<*имя_папки*>. Вместо символа '\\' можно использовать маску **#**#**; в этом случае будут проверяться и сетевые, и локальные папки. Кроме того, можно указывать IP-адрес компьютера с сетевой папкой.

Если в правиле указан IP-адрес компьютера, то правило будет действовать, только если пользователь при доступе к папке указывает IP-адрес, а не сетевой путь. Поэтому если необходимо контролировать доступ и по IP-адресу, и по сетевому пути, создайте два отдельных правила.

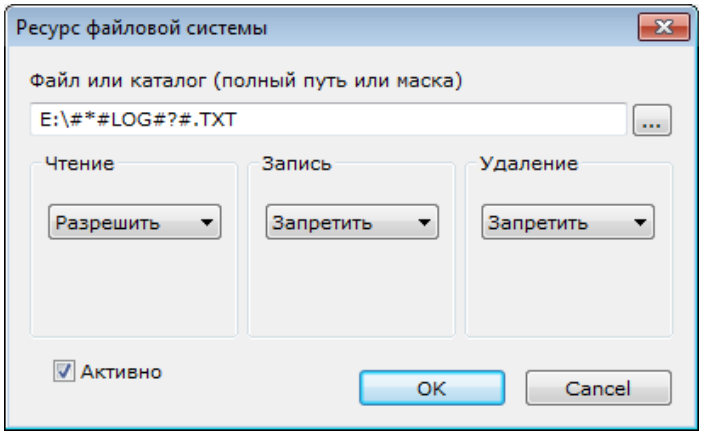

Рисунок 60. Создание правила для объекта файловой системы

При выборе каталога через проводник к нему автоматически добавляется маска[74] **#*#**, т.е. правило устанавливается для каталога и файлов внутри него.

В областях **Чтение**, **Запись** и **Удаление** выберите в выпадающих списках соответствующие права доступа к объекту:

- **Разрешить** – позволить приложению выполнять операцию над объектом;
- **Запретить** – заблокировать выполнение приложением операции над объектом;
- **Запрос** – выводить запрос при совпадении действия над объектом с условием правила.

Чтобы включить созданное правило в список и сделать его действующим, установите флажок **Активно** и нажмите на кнопку **OK**.

Изменение правила

Чтобы изменить правило, нажмите на ссылку **Изменить** и настройте параметры правила аналогично действиям при его создании 74.

Перемещение правила между зонами

Если требуется переместить правило в список для приложений из другой зоны выполнения, вызовите контекстное меню правила и выберите один из вариантов:

- **Для всех** – создать правило для обеих зон выполнения, если правило находится только в одном списке.
- **Ограниченные** – переместить правило в список правил для ограниченных приложений.
- **Доверенные** – переместить правило в список правил для доверенных приложений.

Дополнительные параметры правила и исключения

Выбрав команду **Дополнительно** (в контекстном меню или по одноименной ссылке в нижней части окна), в появившемся окне можно определить следующие дополнительные параметры правила:

- **Пользователи** – на данной вкладке выбираются учетные записи пользователей, группы пользователей или встроенные субъекты безопасности, на которые будет распространяться действие правила (рис. Выбор учетных записей пользователей 76). По умолчанию правила устанавливаются для всех пользователей.

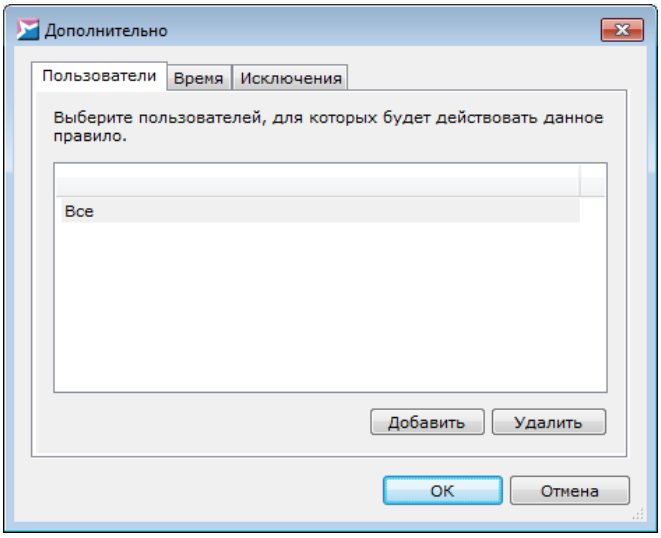

Рисунок 61. Выбор учётных записей пользователей

- **Время** – на данной вкладке задаются временные интервалы действия правила (рис. Выбор времени действия правила 77).

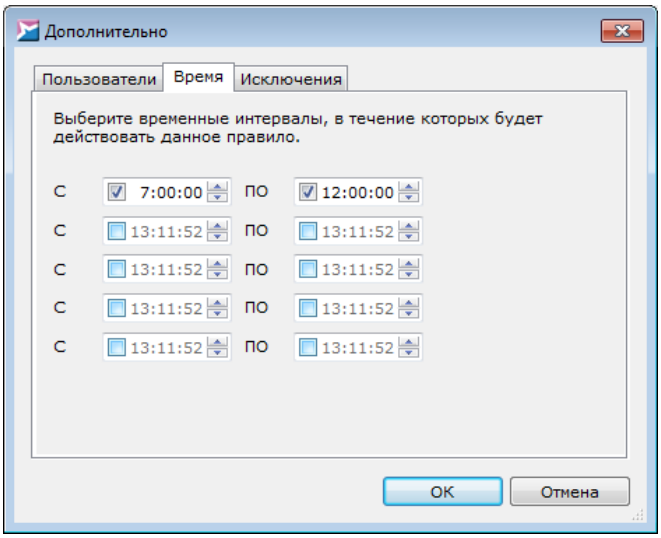

Рисунок 62. Выбор времени действия правила

Если требуется задать интервал, затрагивающий двое суток, необходимо разбить его на два интервала (один из которых заканчивается в 23:59:59, а другой начинается в 0:00:00).

- **Исключения** – на данной вкладке выбираются приложения, на которые не будет распространяться действие правила (рис. Выбор приложений для исключения из правила 77).

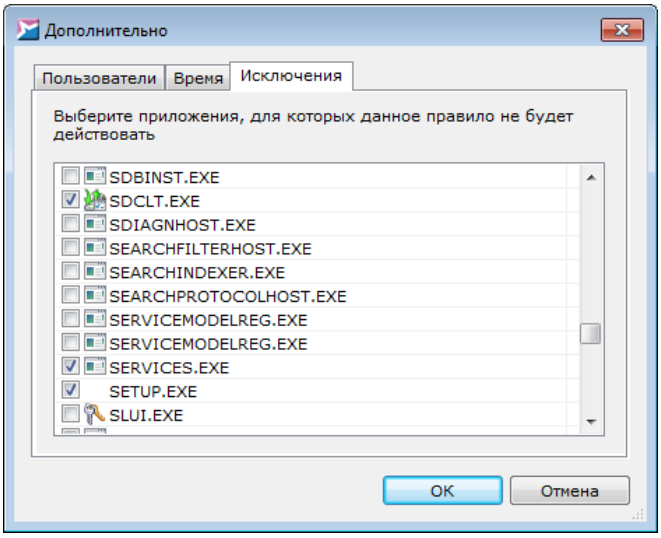

Рисунок 63. Выбор приложений для исключения из правила

Для приложений, выбранных в качестве исключений, создается частное правило, которое недоступно для редактирования на вкладке Ограничения и разрешения [69] в окне свойств приложения.

Нажмите на кнопку **OK**, чтобы сохранить указанные дополнительные параметры.

Удаление правила

Чтобы удалить правило, нажмите на ссылку **Удалить** и подтвердите удаление в диалоговом окне.

В SoftControl SysWatch содержатся предустановленные правила, распространяющиеся на системные каталоги и объекты расположения компонентов продукта. Изменение или удаление предустановленных правил может повлечь за собой нарушение защиты целостности системы.

Для вступления изменений в силу нажмите на кнопку **OK** или **Применить**.

5.5.6.2 Настройка прав доступа к системному реестру

Область контроля **Системный реестр** позволяет создавать правила доступа приложений к объектам системного реестра:

- Запись в ключ или параметр реестра (создание/изменение ключа или параметра);
- Удаление ключа или параметра реестра.

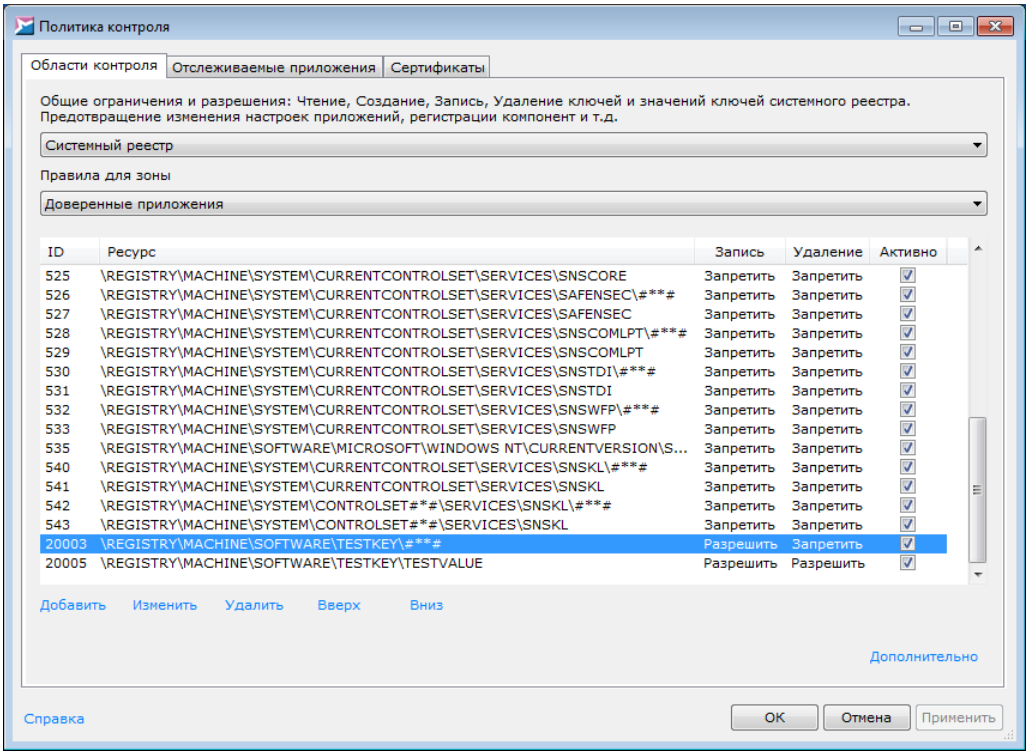

Рисунок 64. Политика контроля системного реестра

Для просмотра и изменения политики контроля системного реестра выберите пункт **Политика контроля** контекстного меню[35] SoftControl SysWatch, в окне **Политика контроля** на вкладке **Области контроля** выберите в выпадающем списке раздел **Системный реестр** (рис. Политика контроля системного реестра[78]).

Правила разделены по спискам для приложений из следующих зон выполнения:

- **Доверенные приложения**;
- **Ограниченные приложения**.

Для переключения между списками выберите соответствующую категорию в выпадающем списке **Правила для зоны**.

Каждое правило представляет собой запись в линейном списке и имеет свой уникальный идентификатор **ID**. Объекты применения указываются в столбце **Ресурс**, права доступа к ним – в столбцах **Запись** и **Удаление**. Включение и выключение правила управляется флажком в столбце **Активно**.

Если несколько правил имеют пересекающиеся области действия, то приоритет выполнения в таком случае имеет правило, расположенное в списке наиболее низко. Положение правила в списке изменяется с помощью ссылок **Вверх** и **Вниз**.

Пример: правило с **ID** 20005, показанное на рис. Политика контроля системного реестра[78], перекрывает действие правила с **ID** 20004, т.к. расположено ниже его по списку.

Синтаксис правила

Строка в столбце **Ресурс** представляет собой путь до объекта или объектов применения правила. В данной строке могут использоваться маски – инструмент задания правил для группы объектов системного реестра. Например, с помощью масок можно создать правило для раздела реестра и всех объектов внутри него.

Ниже приведен синтаксис масок:

#*# – заменяет любое количество символов, кроме символа '\' (в случае размещения в конце строки распространяется только на параметры раздела);

##** – заменяет любое количество символов (в случае размещения в конце строки распространяется на параметры раздела, подразделы и параметры подразделов);

#?# – заменяет ровно 1 любой символ.

Пример: на рис. Политика контроля системного реестра[78] показано правило с **ID** 20004 (*\REGISTRY\MACHINE\SOFTWARE\TESTKEY\#**#*), действующее на следующие объекты – раздел *TestKey*, все его параметры, подразделы и параметры подразделов.

Создание правила

Чтобы создать правило, нажмите на ссылку **Добавить**.

В окне **Ресурс системного реестра** выберите объект из проводника или вручную введите путь до него в реестре в поле под проводником (рис. Создание правила для объекта системного реестра[80]). Обратите внимание, что система воспринимает пробелы в пути к ресурсу. Если в тексте правила стоит пробел, а в названии файла его нет – правило не будет работать. В заданных правилах пробелы отображаются в виде точки.

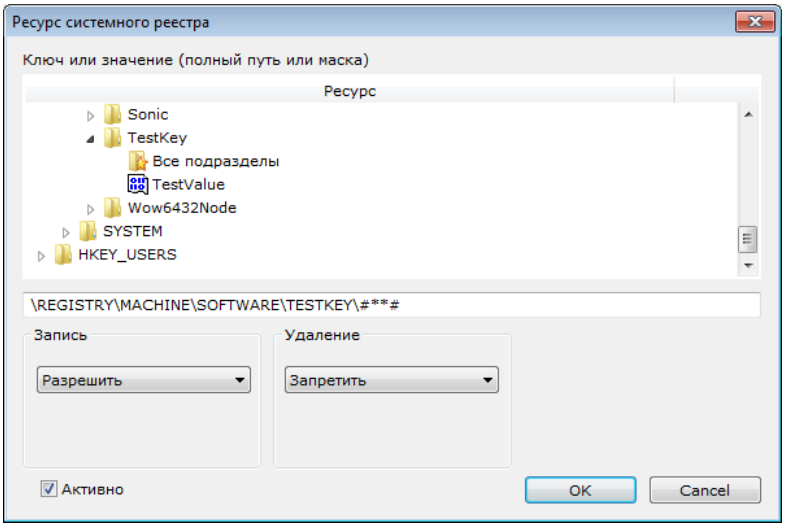

Рисунок 65. Создание правила для объекта системного реестра

В областях **Запись** и **Удаление** выберите в выпадающих списках соответствующие права доступа к объекту:

- **Разрешить** – позволить приложению выполнять операцию над объектом;
- **Запретить** – заблокировать выполнение приложением операции над объектом;
- **Запрос** – выводить запрос при совпадении действия над объектом с условием правила.

Чтобы включить созданное правило в список и сделать его действующим, установите флажок **Активно** и нажмите на кнопку **OK**.

Изменение правила

Чтобы изменить правило, нажмите на ссылку **Изменить** и настройте параметры правила аналогично действиям при его создании 80.

Перемещение правила между зонами

Если требуется переместить правило в список для приложений из другой зоны выполнения, вызовите контекстное меню правила и выберите один из вариантов:

- **Для всех** – создать правило для обеих зон выполнения, если правило находится только в одном списке.
- **Ограниченные** – переместить правило в список правил для ограниченных приложений.
- **Доверенные** – переместить правило в список правил для доверенных

приложений.

Дополнительные параметры правила и исключения

Выбрав команду **Дополнительно** (в контекстном меню или по одноименной ссылке в нижней части окна), в появившемся окне можно определить следующие дополнительные параметры правила:

- **Пользователи** – на данной вкладке выбираются учетные записи пользователей, группы пользователей или встроенные субъекты безопасности, на которые будет распространяться действие правила (рис. Выбор учетных записей пользователей 82). По умолчанию правила устанавливаются для всех пользователей.
- **Время** – на данной вкладке задаются временные интервалы действия правила (рис. Выбор времени действия правила 82).

Если требуется задать интервал, затрагивающий двое суток, необходимо разбить его на два интервала (один из которых заканчивается в 23:59:59, а другой начинается в 0:00:00).

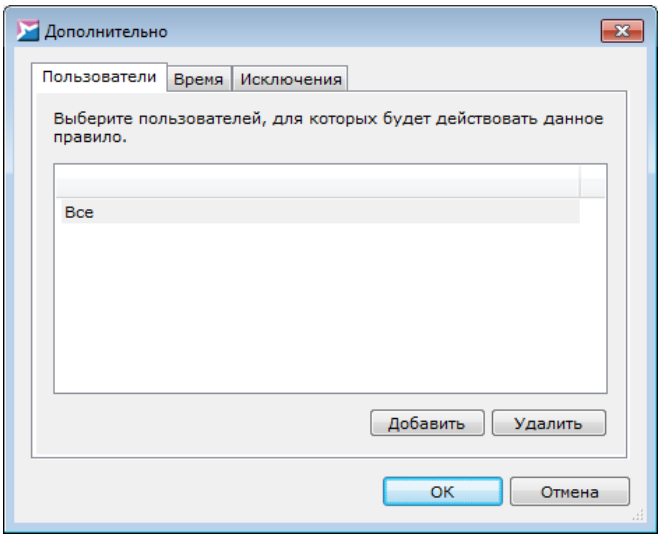

Рисунок 66. Выбор учётных записей пользователей

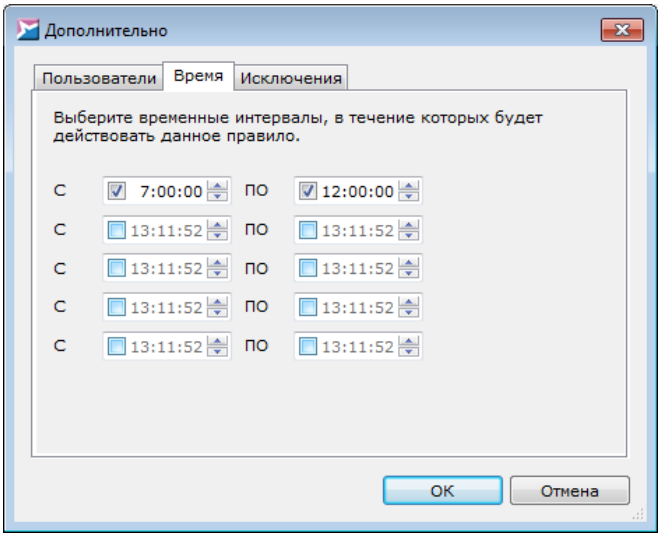

Рисунок 67. Выбор времени действия правила

- **Исключения** – на данной вкладке выбираются приложения, на которые не будет распространяться действие правила (рис. Выбор приложений для исключения из правила 83).

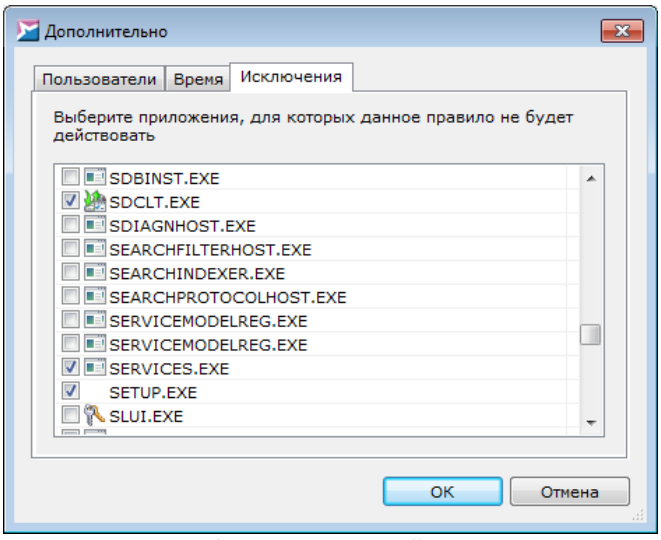

Рисунок 68. Выбор приложений для исключения из правила

Для приложений, выбранных в качестве исключений, создается частное правило, которое недоступно для редактирования на вкладке Ограничения и разрешения 69 в окне свойств приложения.

Нажмите на кнопку **OK**, чтобы сохранить указанные дополнительные параметры.

Удаление правила

Чтобы удалить правило, нажмите на ссылку **Удалить** и подтвердите удаление в диалоговом окне.

В SoftControl SysWatch содержатся предустановленные правила, распространяющиеся на ключи и параметры реестра, влияющие на работу системы и компонентов продукта. Изменение или удаление предустановленных правил может повлечь за собой нарушение защиты целостности системы.

