



SoftControl

ATM Client 6.0.27

Руководство пользователя

Уважаемый пользователь!

ООО «АРУДИТ СЕКЬЮРИТИ» благодарит Вас за то, что выбрали продукт SoftControl ATM Client. 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 ATM Client будет Вам полезен.

АВТОРСКИЕ ПРАВА

Материалы, приведенные в настоящем документе, являются собственностью ООО «АРУДИТ СЕКЬЮРИТИ» и могут быть использованы только для личных целей приобретателя продукта. Запрещается воспроизведение отдельных частей документа, внесение правок, размещение на сетевых ресурсах, распространение в любой форме (в том числе в переводе) на бумажных и электронных носителях, посредством каналов связи и средств массовой информации или каким-либо другим способом без специального письменного разрешения компании и ссылки на источник. Наименования и товарные знаки, приведённые в документе, являются собственностью своих законных владельцев.

ОГРАНИЧЕНИЕ ОТВЕТСТВЕННОСТИ

Содержание данного документа может изменяться без предварительного уведомления. ООО «АРУДИТ СЕКЬЮРИТИ» не несёт ответственности за неточности и/или ошибки, допущенные в данном документе, и возможный ущерб, связанный с этим.

ООО «АРУДИТ СЕКЬЮРИТИ», 2021 г.

Почтовый адрес:

127106, Россия, Москва

Нововладыкинский проезд, дом 8, стр. 3

ООО «АРУДИТ СЕКЬЮРИТИ»

Телефон:

+7 (499) 201-55-12

Электронная почта:

Общие вопросы и предложения: support@sns-control.ru

Коммерческие вопросы: sales@sns-control.ru

Веб-сайт компании: <http://www.sns-control.ru>

Содержание

1. Введение	5
1.1 Назначение.....	5
1.2 Возможности.....	5
1.3 Условные обозначения и термины.....	7
1.3.1 Обозначения.....	7
1.3.2 Сокращения.....	7
1.3.3 Глоссарий.....	7
2. Принцип работы SoftControl SysWatch	10
3. Требования к аппаратному и программному обеспечению	12
3.1 Системные требования SoftControl SysWatch.....	12
4. Установка и настройка SoftControl SysWatch	13
4.1 Локальная установка.....	13
4.1.1 Установка в обычном режиме.....	13
4.1.2 Установка в тихом режиме.....	16
4.1.3 Установка в тихом режиме с применением конфигурационного файла.....	16
4.2 Удаленная установка.....	17
4.2.1 Установка через доменную групповую политику.....	17
4.2.2 Установка с помощью утилиты удаленной инсталляции.....	27
4.2.3 Установка сторонними средствами администрирования.....	32
4.3 Регистрация на сервере.....	32
5. Локальная работа с SoftControl SysWatch	33
5.1 Интерфейс SoftControl SysWatch.....	33
5.1.1 Значок в области уведомлений.....	34
5.1.2 Контекстное меню.....	34
5.1.3 Панель управления.....	35
5.1.4 Настройка интерфейса и оповещений.....	37
5.2 Режимы управления.....	40
5.2.1 Автономный режим.....	41
5.2.2 Удаленное управление с сервера.....	41
5.3 Активация лицензионного ключа.....	43
5.4 Автоматическая настройка (сбор профиля).....	44
5.4.1 Опции сбора профиля.....	45
5.4.2 Запуск по требованию.....	45
5.5 Детальная настройка SoftControl SysWatch.....	48
5.5.1 Опции отслеживания активности.....	50
5.5.2 Обработка инцидентов запуска приложений.....	53

5.5.3	Зоны выполнения приложений.....	58
5.5.4	Белый список сертификатов.....	61
5.5.5	Правила контроля активности.....	63
5.5.5.1	Настройка прав доступа к файловой системе.....	63
5.5.5.2	Настройка прав доступа к системному реестру.....	69
5.5.5.3	Настройка прав доступа к устройствам и портам.....	74
5.5.5.4	Настройка правил сетевой активности.....	78
5.5.5.5	Настройка привилегий процессов.....	84
5.5.5.6	Настройка взаимодействия процессов.....	87
5.6	Отчеты.....	89
5.6.1	Текстовые отчеты.....	89
5.7	Настройка общих параметров программы.....	92
5.7.1	Самозащита системной службы.....	93
5.7.2	Парольная защита.....	94
5.7.3	Отложенный запуск системной службы.....	95
5.7.4	Восстановление БД после аппаратной перезагрузки.....	96
5.8	Сохранение и восстановление настроек.....	97
5.8.1	Выгрузка основного конфигурационного файла.....	97
6.	Расширенные возможности SoftControl SysWatch.....	99
7.	Обновление SoftControl SysWatch.....	100
7.1	Опции обновления.....	100
7.2	Обновление в обычном режиме.....	103
7.3	Обновление в ручном режиме.....	104
8.	Удаление SoftControl SysWatch.....	107
8.1	Локальная деинсталляция.....	107
8.1.1	Удаление в обычном режиме.....	107
8.1.2	Удаление в тихом режиме.....	108
8.2	Удалённая деинсталляция.....	108
8.2.1	Удаление через доменную групповую политику.....	108
8.2.2	Удаление сторонними средствами администрирования.....	110
9.	Техническая поддержка.....	112

1. Введение

1.1 Назначение

SoftControl ATM Client (далее по тексту – SoftControl SysWatch) предназначен для защиты от несанкционированного доступа к информационным ресурсам компьютеров, 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 принима-

ет 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.

▪ **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 защищаемых устройствах с помощью средств администрирования.

Кроме того, SoftControl SysWatch поддерживает совместную работу со сторонними антивирусами. Интеграция SoftControl SysWatch со сторонними антивирусами осуществляется по запросу заказчика.

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.
<u>Условие</u>	Условие выполнения, примечание, пример.
Обновить	– заголовки и сокращения; – названия экранных кнопок, ссылок, пунктов меню, других элементов программного интерфейса.
<i>Политика контроля</i>	– 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.
<u>Приложение</u> ⁷	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;
- ❖ 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 актив-

	ности 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 ис-

	полняемых 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](#)⁴⁴) 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](#)⁵⁸ (доверенная, ограниченная, запрещенная). После сбора профиля всем приложениям в нем назначается доверенная зона.

[Детальная настройка SoftControl SysWatch](#)⁴⁸, в том числе выбор режима обработки инцидентов безопасности ([ручной](#)⁵⁵ или [автоматический](#)⁵⁴), и задание [правил контроля активности](#)⁶³ осуществляется пользователем после сбора профиля.

Профиль работает следующим образом (см. схему [ниже](#)⁵³). 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](#)⁶³. Приложения из запрещенной зоны блокируются. Если приложения нет в профиле, оно считается потенциально опасным, и дальнейшие действия зависят от выбранных настроек.

Для инсталляторов выполняется 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](#)⁶¹, 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. Все [правила контроля активности](#)⁽⁶³⁾, действующие для данной зоны, распространяются и на инсталляторы.

Приложениям из ограниченной зоны можно назначить 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:				
Microsoft® Windows® XP (SP2) 32-разрядная	800 МГц	512 МБ	150 МБ	
Microsoft® Windows® XP (SP3) 32-разрядная	800 МГц	512 МБ		
Microsoft® Windows® XP (SP2) 64-разрядная	800 МГц	512 МБ		
Microsoft® Windows® XP Embedded (SP2 и выше) 32-разрядная	800 МГц	256 МБ		
Microsoft® Windows® Embedded for Point of Service 1.0 32-разрядная	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		
Microsoft® Windows® 10 IoT Enterprise 32-разрядная	1 ГГц	1 ГБ		
Microsoft® Windows® 10 IoT Enterprise 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	2 ГБ		

4. Установка и настройка SoftControl SysWatch

SoftControl SysWatch может быть установлен на клиентские хосты как [локально](#)⁽¹³⁾, так и одним из [удаленных централизованных](#)⁽¹⁷⁾ 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](#)⁽³²⁾ 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 \(с использованием интерфейса пользователя\)](#)⁽¹³⁾;
- [в тихом режиме](#)⁽¹⁶⁾;
- [в тихом режиме с применением конфигурационного файла](#)⁽¹⁶⁾.

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](#)⁽¹³⁾).

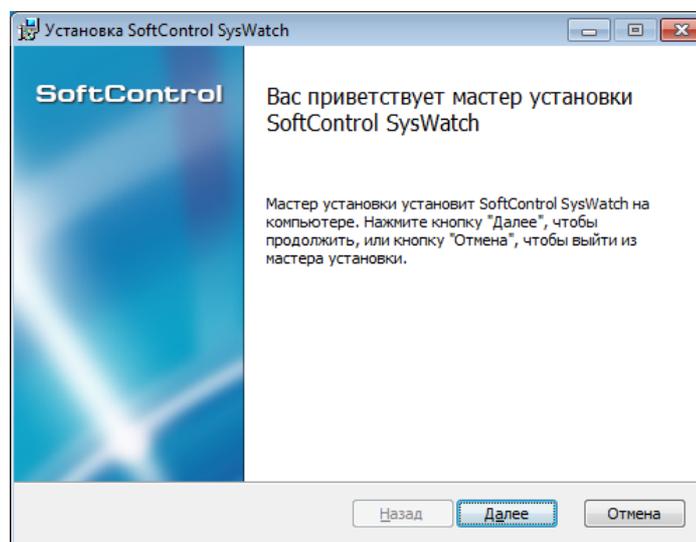


Рисунок 1. Запуск программы установки

- 3) В случае вашего согласия, выберите параметр **Я принимаю условия лицензионного соглашения** и нажмите на кнопку **Далее**.
- 4) Выберите каталог для установки SoftControl SysWatch (с помощью кнопки **Изменить**) и нажмите на кнопку **Далее** (рис. [Путь установки](#)⁽¹⁴⁾).

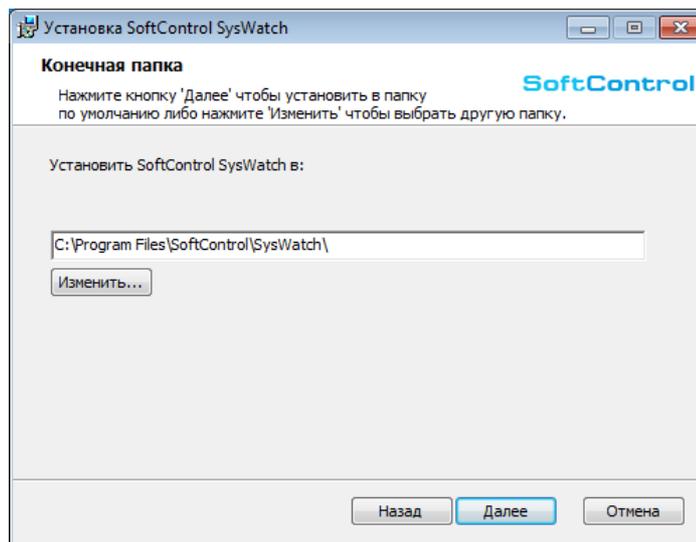


Рисунок 2. Путь установки

- 5) По умолчанию после установки SoftControl SysWatch начинает сбор профиля системы (рис. [Включение сбора профиля](#)⁽¹⁴⁾). 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](#)⁽⁴⁵⁾).

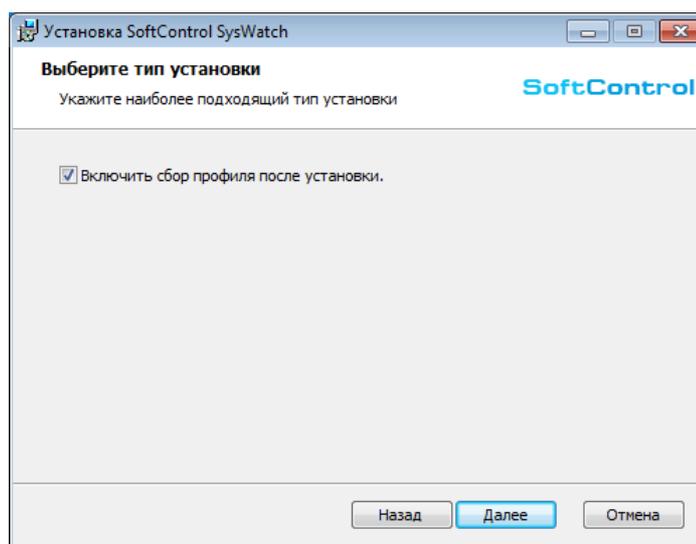


Рисунок 3. Включение сбора профиля

- 6) Нажмите на кнопку **Установить** (рис. [Готовность к установке](#)⁽¹⁴⁾).

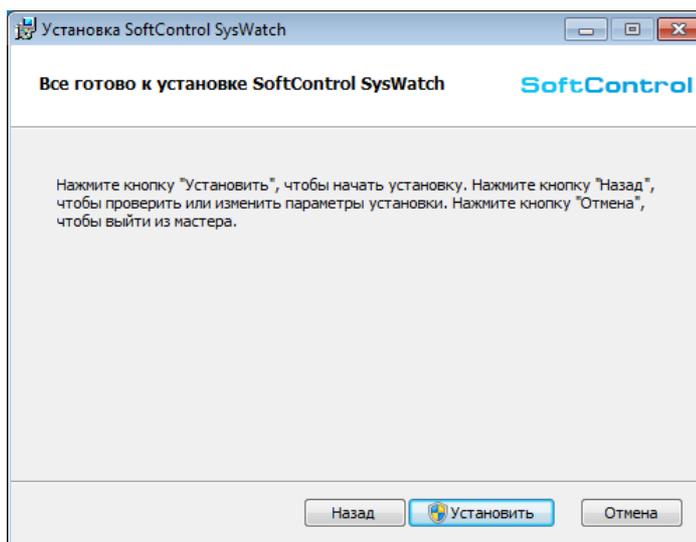


Рисунок 4. Готовность к установке

7) Дождитесь окончания процесса установки (рис. [Процесс установки](#)⁽¹⁵⁾).

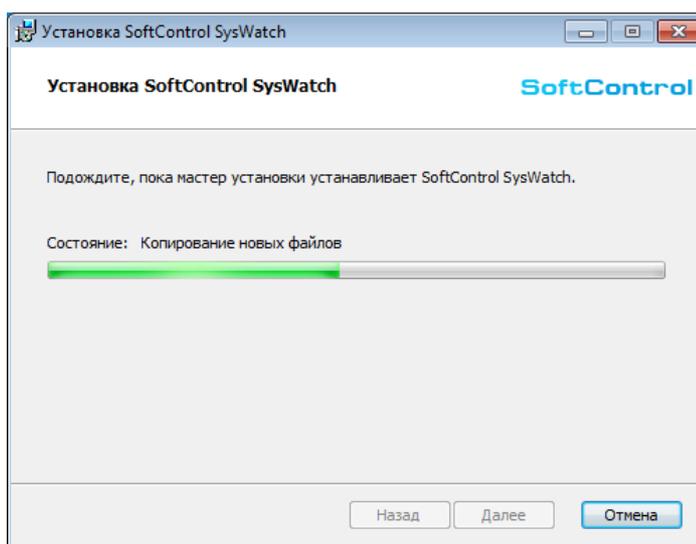


Рисунок 5. Процесс установки

8) После появления сообщения *Установка SoftControl SysWatch завершена* нажмите на кнопку **Готово** (рис. [Завершение установки](#)⁽¹⁵⁾).

