



# **SoftControl**

## **Service Center 6.0.98**

Руководство администратора

Уважаемый пользователь!

ООО «АРУДИТ СЕКЬЮРИТИ» благодарит Вас за то, что выбрали продукт SoftControl Service Center. 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 Service Center 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](mailto:support@sns-control.ru)

Коммерческие вопросы: [sales@sns-control.ru](mailto:sales@sns-control.ru)

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

## Содержание

1. Введение	6
1.1 Назначение	6
1.2 Условные обозначения и термины	6
1.2.1 Обозначения	6
1.2.2 Сокращения	7
1.2.3 Глоссарий	7
2. Требования к аппаратному и программному обеспечению	9
2.1 Системные требования SoftControl Server	9
2.2 Системные требования SoftControl Admin Console	9
3. Установка и настройка компонентов SoftControl Service Center	11
3.1 Установка SoftControl Server и SoftControl Admin Console	11
3.1.1 Обычная установка	11
3.1.2 Полная установка	14
3.1.3 Выборочная установка	18
3.2 Настройка сервера	21
3.3 Регистрация клиентских приложений	27
3.4 Подключение к серверу из консоли управления	27
4. Централизованное управление СИБ	30
4.1 Интерфейс SoftControl Admin Console	30
4.2 Порядок работы	33
4.3 Управление доступом на основе ролей	34
4.3.1 Роли	35
4.3.2 Пользователи	37
4.3.3 События безопасности сервера	42
4.4 Клиенты	45
4.4.1 Управление процессом регистрации	50
4.4.2 Перемещение в подразделения	52
4.4.3 Управление списком разрешенных файлов	52
4.5 Подразделения	53
4.5.1 Управление подразделениями	55
4.5.2 Генерация одноразовых паролей	57
4.6 Настройка клиентских приложений	59
4.6.1 Общие настройки	62
4.6.2 Настройки SoftControl SysWatch	66
4.6.3 Настройки SoftControl DLP Client	115
4.6.4 Настройки SoftControl SysCmd	124

4.7	Профили безопасности.....	125
4.8	Задачи .....	127
4.8.1	Сбор профиля.....	131
4.8.2	Антивирусное сканирование.....	132
4.8.3	Обновление .....	134
4.8.4	Выполнение команд на клиенте и обмен файлами с клиентом.....	136
4.8.4.1	Создание задачи.....	137
4.8.4.2	Описание работы команд.....	139
4.8.4.3	Результаты выполнения команд.....	141
4.9	Просмотр отчетов.....	143
4.9.1	Отчеты SoftControl SysWatch.....	144
4.9.2	Отчеты SoftControl DLP Client.....	151
4.9.3	Отчеты SoftControl SysCmd .....	155
4.9.4	Интегрированный лог событий.....	157
4.9.5	Фильтрация событий.....	159
4.9.6	Запросы к базе данных.....	165
4.9.7	Печать и экспорт в файлы отчетов.....	167
4.9.8	Резервное копирование отчетов.....	168
4.9.9	Отправка событий по протоколу Syslog.....	169
4.10	Оповещения о событиях.....	170
4.10.1	Контакты .....	170
4.10.2	Нотификации.....	171
4.11	Снимки конфигурации.....	178
4.11.1	Снимки .....	179
4.11.2	Задачи снимков.....	182
5.	Обновление компонентов СИБ .....	185
5.1	Настройка обновления программных модулей.....	185
5.2	Настройка обновления антивирусных баз.....	189
5.3	Обновление SoftControl Server и SoftControl Admin Console в ручном режиме.....	191
5.4	Обновление клиентских компонентов.....	194
6.	Удаление компонентов SoftControl Service Center .....	195
7.	Диагностика проблем .....	199
8.	Техническая поддержка .....	203
9.	Приложение .....	204
9.1	Установка и настройка PostgreSQL 9.5.....	204
9.2	Установка и настройка Microsoft® SQL Server® 2008.....	208
9.3	Добавление компонента Desktop Experience.....	225

10. Дополнительная информация	230
10.1 О сертификатах.....	230
10.2 Управление сертификатами.....	232
10.3 Восстановление связи с сервером.....	233
10.4 Резервное копирование SoftControl Service Center.....	234
10.4.1 Создание резервной копии.....	234
10.4.2 Восстановление из резервной копии.....	236
10.5 Привилегии процессов.....	237
10.6 Трафик SoftControl SysWatch.....	239
10.7 Источники .....	242
10.8 Обновление клиентских компонентов и антивирусных баз на Windows XP.....	242

# 1. Введение

## 1.1 Назначение

SoftControl Service Center («Сервисный Центр») представляет собой набор инструментов администрирования для управления системой информационной безопасности, обеспечивающей сохранение целостности программной среды конечных точек сети, защиту от несанкционированного доступа к данным со стороны персонала или злоумышленников, а также мониторинг активности пользователей. В состав Сервисного Центра входят следующие компоненты:

- SoftControl Server – серверный компонент;
- SoftControl Admin Console – консоль управления.

SoftControl Service Center поддерживает работу со следующими клиентскими компонентами:


- SoftControl ATM Client / Endpoint Client / SClient (далее по тексту – SoftControl SysWatch) – клиентские компоненты проактивной защиты устройств самообслуживания, рабочих станций корпоративной сети и серверов соответственно;
- SoftControl DLP Client – клиентский компонент мониторинга и сбора данных;
- SoftControl SysCmd – клиентский компонент для выполнения команд на удаленном компьютере и обмена с ним файлами;
- SoftControl DeCrypt – клиентский компонент для шифрования системных дисков устройств самообслуживания, рабочих станций корпоративной сети и серверов.

## 1.2 Условные обозначения и термины

### 1.2.1 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.
<b>Обновить</b>	– заголовки и сокращения; – названия экранных кнопок, ссылок, пунктов меню, других элементов

	программного интерфейса.
Политика контроля	– термины (определения); – имена файлов и других объектов; – тексты сообщений, выводимых пользователю.
C:\Program Files\SoftControl	Пути к файлам, каталогам, ключам системного реестра.
%windir%\system32 \msiexec.exe /i	Фрагменты программного кода, командных и конфигурационных файлов.
<каталог установки SoftControl Service Center	Поля для замены функциональных названий фактическими значениями.
<a href="#">Приложение</a> <sup>(6)</sup>	Ссылки на внутренние ресурсы (разделы документа) с указанием номера страницы или на внешние ресурсы (URL-адреса).

## 1.2.2 Сокращения

В данном документе употребляются без расшифровки следующие сокращения:

- ❖ **БД** – база данных;
- ❖ **ГИП** – графический интерфейс пользователя;
- ❖ **ОЗУ** – оперативное запоминающее устройство;
- ❖ **ОС** – операционная система;
- ❖ **ПО** – программное обеспечение;
- ❖ **СИБ** – система информационной безопасности;
- ❖ **СУБД** – система управления базами данных;
- ❖ **ЦП** – центральный процессор;
- ❖ **ЭЦП** – электронная цифровая подпись.

## 1.2.3 Глоссарий

Таблица 2. Глоссарий

Термин	Пояснение
Проактивная защита	Комплекс мер по предотвращению вредоносных воздействий, основанный на превентивных технологиях.
Превентивные технологии	Передовые технологии защиты данных, в основе которых лежит анализ активности на компьютере пользователя: действий любых приложений, служб операционной системы, действий пользователя, активности извне и т.д. В отличие от реактивных технологий, на которых построены такие средства защиты, как антивирусы и персональные сетевые экраны, превентивные технологии анализируют не код объекта, а отслеживают потенциально опасные действия, выполняемые им. Следовательно, инструменты проактивной защиты не требуют наличия и постоянного обновления баз вредоносного кода, что является необходимым для традиционных средств защиты.
Реактивные (сигнатурные) технологии	Метод работы антивирусного программного обеспечения и систем обнаружения вторжений, при котором программа в процессе анализа

	объекта обращается к базе данных известных вирусов и проверяет соответствие какого-либо участка кода просматриваемого объекта известному коду (сигнатуре) вируса в базе данных.
Политика контроля	Целостный набор <b>правил контроля активности</b> .
Правило контроля активности	Набор условий, определяющих действие приложения и реакцию на него SoftControl SysWatch.
Профиль системы	База данных, хранящаяся локально на <b>клиентском хосте</b> и содержащая контрольные суммы <b>исполняемых модулей</b> . Профиль системы создается в результате автоматической настройки SoftControl SysWatch (операция сбора профиля).
Приложение в профиле	Приложение, контрольная сумма которого есть в <b>профиле системы</b> .
Отслеживаемое приложение	Приложение, факт запуска которого SoftControl SysWatch обнаружил на <b>клиентском хосте</b> в процессе работы с момента установки.
Доверенное приложение	<b>Отслеживаемое приложение из доверенной зоны выполнения.</b>
Ограниченное приложение	<b>Отслеживаемое приложение из ограниченной зоны выполнения.</b>
Запрещенное приложение	<b>Отслеживаемое приложение из запрещенной зоны выполнения.</b> SoftControl SysWatch запрещает запуск таких приложений на клиентском хосте.
Зона выполнения (доверенная, ограниченная, запрещенная)	Отдельная <b>политика контроля</b> , применяемая к подмножеству <b>отслеживаемых приложений</b> . Всего на каждом <b>клиентском хосте</b> имеется 3 зоны выполнения: доверенная, ограниченная, запрещенная. Любое <b>отслеживаемое приложение</b> 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 <b>ограниченных приложений</b> .
Роль	Совокупность прав пользователя на использование отдельных функций SoftControl Admin Console.
PE-файл	Исполняемый файл в формате PE (Portable Executable). Данный формат используется в операционных системах семейства Microsoft® Windows® для исполняемых файлов (EXE), динамических библиотек (DLL) и некоторых других типов файлов.
Клиентский хост	Средство вычислительной техники (рабочая станция, сервер, терминал самообслуживания), на котором установлен SoftControl SysWatch.



## 2. Требования к аппаратному и программному обеспечению

### 2.1 Системные требования SoftControl Server

Таблица 3. Минимальные системные требования

ОС	Частота ЦП	Объем ОЗУ	Объем свободного пространства на жестком диске
<b>Клиентские операционные системы:</b>	3 ГГц	4 ГБ	100 МБ + дополнительно 4 ГБ в случае установки встроенной СУБД
Microsoft® Windows® 7 (SP1) 32-разрядная/64-разрядная			
Microsoft® Windows® 8 32-разрядная/64-разрядная			
Microsoft® Windows® 8.1 32-разрядная/64-разрядная			
Microsoft® Windows® 10 32-разрядная/64-разрядная			
<b>Серверные операционные системы:</b>			
Microsoft® Windows® Server 2008 (SP2) 32-разрядная/64-разрядная			
Microsoft® Windows® Server 2008 R2 64-разрядная			
Microsoft® Windows® Server 2012 64-разрядная			
Microsoft® Windows® Server 2012 R2 64-разрядная			
Microsoft® Windows® Server 2016 64-разрядная			
Microsoft® Windows® Server 2019 64-разрядная			

#### Дополнительные требования:

- Требуется Microsoft® .NET Framework 4.5.
- Поддерживаемые СУБД: PostgreSQL® 9.5, Microsoft® SQL Server® 2008, SQL Server® 2012, SQL Server® 2014 SP1, SQL Server® 2016, SQL Server® 2017.
- Для работы SQL Server® 2014 SP1 или SQL Server® 2012 на Windows Server 2008 R2 в ОС должен быть установлен пакет обновления SP1.
- Для серверных операционных систем поддерживаются только варианты установки ОС с рабочим столом.

### 2.2 Системные требования SoftControl Admin Console

Таблица 4. Минимальные системные требования

ОС	Частота ЦП	Объем ОЗУ	Объем свободного пространства на жестком диске
<b>Клиентские операционные системы:</b>	3 ГГц	4 ГБ	100 МБ
Microsoft® Windows® 7 (SP1) 32-разрядная/64-разрядная			
Microsoft® Windows® 8 32-разрядная/64-разрядная			
Microsoft® Windows® 8.1 32-разрядная/64-разрядная			

Microsoft® Windows® 10 32-разрядная/64-разрядная			
<b>Серверные операционные системы:</b>			
Microsoft® Windows® Server 2008 (SP2) 32-разрядная/64-разрядная			
Microsoft® Windows® Server 2008 R2 64-разрядная			
Microsoft® Windows® Server 2012 64-разрядная			
Microsoft® Windows® Server 2012 R2 64-разрядная			
Microsoft® Windows® Server 2016 64-разрядная			
Microsoft® Windows® Server 2019 64-разрядная			

**Дополнительные требования:**

- Microsoft® .NET Framework 4.5.
- Для серверных операционных систем поддерживаются только варианты установки ОС с рабочим столом с установленным компонентом Desktop Experience.

## 3. Установка и настройка компонентов SoftControl Service Center

В настоящем разделе приведена информация по [установке](#)<sup>(11)</sup> серверного компонента SoftControl Server («сервера») и консоли управления SoftControl Admin Console, [настройке](#)<sup>(21)</sup> SoftControl Server при первом [запуске](#)<sup>(27)</sup> SoftControl Admin Console, а также даны указания по [регистрации клиентских приложений](#)<sup>(27)</sup>.

### 3.1 Установка SoftControl Server и SoftControl Admin Console

Возможны следующие варианты развертывания SoftControl Service Center:

- [обычная](#)<sup>(11)</sup>: установка компонентов продукта без встроенной СУБД;
- [полная](#)<sup>(14)</sup>: установка компонентов продукта и встроенной СУБД;
- [выборочная](#)<sup>(18)</sup>: установка выбранных пользователем компонентов.

Если в сетевом доступе имеется настроенная СУБД или если ее планируется установить отдельно, выберите вариант обычной установки. Информация по отдельной установке СУБД дана в [приложении](#)<sup>(208)</sup>.

Для наиболее быстрого развертывания и настройки выберите вариант полной установки; в этом случае все необходимые действия, включая установку входящей в инсталлятор СУБД, выполняются установщиком SoftControl Service Center автоматически. В пакет установки SoftControl Service Center входит бесплатная СУБД Microsoft® SQL Server® 2014 Express SP1, обладающая всей необходимой функциональностью для работы сервера.

Если предпочтительно устанавливать серверный компонент, СУБД и консоль управления на разные компьютеры, используйте выборочную установку.

#### 3.1.1 Обычная установка

- 1) Запустите установочный пакет *Service.Center.msi*.
- 2) В окне **Установка SoftControl Service Center** нажмите на кнопку **Далее** (рис. [Запуск программы установки](#)<sup>(11)</sup>).

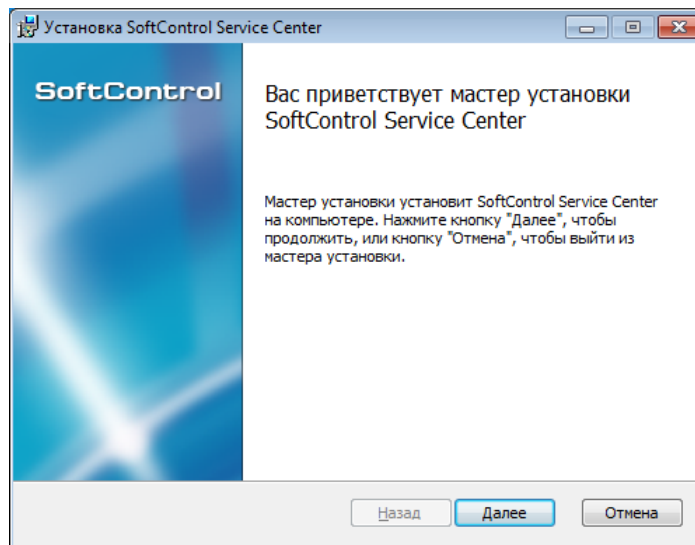


Рисунок 1. Запуск программы установки

3) В случае вашего согласия, отметьте опцию **Я принимаю условия лицензионного соглашения** и нажмите на кнопку **Далее** (рис. [Лицензионное соглашение](#)<sup>(12)</sup>).

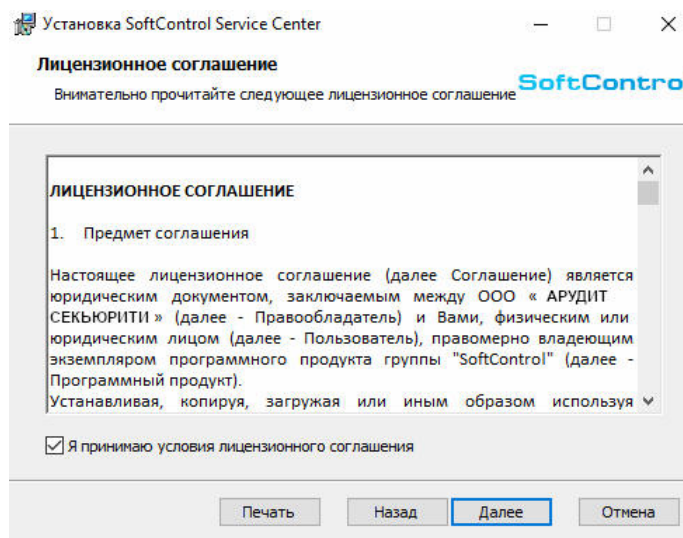


Рисунок 2. Лицензионное соглашение

4) Выберите тип установки **Обычная**, нажав на соответствующую кнопку (рис. [Типы установки](#)<sup>(12)</sup>).

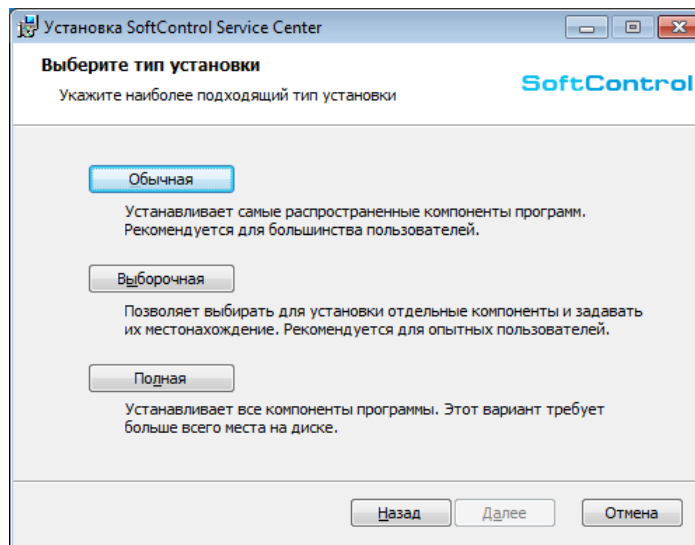


Рисунок 3. Типы установки

5) Нажмите на кнопку **Установить** (рис. [Готовность к установке](#)<sup>13</sup>).

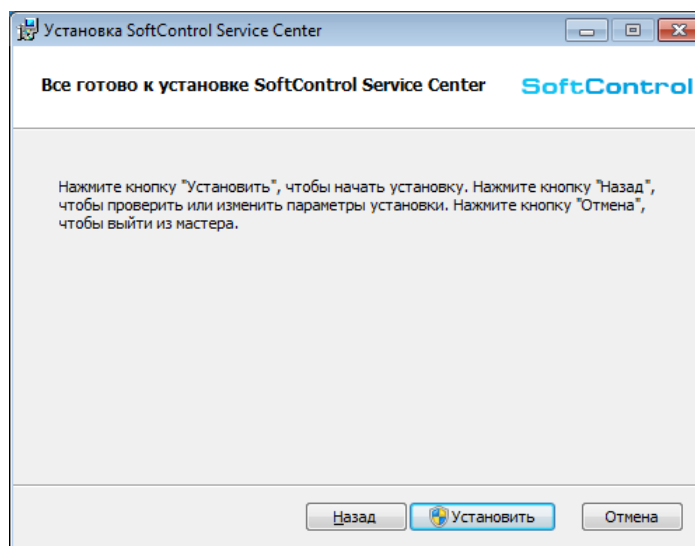


Рисунок 4. Готовность к установке

6) Дождитесь окончания процесса установки (рис. [Процесс установки](#)<sup>13</sup>).

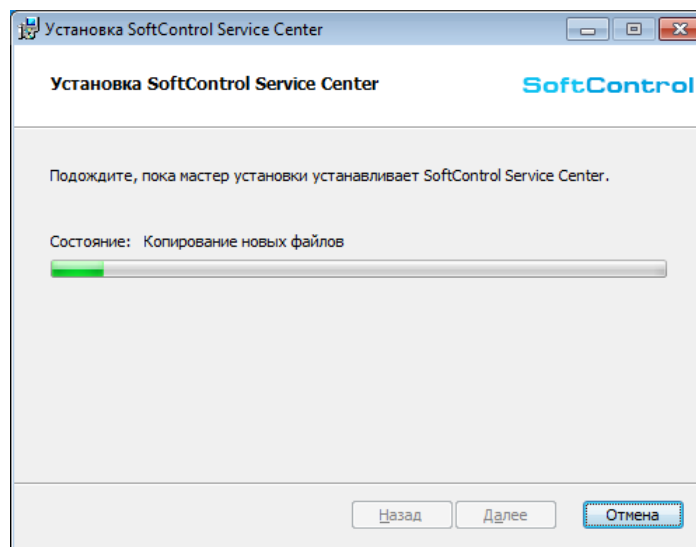


Рисунок 5. Процесс установки

7) После появления сообщения *Установка SoftControl Service Center завершена* нажмите на кнопку **Готово** (рис. [Завершение установки](#)<sup>(14)</sup>).

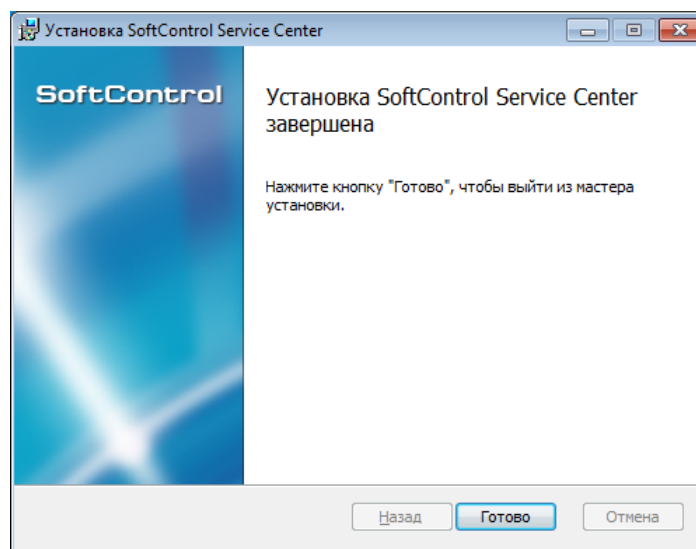


Рисунок 6. Завершение установки

### 3.1.2 Полная установка

- 1) Запустите установочный пакет *Service.Center.msi*.
- 2) В окне **Установка SoftControl Service Center** нажмите на кнопку **Далее** (рис. [Запуск программы установки](#)<sup>(14)</sup>).

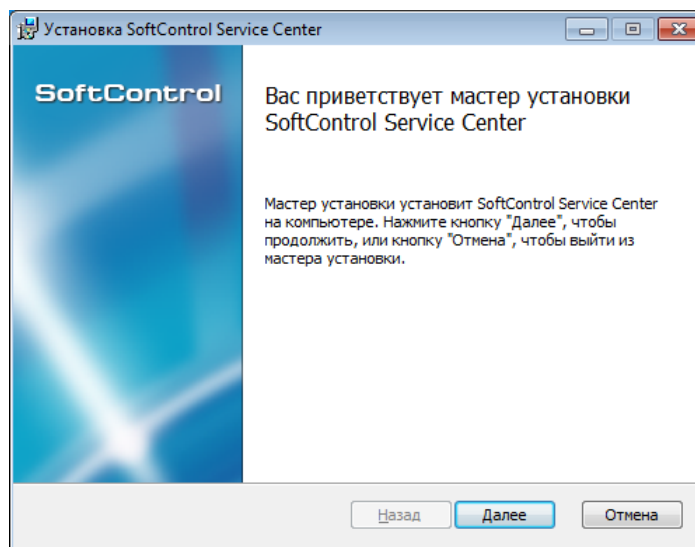


Рисунок 7. Запуск программы установки

3) В случае вашего согласия, отметьте опцию **Я принимаю условия лицензионного соглашения** и нажмите на кнопку **Далее** (рис. [Лицензионное соглашение](#)<sup>(15)</sup>).

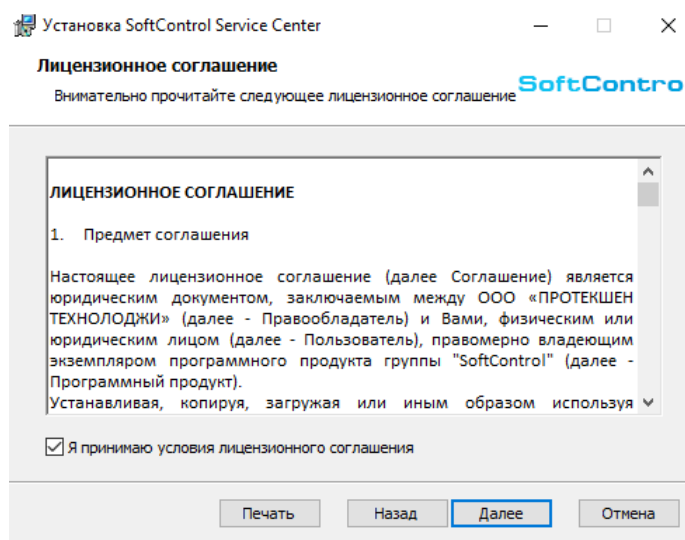


Рисунок 8. Лицензионное соглашение

4) Выберите тип установки **Полная**, нажав на соответствующую кнопку (рис. [Типы установки](#)<sup>(15)</sup>).

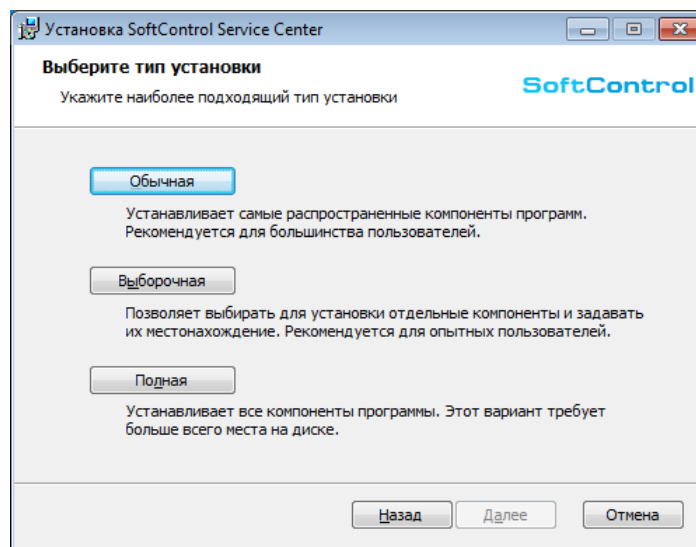


Рисунок 9. Типы установки

5) Нажмите на кнопку **Установить** (рис. [Готовность к установке](#)<sup>16</sup>).

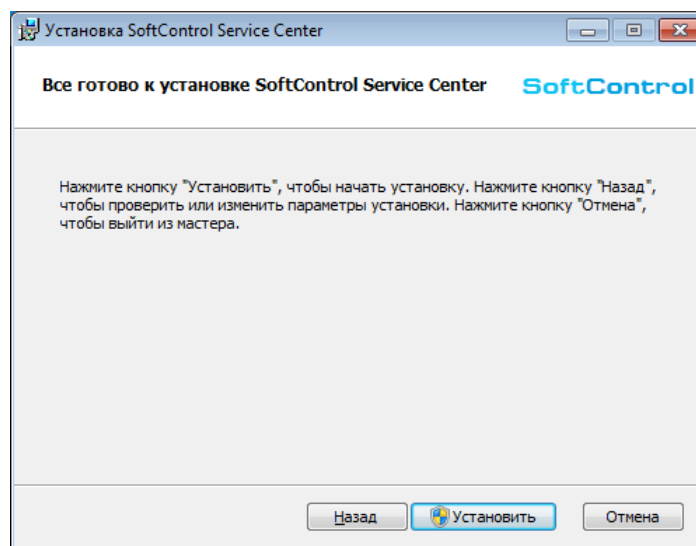


Рисунок 10. Готовность к установке

6) Дождитесь окончания процесса установки (рис. [Процесс установки](#)<sup>16</sup>).



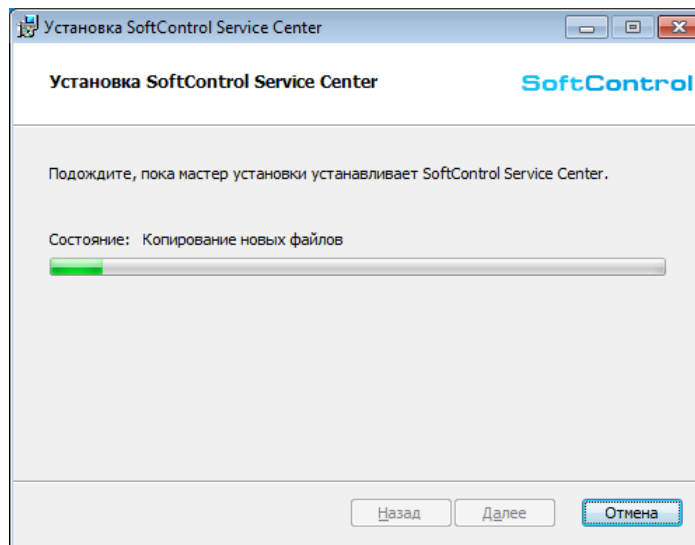


Рисунок 11. Процесс установки

7) После появления сообщения *Установка SoftControl Service Center завершена* нажмите на кнопку **Готово**, чтобы начать установку Microsoft® SQL Server® 2014 Express SP1 (рис. [Завершение установки SoftControl Service Center](#)<sup>(17)</sup>).

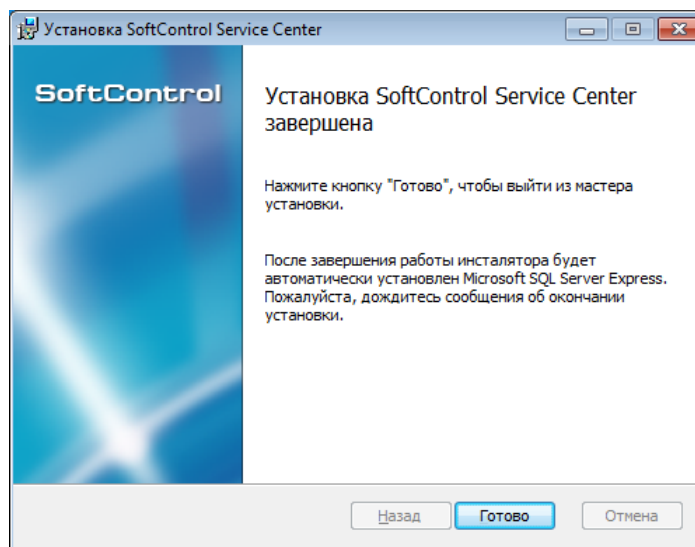


Рисунок 12. Завершение установки SoftControl Service Center

8) Дождитесь окончания установки Microsoft® SQL Server® 2014 Express SP1 и нажмите на кнопку **ОК** (рис. [Завершение установки](#)<sup>(17)</sup>).

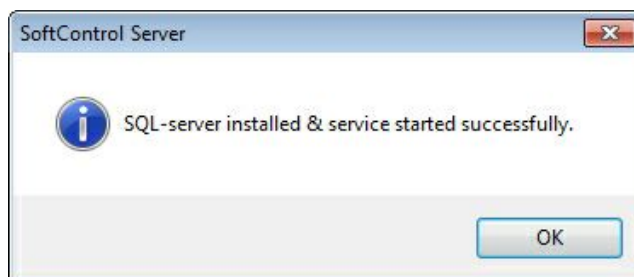


Рисунок 13. Завершение установки

### 3.1.3 Выборочная установка

- 1) Запустите установочный пакет *Service.Center.msi*.
- 2) В окне **Установка SoftControl Service Center** нажмите на кнопку **Далее** (рис. [Запуск программы установки](#)<sup>(18)</sup>).

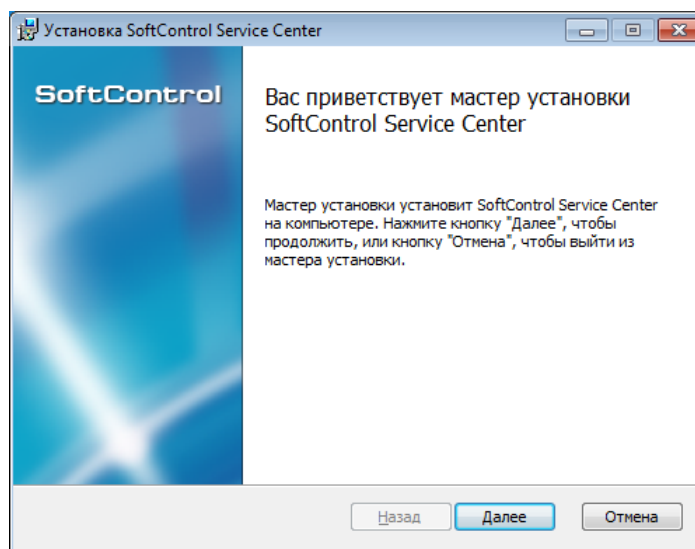


Рисунок 14. Запуск программы установки

- 3) В случае вашего согласия, отметьте опцию **Я принимаю условия лицензионного соглашения** и нажмите на кнопку **Далее** (рис. [Лицензионное соглашение](#)<sup>(18)</sup>).

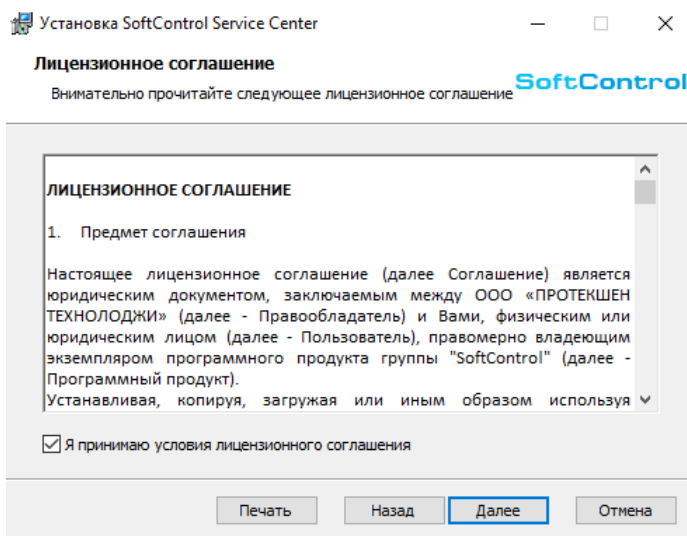


Рисунок 15. Лицензионное соглашение

4) Выберите тип установки **Выборочная**, нажав на соответствующую кнопку (рис. [Типы установки](#)<sup>(19)</sup>).

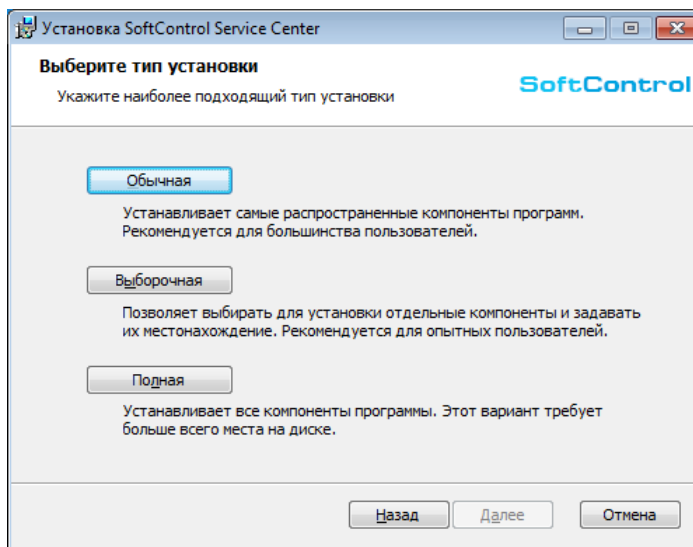


Рисунок 16. Типы установки

5) Настройте конфигурацию установки компонентов (рис. [Конфигурация установки компонентов](#)<sup>(20)</sup>): нажмите на пиктограмму у компонента, который не требуется устанавливать, и в выпадающем меню выберите опцию **Компонент будет полностью недоступен** (рис. [Опции установки компонента](#)<sup>(20)</sup>). Для устанавливаемого компонента должна быть выбрана опция **Будет установлен на локальный жесткий диск** (рис. [Опции установки компонента](#)<sup>(20)</sup>). При необходимости измените путь установки по умолчанию, нажав на кнопку **Обзор**. С помощью кнопки **Использование диска** можно просмотреть суммарный размер устанавливаемых компонентов и доступное место на

жестком диске. После того как все установки завершены, нажмите на кнопку **Далее**.

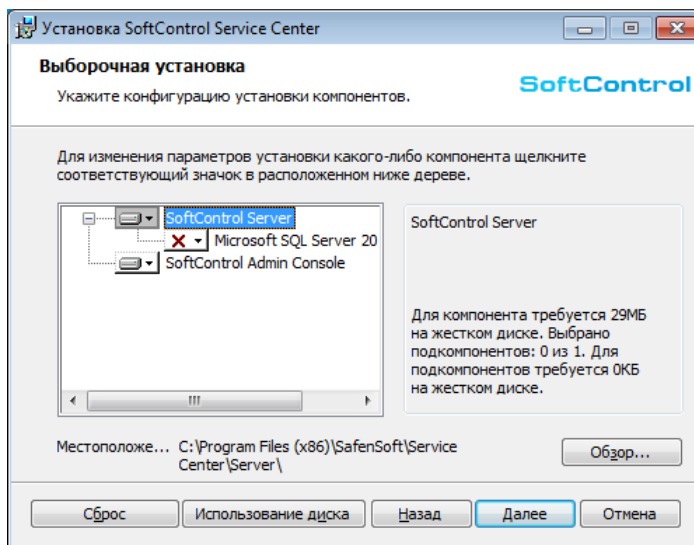


Рисунок 17. Конфигурация установки компонентов

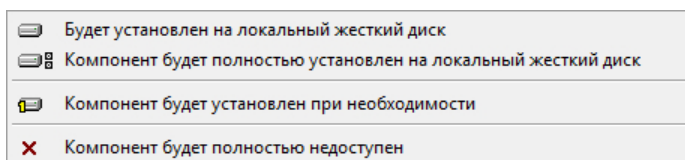


Рисунок 18. Опции установки компонента

- 6) Выберите опцию **Добавить необходимые порты в исключения Брандмауэра Windows** для автоматического добавления порта связи между SoftControl Admin Console и SoftControl Server в исключения брандмауэра (рис. [Опция добавления порта в исключения брандмауэра](#)<sup>(20)</sup>). В обратном случае будет необходимо произвести эту операцию вручную (по умолчанию используется порт 8080). Для продолжения установки нажмите на кнопку **Далее**.

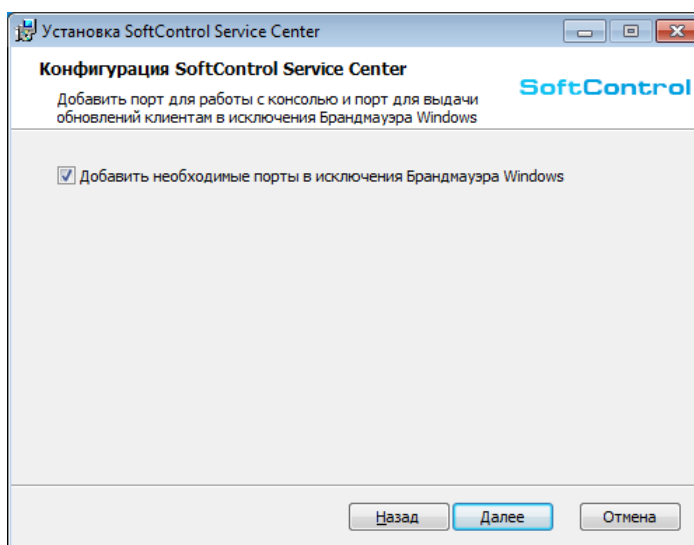


Рисунок 19. Опция добавления порта в исключения брандмауэра

7) В случае выбора установки SoftControl Admin Console и/или SoftControl Server без встроенной СУБД повторите действия 5-7 для [обычной установки](#)<sup>(13)</sup>. Если устанавливается SoftControl Server с подкомпонентом *Microsoft SQL Server® 2014 Express SP1*, повторите действия 5-8 для [полной установки](#)<sup>(16)</sup>.

## 3.2 Настройка сервера

Для запуска консоли управления откройте ярлык SoftControl Admin Console на рабочем столе. В случае неконфигурированного сервера в появившемся окне введите IP-адрес компьютера с установленным SoftControl Server в поле **Адрес сервера** (допускается указывать зарезервированное имя *localhost*, если SoftControl Server и SoftControl Admin Console установлены на одном компьютере) и нажмите на кнопку **Применить** (рис. [Первый запуск SoftControl Admin Console](#)<sup>(21)</sup>).

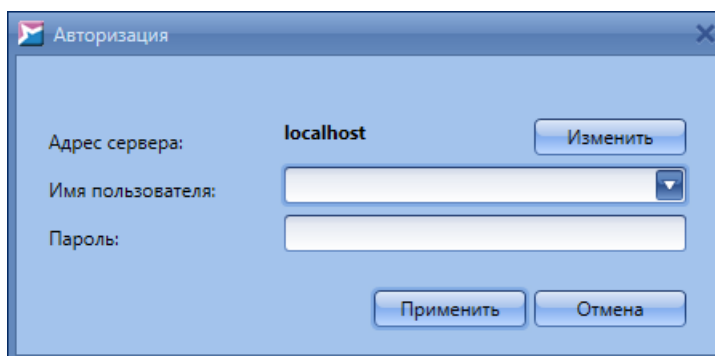


Рисунок 20. Первый запуск SoftControl Admin Console

В диалоговом окне с предложением создания первичной конфигурации сервера выберите **Да** (рис. [Предложение запуска мастера настройки](#)<sup>22</sup>).

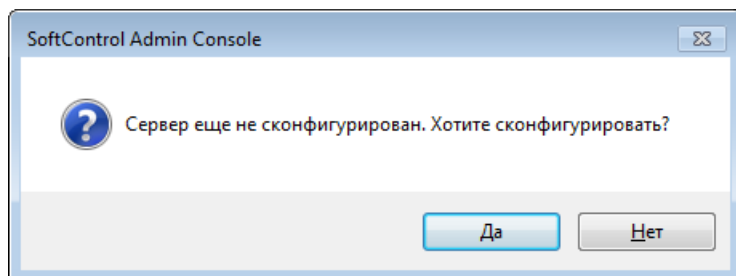


Рисунок 21. Предложение запуска мастера настройки

В окне мастера настройки сервера в разделе **База данных** задаются параметры подключения к СУБД и имя БД, которая будет использоваться серверным компонентом SoftControl Server. Введите следующие параметры (в скобках указаны значения по умолчанию для PostgreSQL):

- **SQL Provider** – тип СУБД (*PostgreSQL*);
- **Сервер СУБД** – сетевой адрес (имя) сервера СУБД (*localhost*);
- **Порт** – номер порта для работы сервера (*5432*);
- **Имя базы данных** – имя БД на сервере СУБД (*tpsecure*);
- **Пользователь** – имя пользователя на сервере СУБД (*postgres*);
- **Пароль** – пароль пользователя на сервере СУБД.

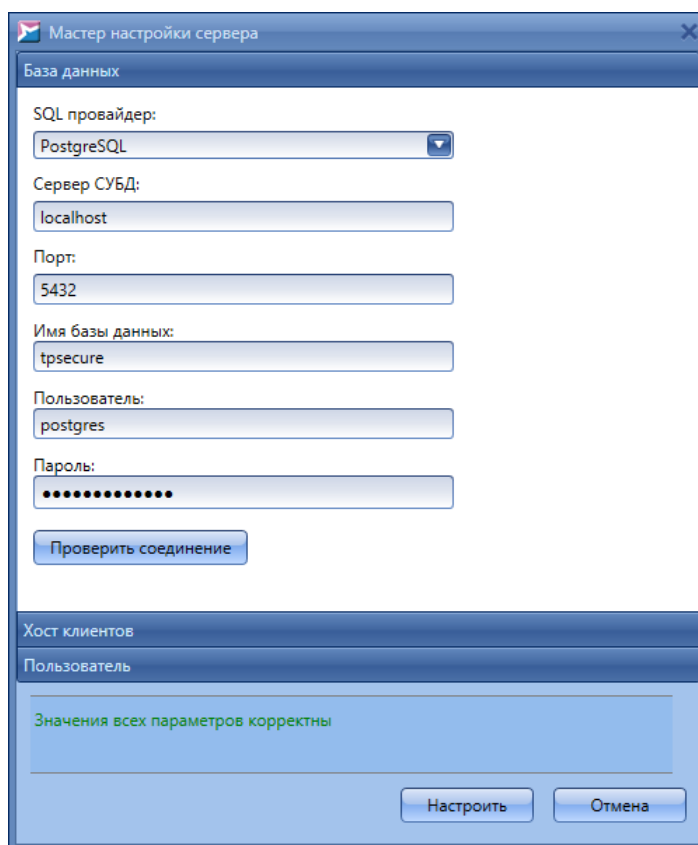


Рисунок 22. Настройка подключения к СУБД PostgreSQL

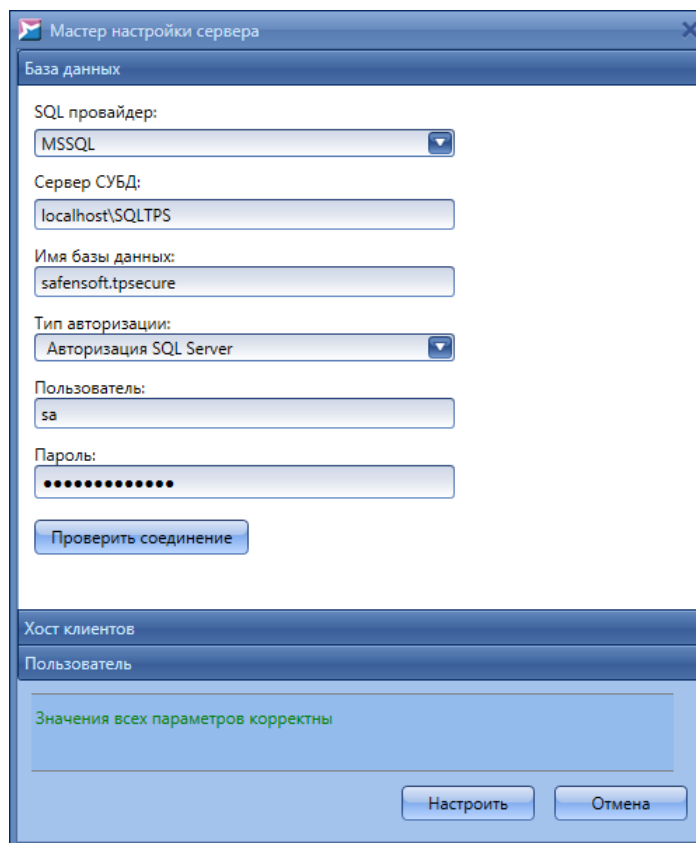


Рисунок 23. Настройка подключения к СУБД MS SQL Server

Для проверки соединения с СУБД и корректности данных учетной записи нажмите на кнопку **Проверить соединение**. Если БД с указанным именем не существует, то она будет создана на сервере СУБД по окончании работы мастера настройки.

В разделе **Хост клиентов** определяются параметры подключения клиентских приложений к серверу (рис. [Настройка подключения клиентских приложений к серверу](#)<sup>24</sup>).



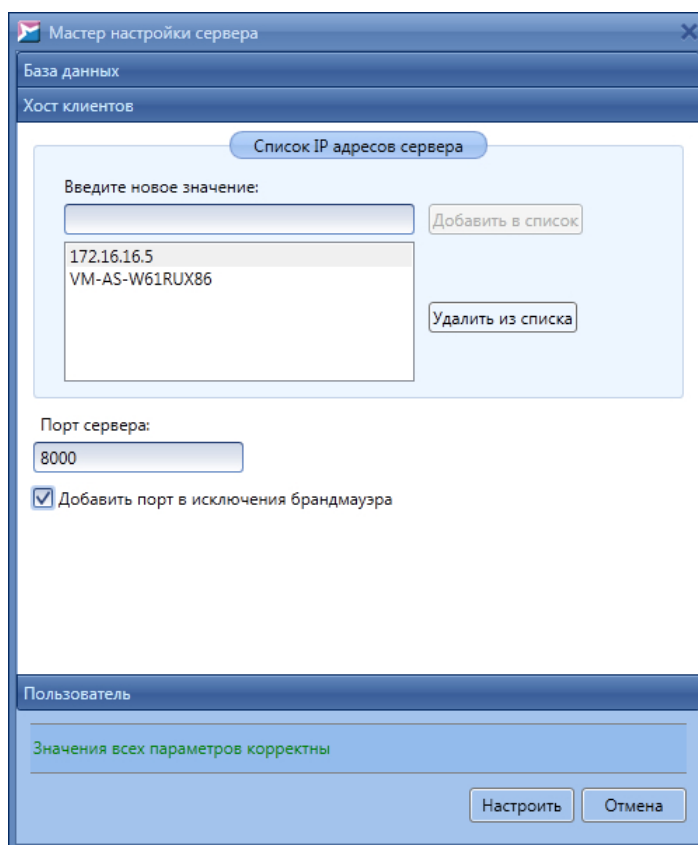


Рисунок 24. Настройка подключения клиентских приложений к серверу

По умолчанию для связи с сервером используется его текущий IP-адрес и порт 8000 протокола TCP. Возможно также осуществлять взаимодействие клиентских приложений с сервером по нескольким резервным каналам. Данная функция реализуется путем задания всех IP-адресов или имен (DNS, NetBIOS), по которым сервер доступен для клиентских приложений. В этом случае клиентский компонент осуществляет поочередное подключение по каждому из адресов до первой успешной обработки запроса, после чего связь с сервером устанавливается по данному адресу. Если подключиться ни по одному из адресов не удалось, то клиентский компонент повторяет перебор адресов по истечении интервала обращения к серверу. Чтобы добавить адрес в перечень, введите новое значение в соответствующем поле и нажмите на кнопку **Добавить в список**. Чтобы удалить адрес из перечня, выберите его и нажмите на кнопку **Удалить из списка**. В поле **Порт сервера** укажите порт связи клиентских приложений с сервером (в случае установки SoftControl Server и SoftControl Admin Console на один компьютер данный порт не должен совпадать с [портом связи SoftControl Server и SoftControl Admin Console](#)<sup>(28)</sup>). Установите флажок **Добавить порт в исключения Брандмауэра Windows** в том случае, если исключение на выбранный порт отсутствует в брандмауэре.

**i** Настоятельно рекомендуется указывать имя сервера в списке адресов, чтобы клиентские приложения не теряли связи с сервером даже в случае автоматической смены его IP-адреса. Если это все же произошло, воспользуйтесь [указаниями по восстановлению связи](#)<sup>233</sup>.

В разделе **Пользователь** создайте учетную запись первого пользователя, введя **Имя пользователя**, **Пароль** и **Подтверждение пароля** (рис. [Создание пользователя](#)<sup>26</sup>). Данный пользователь будет иметь права администратора.

Примечание. В дальнейшем пароль пользователя можно будет сменить, нажав на кнопку **Смена пароля** в правом нижнем углу SoftControl Admin Console на любой открытой вкладке (см. раздел [Пользователи](#)<sup>40</sup>).

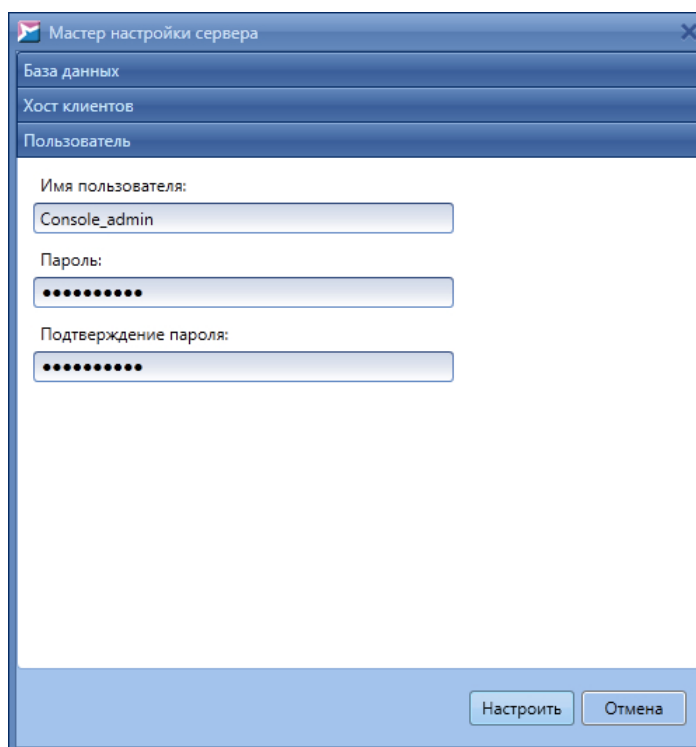


Рисунок 25. Создание пользователя

После того как все настройки введены, нажмите на кнопку **Настроить**. В случае успешного создания конфигурации отобразится соответствующее уведомление (рис. [Успешное создание конфигурации](#)<sup>26</sup>).

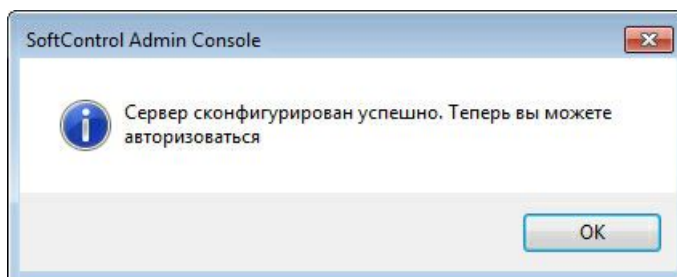


Рисунок 26. Успешное создание конфигурации

В [окне авторизации](#) <sup>(27)</sup> используйте данные созданной учетной записи для подключения к серверу SoftControl Server.

### 3.3 Регистрация клиентских приложений

После того как сервер прошел [первичную настройку](#) <sup>(21)</sup>, на компьютере с установленным SoftControl Server формируется зашифрованный конфигурационный файл по следующему пути:

C:\ProgramData\SafenSoft\ClientSettings.xmlc

Данный файл содержит параметры подключения клиентских приложений к серверу, а также [общий клиентский сертификат](#) <sup>(230)</sup>, используемый по умолчанию для установления безопасного соединения. Для регистрации в SoftControl Service Center необходимо применить указанный файл на устройствах с предварительно установленными по документации клиентскими приложениями.

---

**i** В режиме ожидания регистрации соединение с сервером осуществляется с использованием общего клиентского сертификата, при этом не происходит передача данных от клиента к серверу. Взаимодействие осуществляется в штатном режиме после перехода клиентского компонента в [статус](#) <sup>(45)</sup> **Активен**.

---

Подробные действия по применению файла описаны в документах «Руководство пользователя SoftControl ATM Client / Endpoint Client / SClient» и «Руководство по установке SoftControl DLP Client» для соответствующих компонентов.

### 3.4 Подключение к серверу из консоли управления

Для запуска консоли управления откройте ярлык SoftControl Admin Console на рабочем столе. В окне **Авторизация** введите **Адрес сервера**, **Имя пользователя** и **Пароль**, выберите **Токен** и введите его **PIN-код** (рис. [Авторизация пользователя в SoftControl Admin Console](#) <sup>(27)</sup>).

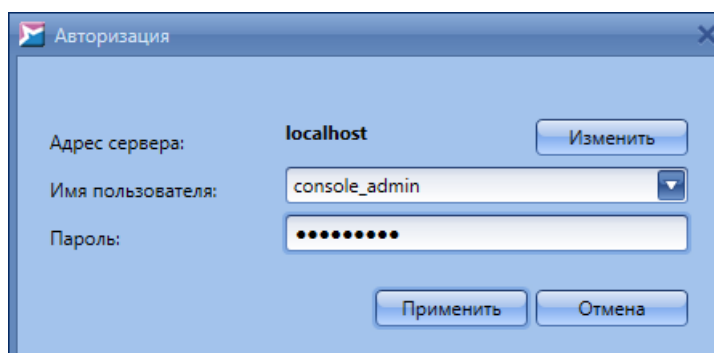


Рисунок 27. Авторизация пользователя в SoftControl Admin Console

Нажмите на кнопку **Применить**, чтобы подключиться к серверу SoftControl Server.

При аутентификации пользователя на сервере создается сессия, имеющая уникальный идентификатор. Вся работа пользователя с консолью управления осуществляется в рамках данной сессии, при этом с постоянной периодичностью проверяется наличие соединения между сервером и консолью управления. Если консоль управления недоступна для сервера более чем 2 минуты, то текущая сессия прекращается.



Для связи между SoftControl Admin Console и SoftControl Server по умолчанию используется порт 8080 протокола TCP. Если по какой-либо причине данный порт использовать не удастся, измените его значение в файлах конфигурации серверного компонента и консоли управления.

Файл конфигурации сервера расположен по следующему пути:

C:\ProgramData\SafenSoft\Server.Config.xml

Значение порта задается в атрибуте *Port* элемента *WebApiHost*.

Файл конфигурации консоли управления расположен по следующему пути:

C:\ProgramData\SafenSoft\SafenSoft.Enterprise.Console.exe.Config

Значение порта задается в следующем участке файла:

```
<Databases>
  <Elements>
    <add name="номер порта" lastconnection="" />
  </Elements>
</Databases>
```

При первом подключении с использованием токена SoftControl Service Center выводит сообщение о необходимости привязки учетной записи пользователя к токenu (см. рис. [ниже](#)<sup>(28)</sup>). Нажмите на кнопку **Да**, чтобы войти в систему и приступить к [централизованному управлению СИБ](#)<sup>(30)</sup>.