Для вступления изменений в силу нажмите на кнопку **OK** или **Применить**.

5.5.6.3 Настройка прав доступа к устройствам и портам

Область контроля **Устройства** позволяет создавать правила использования следующих внешних устройств и портов системы:

- USB-устройства;
- CD/DVD-устройства;
- LPT-порты;
- COM-порты.

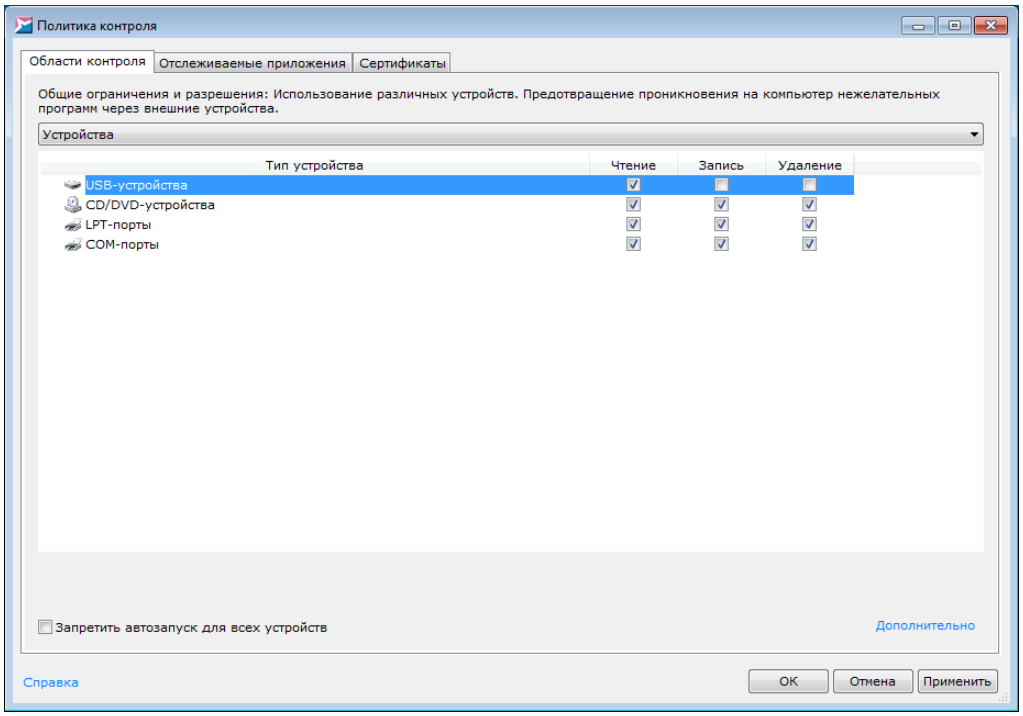

Рисунок 69. Политика контроля устройств и портов

Для просмотра и изменения политики контроля устройств выберите пункт **Политика**

контроля контекстного меню[35] SoftControl SysWatch, в окне **Политика контроля** на вкладке **Области контроля** выберите в выпадающем списке раздел **Устройства** (рис. Политика контроля устройств и портов[84]).

Настройка прав доступа к USB-устройствам

Чтобы определить права доступа к USB-устройствам, задайте права соответствующими флажками в столбцах **Чтение**, **Запись** и **Удаление** для типа **USB-устройства**.

Выбрав команду **Дополнительно** (в контекстном меню или по одноименной ссылке в нижней части окна), в появившемся окне можно определить следующие дополнительные параметры правила:

- **Пользователи** – на данной вкладке выбираются учетные записи пользователей, группы пользователей или встроенные субъекты безопасности, на которые будет распространяться действие ограничений (рис. Выбор учетных записей пользователей[85]).

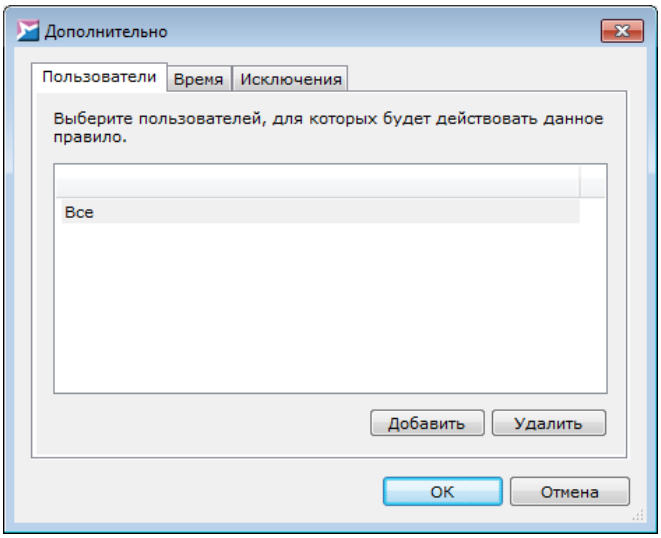

Рисунок 70. Выбор учётных записей пользователей

- **Время** – на данной вкладке задаются временные интервалы действия ограничений (рис. Выбор времени действия правила[85]).

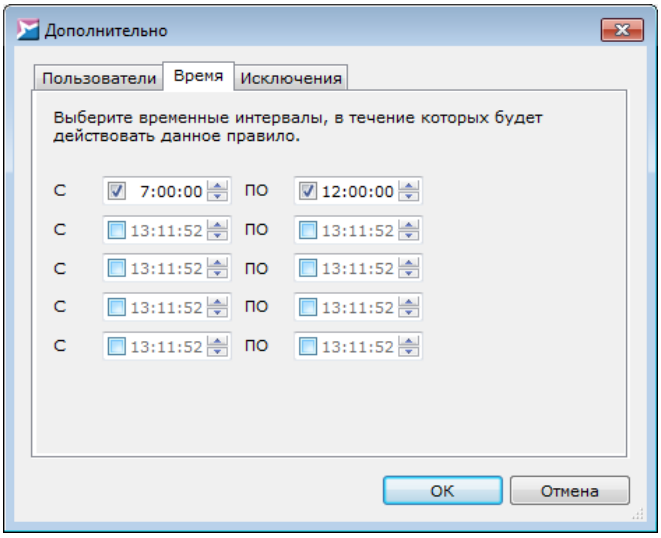

Рисунок 71. Выбор времени действия правила

Если требуется задать интервал, затрагивающий двое суток, необходимо разбить его на два интервала (один из которых заканчивается в 23:59:59, а другой начинается в 0:00:00).

- **Исключения** – на данной вкладке задаются отдельные устройства, на которые не будет распространяться действие общих ограничений (рис. Выбор USB-устройств для исключения из правил 86).

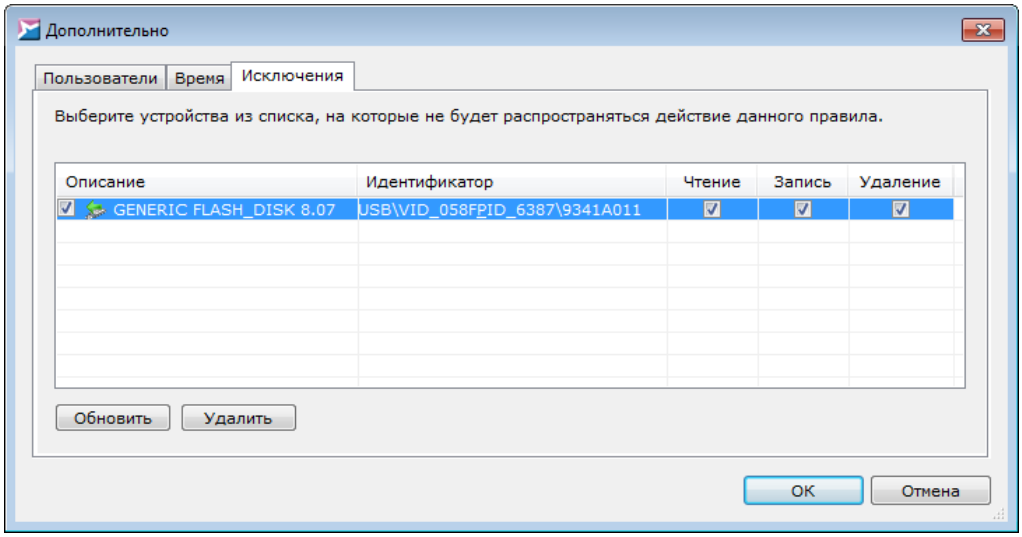

Рисунок 72. Выбор USB-устройств для исключения из правил

В "белом списке" USB-устройств можно задать частные ограничения для каждого накопителя из списка аналогично общим ограничениям. Чтобы активировать включение USB-устройства в "белый список", установите флажок у имени данного накопителя в столбце **Описание**. Чтобы обновить список подключенных USB-

накопителей, нажмите на кнопку **Обновить**. Для удаления накопителя из списка выберите его и нажмите на кнопку **Удалить**.

Нажмите на кнопку **OK**, чтобы сохранить указанные дополнительные параметры.

Запрещение доступа к CD/DVD-накопителям

Чтобы заблокировать доступ к CD/DVD-накопителям, устанавливаемым в оптический привод защищаемого объекта, сбросьте любой из флажков в столбцах **Чтение**, **Запись** или **Удаление** для типа **CD/DVD-устройства** (при этом будут сброшены все флажки для данного типа).

Запрещение автозапуска для всех устройств

Чтобы заблокировать автозапуск для USB- и CD/DVD-устройств, установите флажок **Запретить автозапуск для всех устройств**.

Запрещение доступа к LPT-портам

Чтобы заблокировать доступ к LPT-портам защищаемого объекта, сбросьте любой из флажков в столбцах **Чтение**, **Запись** или **Удаление** для типа **LPT-порты** (при этом будут сброшены все флажки для данного типа).

Для изменения прав доступа дополнительно необходима перезагрузка системы.

Запрещение доступа к COM-портам

Чтобы заблокировать доступ к COM-портам защищаемого объекта, сбросьте любой из флажков в столбцах **Чтение**, **Запись** или **Удаление** для типа **COM-порты** (при этом будут сброшены все флажки для данного типа).

Для изменения прав доступа дополнительно необходима перезагрузка системы.

Для вступления изменений в силу нажмите на кнопку **OK** или **Применить**.

5.5.6.4 Настройка правил сетевой активности

Область контроля **Сеть** позволяет создавать правила контроля сетевой активности приложений:

- Прием данных;
- Передача данных.

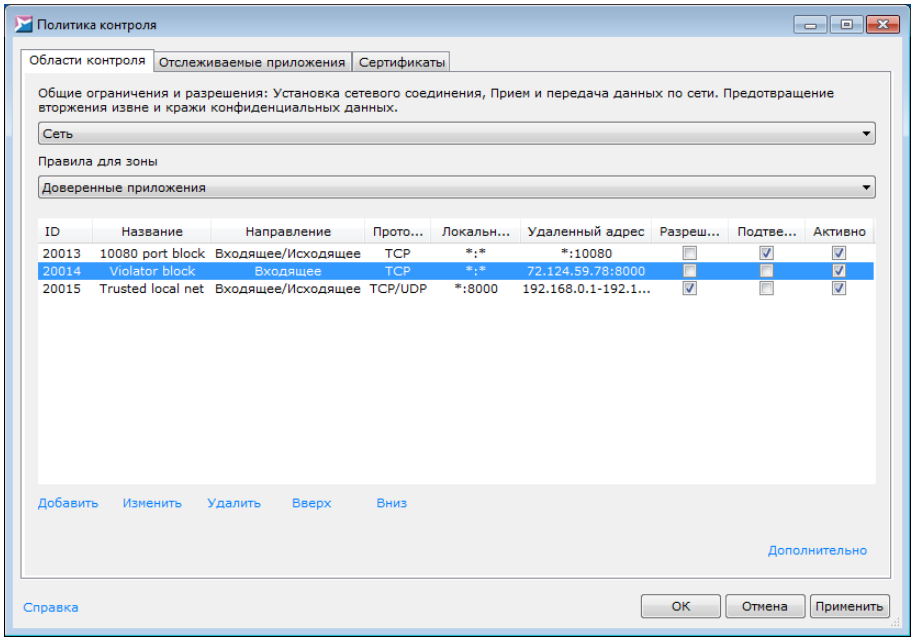

Рисунок 73. Политика контроля сетевой активности

Для просмотра и изменения политики контроля сетевой активности выберите пункт **Политика контроля** контекстного меню[35] SoftControl SysWatch, в окне **Политика контроля** на вкладке **Области контроля** выберите в выпадающем списке раздел **Сеть** (рис. Политика контроля сетевой активности[88]).

Правила разделены по спискам для приложений из следующих зон выполнения:

- **Доверенные приложения**;
- **Ограниченные приложения**.

Для переключения между списками выберите соответствующую категорию в выпадающем списке **Правила для зоны**.

Каждое правило представляет собой запись в линейном списке и имеет свой уникальный идентификатор **ID**. Параметры сетевого соединения указаны в следующих столбцах:

- **Название** – наименование правила, задаваемое пользователем.

- **Направление** – направление сетевой активности, определяющее инициатора соединения:
  - **Входящее** – сетевое соединение, инициируемое удаленным хостом;
  - **Исходящее** – сетевое соединение, инициируемое локальным хостом;
  - **Входящее/Исходящее** – любое из направлений.
- **Протокол** – тип протокола передачи данных по сети:
  - **TCP**;
  - **UDP**;
  - **TCP/UDP** – любой из протоколов.
- **Локальный адрес** – IP-адрес или диапазон IP-адресов локального хоста, участвующих в передаче данных. Если при создании правила[89] для него выбрана опция **Любой адрес**, отображается символ * до знака двоеточия, если выбрана опция **Любой порт** – символ * после знака двоеточия.
- **Удаленный адрес** – IP-адрес или диапазон IP-адресов удаленного хоста, участвующих в передаче данных. Если при создании правила[89] для него выбрана опция **Любой адрес**, отображается символ * до знака двоеточия, если выбрана опция **Любой порт** – символ * после знака двоеточия.

Разрешение или запрет сетевого соединения с указанными параметрами управляется флажком в столбце **Разрешить**. Если предполагается обработка событий сетевой активности приложений пользователем[90], установите флажок **Подтверждать** у требуемого правила. Включение и выключение правила управляется флажком в столбце **Активно**.

Если несколько правил имеют пересекающиеся области действия, то приоритет выполнения в таком случае имеет правило, расположенное в списке наиболее низко. Положение правила в списке изменяется с помощью ссылок **Вверх** и **Вниз**.

Создание правила

Чтобы создать правило, нажмите на ссылку **Добавить**. В окне **Сетевой ресурс** выберите необходимые параметры сетевого соединения (рис. Создание правила контроля сетевой активности[89]).

Чтобы включить созданное правило в список, нажмите на кнопку **OK**.

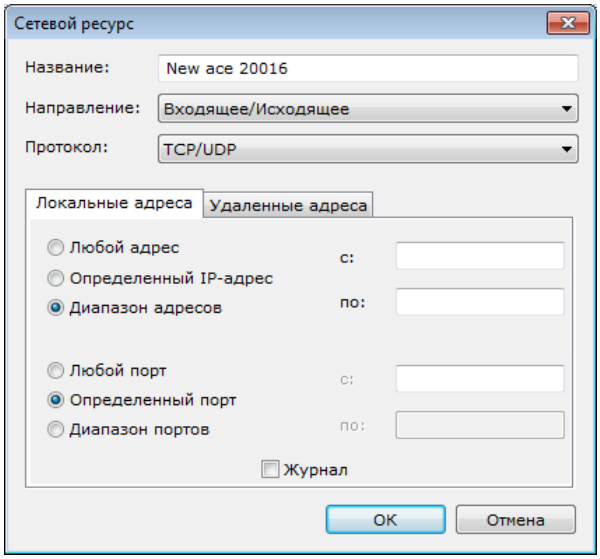

Рисунок 74. Создание правила контроля сетевой активности

Ручная обработка событий сетевой активности

Условие: для включения данной возможности должен быть активирован ручной режим обработки инцидентов, для этого откройте раздел **Защита** настроек программы, установите переключатель **Управление инцидентами** в положение **Включить обработку инцидентов пользователем** и нажмите на кнопку **OK**.

Окно предупреждения, отображаемое SoftControl SysWatch при совпадении параметров сетевого соединения с правилом контроля сетевой активности, показано на рис. ниже 90.

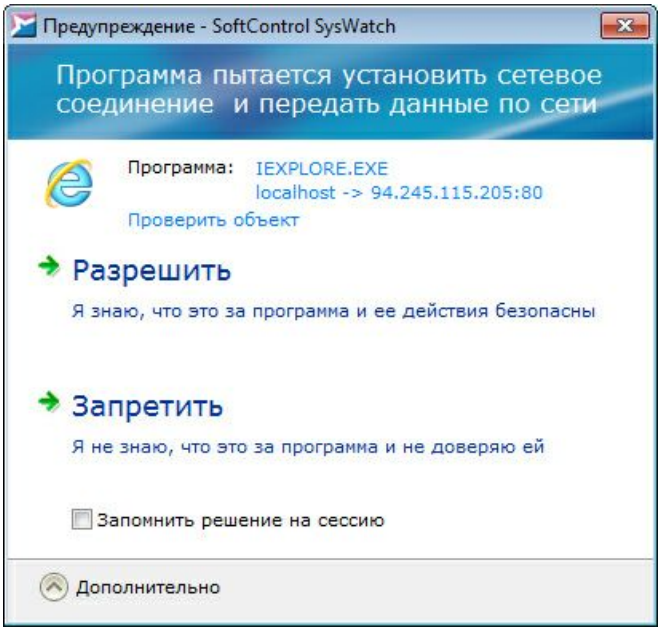

Рисунок 75. Окно предупреждения для сетевой активности

Окно **Предупреждение - SoftControl SysWatch** состоит из 2 частей:

- Область описания сетевой активности. В данном блоке приводится информация об устанавливаемом сетевом соединении: имя приложения, осуществляющего активность, конечные узлы установления соединения и направление соединения, результат антивирусной проверки[98] (можно проверить приложение перед принятием решения, при наличии антивирусного сканера и соответствующей лицензии[45] программы, нажав на ссылку **Проверить объект** и выбрав в контекстном меню вариант **Запустить проверку**).
- Область выбора действия. В блоке выбора действия отображаются возможные действия при попытке установления приложением сетевого соединения:
  - → **Разрешить** – позволить приложению установить сетевое соединение;
  - → **Запретить** – заблокировать сетевую активность приложения;
  - ❑ **Запомнить решение на сессию** – принятое решение будет применено к данному правилу до окончания текущей сессии.

Если в течение 5 минут действие не будет выбрано, SoftControl SysWatch заблокирует сетевую активность и закроет окно предупреждения.

Изменение правила

Чтобы изменить правило, нажмите на ссылку **Изменить** и настройте параметры правила аналогично действиям при его создании[89].

Перемещение правила между зонами

Если требуется переместить правило в список для приложений из другой зоны выполнения, вызовите контекстное меню правила и выберите один из вариантов:

- **Для всех** – создать правило для обеих зон выполнения, если правило находится только в одном списке.
- **Ограниченные** – переместить правило в список правил для ограниченных приложений.
- **Доверенные** – переместить правило в список правил для доверенных приложений.

Дополнительные параметры правила

Выбрав команду **Дополнительно** (в контекстном меню или по одноименной ссылке в нижней части окна), в появившемся окне можно определить следующие дополнительные параметры правила:

- **Пользователи** – на данной вкладке выбираются учетные записи пользователей, группы пользователей или встроенные субъекты безопасности, на которые будет распространяться действие правила (рис. Выбор учетных записей пользователей 92). По умолчанию правила устанавливаются для всех пользователей.

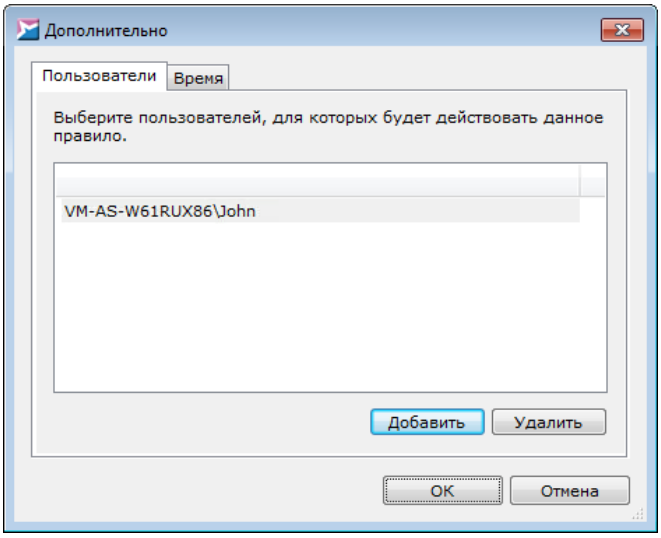

Рисунок 76. Выбор учётных записей пользователей

- **Время** – на данной вкладке задаются временные интервалы действия правила (рис. Выбор времени действия правила 92).