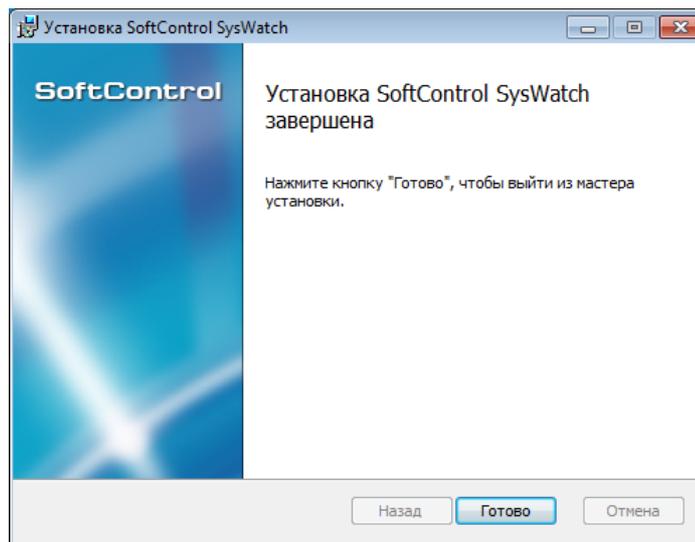


Рисунок 6. Завершение установки

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
```

В случае успеха `msiexec.exe` завершит работу с кодом возврата 0. В противном случае код возврата будет иметь другое значение. Подробнее см. <https://docs.microsoft.com/ru-ru/windows/win32/msi/error-codes>.

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](#)⁹⁷, в примере ниже – *Storage.xmlc*) или файл настроек с [параметрами подключения к управляющему серверу](#)⁴² (*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](#)⁽⁴¹⁾ по окончании установки.

В случае успеха msiexec.exe завершит работу с кодом возврата 0. В противном случае код возврата будет иметь другое значение. Подробнее см. <https://docs.microsoft.com/ru-ru/windows/win32/msi/error-codes>.

4.2 Удаленная 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](#)⁽¹⁷⁾;
- [с помощью утилиты удаленной инсталляции](#)⁽²⁷⁾;
- [сторонними средствами администрирования](#)⁽³²⁾.

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](#)⁽¹⁷⁾).

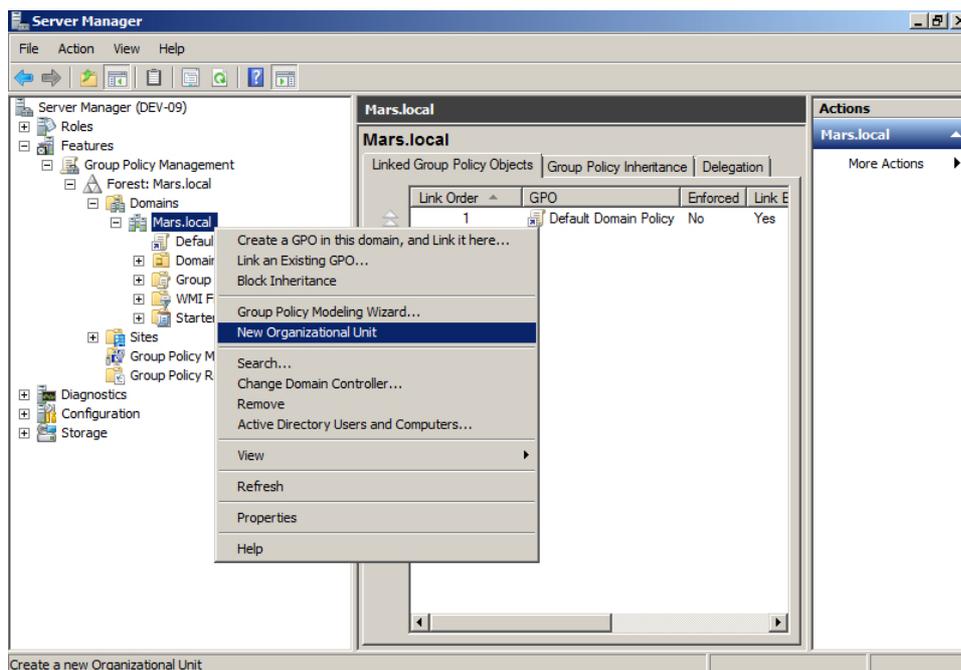


Рисунок 7. Создание нового подразделения домена

- 3) В диалоговом окне **New Organizational Unit** задайте имя (**Name**) нового подразделения и нажмите на кнопку **OK** (рис. [Задание имени подразделения](#)⁽¹⁸⁾).

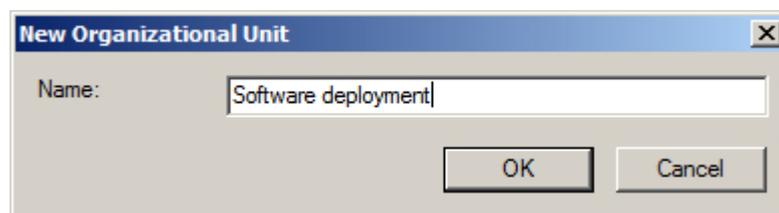


Рисунок 8. Задание имени подразделения

- 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](#)⁽¹⁸⁾).

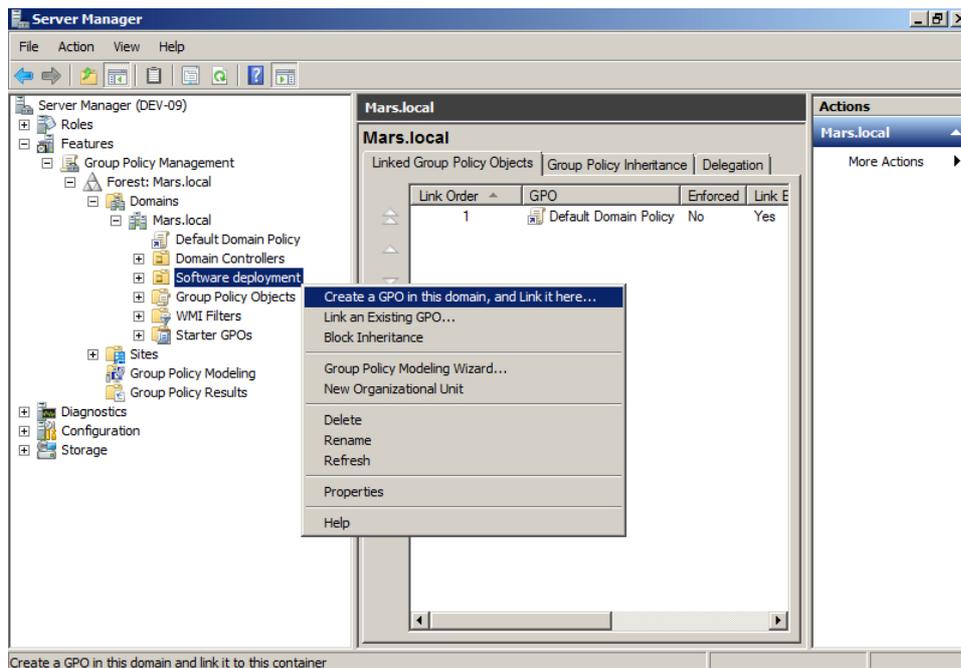


Рисунок 9. Создание нового объекта групповой политики

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](#)¹⁹).

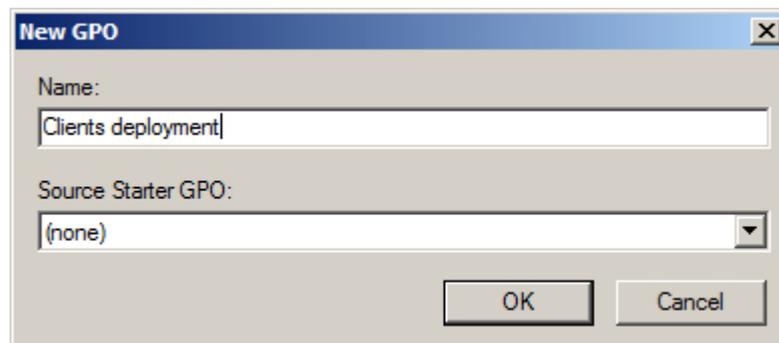


Рисунок 10. Задание имени и начального объекта групповой политики

6) Разверните созданное подразделение, вызовите контекстное меню созданного объекта групповой политики и выберите пункт **Edit** (рис. [Редактирование объекта групповой политики](#)¹⁹).

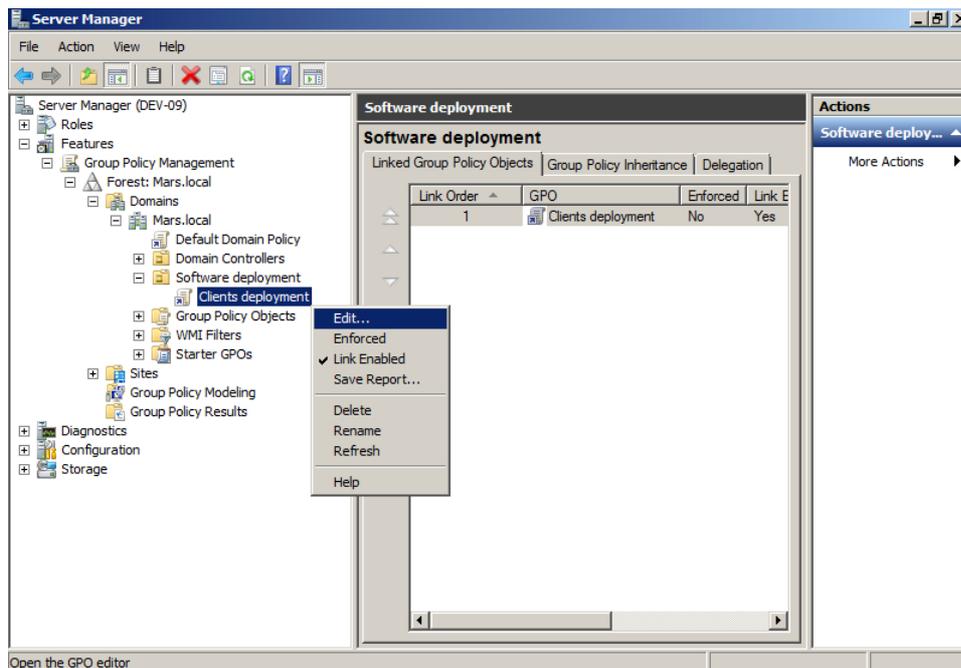


Рисунок 11. Редактирование объекта групповой политики

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](#)⁽²⁰⁾).

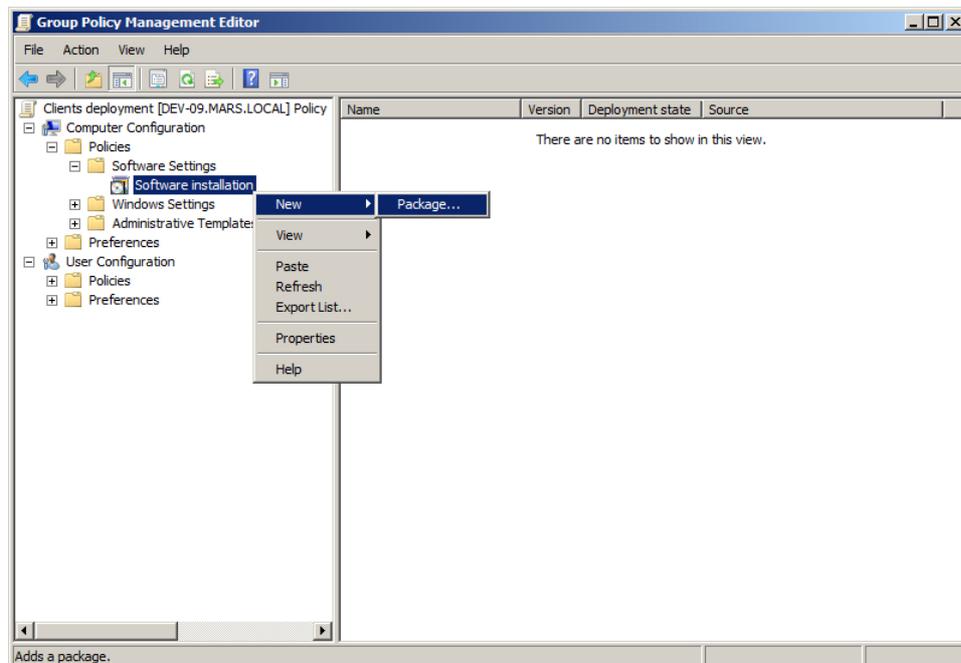


Рисунок 12. Добавление нового пакета установки

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

ный на сетевом ресурсе, доступном для клиентских хостов, на которые предполагается произвести установку, и нажмите на кнопку **Open** (Открыть) (рис. [Выбор пакета установки](#)⁽²¹⁾).

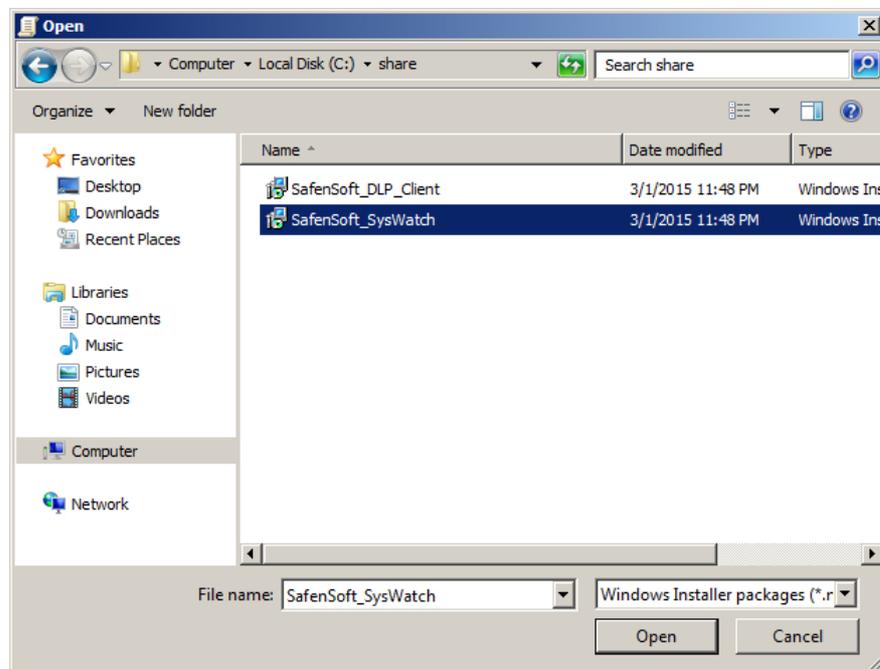


Рисунок 13. Выбор пакета установки

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](#)⁽²¹⁾).

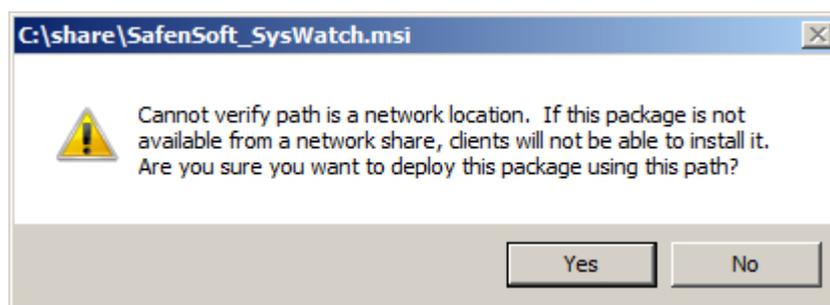


Рисунок 14. Предупреждение при выборе местонахождения пакета установки

10) В диалоговом окне **Deploy Software** выберите метод развертывания **Assigned** и нажмите на кнопку **OK** (рис. [Выбор метода развертывания приложения](#)⁽²¹⁾).

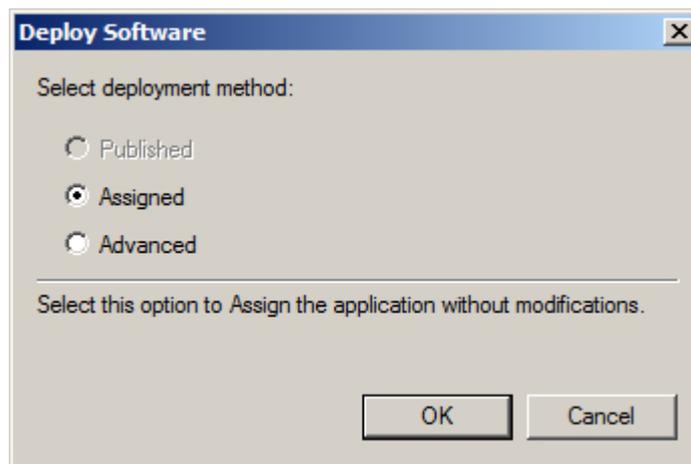


Рисунок 15. Выбор метода развёртывания приложения

- 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 развёртывания приложений](#)⁽²²⁾).

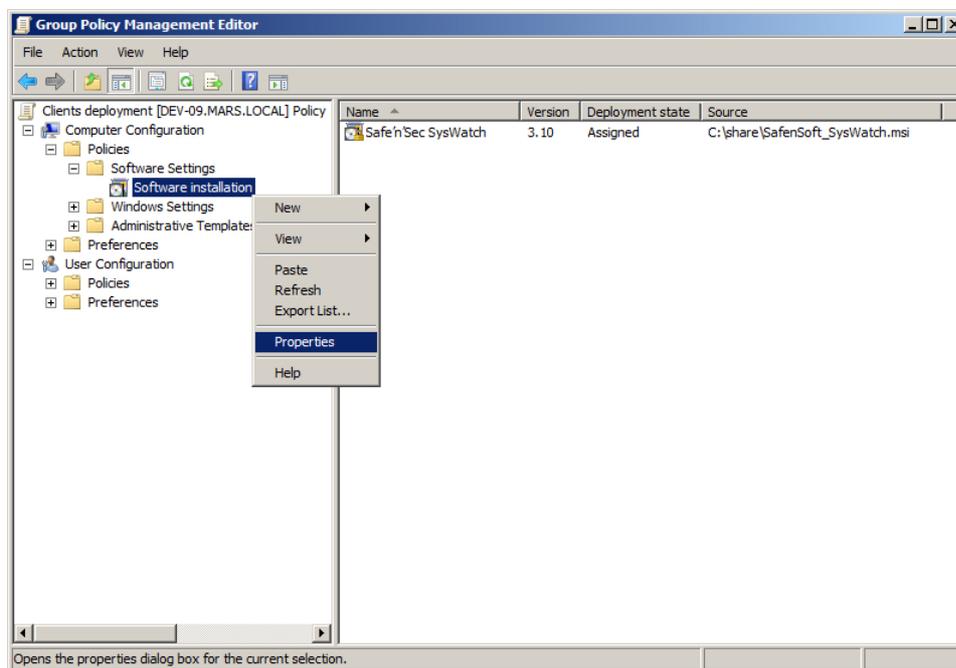


Рисунок 16. Изменение свойств развёртывания приложений

- 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](#)⁽²³⁾). Для вступления изменений в силу нажмите на кнопку **ОК**.

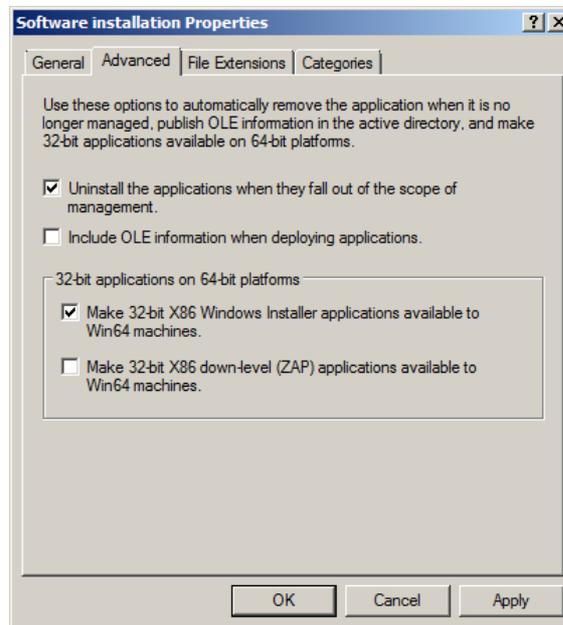


Рисунок 17. Свойства развёртывания приложений

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](#)⁽²³⁾).

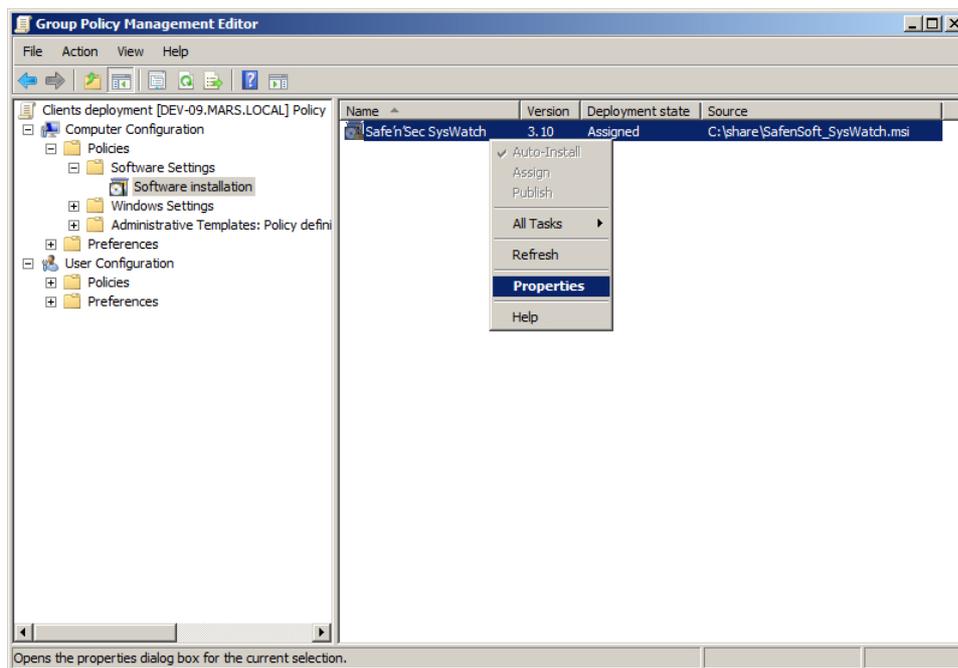


Рисунок 18. Изменение свойств развёртывания конкретного приложения

- 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 развёртывания конкретного приложения](#)⁽²⁴⁾).

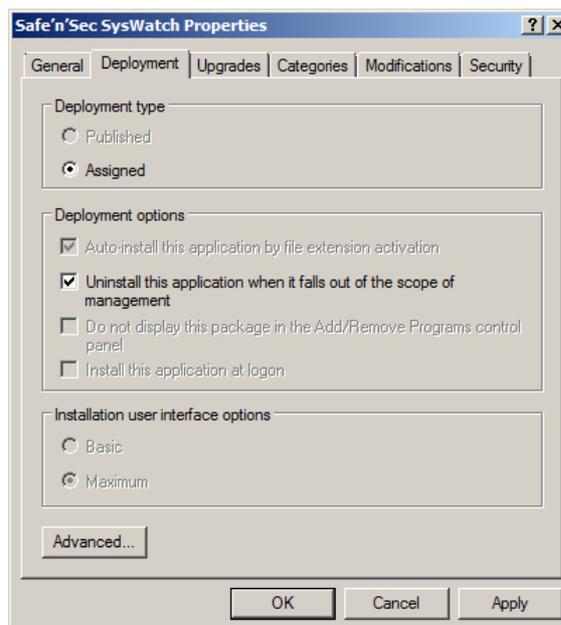


Рисунок 19. Свойства развёртывания конкретного приложения

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

жок **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](#)⁽²⁵⁾). Для вступления изменений в силу нажмите на кнопку **ОК** в обоих окнах настройки.

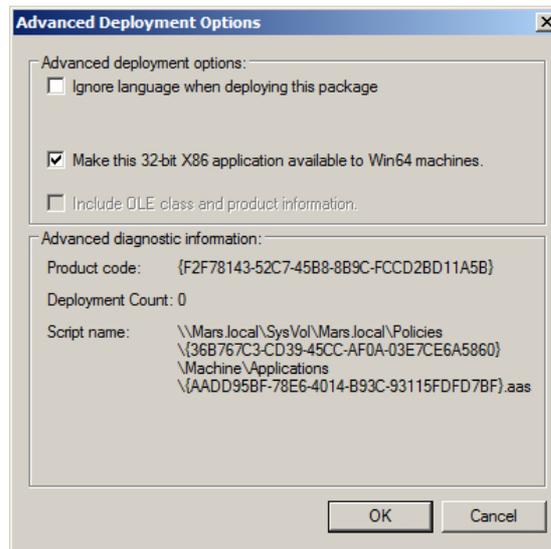


Рисунок 20. Дополнительные свойства

- 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](#)⁽²⁵⁾).

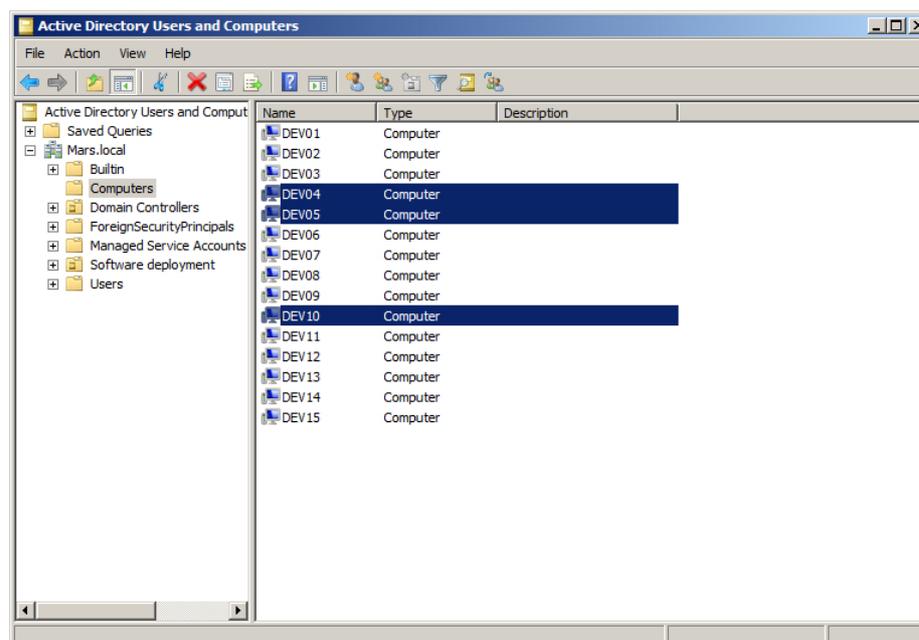


Рисунок 21. Перечень хостов домена

- 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](#)⁽²⁶⁾).

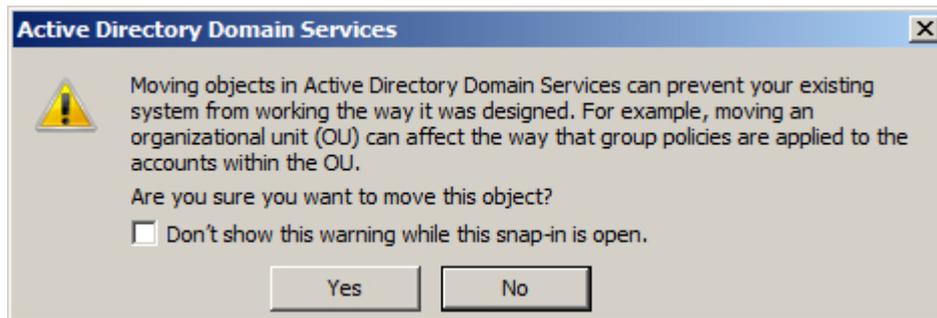


Рисунок 22. Предупреждение при переносе хостов в другое подразделение

- 18) Откройте раздел **Software deployment** и убедитесь, что необходимые клиентские хосты расположены в перечне компьютеров данного подразделения (рис. [Перечень хостов подразделения](#)⁽²⁶⁾).

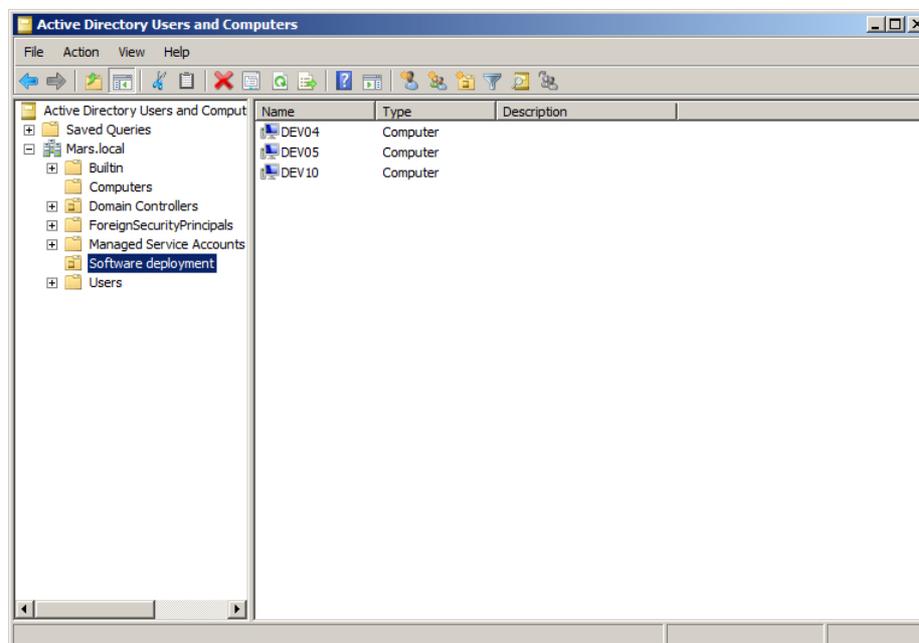


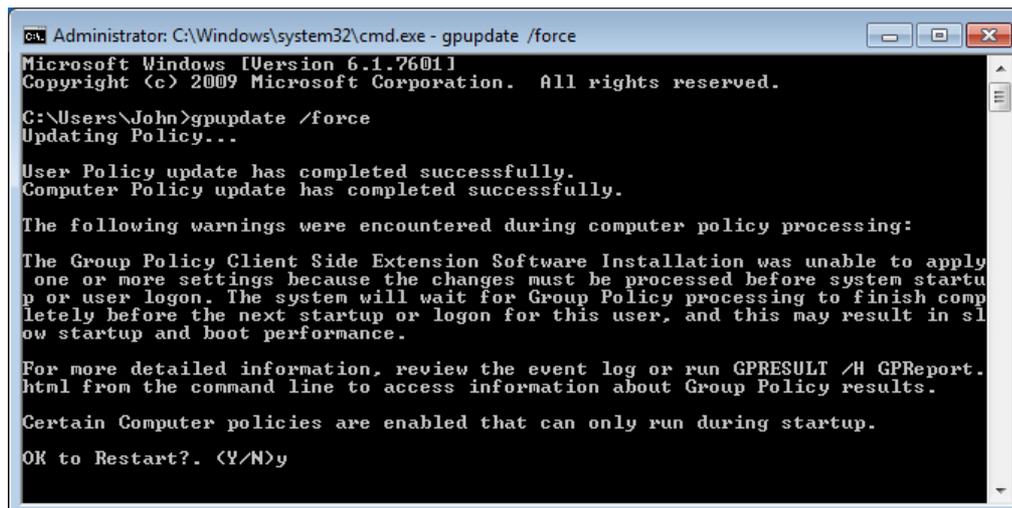
Рисунок 23. Перечень хостов подразделения

- 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](#)⁽²⁷⁾).