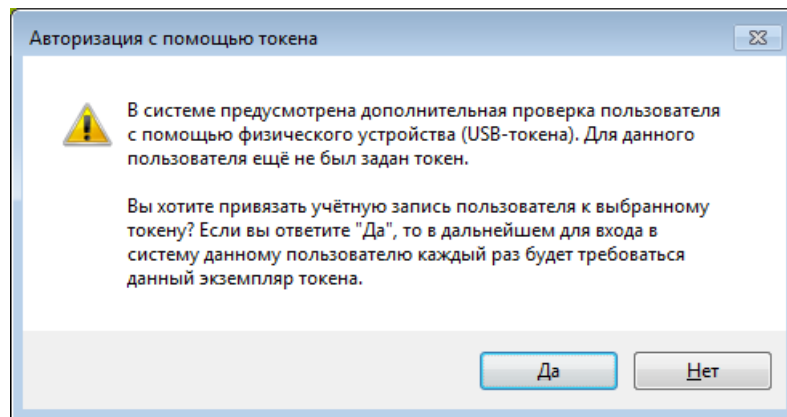


Рисунок 28. Сообщение о привязке учетной записи к токену.

Вы можете поменять токен, к которому была привязана учетная запись, в окне авторизации (см. [выше](#)<sup>27)</sup>) или на любой открытой вкладке SoftControl Admin Console, нажав на кнопку **Смена токена** в правом нижнем углу.

---

**i** Если число попыток подключения превышает заданное значение (5 по умолчанию), учетная запись пользователя блокируется. Значение выставляется в конфигурационном файле сервера с помощью параметра *PasswordAttempts*. Время действия блокировки (в секундах) задается с помощью параметра *LockForSeconds*. Разблокировать учетную запись может только системный администратор.

Кроме того, учетная запись блокируется, если она не использовалась в течение 45 дней (кроме пользователей с ролью **Системный администратор**).

---

**i** Если в течение 5 минут пользователь не совершал никаких действий, его сеанс блокируется. Для возобновления работы необходимо авторизоваться повторно.

---

## 4. Централизованное управление СИБ

Удаленное централизованное управление клиентскими приложениями SoftControl SysWatch, SoftControl DLP Client и SoftControl SysCmd осуществляется из консоли управления SoftControl Admin Console на базе сервисных функций, предоставляемых серверным компонентом SoftControl Server.

Данный раздел посвящен работе с SoftControl Admin Console и предназначен для администраторов системы информационной безопасности (далее по тексту – «СИБ») на основе SoftControl Service Center.

### 4.1 Интерфейс SoftControl Admin Console

Интерфейс консоли управления SoftControl Admin Console состоит из главного окна программы, в котором имеются следующие вкладки:

- [Лог событий](#)<sup>(143)</sup>;
- [События безопасности](#)<sup>(42)</sup>;
- [Интегрированный лог событий](#)<sup>(157)</sup>;
- [Клиенты](#)<sup>(45)</sup>;
- [Настройки клиентов](#)<sup>(59)</sup>;
- [Профили безопасности](#)<sup>(125)</sup>;
- [Подразделения](#)<sup>(53)</sup>;
- [Задачи](#)<sup>(127)</sup>;
- [Пользователи](#)<sup>(37)</sup>;
- [Роли](#)<sup>(35)</sup>;
- [Контакты](#)<sup>(170)</sup>;
- [Управление нотификациями](#)<sup>(171)</sup>;
- [Обновления](#)<sup>(185)</sup>;
- [Снимки конфигурации](#)<sup>(178)</sup>

Перечисленным выше вкладкам соответствуют графические кнопки, расположенные в верхней части главного окна SoftControl Admin Console под основным меню. Кроме того, вкладки [Клиенты](#)<sup>(45)</sup>, [Лог событий](#)<sup>(143)</sup>, [События безопасности](#)<sup>(42)</sup>, [Интегрированный лог событий](#)<sup>(157)</sup>, [Подразделения](#)<sup>(53)</sup>, [Настройки клиентов](#)<sup>(59)</sup>, [Профили безопасности](#)<sup>(125)</sup>, [Задачи](#)<sup>(127)</sup>, [Контакты](#)<sup>(170)</sup> и [Управление нотификациями](#)<sup>(171)</sup> имеют свои графические кнопки,

область действия которых распространяется только на данные вкладки. Основные кнопки SoftControl Admin Console описаны в табл. 5.

Таблица 5. Элементы управления SoftControl Admin Console

Кнопка	Название	Описание	Горячие клавиши
	Лог событий	Вызов вкладки <b>Лог</b> для всех клиентских компонентов.	
	События безопасности	Вызов вкладки <b>События безопасности</b> .	
	Интегрированный лог событий	Вызов вкладки <b>Интегрированный лог событий</b>	
	Клиенты	Вызов вкладки <b>Клиенты</b> .	F4
	Настройки клиентов	Вызов вкладки <b>Настройки клиентов</b> .	
	Профили безопасности	Вызов вкладки <b>Профили безопасности</b> .	
	Подразделения	Вызов вкладки <b>Подразделения</b> .	
	Задачи	Вызов вкладки <b>Задачи</b> .	
	Пользователи	Вызов вкладки <b>Пользователи</b> .	
	Роли	Вызов вкладки <b>Роли</b> .	
	Контакты	Вызов вкладки <b>Контакты</b> .	
	Управление уведомлениями	Вызов вкладки <b>Нотификации</b> .	
	Обновить	Обновление информации в текущей вкладке.	F5
	Выбрать колонки	Изменение состава полей таблицы текущей вкладки.	F6
	Сохранить настройки вида	Сохранение выбранного набора колонок в качестве пользовательского фильтра. Применима только к вкладке <b>Лог</b> .	F2
	Печать	Вывод текущего списка устройств или выборки событий на печать.	Ctrl + P
	Экспорт в Excel	Экспорт текущего списка устройств или выборки событий в файл формата XLSX (Microsoft® Excel®).	Ctrl + E
	Снимки конфигурации	Вызов вкладки <b>Снимки конфигурации</b>	
	Обновления	Вызов вкладки <b>Обновления</b> .	
	Сервер	Вызов настроек соединения с сервером.	

Часть функций, вызываемых с помощью основных кнопок, доступны также из главного

меню программы.

В нижней части окна отображается строка с именем текущего пользователя и его ролями.

В главном окне SoftControl Admin Console дополнительно возможны следующие действия:

#### ▼ **Настройка соединения с сервером**

Если необходимо просмотреть или изменить параметры соединения консоли управления и сервера во время работы SoftControl Admin Console, нажмите на кнопку **Сервер**.

Окно настроек подключения аналогично окну [авторизации](#)<sup>(27)</sup>, открываемому при запуске SoftControl Admin Console.

#### ▼ **Настройка интерфейса**

Для изменения настроек интерфейса SoftControl Admin Console в основном меню выберите пункт **Вид** → **Настройки**.

По умолчанию язык интерфейса SoftControl Admin Console выбирается при первом запуске программы исходя из региональных настроек ОС. Для изменения языка в окне **Настройка интерфейса** выберите требуемый вариант из выпадающего списка (рис. [Настройка интерфейса](#)<sup>(32)</sup>):

- **ru-RU** – русский;
- **en-US** – английский (США).

Чтобы изменения вступили в силу, необходимо перезапустить программу.

Установите флажок **Запускать только один экземпляр консоли**, если необходимо запретить возможность одновременного запуска нескольких экземпляров SoftControl Admin Console.

В поле **Размер страницы событий** задается максимальное количество событий, которое должно отображаться на одной странице вкладки [Лог](#)<sup>(159)</sup>.



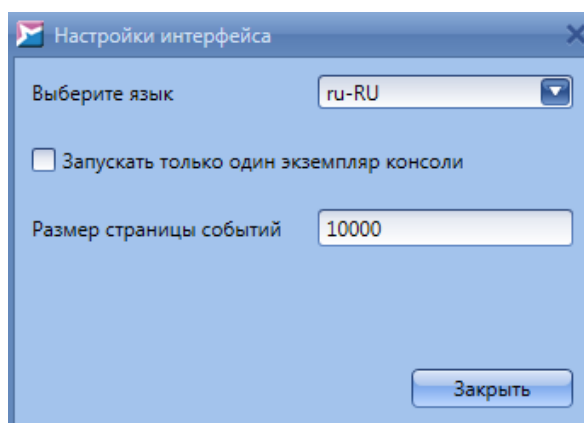


Рисунок 29. Настройка интерфейса

#### ▼ Просмотр информации о программе

В главном меню выберите пункт **О программе**.

## 4.2 Порядок работы

При администрировании СИБ на основе SoftControl Service Center из консоли управления SoftControl Admin Console рекомендуется придерживаться следующего порядка работы для снижения временных затрат и повышения продуктивности работы:

- 1) Откройте консоль управления SoftControl Admin Console, выполните [подключение к серверу SoftControl Server](#)<sup>(27)</sup>.
- 2) На вкладке **Роли** при необходимости создайте дополнительные [роли](#)<sup>(35)</sup> и назначьте [учетным записям](#)<sup>(37)</sup> пользователей роли с выбранными разрешениями. С помощью вкладки **События безопасности** производите [учет действий пользователей](#)<sup>(42)</sup> через консоль управления.
- 3) На вкладке **Клиенты** [подтвердите](#)<sup>(50)</sup> или [отклоните](#)<sup>(51)</sup> запросы на регистрацию от клиентских приложений, установленных на защищаемых устройствах.
- 4) После формирования рабочей области из необходимых устройств перейдите на вкладку **Настройки клиентов** и [создайте необходимые конфигурации](#)<sup>(60)</sup>, которые будут применяться для клиентских приложений.
- 5) После создания клиентских настроек перейдите на вкладку **Подразделения** и [создайте подразделения](#)<sup>(55)</sup> (группы) по какому-либо принципу для распределения в них зарегистрированных компонентов на клиентских хостах. При создании подразделений выполните их [привязку к определенным конфигурациям](#)<sup>(56)</sup>.

- 6) На вкладке **Клиенты** [переместите клиентские компоненты](#)<sup>52</sup> в созданные подразделения.
- 7) На вкладке **Задачи** создайте необходимые [задачи](#)<sup>127</sup> для клиентских приложений.
- 8) Перейдите на вкладку **Лог** и приступите к [просмотру отчетов клиентских компонентов](#)<sup>143</sup>.
- 9) Дополнительно можно [настроить оповещения](#)<sup>171</sup> об определенных событиях, которые будут отправляться на электронные почтовые ящики заданных [адресатов](#)<sup>170</sup>, а также [экспортировать и вывести на печать](#)<sup>167</sup> необходимые данные.

### 4.3 Управление доступом на основе ролей

В SoftControl Service Center реализована подсистема управления доступом на основе ролей (RBAC – Role Based Access Control). Данная подсистема позволяет производить разграничение доступа [пользователей](#)<sup>37</sup> к различным функциям Сервисного Центра в зависимости от делегированной им [роли](#)<sup>35</sup>.

Через SoftControl Admin Console осуществляется контроль действий пользователей с помощью регистрации [событий безопасности сервера](#)<sup>42</sup>.

### 4.3.1 Роли

Вкладка **Роли** позволяет управлять ролями и настраивать разрешения для них (рис. [Вкладка «Роли»](#)<sup>35</sup>).

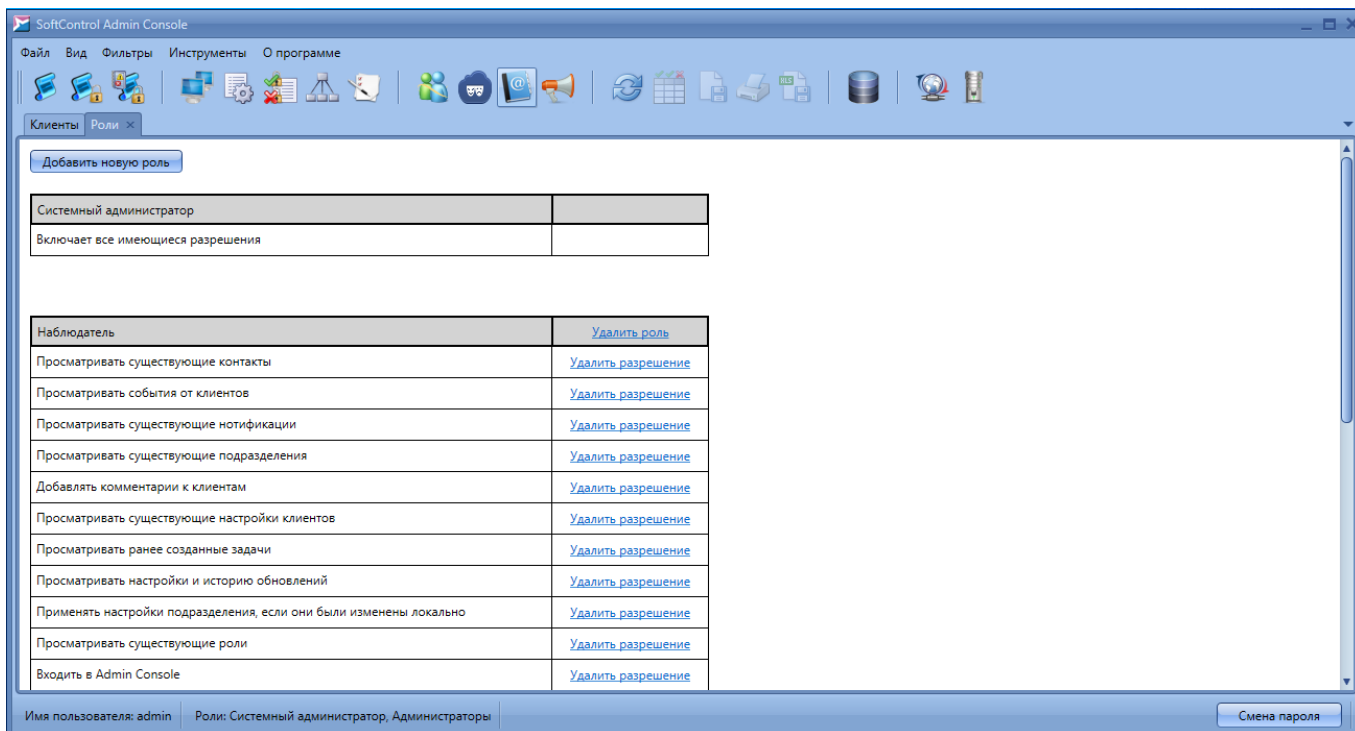


Рисунок 30. Вкладка «Роли»

Роли на вкладке представлены в виде таблиц, в первой строке которой указано имя роли, а в последующих – права на выполнение определенных операций в консоли управления (разрешения).

SoftControl Service Center включает в себя две предустановленные роли:

- **Системный администратор** – позволяет осуществлять доступ ко всей функциональности консоли управления. Рекомендуется для опытных пользователей/администраторов безопасности.
- **Наблюдатель** – дает права на просмотр основной части информации, включая все данные по работе с клиентскими приложениями. Рекомендуется для операторов, ведущих мониторинг инцидентов безопасности на клиентских хостах.

Помимо этого, можно создать новые роли с собственным набором разрешений. Ниже описаны действия с ролями, выполняемые на данной вкладке:

### ▼ Создание роли

Чтобы добавить роль, нажмите на кнопку **Добавить новую роль** (рис. [Вкладка «Роли»](#)<sup>(35)</sup>). В появившемся окне укажите **Имя роли** и нажмите на кнопку **ОК** (рис. [Создание новой роли](#)<sup>(36)</sup>).

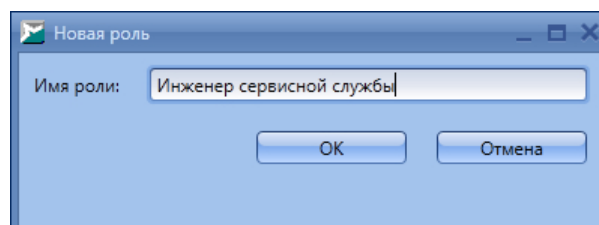


Рисунок 31. Создание новой роли

Новая роль будет добавлена в конец списка ролей. Далее задайте [разрешения](#)<sup>(36)</sup> для нее.

### ▼ Редактирование разрешений

Чтобы добавить разрешения к роли, нажмите на кнопку **Добавить разрешение** после таблицы с данной ролью. В появившемся окне отметьте необходимые разрешения и нажмите на кнопку **ОК** (рис. [Добавление разрешений](#)<sup>(36)</sup>).

Чтобы удалить разрешение, нажмите на ссылку **Удалить разрешение** в соответствующей строке таблицы с ролью (рис. [Вкладка «Роли»](#)<sup>(35)</sup>).

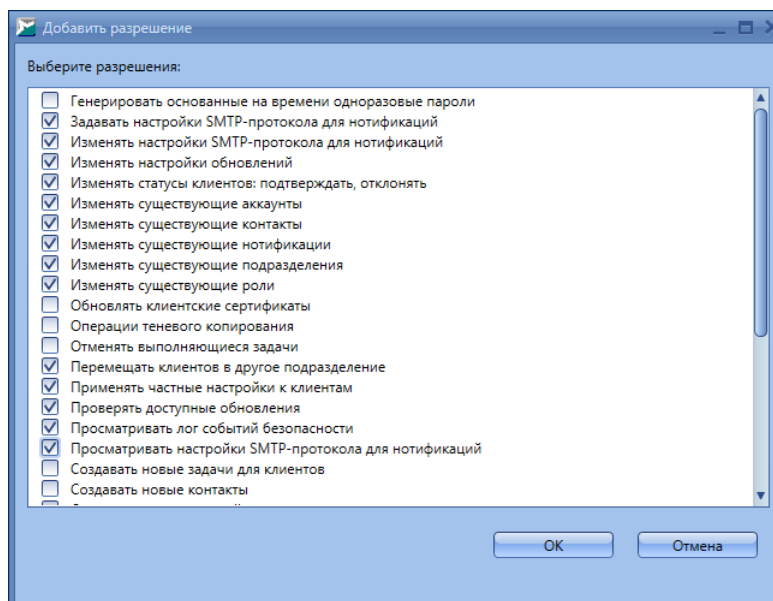


Рисунок 32. Добавление разрешений

### ▼ Удаление роли

Для удаления роли нажмите на ссылку **Удалить роль** в строке таблицы с именем роли (рис. [Вкладка «Роли»](#)<sup>(35)</sup>) и подтвердите удаление в диалоговом окне.

**i** Удаление ролей, которые присвоены имеющимся пользователям (см. раздел [ниже](#)<sup>(37)</sup>), невозможно.

## 4.3.2 Пользователи

На вкладке **Пользователи** производится управление учетными записями пользователей и назначение ролей для них (рис. [Вкладка «Пользователи»](#)<sup>(37)</sup>).

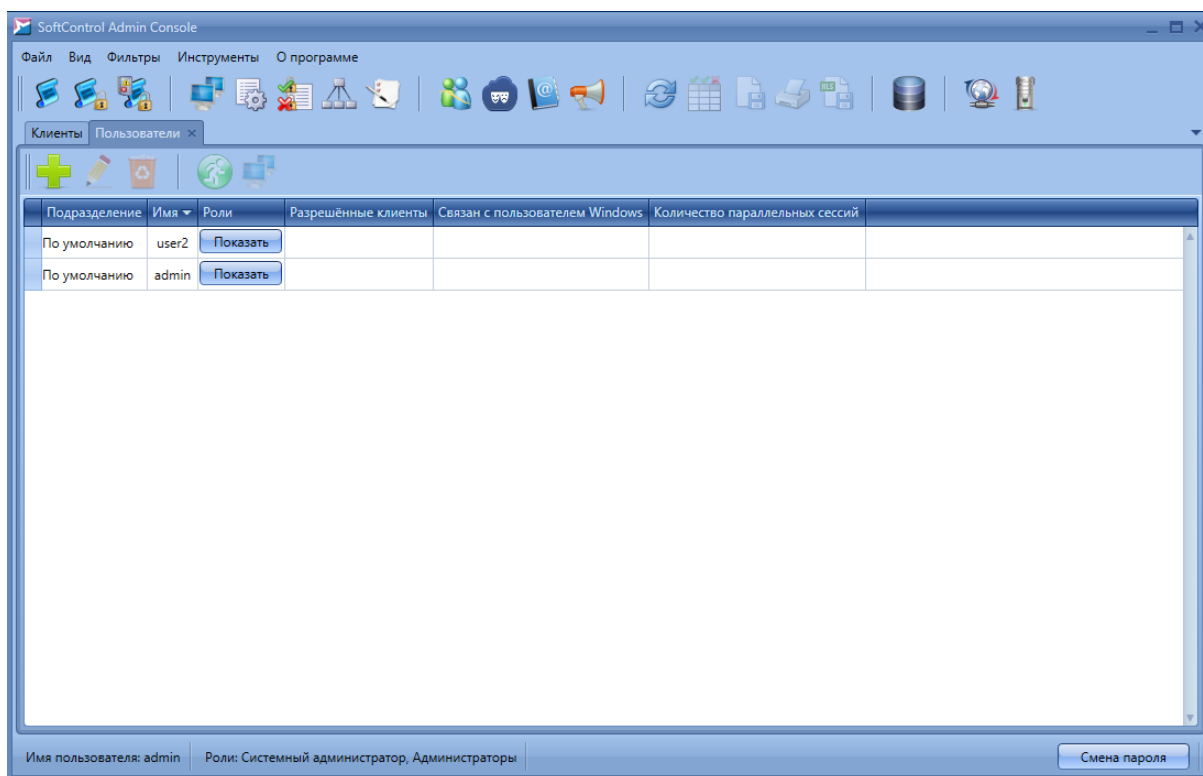






Рисунок 33. Вкладка «Пользователи»

Основные операции с учетными записями пользователей осуществляются с помощью графических кнопок вкладки, предназначение которых приведено в табл. 6.

Таблица 6. Элементы управления вкладки «Пользователи»

Кнопка	Название	Описание
	Добавить	Создание новой учетной записи.
	Редактировать	Редактирование свойств выбранной учетной записи.

Кнопка	Название	Описание
	Удалить	Удаление выбранных учетных записей.
	Переместить	Переместить выбранного пользователя в другое подразделение.

Перечень полей вкладки приведен в табл. 7.

Таблица 7. Поля вкладки «Пользователи»

Поле	Описание
Подразделение	Подразделение, к которому приписан данный пользователь.
Имя	Имя пользователя.
Роли	Роли, присущие пользователю.

Основные действия, выполняемые на данной вкладке:

#### ▼ Создание учетной записи

Чтобы добавить новую учетную запись, нажмите на кнопку **Добавить** (рис. [Вкладка «Пользователи»](#)<sup>37</sup>). В появившемся окне укажите **Имя** пользователя, введите **Пароль** учетной записи и его **Подтверждение**. Укажите необходимые **Роли** для создаваемого пользователя и нажмите на кнопку **Применить** (рис. [Создание учетной записи](#)<sup>38</sup>). Минимальная длина пароля задается в настройках SoftControl Server. Для этого в файле конфигурации сервера (C:\ProgramData\SafenSoft\Server.Config.xml) следует выставить требуемое значение для параметра MinPasswordLength.

Рисунок 34. Создание учетной записи

Область **Пользователь Windows** зарезервирована для будущего использования. Связанная с ней функциональность в текущей версии не реализована.

Все новые учетные записи автоматически помещаются в подразделение **По умолчанию**. Вы можете [переместить](#)<sup>41</sup> выбранную учетную запись в другое подразделение.

В зависимости от [роли](#)<sup>35</sup>, пользователь имеет доступ к информации в текущем подразделении и во всех дочерних подразделениях и не имеет доступа к информации в родительских подразделениях.

Вы также можете сделать учетную запись временной, выставив галочку **Временный пользователь** и указав дату блокировки.

#### ▼ Редактирование учетной записи

Чтобы изменить свойства учетной записи, нажмите на кнопку **Редактировать** (рис. [Вкладка «Пользователи»](#)<sup>37</sup>).

В появившемся окне измените **Имя** пользователя и/или измените **Роли** в соответствующей области, после чего нажмите на кнопку **Применить**

(рис. [Редактирование учетной записи](#)<sup>(40)</sup>). Пароль при этом останется без изменений. Если требуется сменить пароль, то введите новый **Пароль** в одноименном поле и его **Подтверждение**.

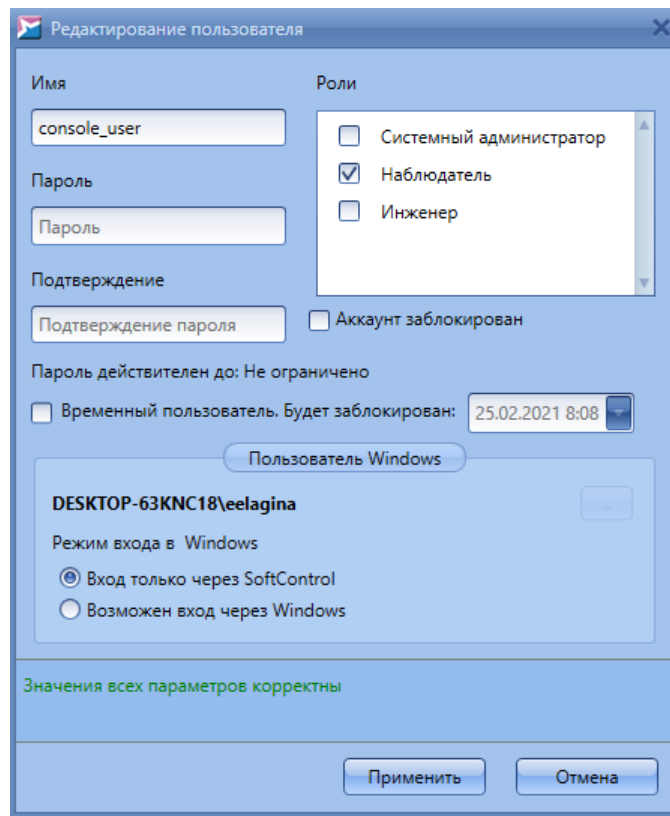


Рисунок 35. Редактирование учетной записи

Кроме того, любой пользователь может сменить свой пароль в окне, которое появляется при нажатии на кнопку **Смена пароля** в правом нижнем углу SoftControl Admin Console (см. рис. [Вкладка «Пользователи»](#)<sup>(37)</sup>). Кнопка доступна на любой открытой вкладке.

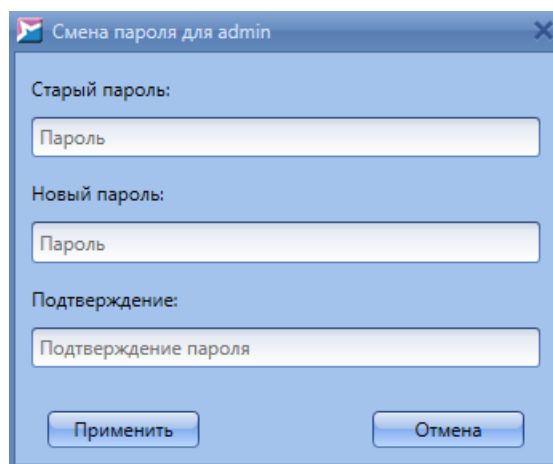


Рисунок 36. Смена пароля пользователя



В появившемся окне (рис. [Смена пароля пользователя](#)<sup>(40)</sup>) необходимо ввести старый **Пароль**, **Новый пароль** и его **Подтверждение** и нажать на кнопку **Применить**.

При смене пароля администратор может ограничить срок его действия. Для этого в файле конфигурации сервера (с:\ProgramData\SafenSoft\Server.Config.xml) следует выставить требуемое значение (количество дней) для параметра *PasswordValidDays* (по умолчанию 60 дней; 0 означает, что время действия пароля не ограничено). Минимальное время действия задается с помощью параметра *MinPasswordPeriodDays* и не может быть больше значения, установленного для параметра *PasswordValidDays*. Кроме того, можно выставить запрет на использование определенного числа старых паролей (от 1 до 10; параметр *ForbidOldPasswordCount*).

Если учетную запись необходимо заблокировать, выставите галочку **Аккаунт заблокирован** (рис. [Редактирование учетной записи](#)<sup>(40)</sup>).

#### ▼ Удаление учетной записи

Для удаления учетной записи выберите ее, нажмите на кнопку **Удалить** (рис. [Вкладка «Пользователи»](#)<sup>(37)</sup>) и подтвердите удаление в диалоговом окне.

Примечание. После удаления учетной записи создать новую учетную запись с таким же именем можно не ранее, чем через 3 года.

#### ▼ Перемещение учетной записи

Для перемещения учетной записи выберите ее, нажмите на кнопку **Переместить** и в появившемся окне укажите подразделение, в которое надо переместить данного пользователя (рис. [Перемещение учетной записи](#)<sup>(41)</sup>).

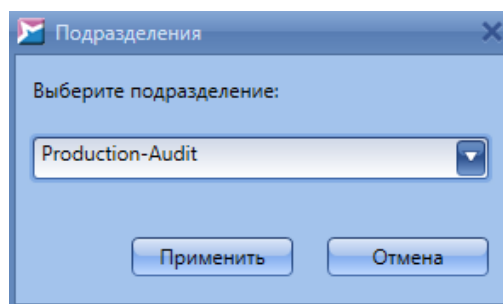


Рисунок 37. Перемещение учетной записи

### 4.3.3 События безопасности сервера

Консоль управления позволяет фиксировать операции, производимые пользователями, для дальнейшего анализа на вкладке **События безопасности** (рис. [Вкладка «События безопасности»](#)<sup>(43)</sup>).

Полный перечень полей вкладки приведен в таблице ниже.

Таблица 8. Поля вкладки «События безопасности»

Поле	Описание
Guid клиента	Уникальный идентификатор клиентского приложения (только для типов событий <b>Подтверждение клиента, Отклонение клиента, Удаление клиента, Перемещение клиента в другое подразделение</b> ).
Тип события	Тип зарегистрированного события: <ul style="list-style-type: none"> <li>• Начало сессии;</li> <li>• Конец сессии;</li> <li>• Роль создана;</li> <li>• Роль удалена;</li> <li>• К роли добавлены разрешения;</li> <li>• Удалено разрешение у роли;</li> <li>• Была создана учетная запись;</li> <li>• Учетная запись была изменена;</li> <li>• Учетная запись была удалена;</li> <li>• Подтверждение клиента;</li> <li>• Отклонение клиента;</li> <li>• Удаление клиента;</li> <li>• Запрос на изменение сертификата клиента;</li> <li>• Новый сертификат назначен клиенту;</li> <li>• Перемещение объекта в другое подразделение;</li> <li>• Создано новое подразделение;</li> <li>• Подразделение было удалено;</li> <li>• Создание новых настроек;</li> <li>• Изменение настроек для подразделения;</li> <li>• Применение частных настроек;</li> <li>• Удалены настройки;</li> <li>• Назначены настройки подразделения;</li> <li>• Создание задачи;</li> <li>• Отмена задачи;</li> <li>• Создан контакт;</li> <li>• Контакт изменен;</li> <li>• Контакт был удален;</li> <li>• Была создана нотификация;</li> <li>• Нотификация была изменена;</li> <li>• Нотификация была удалена;</li> <li>• Неавторизованный запрос;</li> <li>• Недостаточно прав на выполнение запроса;</li> <li>• Ошибка обработки запроса.</li> </ul>

Поле	Описание
Тип задачи	Тип задачи (только для типов событий <b>Создание задачи, Отмена задачи</b> ).
Сообщение об ошибке	Сообщение об ошибке во время обработки запроса.
Причина ошибки авторизации	Причина невозможности авторизации на сервере (только для типа события <b>Неавторизованный запрос</b> ).
ID задачи	Порядковый номер задачи (только для типов событий <b>Создание задачи, Отмена задачи</b> ).
Номер порта запроса	Порт компьютера с установленной консолью управления SoftControl Admin Console, от которой пришел запрос на сервер.
URI запроса	Полный URI запроса консоли управления SoftControl Admin Console, который был отправлен на сервер.
Имя подразделения	Подразделение, в которое перемещен установленный клиентский компонент (только для типов событий <b>Перемещение клиента в другое подразделение, Создано новое подразделение, Подразделение было удалено</b> ).
Разрешения роли	Перечисление добавленных (для типа события <b>К роли добавлены разрешения</b> ) или удаленных (для типа события <b>Удалено разрешение у роли</b> ) разрешений роли.
ID сессии	Контрольная сумма идентификатора сессии, с которой ассоциировано событие.
Имя аккаунта	Имя учетной записи пользователя (только для типов событий <b>Была создана учетная запись, Учетная запись была изменена, Учетная запись была удалена</b> ).
Имя роли	Имя роли (только для типов событий <b>Роль создана, Роль удалена, К роли добавлены разрешения, Удалено разрешение у роли</b> ).
Имя пользователя	Имя пользователя, с которым ассоциировано данное событие.
Имя нотификации	Имя оповещения (только для типов событий <b>Была создана нотификация, Нотификация была изменена, Нотификация была удалена</b> ).
Имя настроек	Имя конфигурации клиентских приложений (только для типов событий <b>Создание новых настроек, Изменение настроек для подразделения, Удалены настройки</b> ).
Имя контакта	Имя адресата получателя оповещений (только для типов событий <b>Создан контакт, Контакт был изменен, Контакт был удален</b> ).
Время возникновения	Дата и время возникновения события.
Время создания настроек	Время создания настроек клиентских приложений на сервере (только для типа события <b>Создание новых настроек</b> ).
Имя клиента	Имя клиентского хоста (только для типов событий <b>Подтверждение клиента, Отклонение клиента, Удаление клиента, Запрос на изменение сертификата клиента, Новый сертификат назначен клиенту, Перемещение клиента в другое подразделение</b> ).
IP адрес запроса	IP-адрес компьютера с установленной консолью управления SoftControl Admin Console, от которой пришел запрос на сервер.

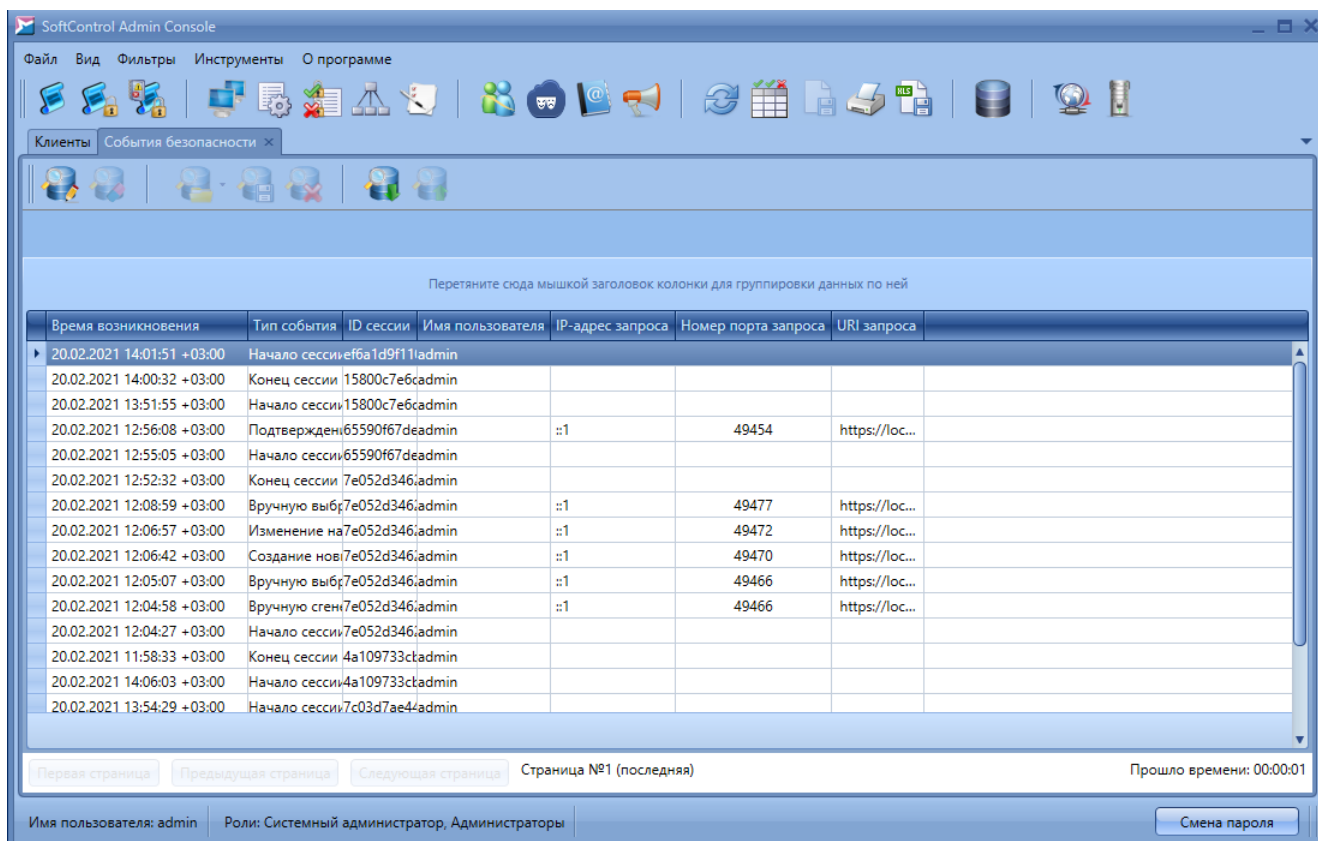


Рисунок 38. Вкладка «События безопасности»

С данными в таблице можно работать с помощью фильтрации или создания запросов к базе данных. Эти операции подробно описаны в разделах [Фильтрация событий](#)<sup>159</sup> и [Запросы к базе данных](#)<sup>165</sup>.

Также на этой вкладке можно выполнить следующие действия:

#### ▼ Изменение состава колонок

Если необходимая колонка отсутствует в заголовке таблицы, то для добавления нового поля нажмите кнопку **Выбрать колонки** и перетащите требуемое поле из окна **Выбор колонок** (рис. [Выбор колонок](#)<sup>44</sup>) в необходимое место заголовка таблицы. Для удаления существующего поля перетащите его в окно **Выбор колонок**, либо за пределы заголовка таблицы.

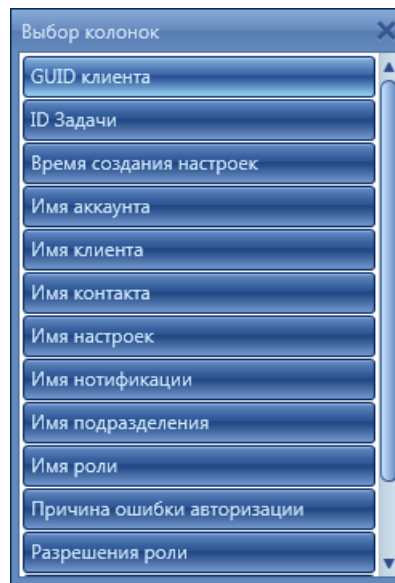


Рисунок 39. Выбор колонок

#### ▼ Группировка данных



Информация на вкладке может группироваться по всем полям (категориям), кроме поля **Время возникновения**, для удобства просмотра. Для группировки по категориям перетащите заголовок колонки на панель, расположенную между заголовком таблицы и группой кнопок вкладки (рис. [Вкладка «События безопасности»](#)<sup>43</sup>). Если группировка производится по нескольким категориям, то приоритет (вложенность категорий) уменьшается слева направо в зависимости от расположения на панели.





## 4.4 Клиенты

Вкладка **Клиенты** служит для управления регистрацией клиентских приложений, перемещением их в подразделения, отслеживания статуса и получения информации о хостах, на которых они установлены (рис. [Вкладка «Клиенты»](#)<sup>46</sup>).

Основные операции с клиентскими компонентами осуществляются с помощью графических кнопок вкладки, предназначение которых приведено в табл. 9.

Таблица 9. Элементы управления вкладки «Клиенты»

Кнопка	Название	Описание	Горячие клавиши
	Удалить	Удаление выбранных клиентских компонентов из БД.	Delete
	Одобрить	Одобрение регистрации клиентского компонента на сервере.	

	Отклонить	Отклонение регистрации клиентского компонента на сервере.	
	Переместить	Перемещение выбранных клиентских компонентов в другое подразделение.	
	Сертификат	Обновление индивидуального сертификата клиентского компонента.	
	Лог событий	Вызов вкладки <b>Лог</b> для выбранных компонентов.	

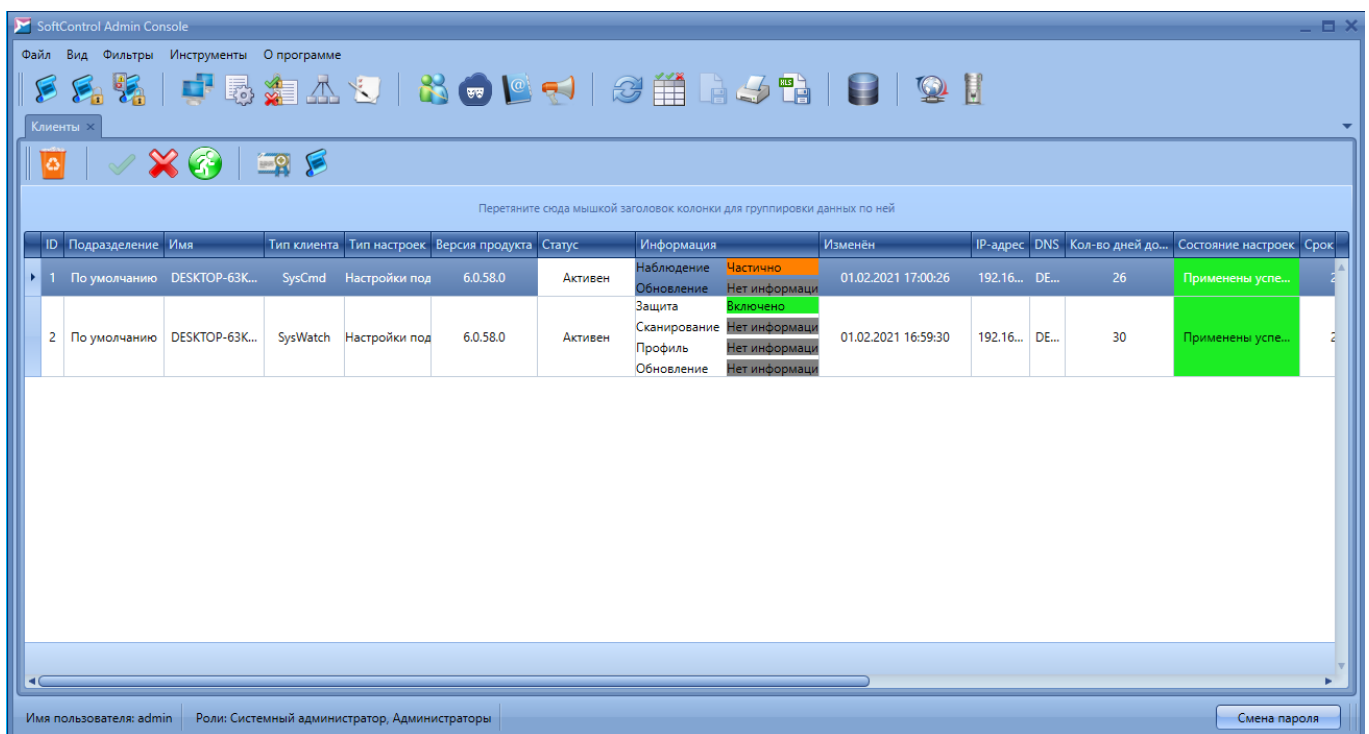


Рисунок 40. Вкладка «Клиенты»

Полный перечень полей вкладки приведен в табл. 10.

Таблица 10. Поля вкладки «Клиенты»

Поле	Описание
ID	Порядковый номер клиентского хоста.
Подразделение	Подразделение, к которому принадлежит клиентский компонент.
Имя	Имя клиентского хоста.
Тип клиента	Тип установленного клиентского компонента на данном клиентском хосте: <ul style="list-style-type: none"> <li>• <b>SysWatch</b> – компонент проактивной защиты (SoftControl ATM Client / Endpoint Client / SClient);</li> <li>• <b>DLP</b> – компонент сбора данных (SoftControl DLP Client);</li> <li>• <b>SysCmd</b> - компонент удаленного выполнения команд и обмена файлами (SoftControl SysCmd).</li> </ul>
Тип настроек	Тип конфигурации клиентского компонента: <ul style="list-style-type: none"> <li>• <b>Настройки подразделения</b> – настройки, общие для подразделения, которому принадлежит клиентский компонент;</li> <li>• <b>Частные настройки</b> – настройки, индивидуальные для клиентского компонента,</li> </ul>

	<p>независимо от подразделения;</p> <ul style="list-style-type: none"> <li>• <b>Локальные настройки</b> – настройки, измененные локально для клиентского компонента типа SysWatch.</li> </ul>
Версия продукта	<p>Версия установленного клиентского компонента. Если версия компонента ниже версии SoftControl Admin Console, данная ячейка подсвечивается красным цветом, если выше – оранжевым.</p>
Статус	<p>Возможные статусы, отражающие текущее состояние клиентского компонента:</p> <ul style="list-style-type: none"> <li>• <b>Ожидает решения:</b> от клиентского приложения получен запрос на регистрацию, ожидается решение администратора.</li> <li>• <b>Одобен:</b> запрос на регистрацию от клиентского приложения одобрен администратором.</li> <li>• <b>Отклонен:</b> запрос на регистрацию от клиентского приложения отклонен администратором.</li> <li>• <b>Активен:</b> за последний отрезок времени, равный удвоенному значению <a href="#">интервала обращения клиента к серверу</a><sup>63</sup>, зафиксирован факт установки связи зарегистрированного клиентского приложения с сервером.</li> <li>• <b>Остановлен:</b> за последний отрезок времени, равный удвоенному значению <a href="#">интервала обращения клиента к серверу</a><sup>63</sup>, не зафиксирован факт установки связи зарегистрированного клиентского приложения с сервером.</li> </ul>
Информация	<p>Дополнительная информация по состоянию клиентского компонента. Для компонента типа <b>SysWatch</b> имеет следующие показатели:</p> <ul style="list-style-type: none"> <li>• <b>Защита</b> – статус проактивной защиты. <ul style="list-style-type: none"> <li>– <b>Включено:</b> защита включена по всем областям контроля;</li> <li>– <b>Отключено:</b> защита отключена по всем областям контроля;</li> <li>– <b>Частично:</b> защита включена по части областей контроля.</li> </ul> </li> <li>• <b>Сканирование</b> – статус последней по времени задачи антивирусного сканирования.</li> <li>• <b>Профиль</b> – статус последней по времени задачи сбора профиля (автоматической настройки). <ul style="list-style-type: none"> <li>– <b>Выполняется:</b> задача находится в процессе выполнения;</li> <li>– <b>Остановлено:</b> задача остановлена пользователем;</li> <li>– <b>Завершено:</b> задача успешно завершена;</li> <li>– <b>Ошибка:</b> возникла ошибка в процессе запуска или завершения задачи.</li> </ul> </li> </ul> <p>Статус <b>Нет информации</b> для операций <b>Сканирование</b>, <b>Профиль</b> и <b>Обновление</b> означает, что указанные действия не производились с момента регистрации клиентского приложения на сервере.</p> <p>Для компонента типа <b>DLP</b> имеет следующие показатели:</p> <ul style="list-style-type: none"> <li>• <b>Наблюдение</b> – статус активности наблюдения. <ul style="list-style-type: none"> <li>– <b>Включено:</b> наблюдение включено по всем областям сбора данных (не включает в себя подкатегорию съемных носителей);</li> <li>– <b>Отключено:</b> наблюдение отключено по всем областям сбора данных;</li> <li>– <b>Частично:</b> наблюдение включено по части областей сбора данных.</li> </ul> </li> </ul> <p>Информация по обновлению присутствует у всех типов клиентов:</p> <ul style="list-style-type: none"> <li>• <b>Обновление</b> – статус последнего по времени обновления компонента. <ul style="list-style-type: none"> <li>– <b>Установлено:</b> обновление было успешно установлено;</li> <li>– <b>Не найдено:</b> обновления для компонента не найдены;</li> <li>– <b>Перезагрузить:</b> необходима перезагрузка клиентского хоста для завершения обновления.</li> </ul> </li> </ul>
Изменен	Время регистрации последнего события выбранным клиентским компонентом.
IP адрес	IP-адрес клиентского хоста.

DNS	Сетевое имя клиентского хоста в рабочей группе либо доменной сети.
Количество дней до окончания лицензии	Количество дней, оставшихся до истечения срока действия текущего лицензионного ключа клиентского приложения.
Состояние настроек	Статус применения настроек клиентского приложения, полученных им со стороны сервера SoftControl Server. Обновляется динамически при каждом изменении настроек через консоль управления SoftControl Admin Console. Возможные состояния: <ul style="list-style-type: none"> <li>• <b>применены успешно;</b></li> <li>• <b>ожидание ответа;</b></li> <li>• <b>ошибка применения;</b></li> <li>• <b>локальные настройки;</b></li> <li>• <b>нет информации.</b></li> </ul>
Срок действия сертификата	Дата, до которой действителен индивидуальный сертификат клиентского приложения.
Комментарий	Поле для ввода комментария к выбранному клиентскому компоненту.
Уникальный ID устройства	Уникальный идентификатор клиентского компонента, который автоматически присваивается ему при первом обращении к серверу SoftControl Server.
Статус постоянного соединения	Возможные статусы, отражающие использование опции <b>Держать постоянное соединение с Сервисным Центром</b> (см. раздел <a href="#">Общие настройки</a> <sup>(63)</sup> ): <ul style="list-style-type: none"> <li>• <b>Активен:</b> постоянное соединение с SoftControl Service Center включено;</li> <li>• <b>Остановлен:</b> постоянное соединение с SoftControl Service Center отключено.</li> </ul>
Запретить локальное управление настройками	Индикатор управления настройками клиентских хостов. Галочка в данном поле означает, что управлять настройками можно только через SoftControl Service Center. Включение и отключение данной опции осуществляется через настройки клиентских приложений (см. раздел <a href="#">Настройки SoftControl SysWatch</a> <sup>(74)</sup> ).

Основные действия, выполняемые на данной вкладке:

- [управление процессом регистрации](#)<sup>(50)</sup>;
- [перемещение в подразделения](#)<sup>(52)</sup>;
- [управление списком файлов, разрешенных к запуску](#)<sup>(52)</sup>.

Дополнительные действия, возможные на данной вкладке:

#### ▼ Работа с несколькими компонентами

Вкладка позволяет работать как с одним, так и с несколькими клиентскими компонентами. Для выполнения действий над несколькими компонентами выберите их с помощью одного из способов выделения и произведите требуемые действия:

- выделение нескольких произвольных компонентов: нажмите клавишу **Ctrl** на клавиатуре и выделите требуемые компоненты;
- выделение диапазона компонентов: выберите первый компонент диапазона, нажмите клавишу **Shift** на клавиатуре и выберите последний компонент



диапазона.

#### ▼ Группировка данных

Информация на вкладке может группироваться по определенным полям для удобства отображения. Полями, по которым возможно произвести группировку (категориями), являются **Подразделение, Тип клиента, Тип настроек, Версия продукта, Статус, IP адрес, DNS, Количество дней до окончания лицензии, Состояние настроек и Комментарий**. Для группировки по указанным категориям перетащите заголовок колонки на панель, расположенную между заголовком таблицы и группой кнопок вкладки (рис. [Вкладка «Клиенты»](#)<sup>46</sup>). Если группировка производится по нескольким категориям, то приоритет (вложенность категорий) уменьшается слева направо в зависимости от расположения на панели.

#### ▼ Просмотр журналов

Для открытия вкладки [Лог событий](#)<sup>143</sup> со списком событий выделите требуемые компоненты и выполните одно из следующих действий:

- нажмите на кнопку **Лог событий** в группе кнопок вкладки (рис. [Вкладка «Клиенты»](#)<sup>46</sup>);
- вызовите контекстное меню нажатием правой кнопки мыши на списке компонентов и выберите команду **Показать события**.

При открытии списка событий в заголовке вкладки [Лог](#)<sup>143</sup> отображается количество выбранных компонентов (рис. [Вкладка «Клиенты»](#)<sup>46</sup>).

#### ▼ Просмотр данных профиля

Выделите нужный профиль и вызовите контекстное меню нажатием правой кнопкой мыши. Выберите команду **Просмотр данных профиля**. Откроется вкладка **Данные профиля** со списком хэш-сумм, включенных в выбранный профиль. При необходимости настройте фильтр для отображения нужных записей. Внизу находится гиперссылка **Экспортировать выборку в файл**. Нажмите ее, чтобы создать файл XML с записями, соответствующими заданным настройкам фильтра. Также вы можете удалить записи или скопировать нужные контрольные суммы, вызвав контекстное меню нажатием правой кнопкой мыши.

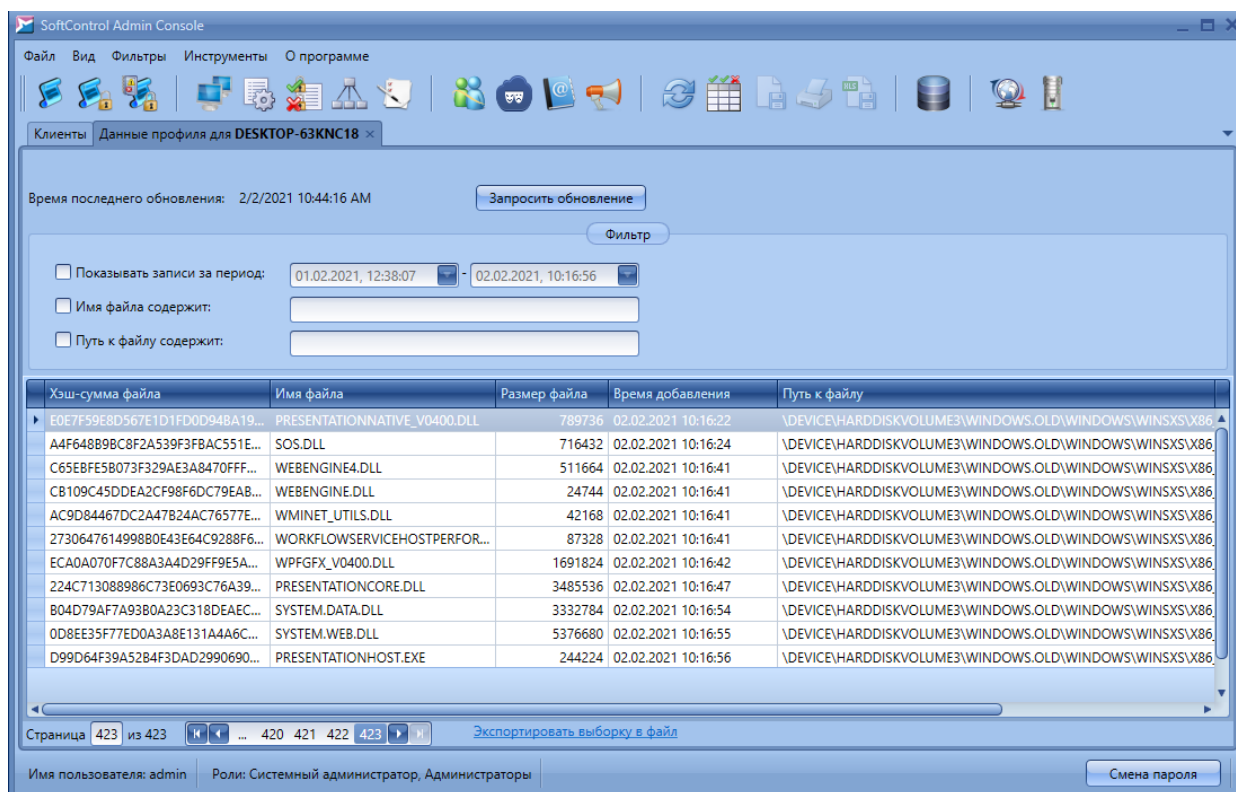


Рисунок 41. Вкладка «Данные профиля»

#### 4.4.1 Управление процессом регистрации

Управление процессом регистрации включает в себя следующие действия:

##### ▼ Подтверждение регистрации

Выберите в списке требуемые клиентские компоненты, находящиеся в состоянии **Ожидает решения**, и нажмите на кнопку **Одобрить** (рис. [Вкладка «Клиенты»](#)<sup>46</sup>).

Поле **Статус** после подтверждения регистрации выбранных клиентов изменяет свое состояние на **Одобен**.

При следующем получении запроса от клиентского компонента происходит проверка его [сертификата](#)<sup>230</sup>: если он общий, то серверный компонент SoftControl Server выдает индивидуальный сертификат для авторизации на сервере. При следующем обращении клиентского компонента (с индивидуальным сертификатом) его статус изменяется на **Активен**. С этого момента клиентский компонент считается введенным в эксплуатацию: между сервером и клиентом установлен безопасный зашифрованный канал связи.

#### ▼ Отклонение регистрации

Выберите в списке требуемые клиентские компоненты, находящиеся в состоянии **Ожидает решения**, и нажмите на кнопку **Отклонить** (рис. [Вкладка «Клиенты»](#)<sup>46</sup>).

Поле **Статус** после отклонения регистрации выбранных клиентов изменяет свое состояние на **Отклонен**, и их дальнейшее взаимодействие с сервером прекращается.

После отклонения регистрации повторную попытку можно совершить только следующим образом:

- 1) Удалите клиентские компоненты из БД с помощью кнопки **Удалить**.
- 2) Повторите процедуру регистрации на сервере с [общим сертификатом](#)<sup>230</sup>.

#### ▼ Обновление клиентского сертификата

Выберите в списке требуемые клиентские компоненты, находящиеся в состоянии **Активен** или **Остановлен**, и нажмите на кнопку **Сертификат** (рис. [Вкладка «Клиенты»](#)<sup>46</sup>).

Поле **Срок действия сертификата** обновляется после следующего обращения клиентского компонента с новым [индивидуальным сертификатом](#)<sup>230</sup>. При этом использование предыдущего сертификата становится невозможным в связи с его помещением в черный список.

#### ▼ Удаление клиентского компонента из БД

Выберите в списке требуемые клиентские компоненты и нажмите на кнопку **Удалить** (рис. [Вкладка «Клиенты»](#)<sup>46</sup>). При этом не происходит отзыва клиентского [сертификата](#)<sup>230</sup> и через интервал обращения клиента к серверу в консоли управления SoftControl Admin Console вновь отобразятся удаленные компоненты в статусе **Ожидает решения**. Для полного вывода клиентских компонентов из эксплуатации необходима следующая последовательность действий:

- 1) Поместите [индивидуальный сертификат](#)<sup>230</sup> клиентского компонента в черный список с помощью кнопки **Отклонить**.
- 2) Удалите клиентские компоненты из БД с помощью кнопки **Удалить**.

## 4.4.2 Перемещение в подразделения

Для перемещения выбранных клиентских компонентов в другое подразделение, нажмите на кнопку **Переместить** и в появившемся окне выберите из выпадающего списка необходимое подразделение (рис. [Выбор подразделения для перемещения компонента](#)<sup>52</sup>).

**i** При перемещении клиентских компонентов в другое подразделение их настройки автоматически изменяются на конфигурацию данного подразделения.