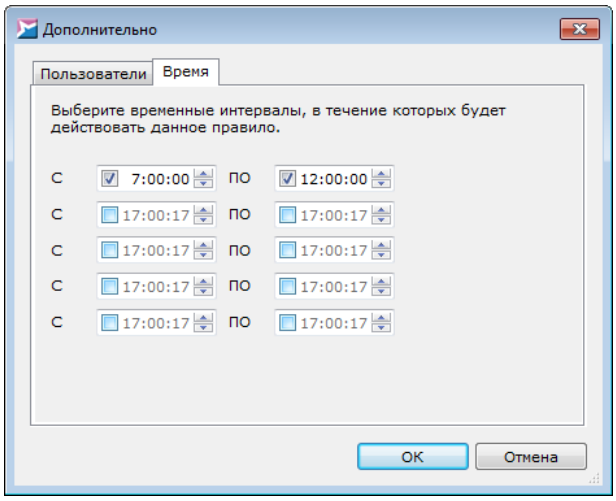

Рисунок 77. Выбор времени действия правила

Если требуется задать интервал, затрагивающий двое суток, необходимо разбить его на два интервала (один из которых заканчивается в 23:59:59, а другой начинается в 0:00:00).

Нажмите на кнопку **OK**, чтобы сохранить указанные дополнительные параметры.

Удаление правила

Чтобы удалить правило, нажмите на ссылку **Удалить** и подтвердите удаление в диалоговом окне.

Для вступления изменений в силу нажмите на кнопку **OK** или **Применить**.

5.5.6.5 Настройка привилегий процессов

Область контроля **Привилегии процессов** позволяет ограничивать использование процессами привилегий Windows:

- Управление аудитом и журналом безопасности;
- Архивация файлов и каталогов;
- Восстановление файлов и каталогов;
- Изменение системного времени;
- Завершение работы системы;
- Принудительное удаленное завершение работы;
- Смена владельцев файлов и других объектов;
- Отладка программ;
- Изменение параметров среды изготовителя;
- Профилирование производительности системы;
- Профилирование одного процесса;
- Увеличение приоритета выполнения;
- Загрузка и выгрузка драйверов устройств;
- Создание файла подкачки;
- Настройка квот памяти для процесса;
- Обход перекрестной проверки;
- Отключение компьютера от стыковочного узла;
- Выполнение задач по обслуживанию томов;

- Имитация клиента после проверки пользователя;
- Создание глобальных объектов.

Условие: правила распространяются на все приложения из ограниченной зоны.

Для просмотра и изменения привилегий процессов выберите пункт **Политика контроля** контекстного меню[35] SoftControl SysWatch, в окне **Политика контроля** на вкладке **Области контроля** выберите в выпадающем списке раздел **Привилегии процессов** (рис. Политика контроля привилегий процессов[94]). Описание привилегий и области их применения представлено в разделе Дополнительная информация[138].

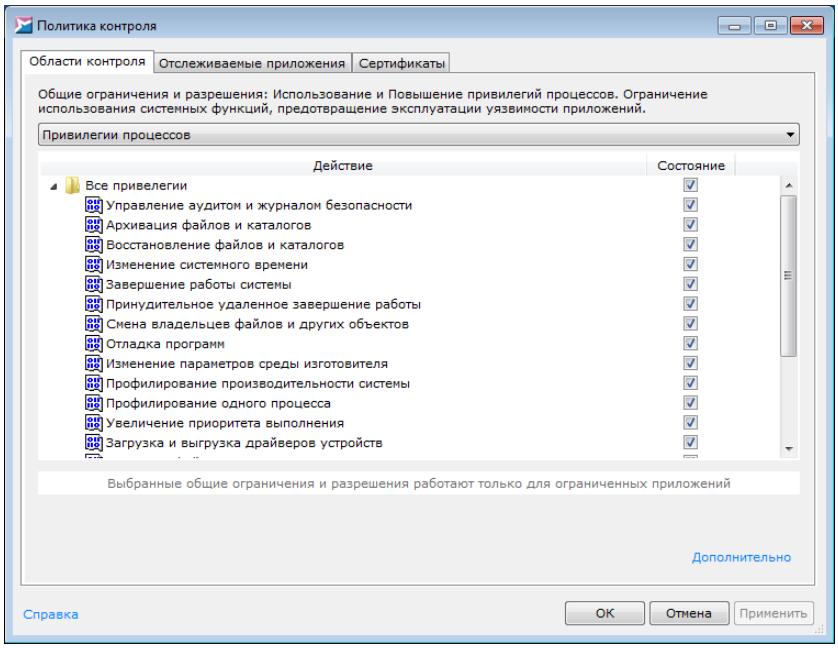

Рисунок 78. Политика контроля привилегий процессов

Создание правила

По умолчанию, приложения (процессы) обладают всеми вышеуказанными привилегиями, но при этом могут быть ограничены ОС. Чтобы ограничить привилегии вручную, сбросьте флажки у требуемых привилегий в столбце **Состояние**.

Дополнительные параметры правила

Выбрав команду **Дополнительно** (в контекстном меню или по одноименной ссылке в нижней части окна), в появившемся окне можно определить следующие дополнительные параметры правила:

- **Пользователи** – на данной вкладке выбираются учетные записи пользователей, группы пользователей или встроенные субъекты безопасности, на которые будет

распространяться действие правила (рис. Выбор учетных записей пользователей 95). По умолчанию правила устанавливаются для всех пользователей.

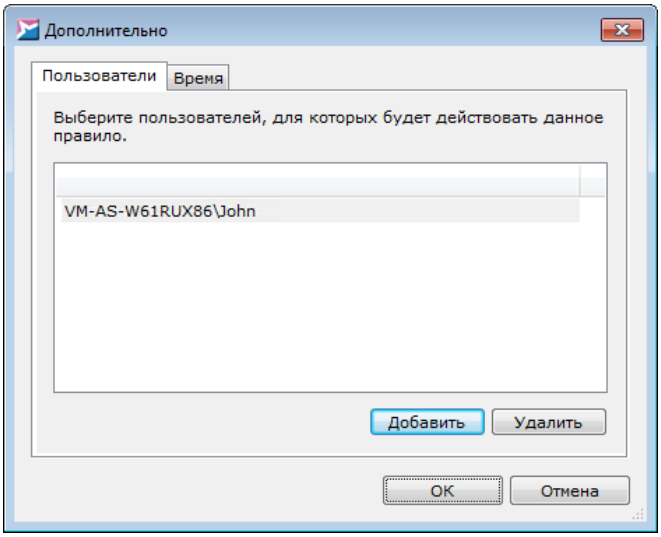

Рисунок 79. Выбор учётных записей пользователей

- **Время** – на данной вкладке задаются временные интервалы действия правила (рис. Выбор времени действия правила 95).

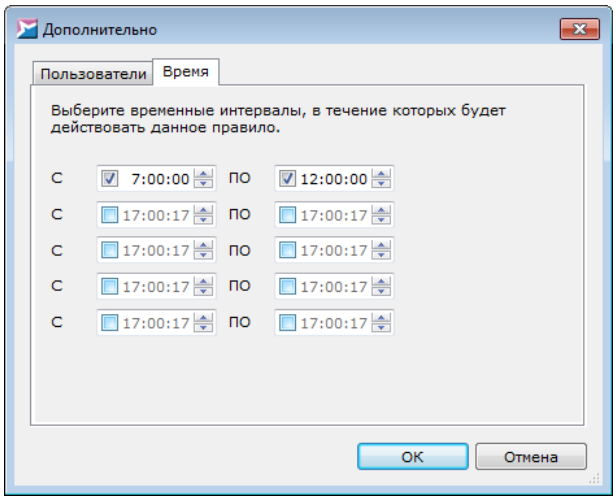

Рисунок 80. Выбор времени действия правила

Если требуется задать интервал, затрагивающий двое суток, необходимо разбить его на два интервала (один из которых заканчивается в 23:59:59, а другой начинается в 0:00:00).

Нажмите на кнопку **OK**, чтобы сохранить указанные дополнительные параметры.

Для вступления изменений в силу нажмите на кнопку **OK** или **Применить**.

5.5.6.6 Настройка взаимодействия процессов

Область контроля **Взаимодействие процессов** позволяет задавать следующие разрешения для взаимодействия процессов:

- Доступ приложения к буферу обмена;
- Установка приложением глобальных перехватчиков;
- Доступ к процессу и его потокам извне.

Условие: правила распространяются на приложения из ограниченной зоны, запущенные под учетной записью пользователя «V.I.P.O.».

Для просмотра и изменения настроек взаимодействия процессов выберите пункт **Политика контроля** контекстного меню [35] SoftControl SysWatch, в окне **Политика контроля** на вкладке **Области контроля** выберите в выпадающем списке раздел **Взаимодействие процессов** (рис. Политика контроля взаимодействия процессов [96]).

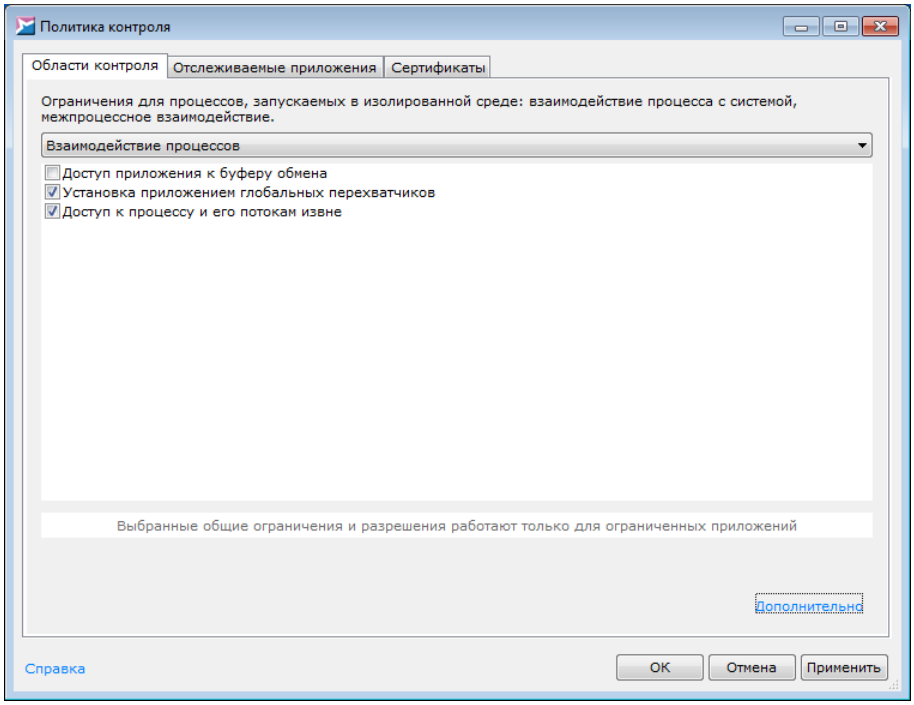

Рисунок 81. Политика контроля взаимодействия процессов

Создание правила

По умолчанию, приложения из ограниченной зоны выполнения, запущенные под учетной записью пользователя «V.I.P.O.», не имеют прав на выполнение

вышеуказанных операций. Для разрешения выполнять какое-либо из данных межпроцессных взаимодействий установите необходимые флажки.

Дополнительные параметры правила

Выбрав команду **Дополнительно** (в контекстном меню или по одноименной ссылке в нижней части окна), в появившемся окне можно определить следующие дополнительные параметры правила:

- **Пользователи** – на данной вкладке выбираются учетные записи пользователей, группы пользователей или встроенные субъекты безопасности, на которые будет распространяться действие правила (рис. Выбор учетных записей пользователей 97). По умолчанию правила устанавливаются для всех пользователей.

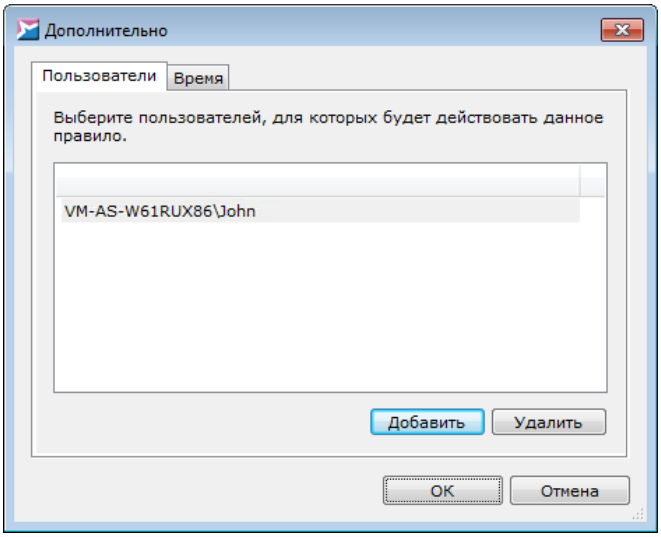

Рисунок 82. Выбор учётных записей пользователей

- **Время** – на данной вкладке задаются временные интервалы действия правила (рис. Выбор времени действия правила 97).

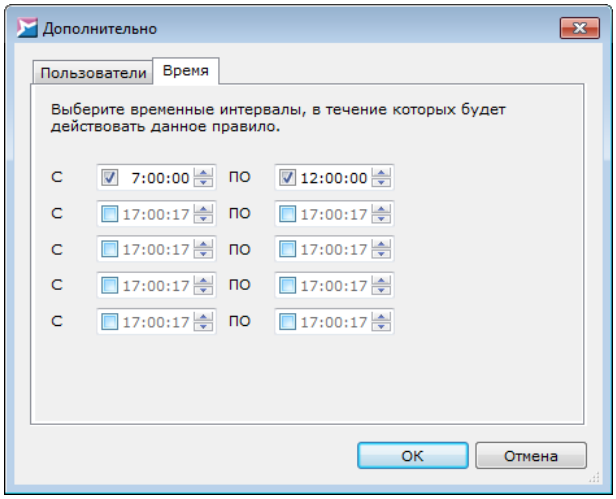

Рисунок 83. Выбор времени действия правила

Если требуется задать интервал, затрагивающий двое суток, необходимо разбить его на два интервала (один из которых заканчивается в 23:59:59, а другой начинается в 0:00:00).

Нажмите на кнопку **OK**, чтобы сохранить указанные дополнительные параметры.

Для вступления изменений в силу нажмите на кнопку **OK** или **Применить**.

5.6 Антивирусное сканирование

SoftControl SysWatch сочетает в себе преимущества как превентивных технологий, так и реактивных (сигнатурных) технологий защиты. Метод проактивной защиты основан на контроле активности приложений [52]. Метод сигнатурной защиты в SoftControl SysWatch реализован в виде антивирусного сканера, использующего базу вирусных сигнатур (наличие зависит от соответсвующей лицензии [45] программы).

Система может быть заражена вредоносным ПО до установки SoftControl SysWatch. Полная антивирусная проверка выполняется в процессе автоматической настройки [46] по умолчанию. В противном случае, рекомендуется провести проверку системы до установки SoftControl SysWatch, воспользовавшись сторонним антивирусным сканером.

В процессе антивирусного сканирования SoftControl SysWatch производит поиск вредоносного кода с использованием:

- антивирусных баз – поиск известных вирусов, троянских программ и других вредоносных объектов;

- баз программ-шпионов – поиск известных программ-шпионов.

Для эффективного поиска вредоносного кода необходимо периодически обновлять антивирусные базы. Рекомендуется настроить ежедневное автоматическое обновление[122]. Для предотвращения несанкционированного запуска приложений обновления не требуются.

Для выполнения проверки необходимо:

1) Произвести настройку параметров проверки[99].
2) Определить объекты в области проверки[103]; к ним относятся как объекты файловой системы (логические диски, файлы), так и объекты других типов (системная память, загрузочные сектора и т.д.). По умолчанию выбраны все объекты области проверки.
3) Осуществить запуск проверки[103].
4) По результатам проверки[105] принять решение об обнаруженных угрозах, если они не были обезврежены.

Рекомендуется выполнять проверку:

- Сразу после установки программы, если в системе не установлено другое антивирусное ПО.
- Каждый раз, когда контроль активности приложений[52] выключен, а в процессе работы были использованы внешние носители данных (USB, CD, DVD и т.д.) или подключение к сети Интернет.

5.6.1 Опции проверки

Перед началом антивирусного сканирования необходимо произвести настройку его параметров. Для этого откройте раздел **Проверка** настроек программы (рис. Настройки параметров проверки[99]).

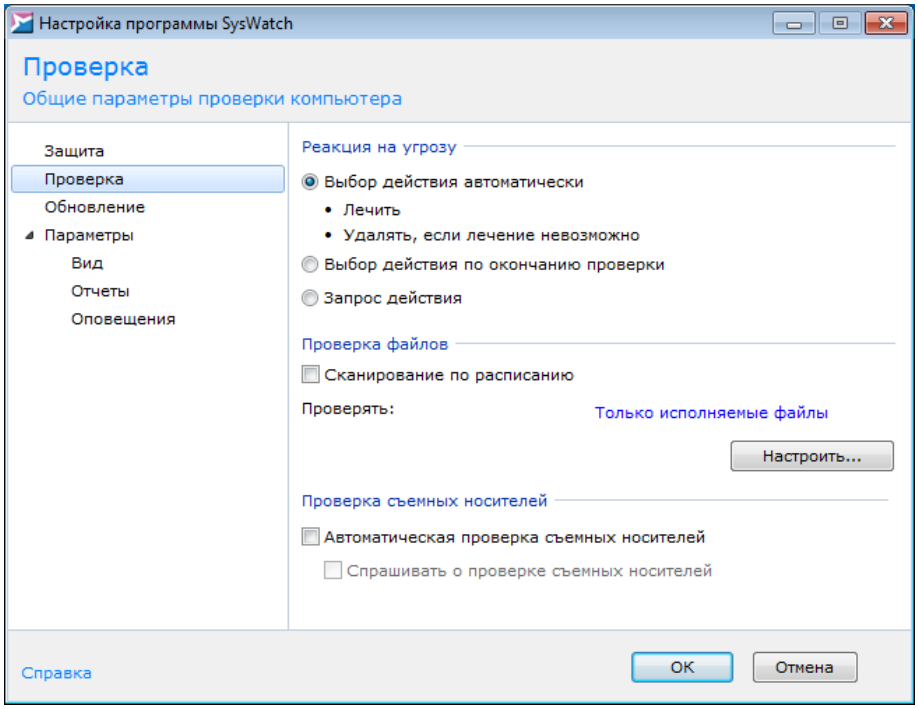

Рисунок 84. Настройки параметров проверки

Настройка реакции на угрозу

В области **Реакция на угрозу** возможны следующие варианты действий при обнаружении угроз в процессе антивирусного сканирования:

- **Выбор действия автоматически**:
  - **Лечить**

    Обезвредить инфицированный объект.
  - **Удалять, если лечение невозможно**

    Удалить инфицированный объект, если обезвредить его не удается.
- **Выбор действия по окончанию проверки**

  Запрос действия будет выведен пользователю по всем обнаруженным угрозам по завершению проверки.
- **Запрос действия**

  Запрос действия будет выведен пользователю при обнаружении каждой угрозы.

Настройка категорий файлов для проверки и режима запуска

В области **Проверка файлов** отображаются категории файлов, которые анализируются антивирусным сканером, и включается **Сканирование по расписанию**. Нажмите на кнопку **Настроить** для изменения параметров.

В окне **Дополнительные настройки** на вкладке **Область действия** возможны следующие варианты выбора (рис. Настройки области действия проверки 101):

- **Все файлы**

  Сканирование всех типов файлов, за исключением не отмеченных в области **Проверка составных файлов** (флажки **Почтовые базы** и **Архивы**).

- **Только исполняемые файлы**

  Сканирование только файлов формата PE (**.exe, *.com* и т.д.).