```
Administrator: C:\Windows\system32\cmd.exe - gpupdate /force
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\John>gpupdate /force
Updating Policy...

User Policy update has completed successfully.
Computer Policy update has completed successfully.

The following warnings were encountered during computer policy processing:

The Group Policy Client Side Extension Software Installation was unable to apply
one or more settings because the changes must be processed before system startu
p or user logon. The system will wait for Group Policy processing to finish comp
pletely before the next startup or logon for this user, and this may result in sl
ow startup and boot performance.

For more detailed information, review the event log or run GPRESULT /H GPreport.
html from the command line to access information about Group Policy results.

Certain Computer policies are enabled that can only run during startup.

OK to Restart?. <Y/N>y
```

Рисунок 24. Ручное обновление групповой политики

4.2.2 Установка с помощью утилиты удаленной 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 *srvimp.exe* предназначена для удаленной установки клиентских приложений ООО «АРУДИТ СЕКЬЮРИТИ». Утилиту можно скачать по следующему адресу: http://updates.safensoft.com/<номер_лицензии>/39/TOOLS/srvimp.exe.

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 **Учетные записи пользователей** → **Изменение параметров контроля учетных записей** (User Accounts → Change 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 **ОК**.
 - 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 `svrrip`

Параметр	Описание
<code>-h</code>	Краткая справка по принимаемым параметрам.
<code>-i</code>	Перевод в режим установки. Требует задания обязательных ключей и их значений, описанных ниже.
<code>--login=<имя></code>	Имя пользователя, имеющего права администратора на удаленном хосте.
<code>--password=<пароль></code>	Пароль пользователя, имеющего права администратора на удаленном хосте.
<code>--client="<путь к установщику>"</code>	Путь к пакету установки SoftControl SysWatch. Если файл расположен в каталоге, откуда вызывается утилита, допускается указывать только имя файла (без кавычек).
<code>--config="<путь к файлу конфигурации>"</code>	Путь к конфигурационному файлу настроек соединения с управляющим сервером. Требуется для автоматической подачи запроса на регистрацию ³² на сервере SoftControl Server после окончания установки. Если файл расположен в каталоге, откуда вызывается утилита, допускается указывать только имя файла (без кавычек).
<code>--hostnames=<имя 1> <имя 2>...<имя N></code>	Список имен удаленных хостов, на которые требуется произвести установку, разделенных пробелами.

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

```
svrrip -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](#)⁽⁴¹⁾ в настройках программы.
- 2) [Примените закодированный конфигурационный файл](#)⁽⁴²⁾ 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](#)⁽³⁴⁾ (поз. 1 на рис. [ниже](#)⁽³³⁾);
- [Контекстное меню](#)⁽³⁴⁾ (поз. 2 на рис. [ниже](#)⁽³³⁾);
- [Панель управления](#)⁽³⁵⁾ (поз. 3 на рис. [ниже](#)⁽³³⁾).

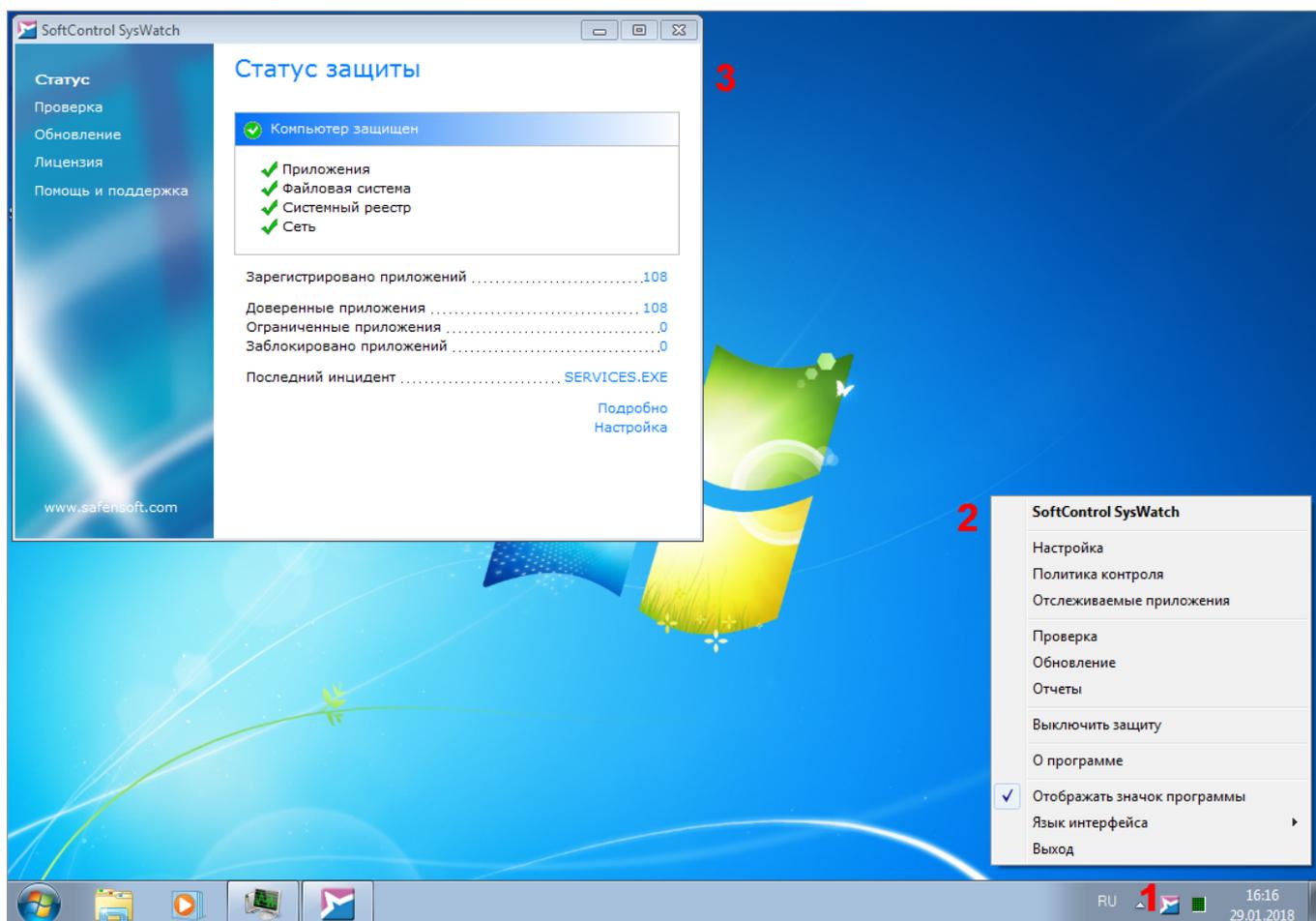


Рисунок 25. Элементы интерфейса программы

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.

Также значок обеспечивает доступ к остальным элементам ГИП приложения – [контекстному меню](#)⁽³⁴⁾ и [панели управления](#)⁽³⁵⁾:

- 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](#)⁽³⁴⁾, описание пунктов – в табл. 5.

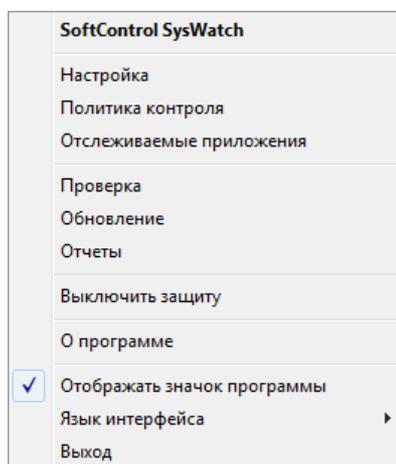


Рисунок 26. Контекстное меню SoftControl SysWatch

Таблица 5. 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.

Пункт меню	Действие
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**, **Обновление**, **Лицензия**, **Помощь и поддержка**.

На вкладке **Статус** отображается текущий статус защиты (рис. [Вкладка «Статус»](#)⁽³⁵⁾). Детальное описание работы с вкладкой приведено в разделе [Детальная настройка SoftControl SysWatch](#)⁽⁴⁸⁾.

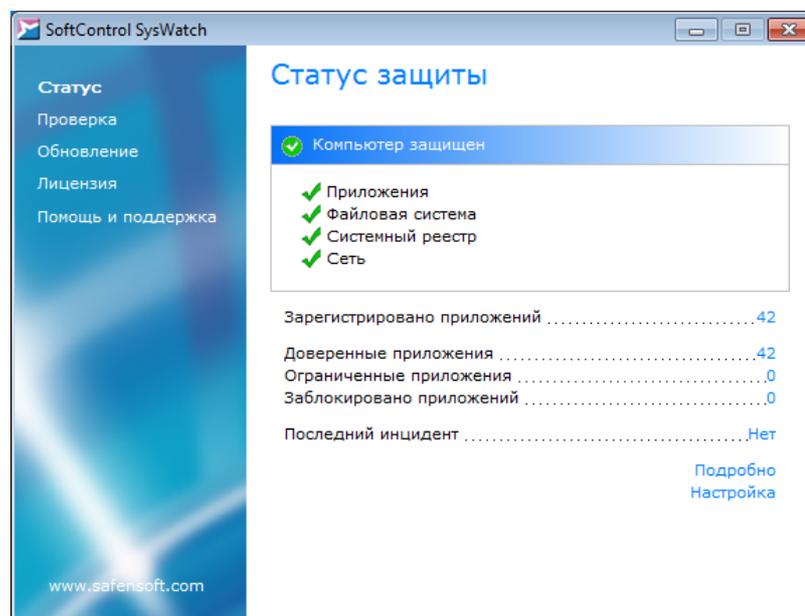


Рисунок 27. Вкладка "Статус"

На вкладке **Обновление** находится информация по наличию [обновлений программных модулей](#)⁽¹⁰⁰⁾ (рис. [Вкладка «Обновление»](#)⁽³⁵⁾).

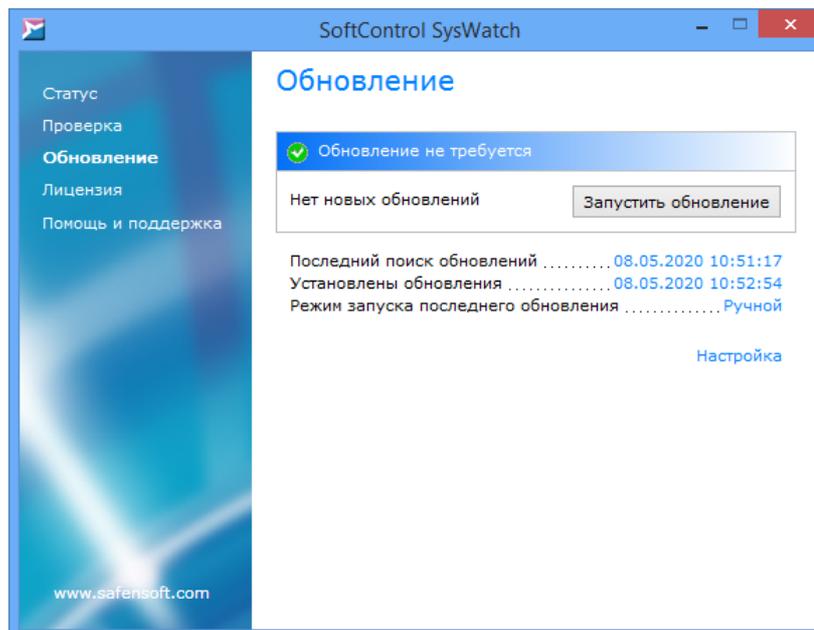


Рисунок 28. Вкладка "Обновление"

Вкладка **Лицензия** содержит данные по используемому [лицензионному ключу](#)⁽⁴³⁾ и компонентам программы (рис. [Вкладка «Лицензия»](#)⁽³⁶⁾).

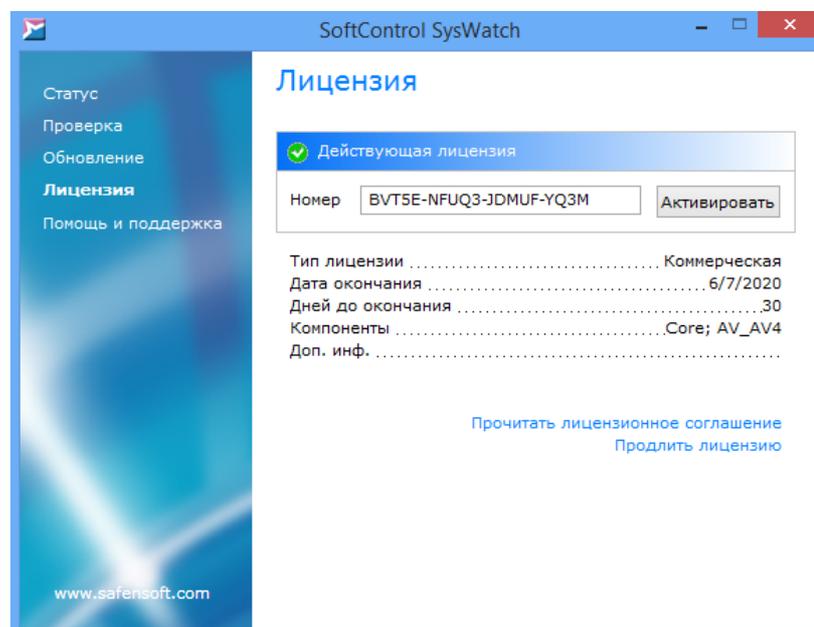


Рисунок 29. Вкладка "Лицензия"

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](#)⁽¹¹²⁾. Внешний вид вкладки представлен на рис. [Вкладка «Помощь и поддержка»](#)⁽³⁶⁾.

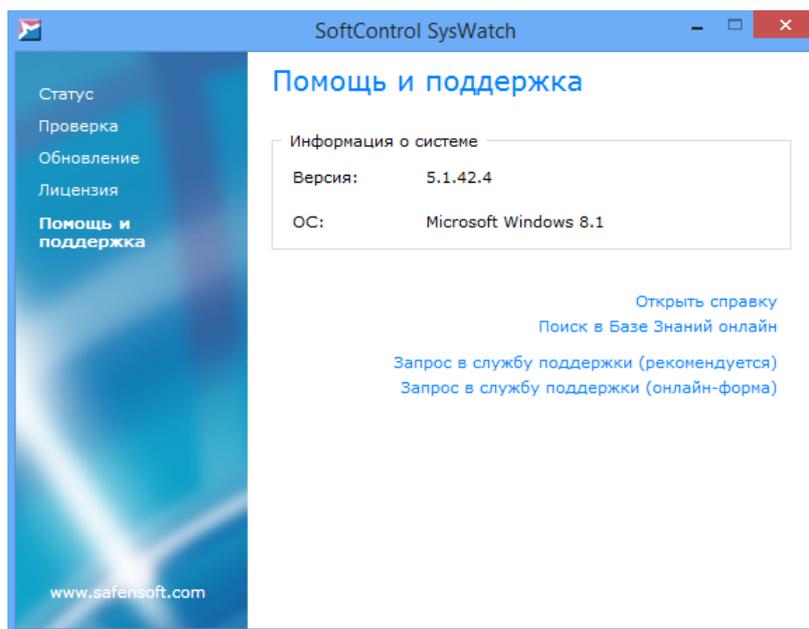


Рисунок 30. Вкладка "Помощь и поддержка"

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](#)⁽³⁷⁾).

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

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

Установите флажок **Показывать значок программы в области уведомлений** для отображения [значка](#)⁽³⁴⁾.

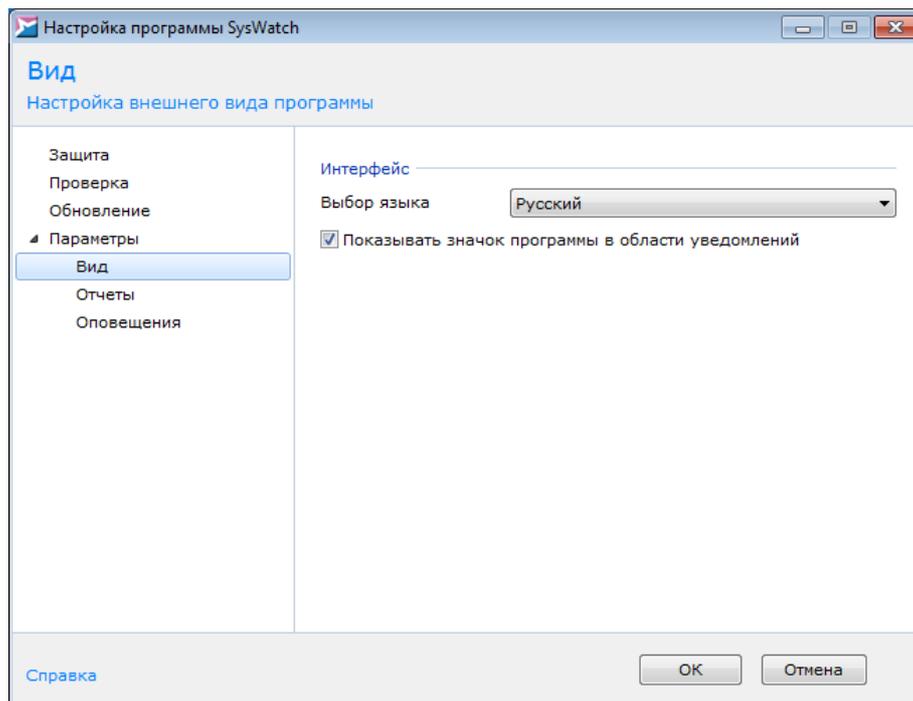


Рисунок 31. Настройка интерфейса

Если вы снимете флажок **Показывать значок программы в области уведомлений**, вы не сможете вызвать контекстное меню. Чтобы открыть панель управления, дважды нажмите левой кнопкой мыши по иконке SoftControl SysWatch  на рабочем столе.

▼ 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](#)⁽³⁸⁾).

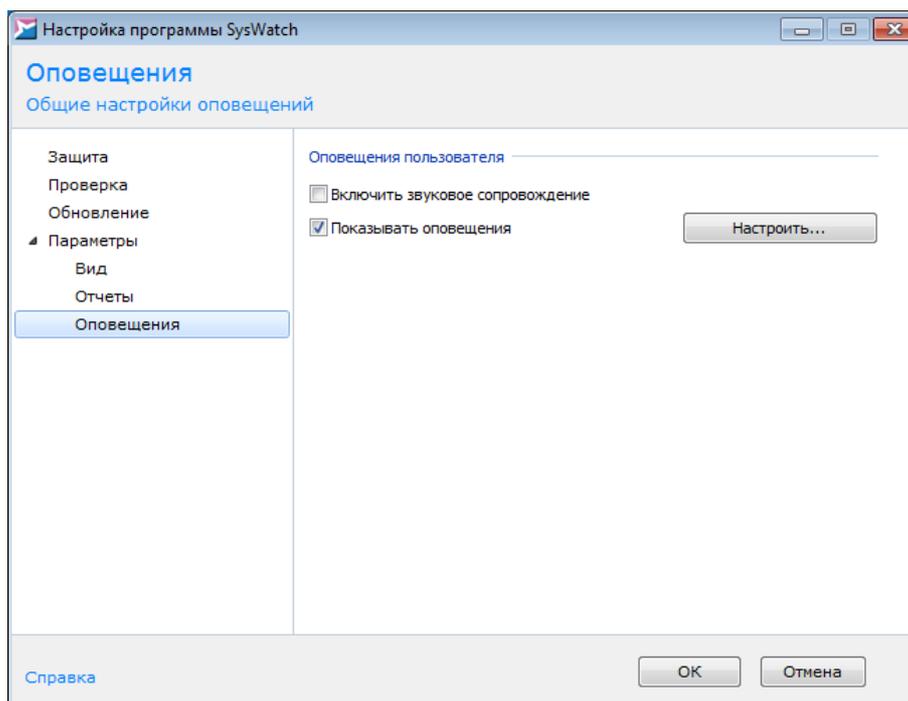


Рисунок 32. Настройка оповещений

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](#)³⁹):

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

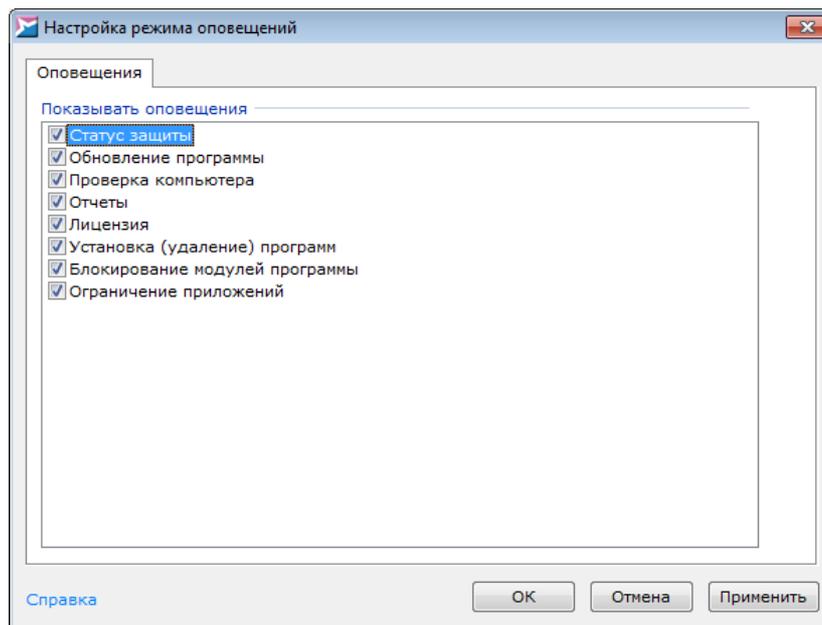


Рисунок 33. Настройка типов событий для оповещения

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

5.2 Режимы управления

Возможны следующие варианты управления работой SoftControl SysWatch:

- [Автономный режим](#)⁽⁴¹⁾;
- [Удаленное управление с сервера](#)⁽⁴¹⁾.

Чтобы установить необходимый режим, откройте настройки программы, перейдите в раздел **Параметры** и выберите требуемый вариант в области **Удаленное управление** (рис. [Настройки параметров программы](#)⁽⁴⁰⁾). Для вступления изменений в силу нажмите на кнопку **ОК**.