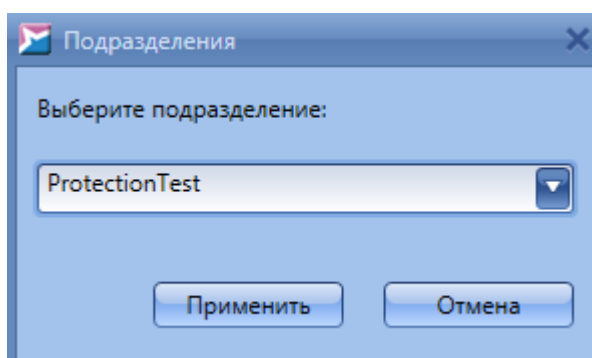


Рисунок 42. Выбор подразделения для перемещения компонента

## 4.4.3 Управление списком разрешенных файлов

SoftControl Admin Console позволяет получить список файлов, разрешенных к запуску на компьютере с установленным клиентским приложением SoftControl SysWatch, и при необходимости отозвать разрешения для выбранных файлов.

Для получения списка файлов щелкните правой кнопкой мыши по требуемому клиентскому приложению SoftControl SysWatch и в контекстном меню выберите команду **Просмотр данных профиля**. Данное действие открывает вкладку **Данные профиля для <имя\_клиентского\_приложения>** (рис. [Вкладка «Данные профиля для...»](#)<sup>52</sup>). Для начала сбора профиля нажмите на кнопку **Запросить обновление**. В процессе сбора данных SoftControl Admin Console показывает примерное время до окончания сбора. Список файлов содержит следующую дополнительную информацию: имя файла в момент добавления в список, его контрольная сумма, полный путь, дата добавления, размер, а также флаг, указывающий, был ли файл добавлен в профиль инсталлятором (**I**) или в процессе сбора профиля (**P**).

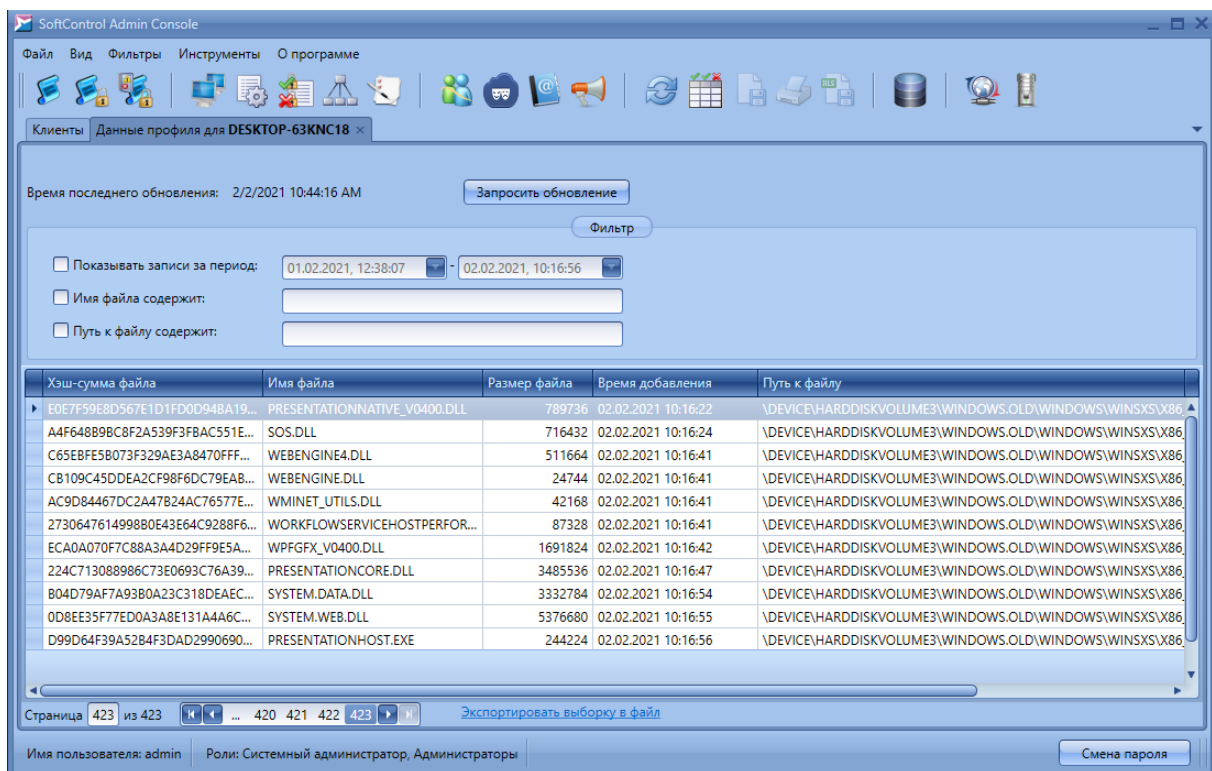


Рисунок 43. Вкладка «Данные профиля для...»

Для просмотра списка файлов за определенный период времени выберите требуемые даты в поле **Фильтр**. Вы также можете указать в фильтре часть имени файла и пути к нему. Для того чтобы отозвать разрешения на запуск для каких-либо файлов, выделите их, используя клавиши **Shift** и **Ctrl**, и в контекстном меню выберите команду **Удалить выбранные**.

## 4.5 Подразделения

Вкладка **Подразделения** предназначена для группирования клиентских компонентов по территориальному, административному или иному признаку (рис. [Вкладка «Подразделения»](#)<sup>53</sup>). Кроме того, на вкладке производится привязка подразделений к определенным наборам настроек и генерация одноразовых паролей.

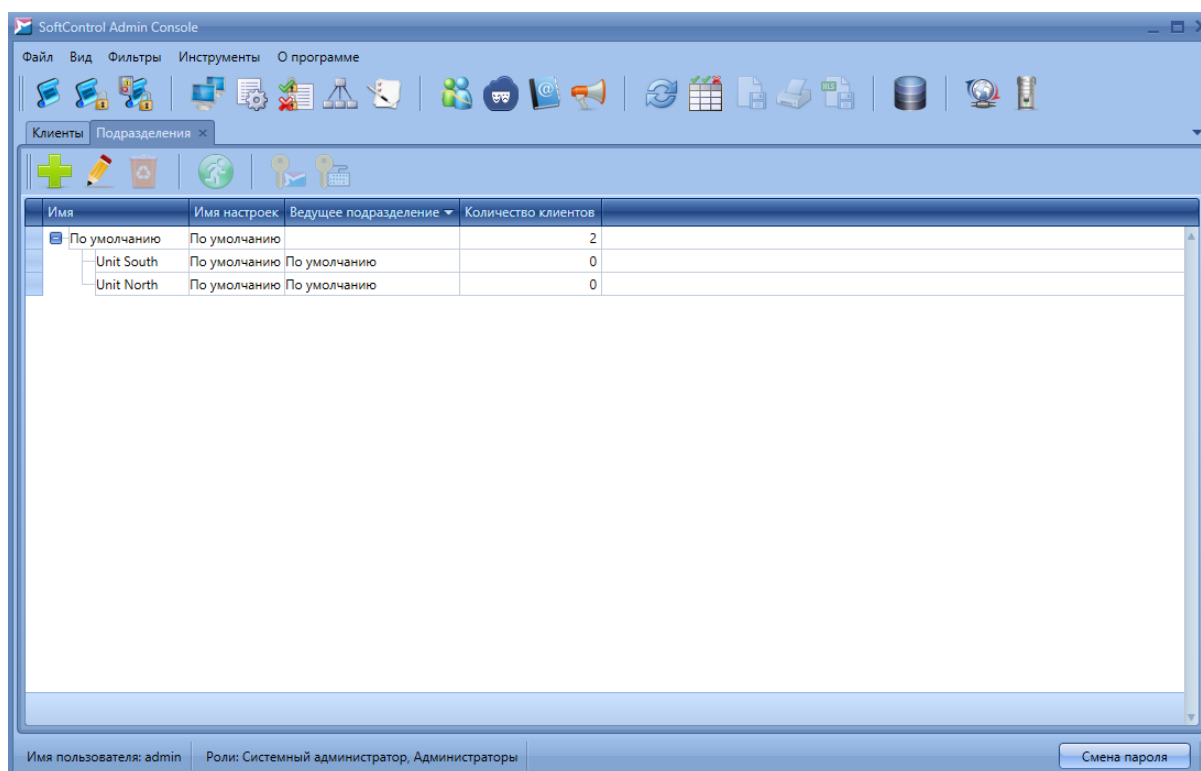



Рисунок 44. Вкладка «Подразделения»

В программе всегда существует как минимум одно подразделение – **По умолчанию**; его удаление невозможно. Все новые клиентские компоненты автоматически помещаются в данное подразделение. В дальнейшем администратор может создать требуемую иерархическую структуру подразделений (с любым уровнем вложенности), используя кнопку **Переместить**. Каждому подразделению при создании назначается конфигурация (настройки) клиентских приложений.

Основные операции с подразделениями осуществляются с помощью графических кнопок вкладки, предназначение которых приведено в табл. 11.

Таблица 11. Элементы управления вкладки «Подразделения»

Кнопка	Название	Описание
	Добавить	Создание нового подразделения.
	Редактировать	Редактирование свойств выбранного подразделения.
	Удалить	Удаление выбранных подразделений.
	Переместить	Переместить выбранное подразделение в другое. Нельзя перемещать подразделение <b>По умолчанию</b> , а также родительское подразделение в дочернее.
	Одноразовый пароль для SysWatch	Открытие окна генератора одноразовых паролей.

Кнопка	Название	Описание
	Одноразовый пароль для разблокировки клавиатуры	Открытие окна генератора паролей для разблокировки клавиатуры на клиентском хосте.

Перечень полей вкладки приведен в табл. 12.

Таблица 12. Поля вкладки «Подразделения»

Поле	Описание
Имя	Наименование подразделения.
Имя настроек	Наименование конфигурации клиентских компонентов, действующее в выбранном подразделении.
Ведущее подразделение	Наименование родительского подразделения.

Основные действия, выполняемые на данной вкладке:

- [управление подразделениями](#) <sup>(55)</sup>;
- [генерация одноразовых паролей](#) <sup>(57)</sup>.

#### 4.5.1 Управление подразделениями

Управление подразделениями включает в себя следующие действия:

##### ▼ Создание подразделения

Чтобы добавить новое подразделение, нажмите на кнопку **Создать** (рис. [Вкладка «Подразделения»](#) <sup>(53)</sup>). В появившемся окне укажите **Имя** подразделения и выберите **Имя настроек** в выпадающем списке, после чего нажмите на кнопку **Применить** (рис. [Создание подразделения](#) <sup>(55)</sup>).

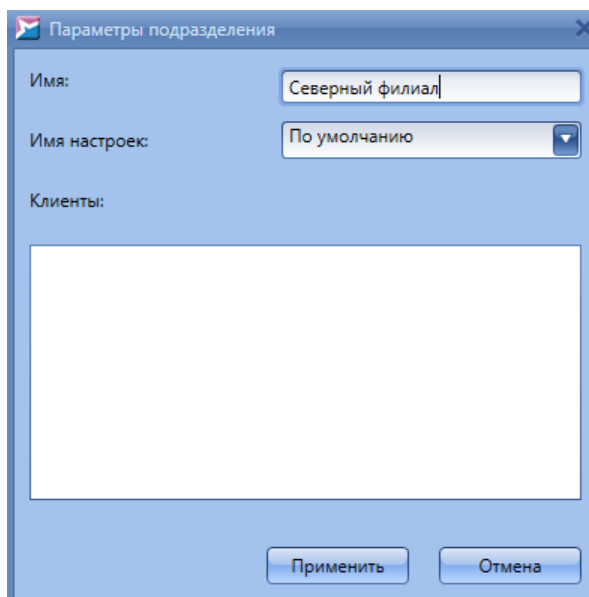


Рисунок 45. Создание подразделения

#### ▼ Изменение свойств подразделения

Чтобы изменить свойства подразделения, нажмите на кнопку **Редактировать** (рис. [Вкладка «Подразделения»](#)<sup>53</sup>).

В появившемся окне измените **Имя** подразделения и/или выберите другое **Имя настроек** в выпадающем списке, после чего нажмите на кнопку **Применить** (рис. [Параметры подразделения](#)<sup>56</sup>). Если данное подразделение содержит компоненты, их перечень отображается в списке **Клиенты**.

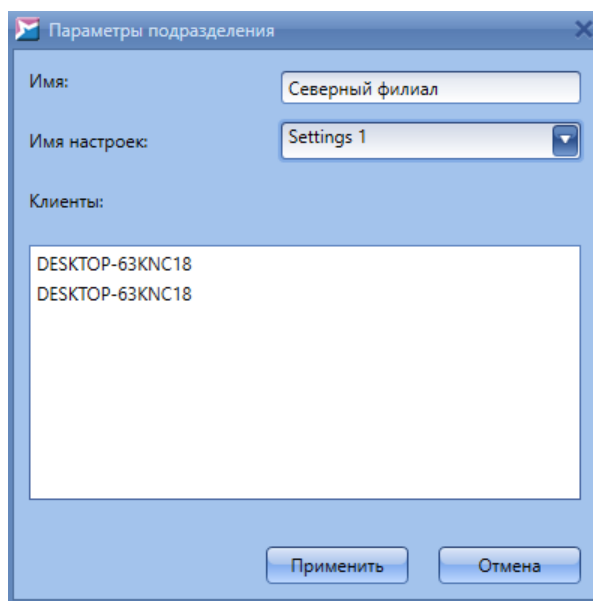


Рисунок 46. Параметры подразделения

#### ▼ Удаление подразделения

Для удаления подразделения выберите его, нажмите на кнопку **Удалить** (рис. [Вкладка «Подразделения»](#)<sup>53</sup>) и подтвердите удаление в диалоговом окне. Все компоненты из удаляемого подразделения будут перемещены в подразделение, которое является для него родительским.



Удаление подразделения **По умолчанию** невозможно.

#### ▼ Перемещение подразделения

Для перемещения подразделения выберите его, нажмите на кнопку **Переместить** и в появившемся окне укажите подразделение, в которое происходит перемещение (рис. [Перемещение подразделения](#)<sup>56</sup>).



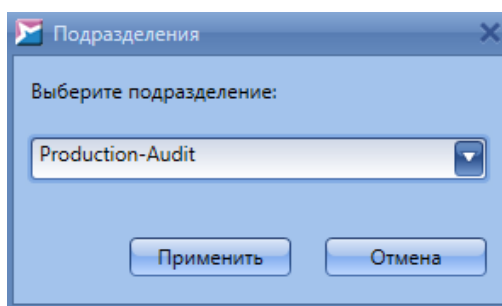


Рисунок 47. Перемещение подразделения





**i** Невозможно переместить подразделение **По умолчанию**, а также родительское подразделение в дочернее.

## 4.5.2 Генерация одноразовых паролей

В SoftControl Service Center реализована подсистема защищенной аутентификации на основе алгоритма создания одноразовых паролей. Данный алгоритм обладает высокой криптографической стойкостью и позволяет генерировать пароли, действительные только в течение определенного промежутка времени. Одноразовые пароли могут быть использованы для доступа к ГИП/деинсталлятору клиентского компонента SoftControl SysWatch в случае необходимости (например, если требуется обеспечить однократный доступ к SoftControl SysWatch без раскрытия основного пароля), а также для разблокировки клавиатуры на клиентском хосте.

Для начала работы с генератором одноразовых паролей необходимо, чтобы в текущей конфигурации подразделения была включена и настроена [соответствующая опция](#) <sup>(83)</sup>.

Генерация одноразовых паролей осуществляется в рамках подразделения: создаваемый пароль применим для всех приложений SoftControl SysWatch, входящих в подразделение.

Выберите подразделение и нажмите на кнопку  (**Одноразовый пароль для SysWatch**) или  (**Одноразовый пароль для разблокировки клавиатуры**), чтобы открыть окно генератора (рис. [Вкладка «Подразделения»](#) <sup>(53)</sup>). В появившемся окне выберите **Время действия пароля** и нажмите на кнопку  (**Сгенерировать пароль**). Пароль отображается в поле **Одноразовый пароль для SysWatch** (или **Одноразовый пароль для разблокировки клавиатуры**); время его жизни – в счетчике **Осталось времени** в формате **дд:чч:мм:сс** (рис. [Окно генерации](#) <sup>(58)</sup>). По истечении интервала времени жизни нажмите на кнопку  еще раз, чтобы сгенерировать новый пароль.

- i** I) Использование одноразовых паролей для SysWatch рассчитано на применение совместно с основным паролем. Для возможности получения доступа к SoftControl SysWatch на клиентском хосте по одноразовым паролям должна быть включена [общая парольная защита](#)<sup>(73)</sup>. При запросе пароля в ГИП SoftControl SysWatch необходимо установить флажок **Использовать одноразовый пароль**.
- II) В связи с тем, что алгоритм создания одноразовых паролей в качестве параметра принимает время, для его корректной работы необходимо, чтобы время по UTC (т.е. независимо от часового пояса) на компьютере с SoftControl Admin Console и хосте с установленным SoftControl SysWatch было синхронизировано с погрешностью, значительно меньшей времени жизни пароля.

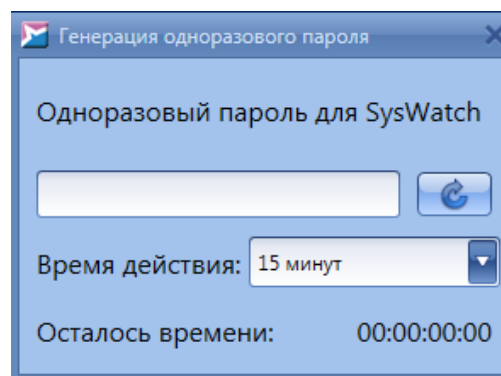


Рисунок 48. Окно генерации пароля для SysWatch

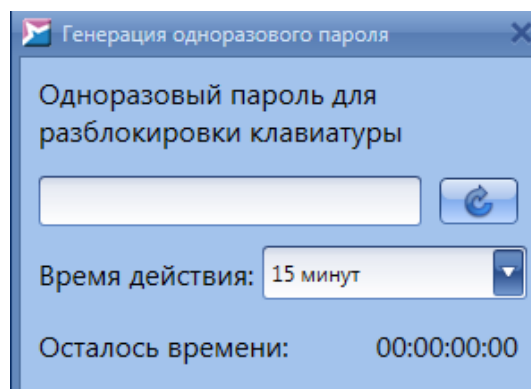


Рисунок 49. Окно генерации пароля для разблокировки клавиатуры

## 4.6 Настройка клиентских приложений

Вкладка **Настройки клиентов** содержит список конфигураций (наборов настроек) клиентских приложений (рис. [Вкладка «Настройки клиентов»](#)<sup>59</sup>).

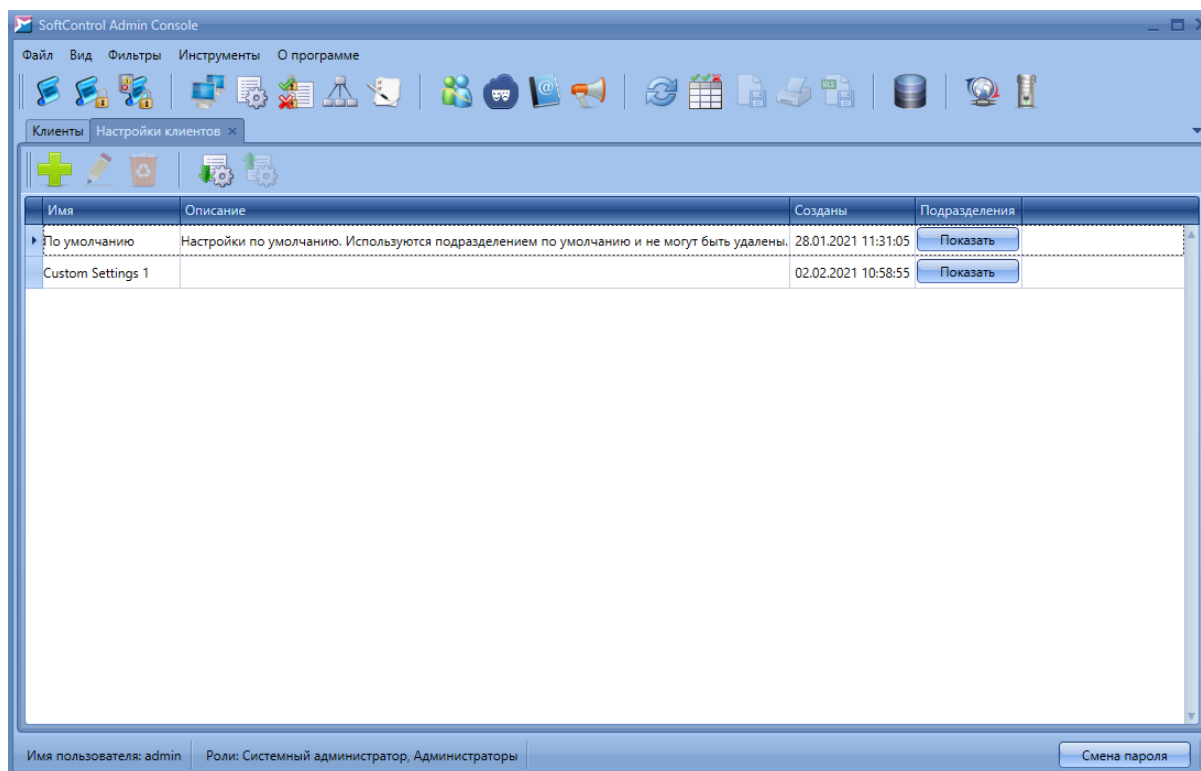


Рисунок 50. Вкладка «Настройки клиентов»






В SoftControl Admin Console различаются следующие типы конфигураций:

- настройки подразделения;
- частные настройки;
- локальные настройки (только для SoftControl SysWatch).

По умолчанию все клиентские компоненты после регистрации на сервере получают настройки подразделения. Частные настройки созданы для тех случаев, когда требуется задать для определенного клиентского компонента конфигурацию, отличную от конфигурации подразделения. На вкладке отображается список всех конфигураций, включая частные. Информация по работе с частными настройками приведена [ниже](#)<sup>61</sup>.

Основные операции с конфигурациями осуществляются с помощью графических кнопок вкладки, предназначение которых приведено в табл. 13.

Таблица 13. Элементы управления вкладки «Настройки клиентов»

Кнопка	Название	Описание
	Добавить	Создание новой конфигурации клиентских компонентов.
	Редактировать	Редактирование выбранной конфигурации.
	Удалить	Удаление выбранных конфигураций.
	Импорт	Импортирование конфигурации из XML-файла.
	Экспорт	Экспортирование выбранной конфигурации в XML-файл.

Перечень полей вкладки приведен в табл. 14.

Таблица 14. Поля вкладки «Настройки клиентов»

Поле	Описание
Имя	Наименование конфигурации клиентских компонентов.
Описание	Описание конфигурации клиентских компонентов.
Созданы	Дата и время создания конфигурации.
Подразделения	Список подразделений, к которым применяется данная конфигурация.

В SoftControl Admin Console представлены следующие категории централизованной настройки клиентских приложений:

- [общие настройки](#) <sup>(62)</sup>;
- [настройки SoftControl SysWatch](#) <sup>(66)</sup>;
- [настройки SoftControl DLP Client](#) <sup>(115)</sup>;
- [настройки SoftControl SysCmd](#) <sup>(124)</sup>.

Основные действия, выполняемые с клиентскими конфигурациями:

#### ▼ Создание конфигурации подразделения

Чтобы добавить новую конфигурацию подразделения, нажмите на кнопку **Добавить** (рис. [Вкладка «Настройки клиентов»](#) <sup>(59)</sup>). В окне **Редактирование настроек клиентов** задайте параметры конфигурации (см. рисунки, начиная с [Раздел «Имя и описание»](#) <sup>(63)</sup> и до [Настройки расписания обновления](#) <sup>(124)</sup>). Если внизу окна отображается статус **Значения всех параметров корректны**, нажмите на кнопку **Применить** для добавления созданной конфигурации; в обратном случае измените некорректные значения параметров.

#### ▼ Создание конфигурации подразделения на основе существующей

Чтобы добавить новую конфигурацию на основе уже существующей, выберите ее и выполните одно из следующих действий:

- нажмите на кнопку **Редактировать** в группе кнопок вкладки (рис. [Вкладка «Настройки клиентов»](#)<sup>59</sup>);
- дважды нажмите левой кнопки мыши на конфигурации.

В окне **Редактирование настроек клиентов** измените имя (обязательно) и параметры конфигурации (в случае необходимости) аналогично работе с новой конфигурацией (см. рисунки, начиная с [Раздел «Имя и описание»](#)<sup>63</sup> и до [Настройки расписания обновления](#)<sup>124</sup>). Если внизу окна отображается статус **Значения всех параметров корректны**, нажмите на кнопку **Применить** для добавления созданной конфигурации; в обратном случае измените некорректные значения параметров.

#### ▼ Изменение типа настроек

Чтобы изменить тип настроек клиентского компонента, перейдите на вкладку [Устройства и статусы](#)<sup>45</sup>, вызовите контекстное меню требуемого клиентского компонента правой кнопкой мыши и выберите один из пунктов:

- **Использовать настройки подразделения:**  
Назначить клиентскому компоненту настройки подразделения, которому он принадлежит.
- **Использовать частные настройки:**  
Назначить клиентскому компоненту частные настройки.
- **Отправить повторно настройки клиенту с локальными настройками:**  
Назначить клиентскому компоненту SoftControl SysWatch, настройки которого были изменены локально, последнюю конфигурацию, заданную с сервера SoftControl Server.

#### ▼ Использование частных конфигураций

Чтобы добавить новую частную конфигурацию и назначить ее клиентскому компоненту, перейдите на вкладку [Клиенты](#)<sup>45</sup>, вызовите контекстное меню требуемого клиентского компонента правой кнопкой мыши и выберите пункт **Использовать частные настройки**. В окне **Выбор частных настроек** нажмите на

кнопку **Добавить** для создания новой частной конфигурации (рис. [Управление частными настройками](#)<sup>(62)</sup>).

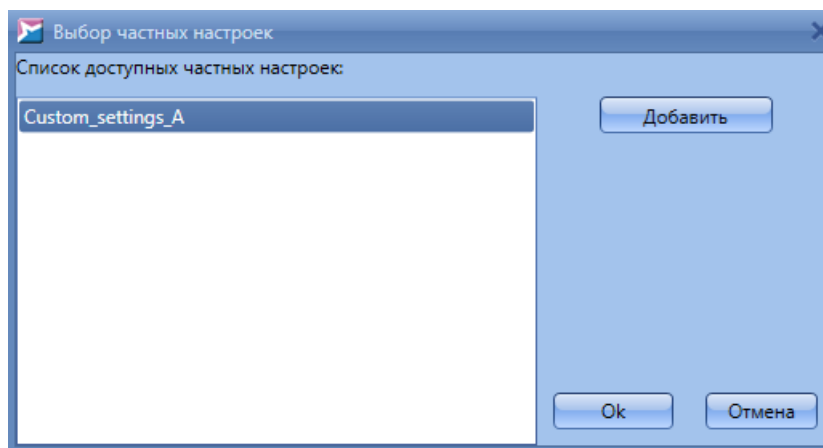


Рисунок 51. Управление частными настройками

В окне **Редактирование настроек клиентов** задайте параметры конфигурации (см. рисунки, начиная с [Раздел «Имя и описание»](#)<sup>(63)</sup> и до [Настройки расписания обновления](#)<sup>(124)</sup>). Если внизу окна отображается статус **Значения всех параметров корректны**, нажмите на кнопку **Применить** для добавления созданной конфигурации; в обратном случае измените некорректные значения параметров. Созданная конфигурация будет добавлена в список частных настроек. Выберите в списке ее или ранее созданную конфигурацию, после чего нажмите на кнопку **ОК** для применения конфигурации к клиентскому компоненту.

#### ▼ Удаление конфигурации

Для удаления конфигурации выберите ее, нажмите на кнопку **Удалить** (рис. [Вкладка «Настройки клиентов»](#)<sup>(59)</sup>) и подтвердите удаление в диалоговом окне.

### 4.6.1 Общие настройки

Данная категория настроек включает в себя общие параметры конфигурации и настройки взаимодействия клиентских приложений с сервером.

#### ▼ Имя и описание

Имя конфигурации клиентских приложений необходимо для однозначной

идентификации определенного набора настроек, описание конфигурации – для его краткой характеристики.

Чтобы задать **Имя и описание**, в одноименном разделе категории **Общие настройки** введите **Имя** и **Описание** в соответствующих полях (рис. [Раздел «Имя и описание»](#)<sup>63</sup>).

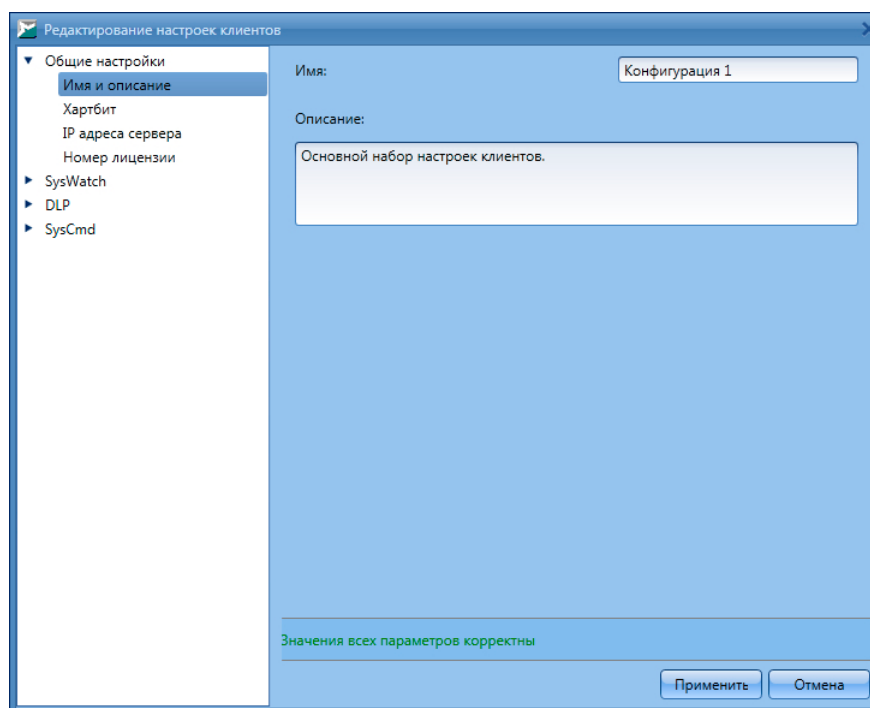


Рисунок 52. Раздел «Имя и описание»

**i** Имя конфигурации должно быть уникальным и не может совпадать с уже существующими конфигурациями.

#### ▼ Хартбит

Хартбит, или интервал обращения клиентского приложения к серверу – параметр клиентских компонентов, отвечающий за периодичность установки связи с серверным компонентом SoftControl Server. По умолчанию устанавливается равным 60 с (1 минута).

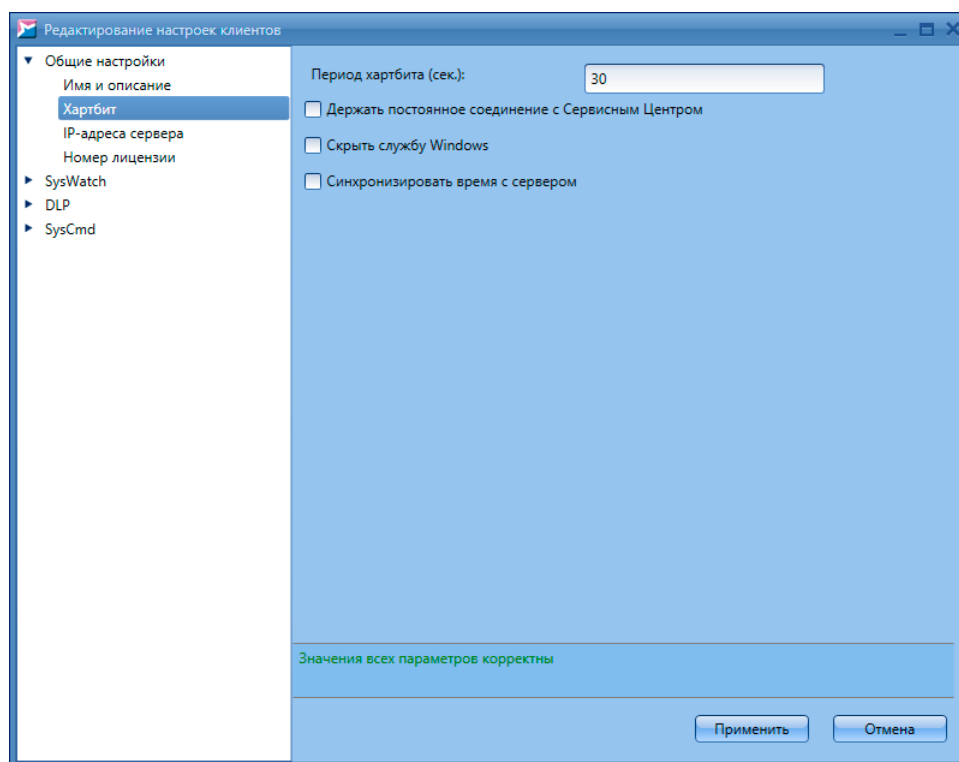


Рисунок 53. Раздел «Хартбит»

Для изменения параметра перейдите в раздел **Хартбит** категории **Общие настройки** и установите значение в поле **Период хартбита (сек.)** (рис. [Раздел «Хартбит»](#)<sup>63</sup>).

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

Кроме того, галочку **Держать постоянное соединение с Сервисным Центром** следует выставить, если для компонента SoftControl DLP Client необходимо включить запись видео по требованию. Настройки записи видео см. в разделе [Настройки SoftControl DLP Client](#)<sup>122</sup>.

Выставьте галочку **Скрыть службу Windows**, если системные службы SoftControl SysWatch (*safensec.exe*), SoftControl DLP Client (*eventsvc.exe*) и SoftControl SysCmd (*SysCmd.exe*) не должны показываться в оснастке **Службы ОС Windows**.

Примечание: скрывание системных служб не работает на ОС Windows XP.

Примечание: если системные службы скрыты, то управлять ими при помощи средств ОС невозможно.

Выставьте галочку **Синхронизировать время с сервером** для того, что бы SoftControl SysWatch синхронизировал время на клиентском компьютере с



временем SoftControl Server.

#### ▼ IP-адреса сервера

Задание адресов сервера для подключения со стороны клиентских приложений производится [мастером настройки сервера](#)<sup>(24)</sup>.

Для изменения списка адресов перейдите в раздел **IP адреса сервера** категории **Общие настройки** (рис. [Раздел «IP адреса сервера»](#)<sup>(65)</sup>). Чтобы добавить адрес в перечень, введите новое значение IP-адреса или имени в соответствующем поле и нажмите на кнопку **Добавить в список**. Чтобы удалить адрес из перечня, выберите его и нажмите на кнопку **Удалить из списка**.

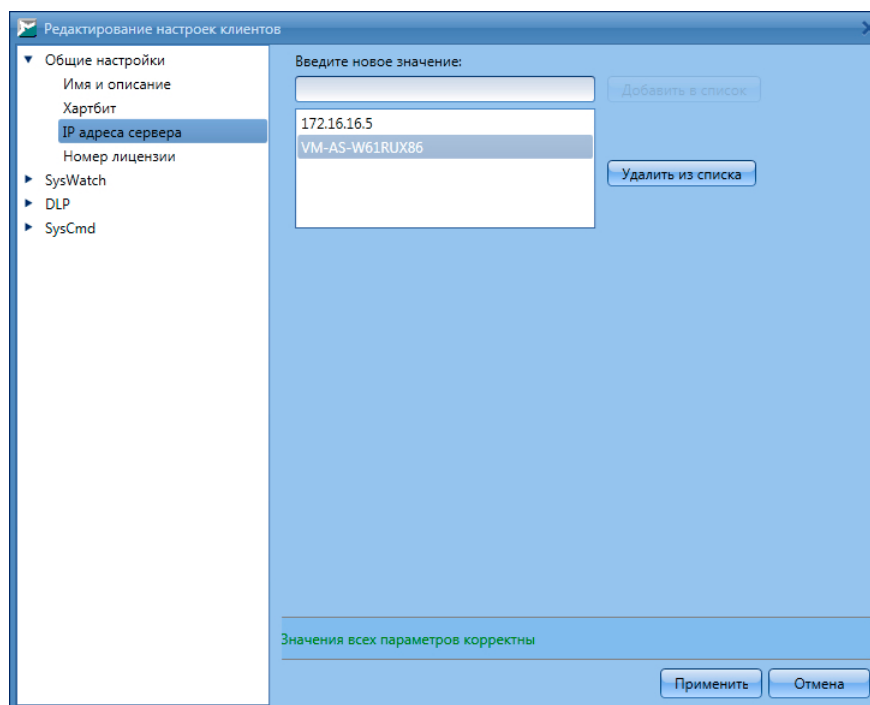


Рисунок 54. Раздел «IP адреса сервера»

#### ▼ Номер лицензии

Лицензионный ключ определяет функциональность клиентских компонентов. По умолчанию устанавливается пробная лицензия сроком действия 30 дней.

Для задания ключа перейдите в раздел **Номер лицензии** категории **Общие настройки**, выберите тип клиентского компонента в выпадающем списке (**SysWatch**, **DLP**, **DeCrypt**, **SysCmd**), введите ключ в текстовое поле и нажмите на кнопку **Проверить** для проверки лицензии и отображения ее параметров в случае

корректного ключа (рис. [Раздел «Номер лицензии»](#)<sup>(66)</sup>).

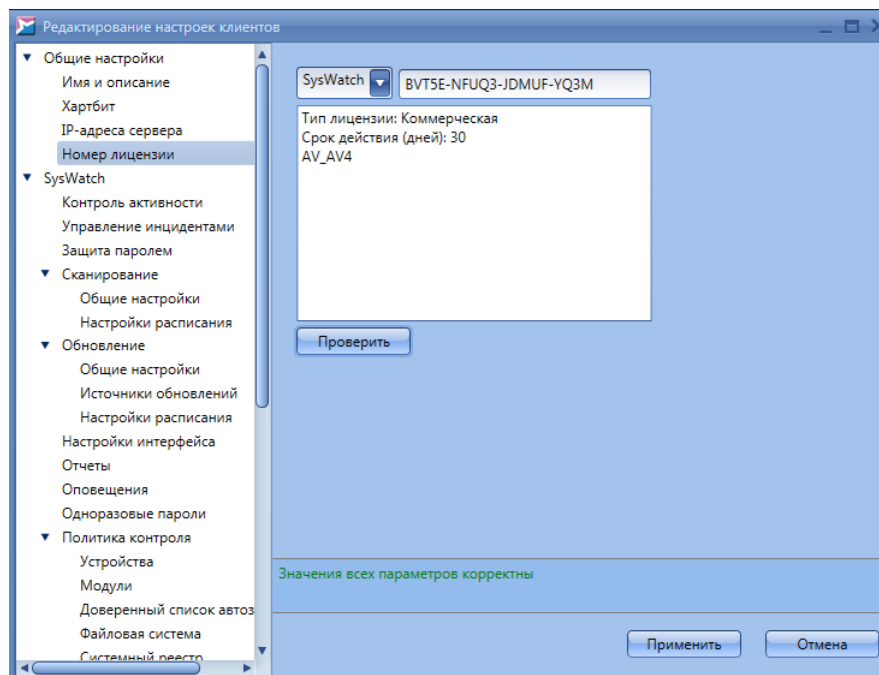


Рисунок 55. Раздел «Номер лицензии»

## 4.6.2 Настройки SoftControl SysWatch

Данная категория настроек включает в себя конфигурацию клиентского компонента SoftControl SysWatch, аналогичную задаваемой с помощью ГИП SoftControl SysWatch, и политики контроля.

### ▼ Контроль активности

В разделе **Контроль активности** категории **SysWatch** установите флажки у требуемых областей контроля (рис. [Настройки контроля активности](#)<sup>(66)</sup>):

- Контроль активности:**
  - Приложения;**
  - Сеть;**
  - Файловая система;**
  - Реестр.**

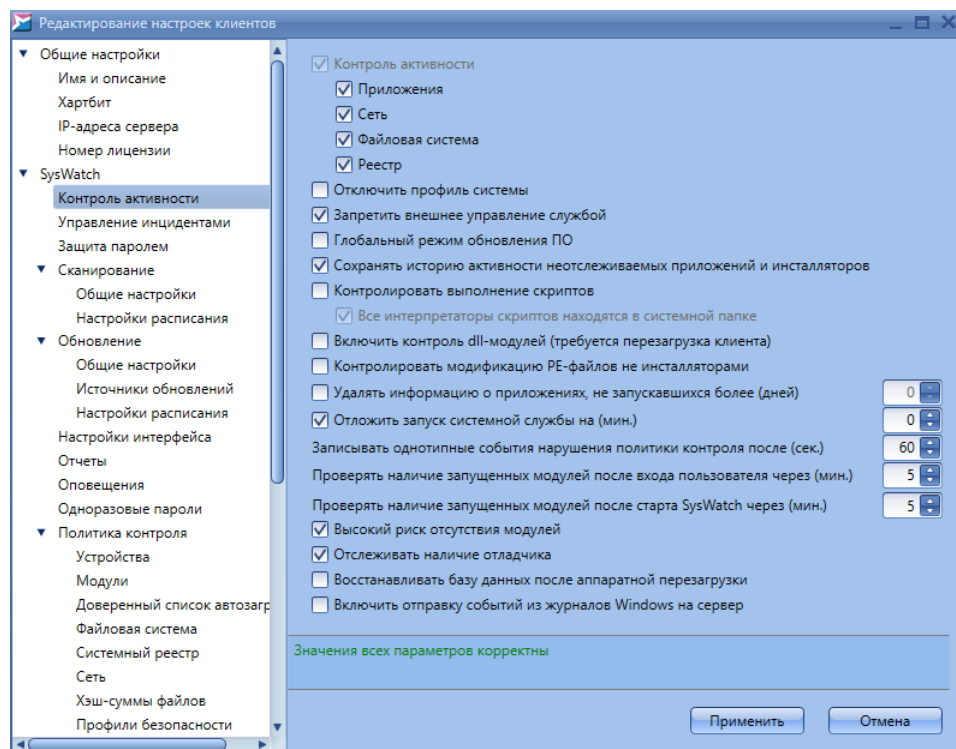


Рисунок 56. Настройки контроля активности

Ниже отметьте необходимые дополнительные опции программы и контроля активности:

**Отключить профиль системы:**

Отключить контроль исполняемых файлов PE на клиентском хосте.

**Запретить внешнее управление службой:**

Запретить выгрузку системной службы SoftControl SysWatch из ОЗУ клиентского хоста.

**Глобальный режим обновления ПО:**

Запускать все приложения в режиме 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. Рекомендуется использовать только на «чистых» системах, все ПО для которых устанавливалось с «золотого» образа. Для включения и выключения режима потребуется перезагрузка клиентского хоста.

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

Автоматически включать опции записи истории активности при первом

запуске приложения, отсутствующего в профиле, или инсталлятора без ЭЦП.

**❑ Контролировать выполнение скриптов:**

Заблокировать выполнение недоверенных скриптов интерпретаторами (кроме скриптов, подписанных ЭЦП из белого списка сертификатов).

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](#)<sup>92</sup>.

Примечание. Если в разделе **Управление инцидентами** для инцидента **Запуск интерпретатора скриптов** выбрано решение **Разрешить**, выполнение скрипта будет разрешено. 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 **Контролировать выполнение скриптов**.

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

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 – запрещается.

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 будет

разрешен. Событие при этом заносится в лог.

**Контролировать модификацию PE-файлов не инсталляторами:**

Запретить изменения исполняемых файлов (exe, dll и т.п.) всеми приложениями, кроме работающих в режиме обновления ПО.

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

**Удалять информацию о приложениях, не запускавшихся более (дней):**

Удалять из базы данных SoftControl SysWatch записи о неактивных приложениях, удовлетворяющих заданному условию (число дней без активности).

**Отложить запуск системной службы на (мин.):**

Установить интервал задержки запуска системной службы SoftControl SysWatch.

**Записывать однотипные события нарушения политики контроля после (сек.):**

Установить интервал, по истечении которого однотипные события будут записываться в отчет (по умолчанию 60 секунд). События нарушения политики контроля считаются *однотипными* и не вносятся в отчет, если одновременно выполняются следующие условия:

- у событий совпадают:
  - действия;
  - исполняемые файлы;
  - командные строки процессов;
  - идентификаторы (PID) процессов;
- время, прошедшее с момента добавления предыдущего события, меньше заданного значения.

При этом в локальный файл отчета на клиентском хосте с SoftControl SysWatch добавляется информация о том, сколько однотипных событий было пропущено.

**□ Проверять наличие запущенных модулей после старта SysWatch через (мин.):**

Установить интервал задержки после запуска SoftControl SysWatch, после которого начнется проверка наличия модулей, имеющих флаг [Должен быть запущенным при старте системы](#)<sup>90</sup>, среди запущенных процессов.

Некоторые модули имеют критическую важность для работы системы. SoftControl Service Center позволяет указать модули, наличие которых необходимо проверять, и задать временной интервал после запуска SoftControl SysWatch, по истечении которого проверяется, запущены ли нужные модули. Если некоторые модули не обнаружены, создается соответствующее событие безопасности.

**□ Проверять наличие запущенных модулей после входа пользователя через (мин.):**

Установить интервал задержки после входа пользователя в систему, после которого начнется проверка наличия модулей, имеющих флаг [Должен быть запущенным в пользовательской сессии](#)<sup>91</sup>, среди запущенных процессов.

Некоторые модули имеют критическую важность для при работе пользователя в системе. SoftControl Service Center позволяет указать модули, наличие которых необходимо проверять, и задать временной интервал после входа пользователя, по истечении которого проверяется, запущены ли нужные модули. Если некоторые модули не обнаружены, создается соответствующее событие безопасности.

**□ Высокий риск отсутствия модулей:**

Если отмечено и в ходе проверки среди запущенных процессов не обнаружены модули, имеющие флаги [Должен быть запущенным в пользовательской сессии](#)<sup>91</sup> или [Должен быть запущенным при старте системы](#)<sup>90</sup>, то в логе будет сгенерировано событие **Критической**, а не **Высокой** важности.

**□ Отслеживать наличие отладчика:**

Если отмечено и будет обнаружено наличие отладчика ядра в системе или подключение отладчиком к процессу safensec.exe, то в логе будет сгенерировано событие **Критической** важности.

**□ Восстанавливать базу данных после аппаратной перезагрузки:**

В случае аппаратной перезагрузки восстановить базу данных из последней

резервной копии. SoftControl SysWatch создает резервную копию базы данных при начале работы, при получении новых настроек с сервера и при локальном изменении настроек.

**Включить отправку событий из журналов Windows на сервер:**

Передавать на сервер события из журналов Windows (System, Security и Application) на клиентском устройстве.

▼ **Управление инцидентами**

В разделе **Управление инцидентами** категории **SysWatch** установите флажок **Включить автоматическую обработку инцидентов** и задайте реакцию на инциденты из перечня **Список инцидентов** в выпадающем списке **Решение** согласно табл. 15 (рис. [Настройки реакции на инциденты](#)<sup>71</sup>).

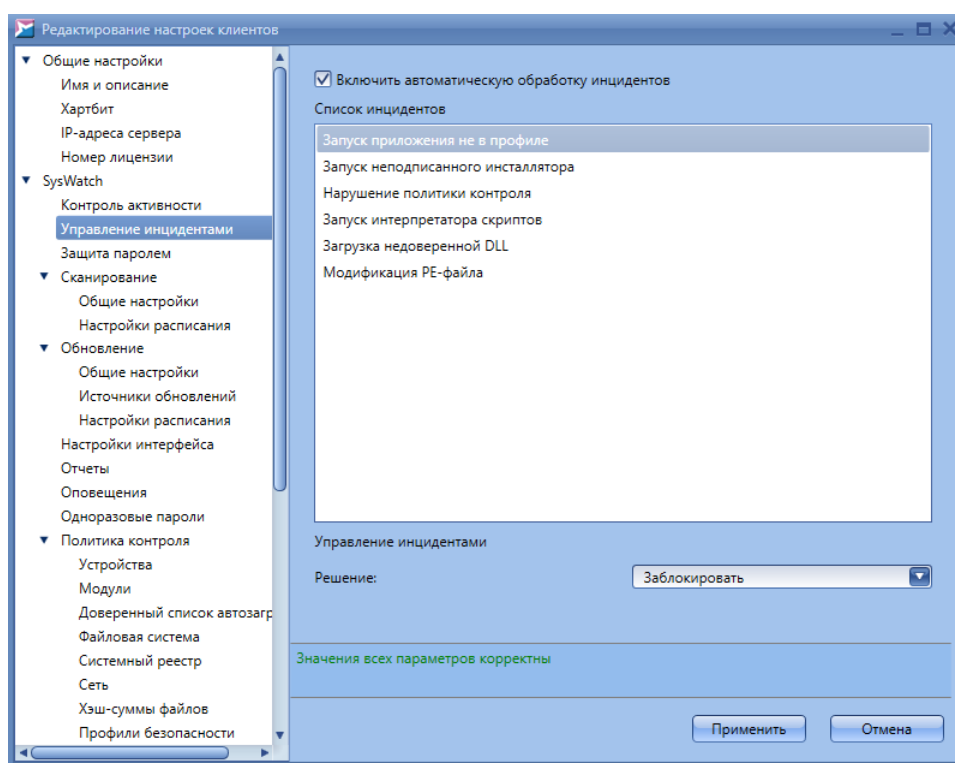


Рисунок 57. Настройки реакции на инциденты

Таблица 15. Возможные действия при инцидентах

Инцидент	Действия
Запуск приложения не в профиле	<ul style="list-style-type: none"> <li>• <b>Выполнить в ограниченном режиме</b> 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</li> </ul>

Инцидент	Действия
	<p>выполнит установку каких-либо дополнительных компонентов, то их последующая загрузка будет предотвращена.</p> <ul style="list-style-type: none"> <li>• <b>Выполнить в ограниченном режиме после проверки</b> Запуск приложения в ограниченном режиме, если при антивирусном сканировании приложения не найдено вредоносного кода. В обратном случае запуск будет заблокирован.</li> <li>• <b>Выполнить в режиме обновления ПО</b> Выполнение приложения под текущей учетной записью без ограничений. При этом приложение и все его дочерние модули помещаются в профиль системы и доверенную зону.</li> <li>• <b>Выполнить в режиме обновления ПО после проверки</b> Запуск приложения в режиме обновления ПО, если при антивирусном сканировании приложения не найдено вредоносного кода. В обратном случае запуск будет заблокирован.</li> <li>• <b>Заблокировать</b> Блокировка запуска приложения.</li> </ul>
Запуск неподписанного инсталлятора	<ul style="list-style-type: none"> <li>• <b>Установить</b> 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.</li> <li>• <b>Установить после проверки</b> Запуск инсталлятора в режиме обновления ПО, если при антивирусном сканировании установщика не найдено вредоносного кода. В обратном случае запуск будет заблокирован.</li> <li>• <b>Установить в ограниченном режиме</b> Выполнение инсталлятора в изолированной среде (песочнице) под учетной записью пользователя «V.I.P.O.» с ограниченными привилегиями. При этом добавления в профиль системы не происходит.</li> <li>• <b>Установить в ограниченном режиме после проверки</b> Запуск инсталлятора в ограниченном режиме, если при антивирусном сканировании установщика не найдено вредоносного кода. В обратном случае запуск будет заблокирован.</li> <li>• <b>Заблокировать</b> Блокировка запуска инсталлятора.</li> </ul>
Нарушение политики контроля	<ul style="list-style-type: none"> <li>• <b>Разрешить</b> Разрешение приложению выполнить действие, совпадающее с условиями правила заданной политики контроля.</li> <li>• <b>Разрешить после проверки</b> Разрешение приложению выполнить действие, совпадающее с условиями правила заданной политики контроля, если при антивирусном сканировании приложения не найдено вредоносного кода. В обратном случае действие будет запрещено.</li> <li>• <b>Запретить</b> Запрет приложению выполнить действие, совпадающее с условиями правила заданной политики контроля.</li> <li>• <b>Запретить и завершить приложение</b> Запрет приложению выполнить действие, совпадающее с условиями правила заданной политики контроля, и последующее завершение приложения.</li> </ul>
Запуск интерпретатора	<ul style="list-style-type: none"> <li>• <b>Разрешить</b> Разрешение запуска без ограничений.</li> </ul>



Инцидент	Действия
скриптов	<ul style="list-style-type: none"> <li>• <b>Запретить</b> Запрет запуска.</li> </ul>
Загрузка недоверенной DLL	<ul style="list-style-type: none"> <li>• <b>Разрешить</b> Разрешение загрузки DLL-библиотеки без ограничений.</li> <li>• <b>Запретить</b> Запрет загрузки.</li> </ul>
Модификация PE-файла не инсталлятором	<ul style="list-style-type: none"> <li>• <b>Разрешить</b> Разрешение модификации PE-файла.</li> <li>• <b>Запретить</b> Запрет модификации.</li> </ul>

Сбросьте флажок **Включить автоматическую обработку инцидентов**, если предполагается делегировать полномочия по обработке инцидентов локальному пользователю SoftControl SysWatch.

#### ▼ Защита паролем

Чтобы установить общий парольный доступ к интерфейсу и/или деинсталлятору SoftControl SysWatch на клиентском хосте, перейдите в раздел **Защита паролем** категории **SysWatch** и установите флажок **Включить защиту паролем** (рис. [Настройки парольной защиты](#)<sup>(73)</sup>).

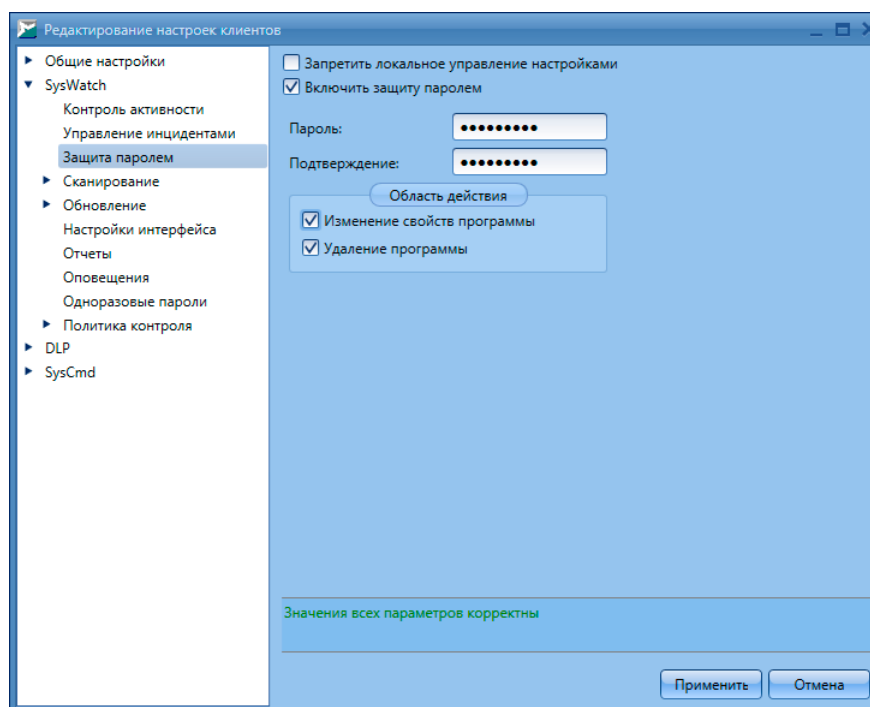


Рисунок 58. Настройки парольной защиты

Задайте **Пароль** и введите его **Подтверждение**, после чего отметьте области

действия:

**Изменение свойств программы:**

Запрос пароля при доступе к ГИП SoftControl SysWatch.

**Удаление программы:**

Запрос пароля при запуске удаления SoftControl SysWatch.

Выставьте флажок **Запретить локальное управление настройками**, если необходимо запретить редактирование настроек SoftControl SysWatch с клиентского хоста. Состояние данной опции будет также отображаться на вкладке [Клиенты](#)<sup>(45)</sup>.

▼ **Настройки сканирования**

В разделе **Сканирование** → **Общие настройки** категории **SysWatch** настройте опции антивирусной проверки (рис. [Общие настройки сканирования](#)<sup>(74)</sup>).

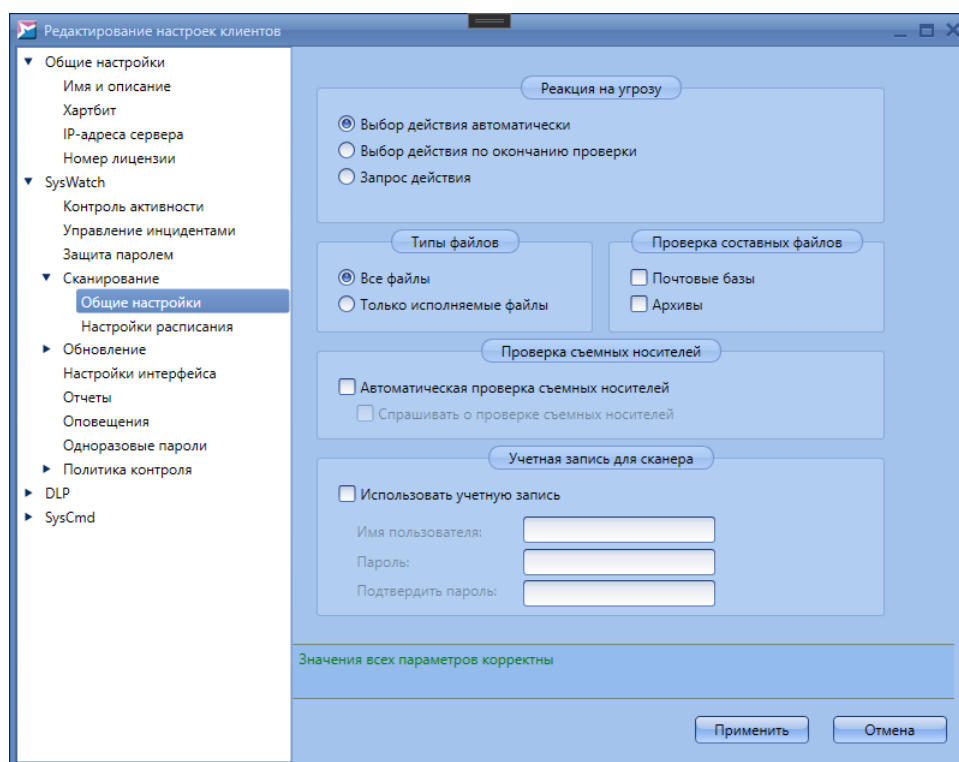


Рисунок 59. Общие настройки сканирования

В области **Реакция на угрозу** выберите один из вариантов действий при обнаружении угроз в процессе антивирусного сканирования:

**Выбор действия автоматически:**

Обезвредить инфицированный объект или удалить его, если лечение не удастся.