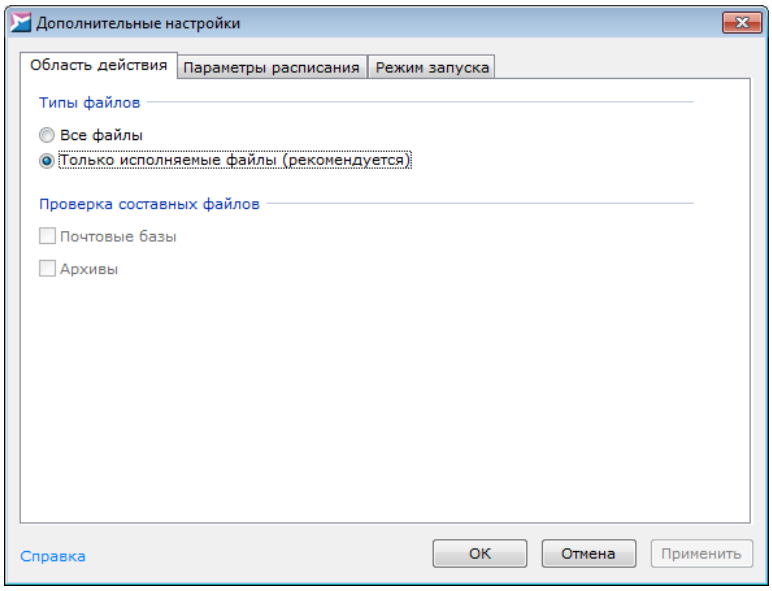

Рисунок 85. Настройки области действия проверки

На вкладке **Режим запуска** выберите учетную запись, под которой будет производиться сканирование (рис. Дополнительные настройки проверки 101):

- **С системной учетной записью**;
- **С учетной записью:** укажите учетные данные.

Установите флажок **Предварительная инициализация сканера**, если требуется инициализация антивирусного движка при каждом запуске сканирования.

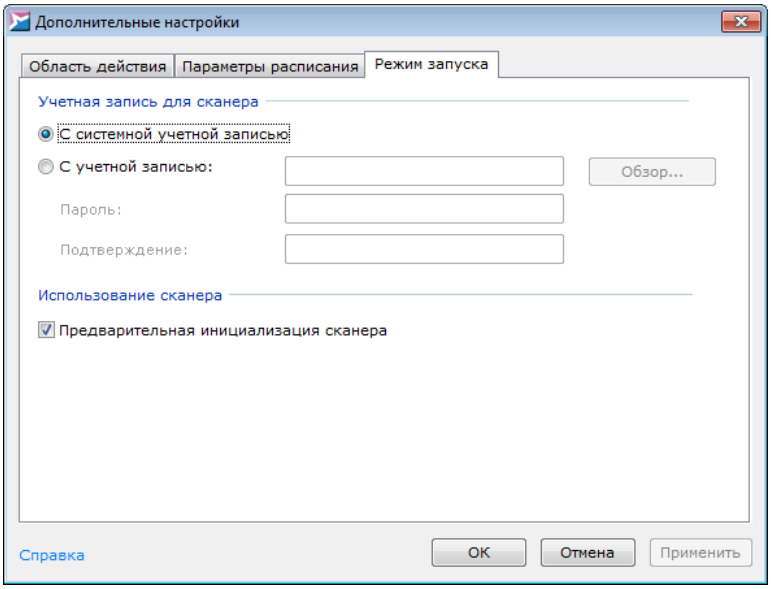

Рисунок 86. Дополнительные настройки проверки

Для применения настроек нажмите на кнопку **OK** или **Применить**.

Настройка сканирования по расписанию

Условие: только для случая работы SoftControl SysWatch в режиме удаленного управления с сервера [43].

Для настройки параметров антивирусного сканирования по расписанию нажмите на кнопку **Настроить** в области **Проверка файлов**.

В окне **Дополнительные настройки** откройте вкладку **Параметры расписания** и в счетчике **Частота дней** укажите периодичность, с которой будет выполняться задача, а в поле **Время запуска** – время начала выполнения задачи в формате *чч:мм:сс* (рис. Настройки параметров проверки по расписанию [102]).

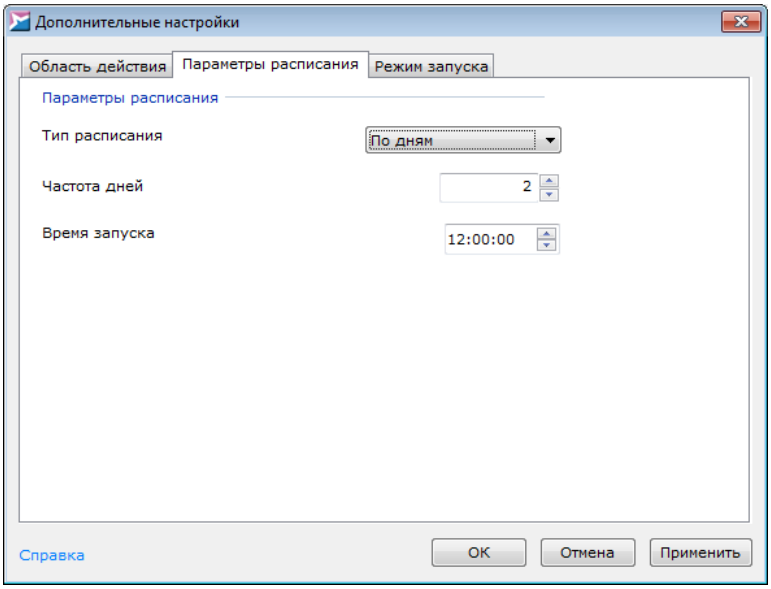

Рисунок 87. Настройки параметров проверки по расписанию

Настройка автоматического сканирования съёмных носителей

В области **Проверка съемных носителей** установите флажок **Автоматическая проверка съемных носителей**, если необходимо автоматически запускать антивирусное сканирование USB-носителей после их подключения. Установите флажок **Спрашивать о проверке съемных носителей**, если требуется появление диалогового окна с предложением проверки.

Для вступления изменений в силу нажмите на кнопку **OK**.

5.6.2 Запуск по требованию

Выбор области проверки и ее запуск производятся с вкладки **Проверка** панели управления [36] SoftControl SysWatch.

Иерархический список объектов для проверки содержит следующие элементы:

- **Системная память** – проверка всех загруженных в памяти процессов.

Рекомендуется выполнять проверку системной памяти каждый раз в случае, если в системе появились неотслеживаемые приложения, запущенные без ведома пользователя.

- **Загрузочные сектора** – проверка загрузочных секторов дисков.
- **Объекты на карантине** – проверка объектов, перенесенных на карантин.

Рекомендуется выполнять повторную проверку объектов на карантине после обновления [122] антивирусных баз программы.

- **Все съемные диски** – проверка файловых объектов на всех съемных дисках.

Рекомендуется выполнять проверку съемных носителей всякий раз, когда предполагается перемещать информацию на компьютер или выполнять приложения со съемного носителя.

- **Все жесткие диски** – проверка файловых объектов на всех жестких дисках.
- **Мой компьютер** – проверка объектов файловой системы на жестких дисках и внешних носителях в дисководах и портах компьютера.
- **Корзина** – проверка файловых объектов, помещенных в корзину.
- **Мои документы** – проверка документов пользователя.
- **Рабочий стол** – проверка всех доступных объектов.

Запуск проверки по требованию

Установите флажки у требуемых объектов и нажмите на кнопку **Запустить проверку** для начала процесса сканирования.

В строке **Последняя проверка** указаны дата и время последней проведенной проверки. В строке **Реакция на угрозу** отображается соответствующая настройка [99] .

При нажатии на ссылку **Объекты на карантине** открывается каталог хранения объектов, помещенных на карантин.

Запуск в тихом режиме

Существует возможность запуска антивирусного сканирования в тихом режиме с помощью дополнительной утилиты changetpsmode [120].

Просмотр отчёта о проверке

Для просмотра подробных сведений о проверке в процессе сканирования нажмите на ссылку **Подробно**. Для просмотра отчета [108] по окончании проверки нажмите на

ссылку с датой и временем последней проверки в строке **Последняя проверка**.

5.6.3 Результат проверки

При обнаружении вредоносного объекта, SoftControl SysWatch определяет его тип (вирус, троянская программа, программа-шпион и т.д.) и выполняет над обнаруженным объектом определенное действие в зависимости от настроек реакции на угрозу 99.

Выбор действия для отдельной угрозы

Если в настройках выбрана опция **Запрос действия**, SoftControl SysWatch предлагает пользователю выбор действия для каждой обнаруженной угрозы.

Окно предупреждения, отображаемое SoftControl SysWatch при нахождении угрозы в процессе антивирусного сканирования, показано на рис. ниже 105.

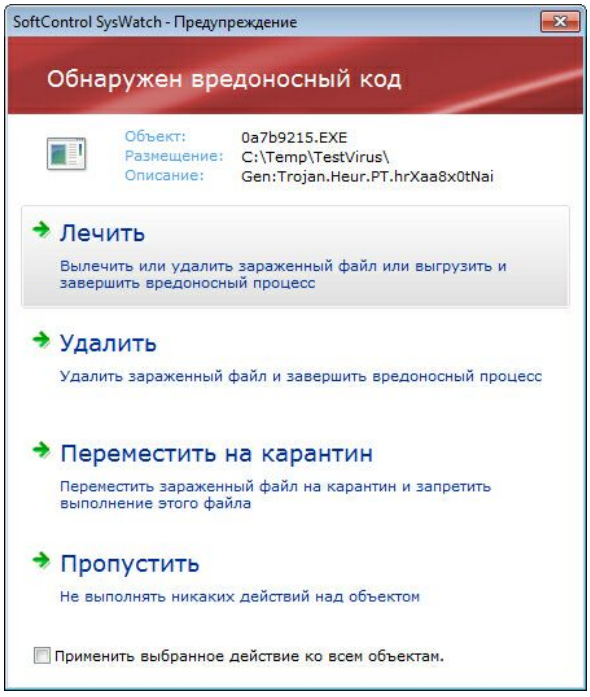

Рисунок 88. Окно предупреждения для заражённого объекта

Окно **SoftControl SysWatch - Предупреждение** состоит из 2 частей:

- Область описания угрозы. В данном блоке приводится информация об объекте, представляющем угрозу: имя, размещение, описание (предполагаемый тип вредоносного кода по установленному соответствию с имеющейся базой вирусных сигнатур).

- Область выбора действия. В блоке выбора действия отображаются возможные действия для обнаруженной угрозы:
  - → **Лечить** – вылечить или удалить зараженный файл, если лечение невозможно, или выгрузить и завершить вредоносное приложение;
  - → **Удалить** – удалить зараженный файл и завершить вредоносное приложение;
  - → **Переместить на карантин** – переместить зараженный объект в специальный каталог и запретить его выполнение;
  - → **Пропустить** – не выполнять никаких действий над объектом.
  - ❑ **Применить выбранное действие ко всем объектам** – применить выбранное действие для данного объекта ко всем последующим угрозам в рамках текущей проверки.

Выбор действий для угроз по окончанию проверки

Если в настройках выбрана опция **Выбор действия по окончанию проверки**, SoftControl SysWatch предлагает пользователю выбор действий для всех найденных объектов в рамках текущей проверки.

Окно **Обнаруженные угрозы** со списком найденных вредоносных объектов и возможных действий для них, отображаемое SoftControl SysWatch по окончании процесса антивирусного сканирования, показано на рис. Окно с обнаруженными угрозами 106.

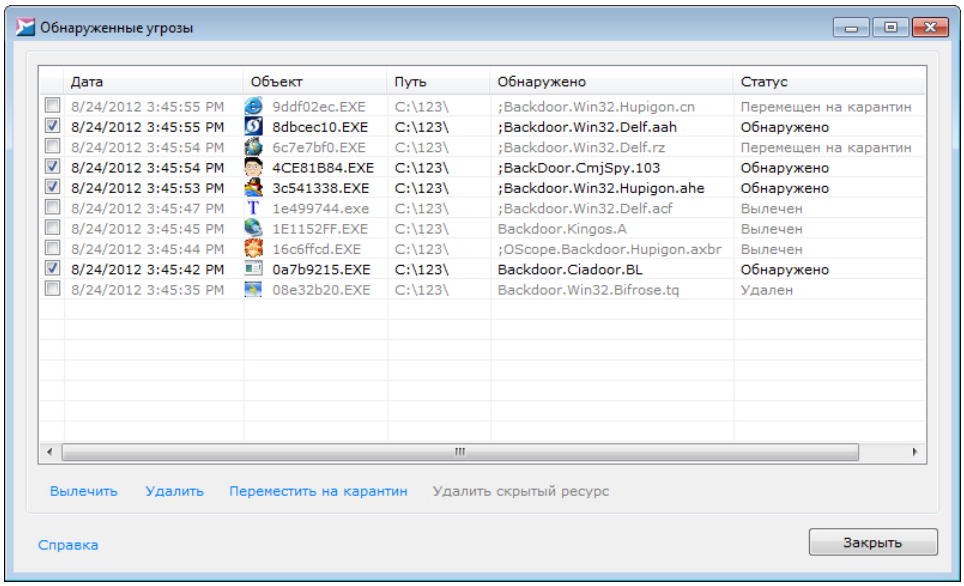

Рисунок 89. Окно с обнаруженными угрозами

В столбцах **Объект**, **Путь**, **Обнаружено** приводится информация об объекте,

представляющем угрозу: имя, размещение, описание (предполагаемый тип вредоносного кода по установленному соответствию с имеющейся базой вирусных сигнатур). В столбце **Дата** указано время обнаружения угрозы, в столбце **Статус** – текущее состояние угрозы.

Установите флажки у объектов, над которыми необходимо выполнить действие и нажмите на одну из ссылок:

- → **Вылечить** – вылечить или удалить зараженный файл, если лечение невозможно, или выгрузить и завершить вредоносное приложение;
- → **Удалить** – удалить зараженный файл и завершить вредоносное приложение;
- → **Переместить на карантин** – переместить зараженный объект в специальный каталог и запретить его выполнение;
- → **Удалить ресурс** – произвести удаление руткита.

По окончании применения действия текст строки с выбранным объектом изменяет цвет на серый, в столбце **Статус** отображается результат выполнения действия.

По окончании работы с окном нажмите на кнопку **Закрыть**.

Просмотр результата автоматического выбора действий для угроз

Если в настройках выбрана опция **Выбор действия автоматически**, SoftControl SysWatch выполняет действия над зараженными объектами без обращения к пользователю.

Для просмотра результата проверки нажмите на ссылку **Обнаружено** на вкладке **Проверка** панели управления[36] SoftControl SysWatch. В окне **Обнаруженные угрозы** (рис. Окно с обнаруженными угрозами[106]) можно просмотреть список угроз и примененные к ним SoftControl SysWatch действия.

По окончании работы с окном нажмите на кнопку **Закрыть**.

Если часть угроз осталась необработанной, на вкладке **Проверка** панели управления[36] SoftControl SysWatch отображается статус *Найденные угрозы не обезврежены*. Завершить обработку угроз можно нажав на ссылку **Обнаружено**.

Если все действия по нейтрализации угроз выполнены успешно, на вкладке **Проверка** панели управления[36] SoftControl SysWatch отображается статус *Компьютер проверен и защищен*.

5.7 Отчёты

В SoftControl SysWatch реализовано протоколирование событий безопасности и статусов программы в отчеты двух видов:

- Текстовые отчеты [108];
- Регистрация событий в Windows Management Instrumentation (WMI) [111].

5.7.1 Текстовые отчёты

Текстовые отчеты являются основным инструментом ретроспективного анализа событий безопасности программного окружения. SoftControl SysWatch создает текстовые отчеты следующих типов:

- **Системный отчет**, включающий в себя следующую информацию:
  - запуск и останов системной службы SoftControl SysWatch (*safensec.exe*);
  - инициализация служебной базы данных;
  - название и версия программы;
  - изменения статусов и настроек программы;
  - инциденты активности приложений [52] и их параметры: название, процесс и его идентификатор (PID), модуль родительского процесса и его идентификатор (PPID), командная строка, имя загружаемого DLL-модуля, учетная запись, зона выполнения, статус;
  - инциденты нарушения политики контроля [72] и их параметры: название, тип активности, учетная запись, программа-источник инцидента, контролируемый объект, решение, количество пропущенных однотипных событий (см. выше [56]);
  - идентификатор (UID) правила, в отношении которого произошло нарушение политики контроля [72];
  - имя настроек, полученных с сервера.
- **Отчет о сборе профиля**, включающий в себя следующую информацию:
  - область сбора профиля [46];
  - список проверенных объектов;
  - результаты сбора профиля [46].
- **Отчет о проверке**, включающий в себя следующую информацию:
  - область проверки [103];
  - настройка реакции на угрозу [100];

- результаты проверки[105].

- **Отчет об обновлении**, включающий в себя информацию о проведенных обновлениях программы[122].

Настройка параметров сохранения отчётов

Для просмотра и изменения параметров отчетов откройте настройки программы и выберите раздел **Параметры** → **Отчеты** (рис. Настройка параметров отчетов[109]).

Для включения функции ведения отчетов установите флажок **Формировать отчеты** и выберите виды событий для протоколирования:

- **Обновление**;
- **Проверка**;
- **Системный**:
  - **Угрозы**;
  - **Службы и неподозрительные приложения**.

Выставите галочку **Службы и неподозрительные приложения**, чтобы включить запись событий запуска/остановки служб. Службы, которые были запущены до системной службы *safensec.exe*, будут помечаться в отчетах как *была запущена ранее*.

В счетчике **Хранить отчеты** установите количество дней, за которые сохраняется история событий. Для удаления всех файлов отчетов нажмите на кнопку **Очистить**.

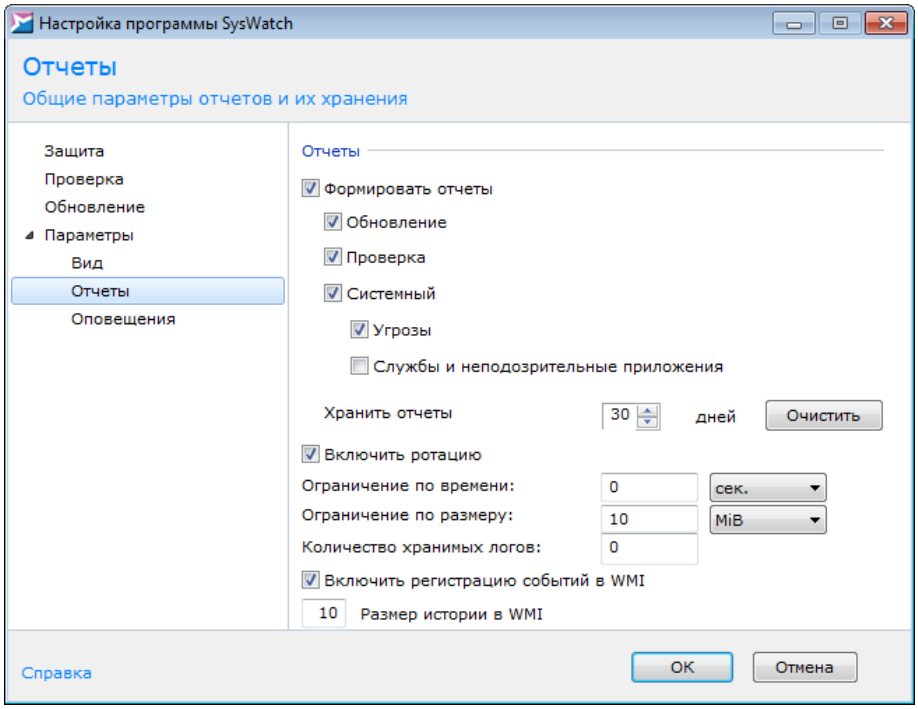

Рисунок 90. Настройка параметров отчётов

В SoftControl SysWatch поддерживается ротация отчетов программы, позволяющая контролировать размер файлов отчетов. Ротация позволяет формировать отчеты, автоматически разбиваемые на идентичные по своим параметрам части вида

<имя файла отчета>.txt.<индекс части отчета>,

при этом последний по времени отчет всегда имеет индекс 1, а наиболее старый – максимальный индекс.

Для включения данной функции установите флажок **Включить ротацию** и укажите параметры ротации (один или несколько):

- **Ограничение по времени**

  Введите в данном поле лимит по времени, по достижении которого файл отчета должен быть ротирован, и выберите единицы величины в выпадающем списке (секунды, минуты, часы, дни).

- **Ограничение по размеру**

  Введите в данном поле лимит по размеру файла отчета, по достижении которого файл отчета должен быть ротирован, и выберите единицы величины в выпадающем списке (Б, КиБ, МиБ).

- **Количество хранимых логов**

  Введите в данном поле максимальное число хранимых частей файлов отчетов.

Для вступления изменений в силу нажмите на кнопку **OK**.