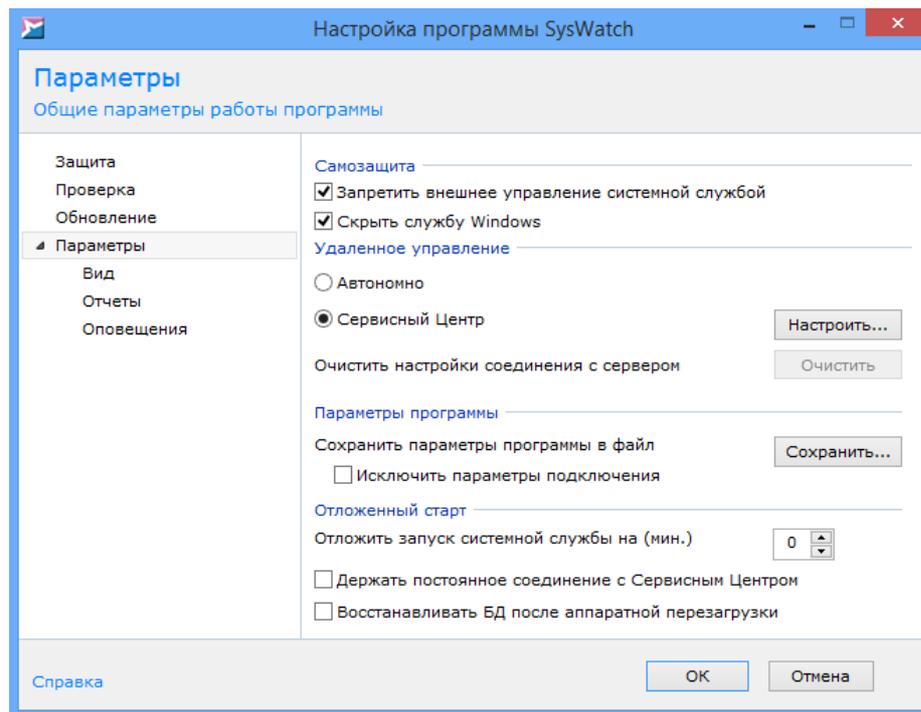


Рисунок 34. Настройки параметров программы

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](#)⁽⁴⁰⁾).

5.2.2 Удаленное 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](#)⁽⁴⁰⁾) и нажмите на кнопку **Настроить**, чтобы открыть окно с подробными настройками подключения к серверу (рис. [Параметры подключения к серверу](#)⁽⁴²⁾).

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](#)⁽⁴²⁾).
- 3) В появившемся окне выберите ранее скопированный файл *ClientSettings.xmlc* и нажмите на кнопку **Открыть**.

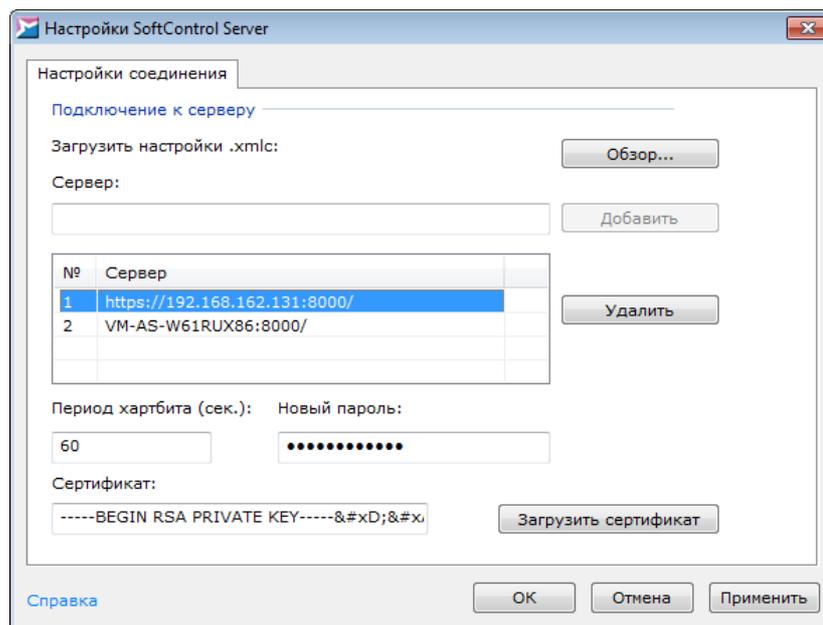


Рисунок 35. Параметры подключения к серверу

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](#)⁽⁴²⁾).

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](#)⁴⁰). В окне с предупреждением выберите вариант **Да** (рис. [Предупреждение при очистке параметров подключения к серверу](#)⁴³).

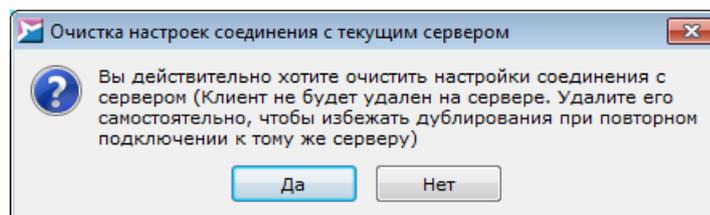


Рисунок 36. Предупреждение при очистке параметров подключения к серверу

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.

Типы лицензий SoftControl SysWatch описаны в табл. 6.

Таблица 6. 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](#)⁽³⁵⁾ 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](#)⁽¹⁰⁰⁾. 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](#)⁽⁴⁵⁾). 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](#)⁽¹⁴⁾). Предполагается, что перед началом сбора профиля система не содержит вредоносных объектов.

Перед началом [сбора профиля по требованию](#)⁽⁴⁵⁾ выполните [настройку его параметров](#)⁽⁴⁵⁾.

5.4.1 Опции сбора профиля

Для настройки параметров сбора профиля откройте раздел **Защита** настроек программы, в области **Режим защиты** нажмите на кнопку **Настроить**.

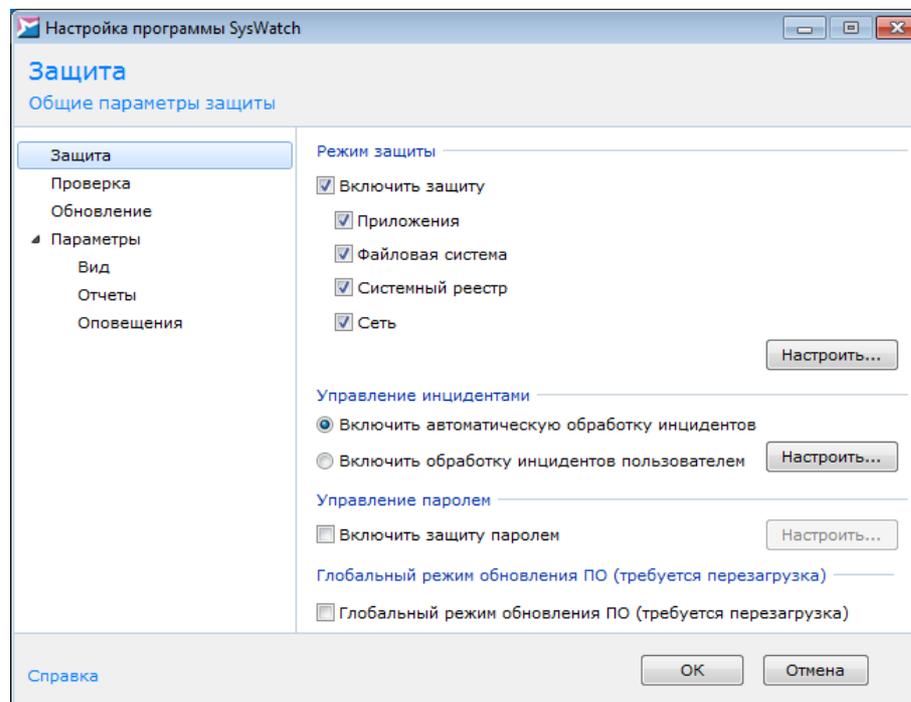


Рисунок 37. Настройки общих параметров защиты

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**.

i Во время автоматической настройки нежелательно выполнять установку ПО в системе.

Если необходимо прервать сбор профиля, нажмите на кнопку **Остановить** (рис. [Процесс сбора профиля](#)⁽⁴⁵⁾).

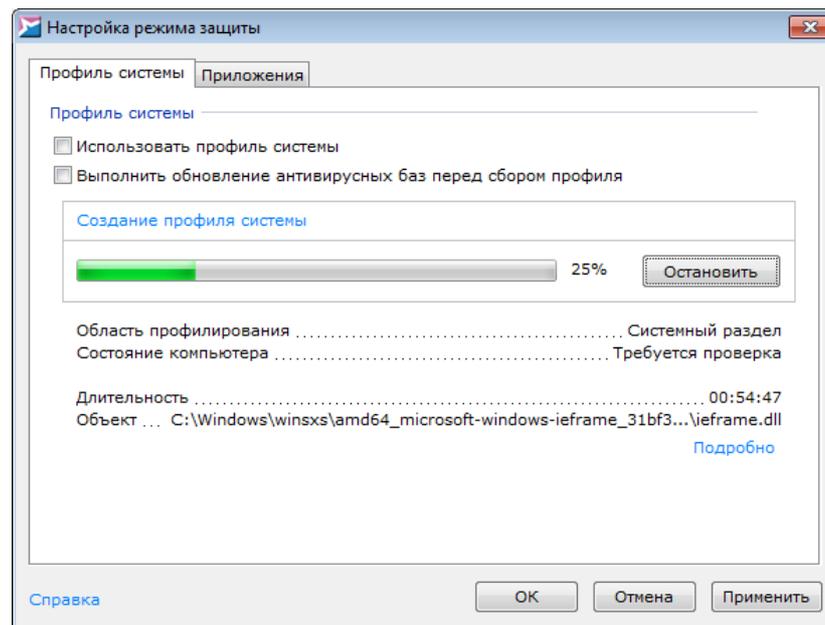


Рисунок 38. Процесс сбора профиля

В диалоговом окне выберите, сохранять ли накопленную информацию о файлах для использования при продолжении сбора профиля (рис. [Выбор режима прерывания сбора профиля](#)⁴⁶⁾). При выборе варианта **Да** вы сможете продолжить сбор профиля с того места, где он был прерван.

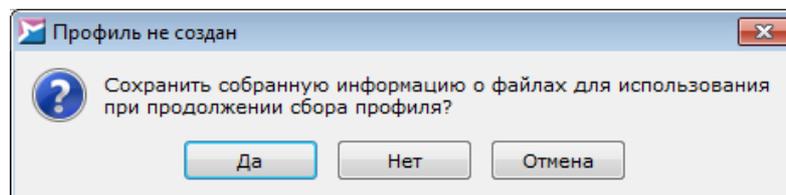


Рисунок 39. Выбор режима прерывания сбора профиля

i 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.

i 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.

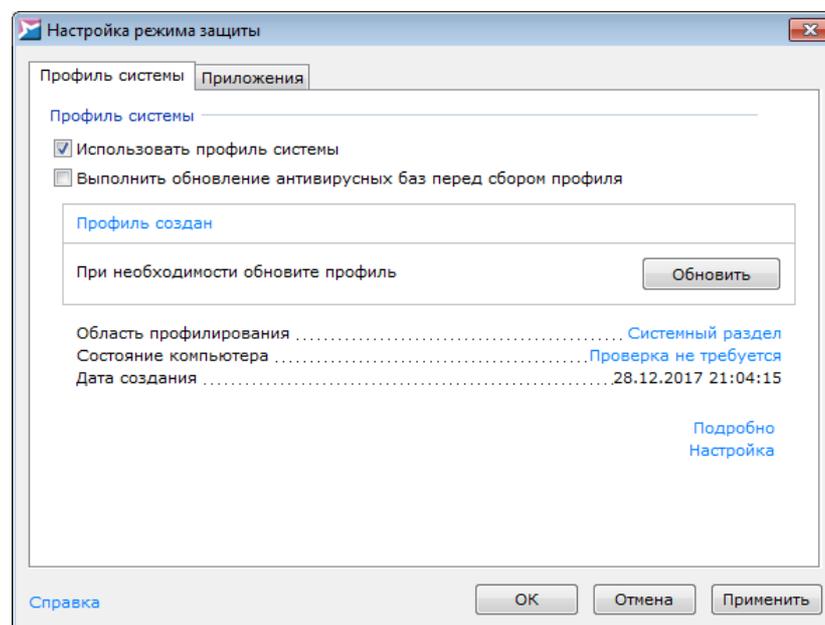


Рисунок 40. Запуск обновления профиля

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](#)⁽⁴⁷⁾).

▼ 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](#)⁽⁴⁷⁾), 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 **Подробнее** (рис. [Запуск обновления профиля](#)⁽⁴⁷⁾).

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;
- Загрузка недоверенной DLL;
- Запуск интерпретатора скриптов;
- Модификация PE-файла не инсталлятором.

Возможные действия для каждой категории инцидентов перечислены в табл. 7.

Таблица 7. Возможные действия при инцидентах

Инцидент	Действия
Запуск приложения не в профиле ⁽⁵⁵⁾	<ul style="list-style-type: none"> • 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 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. • Заблокировать (по умолчанию) Блокировка запуска приложения.
Запуск неподписанного инсталлятора ⁽⁵⁶⁾	<ul style="list-style-type: none"> • 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 в ограниченном режиме Выполнение инсталлятора в изолированной среде (песочнице) под учетной записью

Инцидент	Действия
	пользователя «V.I.P.O.» с ограниченными привилегиями. При этом добавления в профиль системы не происходит. <ul style="list-style-type: none"> • Заблокировать (по умолчанию) Блокировка запуска инсталлятора.
Нарушение политики контроля ⁽⁶³⁾	<ul style="list-style-type: none"> • Разрешить Разрешение приложению выполнить действие, совпадающее с условиями правила заданной политики контроля, однократно/на сессию. • 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.
Загрузка недоверенной DLL ⁽⁵¹⁾	<ul style="list-style-type: none"> • Разрешить Разрешение загрузки DLL-библиотеки без ограничений. • Запретить Запрет загрузки.
Запуск интерпретатора скриптов ⁽⁵⁰⁾	<ul style="list-style-type: none"> • Разрешить Разрешение запуска. • Запретить Запрет запуска.
Модификация PE-файла не инсталлятором ⁽⁵¹⁾	<ul style="list-style-type: none"> • Разрешить Разрешение модификации PE-файла. • Запретить Запрет модификации.

На вкладке **Статус панели управления** ⁽³⁵⁾ 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](#) ⁽⁵⁸⁾, 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](#) ⁽⁴⁹⁾). Отслеживание активности приложений включено, когда отмечена область защиты **Приложения**.

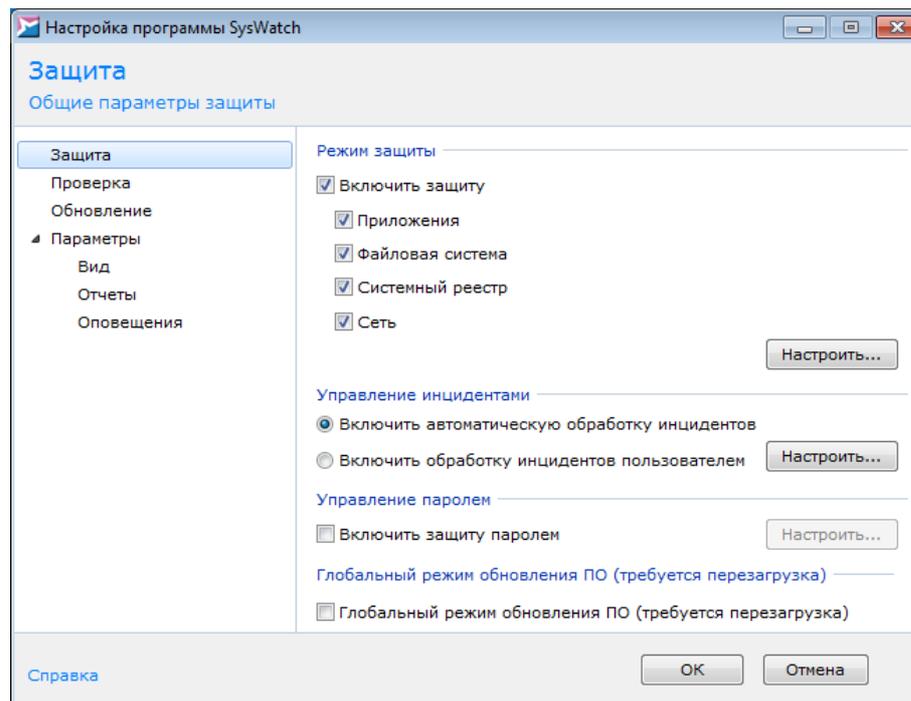


Рисунок 41. Настройки общих параметров защиты

Ниже приведена детальная информация по настройке отслеживания активности приложений:

- [опции отслеживания активности](#) ⁽⁵⁰⁾;
- [обработка инцидентов запуска приложений](#) ⁽⁵³⁾;
- [зоны выполнения приложений](#) ⁽⁵⁸⁾;
- [белый список сертификатов](#) ⁽⁶¹⁾.

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](#) ⁽⁴⁹⁾) и в окне **Настройка режима защиты** перейдите на вкладку **Приложения** (рис. [Опции контроля активности](#) ⁽⁵²⁾).

В области **Приложения** расположены следующие опции:

- Сохранять историю активности неотслеживаемых приложений и инсталляторов:**

Автоматическое включение опции записи истории активности 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](#)⁶¹). 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](#)⁶³.

Примечание. Если в разделе **Управление инцидентами** для инцидента **Запуск интерпретатора скриптов** выбрано решение **Разрешить**, выполнение скрипта не будет отклонено. Событие при этом заносится в лог.

Все интерпретаторы скриптов находятся в системной папке:

Система будет запрещать только процессы, запущенные из системной папки (C:\Windows\System32 или C:\Windows\SysWOW64).

Эта опция активна, только если выбрана опция **Запретить выполнение скриптов**.

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

Примечание 2: если в разделе **Управление инцидентами** для инцидента **Загрузка недоверенной DLL** выбрано решение **Разрешить**, запуск не будет отклонен. Событие при этом заносится в лог.

Запретить всем, кроме инсталляторов, модификацию исполняемых файлов PE:

Запрет изменения исполняемых файлов (exe, dll и т.п.) всеми приложениями, кроме ра-

ботающих в режиме обновления ПО. Позволяет снизить риски нарушения целостности системы.

Примечание. Если в разделе **Управление инцидентами** для инцидента **Модификация PE-файла не инсталлятором** выбрано решение **Разрешить**, изменение исполняемых файлов не будет отклонено. Событие при этом заносится в лог.

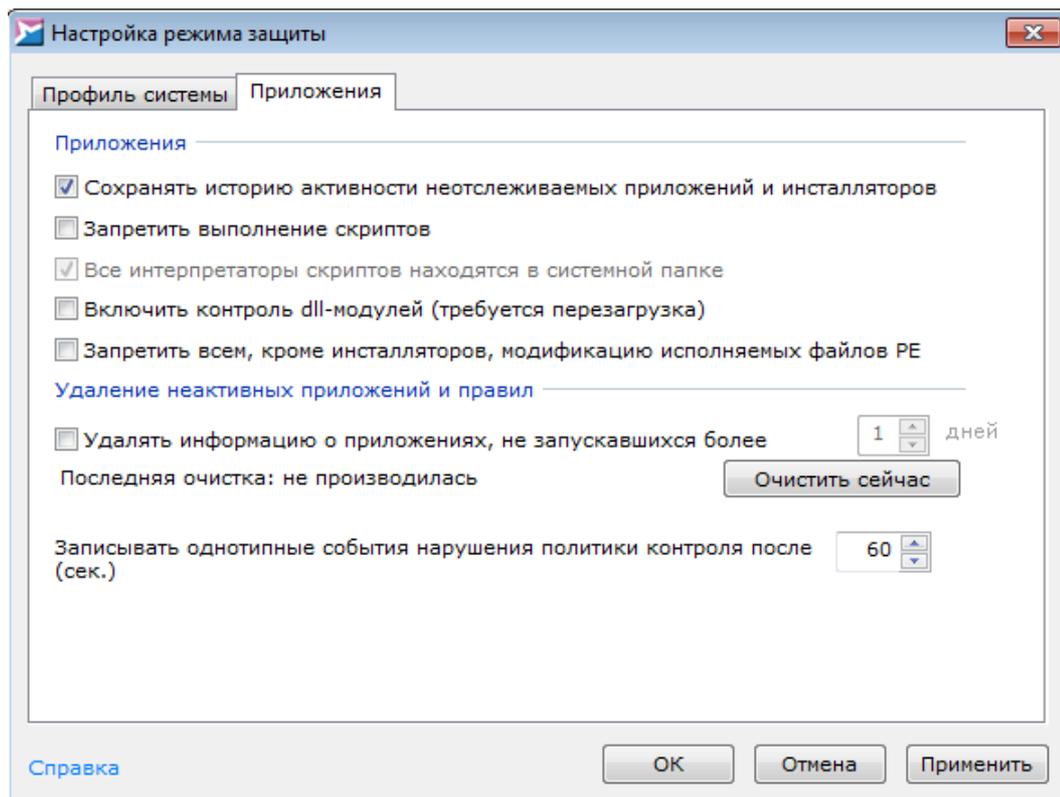


Рисунок 42. Опции контроля активности

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**.

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](#)⁽⁴⁹⁾) и перезагрузите систему.

i 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](#)⁽⁵³⁾.

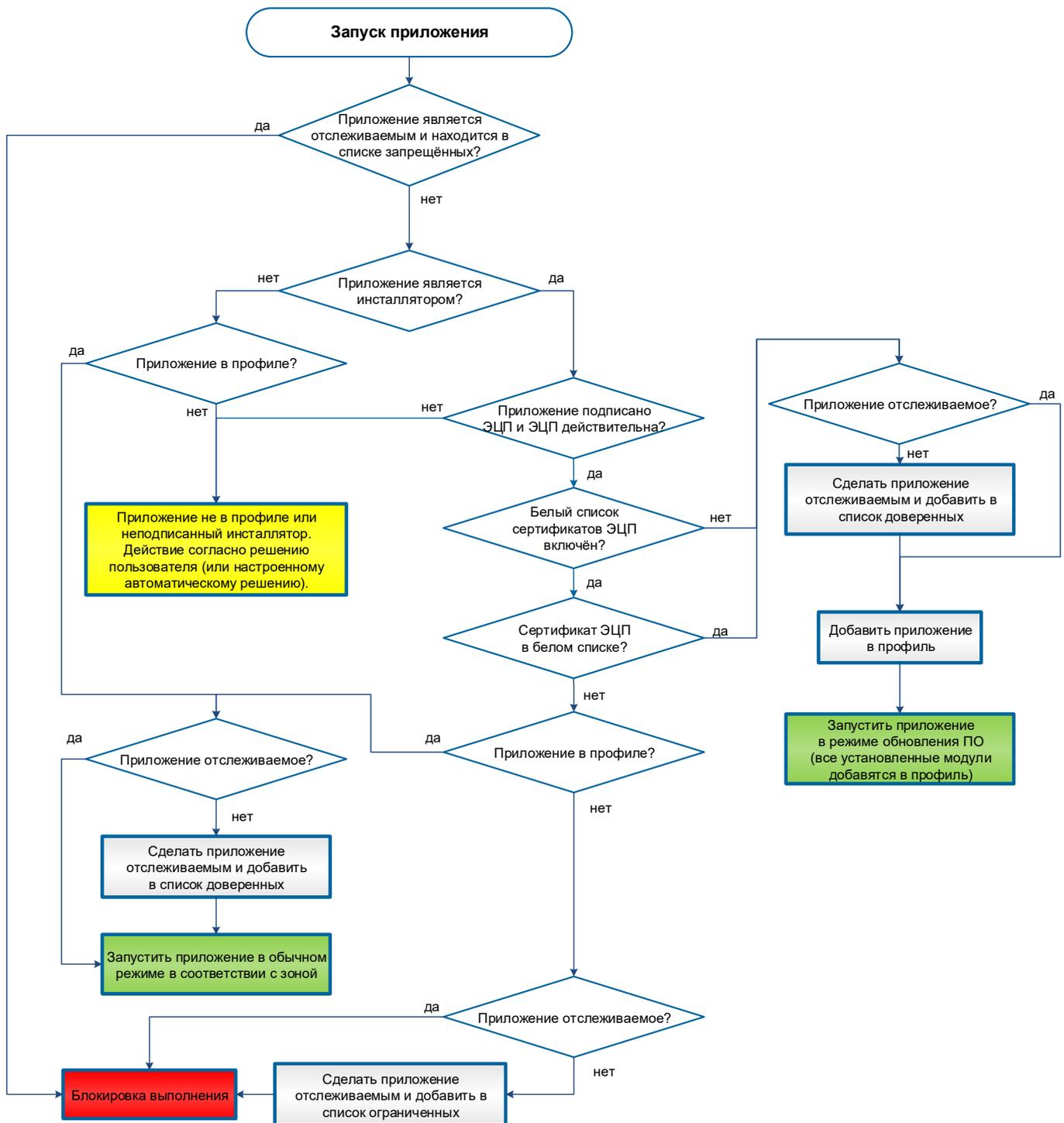


Рисунок 43. Общая схема обработки запуска приложений, отсутствующих в профиле

Окончательное решение (рис. [выше](#)⁵³) 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](#)⁽⁴⁹⁾). В окне **Управление инцидентами** (рис. [Настройка реакции на инциденты](#)⁽⁵⁵⁾) в **Списке инцидентов** выберите требуемый тип события и в выпадающем меню **Решение** установите действие, которое будет производиться SoftControl SysWatch при наступлении данного события.