**Выбор действия по окончании проверки:**

Запрос действия будет выведен локальному пользователю SoftControl SysWatch по всем обнаруженным угрозам по завершению проверки.

**Запрос действия:**

Запрос действия будет выведен локальному пользователю SoftControl SysWatch при обнаружении каждой угрозы.

В области **Типы файлов** выберите типы файлов, которые будут подвергнуты проверке:

**Все файлы:**

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

**Только исполняемые файлы**

Сканирование только файлов формата PE.

В области **Проверка съемных носителей** установите флажок **Автоматическая проверка съемных носителей**, если необходимо автоматически запускать антивирусное сканирование USB-носителей после их подключения к клиентскому хосту. Установите флажок **Спрашивать о проверке съемных носителей** для отображения диалогового окна с предложением проверки на клиентском хосте.

В области **Учетная запись для сканера** установите флажок **Использовать учетную запись** и введите учетные данные, если требуется указать учетную запись, под которой будет производиться проверка, отличную от системной на клиентском хосте.

В разделе **Сканирование** → **Настройки расписания** категории **SysWatch** можно установить расписание антивирусной проверки, для этого установите флажок **Задать расписание** и настройте параметры (рис. [Настройки расписания сканирования](#)<sup>(75)</sup>).

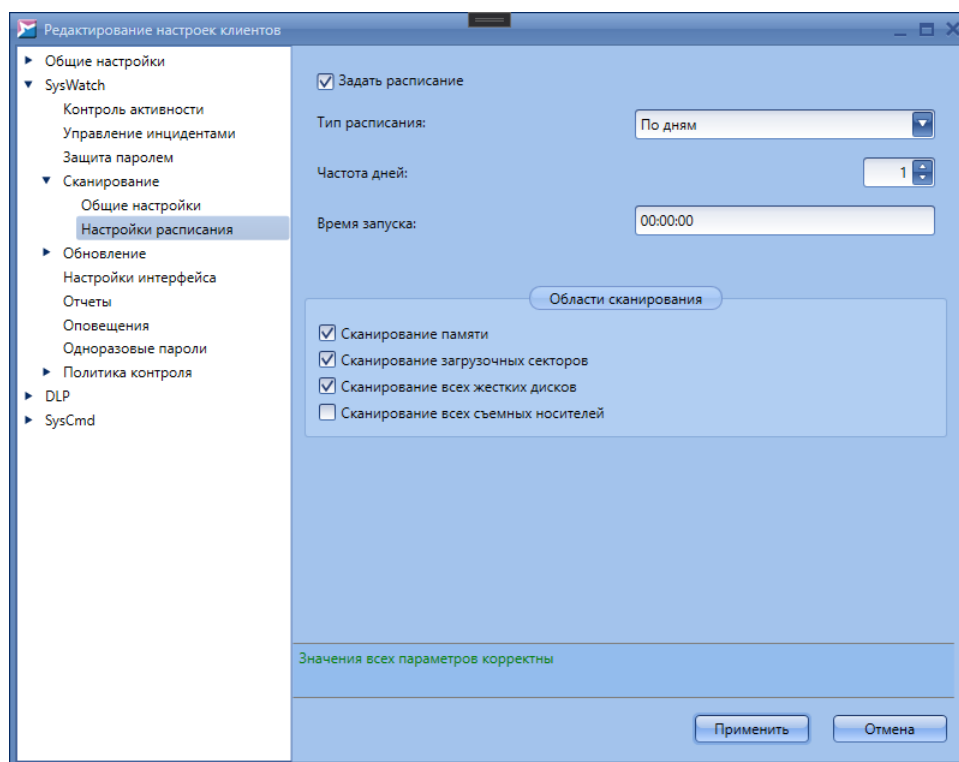


Рисунок 60. Настройки расписания сканирования

В счетчике **Частота дней** укажите периодичность, с которой будет выполняться задача, а в поле **Время запуска** – время начала выполнения задачи в формате **ЧЧ:ММ:СС**.

В разделе **Области сканирования** можно ограничить сканирование только выбранными областями.

#### ▼ Настройки обновления

В разделе **Обновление** → **Общие настройки** категории **SysWatch** настройте опции обновления (рис. [Общие настройки обновления](#)<sup>(76)</sup>).

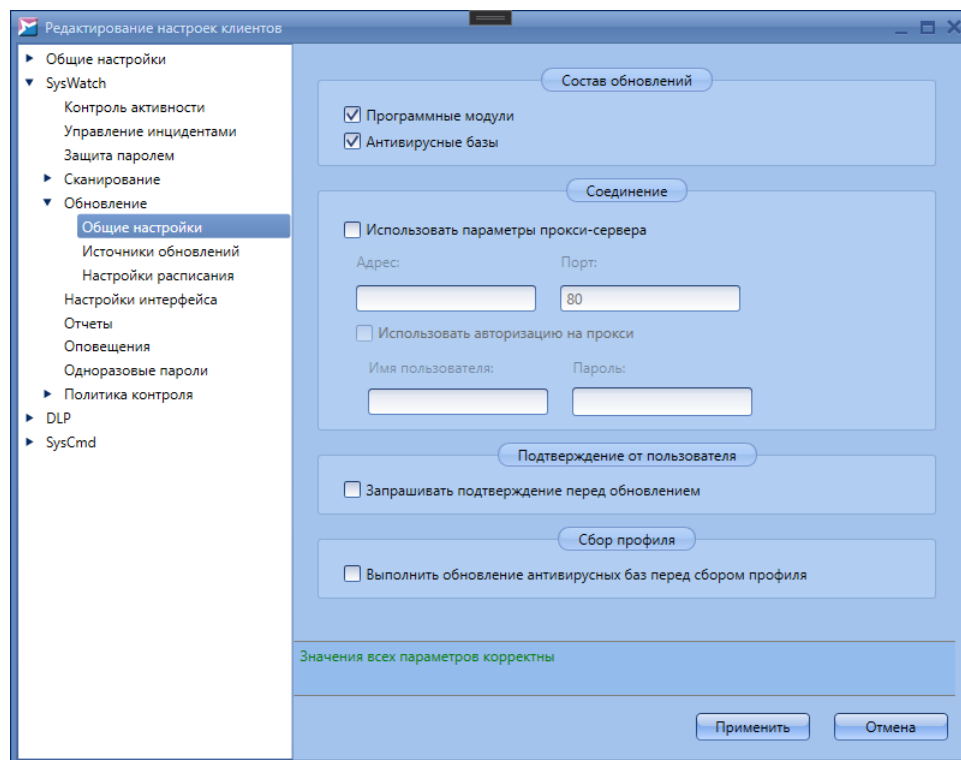


Рисунок 61. Общие настройки обновления

В области **Состав обновлений** выберите требуемые компоненты SoftControl SysWatch для обновления:

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

В области **Соединение** установите флажок **Использовать параметры прокси-сервера** и укажите необходимые настройки, если для соединения с интернет-сервером обновлений используется прокси-сервер.

В области **Подтверждение от пользователя** установите флажок **Запрашивать подтверждение перед обновлением**, если требуется отображать диалог с запросом подтверждения операции на клиентском хосте.

В области **Сбор профиля** установите флажок **Выполнить обновление антивирусных баз перед сбором профиля**, если требуется обновить базы перед сбором профиля на клиентском хосте.

В разделе **Обновление** → **Источники обновлений** можно выбрать способ обновления:

- **Обновить через Сервисный Центр** – обновление посредством внутрисетевого сервера обновлений;

- **Обновить через интернет** – обновление через сервер обновлений ООО «АРУДИТ СЕКЬЮРИТИ», доступный посредством сети Интернет. В области **Источник обновлений** указываются адреса, с которых производится обновление ядра проактивной защиты и баз антивирусных компонентов. Значения по умолчанию берутся из настроек обновления компонента SoftControl Service Center.

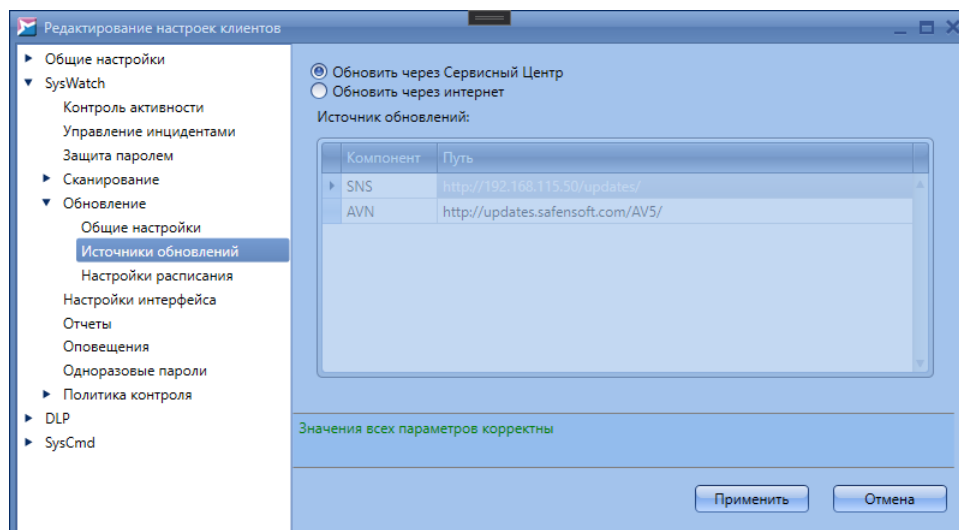


Рисунок 62. Настройки источников обновления

В разделе **Обновление** → **Настройки расписания** категории **SysWatch** можно установить расписание обновления, для этого установите флажок **Задать расписание** и настройте параметры (рис. [Настройки расписания обновления](#)<sup>78</sup>). В счетчике **Частота дней** укажите периодичность, с которой будет выполняться задача, а в поле **Время запуска** – время начала выполнения задачи в формате **ЧЧ:ММ:СС**.

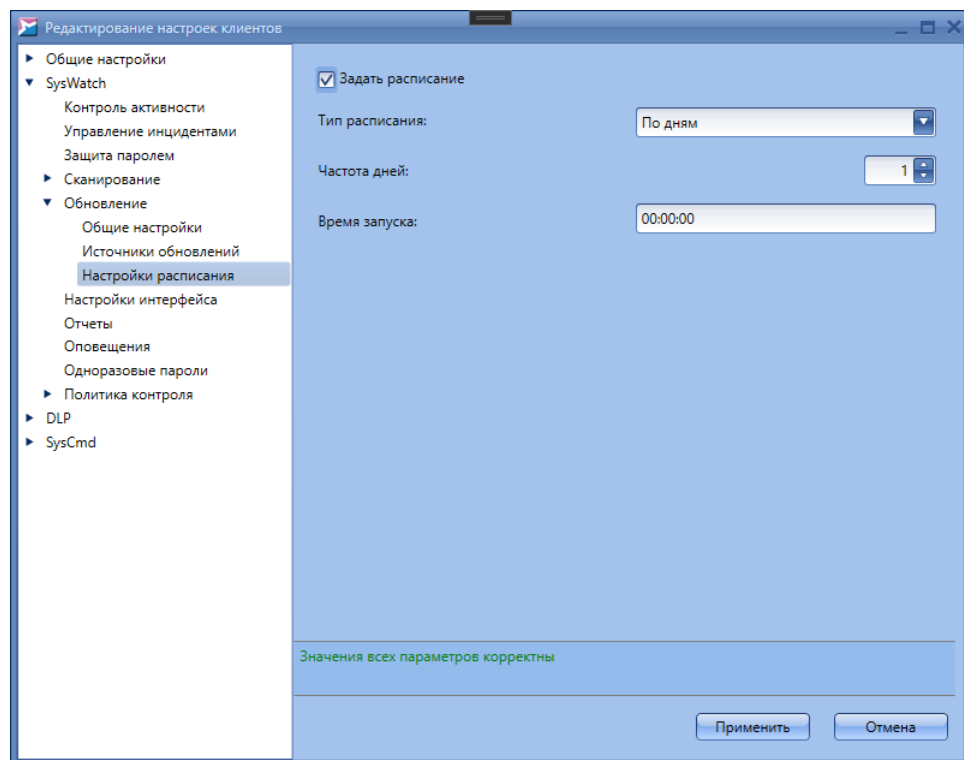


Рисунок 63. Настройки расписания обновления

#### ▼ Настройки интерфейса

В разделе **Настройки интерфейса** категории **SysWatch** выберите необходимые опции интерфейса SoftControl SysWatch на клиентских хостах (рис. [Настройки интерфейса](#)<sup>79</sup>):

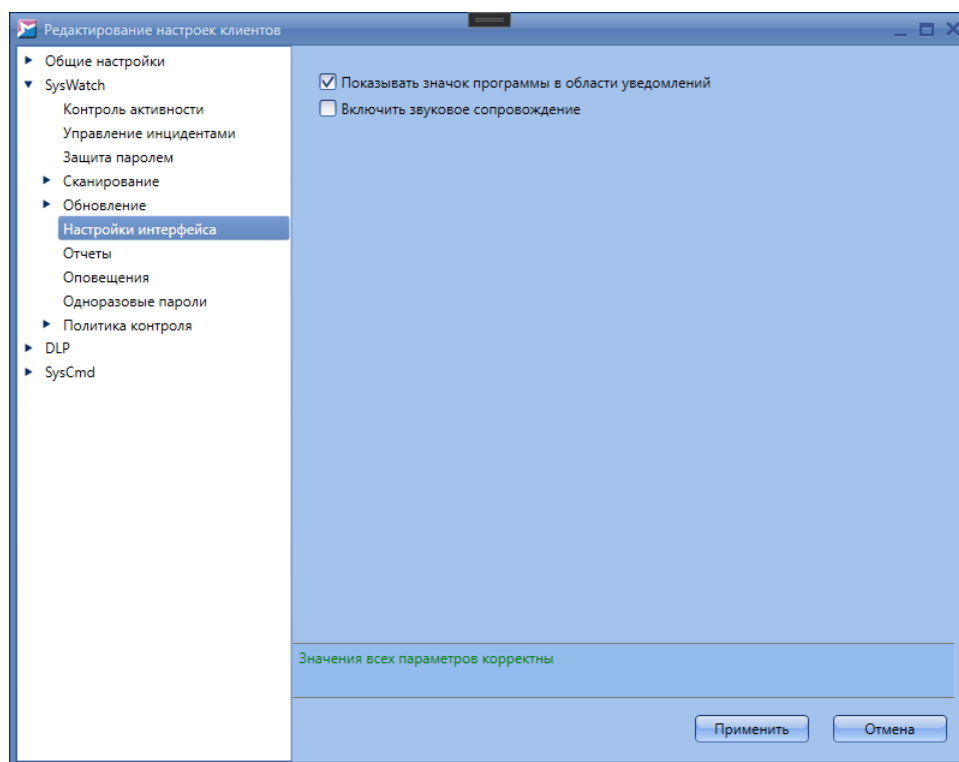


Рисунок 64. Настройки интерфейса

- Показывать значок программы в области уведомлений:**  
отображение значка SoftControl SysWatch в области уведомлений.
- Включить звуковое сопровождение:**  
сопровождать уведомления программы звуками.

#### ▼ **Отчеты**

В разделе **Отчеты** категории **SysWatch** настройте параметры SoftControl SysWatch по протоколированию в текстовые отчеты и регистрации событий в WMI (рис. [Настройки отчетов](#)<sup>(80)</sup>).

В области **Отчеты** установите флажок **Формировать отчеты**, чтобы включить функцию ведения текстовых отчетов, и выберите виды событий для протоколирования:

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



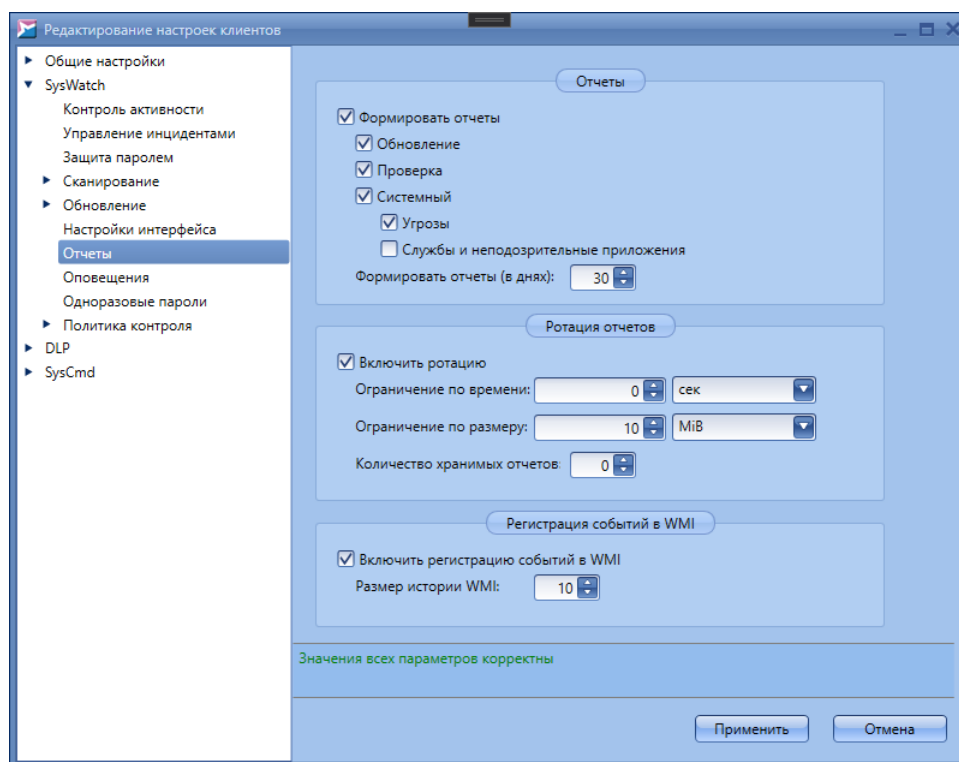


Рисунок 65. Настройки отчётов

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 **Формировать отчеты (в днях)** установите количество дней, за которые сохраняется история событий.

В области **Ротация отчетов** при необходимости установите флажок **Включить ротацию** и укажите параметры ротации (один или несколько), ограничивающие количественные характеристики текстовых отчетов:

- **Ограничение по времени:**

введите в данном поле временной лимит одного файла отчета и выберите единицы величины в выпадающем списке (секунды, минуты, часы, дни).

- **Ограничение по размеру:**

введите в данном поле лимит по размеру одного файла отчета и выберите единицы величины в выпадающем списке (Б, КиБ, МиБ).

- **Количество хранимых логов:**

введите в данном поле максимальное число хранимых частей файлов отчетов.

В области **Регистрация событий в WMI** установите флажок **Включить регистрацию событий в WMI** для включения соответствующей функции и укажите **Размер истории WMI** в одноименном поле.



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

#### ▼ Оповещения

В разделе **Оповещения** категории **SysWatch** установите флажок **Показывать оповещения** для отображения локальных оповещений SoftControl SysWatch на клиентских хостах и выберите необходимые типы сообщений (рис. [Настройка локальных оповещений](#)<sup>82</sup>):

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

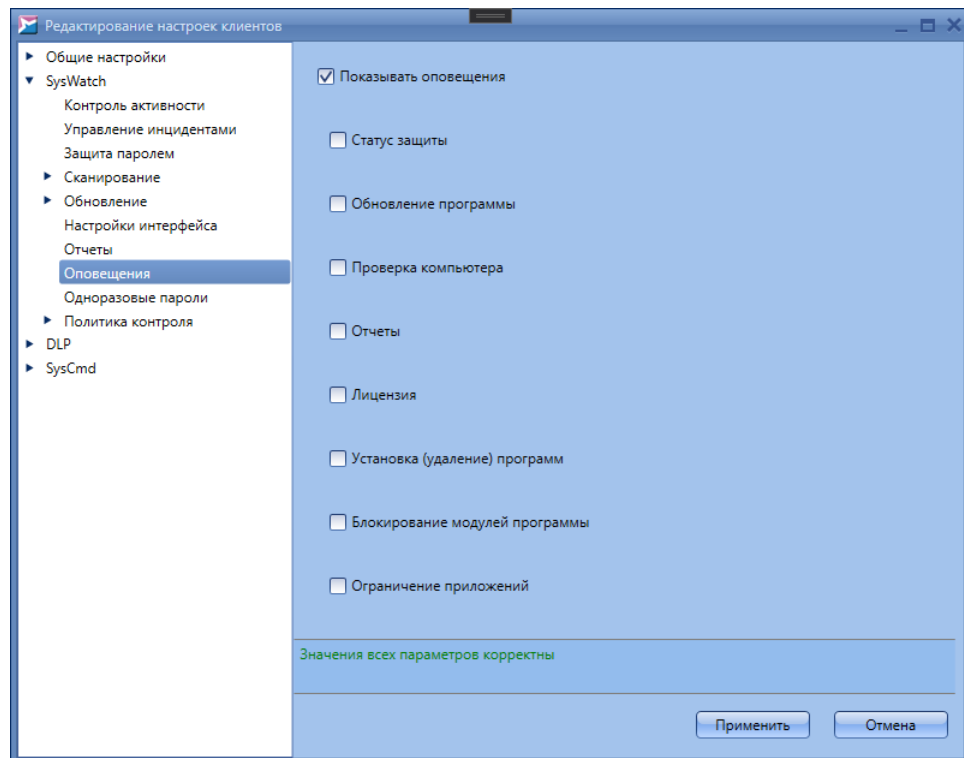




Рисунок 66. Настройка локальных оповещений

#### ▼ Одноразовые пароли

В разделе **Одноразовые пароли** категории **SysWatch** установите флажок **Включить одноразовые пароли** и нажмите на кнопку  (**Сгенерировать ключ**) для выработки 256-битного ключа, на основе которого будут вычисляться одноразовые пароли (рис. [Настройки одноразовых паролей](#)<sup>83</sup>).

---

 Смена ключа делает недействительными все предыдущие пароли.

---

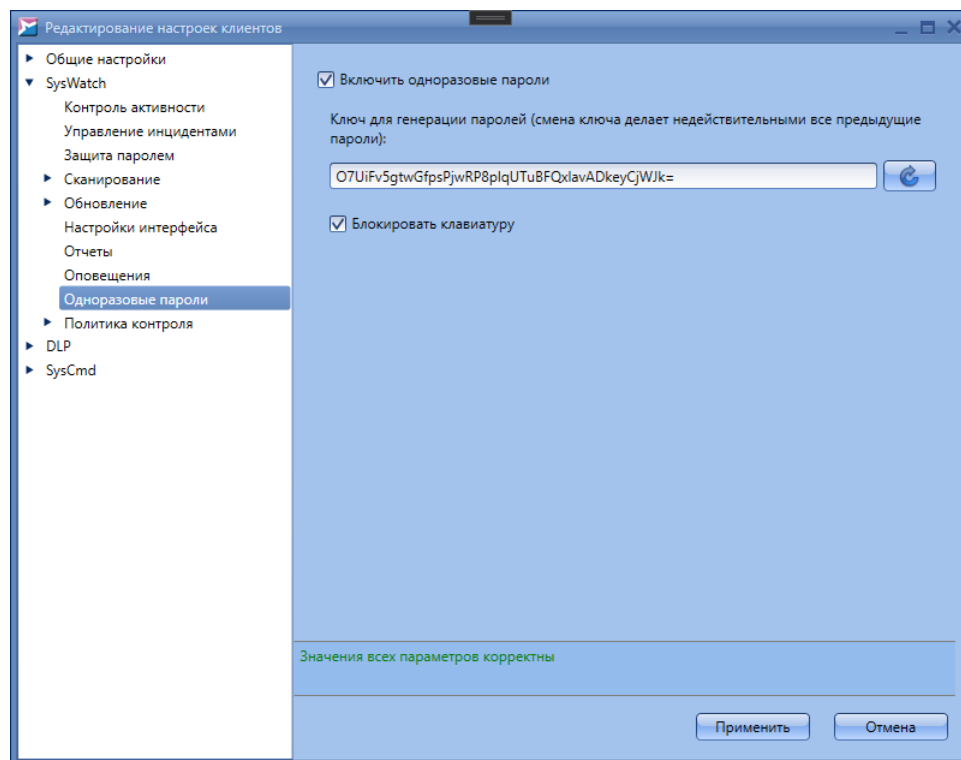


Рисунок 67. Настройки одноразовых паролей

Для блокировки клавиатуры на клиентском хосте выставите галочку **Блокировать клавиатуру**. После того как SoftControl SysWatch получит настройки, клавиатура на клиентском хосте будет заблокирована. Для снятия блокировки необходимо ввести пароль. SoftControl SysWatch проверяет все введенные пользователем последовательности символов, и как только распознает пароль, блокировка клавиатуры снимается. Кроме того, блокировка снимается при отключении и перезапуске системной службы *safensec.exe*.

Если клавиатура не используется в течение 15 минут, она снова блокируется.

Непосредственная генерация одноразовых паролей осуществляется на вкладке [Подразделения](#)<sup>(57)</sup>.

#### ▼ Политика контроля: Устройства

В разделе **Политика контроля** → **Устройства** категории **SysWatch** настройте правила использования следующих внешних устройств и портов системы на клиентских хостах (рис. [Политика контроля устройств](#)<sup>(85)</sup>):

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

- USB-устройства.

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

Дополнительно можно задать исключения – белый список USB-устройств, для которых назначенное правило действовать не будет. Для этого нажмите на ссылку **Дополнительно** и в появившемся окне нажмите на кнопку **+** (**Добавить**) (рис. [Исключения для USB-устройств](#)<sup>85</sup>).

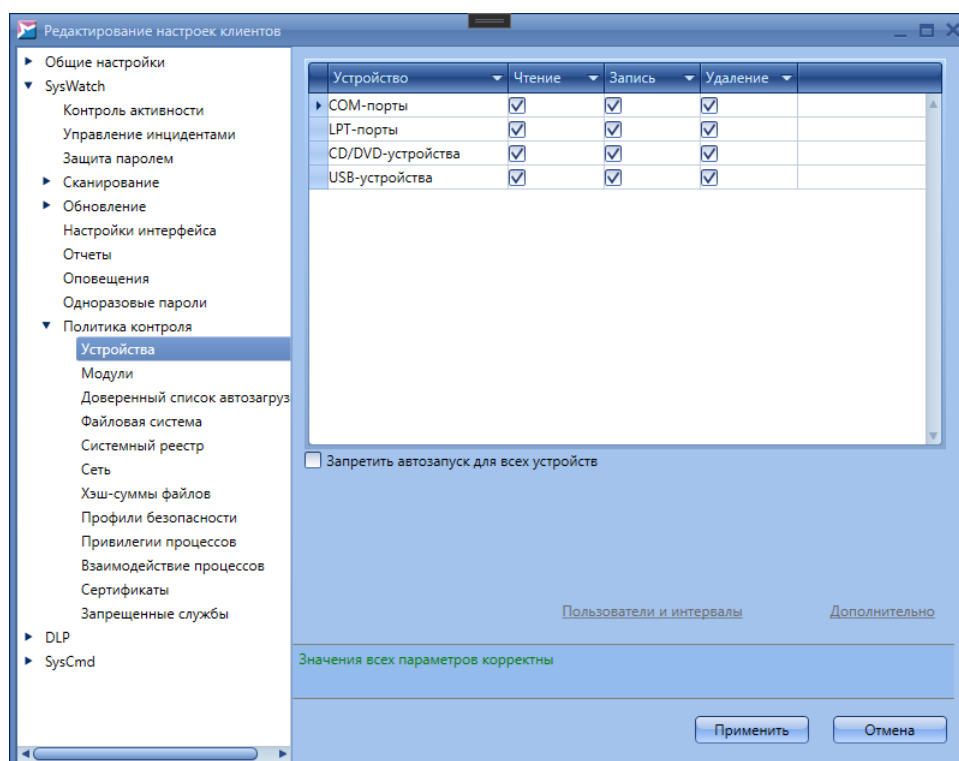


Рисунок 68. Политика контроля устройств

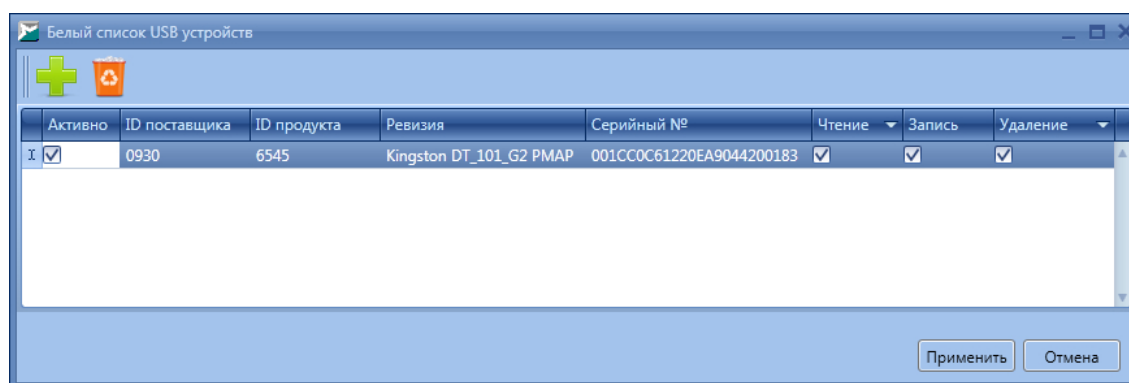


Рисунок 69. Исключения для USB-устройств

Введите параметры USB-устройства в соответствующих полях. Получить данные параметры USB-устройства можно следующим образом:

- 1) Вставьте носитель в USB-порт компьютера.
- 2) Откройте оснастку **Диспетчер устройств** (Device Manager) Панели управления Windows.
- 3) Разверните категорию **Дисковые устройства** (Disk drives) и дважды нажмите левой кнопкой мыши на имени искомого USB-носителя.
- 4) В появившемся окне перейдите на вкладку **Сведения** (Details).
- 5) В выпадающем меню выберите свойство **Родитель** (Parent). В поле **Значение** (Value) отобразится строка вида:

*USB\VID\_<ID поставщика>&PID\_<ID продукта>\<Серийный №>*,

где указаны соответствующие числовые значения параметров **ID поставщика**, **ID продукта** и **Серийный №** (показаны в угловых скобках).

- 6) В выпадающем меню выберите свойство **ID оборудования** (Hardware Ids). В поле **Значение** (Value) отобразится список аппаратных идентификаторов, первый из которых необходимо использовать в качестве параметра **Ревизия**.

После ввода параметров выберите права доступа для данного устройства в соответствующих столбцах **Чтение**, **Запись** и **Удаление**. Чтобы включить устройство в белый список, установите флажок в столбце **Активно**.

Чтобы удалить устройство из списка, нажмите на кнопку  (**Удалить**).

Правила сохраняются после нажатия на кнопку **Применить**.

Для USB-устройств можно также задать временные интервалы и пользователей (или группы пользователей), для которых будут действовать выбранные права доступа. Для этого нажмите на ссылку **Пользователи и интервалы**. В появившемся окне укажите временные интервалы на вкладке **Временные интервалы** и добавьте пользователей на вкладке **Пользователи Windows** с помощью кнопки **Добавить** (функциональность вкладки **Пользователи SoftControl** в текущей версии не реализована). Чтобы изменения вступили в силу, нажмите на кнопку **Применить**.

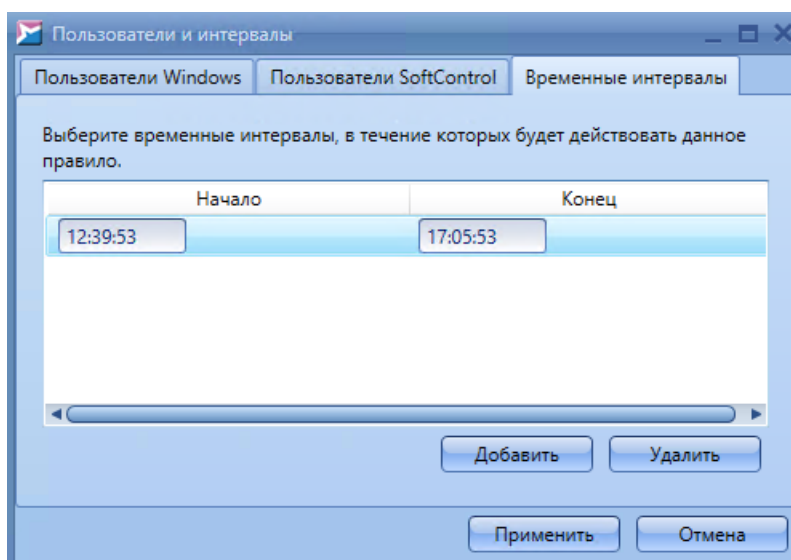


Рисунок 70. Добавление временных интервалов и пользователей для правила

Чтобы заблокировать доступ к CD/DVD-устройствам, COM-портам или LPT-портам, сбросьте любой из флажков в столбцах **Чтение**, **Запись** или **Удаление** для соответствующих типов устройств (при этом будут сброшены все флажки для данного типа).

**i** Для изменения прав доступа к портам (COM, LPT) дополнительно необходима перезагрузка системы на клиентских хостах.

Отметьте опцию **Запретить автозапуск для всех устройств**, если требуется блокировать автозагрузку всех USB- и CD/DVD-устройств.

#### ▼ Политика контроля: Модули

В разделе **Политика контроля** → **Модули** категории **SysWatch** вы можете задать правила для отдельных приложений, установленных на клиентских хостах (рис. [Политика контроля модулей](#)<sup>87</sup>). По умолчанию данная возможность отключена; для включения выставите флажок **Использовать частные настройки для модулей**.

**i** При выставленном флажке **Использовать частные настройки для модулей** после применения настроек на клиентских хостах все локальные настройки будут удалены без возможности восстановления.

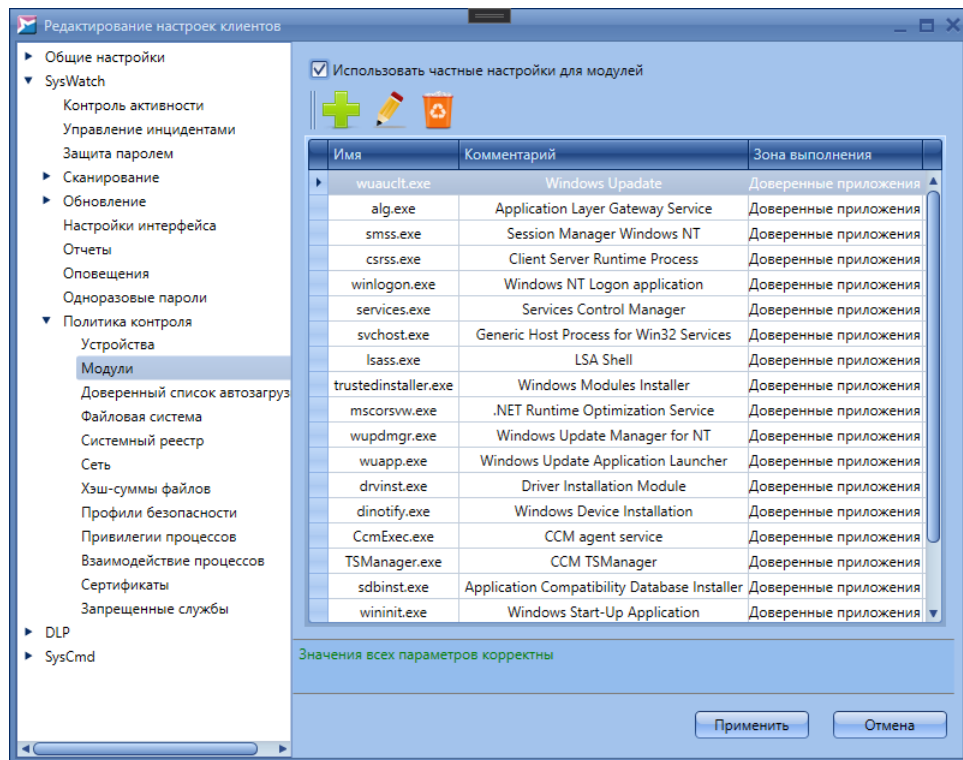


Рисунок 71. Политика контроля модулей

По умолчанию окно содержит ряд модулей ОС Windows. Чтобы добавить в список новый модуль, нажмите на кнопку **+** (**Добавить**). Появившееся окно (рис. [Создание правил для модуля](#)<sup>88</sup>) содержит ряд вкладок для добавления информации о модуле и задания правил для него.

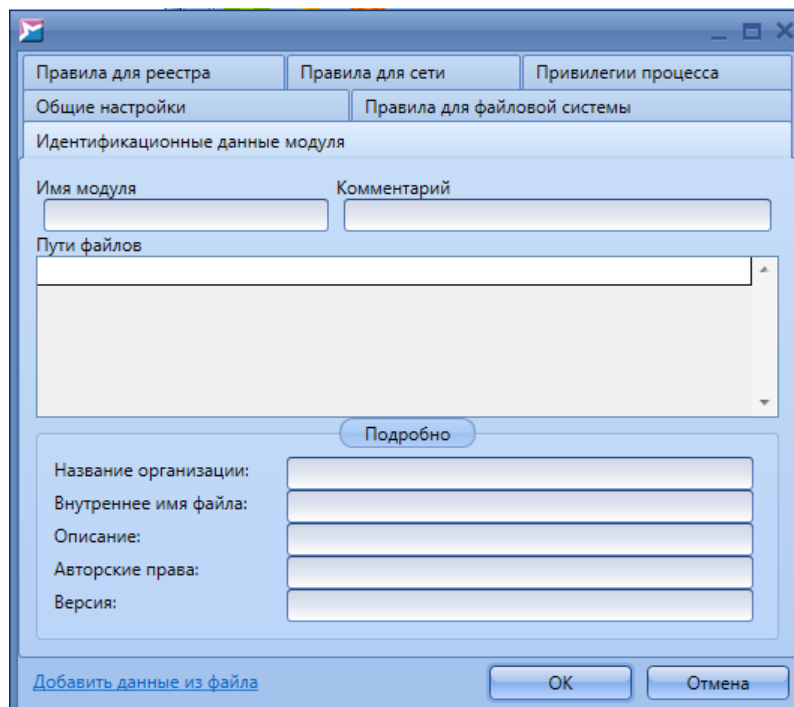


Рисунок 72. Создание правил для модуля



На вкладке **Идентификационные данные модуля** укажите общую информацию по модулю:

- **Имя модуля** – обязательный параметр;
- **Пути файлов** – множество возможных путей к файлу; поле может быть пустым;
- **Комментарий** – краткое описание модуля.

В поле **Пути файлов** могут использоваться маски – инструмент задания правил для добавляемых объектов. Например, с помощью масок можно задать часть пути к файлу. Ниже приведен синтаксис масок:

- **#\*#** – заменяет любое количество символов, кроме символа '\';
- **###** – заменяет любое количество символов;
- **#?#** – заменяет ровно 1 любой символ.

Также вы можете выбрать модуль, щелкнув по ссылке **Добавить данные из файла** (рис. [Создание правил для модуля](#)<sup>88</sup>) и указав в появившемся окне требуемый файл. Данные на вкладке **Идентификационные данные модуля** в этом случае будут заполнены автоматически.

При применении настроек на клиентском хосте исполняемые модули сопоставляются с заданными идентификационными данными следующим образом. Исполняемый модуль считается совпадающим с описанием, если все заданные в идентификационных данных поля соответствуют данному модулю. При этом:

- если для модуля задано несколько путей, достаточно совпадения любого из них;
- если информация о версии модуля представлена в ресурсах на разных языках, то достаточно полного совпадения описания версии на любом языке.

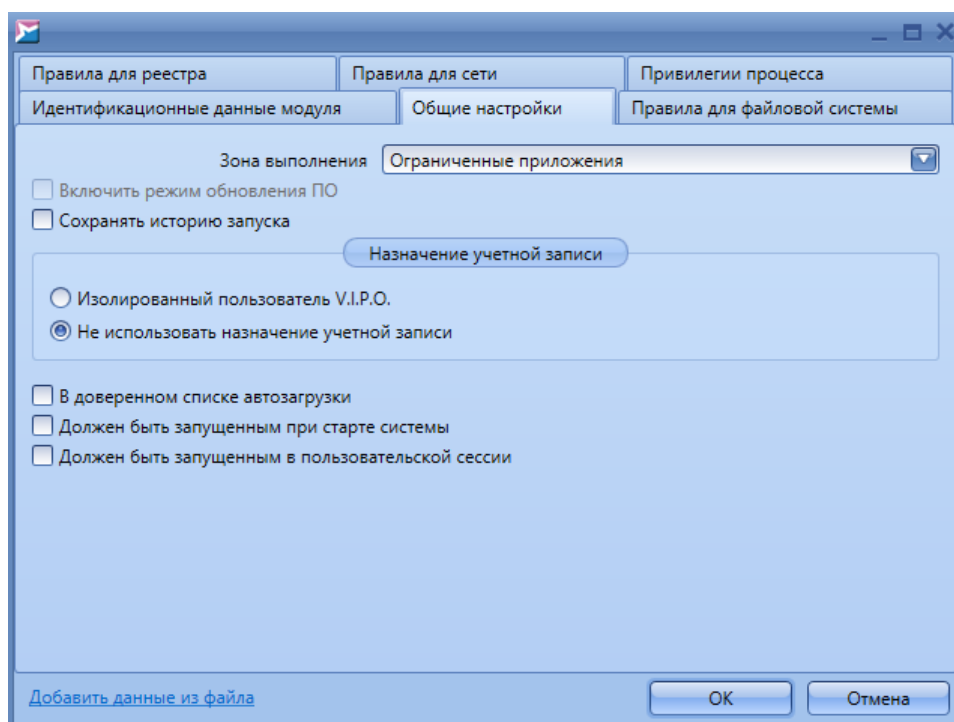


Рисунок 73. Создание правил для модуля: Общие настройки

На вкладке **Общие настройки** укажите условия выполнения модуля.

В области **Зона выполнения** выберите зону, в которой должен запускаться модуль:

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

Выставьте галочки **Включить режим обновления ПО**, если модуль должен запускаться в данном режиме (только для Доверенных приложений), и **Сохранять историю запуска** для записи истории активности модуля.

В группе **Назначение учетной записи** выберите, под какой учетной записью запускать данное приложение (только для Ограниченных приложений):

- **Изолированный пользователь V.I.P.O.;**
- **Не использовать назначение учетной записи.**

Выставьте галочку **В доверенном списке автозагрузки**, если данный модуль необходимо включить в доверенный список автозагрузки (подробнее про доверенный список автозагрузки написано в разделе [Политика контроля → Доверенный список автозагрузки](#)<sup>91</sup>).

Выставьте галочку **Должен быть запущенным при старте системы**, если

необходимо проверить, находится ли этот модуль среди запущенных модулей после старта системы (подробнее в разделе [Контроль активности](#)<sup>(70)</sup>).


Выставьте галочку **Должен быть запущенным в пользовательской сессии**, если необходимо проверить, находится ли этот модуль среди запущенных модулей после входа пользователя в систему (подробнее в разделе [Контроль активности](#)<sup>(70)</sup>).


На вкладке **Правила для файловой системы** задаются правила для доступа приложения к объектам файловой системе (аналогично настройкам в разделе [Политика контроля: Файловая система](#)<sup>(92)</sup>).

На вкладке **Правила для реестра** задаются правила для доступа приложения к объектам системного реестра (аналогично настройкам в разделе [Политика контроля: Системный реестр](#)<sup>(96)</sup>).

На вкладке **Правила для сети** задаются правила контроля сетевой активности для приложения (аналогично настройкам в разделе [Политика контроля: Сеть](#)<sup>(100)</sup>).

На вкладке **Привилегии процесса** задаются ограничения на использование процессом привилегий Windows на клиентских хостах (аналогично настройкам в разделе [Политика контроля: Привилегии процессов](#)<sup>(109)</sup>).

Чтобы изменить данные модуля, нажмите на кнопку  (**Изменить**) или дважды щелкните по нему и настройте параметры аналогично действиям при добавлении модуля.

Чтобы удалить модуль из списка, нажмите на кнопку  (**Удалить**).

Правила сохраняются после нажатия на кнопку **Применить**.

#### ▼ **Политика контроля: Доверенный список автозагрузки**

Доверенный список автозагрузки нужен для того, чтобы отслеживать запуск приложений, не включенных в этот список. Включать в доверенный список автозагрузки следует модули, при запуске которых нет необходимости создавать событие безопасности.

В разделе **Политика контроля** → **Доверенный список автозагрузки** категории **SysWatch** отображается список модулей, включенных в список автозагрузки (рис. [Доверенный список автозагрузки](#)<sup>(92)</sup>). Добавить модули в список можно в

разделе **Политика контроля** → **Модули** (см. [выше](#)<sup>(90)</sup>).

Если параметр **Использовать доверенный список автозагрузки** включен, при логировании процесса отмечается, входит запускаемый модуль в доверенный список или нет.

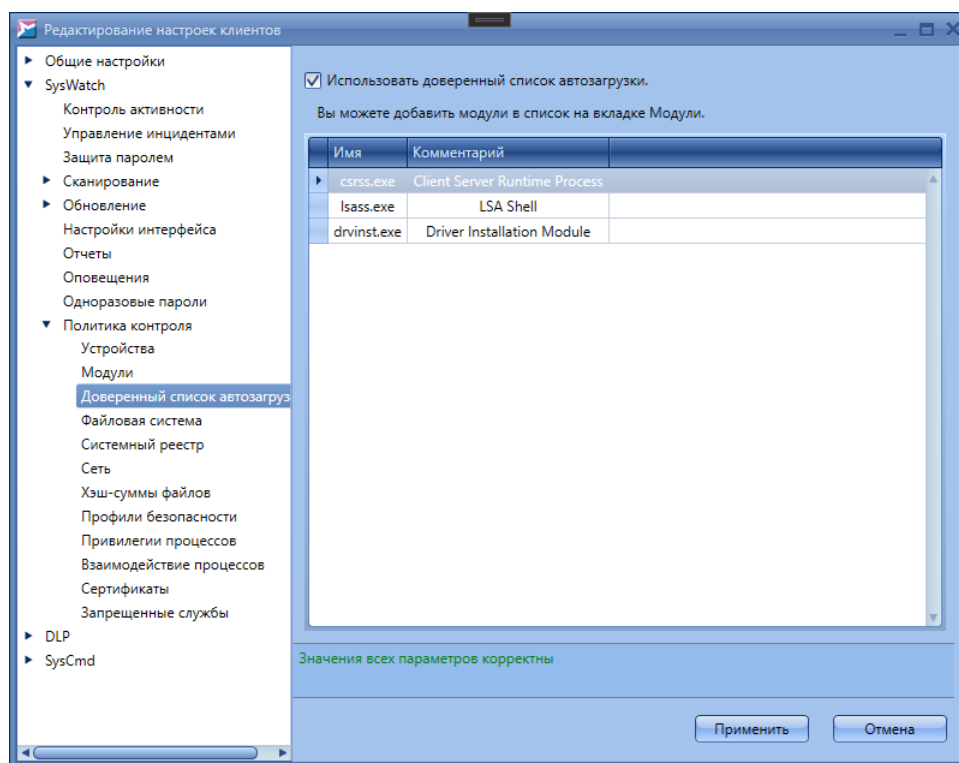


Рисунок 74. Доверенный список автозагрузки

#### ▼ **Политика контроля: Файловая система**

В разделе **Политика контроля** → **Файловая система** категории **SysWatch** определите правила доступа приложений к объектам файловой системы на клиентских хостах (рис. [Политика контроля файловой системы](#)<sup>(92)</sup>):

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

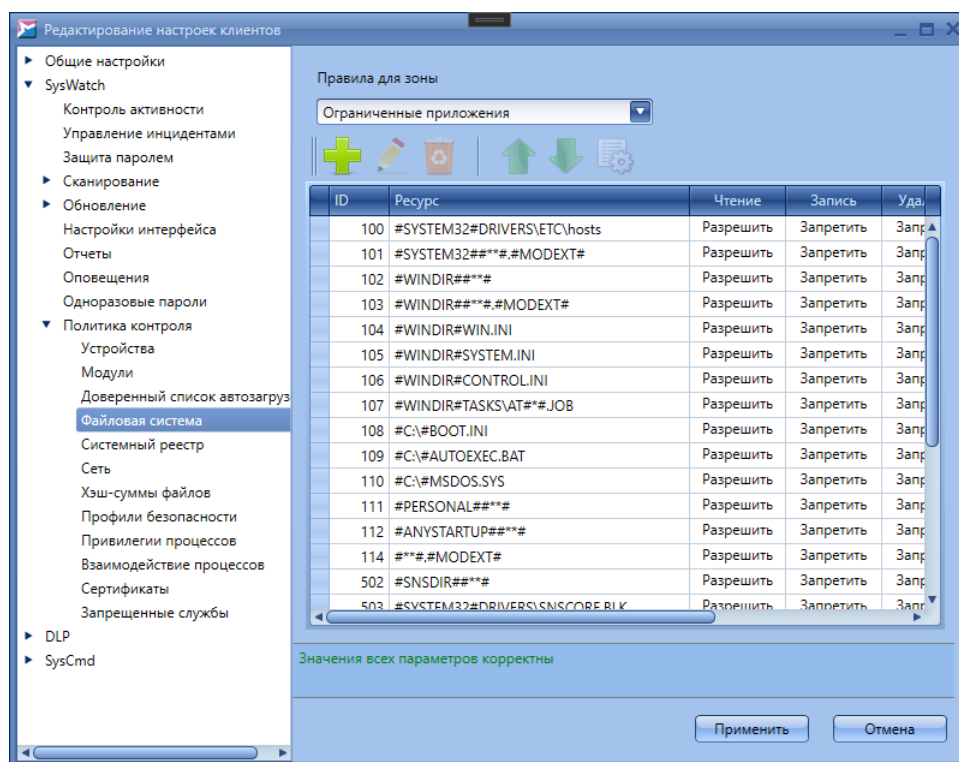


Рисунок 75. Политика контроля файловой системы

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

- **Все** – 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.

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**. Флажок в столбце **Активно** указывает, действует ли данное правило.

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 кнопок  (**Вверх**) и  (**Вниз**).

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

Ниже приведен синтаксис масок:


- **###** – заменяет любое количество символов, кроме символа '\ ' (в случае размещения в конце строки распространяется только на файлы корневой директории);
- **###** – заменяет любое количество символов (в случае размещения в конце строки распространяется на файлы корневой директории, поддиректории и файлы поддиректорий);
- **?#** – заменяет ровно 1 любой символ.

Чтобы создать правило, нажмите на кнопку  (**Добавить**).

В появившемся окне введите полный путь до объекта файловой системы или маску в поле **Файл или каталог** (рис. [Создание правила для объекта файловой системы](#)<sup>94</sup>).

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.

---

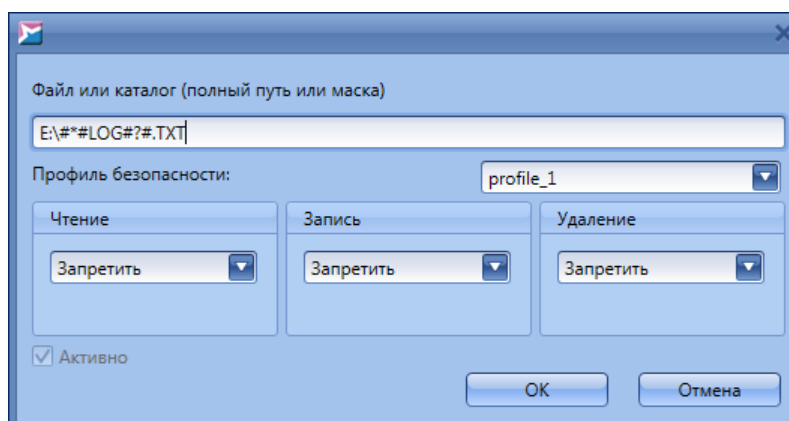


Рисунок 76. Создание правила для объекта файловой системы

Выберите [профиль безопасности для правила](#)<sup>105</sup> в соответствующем выпадающем списке.


Замечание. Установить или снять флажок **Активно** можно только в случае выбора профиля по умолчанию (**No group**). При выборе любого другого профиля, созданного пользователем, данное поле становится неактивным, и его значение совпадает со значением соответствующего поля в разделе **Политика контроля** → **Профили безопасности**.


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.

Обратите внимание, что если запрещено чтение, автоматически запрещены также запись и удаление.

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

Чтобы изменить правило, нажмите на кнопку  (**Изменить**) или дважды нажмите на него и настройте параметры правила аналогично действиям при его создании.

Чтобы задать время действия правила и пользователей (или группы пользователей), к которым оно применяется, нажмите на кнопку  (**Дополнительно**). В появившемся окне укажите временные интервалы на вкладке **Временные интервалы** и добавьте пользователей на вкладке **Пользователи Windows** с помощью кнопки **Добавить** (функциональность вкладки **Пользователи**

**SoftControl** в текущей версии не реализована). Чтобы изменения вступили в силу, нажмите на кнопку **Применить..**

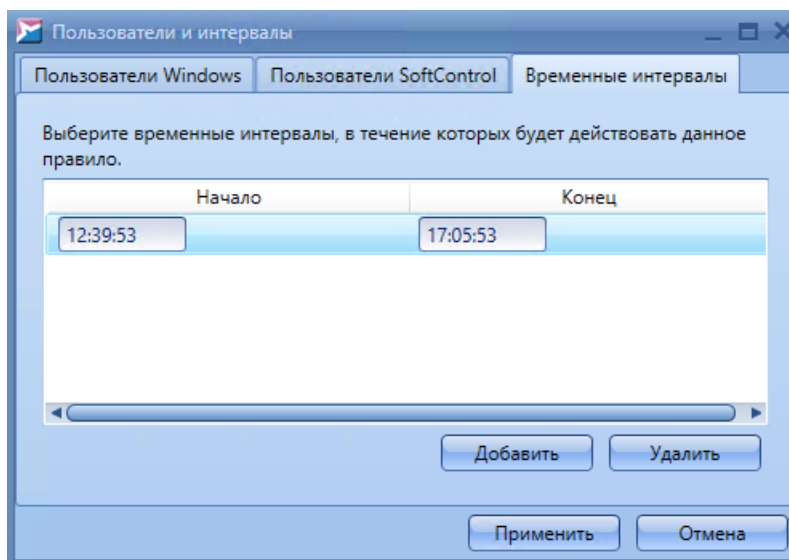


Рисунок 77. Добавление временных интервалов и пользователей для правила

Чтобы удалить правило, нажмите на кнопку  (**Удалить**).

**i** В наборе политик контроля 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 клиентского хоста.

#### ▼ Политика контроля: Системный реестр

В разделе **Политика контроля** → **Системный реестр** категории **SysWatch** определите правила доступа приложений к объектам системного реестра на клиентских хостах (рис. [Политика контроля системного реестра](#)<sup>96</sup>):

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



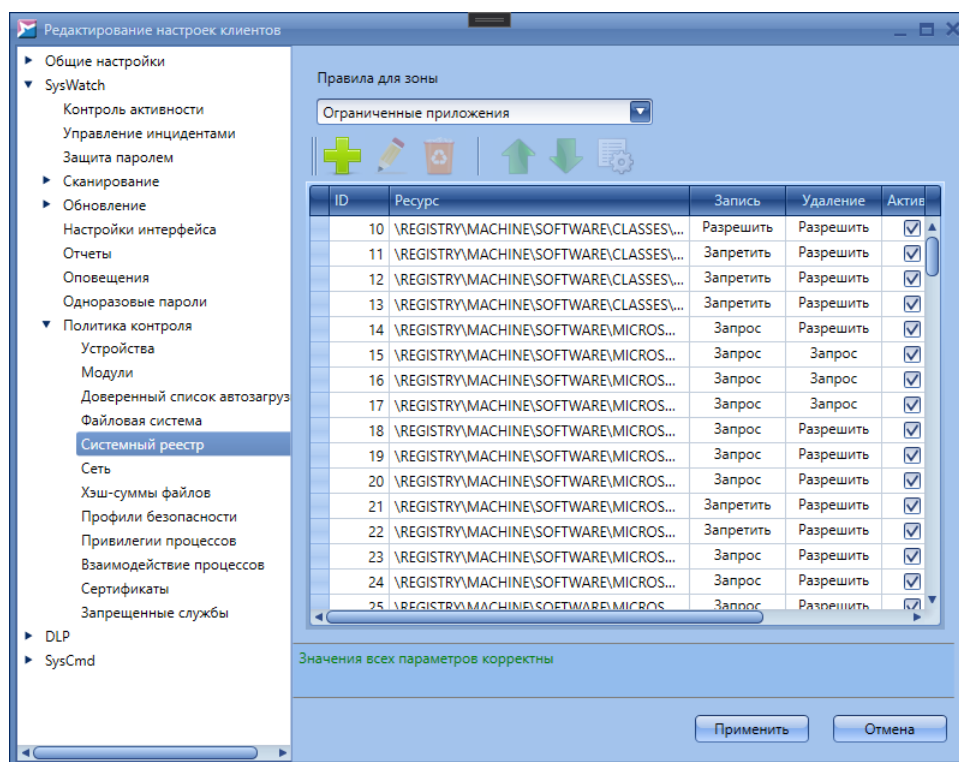


Рисунок 78. Политика контроля системного реестра

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

- **Все** – 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.

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**. Флажок в столбце **Активно** указывает, действует ли данное правило.

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 кнопок **↑ (Вверх)** и **↓ (Вниз)**.

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.

Чтобы создать правило, нажмите на кнопку **+** (**Добавить**).

В появившемся окне введите полный путь до объекта системного реестра или маску в поле **Ключ или параметр реестра**, (рис. [Создание правила для объекта системного реестра](#)<sup>98</sup>), при этом корневые разделы реестра в задаваемом пути должны быть указаны следующим образом:

- `\REGISTRY\MACHINE\SOFTWARE\CLASSES\` – раздел HKEY\_CLASSES\_ROOT;
- `\REGISTRY\MACHINE\` – раздел HKEY\_LOCAL\_MACHINE;
- `\REGISTRY\USER\\` – раздел HKEY\_CURRENT\_USER для пользователя с указанным идентификатором безопасности (<SID>);
- `\REGISTRY\USER\` – раздел HKEY\_USERS.