Механизм ротации последнего отчета (по размеру и по времени) и механизм удаления (очистки) всех файлов отчетов, кроме последнего, работают независимо друг от друга. Пусть, например, для опции **Хранить отчеты** выставлено значение 10 дней, для опции **Ограничение по времени** – 1 день, а для опции **Количество хранимых логов** – 1. Тогда каждый день будут создаваться файлы вида *<тип отчета>_<дд.мм.гг>_<чч.мм.сс.ммм>.txt* и *<тип отчета>_<дд.мм.гг>_<чч.мм.сс.ммм>.txt.1*, причем раз в сутки файл с именем *<тип отчета>_<дд.мм.гг>_<чч.мм.сс.ммм>.txt.1* будет удаляться, расширение файла *<тип отчета>_<дд.мм.гг>_<чч.мм.сс.ммм>.txt* будет меняться на *.txt.1*, и будет создаваться новый файл *<тип отчета>_<дд.мм.гг>_ <чч.мм.сс.ммм>.txt*, в который и будут записываться дальнейшие события.

Однако если в течение указанного в настройках времени (в данном случае одного дня) компьютер или системная служба *safensec.exe* были перезапущены, то создается файл *<тип отчета>_<новая_дата>_<чч.мм.сс.ммм>.txt*, а через день – файл *<тип отчета>_<новая_дата>_<чч.мм.сс.ммм>.txt.1*, и механизм ротации, описанный выше, будет применяться только к ним. Файлы *<тип отчета>_<дд.мм.гг>_ <чч.мм.сс.ммм>.txt* и *<тип отчета>_<дд.мм.гг>_<чч.мм.сс.ммм>.txt.1* будут сохранены без изменения в течение 10 дней, после чего будут удалены.

Просмотр отчётов

Чтобы просмотреть отчеты, выберите пункт **Отчеты** контекстного меню[35] SoftControl SysWatch. В появившемся каталоге откройте текстовый файл с именем вида *<тип отчета>_<дд.мм.гг>_<чч.мм.сс.ммм>.txt*.

5.7.2 Регистрация событий в WMI

В SoftControl SysWatch реализована функция непосредственной записи информации о событиях и статусах программы в агрегированной форме в объекты WMI. Данный функционал предоставляет возможность получения этой информации с клиентских хостов при их удаленном администрировании с помощью средств управления IT-инфраструктурой, таких как MS SCCM.

Далее приведено описание самих объектов, видов событий и статусов SoftControl SysWatch.

Для системной службы *safensec.exe* объект WMI называется **SafenSoftService**, для антивирусного сканера *snsods.exe* – **SafenSoftScanner**.

В табл. 9 указаны виды событий для обоих объектов.

Таблица 9. Виды событий

Объект	Виды событий
SafenSoftService	• *InstallerAllow* – разрешение на запуск инсталлятора; • *InstallerBlock* – блокировка инсталлятора; • *ProcessAllow* – разрешение на запуск приложения; • *ProcessBlock* – блокировка приложения.
SafenSoftScanner	• *SuspectList* – найден подозрительный объект; • *VirusList* – найден инфицированный объект.

Приведенные в перечислении типы являются префиксами, которые ставятся перед свойством соответствующего объекта WMI. За префиксом следует параметр *_Count* – общее количество событий такого типа или *_Item0* - *_Item[N]*, где [N] – последние N событий (количество, установленное в конфигурации).

Ошибки сканирования системы не регистрируются в WMI.

В табл. 10 указаны типы статусов программы для обоих объектов.

Таблица 10. Типы статусов

Объект	Типы статусов	Тип	Значение
SafenSoftService	• *AutoSetup* – статус автоматической настройки (сбора профиля);	строковый	<строка статуса>
	• *FilesystemControl* – контроль файловой системы;	логический	False ("0") – отключен True ("не 0") – включен
	• *RegistryControl* – контроль системного реестра;	логический	
	• *NetworkControl* – контроль сетевой активности;	логический	
	• *GlobalInstallationMode* – глобальный режим обновления ПО;	логический	
	• *SystemScan* – статус сканирования системы;	строковый	<строка статуса>
	• *Version* – информация о версии.	строковый	<название продукта> <номер версии>
SafenSoftScanner	• *Version* – информация о версии.	строковый	<название продукта> <номер версии>

Только сбор профиля может переводить *SystemScan* во все ниже перечисленные состояния:

- *Проверка компьютера начата*;
- *Проверка компьютера прервана пользователем*;
- *Проверка компьютера завершена. Вредоносный код не найден*;
- *Проверка компьютера завершена. Найден вредоносный код*.

Сканирование на вирусы само по себе может перевести *SystemScan* только в состояние:

- *Проверка компьютера завершена. Найден вредоносный код*.

Для сброса состояния *Проверка компьютера завершена. Найден вредоносный код* необходимы запуск сбора профиля и его успешное завершение (условие – не обнаружено вредоносного кода).

Для каждого свойства (за исключением списков) создается еще одно свойство, с суффиксом *_LastChange*, в которое записывается время записи свойства.

Настройка параметров регистрации событий в WMI

Для просмотра и изменения параметров записи событий в WMI откройте настройки программы и выберите раздел **Параметры** → **Отчеты** (рис. Настройка параметров отчетов 109).

Для включения функции установите флажок **Включить регистрацию событий в WMI** и укажите **Размер истории в WMI** в соответствующем поле.

> Для предотвращения проблем с повышенным потреблением системных ресурсов не рекомендуется задавать размер истории равным более 100 событий, оптимальная величина – от 10 до 50 событий.

Для вступления изменений в силу нажмите на кнопку **OK**.

Просмотр зарегистрированных событий

Для просмотра описанных объектов в утилите **Тестер инструментария управления Windows** (Windows Management Instrumentation Tester) выполните следующие шаги:

1) Запустите утилиту *wbemtest.exe* из состава ОС Microsoft® Windows®.

2) Нажмите кнопку **Подключить** (Connect) и в диалоговом окне **Подключение**

(Connect) укажите в верхнем поле ввода пространство имен \\<*URI*>\root\cimv2, где <*URI*> – IP-адрес или имя клиентского хоста с установленным SoftControl SysWatch. Для работы с удаленным клиентским хостом необходимо иметь на нем разрешение на чтение и запись, которое предоставляется с помощью оснастки **Управляющий элемент WMI** (WMI Control).

3) Нажмите кнопку **Подключить** (Connect).
4) В области **IWbemServices** нажмите на кнопку **Классы** (Enum Classes).
5) В появившемся диалоговом окне оставьте поле пустым и нажмите **OK**.
6) В появившемся списке выберите **SafenSoftService** или **SafenSoftScanner** и откройте свойства выбранного объекта двойным нажатием левой кнопки мыши на нем.
7) Установите флажок **Скрыть системные свойства** (Hide system properties) в открывшемся окне.
8) Ознакомьтесь со списком свойств.

5.8 Настройка общих параметров программы

Ниже приведены указания по настройке общих параметров работы SoftControl SysWatch:

- самозащита системной службы [114];
- парольная защита [115];
- отложенный запуск системной службы [117].

5.8.1 Самозащита системной службы

Для включения самозащиты системной службы SoftControl SysWatch (*safensec.exe*) откройте настройки программы, выберите раздел **Параметры** и в области **Самозащита** установите флажок **Запретить внешнее управление системной службой** (рис. Настройки параметров программы [114]).

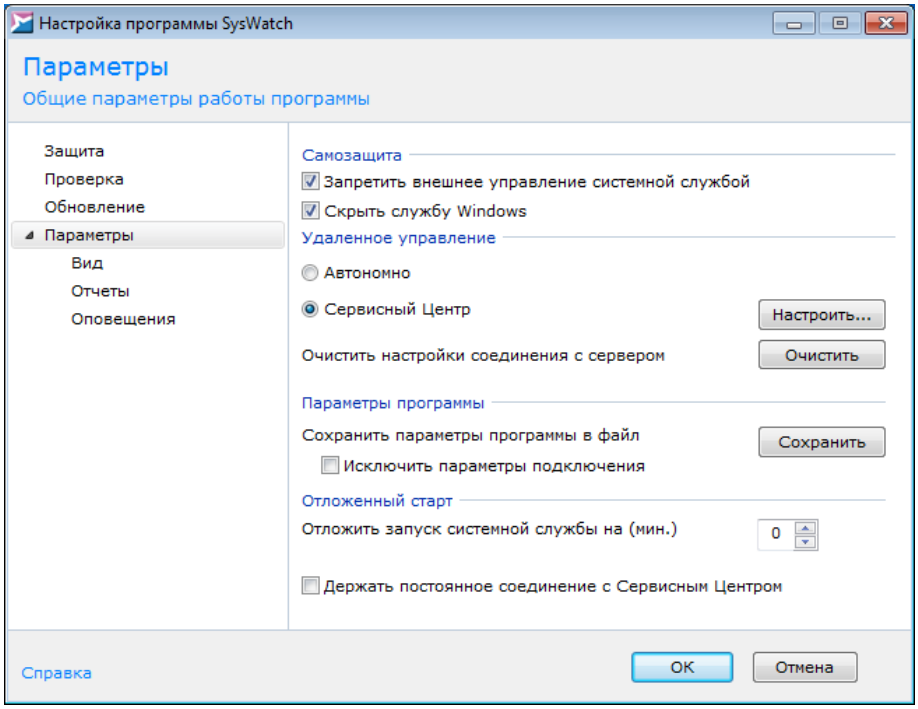

Рисунок 91. Настройки параметров программы

При выборе данной опции принудительная выгрузка системной службы SoftControl SysWatch из ОЗУ становится невозможной.

Установите флажок **Скрыть службу Windows**, если системная служба SoftControl SysWatch (*safensec.exe*) не должна показываться в оснастке **Службы** ОС Windows. В этом случае управление службой *safensec.exe* средствами ОС (запуск/остановка) становится невозможным.

Примечание: скрытие системной службы не работает на ОС Windows XP.

Чтобы изменения вступили в силу, нажмите на кнопку **OK**.

5.8.2 Парольная защита

Для включения парольной защиты откройте раздел **Защита** настроек программы, установите флажок **Включить защиту паролем** и нажмите на кнопку **Настроить** (рис. Настройки общих параметров защиты 115).

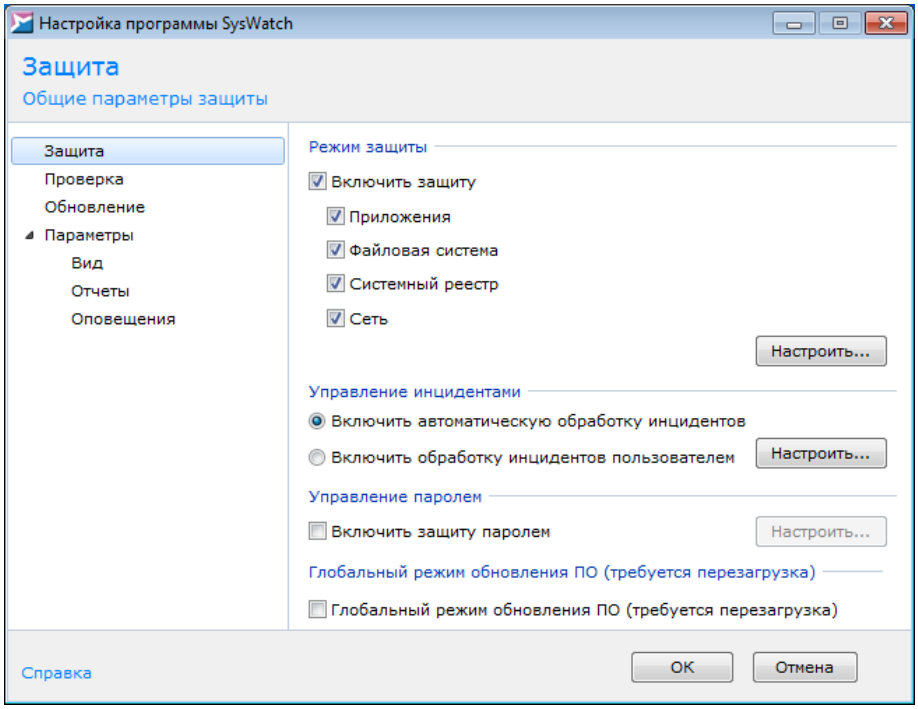

Рисунок 92. Настройки общих параметров защиты

В окне **Защита настроек программы** введите текущий пароль (если был назначен ранее), новый пароль и его подтверждение, после чего отметьте области действия (рис. Настройка парольной защиты 116):

- **Изменение настроек программы**

  запрос пароля при доступе к панели управления 36 и настройкам SoftControl SysWatch.

- **Удаление программы**

  запрос пароля при запуске программы деинсталляции 133 SoftControl SysWatch.

Длина пароля должна составлять не менее 7 символов.

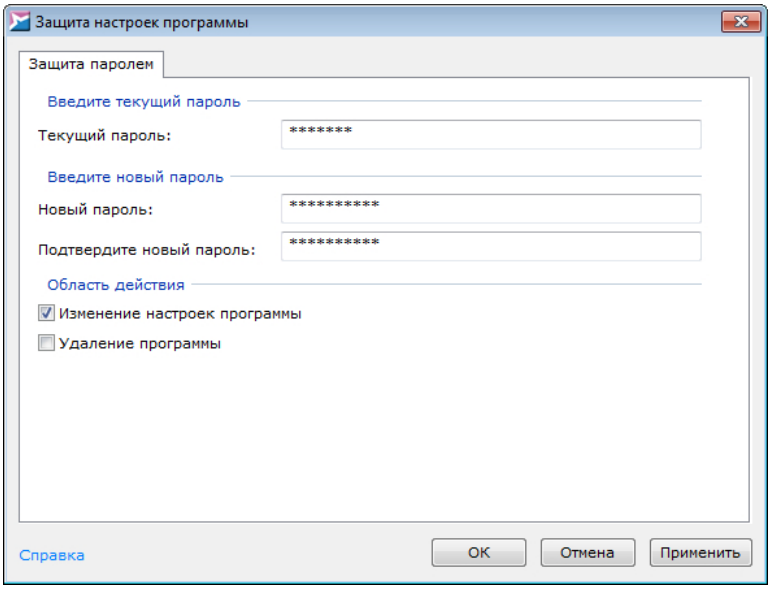

Рисунок 93. Настройка парольной защиты

Чтобы изменения вступили в силу, нажмите на кнопку **OK** в обоих окнах настроек.

5.8.3 Отложенный запуск системной службы

В SoftControl SysWatch предусмотрена возможность установки интервала отложенного запуска системной службы (*safensec.exe*). Данная опция может быть полезна для систем с низким быстродействием (например, УС) при наложении интервалов инициализации аппаратного и программного обеспечения. В этом случае при внештатных ситуациях, таких как перезагрузка системы в результате перебоя питания, может быть некорректно инициализирована часть устройств или служб системы. Установка тайм-аутов инициализации позволяет избежать подобных ситуаций.

Для установки опции в SoftControl SysWatch откройте настройки программы, выберите раздел **Параметры** и в области **Отложенный старт** установите **Отложить запуск системной службы на** в минутах (рис. Настройки параметров программы 117).

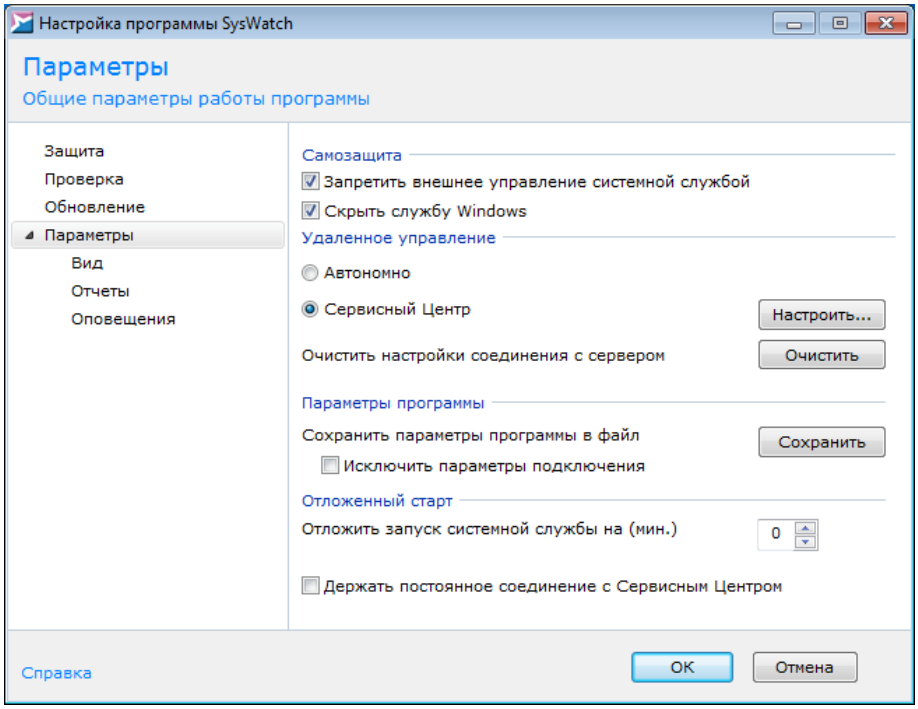

Рисунок 94. Настройки параметров программы

При следующем перезапуске системной службы SoftControl SysWatch ее загрузка будет сдвинута на введенное значение. Чтобы изменения вступили в силу, нажмите на кнопку **OK**.

Если защита выключена, то до момента запуска системной службы запуск всех приложений (как в профиле, так и вне его) разрешается.

Выставите галочку **Держать постоянное соединение с Сервисным Центром**, если необходимо поддерживать соединение с SoftControl Service Center в режиме реального времени.

5.9 Сохранение и восстановление настроек

Полная конфигурация SoftControl SysWatch, в том числе настроенная политика контроля, белый список сертификатов и текущий пароль программы, доступна к выгрузке в основной конфигурационный файл[119], который может быть использован при установке в тихом режиме на другие клиентские хосты (операция клонирования программы с эталонного объекта защиты) и удалении в тихом режиме.

5.9.1 Выгрузка основного конфигурационного файла

Для того чтобы сохранить текущую конфигурацию SoftControl SysWatch, откройте настройки программы, выберите раздел **Параметры** и в области **Параметры программы** нажмите на кнопку **Сохранить** (рис. Настройки параметров программы 119). Если необходимо выгрузить конфигурацию SoftControl SysWatch без настроек подключения к серверу, перед сохранением установите флажок **Исключить параметры подключения**.

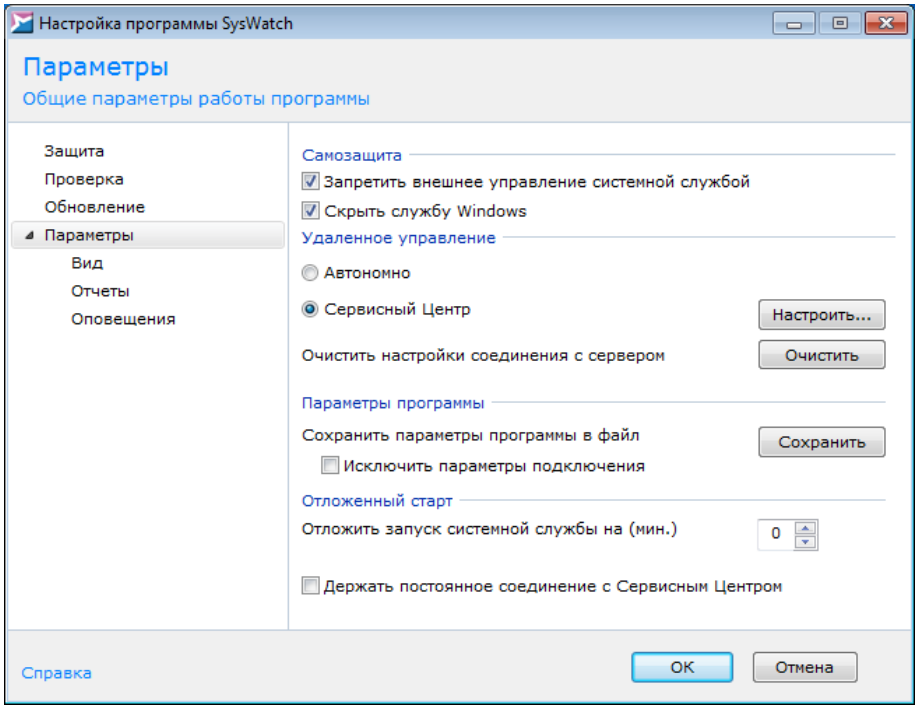

Рисунок 95. Настройки параметров программы

В диалоговом окне просмотрите и в случае необходимости измените имя файла резервной копии настроек (задается автоматически), определите путь, по которому он будет сохранен, выберите расширение файла **xmlc* и нажмите на кнопку **Сохранить**. По умолчанию основной конфигурационный файл после формирования сохраняется в зашифрованном виде в каталог стандартного хранилища SoftControl SysWatch. В хранилище также располагаются файлы *configs.xmlc* и *default.xmlc* для восстановления настроек программы и политики контроля по умолчанию соответственно.