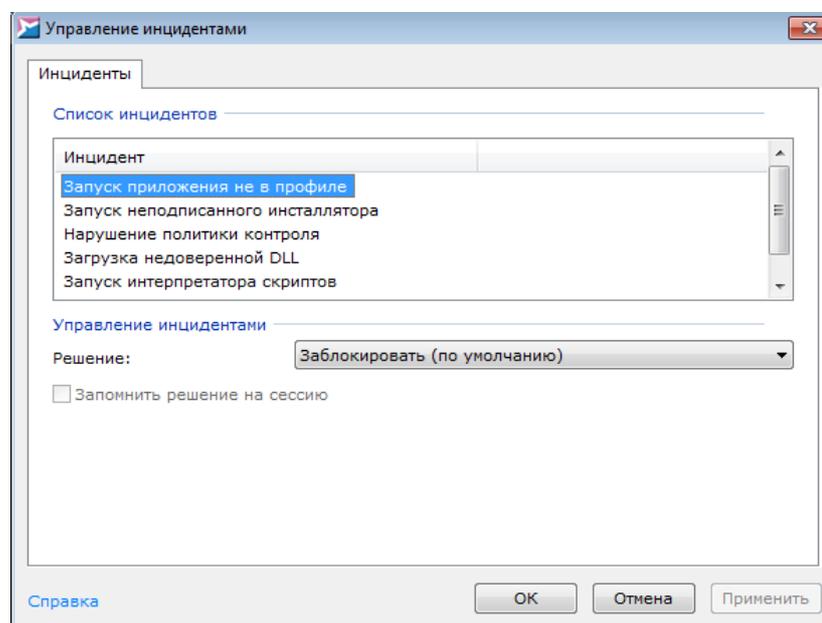


Рисунок 44. Настройка реакции на инциденты

Полный перечень инцидентов и возможных реакций на них приведен в табл. 7 [выше](#)⁽⁴⁸⁾. Для подтверждения выбранных установок нажмите на кнопку **ОК**.

▪ 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 **ОК** (рис. [Настройки общих параметров защиты](#)⁽⁴⁹⁾).

▼ Запуск приложения не в профиле

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

- 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.

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

→ **Запретить** – заблокировать выполнение приложения.

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

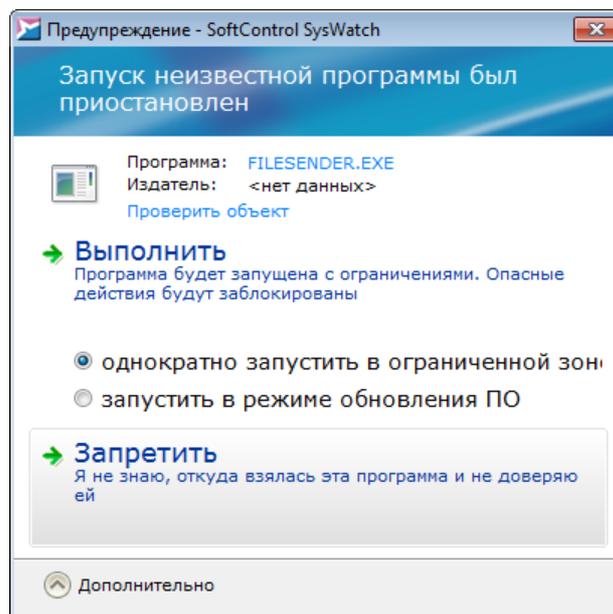


Рисунок 45. Окно предупреждения для приложения не в профиле

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](#) ⁽⁵⁷⁾.

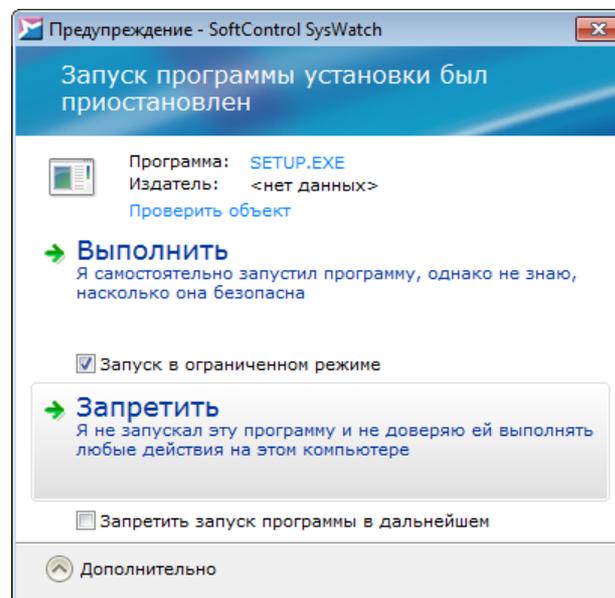


Рисунок 46. Окно предупреждения для неподписанного инсталлятора

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

- 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;

i 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.

i 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 закрывает окно предупреждения.

5.5.3 Зоны выполнения приложений

Чтобы просмотреть и изменить текущее распределение приложений по зонам выполнения, выберите пункт **Отслеживаемые приложения** [контекстного меню](#)³⁴ SoftControl SysWatch. В окне **Политика контроля** на вкладке **Отслеживаемые приложения** содержатся все отслеживаемые приложения, то есть зарегистрированные SoftControl SysWatch с момента установки программы.

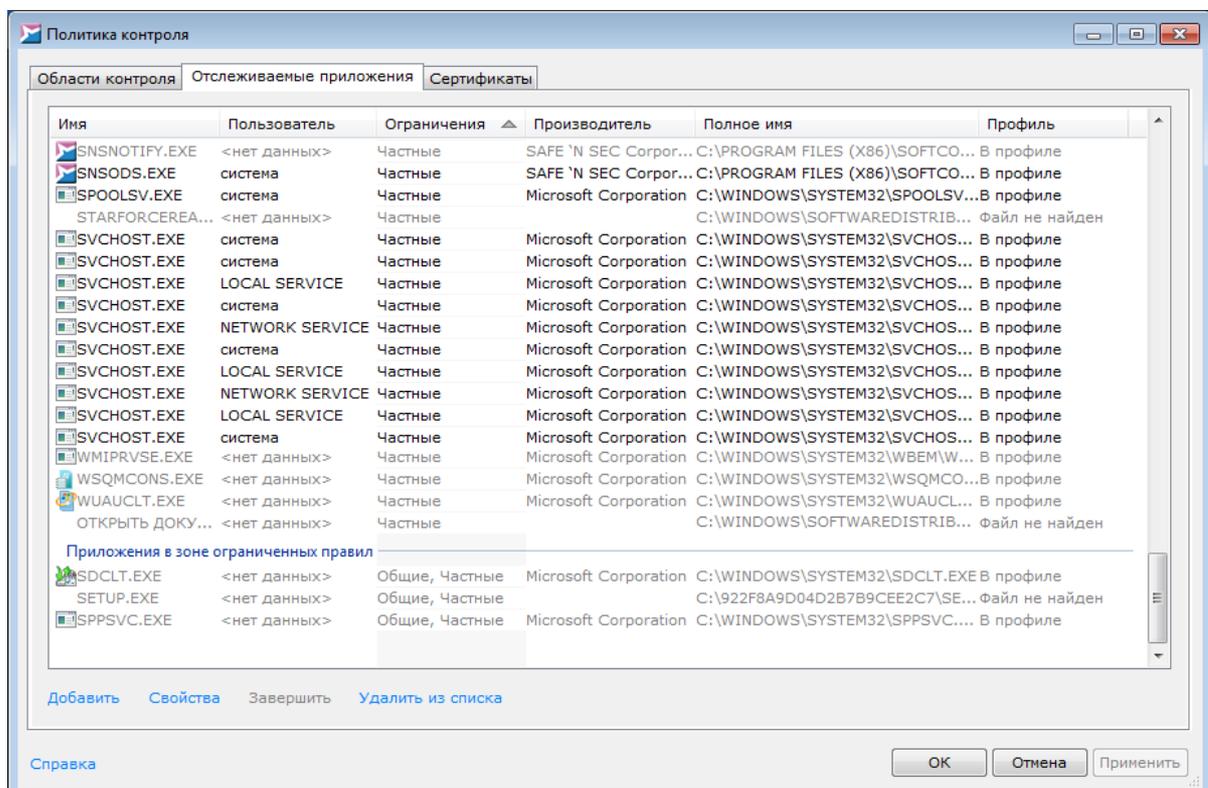


Рисунок 47. Отслеживаемые приложения

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](#)⁶⁰.

▼ Добавление/удаление приложения из профиля системы

Если требуется переместить приложение в профиль системы или удалить его без [обновления всего профиля](#)⁴⁷, 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** и **Приложения** в области **Режим защиты**.

▼ 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 Белый список сертификатов

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

- 1) Выберите пункт **Отслеживаемые приложения** [контекстного меню](#)⁽³⁴⁾ SoftControl SysWatch и в окне **Политика контроля** перейдите на вкладку **Сертификаты** (рис. [Белый список сертификатов](#)⁽⁶¹⁾).

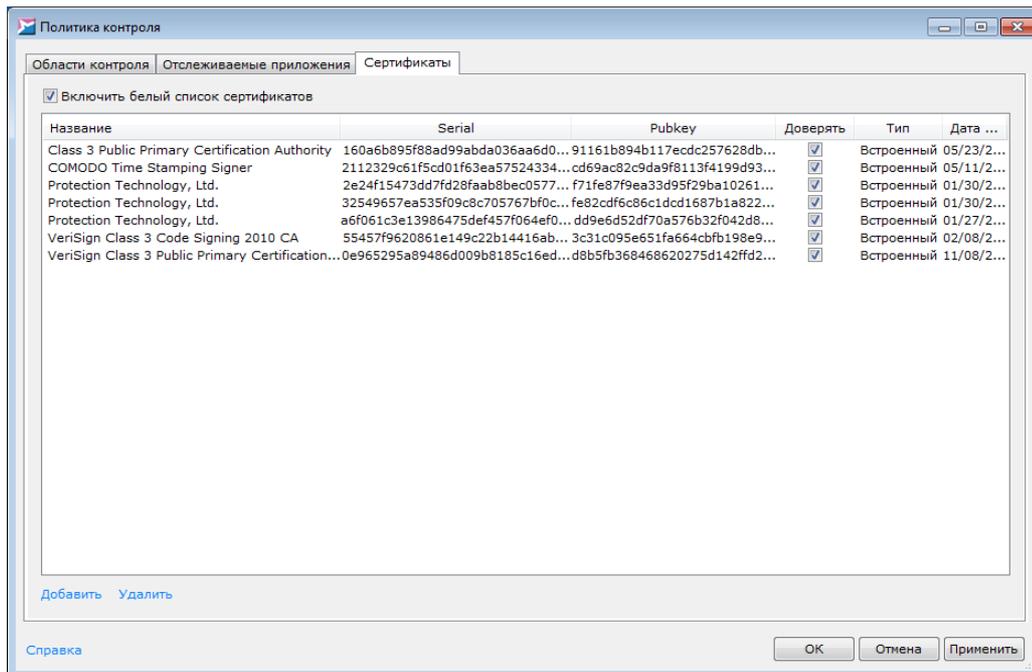


Рисунок 48. Белый список сертификатов

- 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.

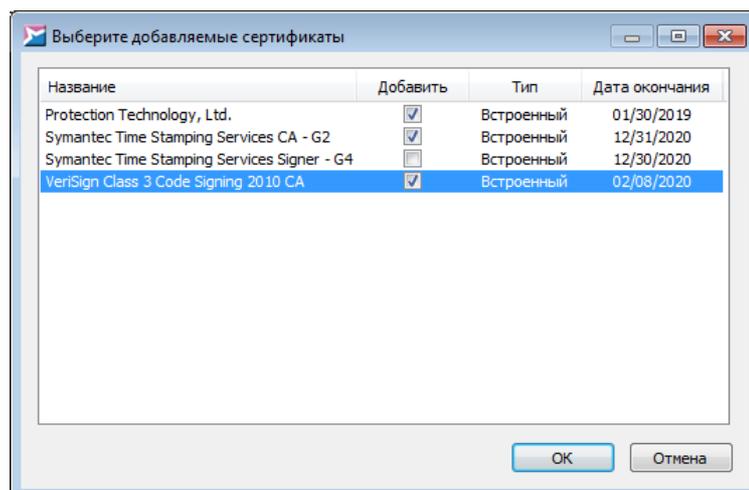


Рисунок 49. Выбор сертификатов для добавления

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 **ОК** (рис. [Выбор сертификатов для добавления](#)⁽⁶¹⁾).

- 4) Установите флажок в столбце **Доверять** для добавленных сертификатов (рис. [Белый список сертификатов](#)⁽⁶¹⁾).
- 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](#)⁽⁶¹⁾).
- 6) Для вступления изменений в силу нажмите на кнопку **ОК** или **Применить** (рис. [Белый список сертификатов](#)⁽⁶¹⁾).



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.

5.5.5 Правила контроля активности

На вкладке **Статус** [панели управления](#)⁽³⁵⁾ 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](#)⁽⁶³⁾;
- [доступа к системному реестру](#)⁽⁶⁹⁾;
- [доступа к устройствам и портам](#)⁽⁷⁴⁾;
- [сетевой активности](#)⁽⁷⁸⁾;
- [привилегий процессов](#)⁽⁸⁴⁾;
- [взаимодействия процессов](#)⁽⁸⁷⁾.

5.5.5.1 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](#)⁽³⁴⁾ SoftControl SysWatch; в окне **Политика контроля** на вкладке **Области контроля** выберите в выпадающем списке раздел **Файловая система** (рис. [Политика контроля файловой системы](#)⁽⁶³⁾).

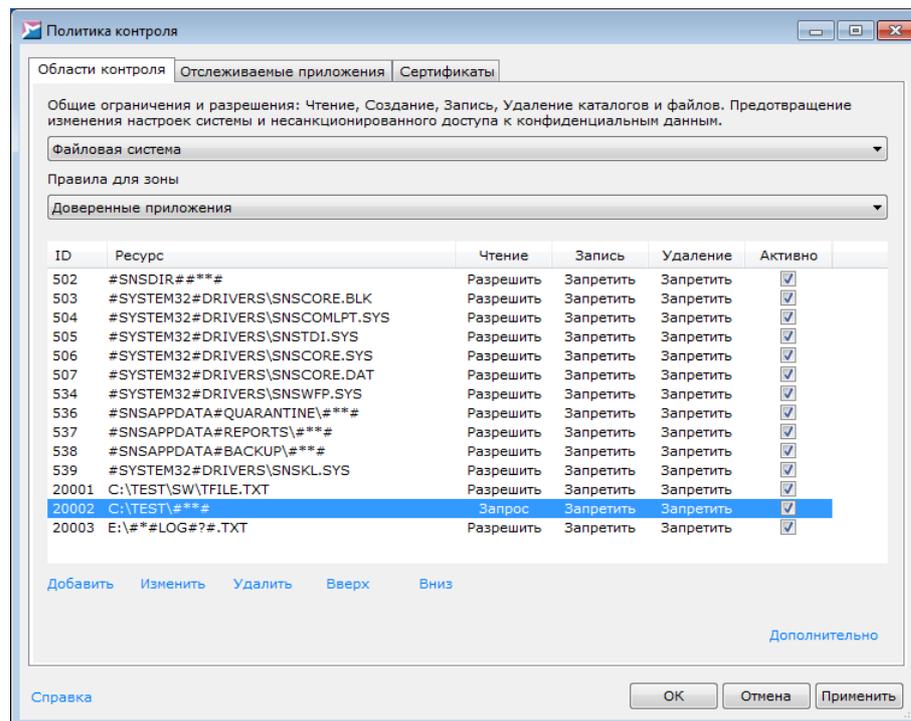


Рисунок 50. Политика контроля файловой системы

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](#)⁶³, 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 при-

менения 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](#)⁽⁶³⁾ 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](#)⁽⁶⁶⁾). 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.

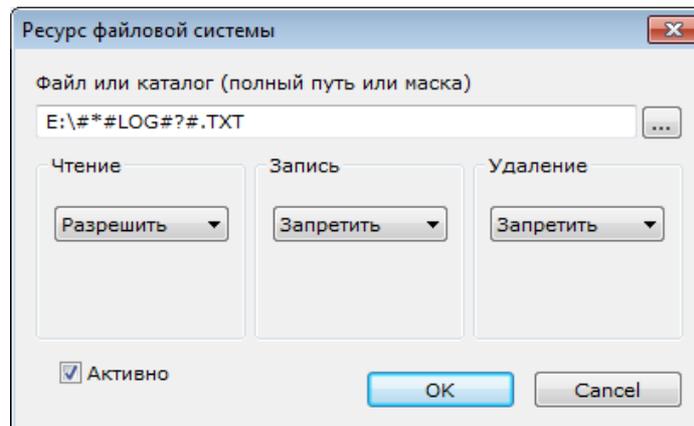


Рисунок 51. Создание правила для объекта файловой системы

i При выборе каталога через проводник к нему автоматически добавляется [маска](#)⁶⁴ **###**, 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 **ОК**.

▼ **Изменение правила**

Чтобы изменить правило, нажмите на ссылку **Изменить** и настройте параметры правила аналогично действиям при его [создании](#)⁶⁵.

▼ **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](#)⁽⁶⁷⁾). По умолчанию правила устанавливаются для всех пользователей.

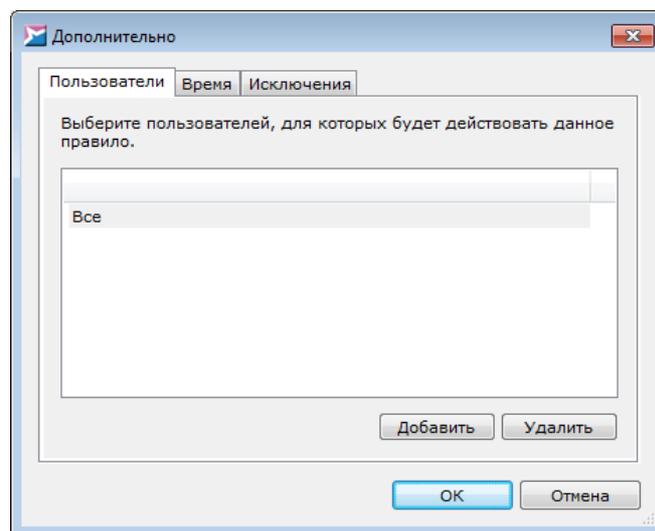


Рисунок 52. Выбор учётных записей пользователей

- **Время** – на данной вкладке задаются временные интервалы действия правила (рис. [Выбор времени действия правила](#)⁽⁶⁷⁾).

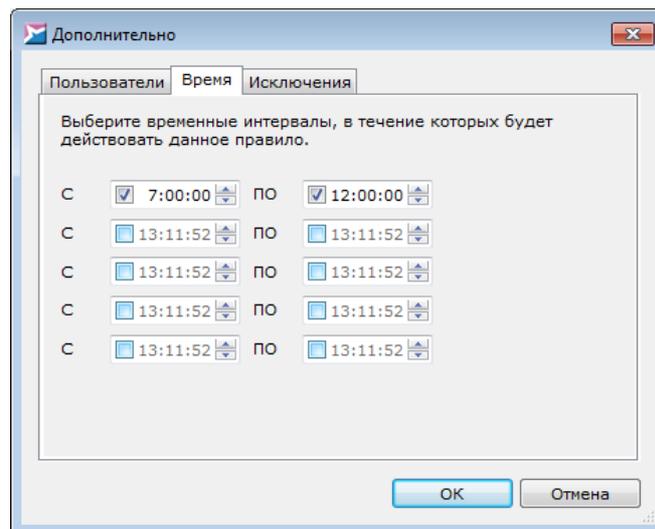


Рисунок 53. Выбор времени действия правила

i 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](#)⁽⁶⁸⁾).

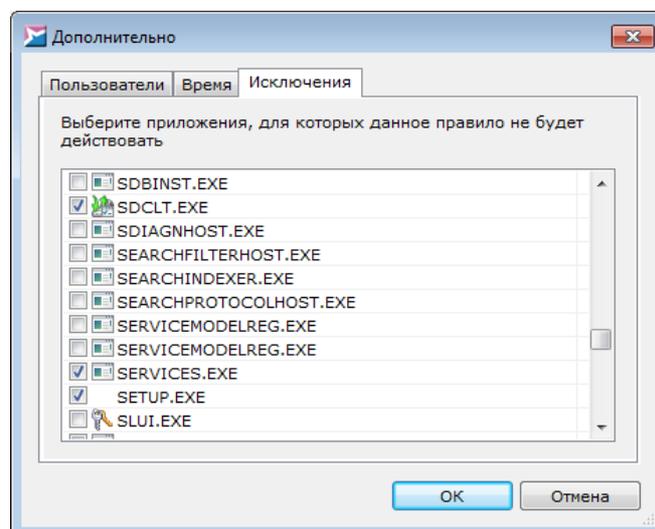


Рисунок 54. Выбор приложений для исключения из правила

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

Нажмите на кнопку **ОК**, 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 **ОК** или **Применить**.

5.5.5.2 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.