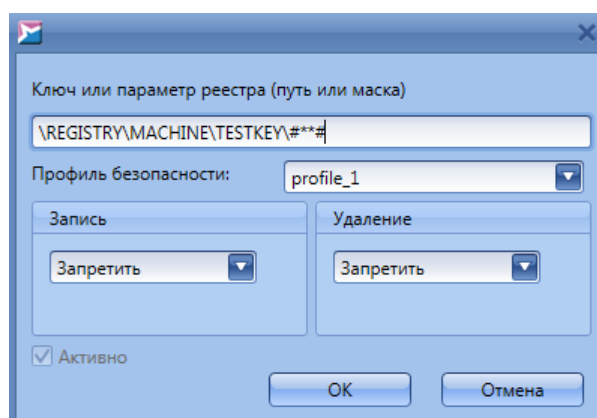


Рисунок 79. Создание правила для объекта системного реестра

Выберите [профиль безопасности для правила](#)<sup>105</sup> в соответствующем выпадающем списке.

Замечание. Установить или снять флажок **Активно** можно только в случае выбора профиля по умолчанию (**No group**). При выборе любого другого профиля, созданного пользователем, данное поле становится неактивным, и его значение совпадает со значением соответствующего поля в разделе **Политика контроля** →


### Профили безопасности


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.

Обратите внимание, что если запрещено чтение, автоматически запрещены также запись и удаление.

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

Чтобы изменить правило, нажмите на кнопку  (**Изменить**) или дважды нажмите на него и настройте параметры правила аналогично действиям при его создании.

Чтобы задать время действия правила и пользователей (или группы пользователей), к которым оно применяется, нажмите на кнопку  (**Дополнительно**). В появившемся окне укажите временные интервалы на вкладке

**Временные интервалы** и добавьте пользователей на вкладке **Пользователи Windows** с помощью кнопки **Добавить** (функциональность вкладки **Пользователи SoftControl** в текущей версии не реализована). Чтобы изменения вступили в силу, нажмите на кнопку **Применить**.

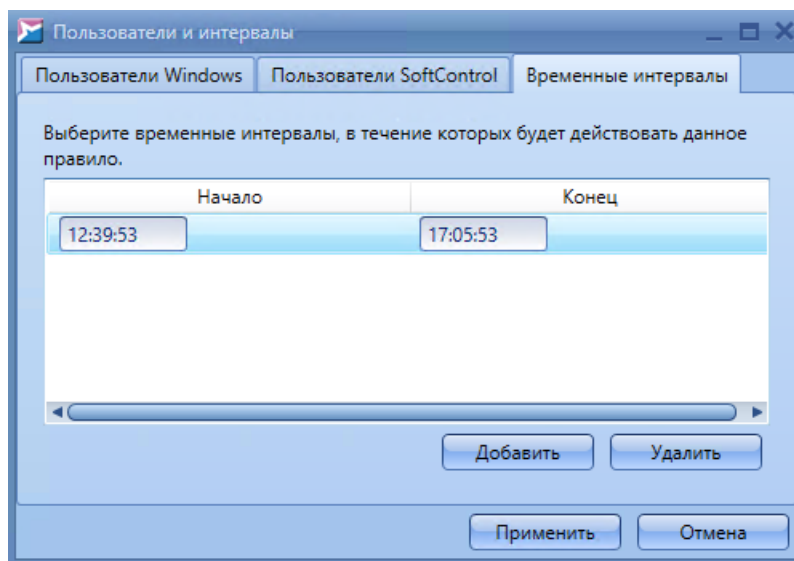


Рисунок 80. Добавление временных интервалов и пользователей для правила

Чтобы удалить правило, нажмите на кнопку  (**Удалить**).

**i** В наборе политик контроля 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 клиентского хоста.

#### ▼ Политика контроля: Сеть

В разделе **Политика контроля** → **Сеть** категории **SysWatch** определите правила контроля сетевой активности приложений на клиентских хостах (рис. [Политика контроля сетевой активности](#)<sup>(101)</sup>):

- Прием данных;
- Передача данных.

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

- **Все** – 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.

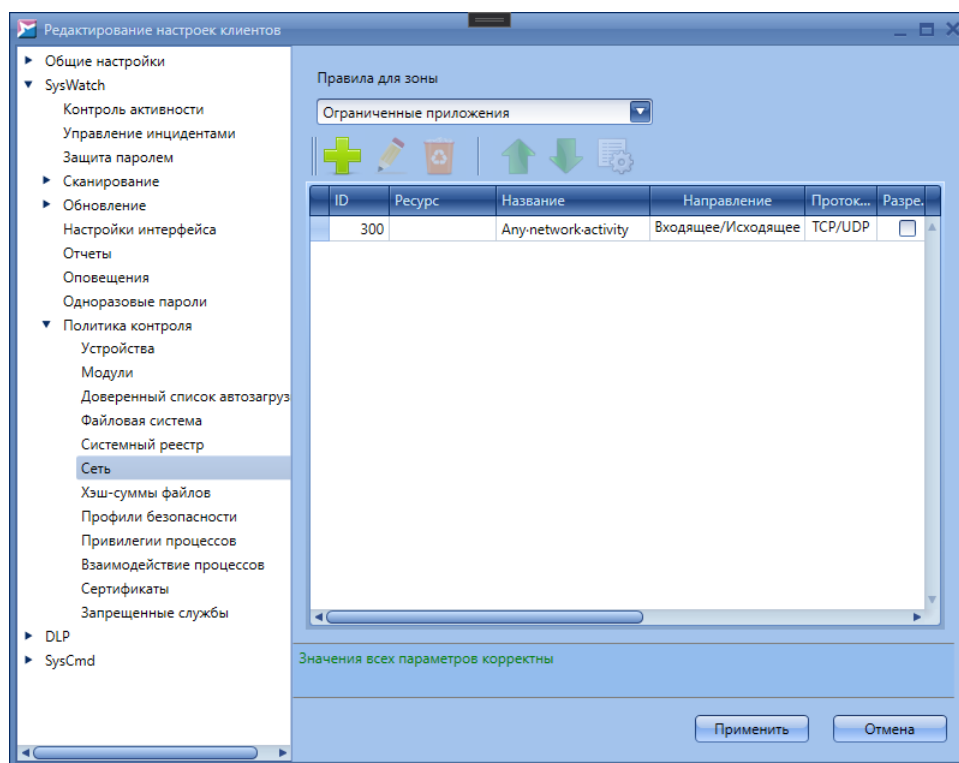


Рисунок 81. Политика контроля сетевой активности

Каждое правило представляет собой запись в линейном списке и имеет свой уникальный идентификатор **ID**. Параметры правила указаны в столбцах **Название**, **Направление** и **Протокол**. Разрешение или запрет сетевого соединения указывается флажком в столбце **Разрешение**; необходимость обработки события, в случае его наступления, локальным пользователем – в столбце **Подтверждение**. Флажок в столбце **Активно** указывает, действует ли данное правило.

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 кнопок **↑ (Вверх)** и **↓ (Вниз)**.

Чтобы создать правило, нажмите на кнопку **+** (**Добавить**).

В появившемся окне задайте параметры правила (рис. [Создание правила контроля](#)

сетевой активности<sup>(102)</sup>):

- **Название** – наименование правила.
- **Направление** – направление сетевой активности, определяющее инициатора соединения:
  - **Входящее** – сетевое соединение, иницируемое удаленным хостом;
  - **Исходящее** – сетевое соединение, иницируемое клиентским хостом;
  - **Входящее/Исходящее** – любое из направлений.
- **Протокол** – тип протокола передачи данных по сети:
  - **TCP**;
  - **UDP**;
  - **TCP/UDP** – любой из протоколов.

На вкладках **Локальный адрес** и **Удаленный адрес** задаются конечные точки, между которыми осуществляется передача данных, на клиентском и удаленном хостах соответственно. В обеих вкладках выберите, на какие сетевые адреса и порты распространяется действие правила, и введите значения в соответствующие поля при необходимости:

- **Адрес** – IP-адрес узла сети:
  - **Любой адрес**;
  - **Определенный адрес**;
  - **Диапазон адресов**.
- **Порт** – сетевой порт:
  - **Любой порт**;
  - **Определенный порт**;
  - **Диапазон портов**.

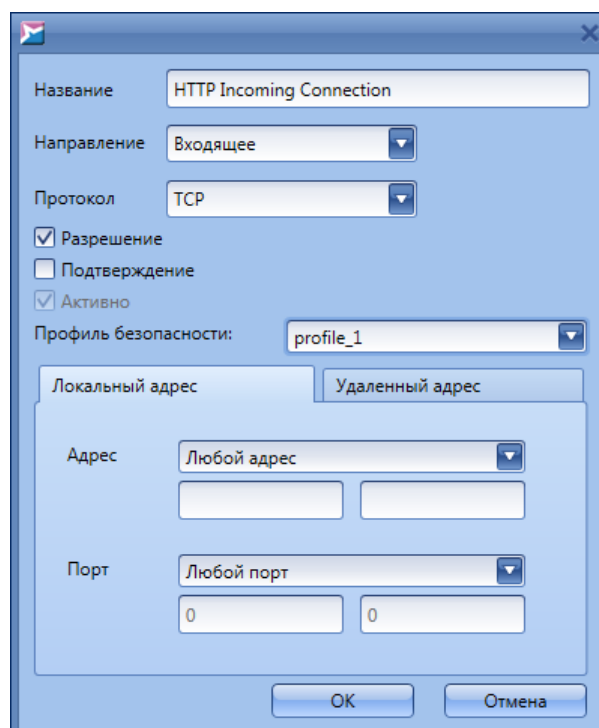



Рисунок 82. Создание правила контроля сетевой активности


Для разрешения сетевого соединения с указанными параметрами установите флажок **Разрешение**, для запрещения – сбросьте его. Если предполагается обработка событий сетевой активности приложений локальным пользователем на клиентском хосте, установите флажок **Подтверждение** (при этом должна быть отключена [автоматическая обработка инцидентов](#)<sup>(71)</sup>).

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

Выберите [профиль безопасности для правила](#)<sup>(105)</sup> в соответствующем выпадающем списке.

**Замечание.** Установить или снять флажок **Активно** можно только в случае выбора профиля по умолчанию (**No group**). При выборе любого другого профиля, созданного пользователем, данное поле становится неактивным, и его значение совпадает со значением соответствующего поля в разделе **Политика контроля** → **Профили безопасности**.

Чтобы изменить правило, нажмите на кнопку  (**Изменить**) или дважды нажмите на него и настройте параметры правила аналогично действиям при его создании.

Чтобы задать время действия правила и пользователей (или группы пользователей), к которым оно применяется, нажмите на кнопку .

(Дополнительно). В появившемся окне укажите временные интервалы на вкладке **Временные интервалы** и добавьте пользователей на вкладке **Пользователи Windows** с помощью кнопки **Добавить** (функциональность вкладки **Пользователи SoftControl** в текущей версии не реализована). Чтобы изменения вступили в силу, нажмите на кнопку **Применить**.

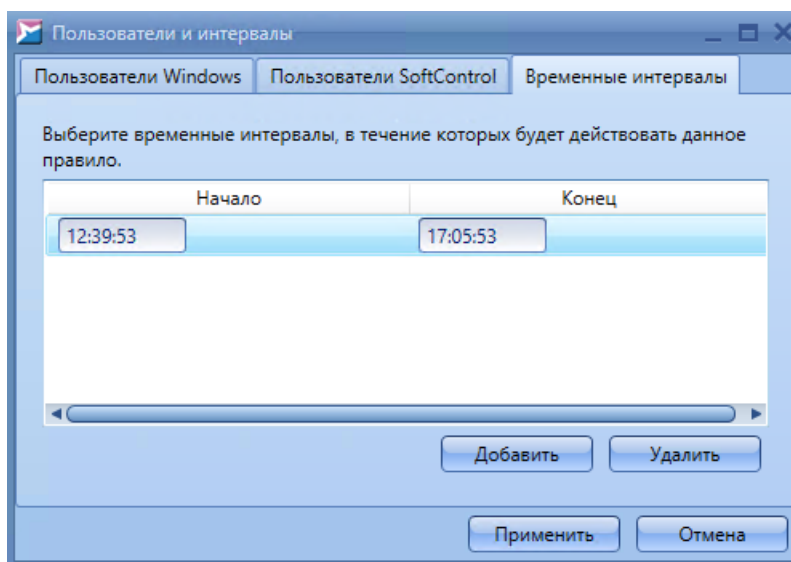


Рисунок 83. Добавление временных интервалов и пользователей для правила

Чтобы удалить правило, нажмите на кнопку  (**Удалить**).

#### ▼ **Политика контроля: Хэш-суммы файлов**

В разделе **Политика контроля** → **Хэш-суммы файлов** вы можете создать список хэш-сумм, которые нужно включить в профиль, а также список хэш-сумм, которые из профиля нужно исключить. Эти хэш-суммы однократно применяются к профилю, но в дальнейшем настройки могут изменяться, например при запуске инсталлятора.

Хэш-суммы файлов можно добавлять в списки двумя способами: через кнопку **Добавить** или через кнопку **Импорт** (загружается файл XML).

Контрольные суммы файлов можно копировать из вкладок [Данные профиля](#)<sup>(49)</sup> и [Сравнение профилей](#)<sup>(183)</sup>.



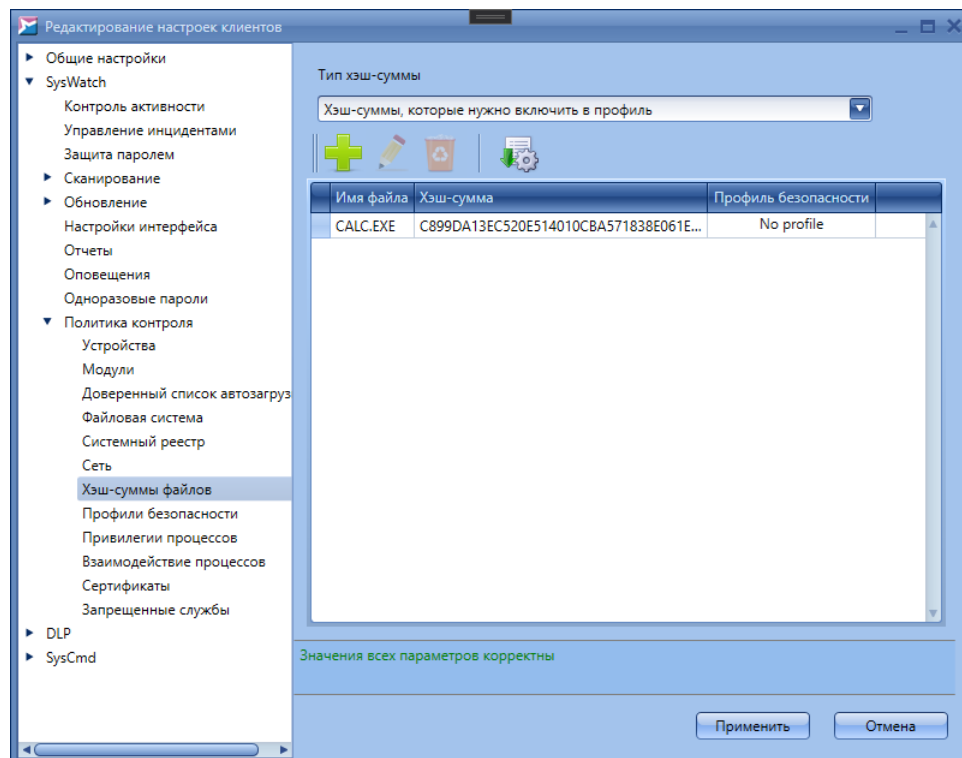


Рисунок 84. Хэш-суммы файлов

#### ▼ Политика контроля: Профили безопасности

В разделе **Политика контроля** → **Профили безопасности** категории **SysWatch** вы можете загрузить из базы данных SoftControl Service Center профили безопасности, объединяющие различные правила контроля активности в логические группы (рис. [Профили безопасности](#)<sup>105</sup>). Создать профили можно на вкладке [Профили безопасности](#)<sup>125</sup>.

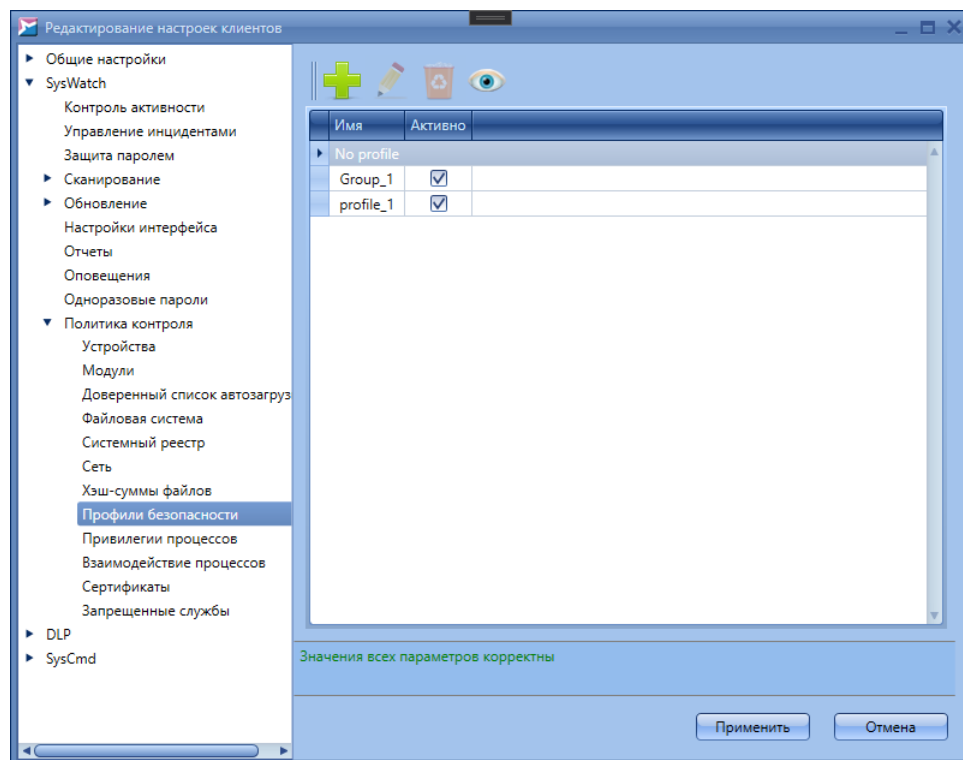



Рисунок 85. Профили безопасности

По умолчанию окно содержит неизменяемый профиль (**No group**), в который включены все правила для файловой системы, системного реестра, сети и модулей, имеющиеся в соответствующих разделах окна настроек (см. рисунки [Политика контроля файловой системы](#)<sup>(92)</sup>, [Политика контроля системного реестра](#)<sup>(96)</sup>, [Политика контроля сетевой активности](#)<sup>(101)</sup> и [Политика контроля модулей](#)<sup>(87)</sup>). Правила этого профиля не подлежат редактированию и удалению. Для просмотра информации по профилю дважды нажмите на него или нажмите на кнопку  (**Просмотр**).

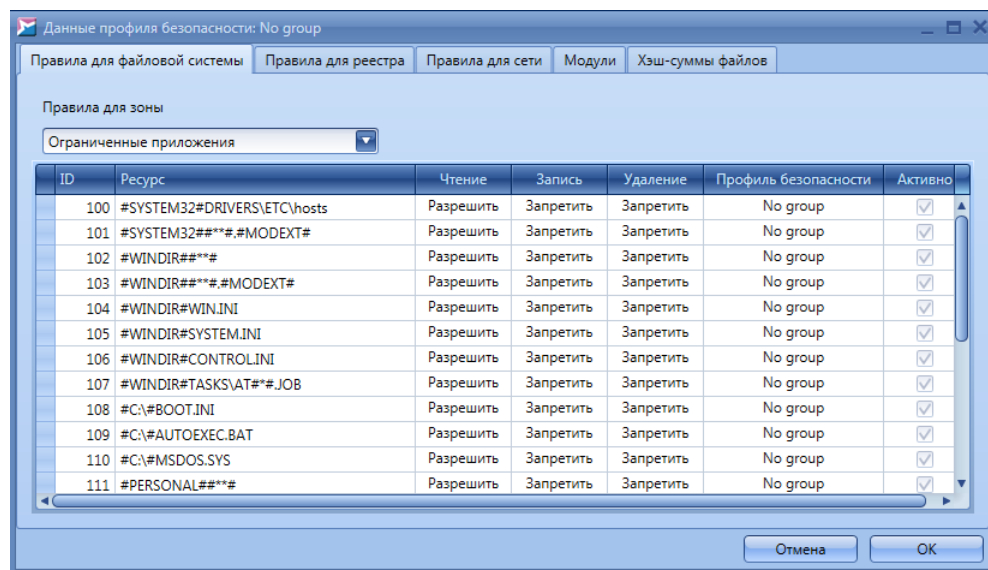


Рисунок 86. Профиль безопасности по умолчанию

Чтобы загрузить профиль из базы данных, нажмите на кнопку **+** (**Загрузить**). В появившемся окне выберите требуемый профиль (рис. [Загрузка профиля безопасности](#)<sup>107</sup>).

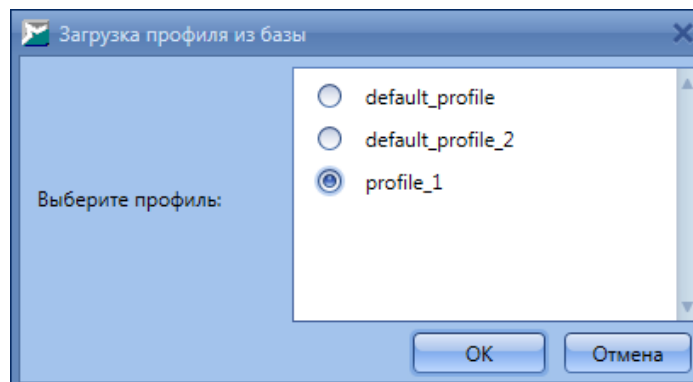


Рисунок 87. Загрузка профиля безопасности


Если профиль с выбранным именем уже имеется в текущих настройках, выдается сообщение об ошибке, и процесс прерывается.


Чтобы добавить правило определенной категории в профиль, выполните следующие действия:


1. Перейдите в соответствующий раздел настроек SoftControl SysWatch.
2. Создайте новое правило или откройте на редактирование существующее.
3. В окне создания правила выберите требуемый профиль в выпадающем списке (см. рисунки [Создание правила для объекта файловой системы](#)<sup>94</sup>, [Создание правила для объекта системного реестра](#)<sup>98</sup>, [Создание правила контроля сетевой активности](#)<sup>102</sup>).

#### 4. Нажмите на кнопку **ОК**.

Чтобы удалить из профиля правило определенной категории, перейдите в соответствующий раздел настроек SoftControl SysWatch и выполните стандартную операцию удаления в этом разделе.

Чтобы переименовать профиль, нажмите на кнопку  (**Переименовать**) и в появившемся окне задайте новое имя профиля.

Для просмотра информации по выбранному профилю нажмите на кнопку  (**Просмотр**). В появившемся окне указана подробная информация по профилю, разделенная по категориям правил (см. рис. [Профиль безопасности по умолчанию](#)<sup>(106)</sup>).

Чтобы удалить профиль безопасности, нажмите на кнопку  (**Удалить**). Если входящие в профиль правила необходимо сохранить, в появившемся окне выберите профиль, в который они будут перенесены, и нажмите на кнопку **Да** (рис. [Удаление профиля](#)<sup>(108)</sup>); в противном случае нажмите на кнопку **Нет** – тогда все правила будут удалены.

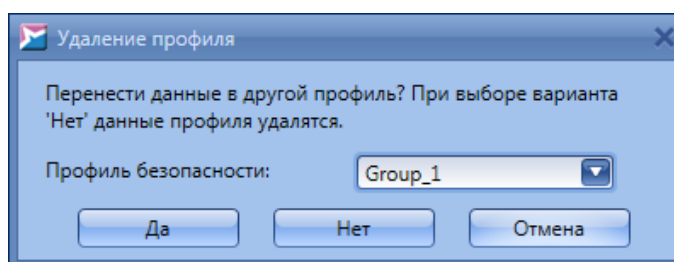


Рисунок 88. Удаление профиля

#### ▼ Политика контроля: Привилегии процессов

В разделе **Политика контроля** → **Привилегии процессов** категории **SysWatch** настройте ограничения на использование процессами следующих привилегий Windows на клиентских хостах (рис. [Политика контроля привилегий процессов](#)<sup>(109)</sup>):

- Архивация файлов и каталогов;
- Обход перекрестной проверки;
- Создание глобальных объектов;
- Создание файла подкачки;
- Отладка программ;
- Имитация клиента после проверки пользователя;
- Увеличение приоритета выполнения;

- Настройка квот памяти для процесса;
- Загрузка и выгрузка драйверов устройств;
- Выполнение задач по обслуживанию томов;
- Профилирование одного процесса;
- Принудительное удаленное завершение работы;
- Восстановление файлов и каталогов;
- Управление аудитом и журналом безопасности;
- Завершение работы системы;
- Изменение параметров среды изготовителя;
- Профилирование производительности системы;
- Изменение системного времени;
- Смена владельцев файлов и других объектов;
- Отключение компьютера от стыковочного узла.

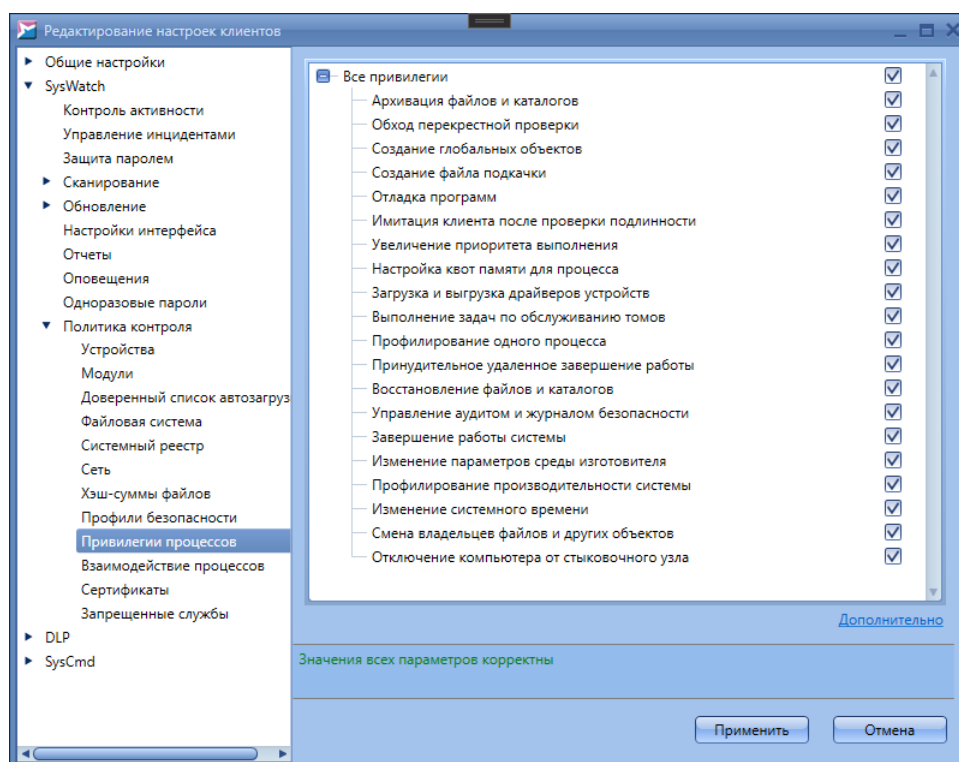



Рисунок 89. Политика контроля привилегий процессов

Условие: правила распространяются на все приложения из ограниченной зоны выполнения.

По умолчанию приложения (процессы) обладают всеми вышеуказанными привилегиями, но при этом могут быть ограничены ОС. Чтобы ограничить

привилегии вручную, сбросьте флажки у требуемых привилегий.

Описание привилегий и области их применения представлено в разделе [Дополнительная информация](#)<sup>237</sup>.

Чтобы задать время действия правила и пользователей (или группы пользователей), к которым оно применяется, нажмите на кнопку  (**Дополнительно**). В появившемся окне укажите временные интервалы на вкладке **Временные интервалы** и добавьте пользователей на вкладке **Пользователи Windows** с помощью кнопки **Добавить** (функциональность вкладки **Пользователи SoftControl** в текущей версии не реализована). Чтобы изменения вступили в силу, нажмите на кнопку **Применить**.

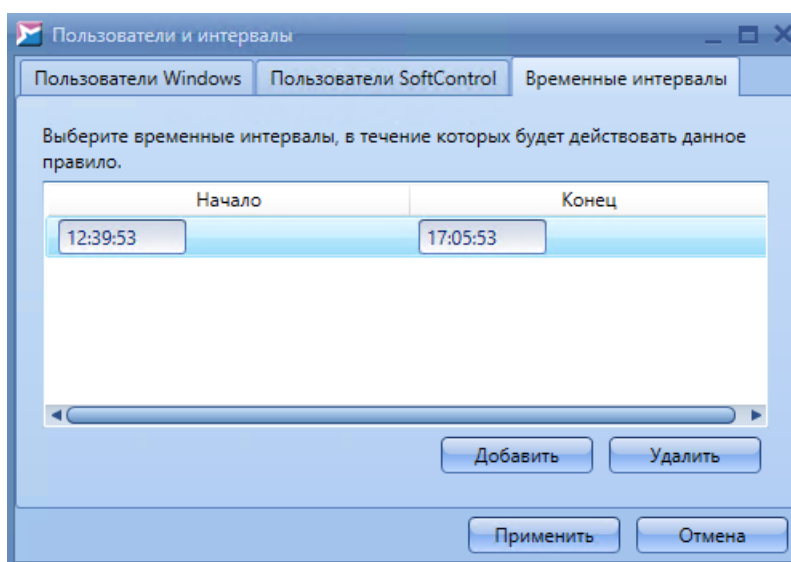


Рисунок 90. Добавление временных интервалов и пользователей для правила

#### ▼ Политика контроля: Взаимодействие процессов

В разделе **Политика контроля** → **Взаимодействие процессов** категории **SysWatch** настройте разрешения для взаимодействия процессов (рис. [Политика контроля взаимодействия процессов](#)<sup>110</sup>):

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

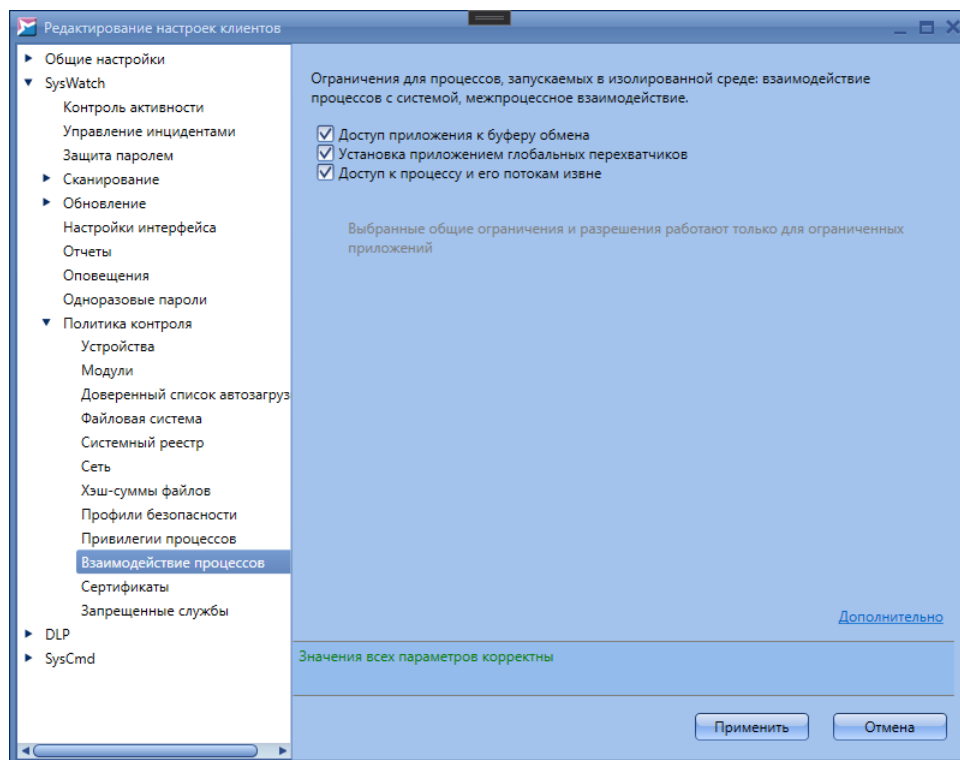


Рисунок 91. Политика контроля взаимодействия процессов

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

Чтобы задать время действия правила и пользователей (или группы пользователей), к которым оно применяется, нажмите на ссылку **Дополнительно**. В появившемся окне укажите временные интервалы на вкладке **Временные интервалы** и добавьте пользователей на вкладке **Пользователи Windows** с помощью кнопки **Добавить** (функциональность вкладки **Пользователи SoftControl** в текущей версии не реализована). Чтобы изменения вступили в силу, нажмите на кнопку **Применить**.

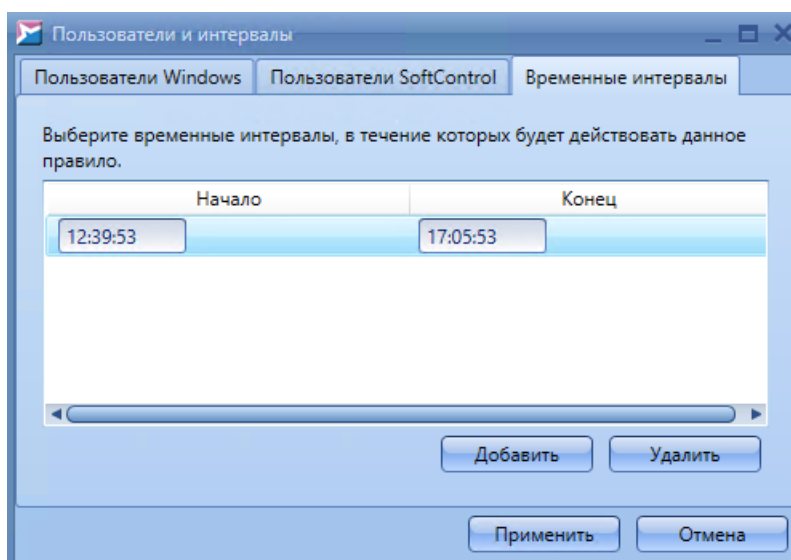


Рисунок 92. Добавление временных интервалов и пользователей для правила

#### ▼ Политика контроля: Сертификаты

В разделе **Политика контроля** → **Сертификаты** категории **SysWatch** определите белый список сертификатов ЭЦП для дополнительного контроля активности процессов на клиентских хостах (рис. [Белый список сертификатов](#)<sup>112</sup>).

При запуске приложения SoftControl SysWatch эвристически определяет, является ли оно инсталлятором или скриптом. По умолчанию инсталлятор запускается в режиме обновления ПО, если имеет действительную ЭЦП. Помимо этого, возможна дополнительная проверка сертификата ЭЦП на наличие в белом списке сертификатов. Для этого установите флажок **Использовать белый список сертификатов** и сформируйте список.



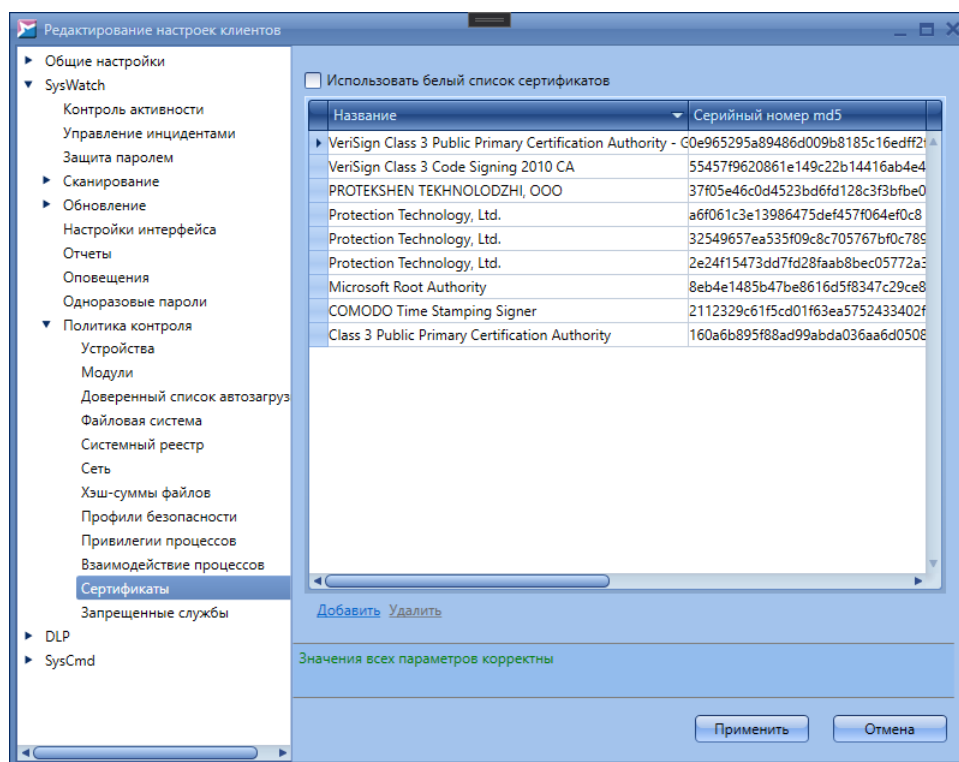


Рисунок 93. Белый список сертификатов

Изначально SoftControl SysWatch содержит базовый список сертификатов доверенных производителей, в том числе сертификаты Protection Technology, Ltd. Чтобы добавить новый сертификат, нажмите на ссылку **Добавить** и укажите приложение, инсталлятор или сценарий, подписанный ЭЦП, сертификат которого требуется включить в перечень, после чего нажмите на кнопку **Открыть**. В появившемся окне со списком сертификатов ЭЦП выбранного файла установите флажки в столбце **Добавить** для требуемых сертификатов и нажмите на кнопку **ОК** (рис. [Выбор сертификатов для добавления](#)<sup>(113)</sup>). Установите флажок в столбце **Доверять** для добавленных сертификатов (рис. [Белый список сертификатов](#)<sup>(112)</sup>).

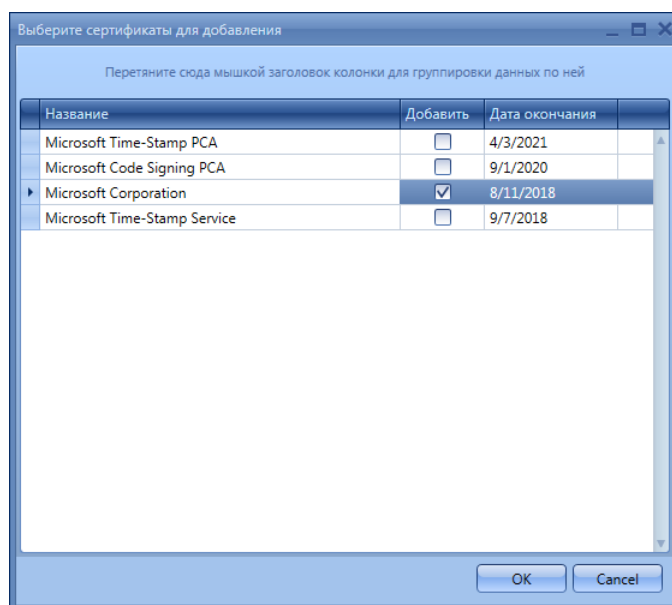


Рисунок 94. Выбор сертификатов для добавления

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](#)<sup>(112)</sup>).

#### ▼ Политика контроля: Запрещенные службы

В разделе **Политика контроля** → **Запрещенные службы** категории **SysWatch** задается список служб, выполнение которых на клиентских хостах требуется заблокировать.

По умолчанию запрещены следующие службы: *RemoteRegistry*, *TermService*, *SSDPSRV*, *RDSessMgr*, *Seclogon* (рис. [Запрещенные службы](#)<sup>(114)</sup>). Чтобы дополнить список, выставите галочку **Запретить выполнение следующих служб**, введите название службы в появившейся ячейке и нажмите **Enter**.

После применения настроек на клиентских хостах перечисленные службы переходят в состояние *Отключена*. Если какая-либо служба была запущена на момент применения настроек, она продолжит работу.

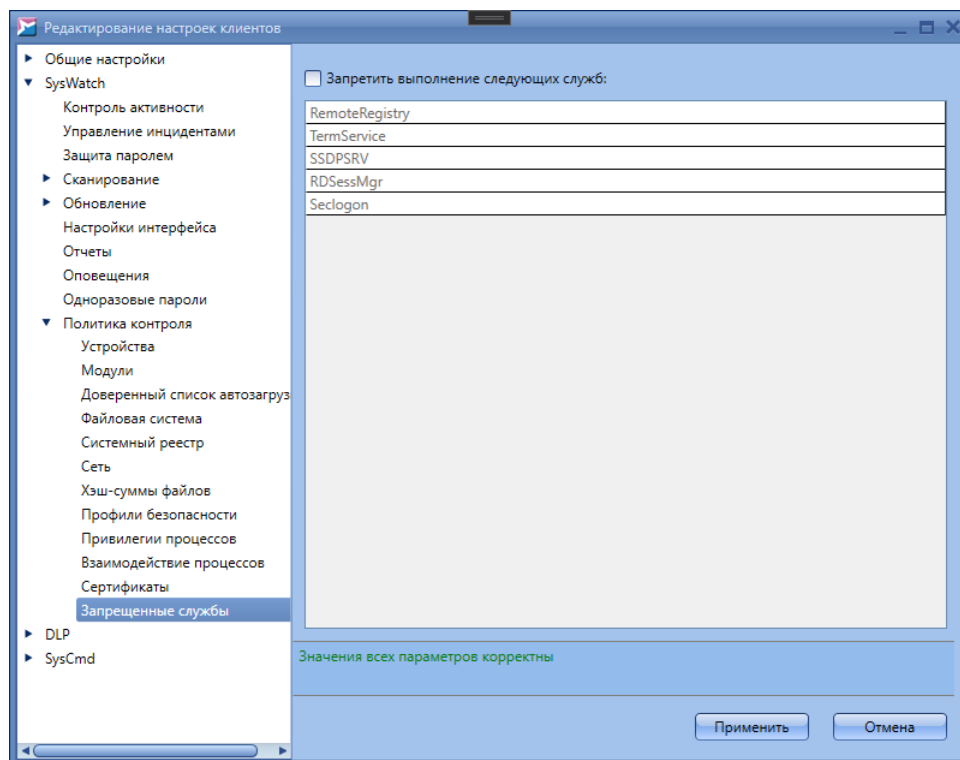


Рисунок 95. Запрещенные службы

**i** Снова включить выполнение служб, внесенных в список, можно только вручную.

### 4.6.3 Настройки SoftControl DLP Client

Данная категория настроек включает в себя конфигурацию клиентского компонента SoftControl DLP Client.

#### ▼ Сбор данных

В разделе **Сбор данных** категории **DLP** установите флажок **Собирать данные** и отметьте необходимые области собираемой информации (рис. [Настройки сбора данных](#)<sup>116</sup>):

- Время работы с приложением;**
- Использование USB-устройств;**
- Печать документов;**
- Ввод текста с клавиатуры.**

**i** Наблюдение за [файловой системой](#)<sup>(117)</sup>, [системным реестром](#)<sup>(119)</sup> и [сетевым трафиком](#)<sup>(121)</sup> активно при выставленной опции **Собирать данные** и заданном правиле (правилах) в соответствующих пунктах раздела **Наблюдение**.

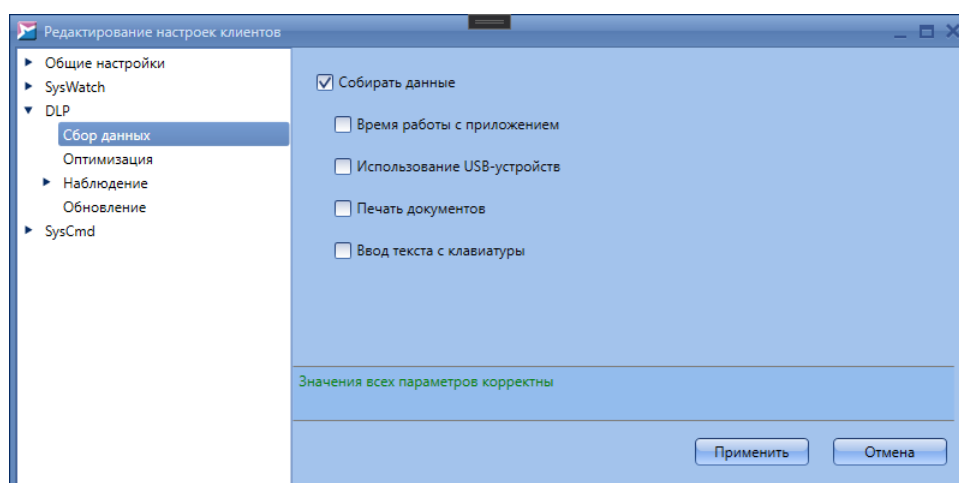


Рисунок 96. Настройки сбора данных

#### ▼ Оптимизация

В разделе **Оптимизация** категории **DLP** задаются временные параметры регистрации событий (рис. [Настройки оптимизации](#)<sup>(116)</sup>).

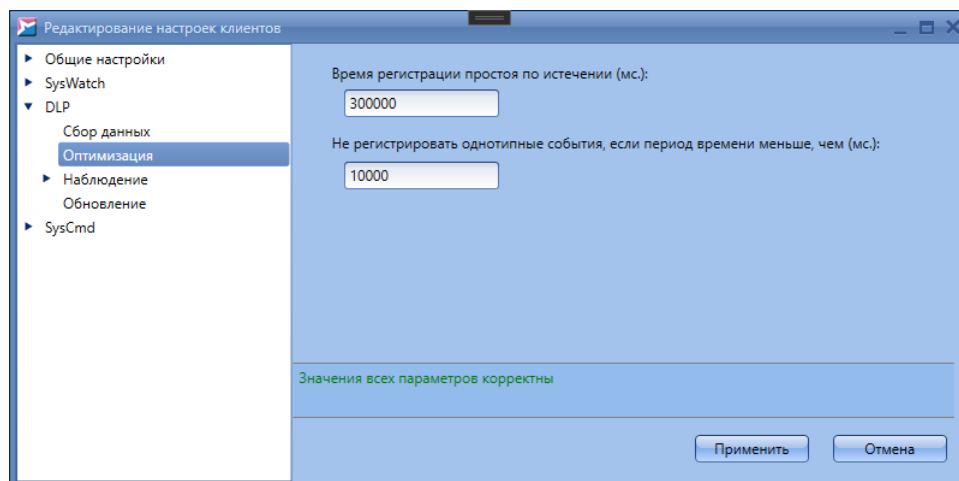


Рисунок 97. Настройки оптимизации

В соответствующих полях задайте временные интервалы **Время регистрации простоя по истечении (мс.)** и **Не регистрировать однотипные события, если период времени меньше, чем (мс.)** в миллисекундах.

Примечание: опция **Не регистрировать однотипные события, если промежуток времени меньше, чем (мс.)** применяется только при наблюдении за ресурсами

файловой системы. Опция **Время регистрации простоя по истечении (мс)** работает при включенной опции **Время работы с приложением** (см. рис. [Настройки сбора данных](#)<sup>(116)</sup>) и учитывает время простоя активного приложения, когда пользователь не нажимает на кнопки и не двигает мышью в течение указанного времени.

#### ▼ Наблюдение: Файловая система

В разделе **Наблюдение** → **Файловая система** категории **DLP** осуществляется выбор объектов файловой системы для наблюдения (рис. [Настройки наблюдения за файловой системой](#)<sup>(118)</sup>).

Чтобы добавить объект для наблюдения, нажмите на кнопку **+** (**Добавить**) и введите полный путь до него в появившемся окне (рис. [Объект наблюдения](#)<sup>(118)</sup>).

Вы можете использовать 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.



Например, чтобы установить наблюдение за каталогом и всеми вложенными объектами, добавьте символы **###** в конец строки. Нажмите на кнопку **ОК** для добавления указанного объекта в список.

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.

Чтобы изменить путь к объекту, выберите его в списке и нажмите на кнопку  (**Изменить**). Для удаления объекта из под наблюдения выберите его и нажмите на кнопку  (**Удалить**).

Для каждого объекта возможен выбор следующих операций, которые должны быть зарегистрированы в отчетах:

- Чтение;
- Запись;
- Удаление;
- Переименование;
- Изменение.

 В случае переименования объекта на клиентском хосте дальнейшее наблюдение за ним не производится.

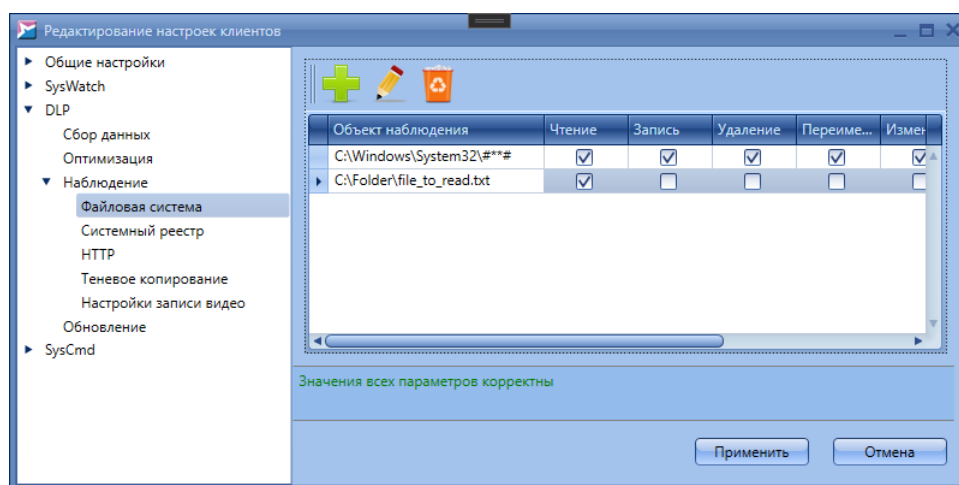


Рисунок 98. Настройки наблюдения за файловой системой

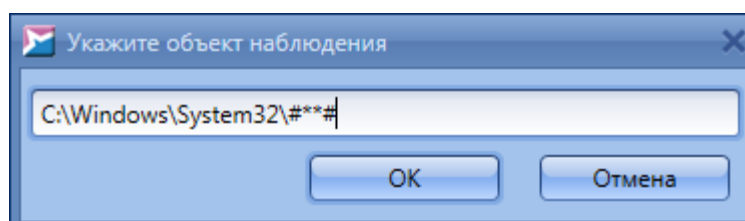


Рисунок 99. Объект наблюдения

Операция **Запись** регистрируется при открытии на запись файла, который еще не существует. Если файл уже существовал, то при открытии его на запись

регистрируется операция **Изменение**.

При установке опции **Теневая копия** будет осуществляться сохранение резервной копии наблюдаемого объекта перед его модификацией, в случае включенной глобальной опции [теневого копирования](#)<sup>(122)</sup> и выставленной галочке в полях **Удаление** или **Изменение**. При установке опции **Запись видео** будет производиться сохранение снимков экрана клиентского хоста с [заданными параметрами](#)<sup>(122)</sup> в момент возникновения наблюдаемого события.

#### ▼ Наблюдение: Системный реестр

В разделе **Наблюдение** → **Системный реестр** категории **DLP** осуществляется выбор объектов системного реестра для наблюдения (рис. [Настройки наблюдения за системным реестром](#)<sup>(119)</sup>).

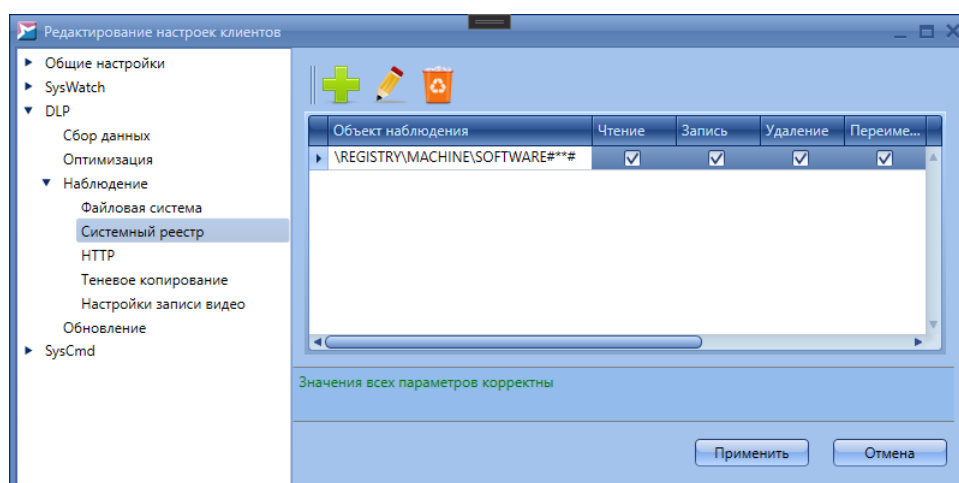


Рисунок 100. Настройки наблюдения за системным реестром

Чтобы добавить объект для наблюдения, нажмите на кнопку **+** (**Добавить**) и введите полный путь до него в появившемся окне (рис. [Объект наблюдения](#)<sup>(120)</sup>), при этом корневые разделы реестра в задаваемом пути должны быть указаны следующим образом:

- `\REGISTRY\MACHINE\SOFTWARE\CLASSES\` – раздел HKEY\_CLASSES\_ROOT;
- `\REGISTRY\MACHINE\` – раздел HKEY\_LOCAL\_MACHINE;
- `\REGISTRY\USER\<SID>\` – раздел HKEY\_CURRENT\_USER для пользователя с указанным идентификатором безопасности (<SID>);
- `\REGISTRY\USER\` – раздел HKEY\_USERS.

Вы можете использовать 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.

Например, чтобы установить наблюдение за ключом реестра и всеми вложенными объектами, добавьте символы **###** в конец строки. Нажмите на кнопку **ОК** для добавления указанного объекта в список.

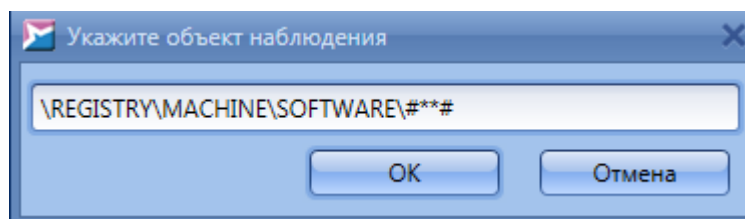





Рисунок 101. Объект наблюдения

Чтобы изменить путь к объекту, выберите его в списке и нажмите на кнопку  (**Изменить**). Для удаления объекта из под наблюдения выберите его и нажмите на кнопку  (**Удалить**).

Для каждого объекта возможен выбор следующих операций, которые должны быть зарегистрированы в отчетах:

- Чтение;**
- Запись;**
- Удаление;**
- Переименование.**

---

 В случае переименования объекта на клиентском хосте дальнейшее наблюдение за ним не производится.

---

При установке опции **Теневая копия** будет осуществляться сохранение резервной копии наблюдаемого объекта перед его модификацией, в случае включенной глобальной опции [теневого копирования](#)<sup>(122)</sup> и выставленной галочке в полях **Удаление** или **Запись**. При установке опции **Запись видео** будет производиться сохранение снимков экрана клиентского хоста с [заданными параметрами](#)<sup>(122)</sup> в



момент возникновения наблюдаемого события.

#### ▼ Наблюдение: HTTP-трафик

В разделе **Наблюдение** → **HTTP** категории **DLP** осуществляется задание наблюдаемых данных в сетевом трафике (рис. [Настройки наблюдения за сетевым трафиком](#)<sup>(121)</sup>).

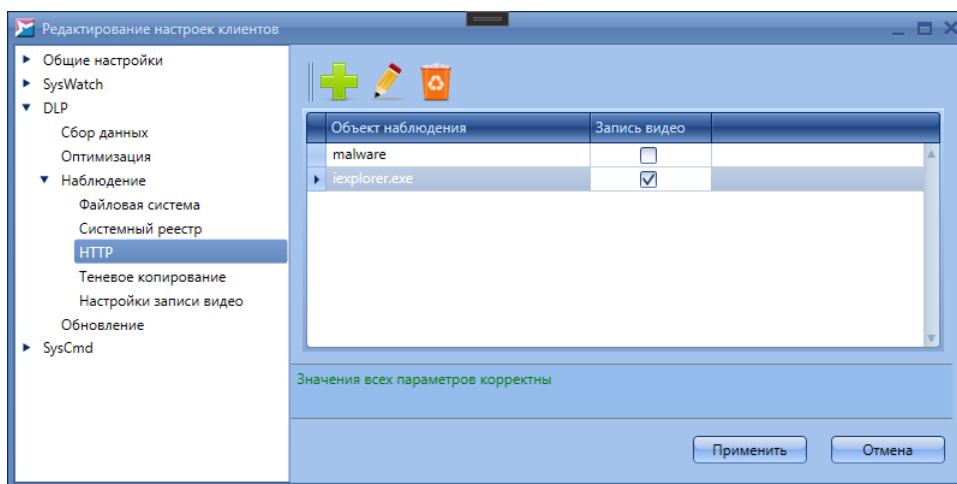


Рисунок 102. Настройки наблюдения за сетевым трафиком

Чтобы добавить данные для наблюдения, нажмите на кнопку **+** (**Добавить**) и введите строку в появившемся окне (рис. [Объект наблюдения](#)<sup>(121)</sup>). Наличие указанного текста будет отслеживаться при передаче данных по протоколу HTTP. В том числе это могут быть запросы пользователя в поисковых системах через интернет-браузер или имя файла, передаваемого по сети. Нажмите на кнопку **OK** для добавления строки в список.

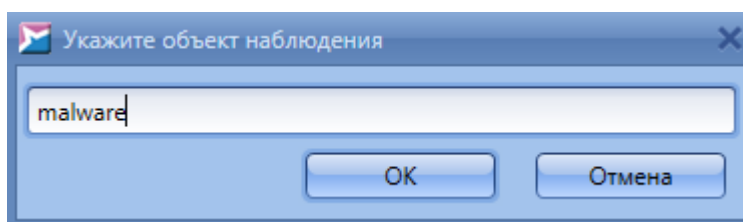


Рисунок 103. Объект наблюдения

Чтобы изменить отслеживаемый текст, выберите строку в списке и нажмите на кнопку **✎** (**Изменить**). Для удаления текста из под наблюдения выберите строку в списке и нажмите на кнопку **🗑** (**Удалить**).

При установке опции **Запись видео** будет производиться сохранение снимков экрана клиентского хоста с [заданными параметрами](#)<sup>(122)</sup> в момент возникновения наблюдаемого события.