Выгрузку основного конфигурационного файла можно также осуществить в тихом режиме с помощью дополнительной утилиты snsdumpsetting 121.

6. Расширенные возможности SoftControl SysWatch

В данном разделе приведены инструкции по локальной работе с расширенными функциями SoftControl SysWatch.

6.1 Дополнительные утилиты

В поставку SoftControl SysWatch могут входить утилиты, реализующие дополнительные функции по работе с программой. Утилиты предоставляются компанией Safe'N'Sec Corporation по запросу.

Запуск утилит осуществляется из командной строки ОС. Данные утилиты могут быть удобны к применению, в частности, при удаленном администрировании клиентских хостов с помощью сторонних средств управления IT-инфраструктурой (например, MS SCCM).

Ниже приведено описание следующих утилит:

- changetpsmode [120];
- snsdumpsetting [121].

6.1.1 changetpsmode

Утилита *changetpsmode.exe* предназначена для управления режимом глобальной установки [52], а также для запуска антивирусного сканирования [98] в тихом режиме.

Параметры, принимаемые утилитой, описаны в табл. 11.

Таблица 11. Опции changetpsmode

Параметр	Действие
-e <пароль>	Включить режим глобальной установки. Пароль, вводимый при использовании утилиты (GRkNVCOLzyz+311FKlrNqlGlqkxXGfZWXb), не регистрируется в отчетах SoftControl SysWatch.
-d	Выключить режим глобальной установки.
-s "<объект 1>" "<объект 2>"... "<объект N>"	Запустить антивирусное сканирование указанных объектов в тихом режиме, где *<объект N>* – полный путь к объекту проверки (жесткому диску, каталогу или отдельному файлу). Антивирусное сканирование ОЗУ происходит автоматически независимо от указанных объектов. В процессе проверки применяется вариант реакции на угрозу **Выбор действия автоматически**. Результаты доступны в файле отчета о проверке [108]. Внимание: для корректного запуска проверки в тихом режиме необходимо строго соблюдать указанный синтаксис команды. В случае нескольких проверок, каждую следующую необходимо начинать только после завершения предыдущей.

6.1.2 snsdumpsetting

Утилита *snsdumpsetting.exe* предназначена для выгрузки основного конфигурационного файла[119] SoftControl SysWatch в тихом режиме.

Параметры, принимаемые утилитой, описаны в табл. 12.

Таблица 12. Опции snsdumpsetting

Параметр	Действие
"<путь к файлу>\<имя файла>"	Выгрузить конфигурацию SoftControl SysWatch в файл с заданным именем (без расширения) по указанному пути (если не указан, используется путь по умолчанию – к каталогу расположения утилиты).

7. Обновление SoftControl SysWatch

На момент установки приложения в модули SoftControl SysWatch могут быть добавлены улучшения и новые функции, а входящие в поставку антивирусные базы могут устареть. Рекомендуется выполнить обновление программы непосредственно после установки SoftControl SysWatch.

Далее описаны необходимые действия по обновлению SoftControl SysWatch:

- опции обновления [122];
- обновление в обычном режиме [125].

В случае, если источник обновления недоступен, выполните обновление в ручном режиме [127].

7.1 Опции обновления

Для настройки параметров обновления откройте раздел **Обновление** настроек программы (рис. Настройки параметров обновления [122]).

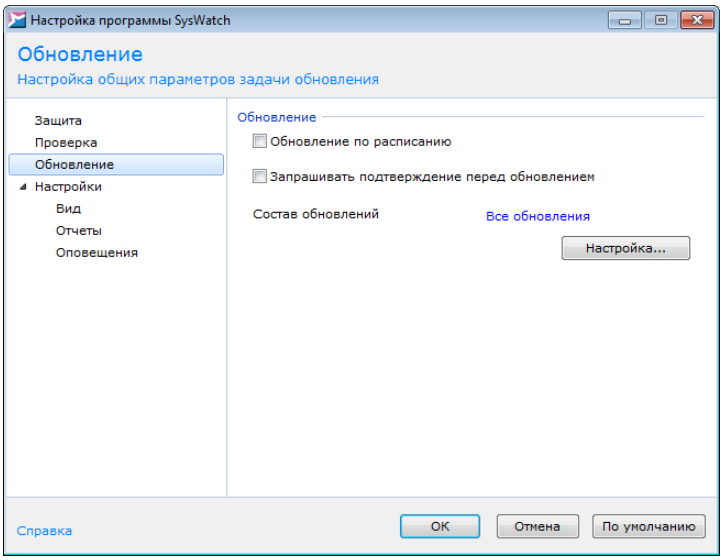

Рисунок 96. Настройки параметров обновления

Настройка состава и источника обновления

В строке **Состав обновлений** указаны компоненты, для которых производится обновление. Для настройки состава и других опций обновления нажмите на кнопку **Настройка**.

В окне **Настройка...** на вкладке **Соединение** выберите способ обновления (рис. Настройки способа обновления [123]):

- **Обновить через Сервисный Центр** – обновление посредством

внутрисетевого сервера обновлений (используется при удаленном режиме управления с сервера[43]);

- **Обновить через интернет** – обновление через сервер обновлений Safe'N'Sec Corporation, доступный посредством сети Интернет.

Если для соединения с сервером обновлений при данном способе используется прокси-сервер, в области **Соединение** установите флажок **Использовать параметры прокси-сервера** и укажите необходимые настройки.

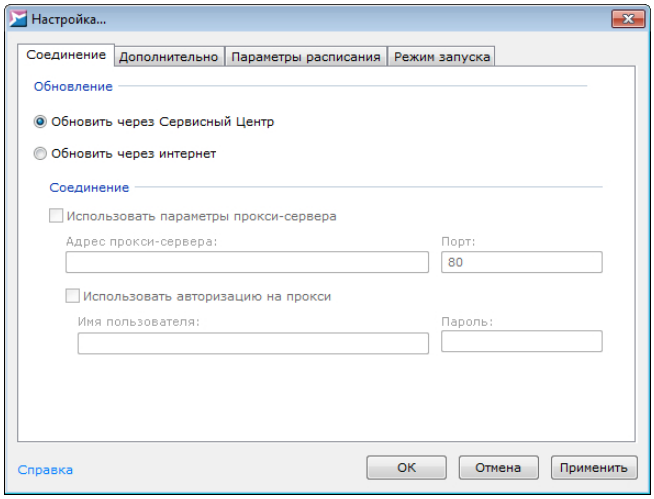

Рисунок 97. Настройки способа обновления

В окне **Настройка...** на вкладке **Дополнительно** выберите требуемые компоненты для обновления (рис. Настройки состава обновлений[123]):

- ❑ **Программные модули**;
- ❑ **Антивирусные базы**.

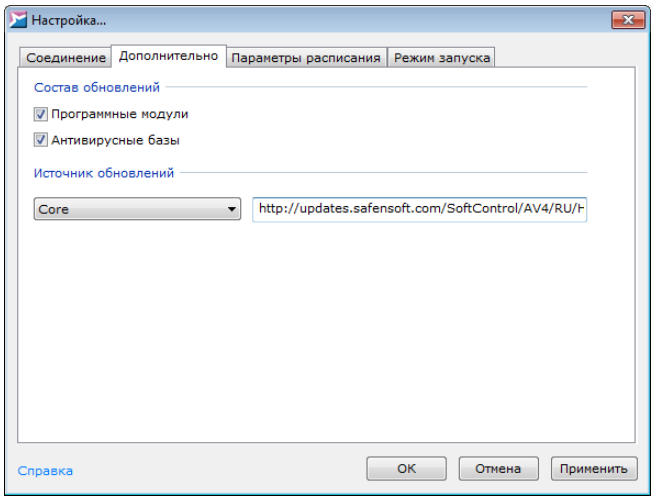

Рисунок 98. Настройки состава обновлений

В области **Источник обновлений** указаны адреса, с которых производится

обновление ядра проактивной защиты и баз каждого из доступных согласно лицензии [45] антивирусных компонентов. При необходимости адреса могут быть отредактированы в соответствующем поле.

Для применения настроек нажмите на кнопку **OK** или **Применить**.

Настройка обновления по расписанию

Условие: только для случая работы SoftControl SysWatch в режиме удаленного управления с сервера [43].

Для включения автоматического обновления по расписанию установите флажок **Обновление по расписанию**. Если необходимо **Запрашивать подтверждение перед обновлением**, установите соответствующий флажок для отображения диалога с запросом подтверждения операции. Чтобы настроить параметры обновления по расписанию, нажмите на кнопку **Настройка**.

В окне **Настройка...** откройте вкладку **Параметры расписания** и в счетчике **Частота дней** укажите периодичность, с которой будет выполняться задача, а в поле **Время запуска** – время начала выполнения задачи в формате *чч:мм:сс* (рис. Настройки параметров обновления по расписанию [124]).

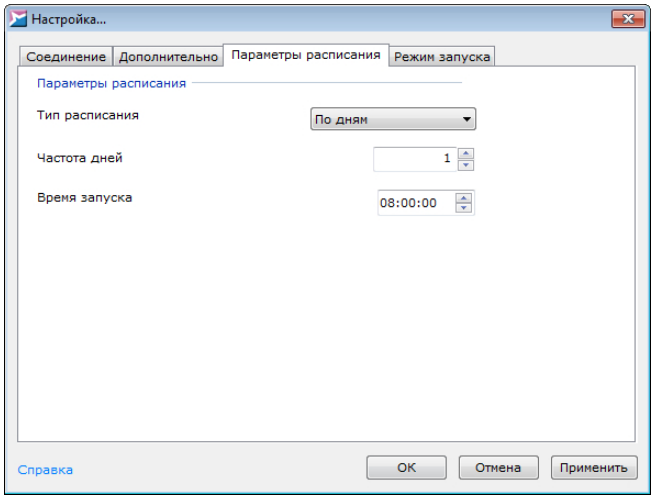

Рисунок 99. Настройки параметров обновления по расписанию

Для применения настроек нажмите на кнопку **OK** или **Применить**.

Настройка учётной записи

Чтобы настроить параметры учетной записи, под которой будет производиться обновление, нажмите на кнопку **Настройка**. В окне **Настройка...** на вкладке **Режим**

запуска выберите одну из опций (рис. Настройки учетной записи для обновления [125]):

- **С системной учетной записью**;
- **С учетной записью:** укажите учетные данные.

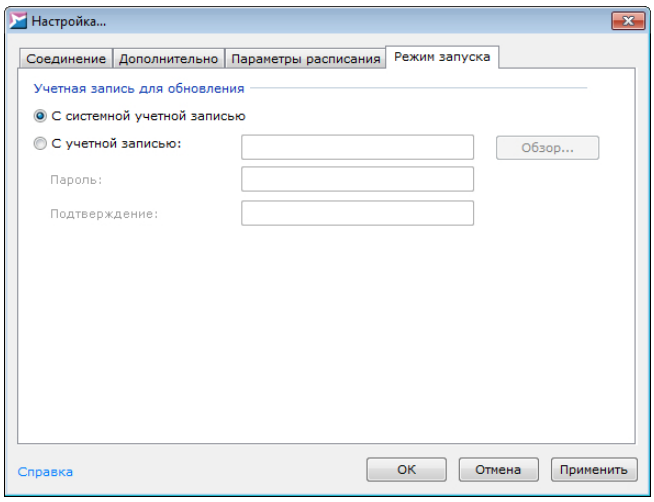

Рисунок 100. Настройки учётной записи для обновления

Для применения настроек нажмите на кнопку **OK** или **Применить**.

Для вступления изменений в силу нажмите на кнопку **OK**.

7.2 Обновление в обычном режиме

Обновление программных модулей и антивирусных баз можно производить как одновременно, так и по отдельности (регулируется соответствующими флажками в опциях обновления [123]).

Обновление программных модулей по требованию

Нажмите на кнопку **Запустить обновление** на вкладке **Обновление** панели управления [36] SoftControl SysWatch. В случае обнаружения модулей программы более новых, чем имеющиеся, произойдет их загрузка с сервера обновлений и установка. По окончании установки необходимо произвести перезагрузку системы для завершения обновления.

Если после проверки отображается статус *Обновление не требуется*, установлена последняя на данный момент версия программы.

Обновление по требованию также может производится администратором удаленно из консоли управления SoftControl Admin Console. Подробное описание процесса

удаленного запуска по требованию приведено в документе «Руководство администратора SoftControl Service Center».

Обновление антивирусных баз по требованию

Нажмите на кнопку **Запустить обновление** на вкладке **Обновление** панели управления[36] SoftControl SysWatch. В случае обнаружения баз данных сигнатур вирусов более новых, чем имеющиеся, произойдет их загрузка с сервера обновлений.

Если после проверки отображается статус *Обновление не требуется*, антивирусные базы находятся в актуальном состоянии.

Обновление по требованию также может производится администратором удаленно из консоли управления SoftControl Admin Console. Подробное описание процесса удаленного запуска по требованию приведено в документе «Руководство администратора SoftControl Service Center».

Обновление по расписанию

Составление расписания обновления производится локальным пользователем SoftControl SysWatch в соответствующих настройках программы[124] или администратором удаленно из консоли управления SoftControl Admin Console. Подробное описание процесса удаленной настройки обновления по расписанию приведено в документе «Руководство администратора SoftControl Service Center».

В данном режиме SoftControl SysWatch с заданной периодичностью проверяет наличие обновлений на определенном в настройках источнике и в случае обнаружения модулей программы и/или антивирусных баз более новых, чем имеющиеся, загружает их с сервера обновлений и запускает установку. По окончании установки программных модулей необходимо вручную произвести перезагрузку системы для завершения обновления.

Просмотр отчёта об обновлении

Для просмотра подробных сведений об обновлении в его процессе нажмите на ссылку **Подробно**. Для просмотра отчета[108] по окончании обновления нажмите на ссылку с датой и временем последней проверки в строке **Последний поиск обновлений**.

В строке **Установлены обновления** указаны дата и время последней произведенной установки обновлений. В строке **Режим запуска** отображается соответствующий способ, которым было запущено последнее обновление (по требованию или по расписанию).

7.3 Обновление в ручном режиме

Ручное обновление программных модулей в обычном режиме

1) Запустите установочный пакет *SysWatch_Patch.msi* версии, на которую необходимо произвести обновление.
2) В окне **Установка SoftControl SysWatch** нажмите на кнопку **Далее** (рис. Запуск программы обновления 127).

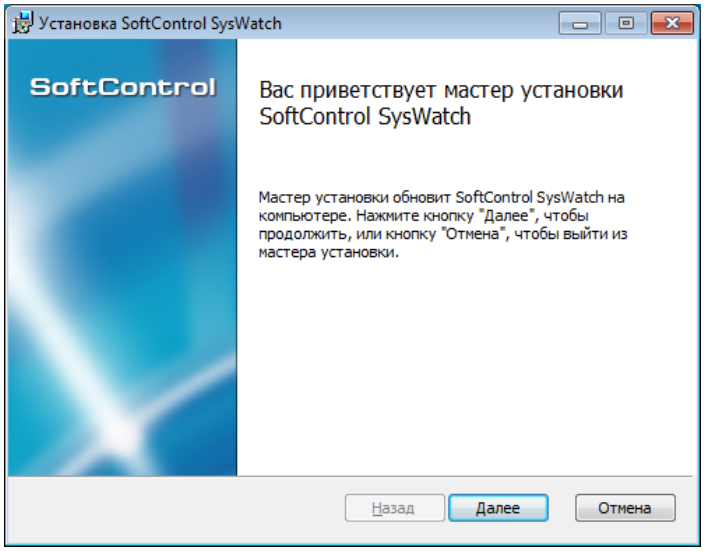

Рисунок 101. Запуск программы обновления

3) В случае вашего согласия, выберите параметр **Я принимаю условия лицензионного соглашения** и нажмите на кнопку **Далее** (рис. Лицензионное соглашение 127).

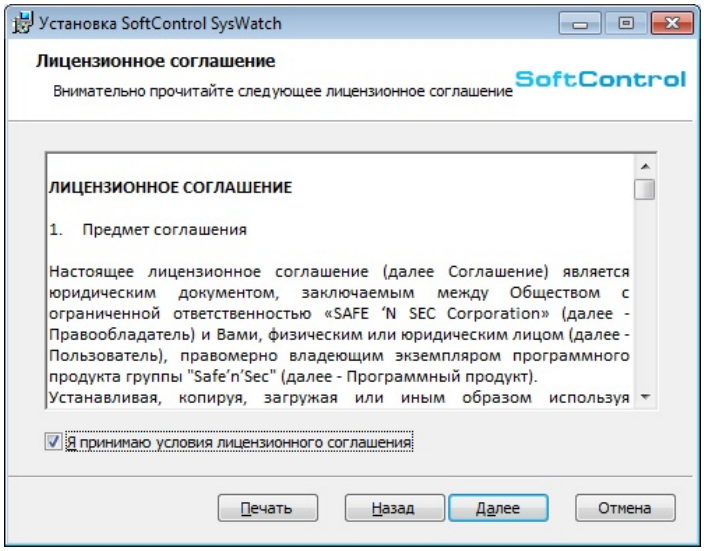

Рисунок 102. Лицензионное соглашение

4) Нажмите на кнопку **Обновить** (рис. Готовность к обновлению 128).

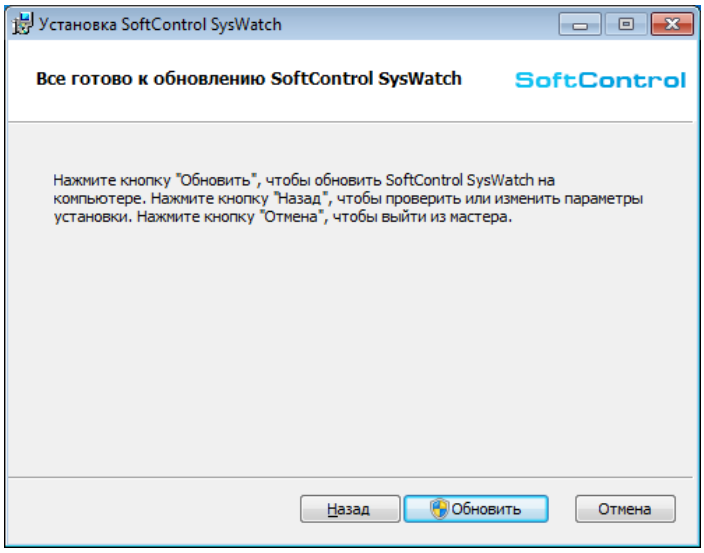

Рисунок 103. Готовность к обновлению

5) Дождитесь окончания процесса обновления (рис. Процесс обновления 128).

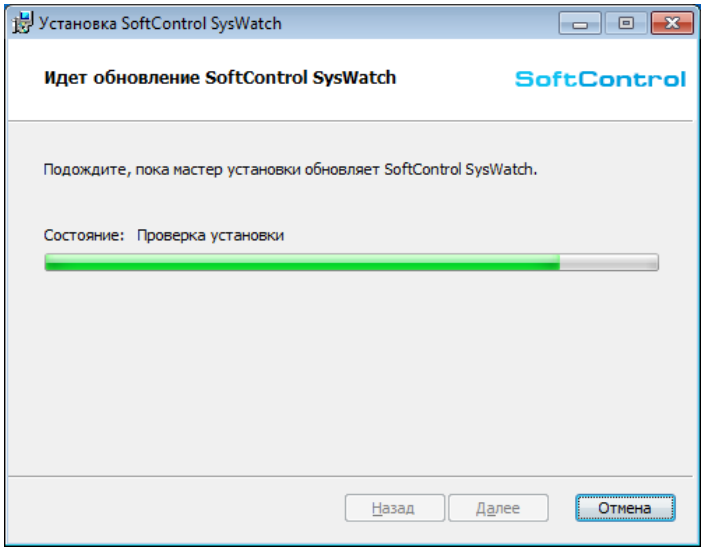

Рисунок 104. Процесс обновления

6) После появления сообщения **Установка SoftControl SysWatch завершена** нажмите на кнопку **Готово** (рис. Завершение обновления 129).