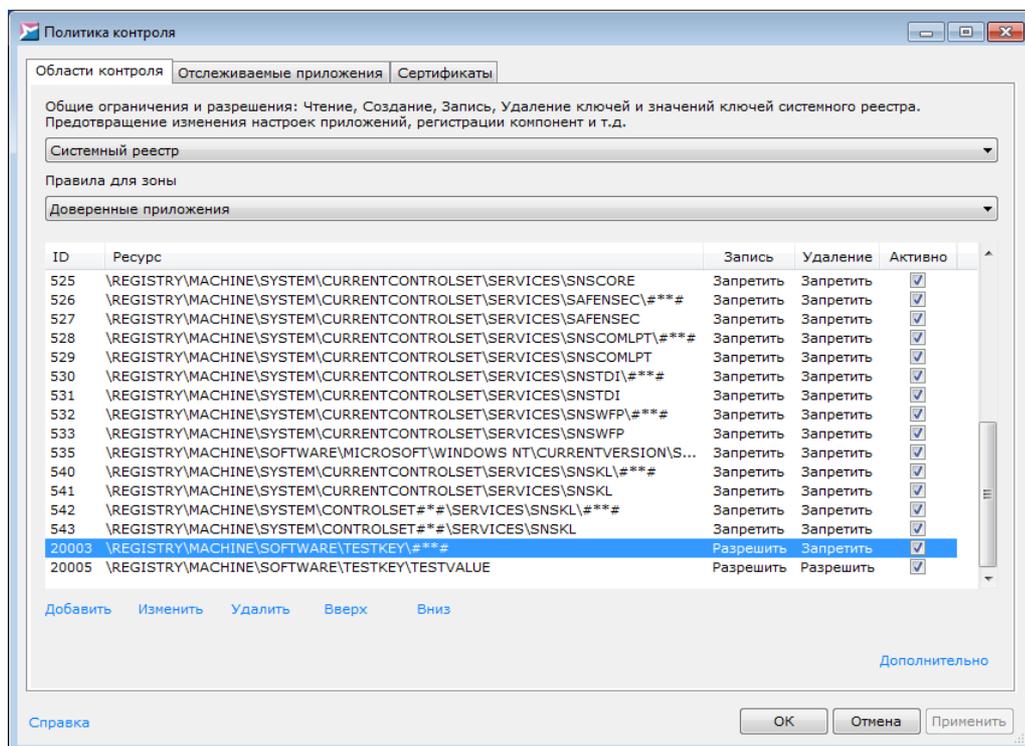


Рисунок 55. Политика контроля системного реестра

Для просмотра и изменения политики контроля системного реестра выберите пункт **Политика контроля контекстного меню**⁽³⁴⁾ SoftControl SysWatch, в окне **Политика контроля** на вкладке **Области контроля** выберите в выпадающем списке раздел **Системный реестр** (рис. [Политика контроля системного реестра](#)⁽⁶⁹⁾).

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](#)⁽⁶⁹⁾, 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](#)⁽⁶⁹⁾ 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](#)⁽⁷¹⁾). 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.

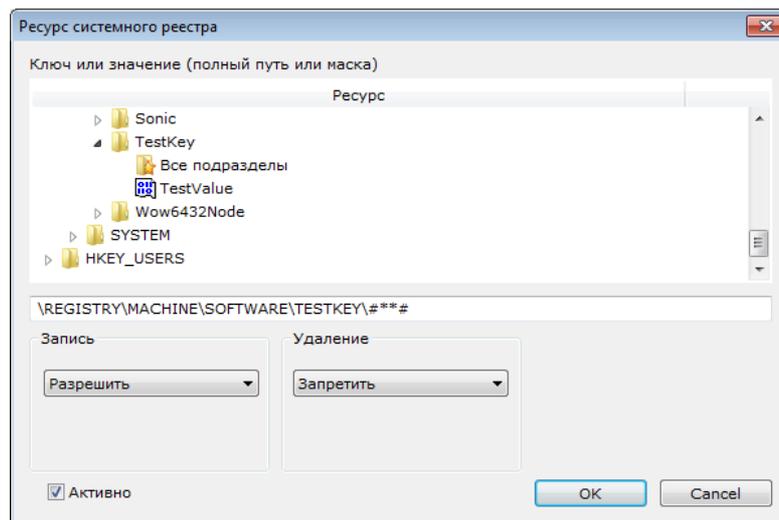


Рисунок 56. Создание правила для объекта системного реестра

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 **ОК**.

▼ Изменение правила

Чтобы изменить правило, нажмите на ссылку **Изменить** и настройте параметры правила аналогично действиям при его [создании](#)⁽⁷¹⁾.

▼ 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](#)⁽⁷²⁾). По умолчанию правила устанавливаются для всех пользователей.
- **Время** – на данной вкладке задаются временные интервалы действия правила (рис. [Выбор времени действия правила](#)⁽⁷³⁾).



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).

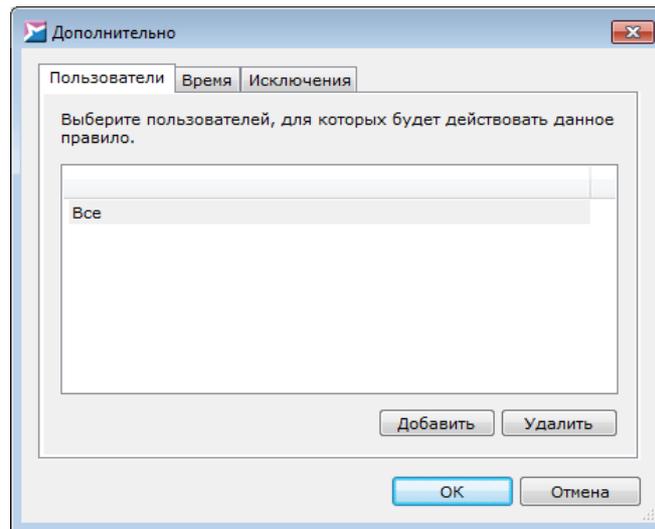


Рисунок 57. Выбор учётных записей пользователей

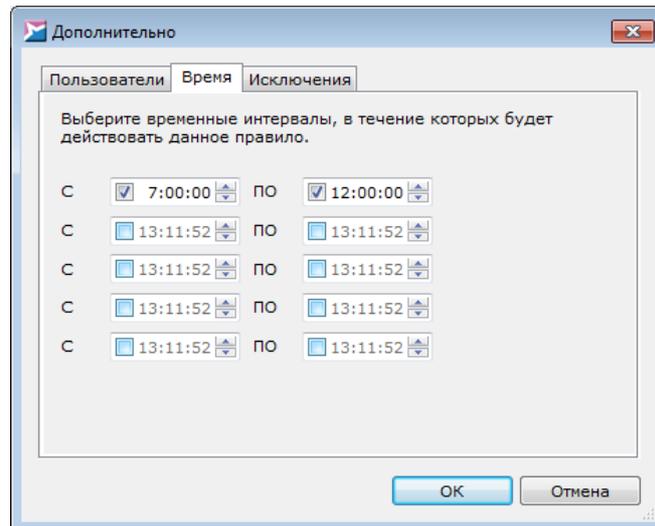


Рисунок 58. Выбор времени действия правила

- **Исключения** – на данной вкладке выбираются приложения, на которые не будет распространяться действие правила (рис. [Выбор приложений для исключения из правила](#)⁽⁷³⁾).

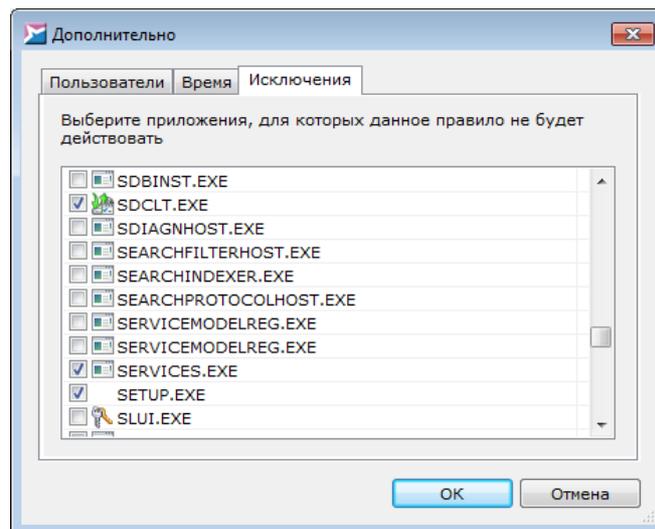


Рисунок 59. Выбор приложений для исключения из правила

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

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

▼ Удаление правила

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

i 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 **ОК** или **Применить**.

5.5.5.3 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.

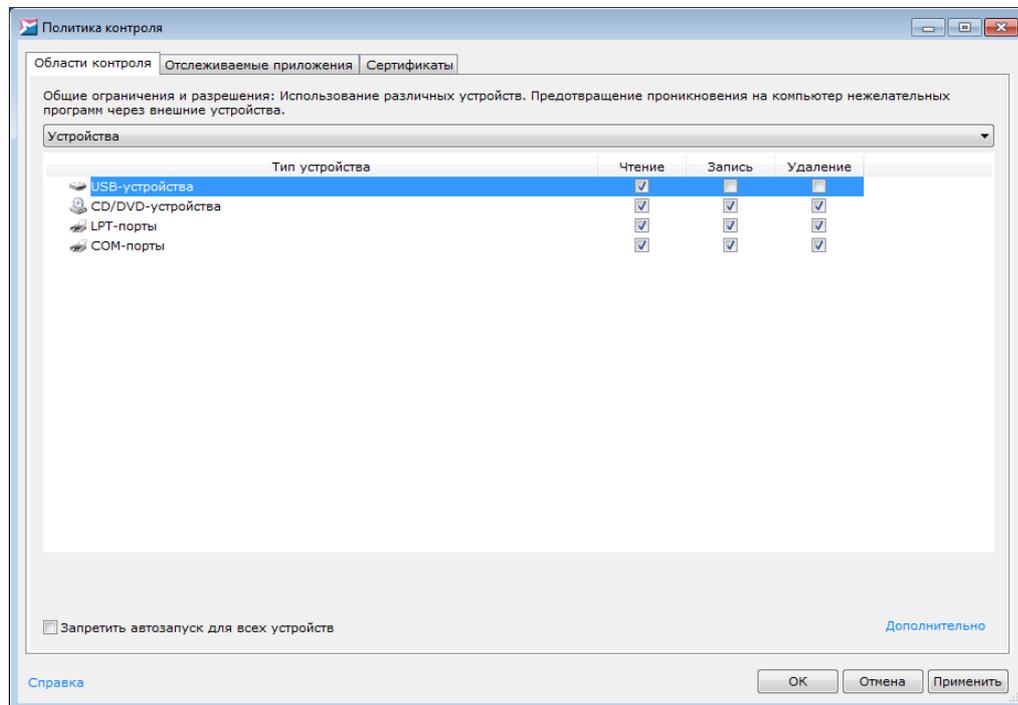


Рисунок 60. Политика контроля устройств и портов

Для просмотра и изменения политики контроля устройств выберите пункт **Политика контроля контекстного меню**⁽³⁴⁾ SoftControl SysWatch, в окне **Политика контроля** на вкладке **Области контроля** выберите в выпадающем списке раздел **Устройства** (рис. [Политика контроля устройств и портов](#)⁽⁷⁵⁾).

▼ 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](#)⁽⁷⁵⁾).

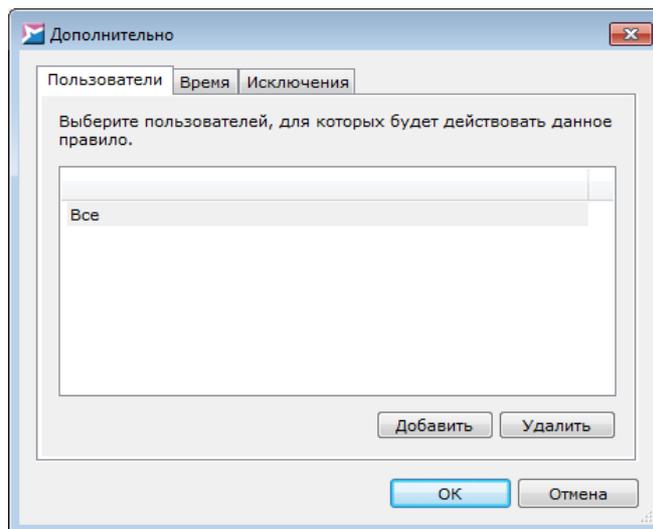


Рисунок 61. Выбор учётных записей пользователей

- **Время** – на данной вкладке задаются временные интервалы действия ограничений (рис. [Выбор времени действия правила](#)⁽⁷⁶⁾).

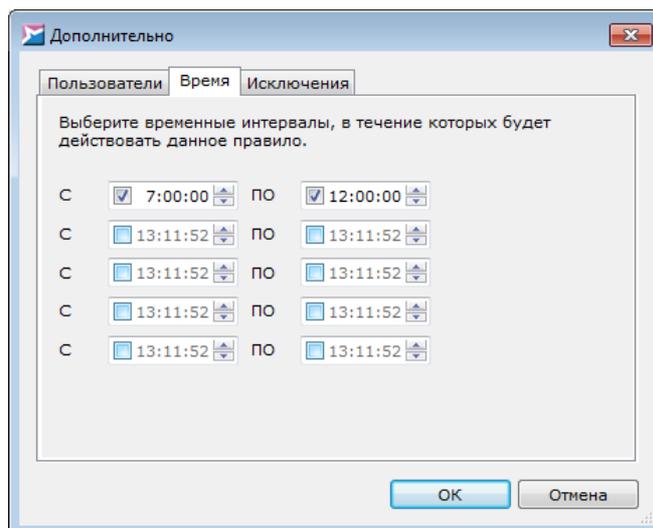


Рисунок 62. Выбор времени действия правила

i 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](#)⁽⁷⁶⁾).

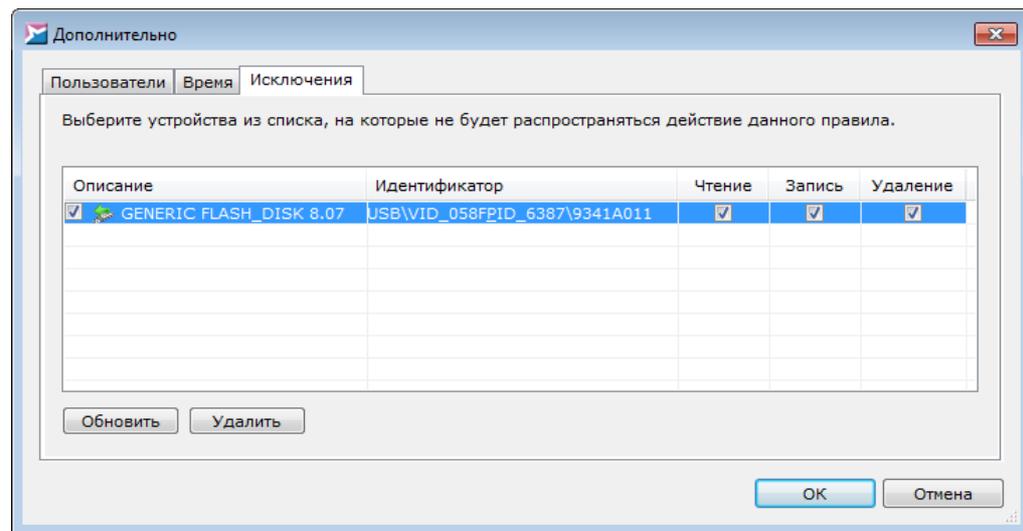


Рисунок 63. Выбор USB-устройств для исключения из правил

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 **ОК**, 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 СОМ-портам**

Чтобы заблокировать доступ к СОМ-портам защищаемого объекта, сбросьте любой из флажков в столбцах **Чтение**, **Запись** или **Удаление** для типа **СОМ-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 **ОК** или **Применить**.

5.5.5.4 Настройка правил сетевой активности

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

- Прием данных;
- Передача данных.

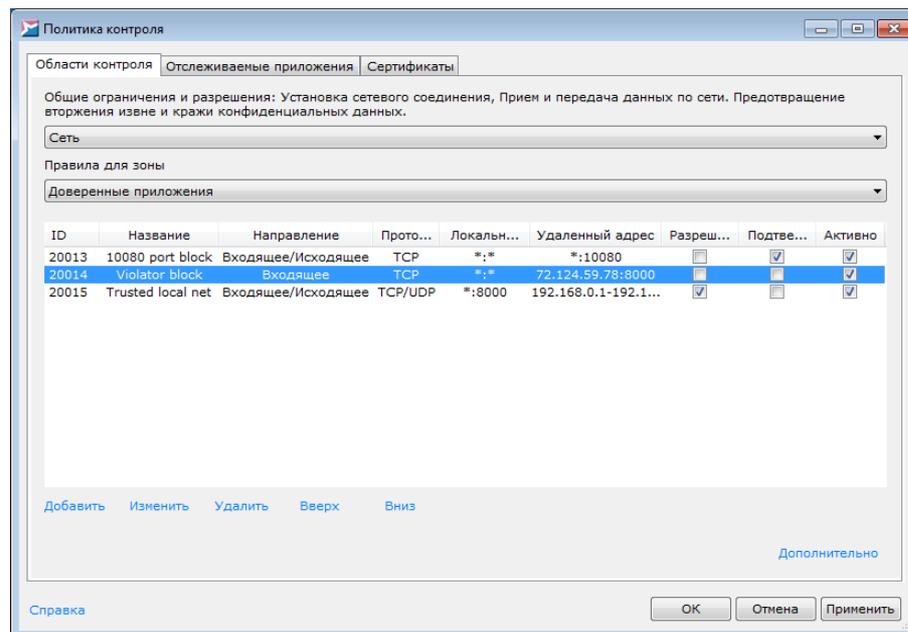


Рисунок 64. Политика контроля сетевой активности

Для просмотра и изменения политики контроля сетевой активности выберите пункт **Политика контроля** [контекстного меню](#)⁽³⁴⁾ SoftControl SysWatch, в окне **Политика контроля** на вкладке **Области контроля** выберите в выпадающем списке раздел **Сеть** (рис. [Политика контроля сетевой активности](#)⁽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**. 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](#)⁽⁸⁰⁾ 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](#)⁽⁸⁰⁾ 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](#)⁽⁸¹⁾, 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](#)⁽⁸⁰⁾).

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

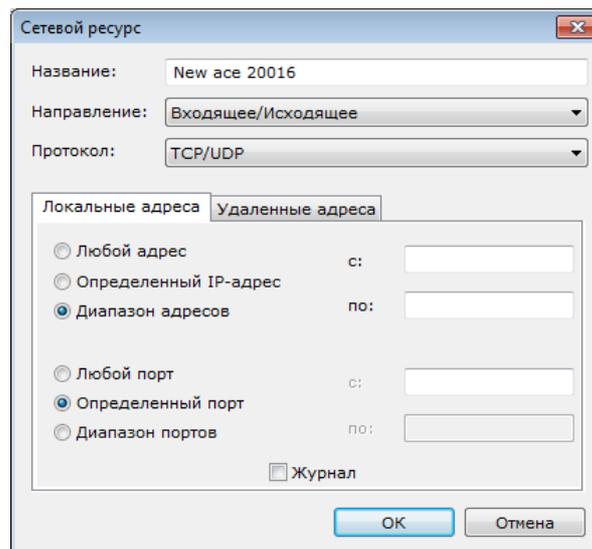


Рисунок 65. Создание правила контроля сетевой активности

▼ 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 **ОК**.

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

[ниже](#) ⁽⁸¹⁾.

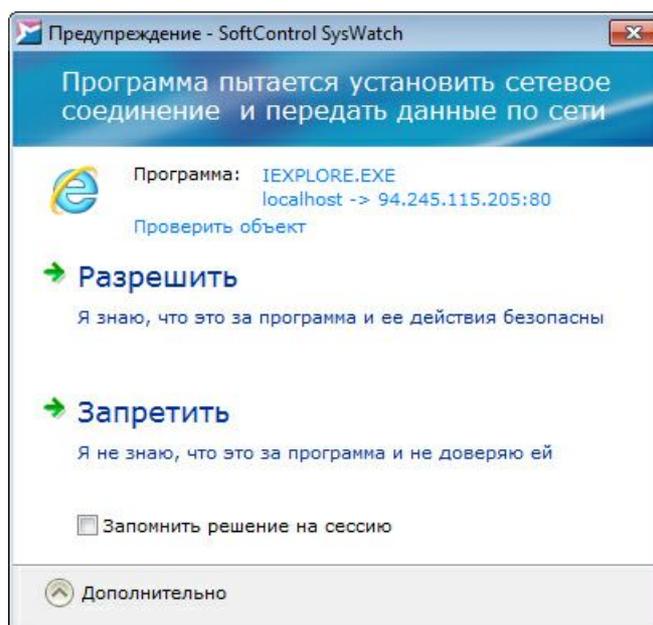


Рисунок 66. Окно предупреждения для сетевой активности

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

- 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](#)⁽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**

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.

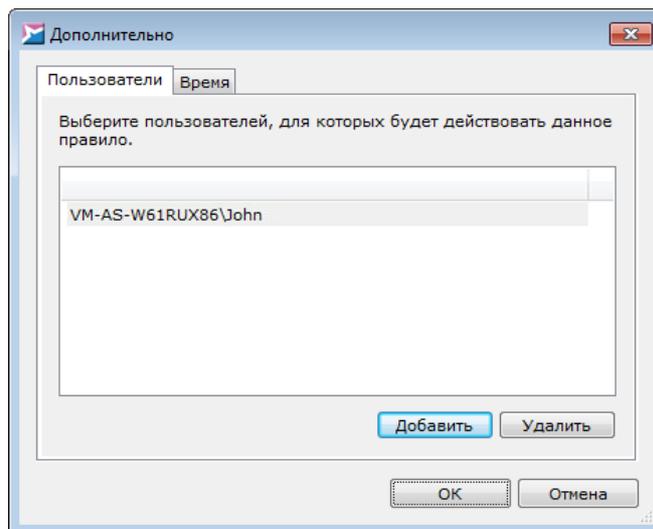


Рисунок 67. Выбор учётных записей пользователей

- **Время** – на данной вкладке задаются временные интервалы действия правила (рис. [Выбор времени действия правила](#)⁸³).

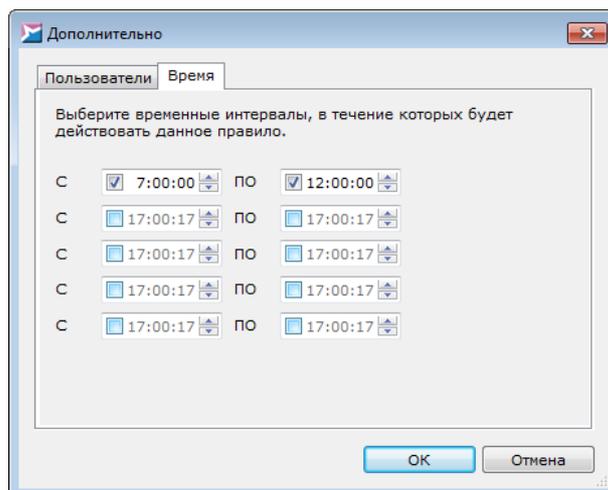


Рисунок 68. Выбор времени действия правила

i 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 **ОК**, чтобы сохранить указанные дополнительные параметры.

▼ Удаление правила

Чтобы удалить правило, нажмите на ссылку **Удалить** и подтвердите удаление в диа-

логовом окне.

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

5.5.5.5 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** ⁽³⁴⁾ SoftControl SysWatch, в окне **Политика контроля** на вкладке **Области контроля** выберите в выпадающем списке раздел **Привилегии процессов** (рис. [По-](#)

[политика контроля привилегий процессов](#)⁽⁸⁵⁾). Описание привилегий и области их применения представлено в разделе **Дополнительная информация**.