#### ▼ Наблюдение: Теневое копирование

В разделе **Наблюдение** → **Теневое копирование** категории **DLP** осуществляется настройка сохранения теневых копий наблюдаемых объектов (рис. [Настройки теневого копирования](#)<sup>(122)</sup>).

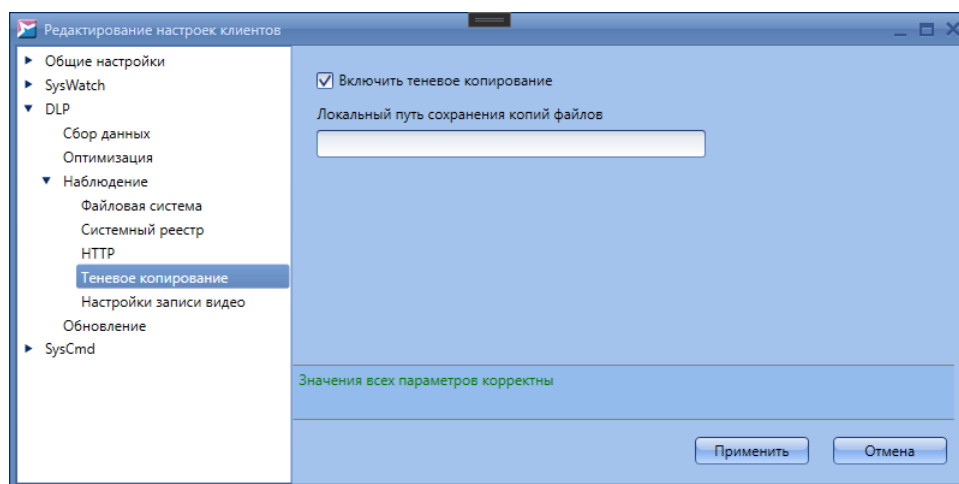


Рисунок 104. Настройки теневого копирования

Установите флажок **Включить теневое копирование** для включения функции сохранения резервных копий наблюдаемых объектов [файловой системы](#)<sup>(117)</sup> и [системного реестра](#)<sup>(119)</sup> в случае их изменения. Индивидуальная настройка по включению данной опции для отдельных объектов задается в свойствах наблюдения. Теневые копии объектов передаются на сервер и доступны через консоль управления. Они также сохраняются локально на клиентских хостах с установленным SoftControl DLP Client по пути, указанному в поле **Локальный путь сохранения копий файлов** или в следующий каталог по умолчанию, если путь не указан:

<каталог установки SoftControl DLP Client>\Backups

#### ▼ Наблюдение: Настройки записи видео

В разделе **Наблюдение** → **Настройки записи видео** категории **DLP** осуществляется настройка сохранения снимков экрана при возникновении наблюдаемых событий (рис. [Настройки записи видео](#)<sup>(122)</sup>).

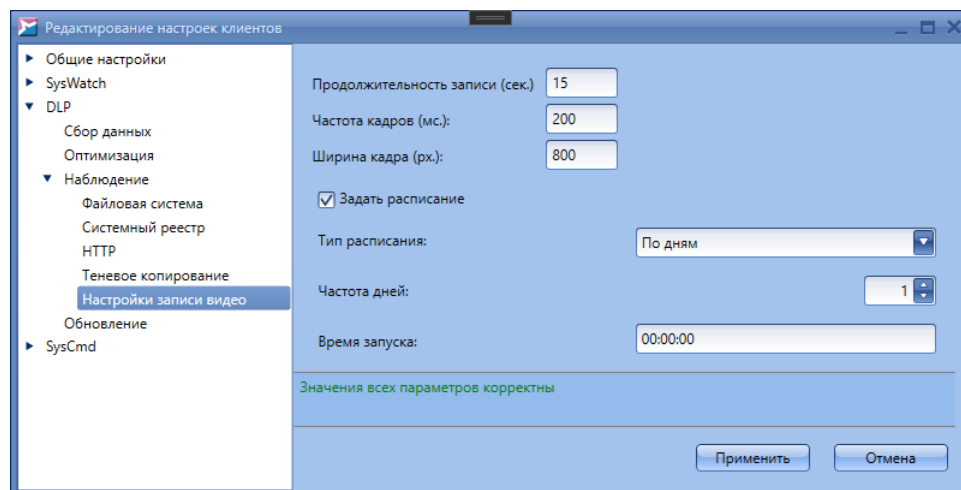


Рисунок 105. Настройки записи видео

Задайте следующие параметры записи:

- **Продолжительность записи** – длительность сохранения снимков экрана, начиная с момента возникновения события (диапазон значений: 5-60 с);
- **Частота кадров** – временной интервал между сохранением снимков экрана (диапазон значений: 50-500 мс);
- **Ширина кадра** – ширина снимка экрана в пикселах (диапазон значений: 0-1920).

Чтобы начать запись видео в режиме реального времени, щелкните правой кнопкой мыши по требуемому клиентскому приложению SoftControl DLP Client на вкладке [Клиенты](#)<sup>(46)</sup> и в контекстном меню выберите команду **Начать запись видео**.

Вы можете включить запись видео по расписанию, выставив галочку **Задать расписание**. В этом случае задайте следующие параметры записи:

- **Тип расписания** – по дням или по часам;
- **Частота дней/Частота часов** – периодичность, с которой будет выполняться задача;
- **Время запуска** – время начала выполнения задачи в формате *чч:мм:сс*.

#### ▼ Настройки обновления

В разделе **Обновление** категории **DLP** можно установить расписание обновления,

для этого установите флажок **Задать расписание** и настройте параметры (рис. [Настройки расписания обновления](#)<sup>124</sup>).

Выберите тип расписания – **По дням** или **По часам**, в счетчике **Частота дней/Частота часов** укажите периодичность, с которой будет выполняться задача, а в поле **Время запуска** – время начала выполнения задачи в формате *чч:мм:сс*.

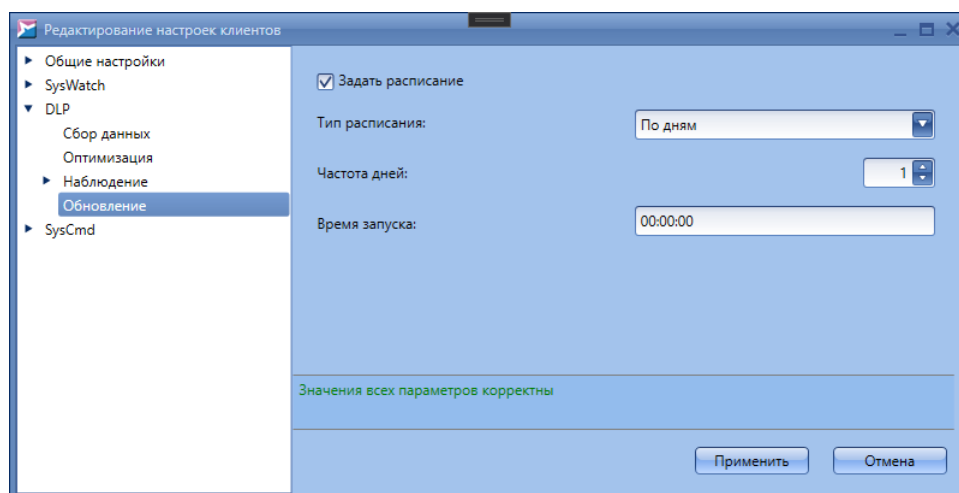


Рисунок 106. Настройки расписания обновления

#### 4.6.4 Настройки SoftControl SysCmd

Данная категория настроек включает в себя конфигурацию клиентского компонента SoftControl SysCmd.

##### ▼ Настройки обновления

В разделе **Обновление** категории **SysCmd** можно установить расписание обновления, для этого установите флажок **Задать расписание** и настройте параметры (рис. [Настройки расписания обновления](#)<sup>124</sup>).

Выберите тип расписания – **По дням** или **По часам**, в счетчике **Частота дней/Частота часов** укажите периодичность, с которой будет выполняться задача, а в поле **Время запуска** – время начала выполнения задачи в формате *чч:мм:сс*.

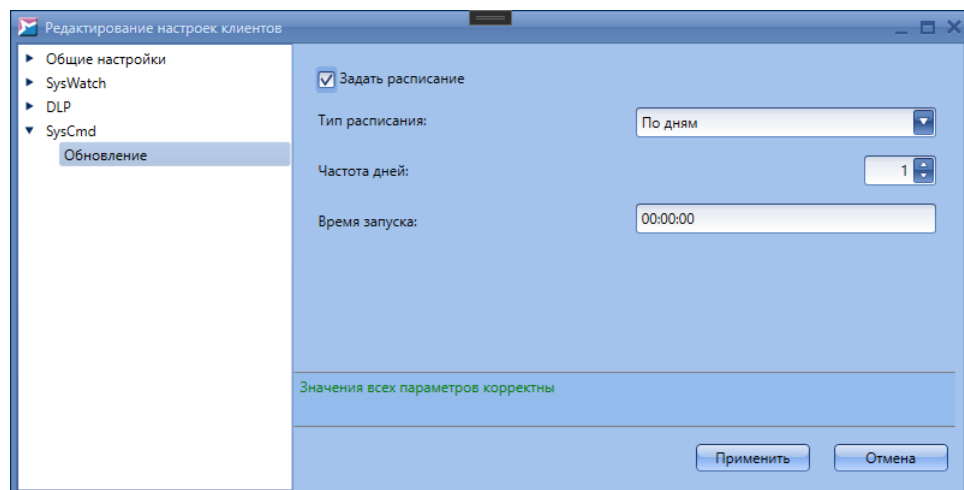


Рисунок 107. Настройки расписания обновления

## 4.7 Профили безопасности

Вкладка **Профили безопасности** предназначена для работы с наборами параметров безопасности (профилями), включающих в себя правила для файловой системы, системного реестра, сети и модулей. Профили объединяют различные правила контроля активности в логические группы. Созданные профили сохраняются в базе данных SoftControl Service Center; впоследствии их можно использовать в [настройках клиентских приложений](#)<sup>105</sup>.

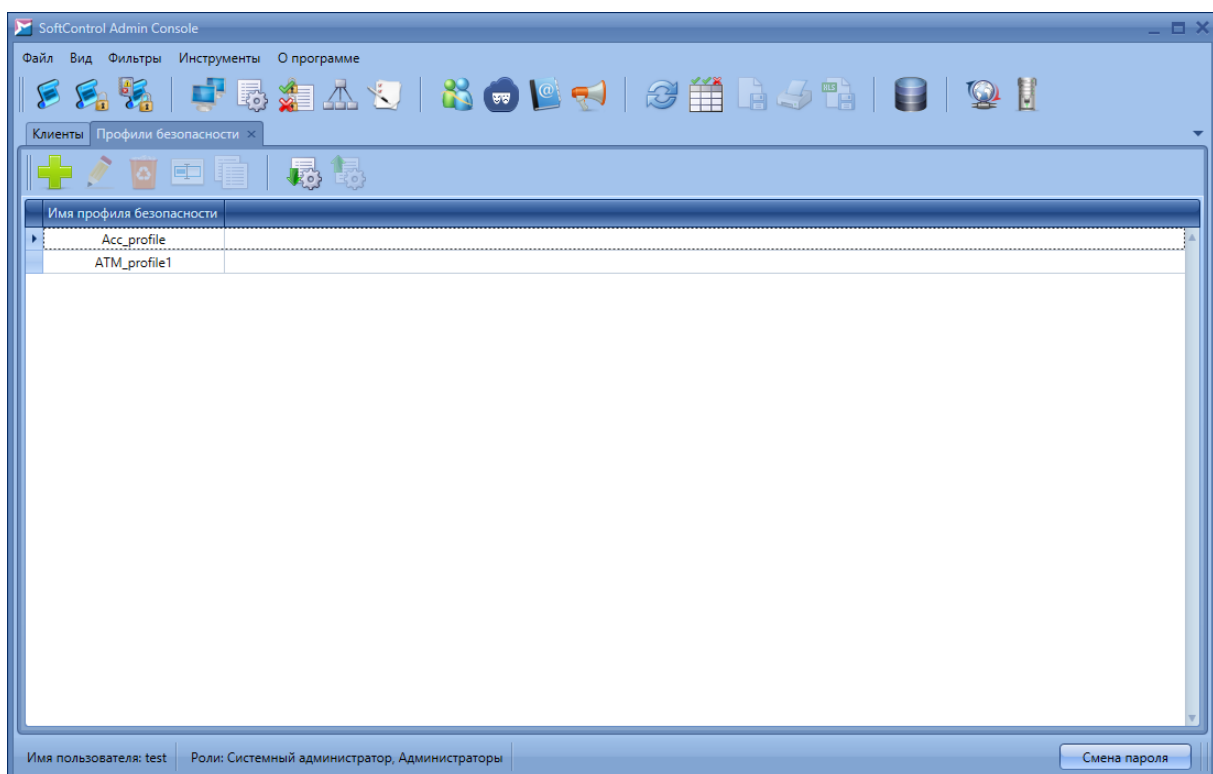









Рисунок 108. Вкладка «Профили безопасности»


Основные операции с профилями осуществляются с помощью графических кнопок вкладки, предназначение которых приведено в табл. 16.

Таблица 16. Элементы управления раздела «Профили безопасности»

Кнопка	Название	Описание
	Добавить	Создание нового профиля безопасности.
	Изменить	Редактирование выбранного профиля.
	Удалить	Удаление выбранного профиля.
	Переименовать	Переименование выбранного профиля.
	Скопировать	Сохранение выбранного профиля под другим именем.
	Импорт	Импортирование профиля из XML-файла.
	Экспорт	Экспортирование выбранного профиля в XML-файл.


Основные действия, выполняемые на данной вкладке:

#### ▼ Создание профиля


Чтобы создать профиль безопасности, нажмите на кнопку  (**Добавить**) и укажите имя профиля. В появившемся окне **Данные профиля безопасности: <имя\_профиля>** задайте правила для файловой системы, системного реестра, сети и модулей.

Подробную информацию о добавлении правил контроля активности см. в соответствующих пунктах раздела **Настройки SoftControl SysWatch** ([Политика контроля: Файловая система](#)<sup>92</sup>, [Политика контроля: Системный реестр](#)<sup>96</sup>, [Политика контроля: Сеть](#)<sup>100</sup>, [Политика контроля: Модули](#)<sup>87</sup>).

#### ▼ Редактирование профиля


Чтобы изменить профиль безопасности, выберите его и нажмите на кнопку  (**Изменить**) (рис. [Вкладка «Профили безопасности»](#)<sup>125</sup>). В появившемся окне **Данные профиля безопасности: <имя\_профиля>** отредактируйте требуемые данные.

#### ▼ Удаление профиля


Для удаления профиля выберите его, нажмите на кнопку  (**Удалить**)

(рис. [Вкладка «Профили безопасности»](#)<sup>125</sup>) и подтвердите удаление в диалоговом окне.


#### ▼ Переименование профиля

Для переименования профиля выберите его, нажмите на кнопку  (**Переименовать**) (рис. [Вкладка «Профили безопасности»](#)<sup>125</sup>) и укажите новое название в появившемся окне.


#### ▼ Копирование профиля

Для создания копии профиля выберите его, нажмите на кнопку  (**Скопировать**) (рис. [Вкладка «Профили безопасности»](#)<sup>125</sup>) и укажите название нового профиля в появившемся окне.

#### ▼ Импорт профиля

Чтобы загрузить профиль безопасности из XML-файла, нажмите на кнопку  (**Импорт**) (рис. [Вкладка «Профили безопасности»](#)<sup>125</sup>). В окне выбора файла укажите имя XML-файла и нажмите на кнопку **ОК**.

#### ▼ Экспортирование профиля

Чтобы сохранить профиль безопасности в XML-файл, нажмите на кнопку  (**Экспорт**) (рис. [Вкладка «Профили безопасности»](#)<sup>125</sup>), затем в стандартном окне выбора файла укажите имя и путь к XML-файлу.



## 4.8 Задачи


Вкладка **Задачи** позволяет создавать задачи для клиентских приложений и отслеживать детали их выполнения (рис. [Вкладка «Задачи»](#)<sup>128</sup>).

На вкладке представлен список всех задач и их параметры.

Основные операции с задачами осуществляются с помощью графических кнопок вкладки, предназначение которых приведено в табл. 17.

Таблица 17. Элементы управления вкладки «Задачи»

Кнопка	Название	Описание
	Добавить	Создание задачи для клиентских компонентов.
	Подробная информация	Просмотр отчета о выполнении выбранной задачи.

Кнопка	Название	Описание
	Отменить	Отмена задачи, находящейся в статусе <b>ожидание</b> .

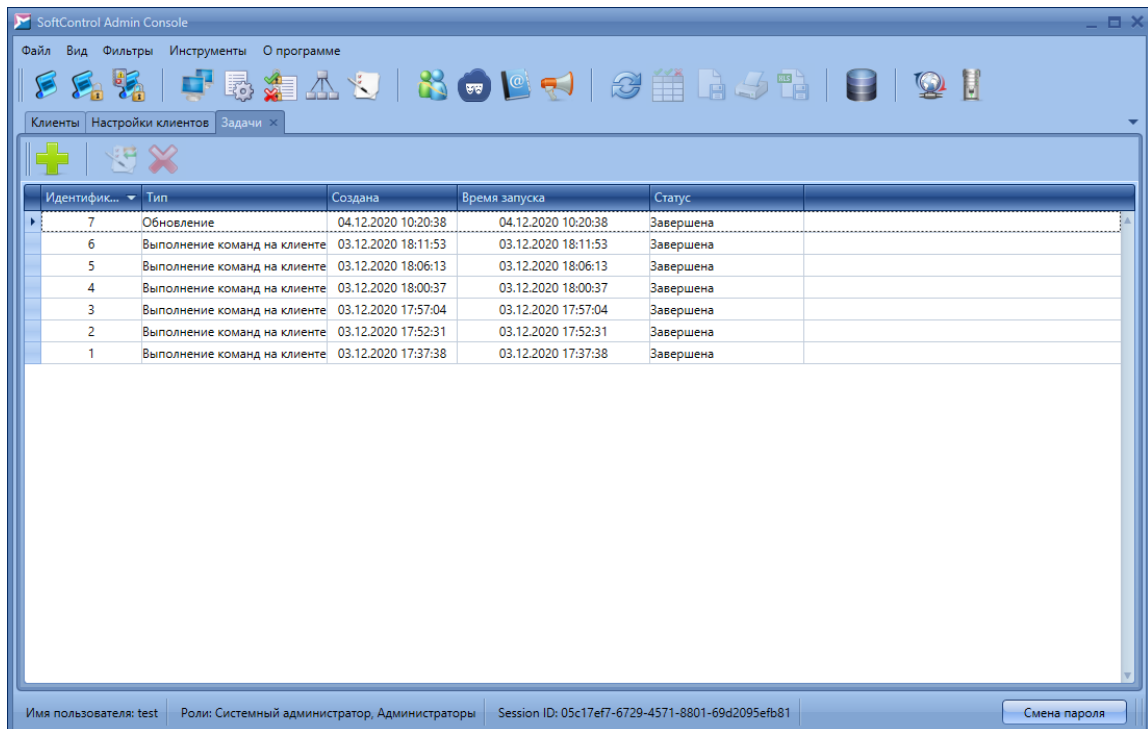


Рисунок 109. Вкладка «Задачи»

Перечень полей вкладки приведен в табл. 18.

Таблица 18. Поля вкладки «Задачи»

Поле	Описание
Идентификатор	Порядковый номер задачи.
Тип задачи	Тип задачи: <ul style="list-style-type: none"> <li>• сканирование;</li> <li>• сбор профиля;</li> <li>• обновление;</li> <li>• выполнение команд на клиенте.</li> </ul>
Создана	Дата и время создания задачи.
Время запуска	Дата и время запуска задачи.
Статус	Статус завершения задачи: <ul style="list-style-type: none"> <li>• <b>ожидание</b> – выполнение задачи не начал ни один клиентский компонент;</li> <li>• <b>отменена</b> – задача была отменена до начала выполнения;</li> <li>• <b>выполняется</b> – выполнение задачи начато как минимум одним из клиентских компонентов;</li> <li>• <b>завершена</b> – задача выполнена всеми клиентскими компонентами.</li> </ul>

Основные действия, выполняемые на данной вкладке:



#### ▼ Создание задачи

Чтобы добавить новую задачу, нажмите на кнопку **Создать** (рис. [Вкладка «Задачи»](#)<sup>128</sup>). В окне **Новая задача** задайте параметры задачи в зависимости от ее типа (см. рисунки, начиная с [Шаг «Тип задачи»](#)<sup>131</sup> и до [Шаг «Клиенты»](#)<sup>135</sup> в разделе [Обновление](#)<sup>134</sup>):

- [сбор профиля](#)<sup>131</sup>;
- [антивирусное сканирование](#)<sup>132</sup>;
- [обновление](#)<sup>134</sup>;
- [выполнение команд на клиенте](#)<sup>136</sup>.

#### ▼ Просмотр подробностей выполнения задачи

Чтобы просмотреть подробности выполнения задачи, выберите ее и выполните одно из следующих действий:

- нажмите на кнопку **Подробная информация** в группе кнопок вкладки (рис. [Вкладка «Задачи»](#)<sup>128</sup>);
- дважды нажмите левой кнопки мыши на задаче.

В появившейся дополнительной вкладке **Задача: подробно** приведена детальная информация по задаче и ход выполнения для каждого клиентского компонента в отдельности (рис. [Подробности выполнения задачи](#)<sup>129</sup>).

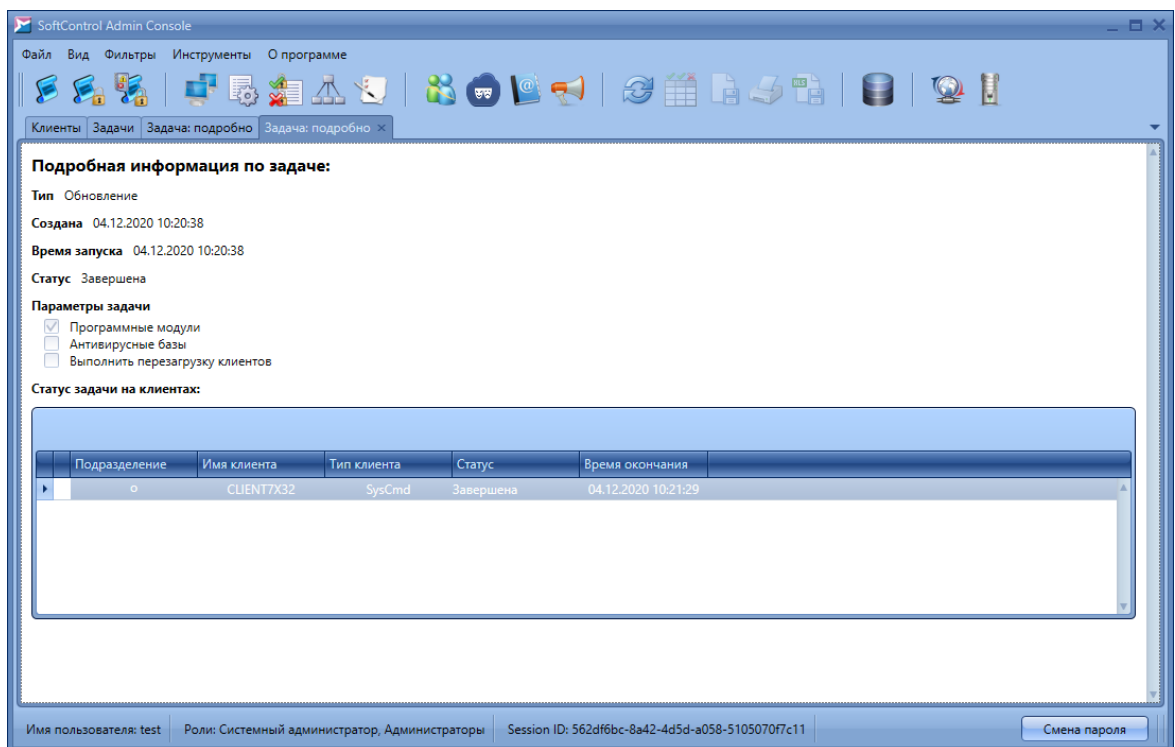


Рисунок 110. Подробности выполнения задачи

Помимо основной информации (табл. 18) и параметров задачи, на вкладке отображается дополнительная таблица **Статус задачи на клиентах**, описание полей которой дано в табл. 19.

Таблица 19. Поля таблицы «Статус задачи на клиентах»

Поле	Описание
Подразделение	Подразделение, к которому относится клиентский компонент.
Имя клиента	Имя клиентского хоста.
Статус	Статус завершения задачи для данного клиентского компонента: <ul style="list-style-type: none"> <li>• <b>ожидание</b> – выполнение задачи не начато;</li> <li>• <b>запуск</b> – клиентскому компоненту успешно отправлена команда на запуск задачи;</li> <li>• <b>ошибка запуска</b> – клиентский компонент не смог произвести запуск задачи;</li> <li>• <b>выполняется</b> – задача находится в процессе выполнения клиентским компонентом;</li> <li>• <b>ошибка выполнения</b> – в процессе выполнения задачи возникла ошибка;</li> <li>• <b>отменена</b> – задача была отменена;</li> <li>• <b>завершена</b> – выполнение задачи завершено;</li> <li>• <b>ошибка завершения</b> – при завершении задачи возникла ошибка.</li> </ul>
Время окончания	Время завершения задачи на данном клиентском хосте.

Чтобы просмотреть отчеты непосредственно по выполненным операциям, перейдите на вкладку **Лог** и примените [фильтры](#)<sup>160</sup> для соответствующих типов операций.

**Подробная информация** для задачи **Выполнение команд на клиенте** так же включает в себя результаты выполнения команд. Просмотр результатов выполнения описан в разделе [Результаты выполнения команд](#)<sup>141</sup>.

### 4.8.1 Сбор профиля

- 1) На шаге **Тип задачи** выберите **Сбор профиля** в выпадающем списке и нажмите на кнопку **Вперед** (рис. [Шаг «Тип задачи»](#)<sup>131</sup>).

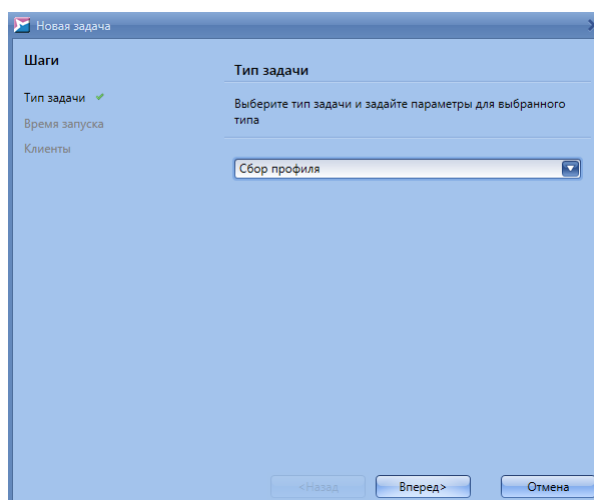


Рисунок 111. Шаг «Тип задачи»

- 2) На шаге **Время запуска** выберите опцию **Сейчас** для немедленного запуска задачи после ее добавления, либо выберите опцию **Указать время** и определите дату и время запуска (рис. [Шаг «Время запуска»](#)<sup>131</sup>). Нажмите на кнопку **Вперед** для продолжения.

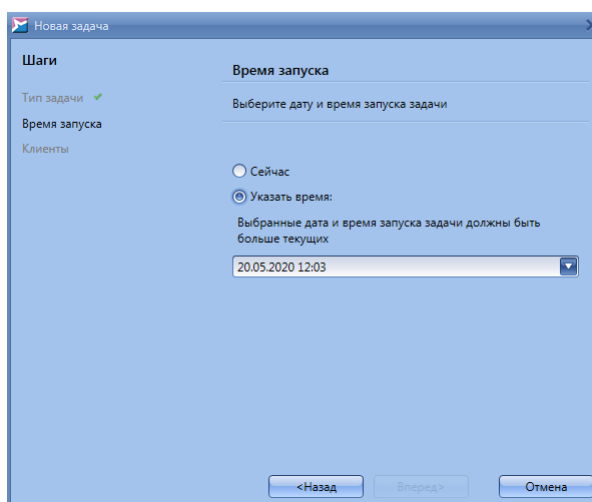


Рисунок 112. Шаг «Время запуска»

3) На шаге **Клиенты** отметьте клиентские компоненты, для которых необходимо создать задачу (рис. [Шаг «Клиенты»](#)<sup>(132)</sup>). При выборе типа клиента **SysWatch** задача будет назначена всем клиентским компонентам, при выборе подразделения – всем клиентским компонентам подразделения. Нажмите на кнопку **Готово**, чтобы создать задачу, или на кнопку **Назад**, если требуется изменить параметры задачи.

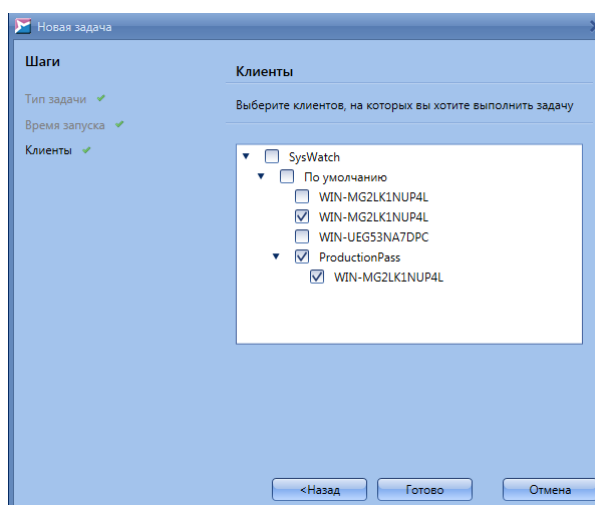


Рисунок 113. Шаг «Клиенты»

## 4.8.2 Антивирусное сканирование

1) На шаге **Тип задачи** выберите **Сканирование** в выпадающем списке и отметьте области клиентского хоста для антивирусной проверки (рис. [Шаг «Тип задачи»](#)<sup>(133)</sup>):

- Сканирование памяти;
- Сканирование загрузочных секторов;

- Сканирование всех жестких дисков;
- Сканирование всех съемных носителей.

Нажмите на кнопку **Вперед** для продолжения.

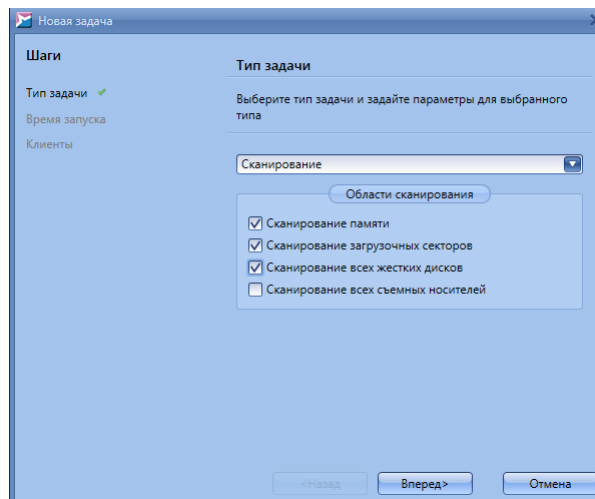


Рисунок 114. Шаг «Тип задачи»

2) На шаге **Время запуска** выберите опцию **Сейчас** для немедленного запуска задачи после ее добавления, либо выберите опцию **Указать время** и определите дату и время запуска (рис. [Шаг «Время запуска»](#)<sup>133</sup>). Нажмите на кнопку **Вперед** для продолжения.

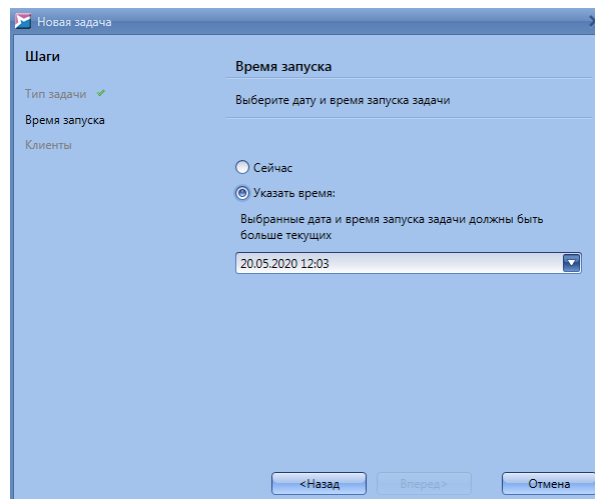


Рисунок 115. Шаг «Время запуска»

3) На шаге **Клиенты** отметьте клиентские компоненты, для которых необходимо создать задачу (рис. [Шаг «Клиенты»](#)<sup>133</sup>).

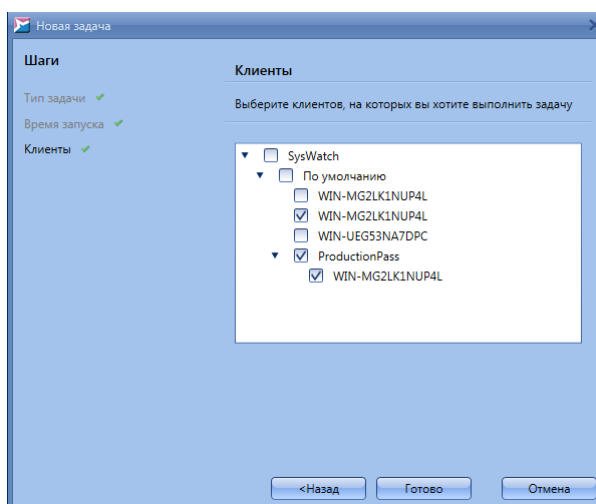


Рисунок 116. Шаг «Клиенты»

При выборе типа клиента **SysWatch** задача будет назначена всем клиентским компонентам, при выборе подразделения – всем клиентским компонентам подразделения. Нажмите на кнопку **Готово**, чтобы создать задачу, или на кнопку **Назад**, если требуется изменить параметры задачи.

### 4.8.3 Обновление

1) На шаге **Тип задачи** выберите **Обновление** в выпадающем списке и отметьте необходимые компоненты для обновления и параметры задачи (рис. [Шаг «Тип задачи»](#)

<sup>134</sup>):

- Программные модули** – обновление программных модулей компонентов типа SysWatch, DLP и SysCmd.
- Антивирусные базы** – обновление антивирусных баз компонентов типа SysWatch.
- Выполнить перезагрузку клиентов** – перезагрузка клиентских хостов по окончании обновления. Если данная опция не выбрана, то для завершения обновления программных модулей перезагрузку необходимо выполнить локально вручную на клиентском хосте, что отображается в статусе компонента на вкладке [Клиенты](#)<sup>45</sup> и событиях обновления в [отчетах](#)<sup>143</sup>. Модулю SysCmd не требуется перезагрузка компьютера после обновления, поэтому этот параметр игнорируется в процессе обновления SysCmd.

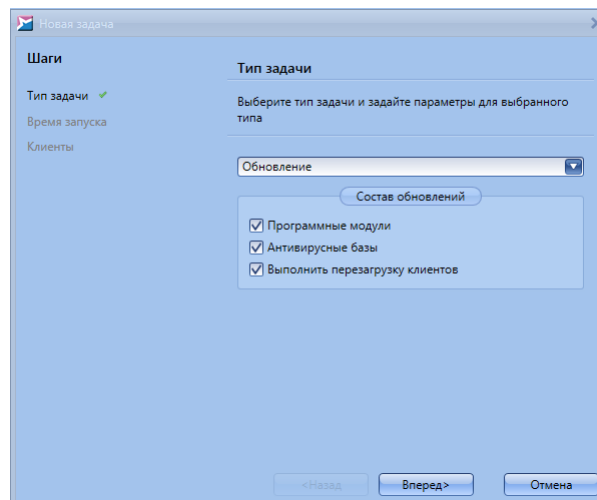


Рисунок 117. Шаг «Тип задачи»

Нажмите на кнопку **Вперед** для продолжения.

- 2) На шаге **Время запуска** выберите опцию **Сейчас** для немедленного запуска задачи после ее добавления, либо выберите опцию **Указать время** и определите дату и время запуска (рис. [Шаг «Время запуска»](#)<sup>135</sup>). Нажмите на кнопку **Вперед** для продолжения.

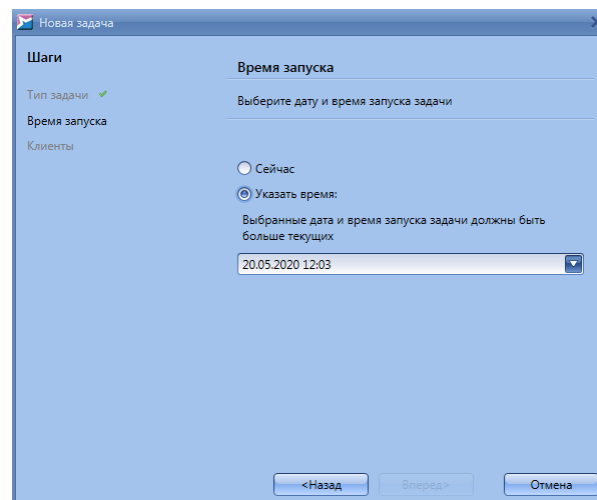


Рисунок 118. Шаг «Время запуска»

- 3) На шаге **Клиенты** отметьте клиентские компоненты, для которых необходимо создать задачу (рис. [Шаг «Клиенты»](#)<sup>135</sup>). При выборе типа клиента задача будет назначена всем клиентским компонентам данного типа, при выборе подразделения – всем клиентским компонентам подразделения. Нажмите на кнопку **Готово**, чтобы создать задачу, или на кнопку **Назад**, если требуется изменить параметры задачи.

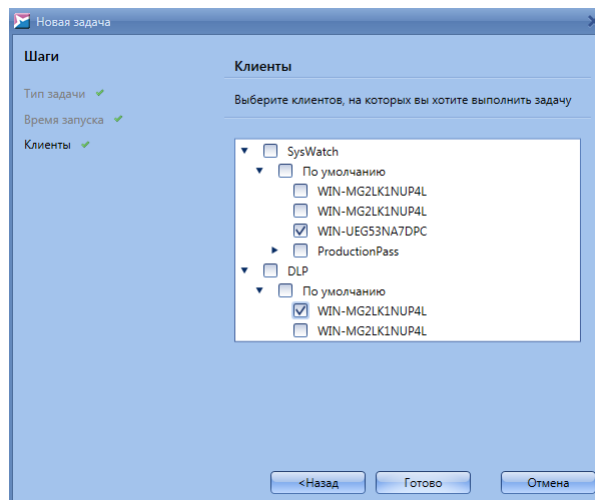


Рисунок 119. Шаг «Клиенты»

#### 4.8.4 Выполнение команд на клиенте и обмен файлами с клиентом

Задача типа **Выполнение команд на клиенте** может быть выполнена на удаленном компьютере, где установлен клиент SoftControl SysCmd. В рамках одной задачи могут быть выполнены следующие команды: передача файлов на удаленный компьютер, запуск процессов на удаленном компьютере, скачивание файлов с удаленного компьютера.

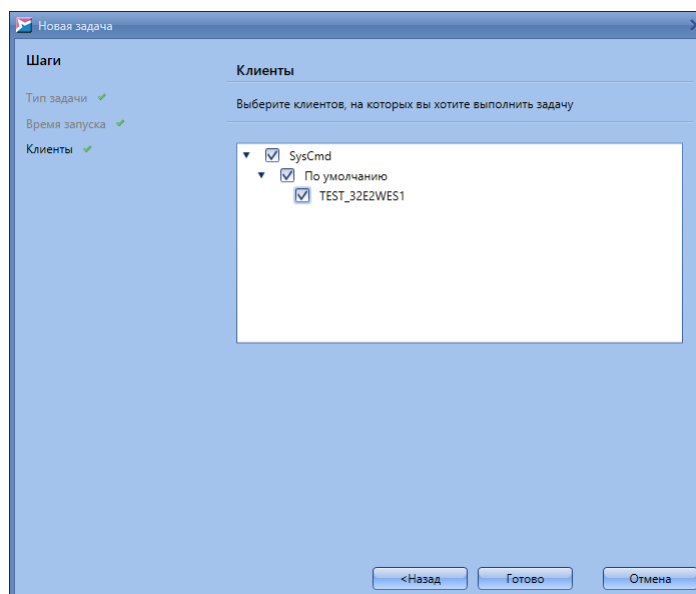


Рисунок 120. Шаг «Клиенты»



## 4.8.4.1 Создание задачи

1) На шаге **Тип задачи** выберите **Выполнение команд на клиенте** в выпадающем списке и отметьте те **команды**<sup>(139)</sup>, которые необходимо выполнить (рис. [Шаг «Тип задачи»](#)<sup>(136)</sup>):

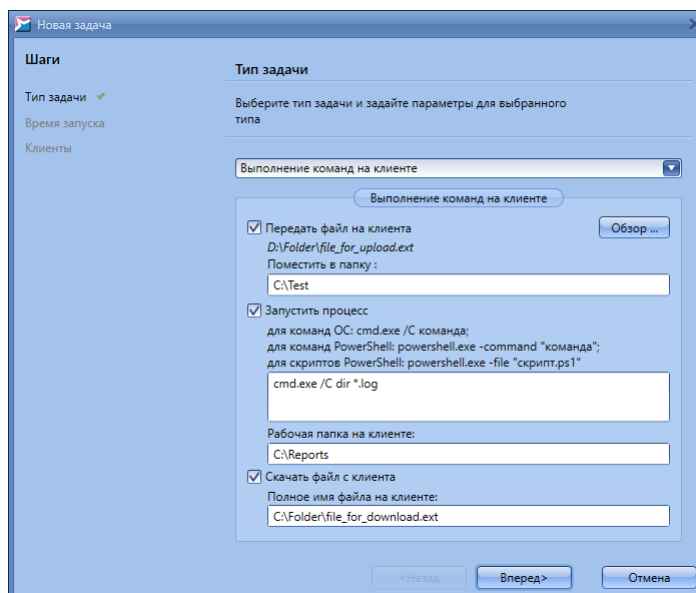


Рисунок 121. Шаг «Тип задачи»

❑ **Передать файл на клиент** – скопировать файл с локального компьютера, где в данный момент запущена консоль управления SoftControl Admin Console, на удаленный компьютер, где работает модуль SoftControl SysCmd.

Параметры:

Выберите файл с помощью кнопки **Обзор** и введите в поле **Поместить в папку** полный путь на удаленном компьютере куда необходимо этот файл сохранить. Оба параметра являются обязательными.

❑ **Запустить процесс** – запускает указанный в параметрах исполняемый файл.

Параметры:

Команда для запуска процесса (обязательный параметр).

**Рабочая папка на клиенте** (необязательный параметр).

В команде указывается исполняемый файл для запуска с необходимыми параметрами. Можно указать рабочую папку, которая будет установлена как текущая для процесса.

❑ **Скачать файл с клиента** – скопировать файл с удаленного компьютера, где работает модуль SoftControl SysCmd, на сервер SoftControl Server. Затем этот файл

можно скачать на локальный компьютер с помощью консоли управления SoftControl Admin Console.

Параметры:

Имя скачиваемого файла с полным путем в файловой системе клиента (обязательный параметр).

После заполнения параметров команд нажмите на кнопку **Вперед** для продолжения.

- 2) На шаге **Время запуска** выберите опцию **Сейчас** для немедленного запуска задачи после ее добавления, либо выберите опцию **Указать время** и определите дату и время запуска (рис. [Шаг «Время запуска»](#)<sup>(135)</sup>). Нажмите на кнопку **Вперед** для продолжения.

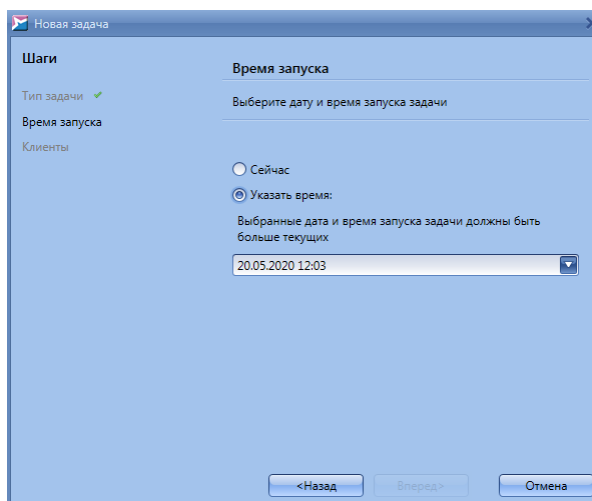


Рисунок 122. Шаг «Время запуска»

- 3) На шаге **Клиенты** отметьте клиентские компоненты, для которых необходимо создать задачу (рис. [Шаг «Клиенты»](#)<sup>(135)</sup>). При выборе типа клиента задача будет назначена всем клиентским компонентам данного типа, при выборе подразделения – всем клиентским компонентам подразделения. Нажмите на кнопку **Готово**, чтобы создать задачу, или на кнопку **Назад**, если требуется изменить параметры задачи.

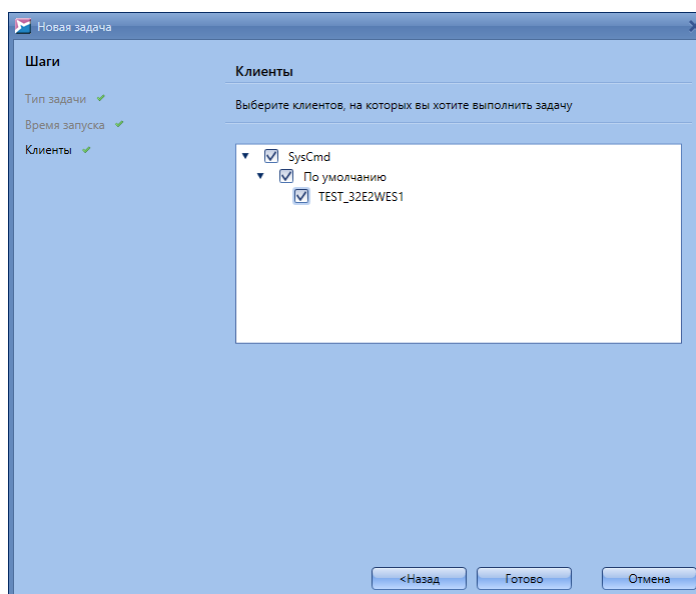


Рисунок 123. Шаг «Клиенты»

#### 4.8.4.2 Описание работы команд

В процессе выполнения задачи типа **Выполнение команд на клиенте** производятся следующие действия:

**Подготовка задачи.** Если задача содержит команду передачи файла на клиент, то сначала SoftControl Admin Console передает файл на сервер. Файл сохраняется на сервере в папке, указанной в параметре *CmdFileStoreDir* файла конфигурации сервера (C:\ProgramData\SafenSoft\Server.Config.xml), по умолчанию C:\ProgramData\SafenSoft\CmdFileStore. Если передача файла на сервер не прошла успешно, то выдается сообщение об ошибке и задача не создается. Максимальный размер файла, который можно передавать на клиент и скачивать с него, задается параметром *MaxFileSizeByte* в файле конфигурации сервера.

**Запуск задач на клиенте.** Во время очередного хартбита клиент связывается с сервером и получает список задач. Для каждой задачи создается новый поток, в котором будут выполняться команды из данной задачи. Поэтому несколько разных задач по выполнению команд могут выполняться в произвольном порядке, а команды внутри одной задачи выполняются строго в том порядке, в каком они описаны внутри задачи.

**Передача файла на клиент.** Клиент скачивает файл с сервера и сохраняет его в соответствии с заданными параметрами команды (путь, имя, времена и атрибуты файла). Если такой файл уже существует, он будет перезаписан. Если указанного в

параметрах пути не существует, будет предпринята попытка создать этот путь вне зависимости от его глубины. Информация о результате передается на сервер. После выполнения команды файл с сервера удаляется вне зависимости от успешности выполнения команды. В случае прерывания передачи файла с сервера на клиент вследствие разрыва связи или перезапуска клиента загрузка продолжится, когда связь возобновится и служба SysCmd будет работать.

**Запуск процесса.** Клиент создает процесс в соответствии с параметрами команды и подключается к его потокам stdout и errout. По окончании чтения данных из выходного потока процесса клиент отправляет его содержимое и сопутствующую информацию на сервер. Размер буфера в символах для приема выходного потока процесса задается параметром *MaxCmdOutputChars* в файле конфигурации сервера. В случае запуска процесса перезагрузки или выключения компьютера не следует заказывать немедленное действие, чтобы дать время на сохранение результата команды и отправку хартбита на сервер. Например, для команды shutdown следует использовать ключ /t. Поскольку процесс запускается в сессии, в которой работают службы и [ГИП](#)<sup>(7)</sup> не доступен, не следует запускать процессы, требующие участия пользователя как для работы, так и для своего завершения.

**Скачивание файла с клиента.** Клиент отправляет файл на сервер, и сервер сохраняет файл в папке, указанной в параметре *CmdFileStoreDir* в Server.Config.xml. Также клиент отправляет на сервер имя, время и атрибуты файла. В случае прерывания передачи файла с клиента на сервер вследствие разрыва связи или перезапуска клиента загрузка продолжится, когда связь возобновится и служба SysCmd будет работать.


**Завершение задачи.** После завершения выполнения всех команд задаче устанавливается соответствующий статус, который будет передан на сервер только при очередном хартбите. Т.е. результаты выполнения отдельных команд на сервере могут быть доступны до обновления статуса всей задачи.

Время выполнения всего набора команд в задаче можно ограничить параметром *MaxCmdExecTimeSec* в файле конфигурации сервера. При превышении этого времени команда будет прервана и ее (и всем следующим за ней командам) будет установлен статус «Превышено время ожидания». Если после перезапуска службы SysCmd или перезагрузки клиента продолжается выполнение команд в задаче, то отсчет времени начинается заново.

При выполнении команд могут возникнуть ошибки. В случае критических ошибок (отсутствие запрашиваемого или запускаемого файла, невозможность создания пути или файла) выполнение команды прекращается. В случае не критических ошибок (сетевые ошибки передачи файлов) производится повторная попытка выполнения команды до тех пор, пока она не выполнится успешно, не произойдет критическая ошибка или не будет превышено время *MaxCmdExecTimeSec*. До успешного завершения команды перехода к следующей команде не произойдет. Между выполнением команд набора выдерживается пауза 5 сек.

Перед и после выполнения каждой команды передачи файлов ее состояние сохраняется на клиенте для возобновления выполнения незавершенных команд после перезапуска службы.

#### 4.8.4.3 Результаты выполнения команд

Информация о результатах выполнения команд доступна на вкладке [Задача: подробно](#)<sup>129</sup> в таблице **Статус задачи на клиентах**. Если результаты доступны, в первом столбце появится значок , который позволяет открыть подробную информацию о результатах (рисунки [Просмотр результатов работы команд передачи файла на клиент и запуска процесса](#)<sup>142</sup> и [Просмотр результатов работы команды скачивания файла с клиента](#)<sup>143</sup>).

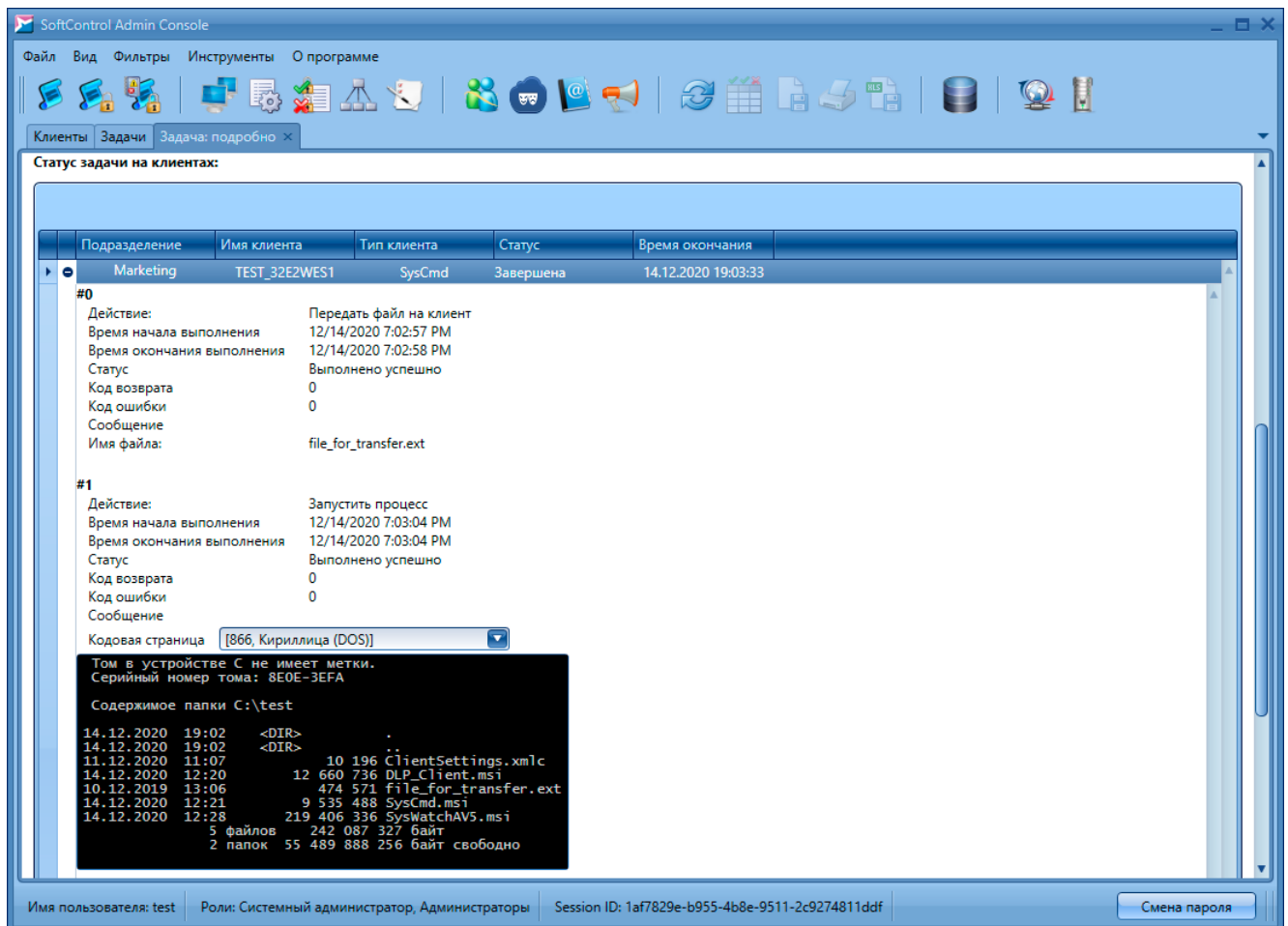


Рисунок 124. Просмотр результатов работы команд передачи файла на клиент и запуска процесса

**Статус** выполнения команды может принимать следующие значения:

- Выполнено успешно.
- Произошла ошибка.
- Превышено время ожидания.

**Код возврата** содержит код, возвращенный процессом в команде **Запуск процесса**.

Если в ходе выполнения команды произошла ошибка при вызове функций API Windows или запросе к веб-серверу, то номер ошибки будет указан в поле **Код ошибки**, и в поле **Сообщение** краткое описание случившегося.

Для команды **Запуск процесса** можно выбрать **Кодовую страницу**, в которой будет представлен вывод процесса.

Если команда **Скачать файл** с клиента выполнена успешно и файл сохранен на сервере, то воспользовавшись кнопкой **Скачать** можно получить файл с сервера, а с помощью кнопки **Удалить** с сервера удалить его.

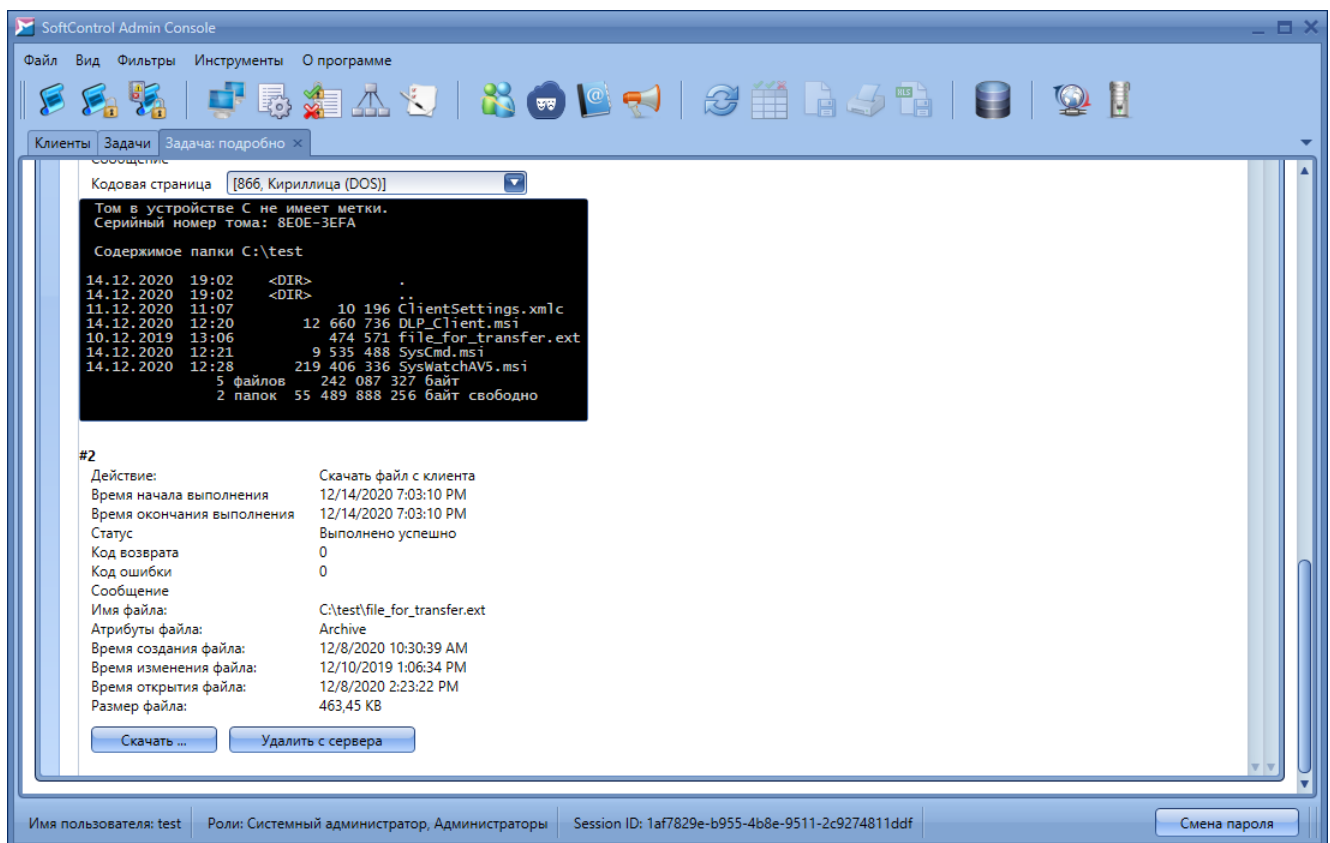


Рисунок 125. Просмотр результатов работы команды скачивания файла с клиента

## 4.9 Просмотр отчетов

Для просмотра отчетов клиентских приложений в агрегированном виде через консоль управления SoftControl Admin Console предназначена вкладка **Лог событий**. Она позволяет в реальном времени отслеживать события на нескольких клиентских хостах одновременно и производить выборку необходимых данных с помощью гибкого [механизма фильтрации](#)<sup>(159)</sup>. На вкладке администратор получает доступ к следующим данным в удобной форме:

- [Отчеты SoftControl SysWatch](#)<sup>(144)</sup>;
- [Отчеты SoftControl DLP Client](#)<sup>(151)</sup>;
- [Отчеты SoftControl SysCmd](#)<sup>(155)</sup>.