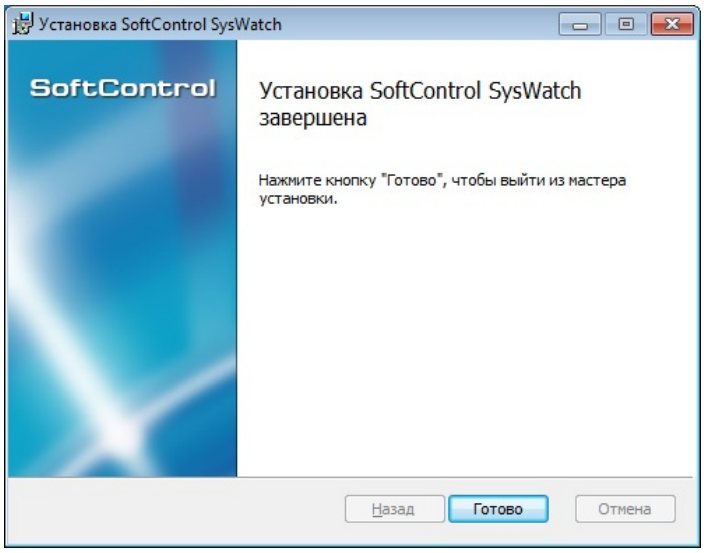

Рисунок 105. Завершение обновления

7) В диалоговом окне с предложением перезапуска системы выберите **Да**, после чего система будет отправлена на перезагрузку для завершения обновления (рис. Запрос перезагрузки системы 129).

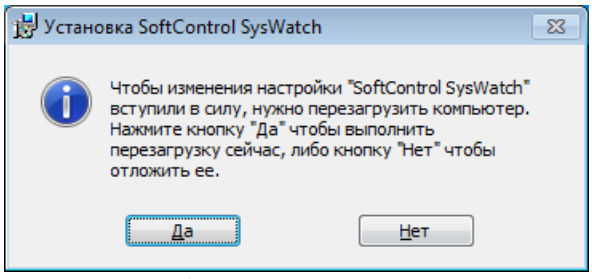

Рисунок 106. Запрос перезагрузки системы

Ручное обновление программных модулей в тихом режиме

Условие: все шаги выполняются под учетной записью с правами администратора.

1) Скопируйте установочный пакет *SysWatch_Patch.msi* версии, на которую необходимо произвести обновление, в каталог `C:\Temp` клиентского хоста.
2) Запустите командную строку Windows и выполните следующую команду:

```
%windir%\system32\msiexec.exe /i "C:\Temp\SysWatch_Patch.msi" /quiet
```

По окончании обновления система будет отправлена на перезагрузку автоматически.

Ручное обновление антивирусных баз

Для обновления антивирусных баз вручную выполните следующие действия:

1) Обновите антивирусные базы на тестовом устройстве любым доступным способом.
2) Скопируйте новое содержимое папки с антивирусными базами (например, `<каталог установки SoftControl SysWatch>\Plugins\AV\Av4` для антивирусного сканера *Avira*) на внешний носитель.
3) В клиентских настройках отключите правило 502 (**Политика контроля –> Файловая система**) для обеих зон (**Ограниченные приложения** и **Доверенные приложения**), сохраните настройки под новым именем и примените к подразделению устройства, на котором вы хотите обновить антивирусные базы.

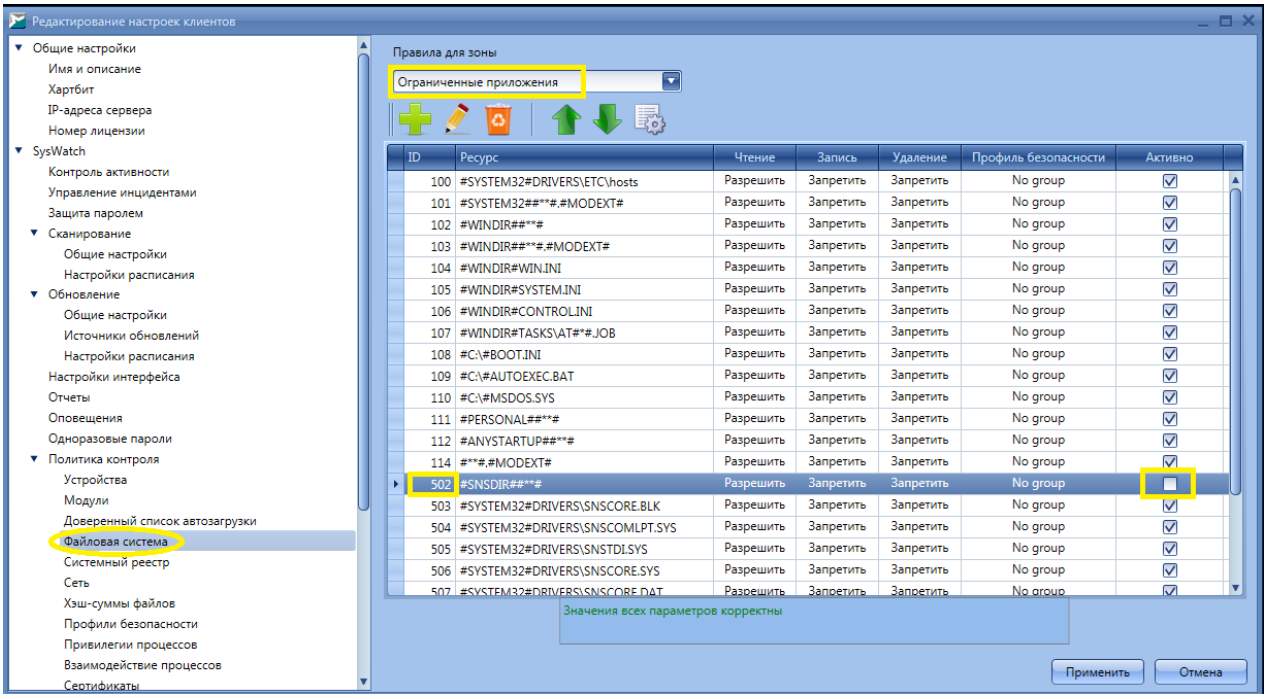

Рисунок 107. Отключите правило 502 в клиентских настройках. Ограниченные приложения

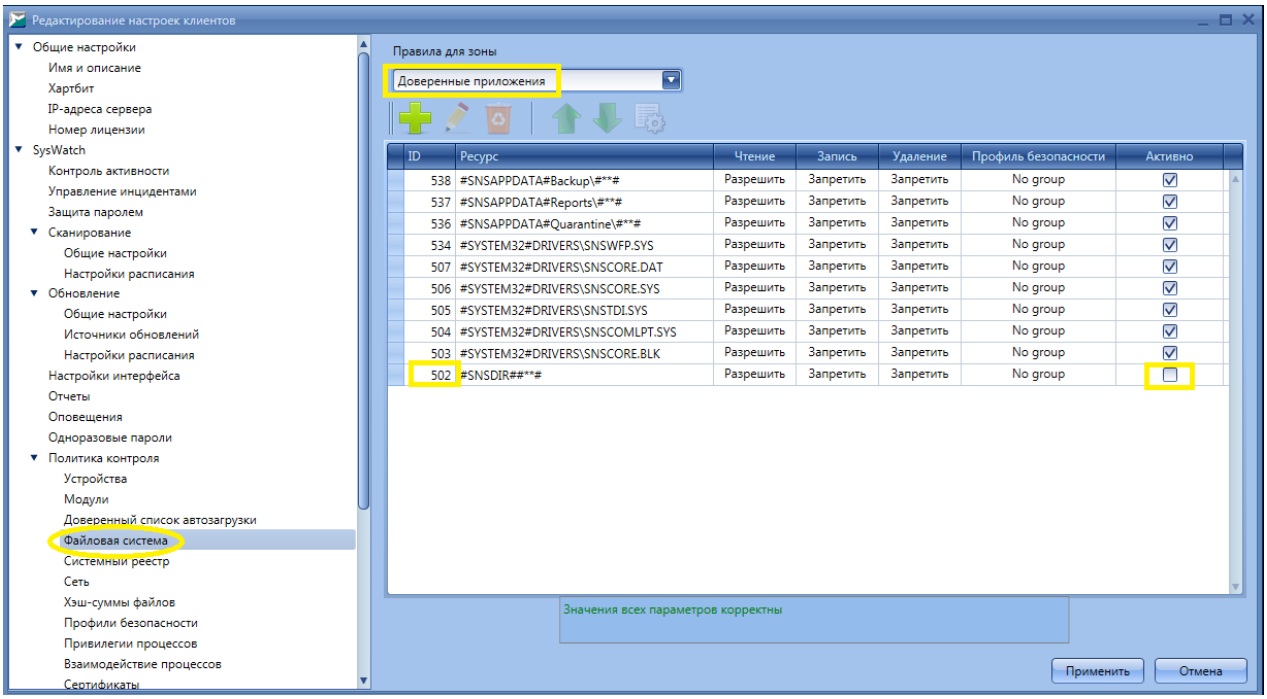

Рисунок 108. Отключите правило 502 в клиентских настройках. Доверенные приложения

4) Скопируйте содержимое папки с антивирусными базами с внешнего носителя в соответствующую директорию (для антивирусного сканера *Avira* это `<каталог установки SoftControl SysWatch>\Plugins\AV\Av4`) на устройстве, для которого вы обновляете антивирусные базы (с заменой существующих файлов).

5) Включите в клиентских настройках правило 502 для обеих зон (**Ограниченные приложения** и **Доверенные приложения**) и примените настройки к подразделению устройства, на котором вы обновляете антивирусные базы.

8. Удаление SoftControl SysWatch

SoftControl SysWatch может быть деинсталлирован с клиентских хостов как локально[133], так и одним из удаленных централизованных[134] способов.

8.1 Локальная деинсталляция

Возможны следующие варианты локальной деинсталляции SoftControl SysWatch:

- в обычном режиме (с использованием интерфейса пользователя)[133];
- в тихом режиме[134].

8.1.1 Удаление в обычном режиме

1) Для ОС Microsoft® Windows® XP, Microsoft® Windows® Server 2003: в Панели управления Windows в разделе **Установка и удаление программ** (Add or Remove Programs) на вкладке **Изменение или удаление программ** (Change or Remove Programs) выберите *SoftControl SysWatch* и нажмите на кнопку **Удалить** (Remove).

   Для ОС Microsoft® Windows® 7, Microsoft® Windows® Server 2008, Microsoft® Windows® 8, Microsoft® Windows® Server 2012: в Панели управления Windows в разделе **Программы** (Programs) → **Программы и компоненты** (Programs and Features) выберите *SoftControl SysWatch* и нажмите на кнопку **Удалить** (Uninstall).
2) В диалоговом окне с предложением перезапуска системы выберите **Да**, после чего система будет отправлена на перезагрузку для завершения деинсталляции (рис. Запрос перезагрузки системы[133]).

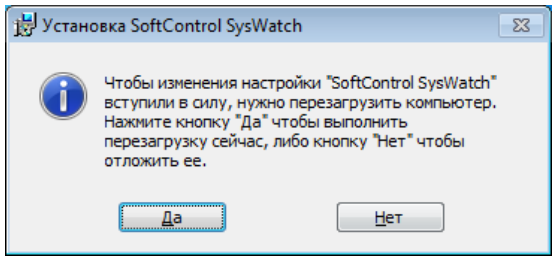

Рисунок 109. Запрос перезагрузки системы

8.1.2 Удаление в тихом режиме

Условие: все шаги выполняются под учетной записью с правами администратора.

1) Скопируйте установочный пакет *SysWatch.msi* (или *SysWatch_Patch.msi* в случае, если производилось обновление) текущей версии в каталог `C:\Temp` клиентского хоста.
2) Запустите командную строку Windows и выполните следующую команду:

```
%windir%\system32\msiexec.exe /x "C:\Temp\SysWatch.msi" /quiet
```

По окончании процедуры деинсталляции система будет отправлена на перезагрузку автоматически.

8.2 Удалённая деинсталляция

Удаленная деинсталляция SoftControl SysWatch подразумевает централизованно управляемое удаление клиентских приложений с группы хостов, объединенных в одну сеть.

Возможны следующие варианты удаленной централизованной деинсталляции SoftControl SysWatch:

- через доменную групповую политику (134);
- сторонними средствами администрирования (136).

8.2.1 Удаление через доменную групповую политику

Примечание: продемонстрировано на примере ОС Microsoft® Windows® Server 2008 R2.

1) Откройте оснастку **Server Manager** (Диспетчер сервера) из раздела **Administrative Tools** (Администрирование) меню **Start** (Пуск) в ОС контроллера домена.
2) Выберите раздел **Features** → **Group policy Management** → **Forest: <имя домена>** → **Domains** → **<имя домена>**, разверните подразделение **Software deployment**, вызовите контекстное меню объекта групповой политики, созданного ранее (18) для развертывания клиентских приложений (**Clients deployment**), и выберите пункт **Edit** (рис. Редактирование объекта групповой политики (134)).

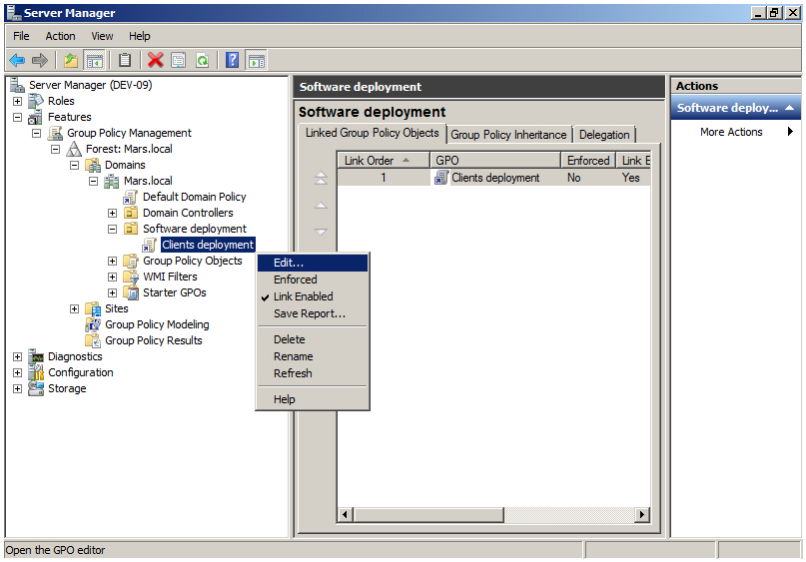

Рисунок 110. Редактирование объекта групповой политики

3) В открывшемся окне оснастки **Group Policy Management Editor** (Управление групповой политикой) выберите раздел **Computer configuration** → **Policies** → **Software Settings** → **Software installation**, в списке устанавливаемых приложений справа выберите требуемое приложение для удаления, вызовите контекстное меню и выберите пункт **All tasks** → **Remove** (рис. Вызов задачи удаления приложения 135).
4) В диалоговом окне **Remove Software** выберите метод деинсталляции приложений **Immediately uninstall the software from users and computers** (немедленное удаление ПО с компьютеров) и нажмите на кнопку **OK** (рис. Выбор метода деинсталляции приложения 135).

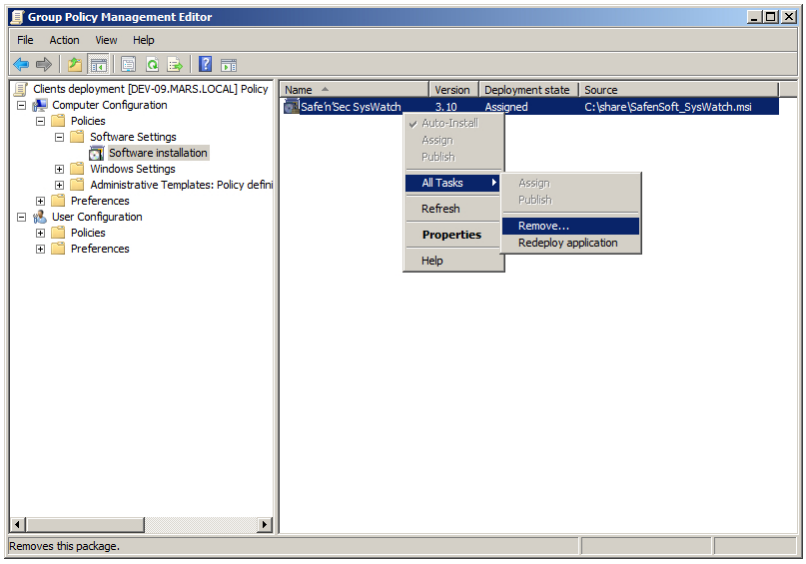

Рисунок 111. Вызов задачи удаления приложения

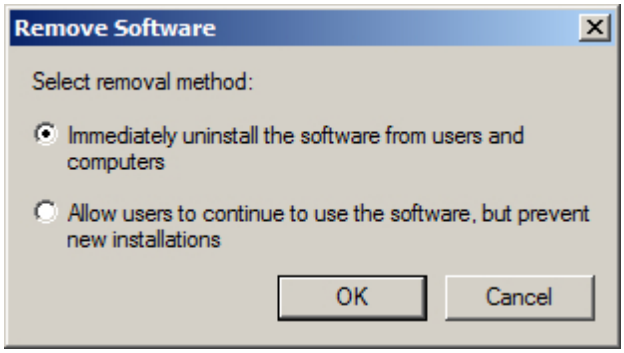

Рисунок 112. Выбор метода деинсталляции приложения

5) По истечении интервала обновления групповых политик (данный параметр зависит от настроек Active Directory), измененная политика применяется к клиентским хостам. Удаление выбранных приложений будет произведено после очередного перезапуска клиентских хостов. Для мгновенного применения созданной групповой политики запустите командную строку от имени администратора на клиентском хосте и выполните следующую команду:

```
gpupdate /force
```

По окончании выполнения команды подтвердите перезагрузку системы командой *Y* для применения обновленной групповой политики (рис. Ручное обновление параметров групповой политики 136).

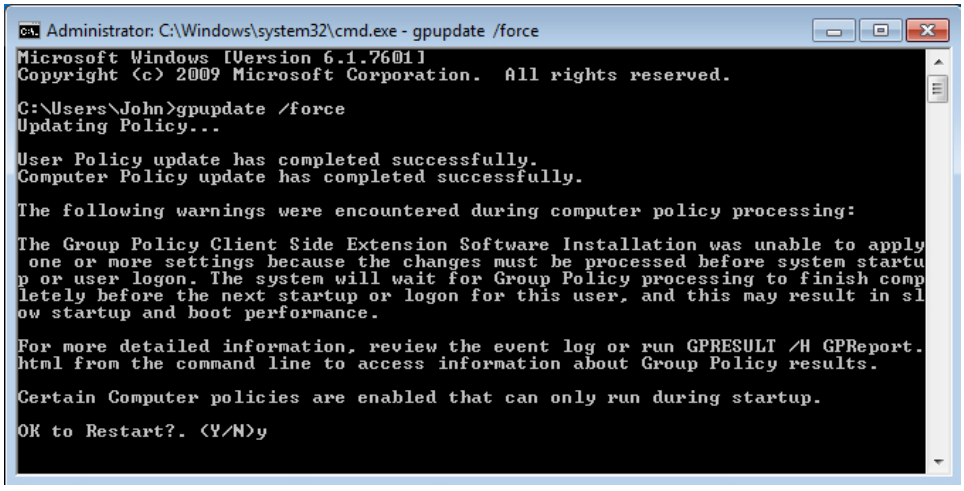

Рисунок 113. Ручное обновление параметров групповой политики

8.2.2 Удаление сторонними средствами администрирования

Как и в случае установки, для удаленной деинсталляции SoftControl SysWatch могут применяться сторонние системы управления IT-инфраструктурой. Методика удаления в

данном случае определяется исходя из конкретной системы и принятыми в ней способами деинсталляции ПО.

9. Дополнительная информация

9.1 Привилегии процессов

В табл. 13 представлено описание привилегий Windows, используемых процессами (см. также https://msdn.microsoft.com/ru-ru/library/windows/desktop/bb530716(v=vs.85).aspx и https://docs.microsoft.com/en-us/windows/device-security/auditing/event-4704).