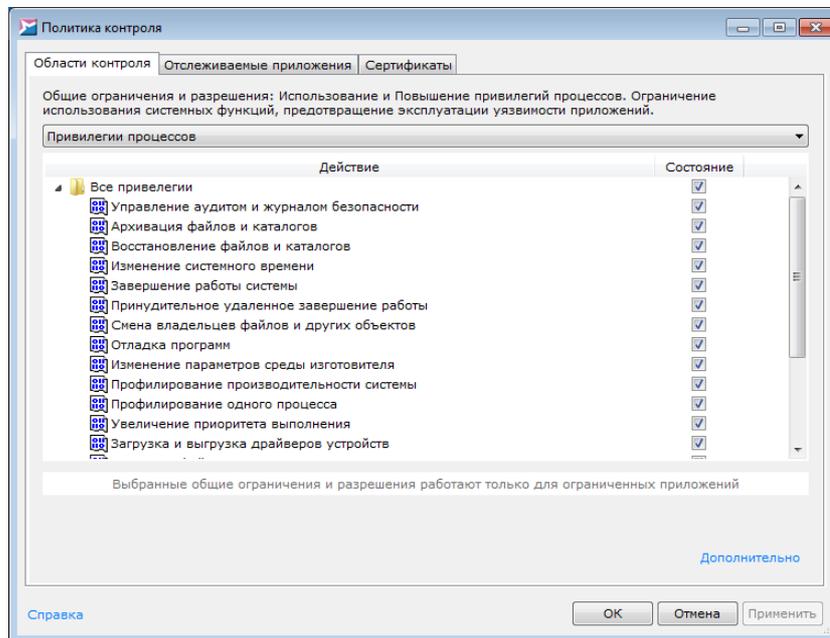


Рисунок 69. Политика контроля привилегий процессов

▼ 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](#)⁽⁸⁵⁾). По умолчанию правила устанавливаются для всех пользователей.

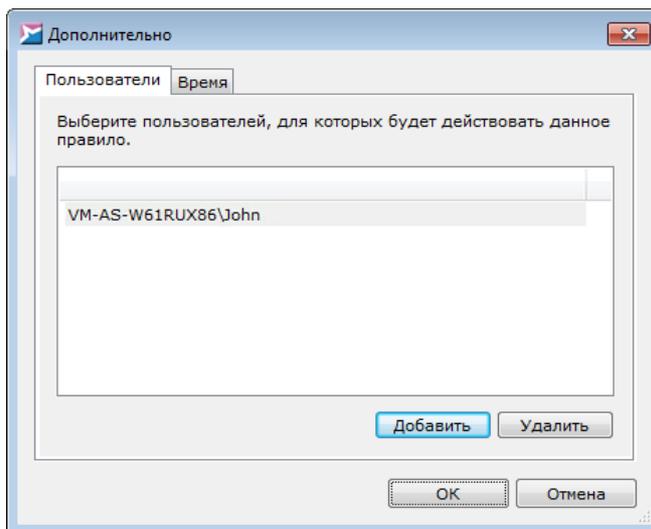


Рисунок 70. Выбор учётных записей пользователей

- **Время** – на данной вкладке задаются временные интервалы действия правила (рис. [Выбор времени действия правила](#)⁸⁶).

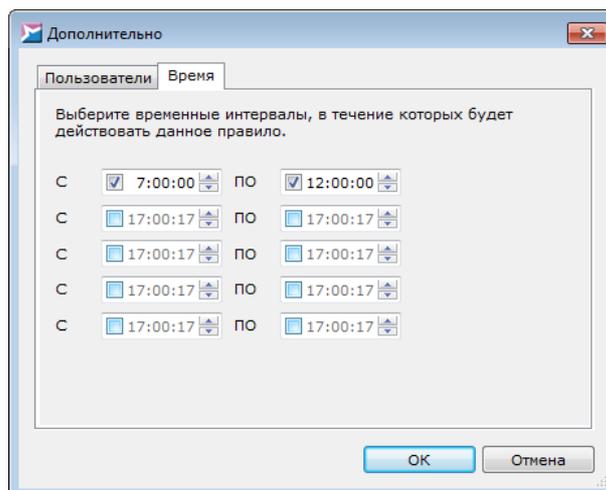


Рисунок 71. Выбор времени действия правила

i 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 **ОК**, чтобы сохранить указанные дополнительные параметры.

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

5.5.5.6 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**⁽³⁴⁾ SoftControl SysWatch, в окне **Политика контроля** на вкладке **Области контроля** выберите в выпадающем списке раздел **Взаимодействие процессов** (рис. [Политика контроля взаимодействия процессов](#)⁽⁸⁷⁾).

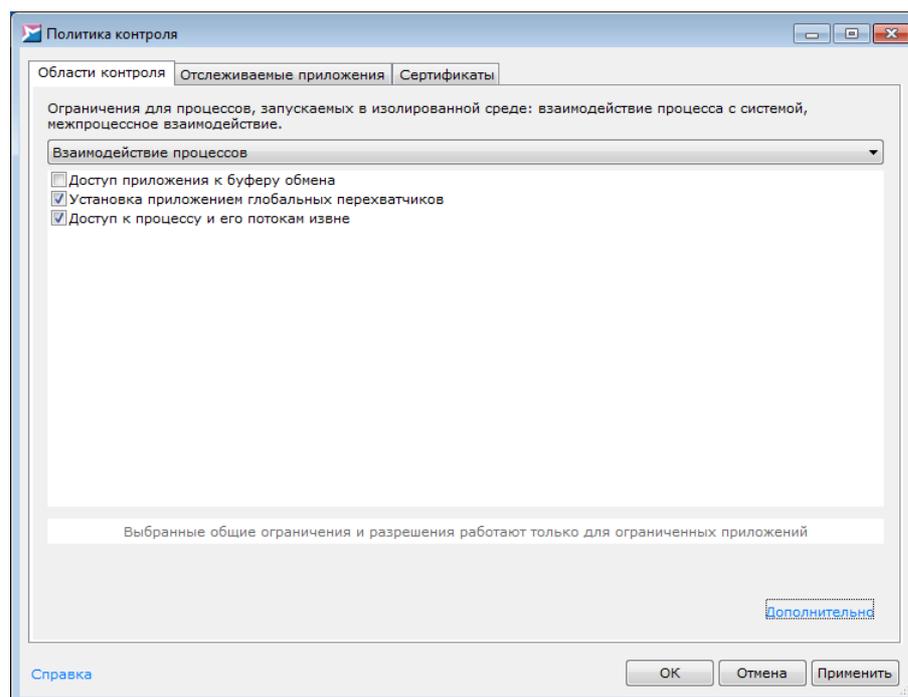


Рисунок 72. Политика контроля взаимодействия процессов

▼ 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](#)⁽⁸⁸⁾). По умолчанию правила устанавливаются для всех пользователей.

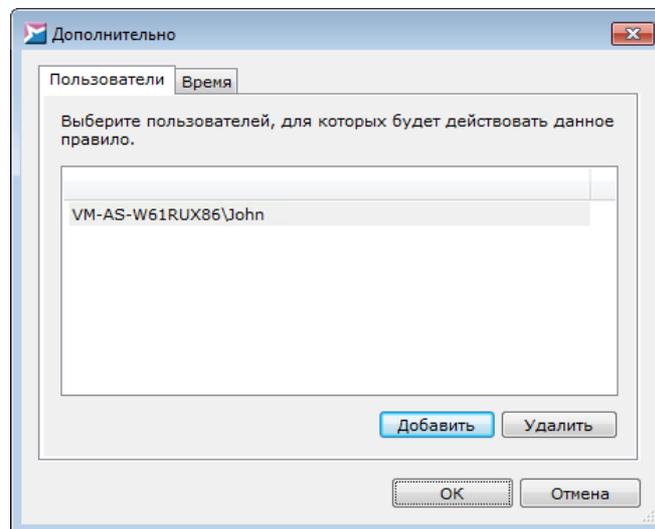


Рисунок 73. Выбор учётных записей пользователей

- **Время** – на данной вкладке задаются временные интервалы действия правила (рис. [Выбор времени действия правила](#)⁽⁸⁸⁾).

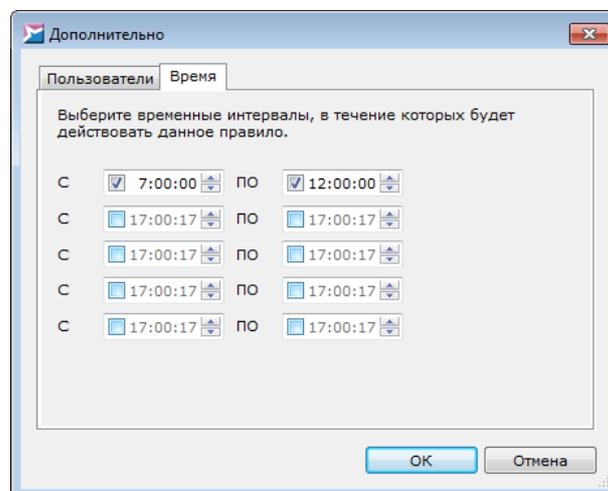


Рисунок 74. Выбор времени действия правила

-
- i** 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 **ОК**, чтобы сохранить указанные дополнительные параметры.

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

5.6 Отчеты

В SoftControl SysWatch реализовано протоколирование событий безопасности и статусов программы в отчеты.

5.6.1 Текстовые отчеты

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](#)⁽⁴⁸⁾ 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](#)⁽⁶³⁾ и их параметры: название, тип активности, учетная запись, программа-источник инцидента, контролируемый объект, решение, количество пропущенных однотипных событий (см. [выше](#)⁽⁵²⁾);
 - идентификатор (UID) правила, в отношении которого произошло нарушение [политики контроля](#)⁽⁶³⁾;
 - имя настроек, полученных с сервера.
- **Отчет о сборе профиля**, включающий в себя следующую информацию:

- область [сбора профиля](#)⁽⁴⁴⁾;
 - список проверенных объектов;
 - результаты [сбора профиля](#)⁽⁴⁴⁾.
- **Отчет об обновлении**, включающий в себя информацию о проведенных [обновлениях программы](#)⁽¹⁰⁰⁾.

▼ **Настройка параметров сохранения отчетов**

Для просмотра и изменения параметров отчетов откройте настройки программы и выберите раздел **Параметры** → **Отчеты** (рис. [Настройка параметров отчетов](#)⁽⁹⁰⁾).

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

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

Выставьте 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**.

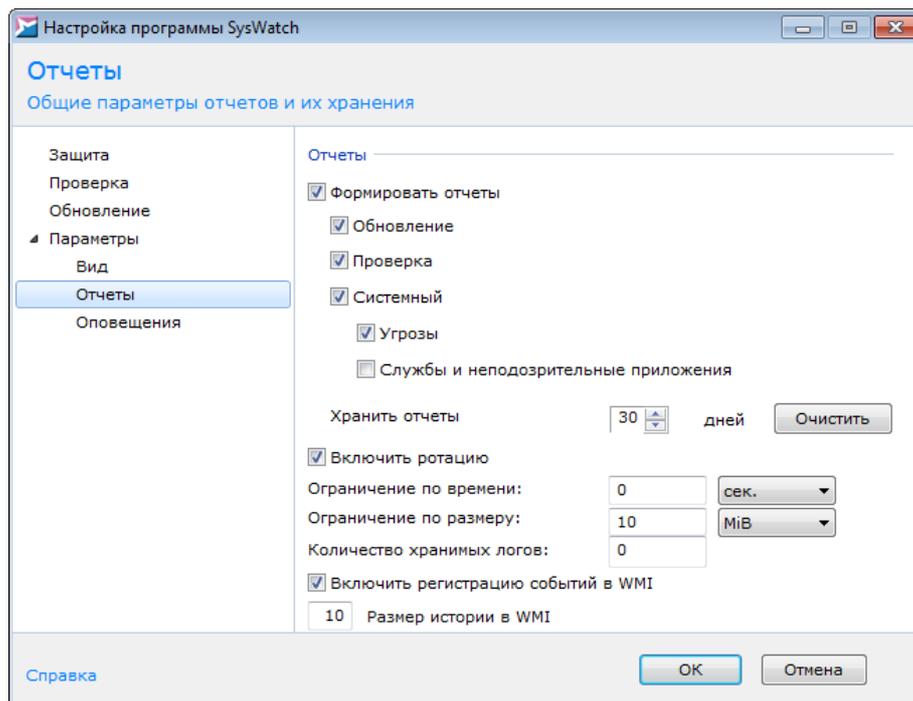


Рисунок 75. Настройка параметров отчётов

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 **ОК**.

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 отчетов

Чтобы просмотреть отчеты, выберите пункт **Отчеты** [контекстного меню](#)⁽³⁴⁾ SoftControl SysWatch. В появившемся каталоге откройте текстовый файл с именем вида *<тип отчета>_<дд.мм.гг>_<чч.мм.сс.ммм>.txt*.

5.7 Настройка общих параметров программы

Ниже приведены указания по настройке общих параметров работы SoftControl SysWatch:

- [самозащита системной службы](#)⁽⁹³⁾;
- [парольная защита](#)⁽⁹⁴⁾;
- [отложенный запуск системной службы](#)⁽⁹⁵⁾;
- [восстановление БД после аппаратной перезагрузки](#)⁽⁹⁶⁾.

5.7.1 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](#)⁹³).

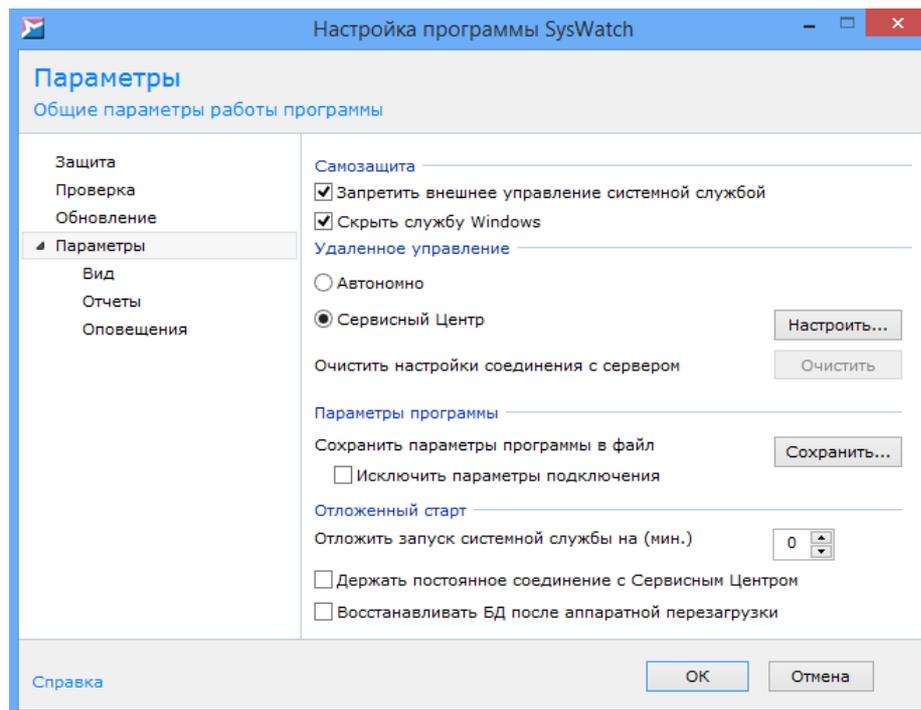


Рисунок 76. Настройки параметров программы

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: скрывание системной службы не работает на ОС Windows XP.

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

5.7.2 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](#)⁽⁹⁴⁾).

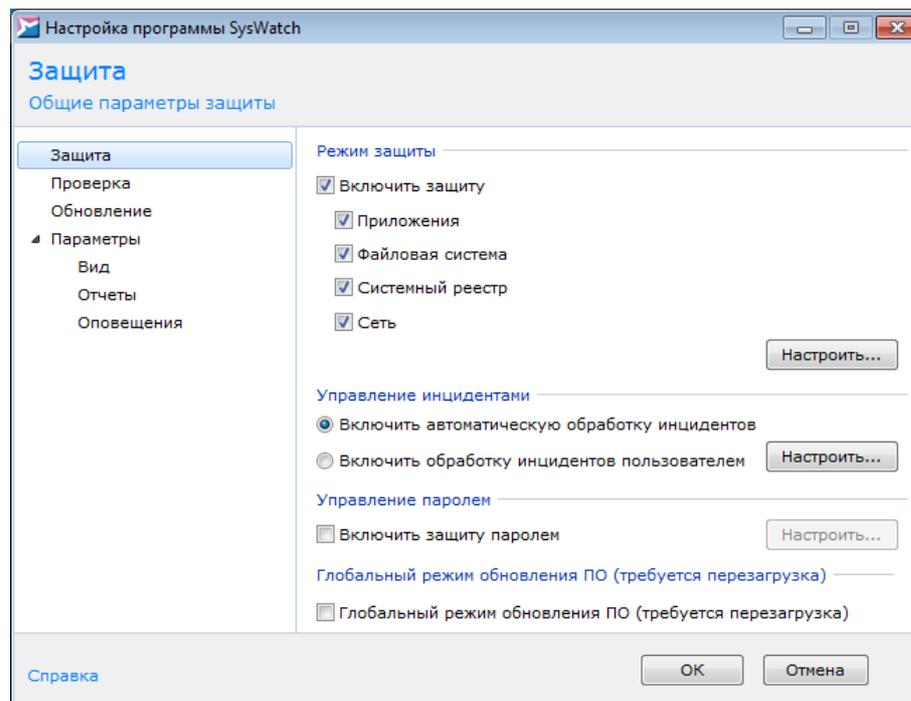


Рисунок 77. Настройки общих параметров защиты

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](#)⁽⁹⁴⁾):

Изменение настроек программы

запрос пароля при доступе к [панели управления](#)⁽³⁵⁾ и настройкам SoftControl SysWatch.

Удаление программы

запрос пароля при запуске программы [деинсталляции](#)⁽¹⁰⁷⁾ SoftControl SysWatch.



Длина пароля должна составлять не менее 7 символов.

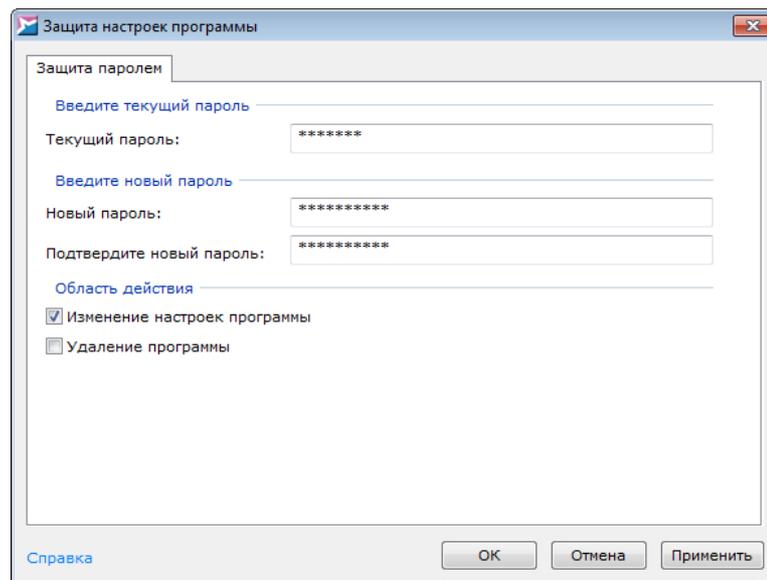


Рисунок 78. Настройка парольной защиты

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

5.7.3 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](#)⁹⁵).

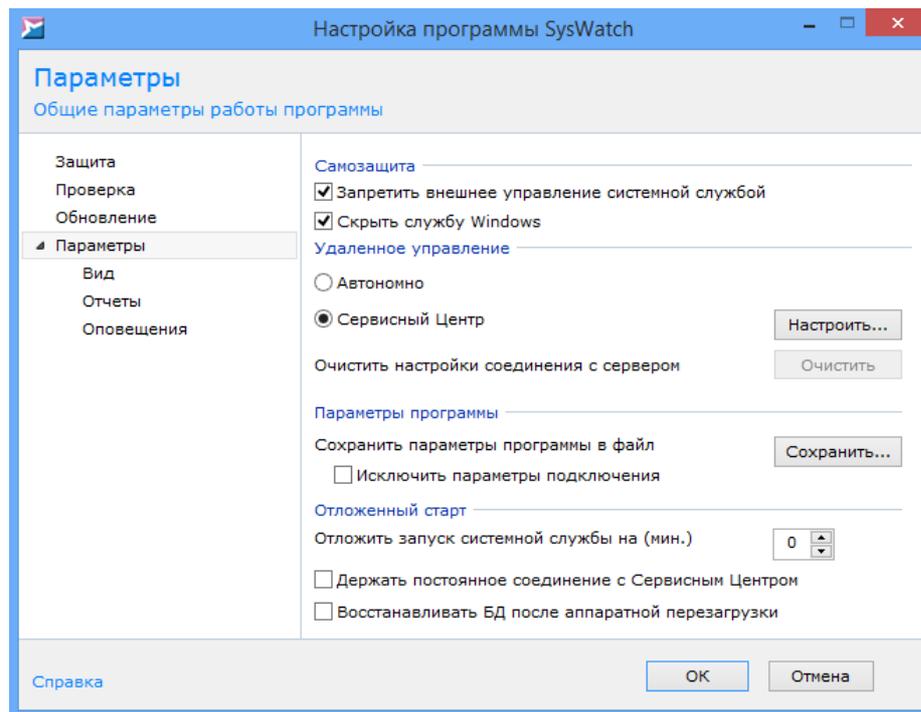


Рисунок 79. Настройки параметров программы

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

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

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

5.7.4 Восстановление БД после аппаратной перезагрузки

При работе SoftControl SysWatch каждый час создается резервная копия базы данных. Также резервная копия создается при начале работы, при получении новых настроек с сервера и при локальном изменении настроек. Если вы хотите в случае аппаратной перезагрузки восстанавливать базу данных из последней копии, поставьте флажок **Восстанавливать БД после аппаратной перезагрузки** в разделе **Параметры** (рис. [Настройки параметров программы](#)⁽⁹⁶⁾).

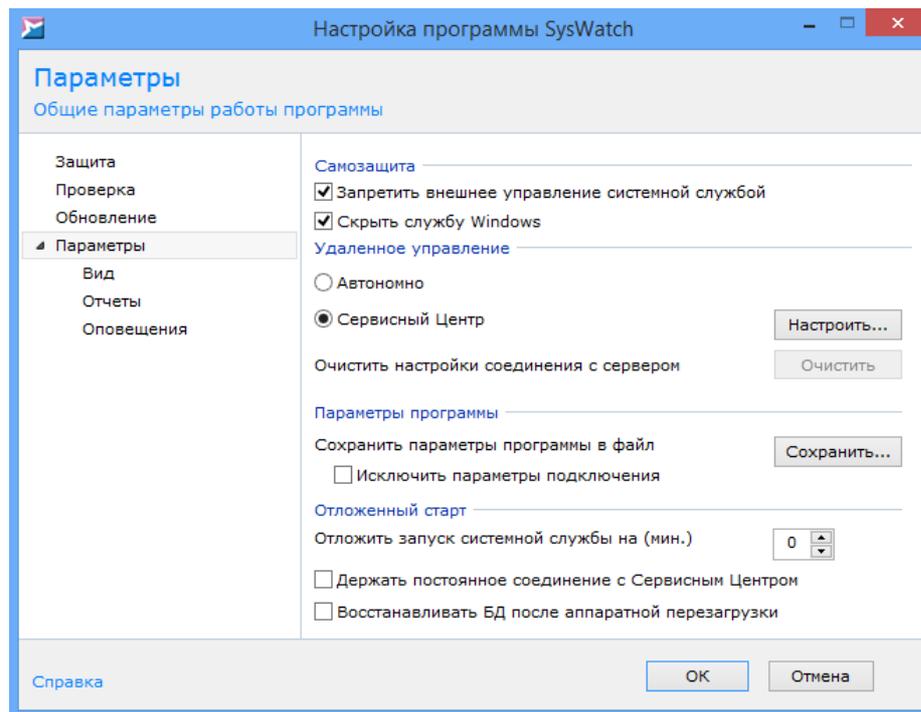


Рисунок 80. Настройки параметров программы

5.8 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](#)⁽⁹⁷⁾, 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.