Полученные отчеты могут быть [выведены на печать или экспортированы в электронный формат](#)<sup>(167)</sup>.

Кроме того, поддерживается [резервное копирование отчетов](#)<sup>(168)</sup>.

### 4.9.1 Отчеты SoftControl SysWatch

Вкладка **Лог событий** предоставляет возможности по детальному мониторингу событий безопасности, регистрируемых SoftControl SysWatch на клиентских хостах (рис. [Вкладка «Лог событий» для компонента SoftControl SysWatch](#)<sup>144</sup>). Чтобы просмотреть все события, поступившие с клиентов SysWatch, выделите нужные клиенты и следуйте инструкции, приведенной в разделе [Клиенты](#)<sup>49</sup>.

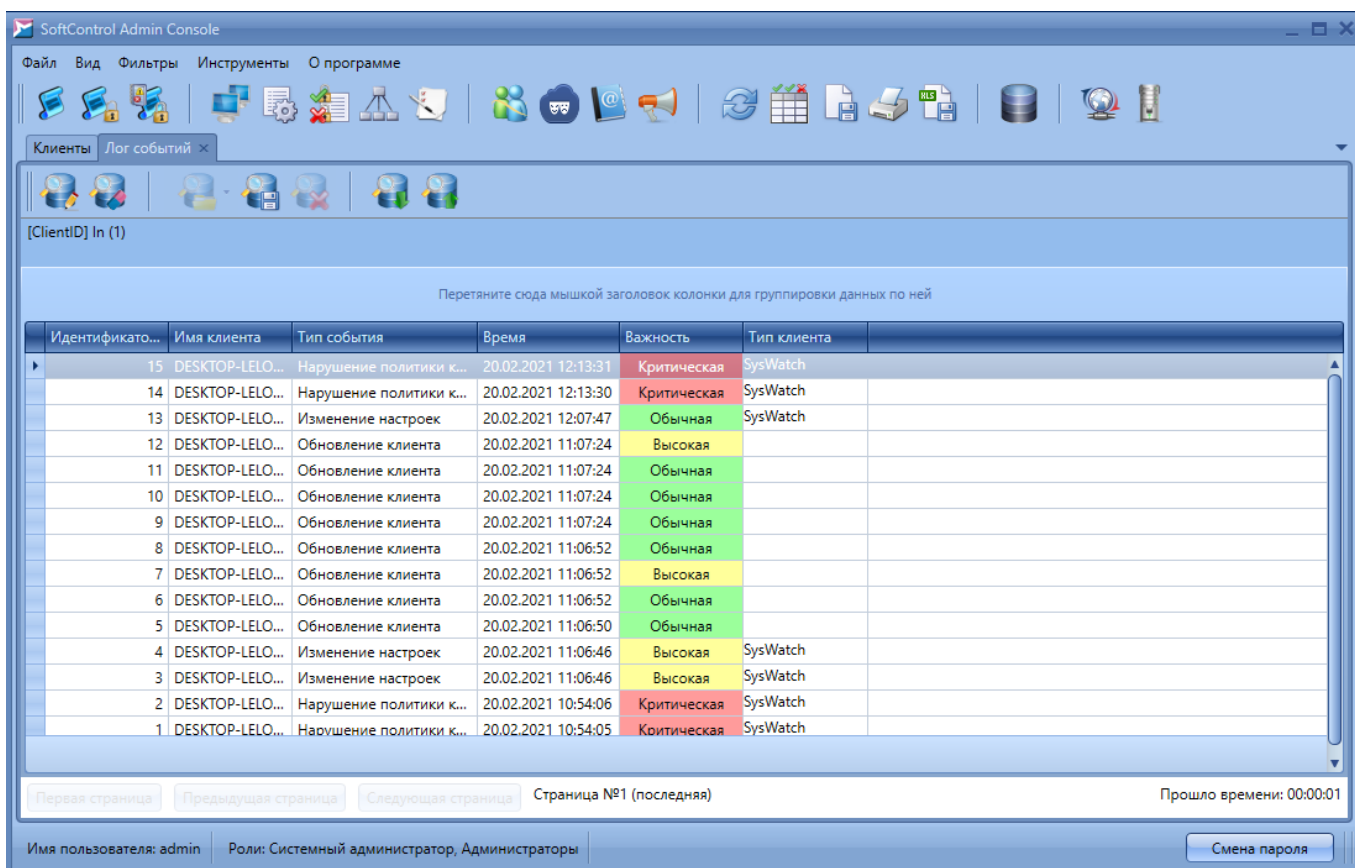


Рисунок 126. Вкладка «Лог событий» для компонента SoftControl SysWatch

Полный перечень полей вкладки **Лог событий** для компонента SoftControl SysWatch приведен в табл. 20.

Таблица 20. Поля вкладки «Лог событий» для SoftControl SysWatch

Поле	Описание
Имя	Имя клиентского хоста.
Идентификатор события	Уникальный идентификатор события. Если происходит прием события с дублированным идентификатором, дублируемая строка помечается красным цветом. В случае нарушения целостности порядка идентификаторов (разрывы в последовательности), в <a href="#">отчет серверного компонента в журнале Windows</a> <sup>199</sup> вносится соответствующее предупреждение. Исключением являются события типа <b>Статус</b> , для которых данный параметр принимает значения -1 или -2.



Поле	Описание
Уникальный ID устройства	Уникальный идентификатор клиентского хоста, который автоматически присваивается ему при первом обращении клиентского приложения SoftControl SysWatch к серверу SoftControl Server.
Тип события	Тип события безопасности (инцидента): <ul style="list-style-type: none"> <li>• нарушение политики контроля;</li> <li>• контроль активности;</li> <li>• обновление клиента;</li> <li>• запуск процесса;</li> <li>• антивирус;</li> <li>• изменение настроек;</li> <li>• статус;</li> <li>• вход пользователя;</li> <li>• выход пользователя;</li> <li>• события DeCrypt.</li> </ul>
Время	Дата и время регистрации события.
Важность	Важность (приоритет) события с точки зрения угрозы информационной безопасности клиентского хоста: <ul style="list-style-type: none"> <li>• обычная;</li> <li>• высокая;</li> <li>• критическая.</li> </ul> Каждому уровню приоритета соответствует свой цвет ячейки.
Действие	<p>Действие в случае события типа <b>нарушение политики контроля</b>:</p> <ul style="list-style-type: none"> <li>• чтение файла;</li> <li>• изменение файла;</li> <li>• переименование файла;</li> <li>• удаление файла;</li> <li>• открытие каталога;</li> <li>• удаление каталога;</li> <li>• открытие ключа реестра;</li> <li>• создание ключа реестра;</li> <li>• удаление ключа реестра;</li> <li>• изменение значения реестра;</li> <li>• удаление значения реестра;</li> <li>• загрузка DLL-модуля;</li> <li>• введен неверный пароль.</li> </ul> <p>Действие в случае события типа <b>запуск процесса</b> (данные выводятся в одну строку):</p> <ul style="list-style-type: none"> <li>• <b>Инсталлятор</b>: да/нет;</li> <li>• <b>В профиле</b>: да/нет (отсутствует, если на клиентском хосте отключен профиль системы или если в <a href="#">настройках</a> <sup>(66)</sup> в разделе <b>Контроль активности</b> снят флажок <b>Приложения</b>);</li> <li>• <b>Имеет действительную ЭЦП</b>: да/нет (только для инсталляторов);</li> <li>• <b>Белый список сертификатов включен</b>: да/нет (только для инсталляторов);</li> <li>• <b>Сертификат в белом списке</b>: да/нет (только для инсталляторов, и если включен белый список);</li> <li>• <b>Глобальный режим обновления ПО включен</b>: да/нет (только для инсталляторов);</li> </ul>

Поле	Описание
	<ul style="list-style-type: none"> <li>• <b>Был ли отслеживаемым:</b> да/нет;</li> <li>• <b>Запуск в режиме обновления ПО:</b> да/нет.</li> </ul> <p>Действие в случае события типа <b>антивирус:</b></p> <ul style="list-style-type: none"> <li>• <b>запуск сканера;</b></li> <li>• <b>запуск сбора профиля;</b></li> <li>• <b>завершение сканирования;</b></li> <li>• <b>профиль собран;</b></li> <li>• <b>сканирование объекта.</b></li> </ul> <p>Действие в случае события типа <b>обновление:</b></p> <ul style="list-style-type: none"> <li>• <b>запуск обновлений;</b></li> <li>• <b>обновление завершено.</b></li> </ul> <p>Действие в случае события типа <b>изменение настроек:</b></p> <ul style="list-style-type: none"> <li>• <b>настройки изменены локально;</b></li> <li>• <b>настройки изменены сервером.</b></li> </ul> <p>Действие в случае события типа <b>события DeCrypt:</b></p> <ul style="list-style-type: none"> <li>• <b>NOTIFY-DEV0;Загрузка, все устройства найдены;</b></li> <li>• <b>NOTIFY-PRETEST;Загрузка с незашифрованным контейнером;</b></li> <li>• <b>NOTIFY-ERROR;Ошибка при загрузке;</b></li> <li>• <b>NOTIFY-PW;Загрузка с паролем;</b></li> <li>• <b>NOTIFY-DEV1;Загрузка, одно из устройств не найдено;</b></li> <li>• <b>NOTIFY-DEV2;Загрузка, два устройства не найдены (КРИТИЧНО);</b></li> <li>• <b>NOTIFY-ACTION: DEV-GET;Запрос списка найденных устройств;</b></li> <li>• <b>NOTIFY-ACTION: DEV-CHANGE;Обновить список устройств;</b></li> <li>• <b>NOTIFY-ACTION: PW-CHANGE;Изменить пароль;</b></li> <li>• <b>NOTIFY-ACTION: DISK-ENC STARTED;Шифрование диска начато;</b></li> <li>• <b>NOTIFY-ACTION: DISK-ENC FINISHED;Шифрование диска завершено;</b></li> <li>• <b>NOTIFY-ACTION: DISK-DEC STARTED;Дешифрование диска начато;</b></li> <li>• <b>NOTIFY-ACTION: DISK-DEC FINISHED;Дешифрование диска завершено;</b></li> <li>• <b>NOTIFY-ACTION: BOOT-PREPARE;Установить системный загрузчик;</b></li> <li>• <b>NOTIFY-ACTION: BOOT-CLEAR;Удалить системный загрузчик.</b></li> </ul>
Статус действия	<p>Статус действия в случае события типа <b>антивирус:</b></p> <ul style="list-style-type: none"> <li>• <b>сканер запущен;</b></li> <li>• <b>ошибка при запуске сканера;</b></li> <li>• <b>сканер был остановлен;</b></li> <li>• <b>успешно;</b></li> <li>• <b>неудачно.</b></li> </ul> <p>Статус действия в случае события типа <b>обновление:</b></p> <ul style="list-style-type: none"> <li>• <b>процесс обновления запущен;</b></li> <li>• <b>ошибка запуска;</b></li> <li>• <b>новых обновлений не найдено;</b></li> <li>• <b>обновление прервано пользователем;</b></li> <li>• <b>обновления успешно установлены;</b></li> <li>• <b>нужна перезагрузка системы;</b></li> <li>• <b>обновление завершено с ошибками.</b></li> </ul> <p>Статус действия в случае события типа <b>события DeCrypt:</b></p> <ul style="list-style-type: none"> <li>• <b>SUCCESS;</b></li> <li>• <b>FAIL.</b></li> </ul>

Поле	Описание
Статус клиента	Статус зарегистрированного клиентского компонента: <ul style="list-style-type: none"> <li>• <b>активен;</b></li> <li>• <b>остановлен;</b></li> <li>• <b>работа службы была прервана;</b></li> <li>• <b>ошибка статуса. неверный статус.</b></li> </ul>
Исполняемый файл	Приложение или инсталлятор, вызвавшая события типов <b>нарушение политики контроля</b> или <b>запуск процесса</b> .
Командная строка процесса	<ul style="list-style-type: none"> <li>– Команда, вызвавшая событие типа <b>запуск процесса</b>.</li> <li>– Имя объекта файловой системы/реестра, в отношении которого произошло событие типа <b>нарушение политики контроля</b>, или имя DLL-модуля, загружаемого процессом, вызвавшим событие <b>нарушение политики контроля</b>.</li> <li>– Неверно введенный пароль.</li> </ul>
Пользователь	Учетная запись, под которой произошли события типов <b>запуск процесса</b> или <b>изменение настроек</b> .
Зона	Зона выполнения приложения: <ul style="list-style-type: none"> <li>• <b>доверенные</b> (разрешенные);</li> <li>• <b>по умолчанию</b> (ограниченные);</li> <li>• <b>блокированные</b> (запрещенные).</li> </ul>
Идентификатор процесса	Уникальный порядковый идентификатор процесса (PID) в ОС для события типа <b>запуск процесса</b> .
Идентификатор родительского процесса	Уникальный порядковый идентификатор родительского процесса (PPID) в ОС для события типа <b>запуск процесса</b> .
Родительский процесс	Наименование родительского процесса для события типа <b>запуск процесса</b> .
Решение	Решение по запуску приложения: <ul style="list-style-type: none"> <li>• <b>разрешен;</b></li> <li>• <b>запрещен.</b></li> </ul> Каждому решению соответствует свой цвет ячейки.
Проверено объектов	Количество объектов, проверенных в процессе антивирусного сканирования.
Угроз найдено	Количество найденных угроз в процессе антивирусного сканирования.
Угроз обезврежено	Количество обезвреженных угроз в процессе антивирусного сканирования.
Встроенные сертификаты	Количество встроенных сертификатов, обнаруженных в процессе автоматической настройки (сбора профиля).
Сертификаты каталогов	Количество сертификатов каталогов, обнаруженных в процессе автоматической настройки (сбора профиля).
Приложения	Статус контроля активности приложений: <ul style="list-style-type: none"> <li>• <b>активно;</b></li> <li>• <b>неактивно.</b></li> </ul>
Файловая система	Статус контроля файловой системы: <ul style="list-style-type: none"> <li>• <b>активно;</b></li> <li>• <b>неактивно.</b></li> </ul>
Системный реестр	Статус контроля системного реестра: <ul style="list-style-type: none"> <li>• <b>активно;</b></li> <li>• <b>неактивно.</b></li> </ul>
Сеть	Статус контроля сетевой активности: <ul style="list-style-type: none"> <li>• <b>активно;</b></li> <li>• <b>неактивно.</b></li> </ul>

Поле	Описание
Имя вошедшего пользователя	Учетная запись, под которой произошел вход в ОС клиентского хоста.
Имя вышедшего пользователя	Учетная запись, под которой произошел выход из ОС клиентского хоста.
Ошибка	Код ошибки в базе данных на сервере.
Тип клиента	Тип клиента, для которого отображается отчет. Для общих событий (SysWatch и DLP) поле имеет пустое значение.
Детали	Идентификатор (UID) правила, в отношении которого произошло нарушение политики контроля.
Имя службы	Системное имя службы, которая была запущена/остановлена.
Отображаемое имя	Название службы в оснастке <b>Службы</b> ОС Windows.
Событие службы	Статус службы: <ul style="list-style-type: none"> <li>• <b>ServiceStarted</b>;</li> <li>• <b>ServiceFoundRunning</b>;</li> <li>• <b>ServiceStopped</b>.</li> </ul>

Следующие события содержат в себе расширенную информацию об инциденте:

#### ▼ Событие антивирусного сканера

Событие антивирусного сканера позволяет просматривать подробный отчет о результатах проведения [антивирусного сканирования](#)<sup>132</sup> клиентских хостов.

Откройте список событий на вкладке **Лог событий** для компонента SoftControl SysWatch и выберите событие типа **Антивирус** с действием **Завершение сканирования**. Чтобы вызвать отчет с дополнительной информацией, выполните одно из следующих действий для выбранного события:

- дважды нажмите левой кнопки мыши на событии;
- вызовите контекстное меню нажатием правой кнопки мыши на событии и выберите команду **Показать дополнительную информацию события антивируса**.



Отчет с дополнительной информацией будет открыт только в том случае, если в результате антивирусного сканирования найдены угрозы (ненулевой счетчик в поле **Угроз найдено**) или в случае наличия необезвреженных угроз при предыдущей проверке.

В появившейся дополнительной вкладке **Сканер** представлены все объекты, содержащие обнаруженные угрозы по результатам проверки (рис. [Вкладка «Сканер»](#)<sup>148</sup>).

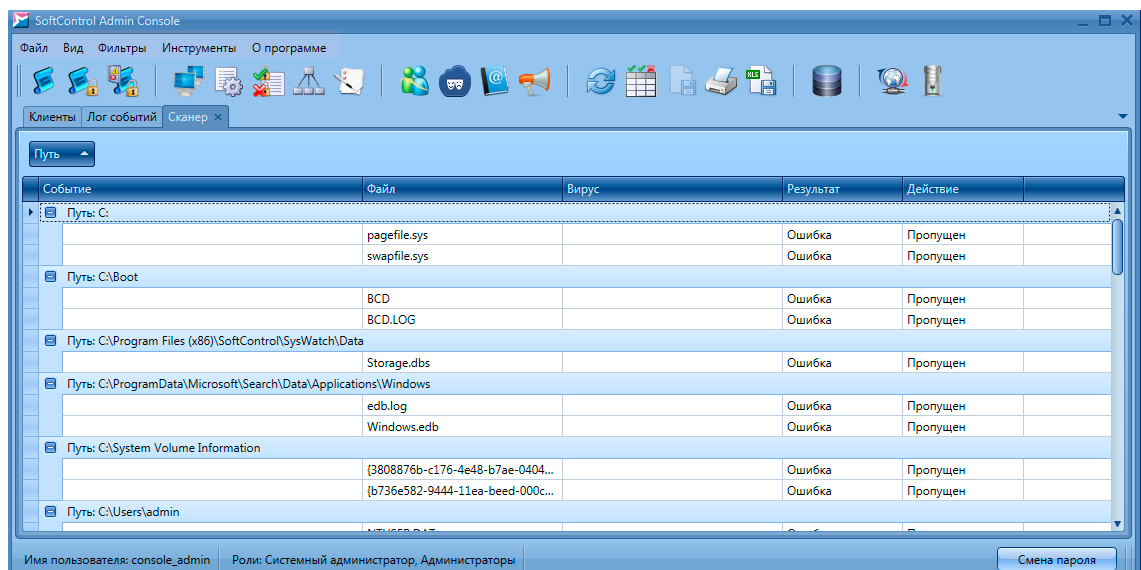


Рисунок 127. Вкладка «Сканер»

Полный перечень полей вкладки приведен в табл. 21.

Таблица 21. Поля вкладки «Сканер»

Поле	Описание
Событие	Дата и время окончания антивирусного сканирования.
Путь	Каталог расположения объекта в файловой системе клиентского хоста.
Файл	Имя объекта.
Вирус	Наименование вредоносного кода, которым заражен объект.
Результат	Результат антивирусного сканирования: <ul style="list-style-type: none"> <li>• Чист;</li> <li>• Заражен;</li> <li>• Подозрителен;</li> <li>• Ошибка;</li> <li>• Ошибка лечения;</li> <li>• Ошибка перемещения;</li> <li>• Ошибка удаления.</li> </ul>
Действие	Действие, выполненное для данного объекта по результатам антивирусного сканирования: <ul style="list-style-type: none"> <li>• Излечен;</li> <li>• Перемещен;</li> <li>• Пропущен;</li> <li>• Удален;</li> <li>• Нет действия.</li> </ul>

#### ▼ Событие изменения настроек

Событие изменения настроек позволяет просматривать полный список изменений в конфигурации SoftControl SysWatch. Настройки SoftControl SysWatch могут быть

изменены следующими способами:

- [администратором через SoftControl Admin Console](#) <sup>(66)</sup>;
- локальным пользователем с помощью:
  - ГИП программы;
  - применения конфигурационного файла.

Откройте список событий на вкладке **Лог событий** для компонента SoftControl SysWatch и выберите событие типа **Изменение настроек**. Чтобы вызвать отчет с дополнительной информацией, выполните одно из следующих действий для выбранного события:

- дважды нажмите левой кнопки мыши на событии;
- вызовите контекстное меню нажатием правой кнопки мыши на событии и выберите команду **Показать дополнительную информацию события изменения настроек**.

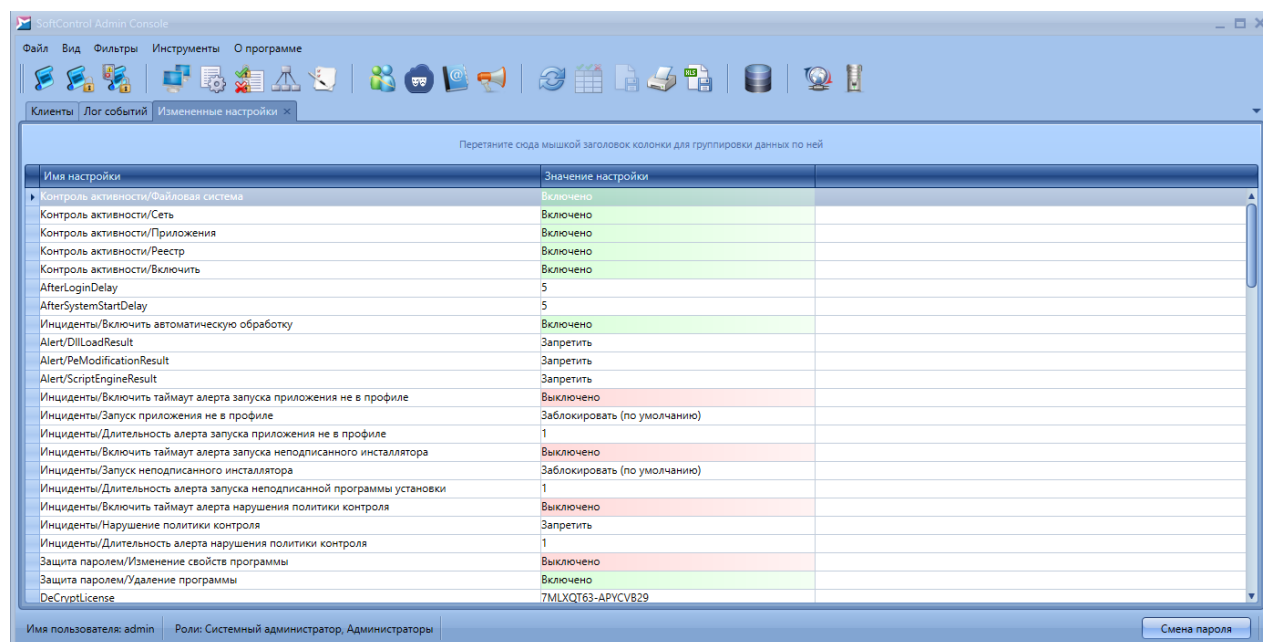


Рисунок 128. Вкладка «Измененные настройки»

В появившейся дополнительной вкладке **Измененные настройки** представлен перечень настроек SoftControl SysWatch с указанием их нового состояния (рис. [Вкладка «Измененные настройки»](#) <sup>(150)</sup>).

Полный перечень полей вкладки приведен в табл. 22.

Таблица 22. Поля вкладки «Измененные настройки»

Поле	Описание
Имя настройки	Название настройки.
Значение настройки	Значение настройки, на которое оно было изменено в результате события.

## 4.9.2 Отчеты SoftControl DLP Client

Вкладка **Лог событий** предоставляет возможность просмотра отчетов по данным, собираемым SoftControl DLP Client на клиентских хостах (рис. [Вкладка «Лог событий» для компонента SoftControl DLP Client](#)<sup>151</sup>). Чтобы просмотреть все события, поступившие с клиентов DLP, выделите нужные клиенты и следуйте инструкции, приведенной в разделе [Клиенты](#)<sup>49</sup>.

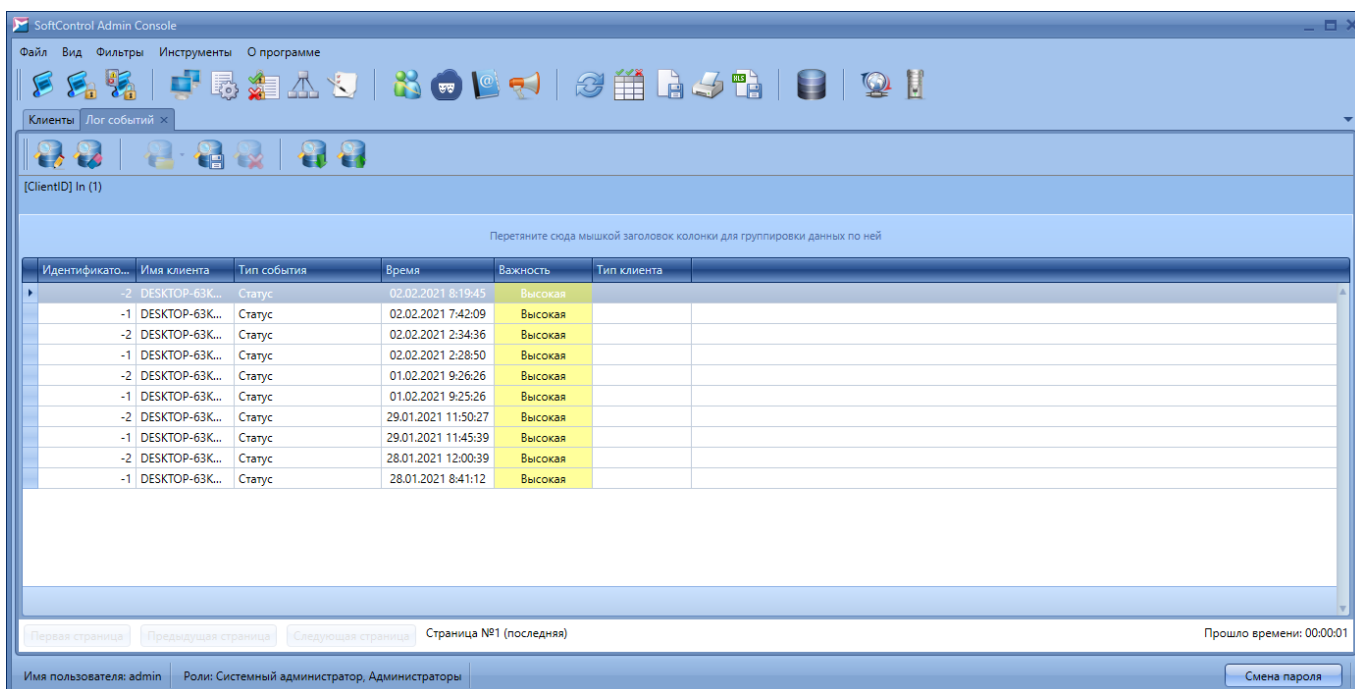


Рисунок 129. Вкладка «Лог событий» для компонента SoftControl DLP Client

Полный перечень полей вкладки **Лог событий** для компонента SoftControl DLP Client приведен в табл. 23.

Таблица 23. Поля вкладки «Лог СОБЫТИЙ» для SoftControl DLP Client

Поле	Описание
Имя	Имя клиентского хоста.
Идентификатор события	Уникальный идентификатор события. Если происходит прием события с дублированным идентификатором, дублируемая строка помечается красным цветом. В случае нарушения целостности порядка идентификаторов (разрывы в последовательности), в <a href="#">отчет серверного компонента в журнале Windows</a> <sup>199</sup>

Поле	Описание
	вносится соответствующее предупреждение. Исключением являются события типа <b>Статус</b> , для которых данный параметр принимает значения -1 или -2.
Уникальный ID устройства	Уникальный идентификатор клиентского хоста, который автоматически присваивается ему при первом обращении клиентского приложения SoftControl DLP Client к серверу SoftControl Server.
Тип события	Тип события сбора данных: <ul style="list-style-type: none"> <li>• <b>добавлено устройство;</b></li> <li>• <b>файл;</b></li> <li>• <b>HTTP;</b></li> <li>• <b>монитор клавиатуры;</b></li> <li>• <b>принтер;</b></li> <li>• <b>реестр;</b></li> <li>• <b>устройство отсоединено;</b></li> <li>• <b>время работы.</b></li> </ul>
Время	Дата и время регистрации события.
Важность	Важность (приоритет) события с точки зрения угрозы информационной безопасности клиентского хоста: <ul style="list-style-type: none"> <li>• <b>обычная;</b></li> <li>• <b>высокая;</b></li> <li>• <b>критическая.</b></li> </ul> Каждому уровню приоритета соответствует свой цвет ячейки.
Статус клиента	Статус зарегистрированного клиентского компонента: <ul style="list-style-type: none"> <li>• <b>активен;</b></li> <li>• <b>остановлен;</b></li> <li>• <b>работа службы была прервана;</b></li> <li>• <b>ошибка статуса. неверный статус.</b></li> </ul>
Путь к процессу	Путь к процессу, вызвавшему событие типов <b>файл, реестр, HTTP, монитор клавиатуры, время работы, принтер.</b>
Описание процесса	Описание процесса, вызвавшего событие типов <b>файл, реестр, HTTP, монитор клавиатуры, время работы, принтер.</b>
Пользователь	Учетная запись пользователя, под которой был запущен процесс, вызвавший событие типов <b>файл, реестр, HTTP, монитор клавиатуры, время работы, принтер.</b>
IP	IP-адрес назначения HTTP-запроса для события типа <b>HTTP.</b>
Url	URL назначения HTTP-запроса для события типа <b>HTTP.</b>
Заголовок	Заголовок HTTP для события типа <b>HTTP.</b>
Маска доступа	Тип операции над наблюдаемым объектом для событий типов <b>файл и реестр:</b> <ul style="list-style-type: none"> <li>• <b>чтение;</b></li> <li>• <b>запись;</b></li> <li>• <b>удаление;</b></li> <li>• <b>переименование;</b></li> <li>• <b>изменение.</b></li> </ul>
Резервная копия	Локальный путь к теневой копии наблюдаемого объекта с именем вида <i>&lt;Полное имя оригинального объекта&gt;_&lt;N&gt;.bkr</i> , где <i>N</i> – порядковый номер сохраненной копии, для событий типов <b>файл и реестр.</b>
Путь к файлу	Путь к наблюдаемому каталогу или файлу для события типа <b>файл.</b>
Тип диска	Тип носителя, на котором располагается наблюдаемый каталог или файл для



Поле	Описание
	события типа <b>файл</b> : <ul style="list-style-type: none"> <li>• <b>локальный носитель</b>;</li> <li>• <b>съёмный носитель</b>.</li> </ul>
Ветка реестра	Путь к наблюдаемому разделу реестра или параметру раздела реестра для события типа <b>реестр</b> .
Время записи события	Дата записи ввода с клавиатуры для события типа <b>монитор клавиатуры</b> .
Записанные данные	Текст, введенный пользователем с клавиатуры, для события типа <b>монитор клавиатуры</b> .
Детали	Описание источника печати для события типа <b>принтер</b> .
ID устройства	ID периферийного устройства для событий типов <b>добавлено устройство</b> и <b>устройство отсоединено</b> .
Класс устройства	Класс периферийного устройства для событий типов <b>добавлено устройство</b> и <b>устройство отсоединено</b> .
Описание устройства	Описание периферийного устройства для событий типов <b>добавлено устройство</b> и <b>устройство отсоединено</b> .
Время старта	Время начала работы с приложением для события типа <b>время работы</b> .
Время окончания	Время окончания работы с приложением для события типа <b>время работы</b> .
Продолжительность	Продолжительность работы с приложением для события типа <b>время работы</b> .
Индекс файла	Индекс файла для события типа <b>HTTP</b> .
Тип клиента	Тип клиента, для которого отображается отчет. Для общих событий (SysWatch и DLP) поле имеет пустое значение.
Имя принтера	Логическое имя принтера, на который отправлено задание на печать.

События типов **файл**, **реестр** и **HTTP** выделяются в отчетах цветом, если содержат в себе дополнительные данные (видеозаписи, теневые копии) (рис. [Контекстное меню события с дополнительными данными](#)<sup>153</sup>).

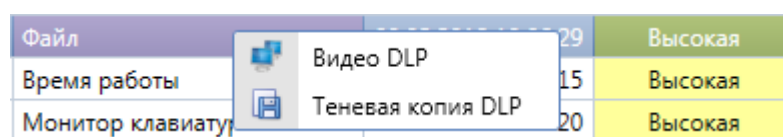


Рисунок 130. Контекстное меню события с дополнительными данными

#### ▼ Просмотр видеозаписей

SoftControl DLP Client сохраняет последовательность снимков экрана клиентского хоста, которая может быть воспроизведена как видеозапись в консоли управления. Для событий типов **файл**, **реестр** и **HTTP** доступен просмотр видеозаписей, если в настройках наблюдаемых объектов выставлена опция **Запись видео**. Вызовите контекстное меню нажатием правой кнопки мыши на событии и выберите пункт **Видео DLP**, чтобы открыть видеозапись (рис. [Контекстное меню события с дополнительными данными](#)<sup>153</sup>).

В появившемся окне проигрывателя нажмите на кнопку **Загрузить** и управляйте воспроизведением с помощью кнопок (рис. [Проигрыватель видеозаписей SoftControl DLP Client](#)<sup>154</sup>), предназначение которых приведено в табл. 24.

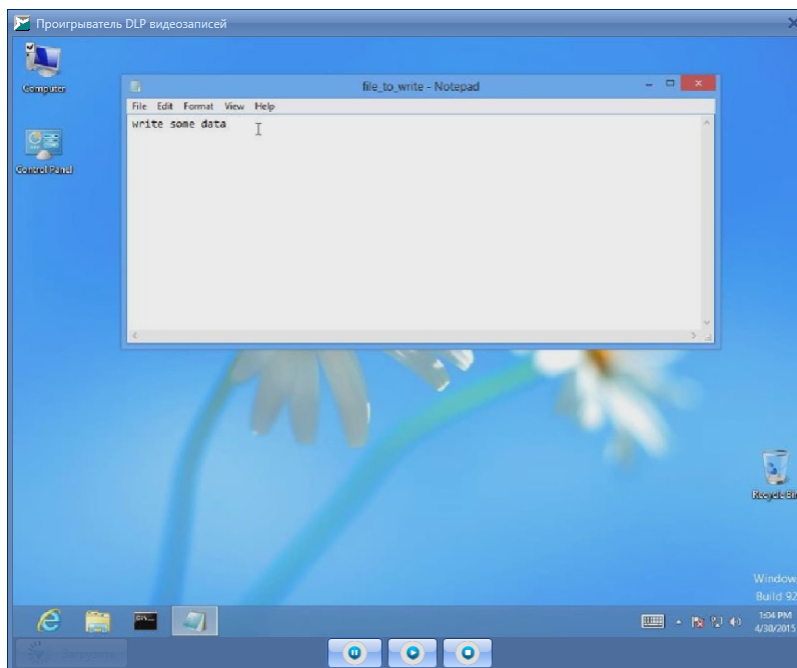





Рисунок 131. Проигрыватель видеозаписей SoftControl DLP Client

Таблица 24. Элементы управления видеопроигрывателя

Кнопка	Название	Описание
	Воспроизвести	Воспроизведение записи.
	Пауза	Пауза воспроизведения.
	Стоп	Остановка воспроизведения.

**i** Для корректной обработки записей серверным компонентом SoftControl Server в ОС Microsoft® Windows® Server 2008 R2 и Microsoft® Windows® Server 2012 / 2012 R2 необходимо предварительно установить дополнительный системный компонент *Возможности рабочего стола (Desktop Experience)*. Указания по установке даны в [приложении](#)<sup>225</sup>.

#### ▼ Просмотр теневых копий

Для событий типов **файл** и **реестр** доступен просмотр теневых копий объектов, если в настройках наблюдения для данных объектов выставлена опция **Теневая копия**. Вызовите контекстное меню нажатием правой кнопки мыши на событии, выберите пункт **Теневая копия DLP** (рис. [Контекстное меню события с дополнительными данными](#)<sup>153</sup>) и в появившемся окне **Просмотр теневой копии DLP** нажмите на кнопку **Открыть**, чтобы просмотреть сохраненную копию указанного объекта наблюдения (рис. [Теневая копия объекта наблюдения](#)<sup>155</sup>).

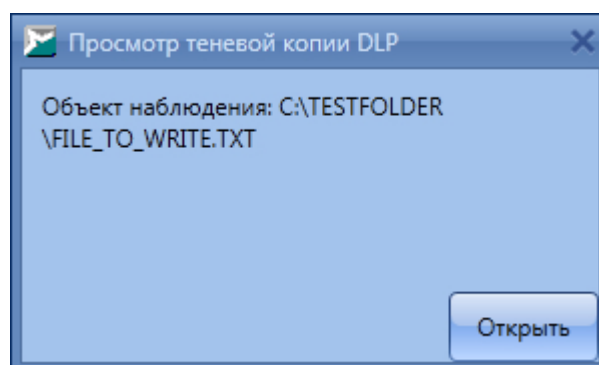


Рисунок 132. Теневая копия объекта наблюдения

### 4.9.3 Отчеты SoftControl SysCmd

Вкладка **Лог событий** предоставляет возможность просмотра отчетов по данным, собираемым SoftControl SysCmd на клиентских хостах (рис. [Вкладка «Лог событий» для компонента SoftControl SysCmd](#)<sup>155</sup>). Чтобы просмотреть все события, поступившие с клиентов, выделите нужные клиенты и следуйте инструкции, приведенной в разделе [Клиенты](#)<sup>49</sup>.

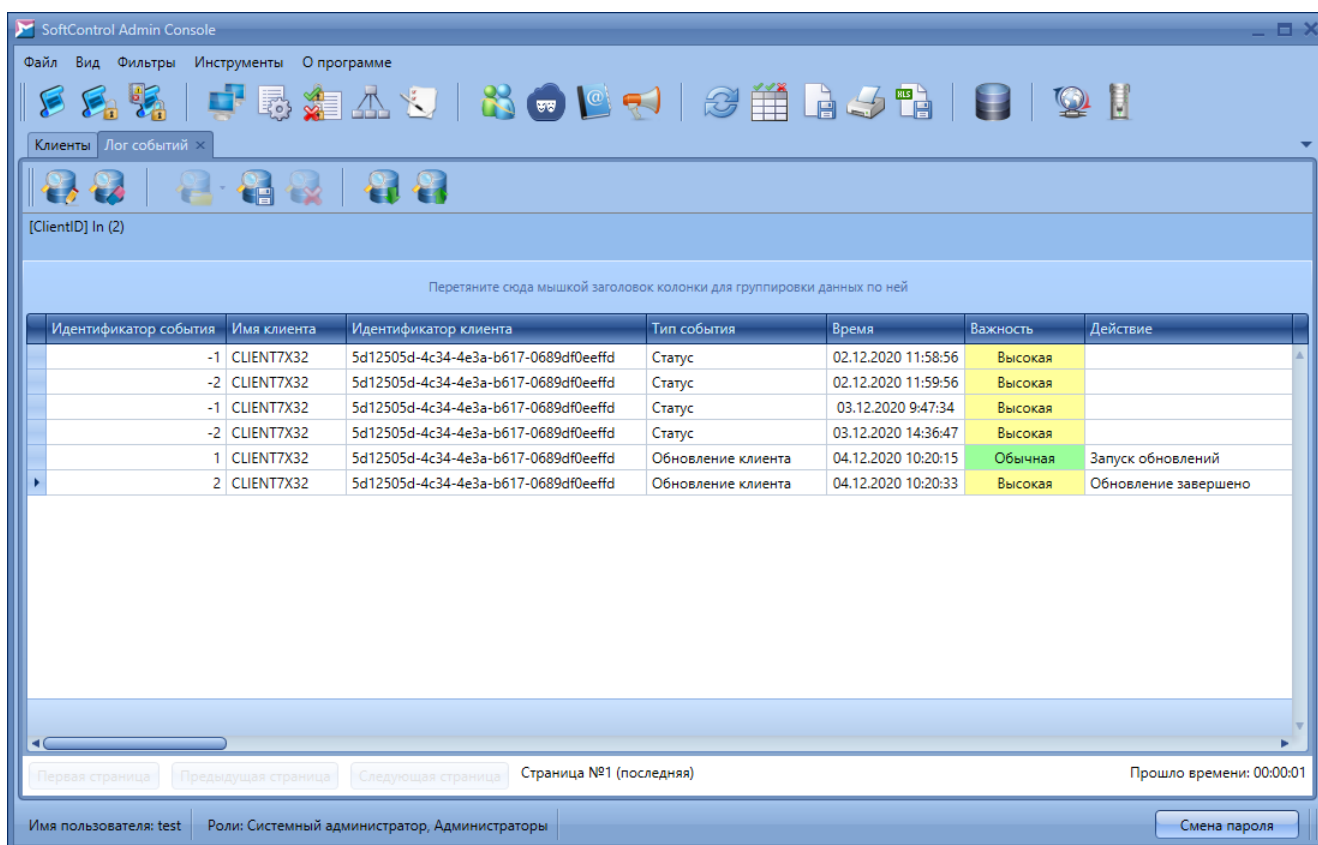


Рисунок 133. Вкладка «Лог событий» для компонента SoftControl SysCmd

Полный перечень полей вкладки **Лог событий** для компонента SoftControl SysCmd приведен в табл. 25.

Таблица 25. Поля вкладки «Лог СОБЫТИЙ» для SoftControl SysCmd

Поле	Описание
Имя	Имя клиентского хоста.
Идентификатор события	Уникальный идентификатор события. Если происходит прием события с дублированным идентификатором, дублируемая строка помечается красным цветом. В случае нарушения целостности порядка идентификаторов (разрывы в последовательности), в <a href="#">отчет серверного компонента в журнале Windows</a> <sup>199</sup> вносится соответствующее предупреждение. Исключением являются события типа <b>Статус</b> , для которых данный параметр принимает значения -1 или -2.
Уникальный ID устройства	Уникальный идентификатор клиентского хоста, который автоматически присваивается ему при первом обращении клиентского приложения SoftControl SysCmd к серверу SoftControl Server.
Тип события	Тип события сбора данных: <ul style="list-style-type: none"> <li>• <b>обновление клиента</b>;</li> <li>• <b>статус</b>.</li> </ul>
Время	Дата и время регистрации события.
Важность	Важность (приоритет) события с точки зрения угрозы информационной безопасности клиентского хоста: <ul style="list-style-type: none"> <li>• <b>обычная</b>;</li> <li>• <b>высокая</b>;</li> </ul>

Поле	Описание
	<ul style="list-style-type: none"> <li>критическая.</li> </ul> Каждому уровню приоритета соответствует свой цвет ячейки.
Статус клиента	Статус зарегистрированного клиентского компонента: <ul style="list-style-type: none"> <li>активен;</li> <li>остановлен;</li> <li>работа службы была прервана;</li> <li>ошибка статуса. неверный статус.</li> </ul>
Действие	Действие в случае события типа <b>обновление</b> : <ul style="list-style-type: none"> <li>запуск обновлений;</li> <li>обновление завершено.</li> </ul>
Статус действия	Статус действия в случае события типа <b>обновление</b> : <ul style="list-style-type: none"> <li>процесс обновления запущен;</li> <li>ошибка запуска;</li> <li>новых обновлений не найдено;</li> <li>обновление прервано пользователем;</li> <li>обновления успешно установлены;</li> <li>нужна перезагрузка системы;</li> <li>обновление завершено с ошибками.</li> </ul>

#### 4.9.4 Интегрированный лог событий

Вкладка **Интегрированный лог событий** предоставляет возможность просмотра всех логов событий в общем списке (рис. [Вкладка «Интегрированный лог событий»](#)<sup>157</sup>), а именно:

- события, регистрируемые SoftControl SysWatch, SoftControl DLP Client и SoftControl SysCmd на клиентских хостах;
- события из журналов Windows с клиентских хостов, на которых работает SoftControl SysWatch;
- события безопасности SoftControl Service Center.

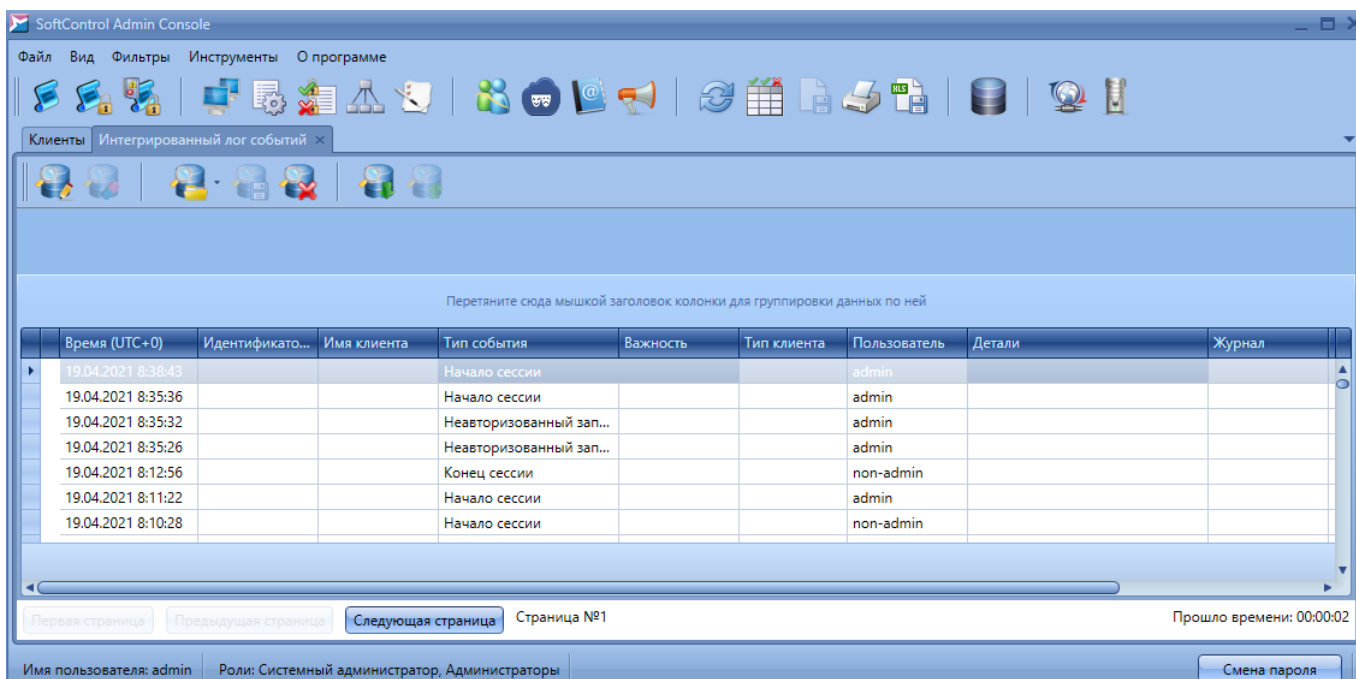


Рисунок 134. Вкладка «Интегрированный лог событий»

Обратите внимание, что за один хартбит (интервал между обращениями SoftControl SysWatch к SoftControl Server, по умолчанию 60 секунд) клиентское приложение передает не более 1000 событий из журналов Windows. Если в течение длительного времени в среднем за хартбит в журналах Windows появляется больше событий, то события не будут успевать приходить на сервер и могут теряться.

Описание полей вкладки **Интегрированный лог событий**, относящихся к событиям клиентам и SoftControl Service Center можно найти в соответствующих разделах данного документа:

- [Отчеты SoftControl SysWatch](#)<sup>144</sup>;
- [Отчеты SoftControl DLP Client](#)<sup>151</sup>;
- [Отчеты SoftControl SysCmd](#)<sup>151</sup>;
- [События безопасности](#)<sup>42</sup>;

Поля, относящиеся к событиям из журнала Windows и не описанные в указанных выше разделах, приведены в таблице 26.

Таблица 26. Поля вкладки «Интегрированный лог событий», относящиеся к событиям из журнала Windows

Поле	Описание
<Без названия>	Для событий, содержащих подробную информацию, присутствует значок <b>+</b> , позволяющий просмотреть ее.
Идентификатор события	Идентификатор события в журнале Windows.

Поле	Описание
Тип события	Поле всегда имеет значение <b>Событие журнала Windows</b> .
Важность	Значение соответствует полю <b>Уровень</b> в журнале Windows.
Журнал	Название журнала, где зарегистрировано событие: <ul style="list-style-type: none"> <li>• <b>Application</b>;</li> <li>• <b>System</b>;</li> <li>• <b>Security</b>;</li> <li>• <b>SafenSoft</b>.</li> </ul> События из журнала SafenSoft регистрируются SoftControl Server и могут присутствовать в данном логе, если на сервере работает SoftControl SysWatch.
Источник	Источник (провайдер) события
Код операции	Код операции. Значение, определенное провайдером для логической группировки событий.
ID задачи	Идентификатор задачи. Значение, определенное провайдером для логической группировки событий.

## 4.9.5 Фильтрация событий

### ▼ Страничное отображение

Информация на вкладке **Лог событий** отображается в постраничном режиме. Ограничение максимального количества событий на странице задается в [настройках интерфейса SoftControl Admin Console](#)<sup>32</sup> (по умолчанию – 10 000 событий).

**i** Не рекомендуется выставлять значение параметра **Размер страницы событий** большим 100 000 событий, так как это может снизить производительность.

Записи расположены в обратном хронологическом порядке, т.е. на первой странице находятся записи о последних событиях. Для навигации по страницам используйте соответствующие кнопки в нижней части вкладки (рис. [Навигация по страницам](#)<sup>159</sup>). Переход осуществляется только на соседние страницы.

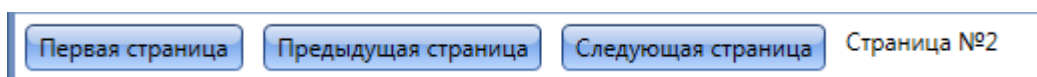


Рисунок 135. Навигация по страницам

### ▼ Группировка данных

Информация на вкладке **Лог событий** может группироваться по всем полям (категориям) для удобства отображения. На дополнительной вкладке **Сканер** можно группировать по следующим полям (категориям): **Путь** (по умолчанию), **Вирус**, **Результат** и **Действие**. Для группировки по категориям перетащите

заголовок колонки на панель, расположенную между заголовком таблицы и группой кнопок вкладки. Если группировка производится по нескольким категориям, то приоритет (вложенность категорий) уменьшается слева направо в зависимости от расположения на панели.

#### ▼ **Фильтрация с использованием предустановленных фильтров**

В SoftControl Admin Console предусмотрены встроенные фильтры для выборки событий.

Чтобы применить предустановленные в программе общие фильтры, откройте меню **Фильтры** и выберите один из вариантов:

- **По умолчанию** – отображение всех типов событий по полям, несущим основную информацию (применяется по умолчанию при открытии вкладки).
- **Полный вид** – отображение всех типов событий по всем возможным полям.
- **Статус** – отображение событий по изменению статуса клиентских приложений.
- **Обновление клиента** – отображение событий по обновлению клиентских приложений.

Чтобы применить предустановленные фильтры, соответствующие типам событий клиентского компонента SoftControl SysWatch, откройте меню **Фильтры** → **Фильтры событий SysWatch** и выберите один из вариантов:

- **Все;**
- **Нарушение политики контроля;**
- **Контроль активности;**
- **Запуск процесса;**
- **Антивирус;**
- **Изменение настроек;**
- **Вход пользователя;**
- **Выход пользователя;**
- **Событие службы.**

Чтобы применить предустановленные фильтры, соответствующие типам событий клиентского компонента SoftControl DLP Client, откройте меню **Фильтры** → **Фильтры событий DLP** и выберите один из вариантов:

- **Все;**
- **Добавлено устройство;**



- Файл;
- HTTP;
- Монитор клавиатуры;
- Принтер;
- Реестр;
- Устройство отсоединено;
- Время работы.



Фильтрация применяется только к записям текущей страницы.

При наличии большого количества событий во время работы фильтра отображается индикатор выполнения. При необходимости процесс можно остановить.

#### ▼ Фильтрация с использованием пользовательских фильтров

Возможно самостоятельно настроить параметры выборки и сохранить их в качестве нестандартного фильтра, который вызывается из меню **Фильтры** → **Пользовательские фильтры**.

Чтобы добавить новое поле в таблицу текущей вкладки нажмите кнопку **Выбрать колонки** и перетащите требуемое поле из окна **Выбор колонок** (рис. [Выбор колонок](#) <sup>(161)</sup>) в необходимое место заголовка таблицы. Для удаления существующего поля перетащите его в окно **Выбор колонок**, либо за пределы заголовка таблицы.

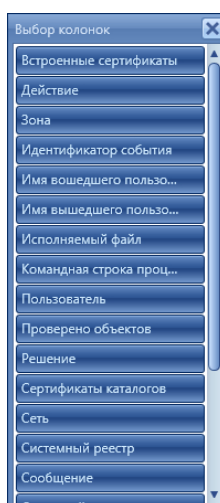


Рисунок 136. Выбор колонок

Для того чтобы отфильтровать выборку по значениям полей, переместите курсор мыши на название поля и нажмите левой кнопкой мыши на появившемся значке ключа, после чего укажите критерий выборки в выпадающем списке (рис. [Фильтр по полю](#)<sup>(162)</sup>).

Фильтрацию выборки можно производить по нескольким полям одновременно. В заголовках полей, по которым производится фильтрация, значок ключа отображается постоянно.

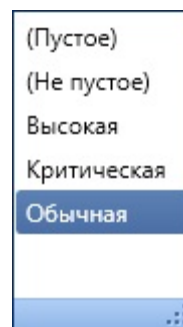


Рисунок 137. Фильтр по полю

Когда вы отфильтруете записи, внизу окна появится строка, описывающая настроенный фильтр. Его можно удалить или изменить с помощью соответствующих иконок справа от строки.

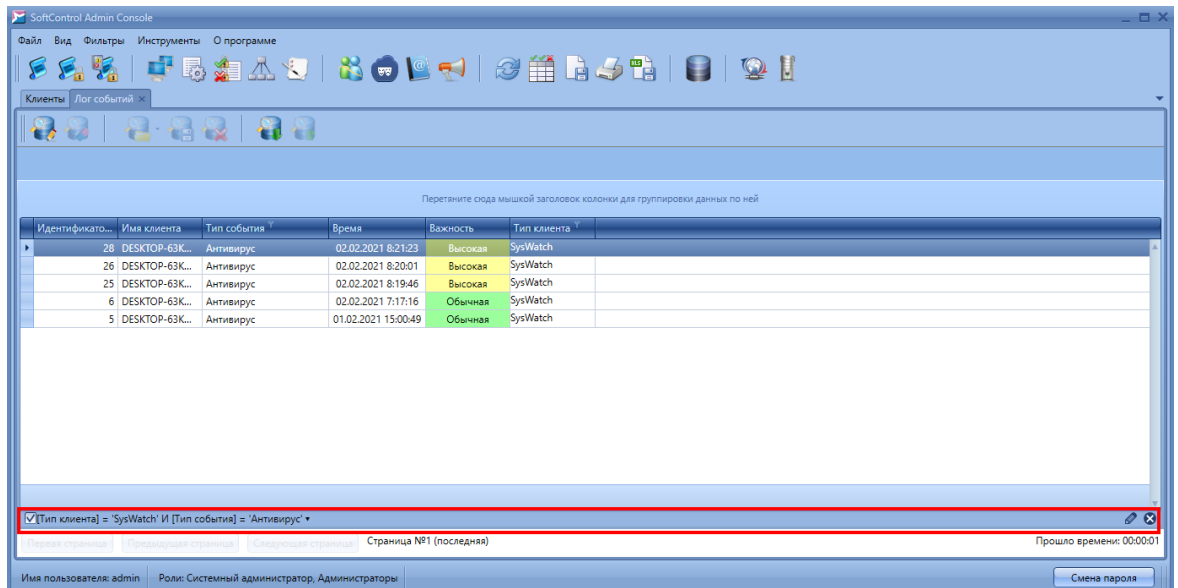


Рисунок 138. Настроенный фильтр

Нажмите на значок карандаша в правой части строки фильтра, чтобы открыть средство **Редактор фильтра**.

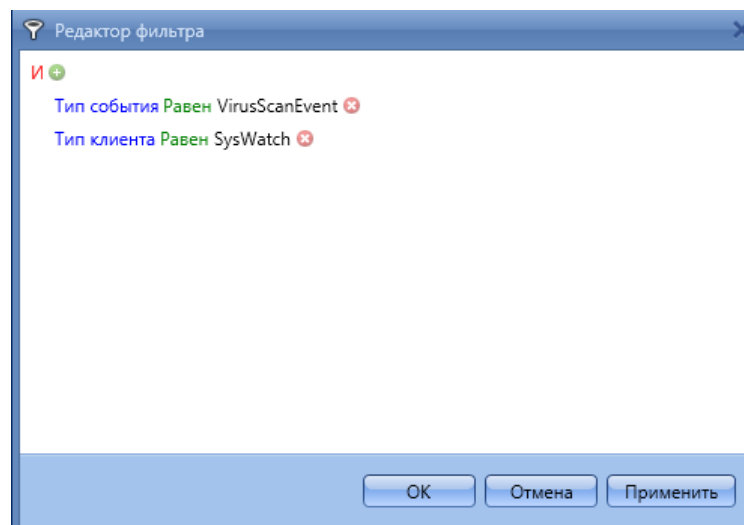


Рисунок 139. Редактор фильтра

В первой строке редактора красным цветом указан логический оператор, по которому объединяются параметры фильтра. Чтобы изменить логический оператор, нажмите на него левой кнопкой мыши. При этом в выпадающем меню вы увидите следующие варианты:

- И;
- ИЛИ;
- Не И;
- Не ИЛИ.

Чтобы добавить новый параметр фильтра, нажмите на значок плюса около логического оператора. Чтобы удалить условие из фильтра, нажмите на крестик. Синтаксис строки параметра фильтра выглядит следующим образом: *<поле, по которому производится фильтрация> <оператор сравнения> <значение>*. Каждый элемент строки параметра можно изменить, нажав на него. Варианты автоматически определяются исходя из типа поля.