Таблица 13. Описание привилегий процессов

Привилегия	Описание
Управление аудитом и журналом безопасности	Добавление записей в журнал безопасности.
Архивация файлов и каталогов	Выполнение операций по резервному копированию. Эта привилегия заставляет систему выдать права на чтение любого файла, независимо от того, что указано в списке управления доступом (ACL) для этого файла. Любой другой запрос на доступ, кроме чтения, по-прежнему оценивается с помощью ACL.
Восстановление файлов и каталогов	Выполнение операций восстановления. Эта привилегия заставляет систему выдать права на запись любого файла, независимо от того, что указано в списке управления доступом (ACL) для этого файла. Пользователь с данной привилегией может обходить разрешения файлов, папок, реестра и других постоянных объектов при восстановлении файлов и папок из резервных копий. Дополнительно данная привилегия позволяет назначить любого пользователя или группу с действующим идентификатором безопасности (SID) владельцем файла.
Изменение системного времени	Изменение системного времени. Пользователь с данной привилегией может изменять время и дату на внутренних часах компьютера. Пользователи с такими правами могут влиять на вид журналов событий. Если системное время изменено, события, которые были записаны, будут отображать это новое время, а не реальное время, в которое они произошли.
Завершение работы системы	Завершение работы локальной системы.
Принудительное удаленное завершение работы	Выключение системы с помощью запроса по сети.
Смена владельцев файлов и других объектов	Привилегия необходима, чтобы стать владельцем объекта без получения избирательного доступа. Пользователь с данной привилегией может стать владельцем любого защищаемого объекта в системе, включая объекты Active Directory, файлы и папки, принтеры, разделы реестра, процессы и потоки.
Отладка программ	Отладка и настройка памяти процесса, который принадлежит другой учетной записи. Пользователь с данной привилегией может присоединять отладчик к любому процессу или ядру. Разработчикам, отлаживающим свои собственные приложения, это пользовательское право не нужно. Разработчикам,

Привилегия	Описание
	отлаживающим новые компоненты системы, это право нужно. Данное право дает полный доступ к чувствительным и критичным компонентам операционной системы.
Изменение параметров среды изготовителя	Изменение энергонезависимой памяти (RAM) систем, которые используют данный тип памяти для хранения информации о конфигурации.
Профилирование производительности системы	Сбор профиля всей системы. Пользователь с данной привилегией может использовать средства наблюдения за производительностью для контроля производительности системных процессов.
Профилирование одного процесса	Сбор профиля по одному процессу. Пользователь с данной привилегией может использовать средства наблюдения за производительностью для контроля производительности несистемных процессов.
Увеличение приоритета выполнения	Увеличение базового приоритета процесса. Пользователь с данной привилегией может использовать процесс с доступом к свойству "запись" другого процесса для увеличения приоритета выполнения, назначенного этому другому процессу. Такой пользователь может изменять запланированный приоритет процесса через пользовательский интерфейс Диспетчера задач.
Загрузка и выгрузка драйверов устройств	Загрузка и выгрузка драйверов устройств. Пользователь с данной привилегией может динамически загружать и выгружать драйвера устройств или другой код в режиме ядра. Это пользовательское право не применяется к драйверам устройств Plug and Play.
Создание файла подкачки	Создание файла подкачки. Пользователь с данной привилегией может создавать и изменять размер файла подкачки.
Настройка квот памяти для процесса	Увеличение квоты, назначенной процессу.
Обход перекрестной проверки	Получение уведомлений об изменениях в файлах и директориях. Привилегия также заставляет систему пропустить все перекрестные проверки на доступ. По умолчанию включена для всех пользователей.
Отключение компьютера от стыковочного узла	Отстыковка ноутбука. Пользователь с данной привилегией может отключить портативный компьютер от стыковочного узла, не выполняя вход в систему.
Выполнение задач по обслуживанию томов	Включение привилегий по обслуживанию томов. Необходима для проведения задач по обслуживанию на томе, например, удаленной дефрагментации.
Имитация клиента после проверки пользователя	Имитация клиента. Пользователь с данной привилегией может имитировать другие учетные записи.
Создание глобальных объектов	Создание именованных объектов сопоставления файлов в глобальном пространстве имен во время удаленных терминальных сессий. Привилегия по умолчанию включена для администраторов, сервисов и учетной записи LocalSystem.

9.2 Источники

Источники дополнительной информации приведены в табл. 14.

Таблица 14. Вспомогательная документация

Название	Описание
Руководство администратора SoftControl Service Center	Руководство по работе с инструментами администрирования SoftControl Server и SoftControl Admin Console.

10. Техническая поддержка

При возникновении вопросов по установке, настройке и работе SoftControl SClient вы можете обращаться в техническую поддержку по электронной почте support@safensoft.com.

11. Приложение

11.1 Совместимость с другими продуктами информационной безопасности

SoftControl SysWatch является проактивным средством защиты и может применяться совместно с большинством антивирусов других производителей.

В данной главе приведены инструкции по дополнительным настройкам, которые требуются для обеспечения совместной работы SoftControl SysWatch и следующих продуктов:

- Антивирус Dr.Web® 142.

11.1.1 Антивирус Dr.Web®

Для корректной установки и функционирования SoftControl SysWatch в системе с установленным антивирусом Dr.Web® выполните следующую последовательность действий:

1) Вызовите контекстное меню антивируса Dr.Web®, нажав на его иконку в области уведомлений Windows, и выберите пункт **Инструменты** → **Настройки** (рис. Выбор основных настроек программы 142).

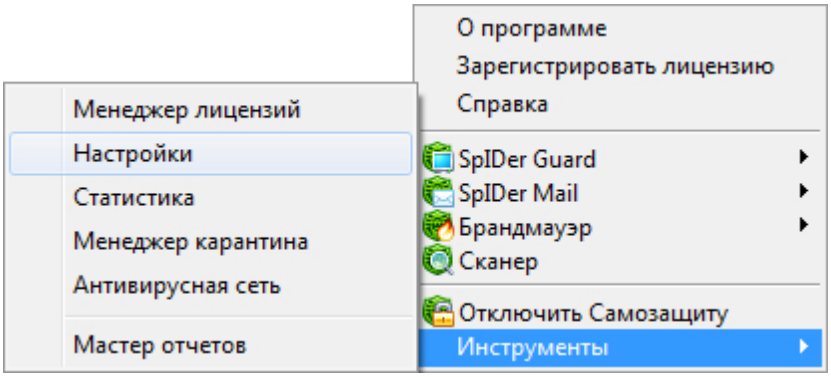

Рисунок 114. Выбор основных настроек программы

2) В окне настроек в категории **Основные** откройте раздел **Превентивная защита** и нажмите на кнопку **Пользовательский** для открытия детальных настроек (рис. Настройки превентивной защиты 142).

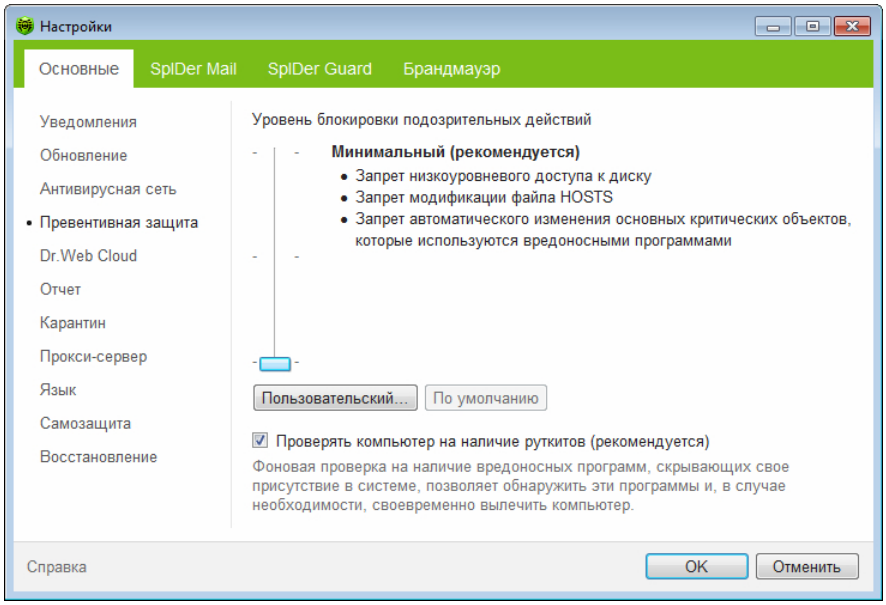

Рисунок 115. Настройки превентивной защиты

3) В окне пользовательских настроек установите переключатели **Автозапуск программ** и **Конфигурация безопасного режима** в положение **Разрешить**, после чего нажмите на кнопку **OK** (рис. Пользовательские настройки превентивной защиты 143).

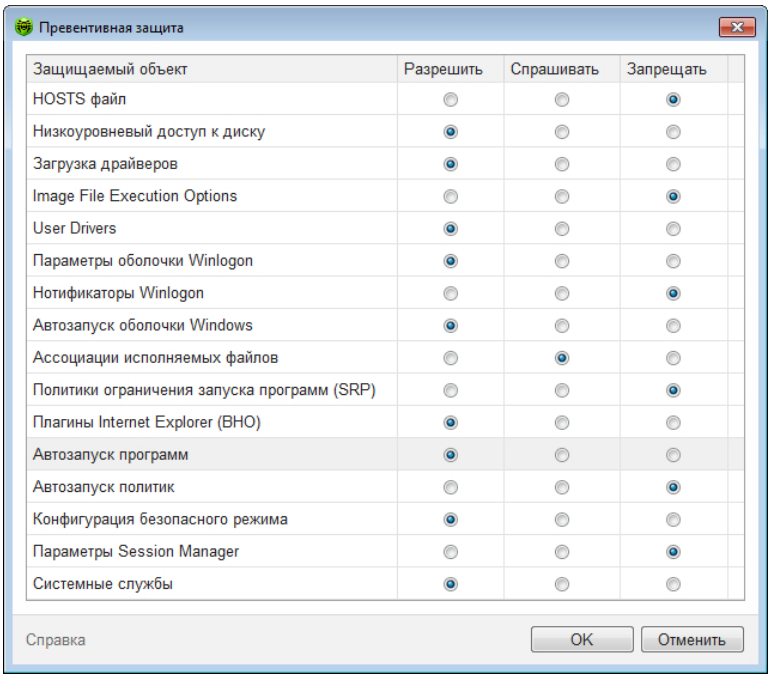

Рисунок 116. Пользовательские настройки превентивной защиты

4) Подтвердите изменения в окне основных настроек, нажав на кнопку **OK** (рис. Настройки превентивной защиты 143).

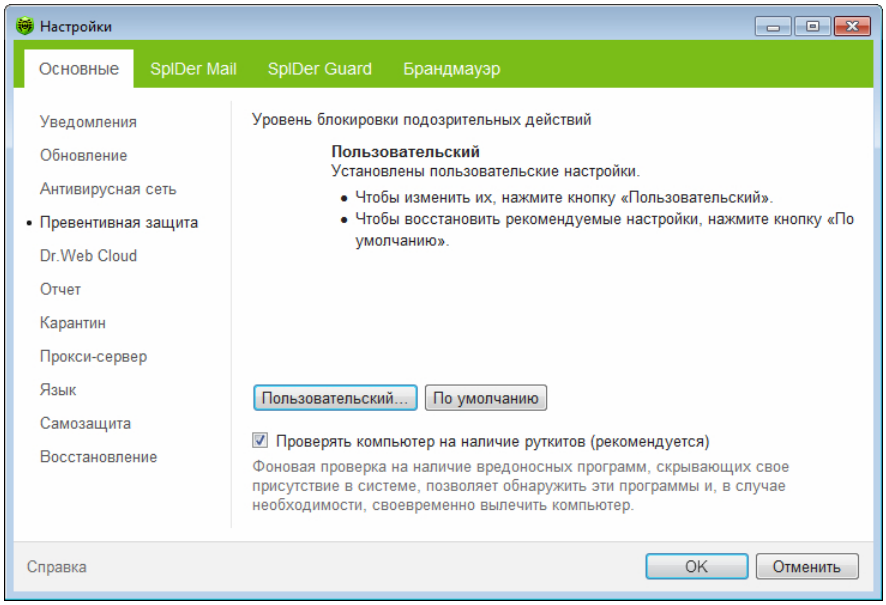

Рисунок 117. Настройки превентивной защиты

5) Выключите компонент защиты SpIDer Guard, выбрав в контекстном меню пункт **SpIDer Guard → Отключить** (рис. Отключение SpIDer Guard [144]).

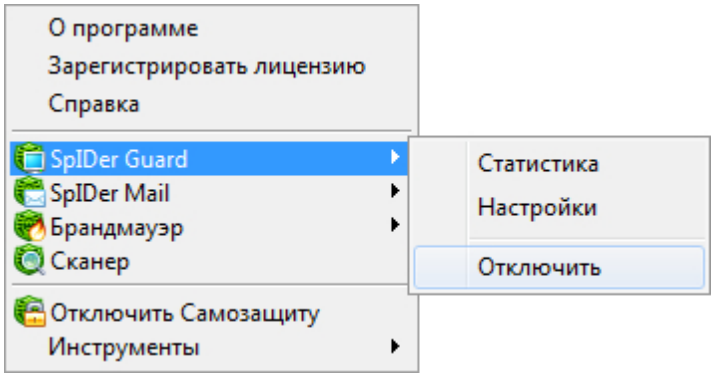

Рисунок 118. Отключение SpIDer Guard

6) Запустите установку SoftControl SysWatch [14].

7) В процессе установки брандмауэр Dr.Web® отобразит уведомление о попытке доступа к сети. Создайте разрешающее правило для исходящих соединений на порт 80 (протокол HTTP), нажав на кнопку **Создать правило** и подтвердив вариант **Применить предустановленное правило** с помощью кнопки **OK** (рис. Уведомление брандмауэра Dr.Web® [144], Создание правила в брандмауэре Dr.Web® [145]).

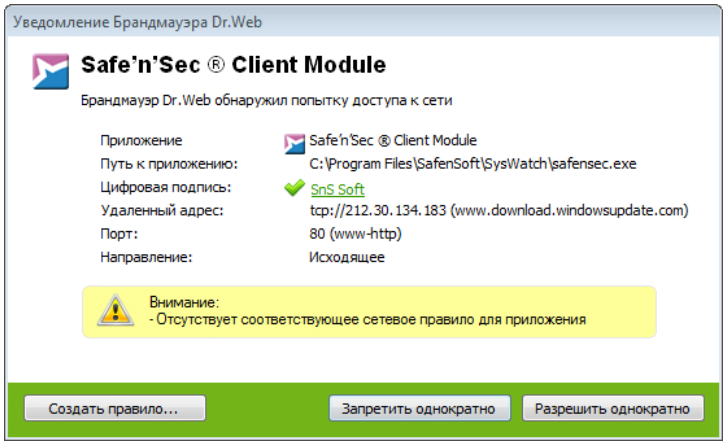

Рисунок 119. Уведомление брандмауэра Dr.Web®

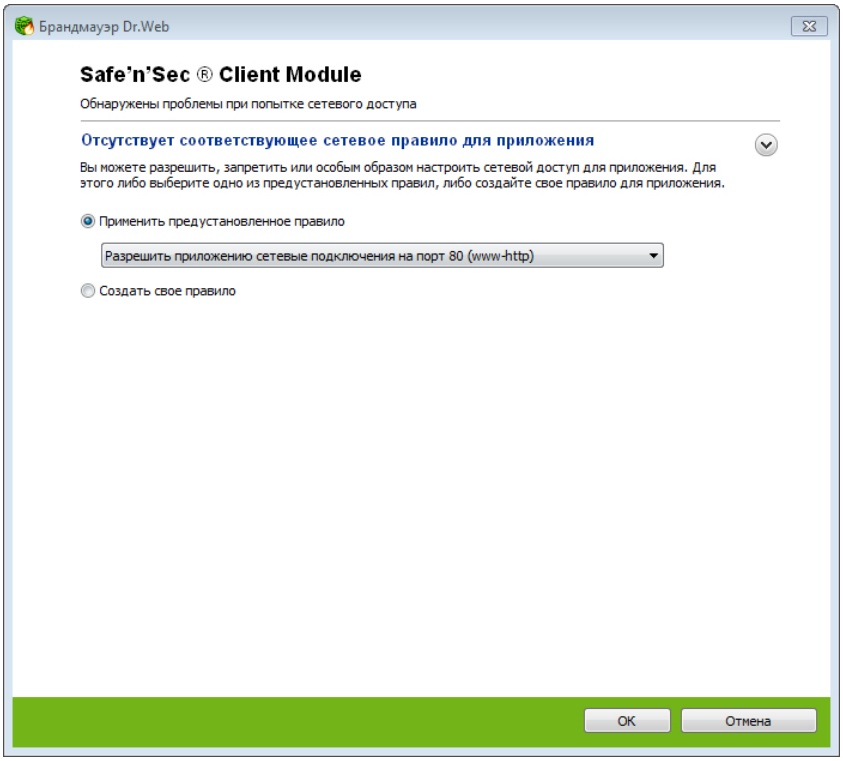

Рисунок 120. Создание правила в брандмауэре Dr.Web®

8) Дождитесь окончания сбора профиля [46] системы, автоматически запускаемого по окончании установки. Не рекомендуется выполнять какие-либо действия на компьютере в процессе сбора профиля.
9) Откройте настройки компонента SplDer Guard, выбрав в контекстном меню пункт **SplDer Guard** → **Настройки** (рис. Настройки SplDer Guard [145]).

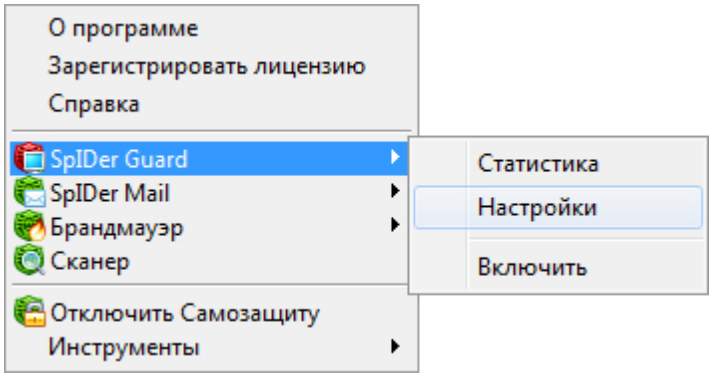

Рисунок 121. Настройки SpIDer Guard

10) В окне настроек в категории **SpIDer Guard** откройте раздел **Исключения**, выберите каталог установки SoftControl SysWatch с помощью кнопки **Обзор** и нажмите на кнопку **Добавить** для его добавления в исключения Dr.Web® (рис. Добавление исключений в SpIDer Guard 146). Нажмите на кнопку **OK** для подтверждения изменений.

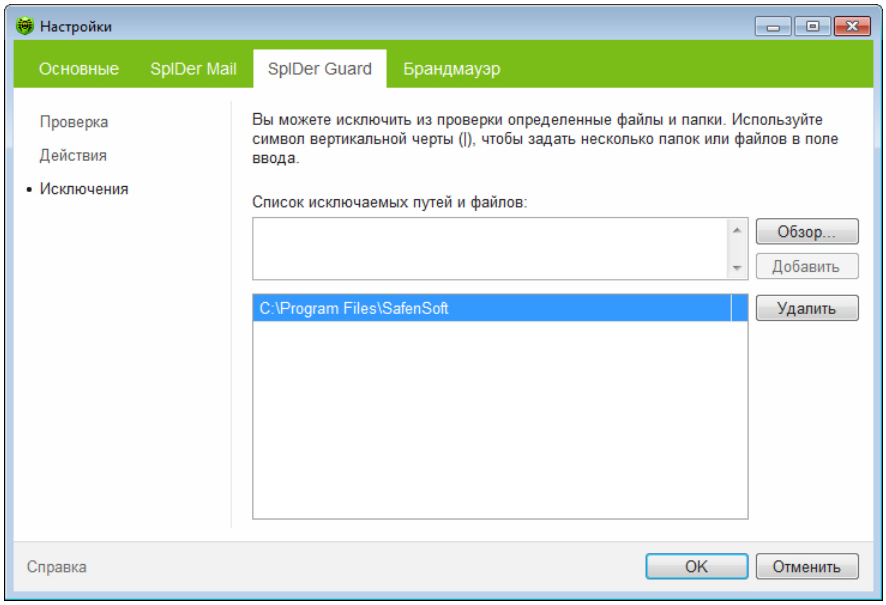

Рисунок 122. Добавление исключений в SpIDer Guard

11) Включите компонент защиты SpIDer Guard, выбрав в контекстном меню пункт **SpIDer Guard** → **Включить** (рис. Включение SpIDer Guard 146).

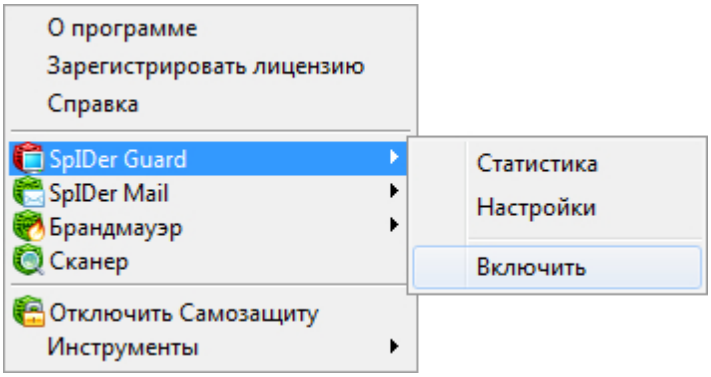

Рисунок 123. Включение SpIDer Guard

12) Откройте список процессов[62] SoftControl SysWatch и в свойствах[65] всех модулей Dr.Web® выставите опцию **Включить режим обновления ПО**.