5.8.1 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](#)⁽⁹⁷⁾). Если необходимо выгрузить конфигурацию SoftControl SysWatch без настроек подключения к серверу, перед сохранением установите флажок **Исключить параметры подключения**.

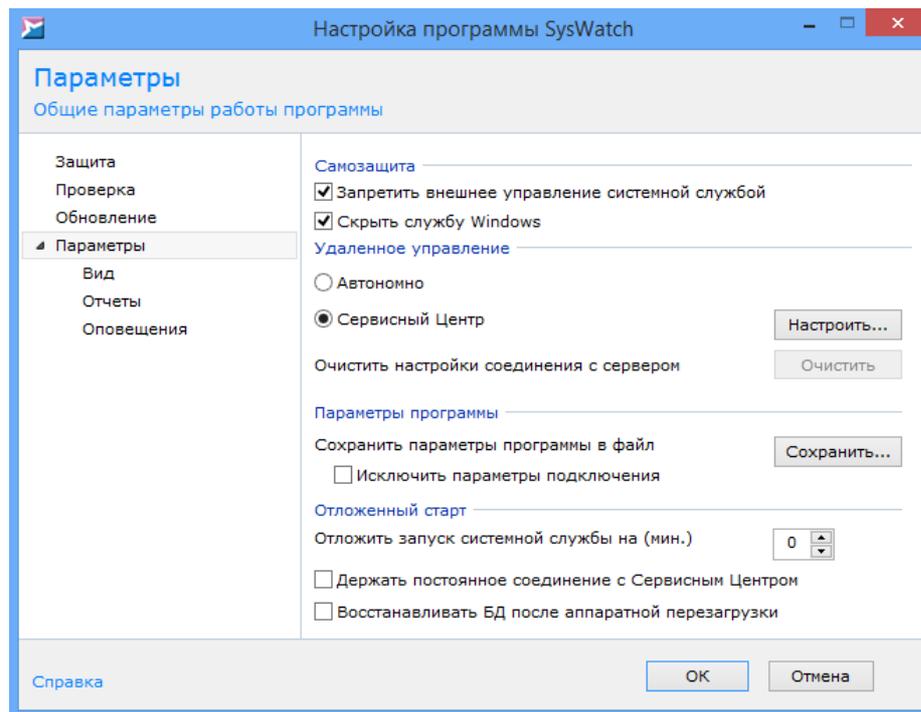


Рисунок 81. Настройки параметров программы

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 закодированном 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.

6. Расширенные возможности SoftControl SysWatch

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

7. Обновление SoftControl SysWatch

На момент установки приложения в модули SoftControl SysWatch могут быть добавлены улучшения и новые функции. Рекомендуется выполнить обновление программы непосредственно после установки SoftControl SysWatch.

Далее описаны необходимые действия по обновлению SoftControl SysWatch:

- [опции обновления](#)⁽¹⁰⁰⁾,
- [обновление в обычном режиме](#)⁽¹⁰³⁾.

В случае, если источник обновления недоступен, выполните [обновление в ручном режиме](#)⁽¹⁰⁴⁾.

7.1 Опции обновления

Для настройки параметров обновления откройте раздел **Обновление** настроек программы (рис. [Настройки параметров обновления](#)⁽¹⁰⁰⁾).

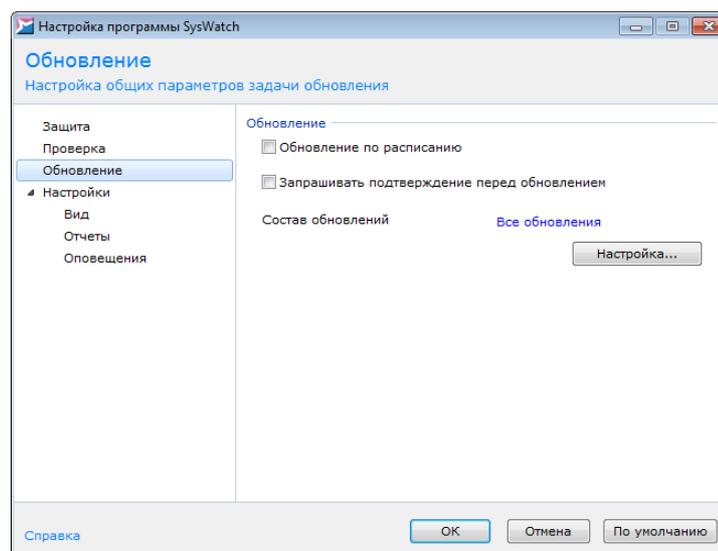


Рисунок 82. Настройки параметров обновления

▼ 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](#)⁽¹⁰¹⁾):

- **Обновить через Сервисный Центр** – обновление посредством внутрисетевого сервера обновлений (используется при [удаленном режиме управления с сер-](#)

[вера](#)⁽⁴¹⁾);

- **Обновить через интернет** – обновление через сервер обновлений ООО «АРУДИТ СЕКЬЮРИТИ», 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.

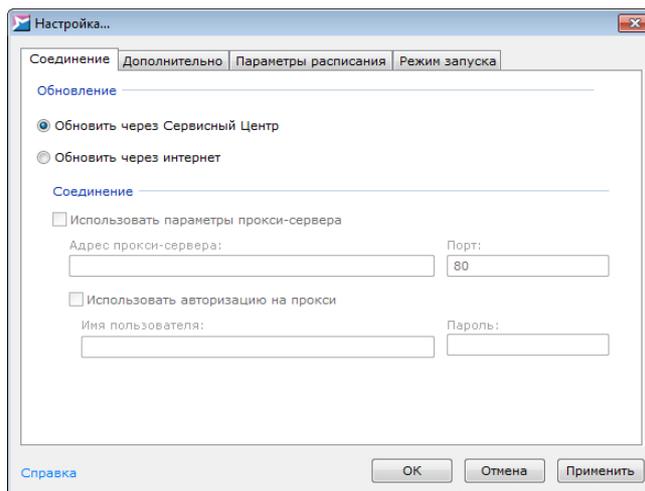


Рисунок 83. Настройки способа обновления

В окне **Настройка...** на вкладке **Дополнительно** выберите требуемые компоненты для обновления.

В области **Источник обновлений** указаны адреса, с которых производится обновление ядра проактивной защиты и каждого из доступных согласно [лицензии](#)⁽⁴³⁾ компонентов. При необходимости адреса могут быть отредактированы в соответствующем поле.

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

▼ **Настройка обновления по расписанию**

Условие: только для случая работы SoftControl SysWatch в режиме [удаленного управления с сервера](#)⁽⁴¹⁾.

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

В окне **Настройка...** откройте вкладку **Параметры расписания** и в счетчике **Часто-**

та 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](#)⁽¹⁰²⁾).

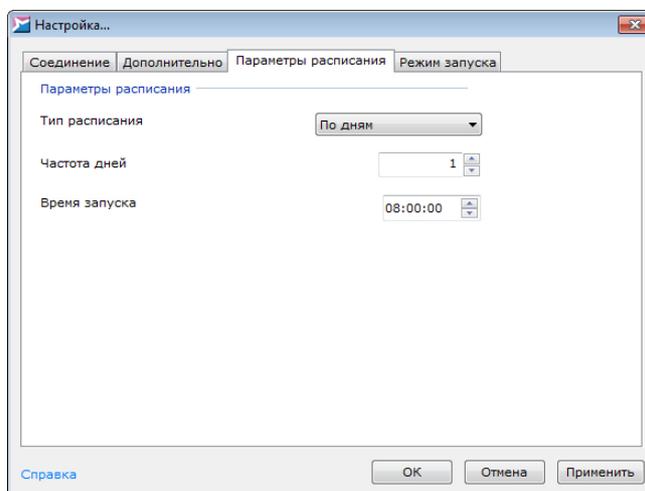


Рисунок 84. Настройки параметров обновления по расписанию

Для применения настроек нажмите на кнопку **ОК** 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](#)⁽¹⁰²⁾):

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

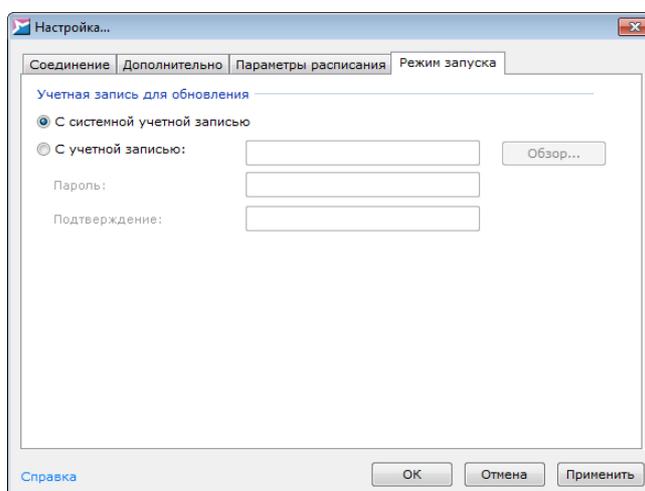


Рисунок 85. Настройки учётной записи для обновления

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

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

7.2 Обновление в обычном режиме

▼ Обновление программных по требованию

Нажмите на кнопку **Запустить обновление** на вкладке **Обновление панели управления**⁽³⁵⁾ 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 производиться 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⁽¹⁰¹⁾ 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 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

ку **Подробнее**. Для просмотра [отчета](#)⁽⁸⁹⁾ 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 последнего обновления** 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](#)⁽¹⁰⁴⁾).

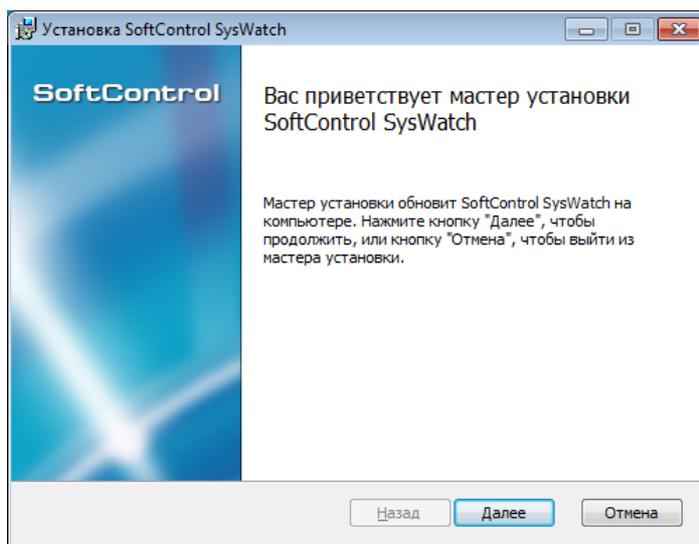


Рисунок 86. Запуск программы обновления

- 3) В случае вашего согласия, выберите параметр **Я принимаю условия лицензионного соглашения** и нажмите на кнопку **Далее**.
- 4) Нажмите на кнопку **Обновить** (рис. [Готовность к обновлению](#)⁽¹⁰⁴⁾).

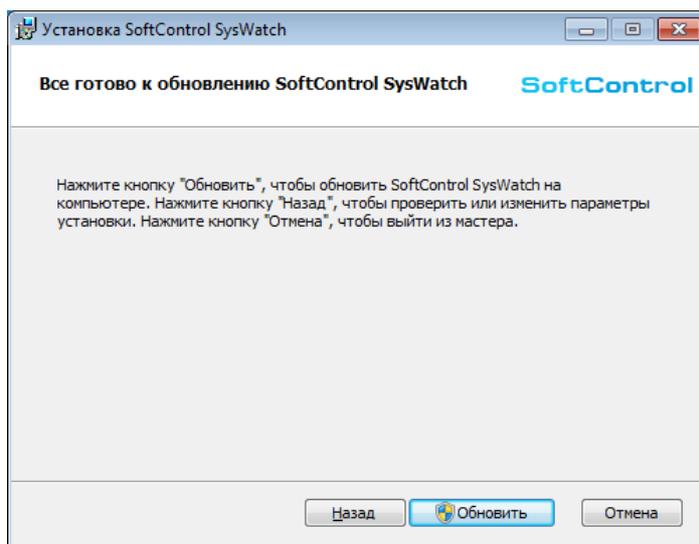


Рисунок 87. Готовность к обновлению

5) Дождитесь окончания процесса обновления (рис. [Процесс обновления](#)⁽¹⁰⁵⁾).

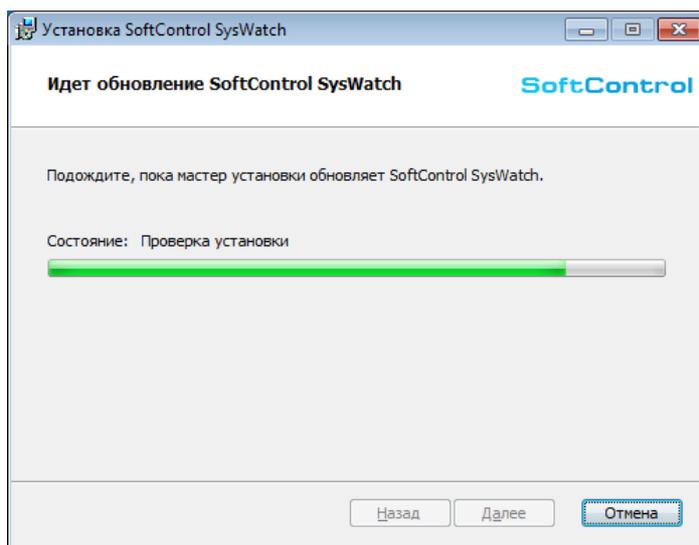


Рисунок 88. Процесс обновления

6) После появления сообщения **Установка SoftControl SysWatch завершена** нажмите на кнопку **Готово** (рис. [Завершение обновления](#)⁽¹⁰⁵⁾).

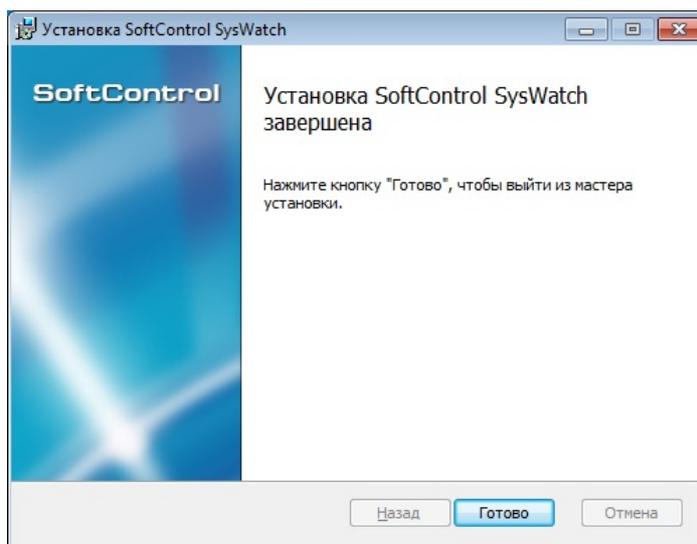


Рисунок 89. Завершение обновления

- 7) В диалоговом окне с предложением перезапуска системы выберите **Да**, после чего система будет отправлена на перезагрузку для завершения обновления (рис. [Запрос перезагрузки системы](#)⁽¹⁰⁶⁾).

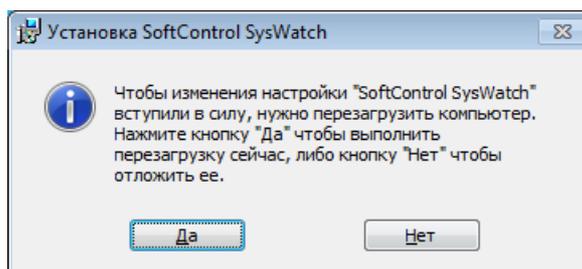


Рисунок 90. Запрос перезагрузки системы

▼ 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.

8. Удаление SoftControl SysWatch

SoftControl SysWatch может быть деинсталлирован с клиентских хостов как [локально](#)⁽¹⁰⁷⁾, так и одним из [удаленных централизованных](#)⁽¹⁰⁸⁾ способов.

8.1 Локальная деинсталляция

Возможны следующие варианты локальной деинсталляции SoftControl SysWatch:

- [в обычном режиме \(с использованием интерфейса пользователя\)](#)⁽¹⁰⁷⁾;
- [в тихом режиме](#)⁽¹⁰⁸⁾.

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](#)⁽¹⁰⁷⁾).

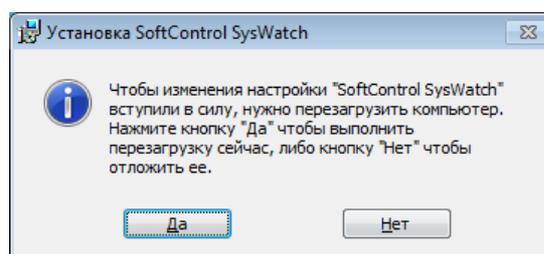


Рисунок 91. Запрос перезагрузки системы

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](#)⁽¹⁰⁸⁾;
- [сторонними средствами администрирования](#)⁽¹¹⁰⁾.

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](#)⁽¹⁷⁾ для развертывания клиентских приложений (**Clients deployment**), и выберите пункт **Edit** (рис. [Редактирование объекта групповой политики](#)⁽¹⁰⁸⁾).

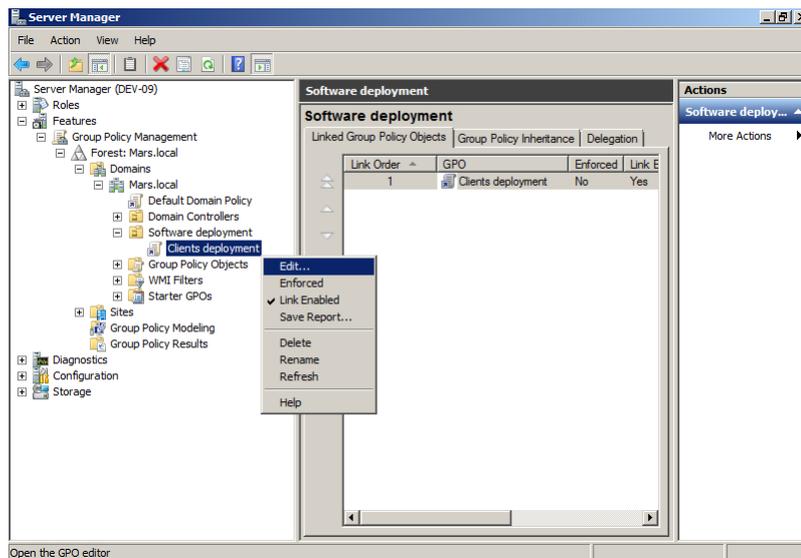


Рисунок 92. Редактирование объекта групповой политики

- 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](#)⁽¹⁰⁹⁾).
- 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 **ОК** (рис. [Выбор метода деинсталляции приложения](#)⁽¹⁰⁹⁾).

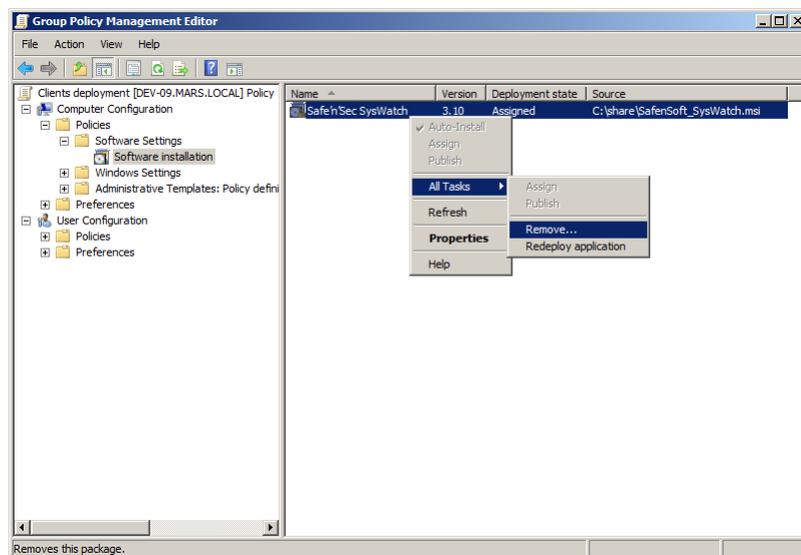


Рисунок 93. Вызов задачи удаления приложения

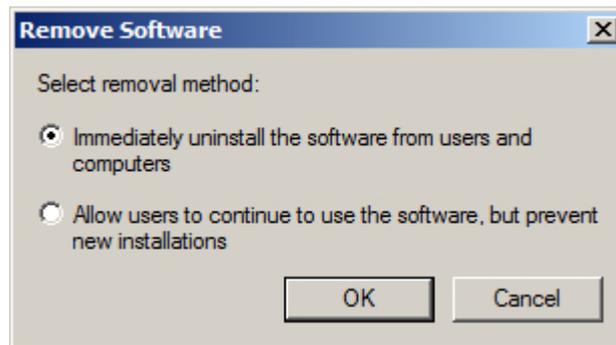


Рисунок 94. Выбор метода деинсталляции приложения

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](#)⁽¹¹⁰⁾).

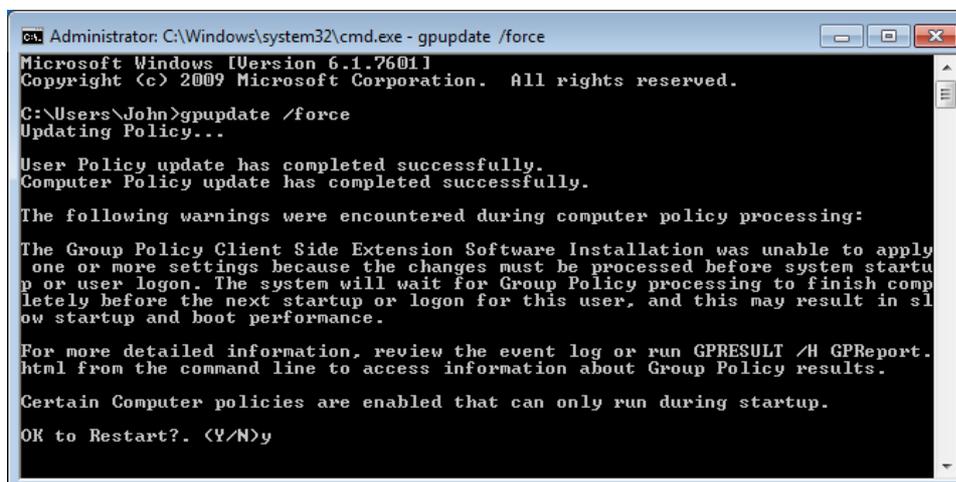


Рисунок 95. Ручное обновление параметров групповой политики

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 деинстал-

ляции ПО.

9. Техническая поддержка

При возникновении вопросов по установке, настройке и работе SoftControl ATM Client вы можете обращаться в техническую поддержку по электронной почте support@sns-control.ru.