На вкладке **Интегрированный лог событий** редактор фильтра состоит из трех разделов, позволяющих отдельно редактировать фильтры для логов клиентов, событий безопасности сервера и журнала событий Windows.

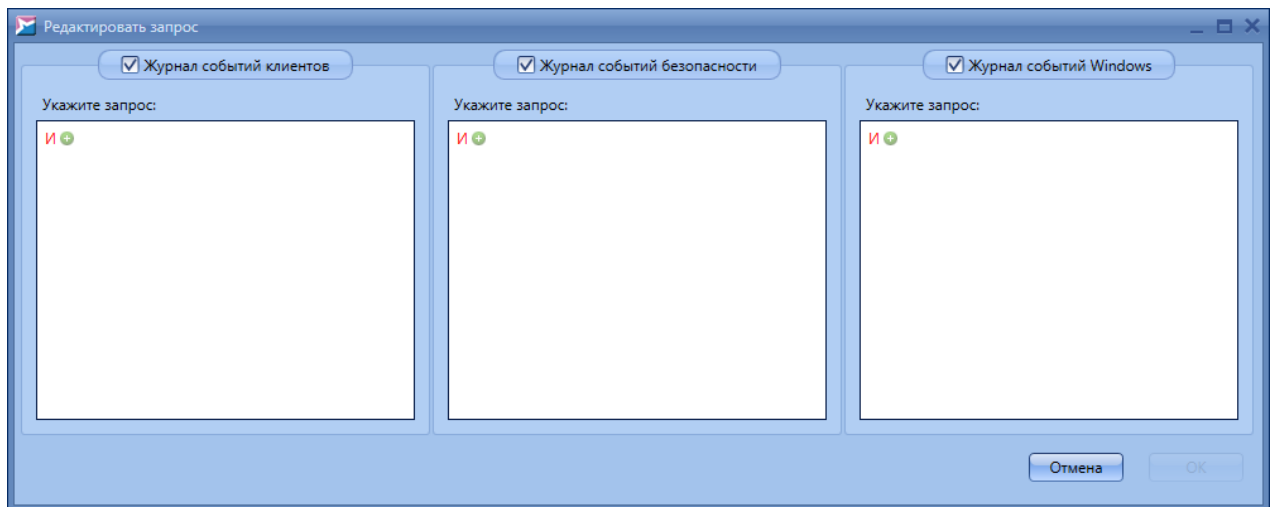


Рисунок 140. Редактор фильтра интегрированного лога событий

Для упорядочивания данных в таблицах вкладок по определенным полям нажмите левой кнопкой мыши на требуемом поле и одиночным нажатием задайте направление сортировки, которое обозначается стрелкой правее названия поля. Чтобы сохранить полученную с параметрами пользователя выборку для дальнейшего использования, нажмите на кнопку **Сохранить настройки вида**, введите имя фильтра в появившемся окне и нажмите **ОК** (рис. [Сохранение фильтра](#)<sup>164</sup>).

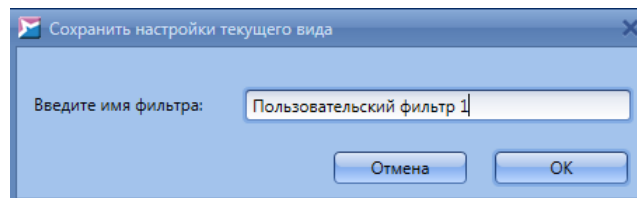


Рисунок 141. Сохранение фильтра

---

**i** Фильтрация применяется только к записям текущей страницы.

---

При наличии большого количества событий во время работы фильтра отображается индикатор выполнения. При необходимости процесс можно остановить.

## 4.9.6 Запросы к базе данных

Если вам часто приходится искать записи о событиях, отвечающих определенным условиям, вы можете создать запрос с этими условиями и сохранить его. Тогда в следующий раз можно будет загрузить созданный ранее запрос и получить по нему соответствующие записи из базы данных.

Работать с запросами к базе данных позволяют иконки, расположенные на дополнительной панели.

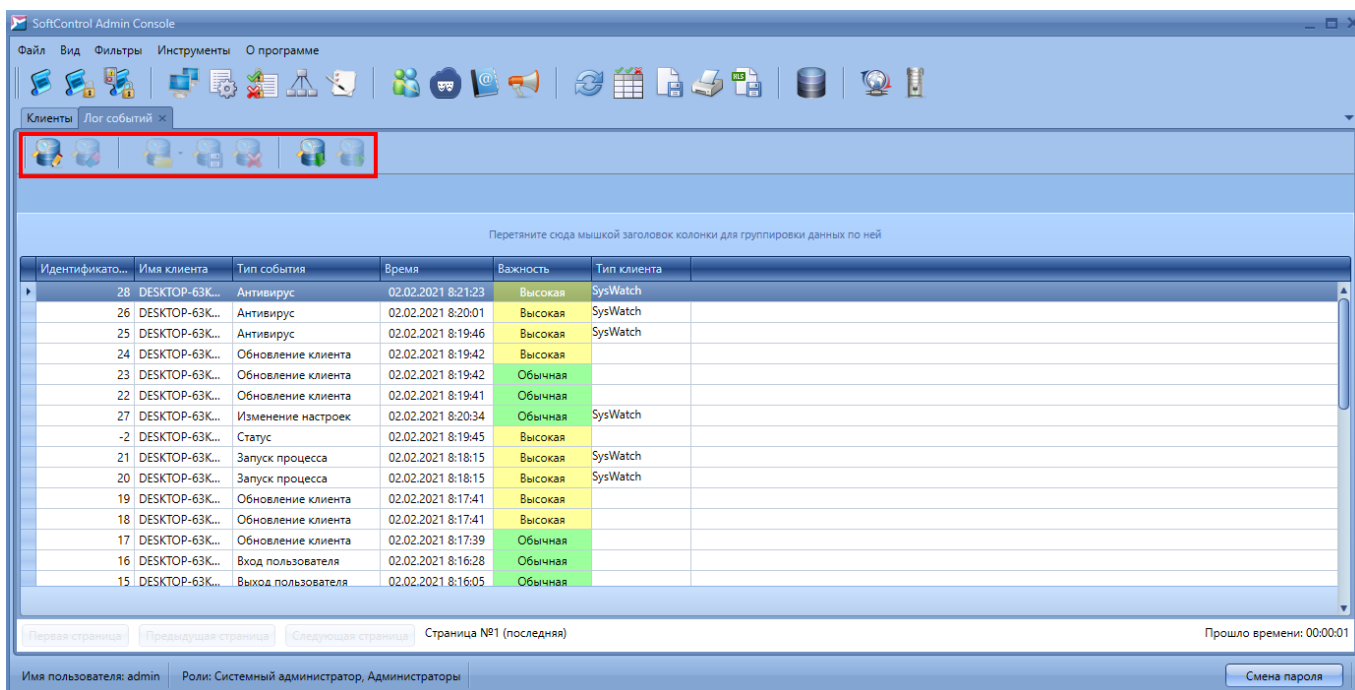



Рисунок 142. Кнопки для работы с запросами

Чтобы создать запрос, нажмите на кнопку  (Редактировать запрос). Откроется окно редактора запроса.

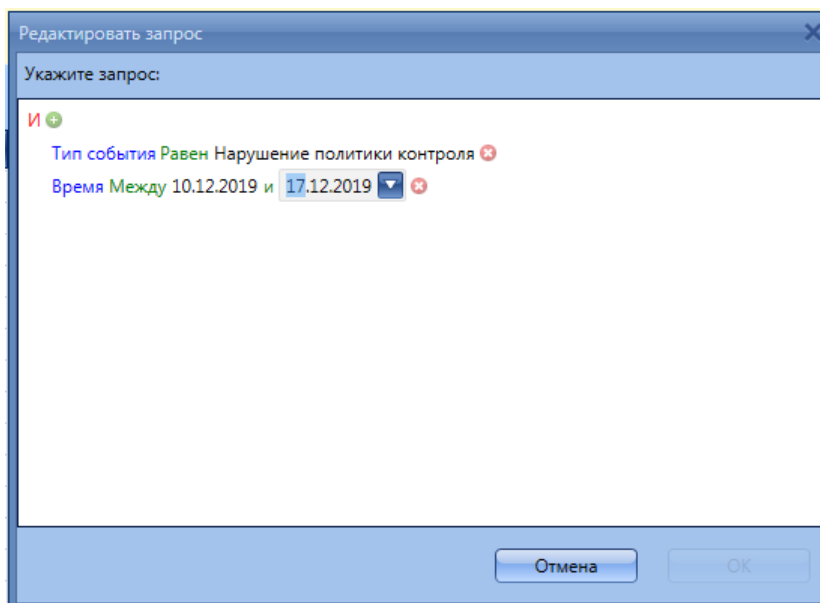


Рисунок 143. Редактирование запроса

В первой строке редактора красным цветом указан логический оператор, по которому объединяются параметры фильтра. Чтобы изменить логический оператор, нажмите на него левой кнопкой мыши. При этом в выпадающем меню вы увидите следующие варианты:



- И;
- ИЛИ;
- Не И;
- Не ИЛИ.






Чтобы добавить новый параметр фильтра, нажмите на значок плюса около логического оператора. Чтобы удалить условие из фильтра, нажмите на крестик

Синтаксис строки параметра фильтра выглядит следующим образом: *<поле, по которому производится фильтрация> <оператор сравнения> <значение>*. Каждый элемент строки параметра можно изменить, нажав на него. Варианты автоматически определяются исходя из типа поля.

Все кнопки для работы с запросами перечислены в таблице ниже.

Таблица 27. Запросы к базе данных

Кнопка	Название	Описание
	Редактировать запрос	Открывает редактор запроса. Здесь можно выбрать параметры и желаемые значения
	Очистить запрос	Сбрасывает введенные критерии запроса

Кнопка	Название	Описание
	Выбрать запрос	Предлагает выбрать запрос из списка сохраненных запросов. Запросы хранятся в файле C:\ProgramData\SafenSoft\UserFilters\QueryCriteria.xml
	Сохранить запрос	Сохраняет текущий запрос в файле C:\ProgramData\SafenSoft\UserFilters\QueryCriteria.xml
	Удаление запросов	Открывает окно со списком сохраненных запросов, откуда вы можете их удалить
	Импорт запроса	Позволяет выбрать файл XML и импортировать из него запрос
	Экспорт запроса	Экспортирует текущий запрос в файл XML

#### 4.9.7 Печать и экспорт в файлы отчётов

В SoftControl Admin Console существует несколько возможностей экспорта накопленной информации в отчетах клиентских приложений.

Для вывода отчета на печать произведите выборку с помощью необходимых [фильтров](#)<sup>159</sup> и нажмите на кнопку **Печать**. В открывшемся окне предварительного просмотра можно задать **Настройки страницы** и **Масштаб** с помощью соответствующих кнопок (рис. [Предварительный просмотр печати](#)<sup>167</sup>).

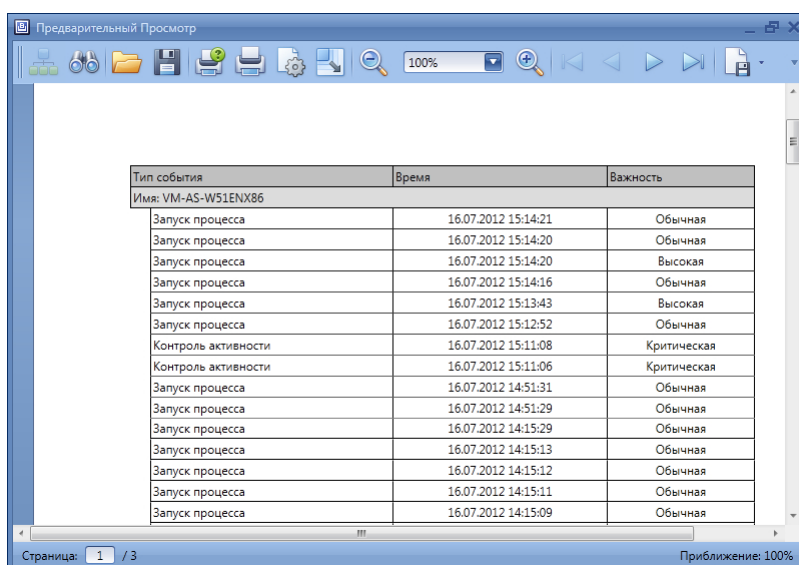


Рисунок 144. Предварительный просмотр печати

Нажмите на кнопку **Печать** для вывода стандартного окна настроек принтера, либо на

кнопку **Быстрая печать** для мгновенной отправки на печать с установками принтера по умолчанию.

Для сохранения отчета в таблицу Excel произведите выборку с помощью необходимых [фильтров](#)<sup>159</sup> и нажмите на кнопку **Экспорт в Excel**. В диалоговом окне сохранения укажите место для сохранения отчета и его имя, после чего нажмите на кнопку **Сохранить (Save)**.

#### 4.9.8 Резервное копирование отчетов

В SoftControl Admin Console существует возможность резервного копирования таблиц с логом событий и с событиями безопасности. Для настройки копирования выберите команду **Настройки сервера** в меню **Файл** SoftControl Admin Console. В появившемся окне (рис. [Резервное копирование событий](#)<sup>168</sup>) перейдите на вкладку **Таблица Событий** или **Таблица Событий безопасности**, в зависимости от того, какие события необходимо сохранить. На каждой из вкладок установите переключатель в положение **Осуществлять резервное копирование** и укажите **Путь** на сервере для сохранения таблиц, **Период** сохранения (в днях) и **Время** создания резервных копий.

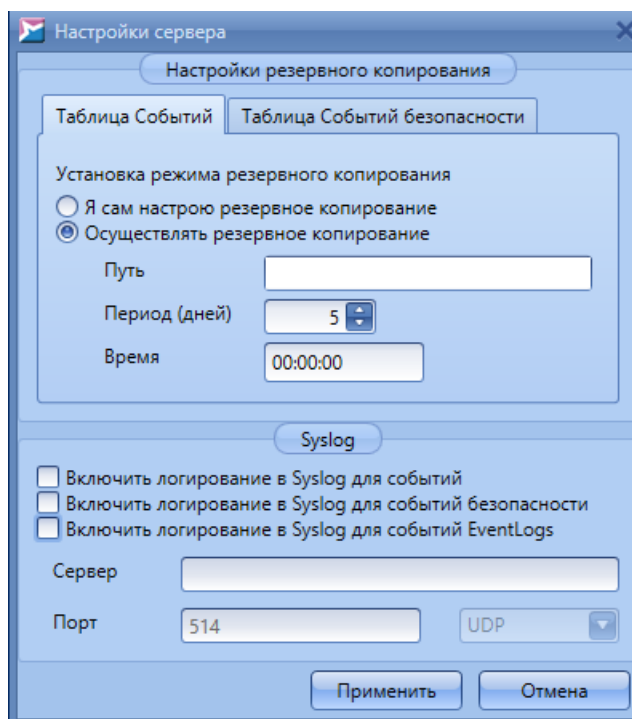


Рисунок 145. Резервное копирование событий



Вы также можете настроить резервное копирование с помощью сторонних средств, без использования инструментов SoftControl Service Center. В этом случае в окне **Настройки сервера** (см. [выше](#)<sup>168</sup>) выберите пункт **Я сам настрою резервное копирование**.

#### 4.9.9 Отправка событий по протоколу Syslog

Вы можете отправлять события на сторонний сервер по протоколу Syslog. Для этого выберите команду **Настройки сервера** в меню **Файл** SoftControl Admin Console.

В области **Syslog** отметьте флажками необходимые варианты:

- Включить логирование в Syslog для событий – все события клиентских устройств (**Event**),
- Включить логирование в Syslog для событий безопасности – все события по управлению системой SoftControl (**SecurityEvent**),
- Включить логирование в Syslog для событий EventLogs – все события из отслеживаемых журналов событий Windows на устройствах (**EventLog**).

Затем введите имя сервера, номер порта и выберите тип протокола.

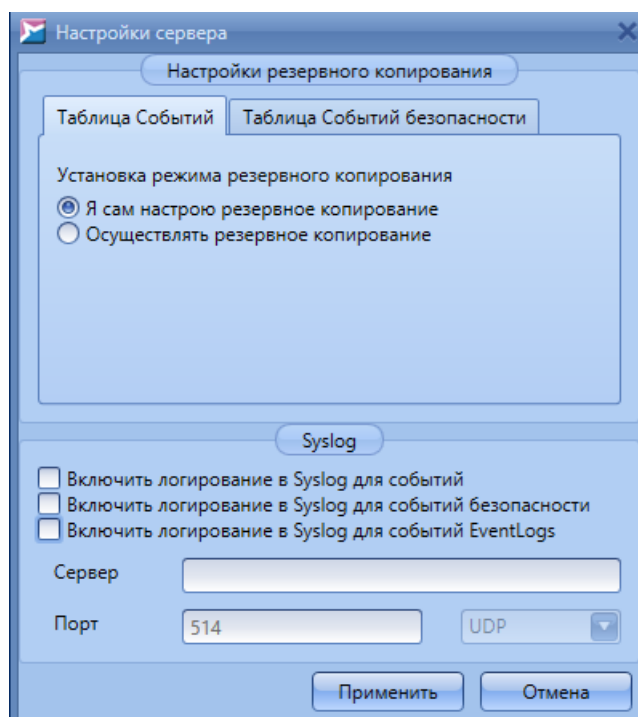


Рисунок 146. Настройки для Syslog

Сообщения для отправки на сторонний сервер с использованием протокола Syslog соответствуют стандарту RFC 5424. Основные сведения о событии находятся внутри

элемента Syslog-сообщения STRUCTURED-DATA. Дополнительную информацию вы можете найти в статьях:

- [http://kb.safensoft.com/index.php/Sending\\_events\\_with\\_Syslog\\_protocol](http://kb.safensoft.com/index.php/Sending_events_with_Syslog_protocol) – элементы Syslog-сообщений;
- [http://kb.safensoft.com/index.php/Information\\_about\\_SoftControl\\_events](http://kb.safensoft.com/index.php/Information_about_SoftControl_events) – события SoftControl.

## 4.10 Оповещения о событиях

Оповещения (нотификации) о событиях, регистрируемых в Сервисном Центре, позволяют администратору оперативно реагировать на возникающие угрозы, даже в случае отсутствия за штатной рабочей станцией с установленной консолью управления SoftControl Admin Console.

Первоначально необходимо задать [контактные данные](#)<sup>(170)</sup> получателей оповещений, после чего настроить [параметры отправки](#)<sup>(171)</sup>.

### 4.10.1 Контакты

На вкладке **Контакты** производится задание адресатов – получателей нотификаций (рис. [Вкладка «Контакты»](#)<sup>(170)</sup>).

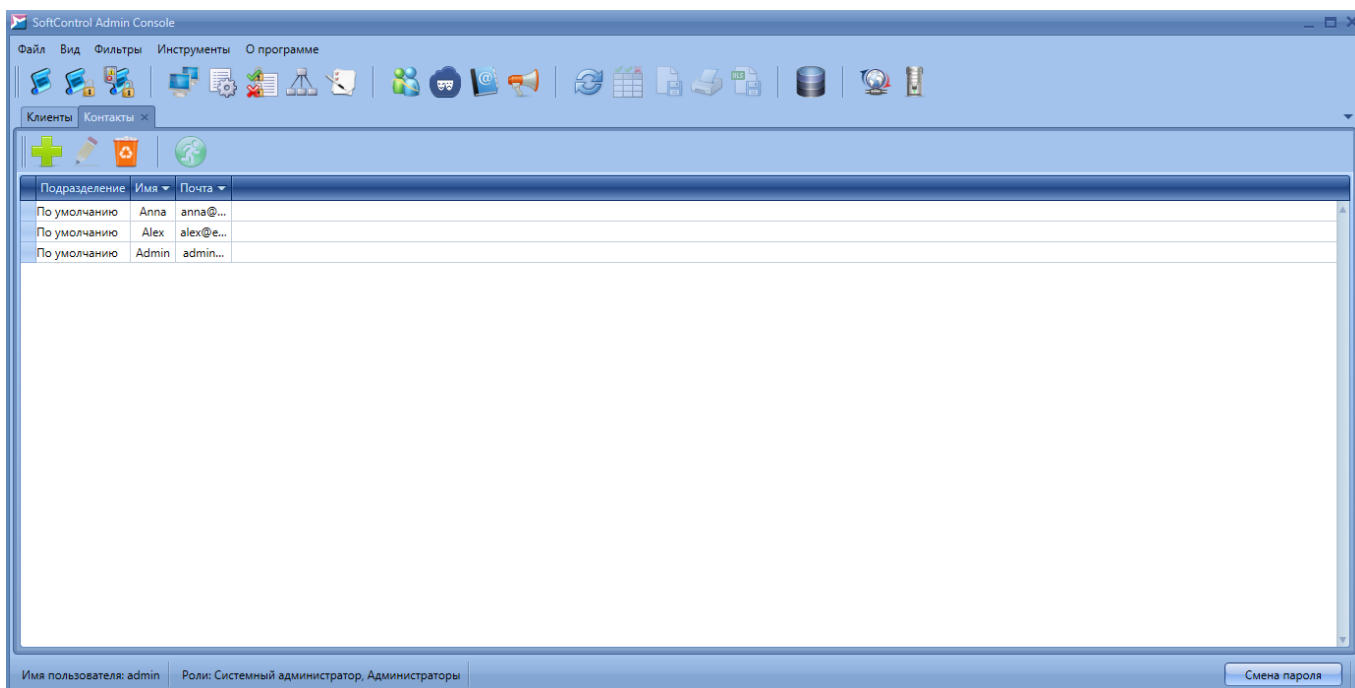






Рисунок 147. Вкладка «Контакты»

Основные операции с контактами осуществляются с помощью графических кнопок

вкладки, предназначение которых приведено в табл. 28.

Таблица 28. Элементы управления вкладки «Контакты»

Кнопка	Название	Описание
	Добавить	Создание нового контакта.
	Редактировать	Редактирование свойств выбранного контакта.
	Удалить	Удаление выбранных контактов.
	Переместить	Перемещение выбранного контакта в другое подразделение.

Перечень полей вкладки приведен в табл. 29.

Таблица 29. Поля вкладки «Контакты»

Поле	Описание
Подразделение	Подразделение, к которому принадлежит данный контакт.
Имя	Имя получателя.
Почта	Адрес электронного почтового ящика получателя.

Чтобы добавить нового получателя, нажмите на кнопку **Создать** (рис. [Вкладка «Контакты»](#)<sup>(170)</sup>). В появившемся окне укажите данные получателя в полях **Имя** и **Электронная почта** и нажмите на кнопку **Применить** (рис. [Добавление контакта](#)<sup>(171)</sup>).

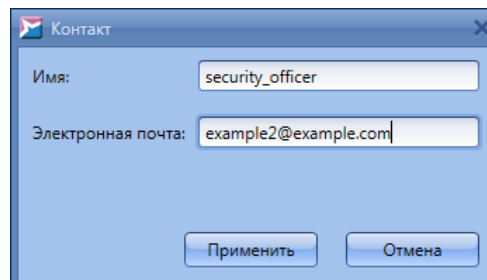


Рисунок 148. Добавление контакта

Для правки и удаления контактов воспользуйтесь соответствующими кнопками.

## 4.10.2 Нотификации

Вкладка **Управление нотификациями** предназначена для настройки параметров отправки оповещений о событиях посредством электронной почты (рис. [Вкладка «Управление нотификациями»](#)<sup>(171)</sup>).

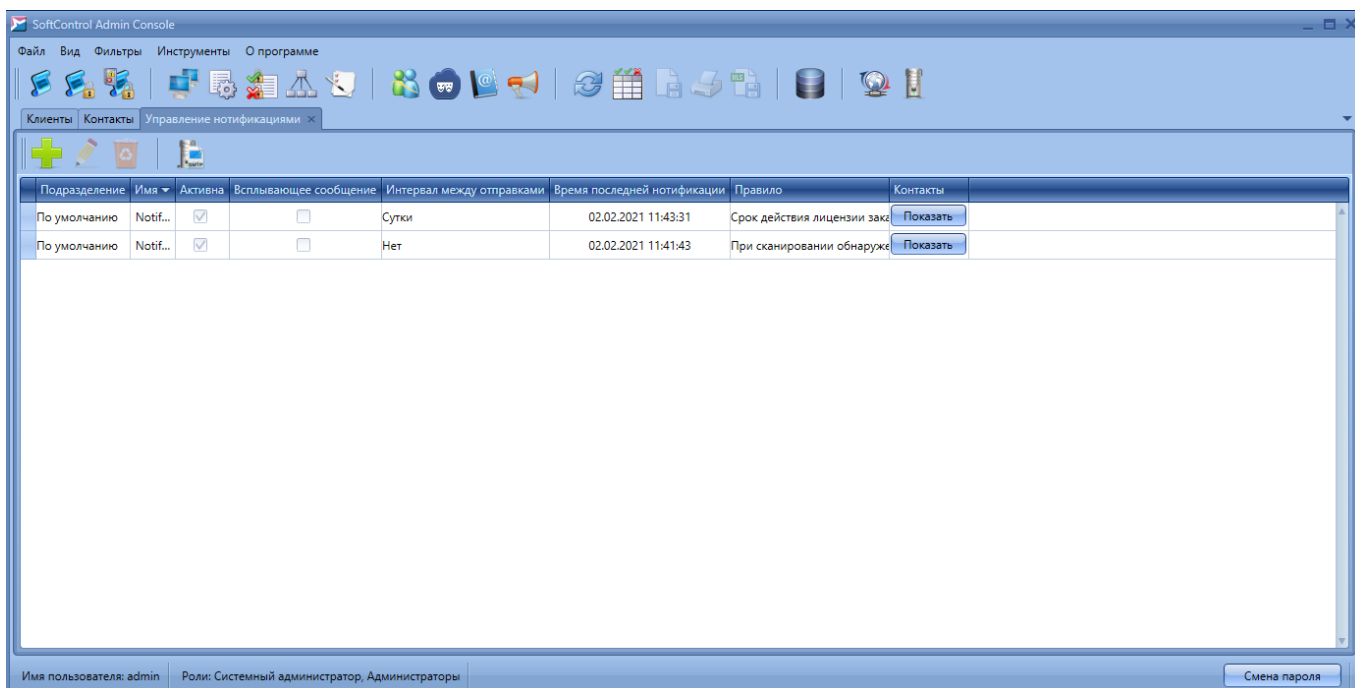


Рисунок 149. Вкладка «Управление уведомлениями»

Основные операции с уведомлениями осуществляются с помощью графических кнопок вкладки, предназначение которых приведено в табл. 30.

Таблица 30. Элементы управления вкладки «Управление уведомлениями»

Кнопка	Название	Описание
	Создать	Создание новой нотификации.
	Редактировать	Редактирование выбранной нотификации.
	Удалить	Удаление выбранных нотификаций.
	SMTP	Настройка SMTP-сервера.

Перечень полей вкладки приведен в табл. 31.

Таблица 31. Поля вкладки «Управление уведомлениями»

Поле	Описание
Подразделение	Подразделение, к которому относится данная нотификация. Перемещение нотификаций между подразделениями не поддерживается. Каждой нотификации назначается то подразделение, к которому принадлежит создавший ее пользователь.
Имя	Наименование нотификации.
Активна	Флажок состояния нотификации.
Всплывающее сообщение	Флажок, указывающий, отображается ли всплывающее уведомление при отправке нотификации.
Интервал между отправками	Минимальный временной интервал после отправки предыдущей нотификации, по истечении которого возможна отправка следующей.

Поле	Описание
Время последней нотификации	Время отправки последней нотификации.
Правило	Условия отправки нотификации.
Контакты	Список адресатов электронного письма с нотификацией.

Основные действия, выполняемые на данной вкладке:

#### ▼ Настройка SMTP-сервера

Для работы нотификаций необходимо предварительно настроить параметры сервера исходящей почты по протоколу SMTP, для этого нажмите на кнопку **SMTP** (рис. [Вкладка «Управление нотификациями»](#)<sup>(171)</sup>).

В окне **Настройка почтового сервера** введите в поле **Почтовый сервер** адрес почтового сервера, с электронного ящика которого предполагается отправка нотификаций, а также **Номер порта** для отправки (рис. [Настройка почтового сервера](#)<sup>(173)</sup>). В полях **Логин**, **Пароль** и **Почтовый ящик** введите данные учетной записи и адрес почтового ящика, с которого предполагается отправка нотификаций. Установите флажок **Использовать SSL** для криптографической защиты при передаче данных.

Чтобы проверить работоспособность введенных настроек, нажмите на кнопку **Отправить тестовое письмо**.

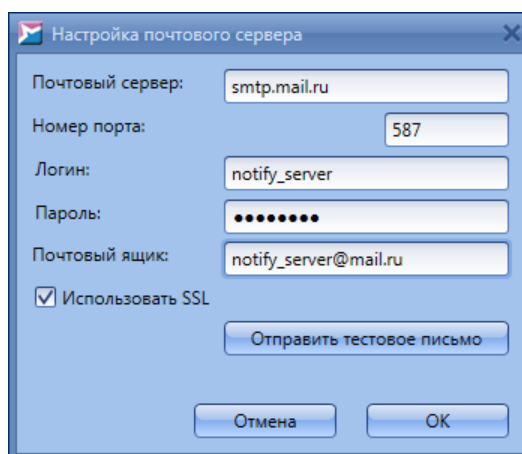


Рисунок 150. Настройка почтового сервера

Нажмите на кнопку **OK** для применения настроек.

#### ▼ Создание нотификации

Чтобы добавить новую нотификацию, нажмите на кнопку **Создать** (рис. [Вкладка «Управление нотификациями»](#)<sup>(171)</sup>).

В появившемся окне на вкладке **Общие** укажите **Имя** нотификации, выберите минимальный **Интервал между отправками** в выпадающем списке, введите **Тему** письма и установите флажок **Активировать** (рис. [Общие параметры нотификации](#)<sup>(174)</sup>).

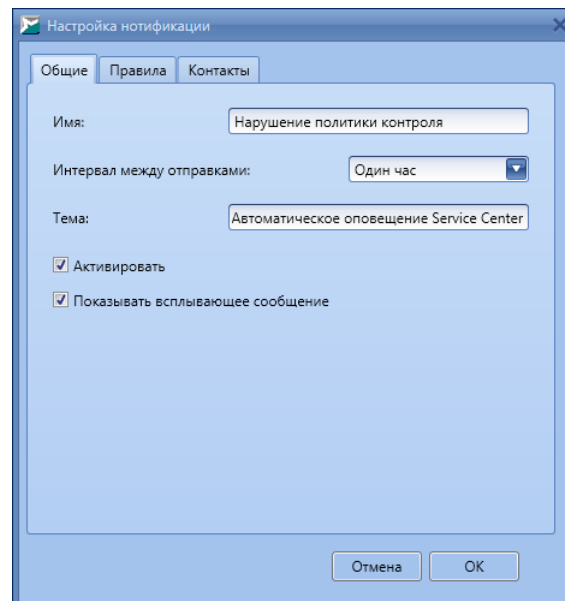


Рисунок 151. Общие параметры нотификации

Чтобы **Показывать всплывающее сообщение** при отправке нотификации, установите соответствующий флажок. В этом случае после отправки нотификации будет отображаться всплывающее уведомление с заголовком оповещения.

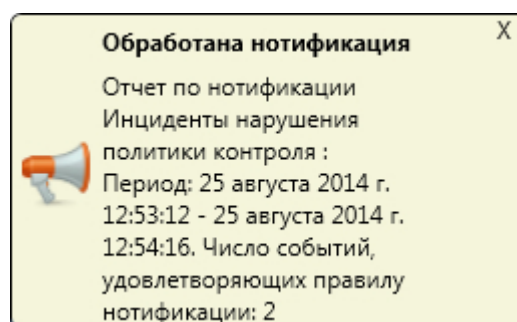


Рисунок 152. Всплывающее уведомление

На вкладке **Правила** выберите условие, при наступлении которого будет производиться отправка нотификации (рис. [Условия срабатывания отправки нотификации](#)<sup>(174)</sup>):

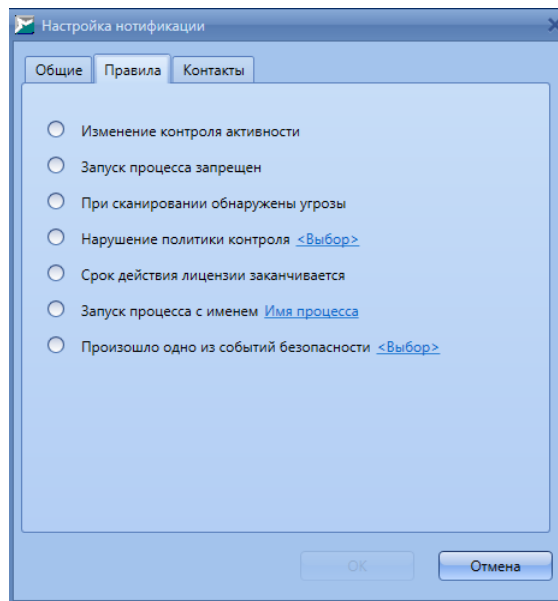


Рисунок 153. Условия срабатывания отправки нотификации

○ **Изменение контроля активности:**

Изменение статусов контроля активности компонента SoftControl SysWatch по любой из областей.

○ **Запуск процесса запрещен:**

Регистрация события типа **Запуск процесса** компонентом SoftControl SysWatch с решением «запрещено».

○ **При сканировании обнаружены угрозы:**

Обнаружение вредоносного кода в процессе антивирусной проверки компонентом SoftControl SysWatch.

○ **Нарушение политики контроля:**

Регистрация компонентом SoftControl SysWatch одного или нескольких событий типа **Нарушение политики контроля**, выбираемых по ссылке **<Выбор>** (рис. [Выбор типов политик контроля для отправки нотификации](#)<sup>(175)</sup>).

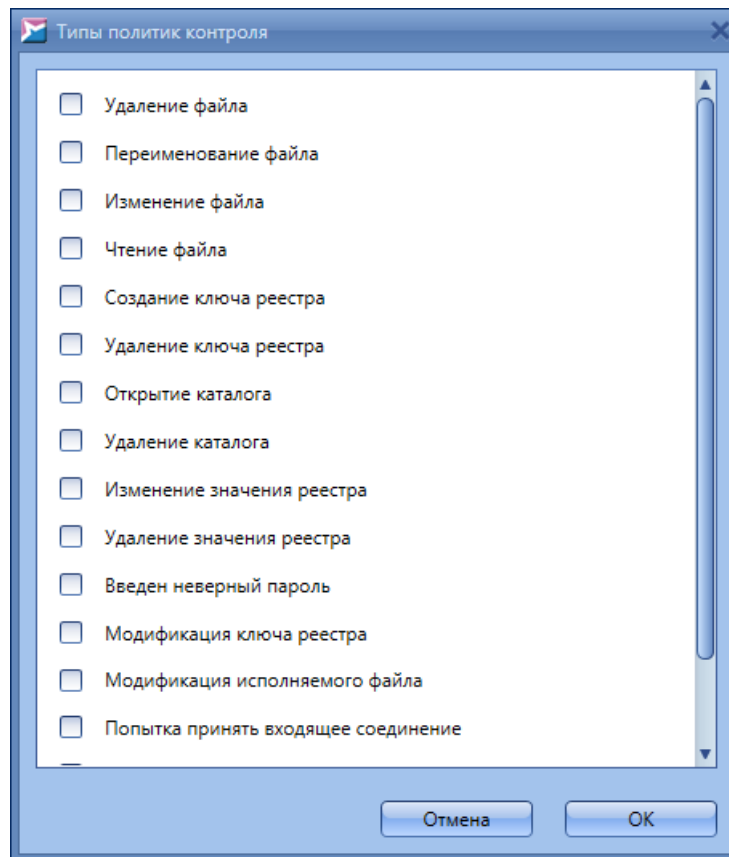


Рисунок 154. Выбор типов политик контроля для отправки нотификации

○ **Срок действия лицензии заканчивается:**

До конца срока действия лицензионного ключа клиентского компонента остается меньше 10 дней.

---

**i** Рекомендуется устанавливать значение параметра **Интервал между отправками** для данной нотификации не менее 4 часов.

---

○ **Запуск процесса с именем:**

Регистрация события типа **Запуск процесса** с именем, заданным по ссылке **Имя процесса**, компонентом SoftControl SysWatch.

○ **Произошло одно из событий безопасности:**

Обнаружение компонентом SoftControl SysWatch одного или нескольких событий безопасности, выбираемых по ссылке **<Выбор>** (рис. [Выбор событий безопасности для отправки нотификации](#)<sup>(176)</sup>).



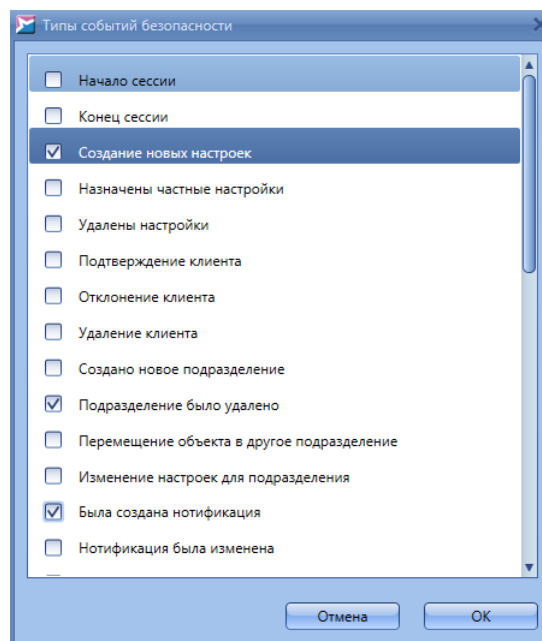


Рисунок 155. Выбор событий безопасности для отправки нотификации

На вкладке **Контакты** отметьте адресатов отправки нотификации (рис. [Выбор получателей нотификации](#)<sup>(177)</sup>).

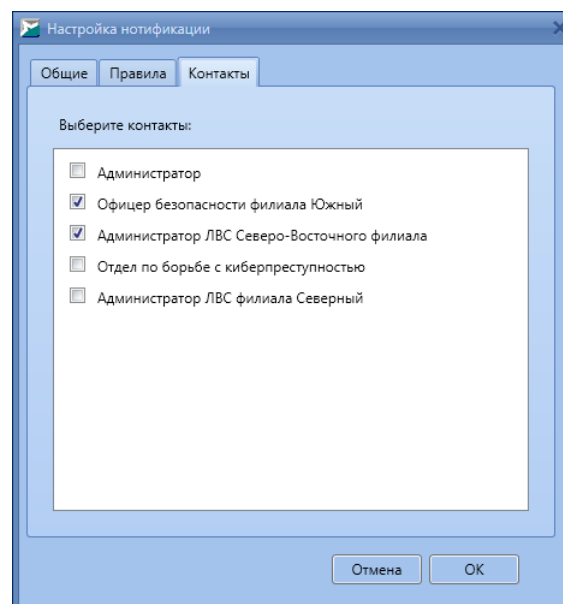


Рисунок 156. Выбор получателей нотификации

Нажмите на кнопку **ОК**, чтобы подтвердить создание нотификации.

#### ▼ Изменение свойств нотификации

Чтобы изменить свойства нотификации, выберите ее и выполните одно из следующих действий:

- нажмите на кнопку **Редактировать** в группе кнопок вкладки (рис. [Вкладка](#)

[«Управление нотификациями»<sup>\(171\)</sup>](#));

- дважды нажмите левой кнопки мыши на нотификации.

В появившемся окне измените необходимые параметры аналогично работе с новой нотификацией (рис. [Общие параметры нотификации<sup>\(174\)</sup>](#), [Условия срабатывания отправки нотификации<sup>\(174\)</sup>](#), [Выбор получателей нотификации<sup>\(177\)</sup>](#)).

Нажмите на кнопку **ОК**, чтобы подтвердить изменения.

#### ▼ Отключение и удаление нотификации

Если необходимо отключить получение нотификации без ее удаления из списка, вызовите окно редактирования свойств, сбросьте флажок **Активировать** на вкладке **Общие** и нажмите на кнопку **ОК** (рис. [Общие параметры нотификации<sup>\(174\)</sup>](#)).

Для удаления нотификации выберите ее, нажмите на кнопку **Удалить** (рис. [Вкладка «Управление нотификациями»<sup>\(171\)</sup>](#)) и подтвердите удаление в диалоговом окне.

## 4.11 Снимки конфигурации

Вкладка **Снимки конфигурации** предназначена для создания снимков конфигурации любого подключенного клиентского хоста. Снимок конфигурации – это профиль компьютера с установленным клиентским приложением SoftControl SysWatch. SoftControl Admin Console также позволяет сравнить снимок с текущим состоянием выбранных клиентских хостов.

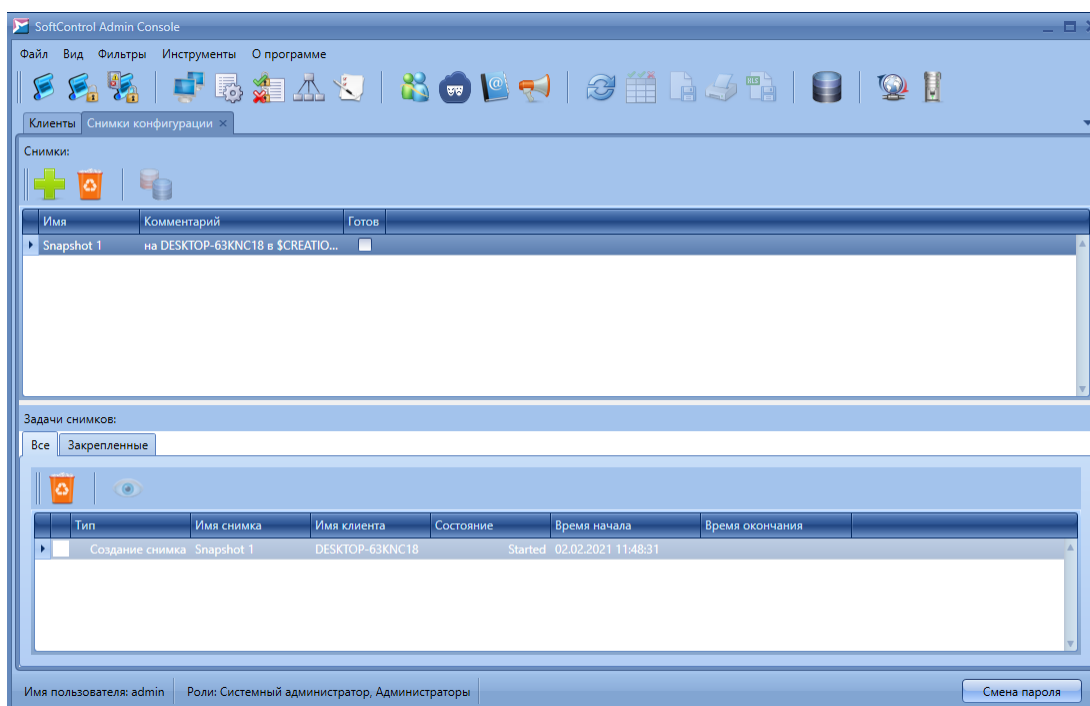


Рисунок 157. Вкладка «Снимки конфигурации»

**i** Кнопка **Снимки конфигурации** доступна только для пользователей, у которых есть все перечисленные ниже разрешения: **Просматривать клиентов, подключенных к серверу, Создавать новые задачи для клиентов, Просматривать существующие подразделения.**

Вкладка состоит из двух разделов:

- [СНИМКИ](#)<sup>179</sup>,
- [задачи снимков](#)<sup>182</sup>.

#### 4.11.1 Снимки

Основные операции со снимками в разделе **Снимки** осуществляются с помощью графических кнопок вкладки, предназначение которых приведено в табл. 32.

Таблица 32. Элементы управления раздела «Снимки»

Кнопка	Название	Описание
	Добавить	Создание нового снимка конфигурации.
	Удалить	Удаление выбранного снимка.
	Сравнить	Сравнение созданного снимка с профилем клиентского хоста.

Перечень полей раздела приведен в табл. 33.

Таблица 33. Поля раздела «Снимки»

Поле	Описание
Имя	Наименование задачи.
Комментарий	Текстовый комментарий. По умолчанию указывается имя клиентского хоста и время создания снимка.
Готов	Индикатор завершения задачи. В данном поле выставляется галочка для снимков после получения ответа от клиентского хоста.

Основные действия, выполняемые на данной вкладке:

#### ▼ Создание снимка

Чтобы создать снимок конфигурации, нажмите на кнопку **+** (**Добавить**) (рис. [Вкладка «Снимки конфигурации»](#)<sup>178</sup>). В появившемся окне укажите имя снимка и комментарий, выберите клиентский хост, с которого требуется сделать снимок, и нажмите на кнопку **Создать** (рис. [Создание снимка](#)<sup>180</sup>). После этого генерируется задача по созданию снимка, и в [таблице](#)<sup>182</sup> в разделе **Задачи снимков** появляется соответствующая запись.

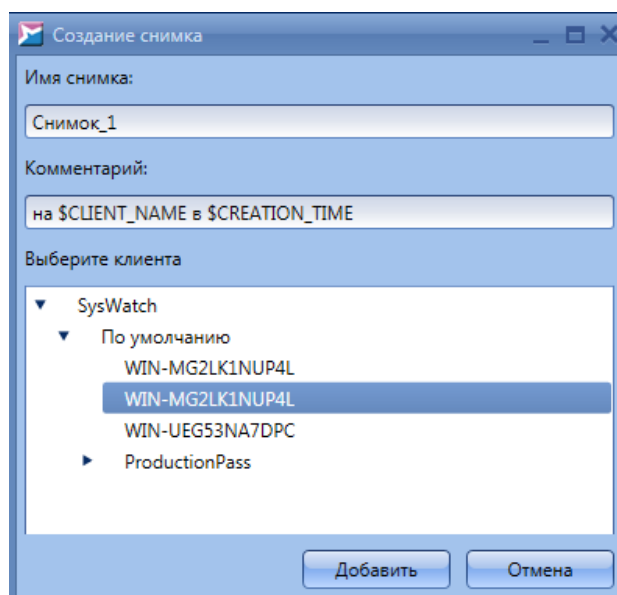



Рисунок 158. Создание снимка

В комментарии по умолчанию используются следующие макросы: \$CLIENT\_NAME и \$CREATION\_TIME. При создании задачи они автоматически заменяются на имя клиентского хоста и время создания задачи соответственно.

До того как будет получен ответ от клиентского хоста, статус задачи в таблице в разделе **Задачи снимков** (см. [ниже](#))<sup>182</sup> помечается как **Started**. После получения

ответа снимок помечается как **Готов** (в соответствующем столбце [таблицы](#)<sup>(180)</sup> выставляется галочка), а задача по получению снимка становится завершенной (в таблице статус задачи сменяется на **Finished**).

#### ▼ Сравнение снимков конфигурации

Чтобы сравнить снимок конфигурации с текущим состоянием выбранного клиентского хоста, выберите снимок и нажмите на кнопку  (**Сравнить**) (рис. [Вкладка «Снимки конфигурации»](#)<sup>(178)</sup>). В появившемся окне выберите клиентский хост (или несколько хостов) и нажмите на кнопку **Создать** (рис. [Выбор клиентских хостов для сравнения](#)<sup>(181)</sup>). Если для сравнения выбрано несколько клиентских хостов, для каждого из них создается отдельная задача сравнения.

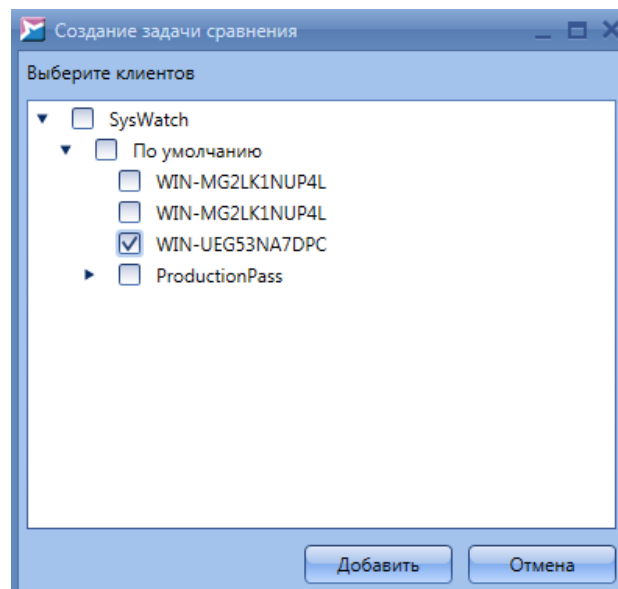



Рисунок 159. Выбор клиентских хостов для сравнения



Для сравнения можно использовать только снимки со статусом **Готов**.

#### ▼ Удаление снимка

Для удаления снимка выберите его, нажмите на кнопку  (**Удалить**) (рис. [Вкладка «Снимки конфигурации»](#)<sup>(178)</sup>) и подтвердите удаление в диалоговом окне.





Удалить можно только те снимки, с которыми не связана ни одна задача. Если для данного снимка имеются связанные с ним задачи, то для его удаления необходимо сначала удалить эти задачи.

### 4.11.2 Задачи снимков

Раздел **Задачи снимков** содержит список задач, выполняемых на вкладке **Снимки конфигурации** (создание снимков и их сравнение), и состоит из двух вкладок: **Все** и **Закрепленные**.

Основные операции с задачами осуществляются с помощью графических кнопок вкладки, предназначение которых приведено в табл. 34.


Таблица 34. Элементы управления раздела «Задачи снимков», вкладка «Все»

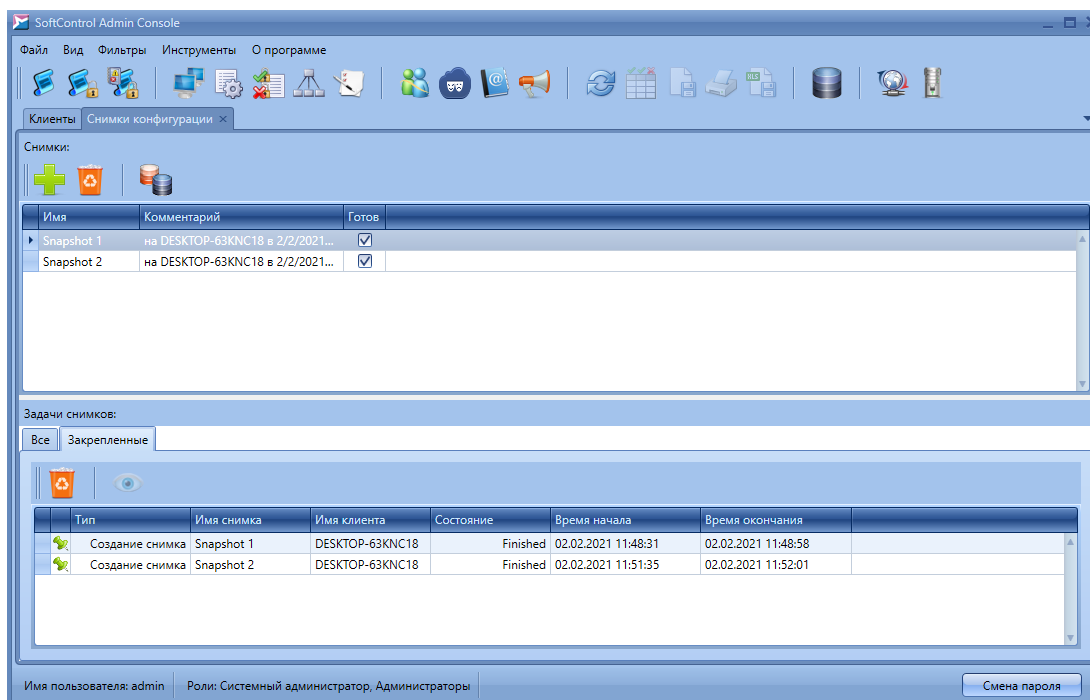
Кнопка	Название	Описание
	Удалить	Удаление выбранного снимка.
	Показать результаты	Просмотреть результаты сравнения снимка конфигурации и профиля клиентского хоста.


Перечень полей вкладки приведен в табл. 35.

Таблица 35. Поля раздела «Задачи снимков», вкладка «Все»

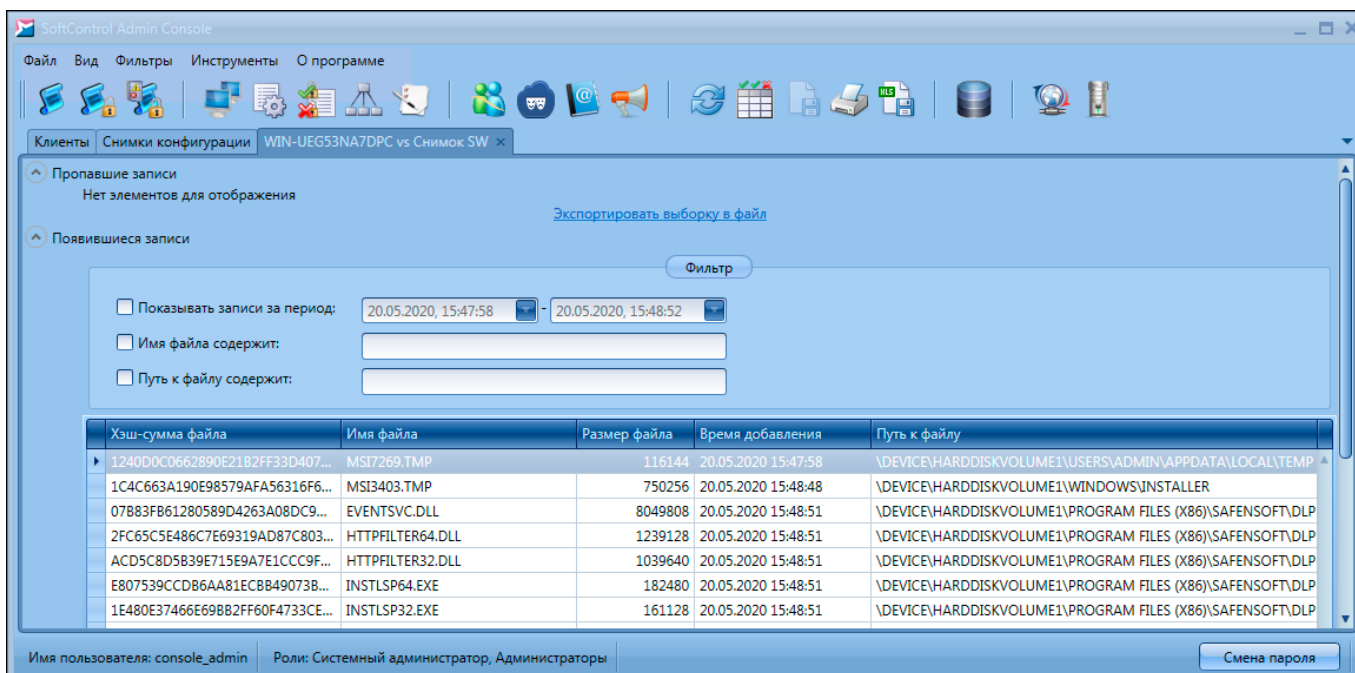
Поле	Описание
Тип	Тип задачи: <b>Создание снимка</b> или <b>Сравнение снимков</b> .
Имя снимка	Наименование задачи, заданное в разделе <b>Снимки</b> .
Имя клиента	Наименование клиентского хоста.
Состояние	Состояние задачи: <b>Started, Finished</b>
Время начала	Время начала задачи
Время окончания	Время окончания задачи

Для закрепления требуемой задачи выберите ее в таблице и щелкните левой кнопкой мыши по левой (пустой) ячейке таблицы. После этого в данной ячейке появляется иконка , задача становится **Закрепленной** и появляется в таблице на вкладке **Закрепленные** (рис. [Закрепленные задачи](#)<sup>182</sup>). Задачи, которые не были закреплены, удаляются через 180 дней после их завершения.

**Рисунок 160. Закрепленные задачи**

Чтобы просмотреть результаты сравнения снимка с текущей конфигурацией клиентского хоста, выберите требуемую задачу сравнения и нажмите на кнопку  (**Показать результаты**). Открывшаяся вкладка **Результаты сравнения** содержит два поля: **Пропавшие записи** и **Появившиеся записи** (рис. [Результаты сравнения снимков](#)<sup>183</sup>).

При необходимости хэш-суммы можно копировать, вызывая контекстное меню нажатием правой кнопки мыши.



**Рисунок 161. Результаты сравнения снимков**

Для просмотра изменений за определенный период времени выберите требуемые даты в поле **Фильтр**. Вы также можете указать в фильтре часть имени файла и пути к нему. Внизу каждого из разделов есть гиперссылка **Экспортировать выборку в файл**. Нажмите на нее, чтобы создать файл XML с выбранными записями.



## 5. Обновление компонентов СИБ

SoftControl Service Center предоставляет возможность централизованного обновления всех компонентов системы с сервера обновлений. Это может быть либо сервер SoftControl, либо сервер, развернутый на предприятии. Вкладка **Обновления** позволяет произвести настройку и просмотреть историю обновлений (рис. [Вкладка «Обновления» для программных модулей](#)<sup>185</sup>, [Вкладка «Обновления» для антивирусных баз](#)<sup>189</sup>).

В верхней части вкладки представлено две категории настроек для обновления соответствующих компонентов:

- [Программные модули](#)<sup>185</sup>,
- [Антивирусные базы](#)<sup>189</sup>.

В нижней части вкладки представлена история обновлений, содержащая список выполняемых операций. Перечень полей списка приведен в табл. 36.

Таблица 36. Поля списка истории обновлений

Поле	Описание
Последняя проверка	Дата и время последней проверки наличия обновлений.
Последнее обновление	Дата и время последней установки обновлений.
Компонент	Название обновляемого компонента.
Статус обновления	Состояние обновления: <ul style="list-style-type: none"> <li>• Обновление не требуется;</li> <li>• Доступно обновление;</li> <li>• Обновление загружено;</li> <li>• Обновление установлено;</li> <li>• Ошибка обновления.</li> </ul>
Размер обновления	Размер обновления в байтах.
Актуальная версия	Текущая версия установленного компонента.
Новая версия	Версия компонента, доступная к обновлению.
Детали	Дополнительная информация.

### 5.1 Настройка обновления программных модулей

Данная категория настроек позволяет настраивать и управлять обновлением программных модулей компонентов SoftControl Service Center, а также скачиванием обновлений программных модулей клиентских компонентов SoftControl SysWatch, SoftControl DLP Client и SoftControl SysCmd с внешних (Интернет) серверов.

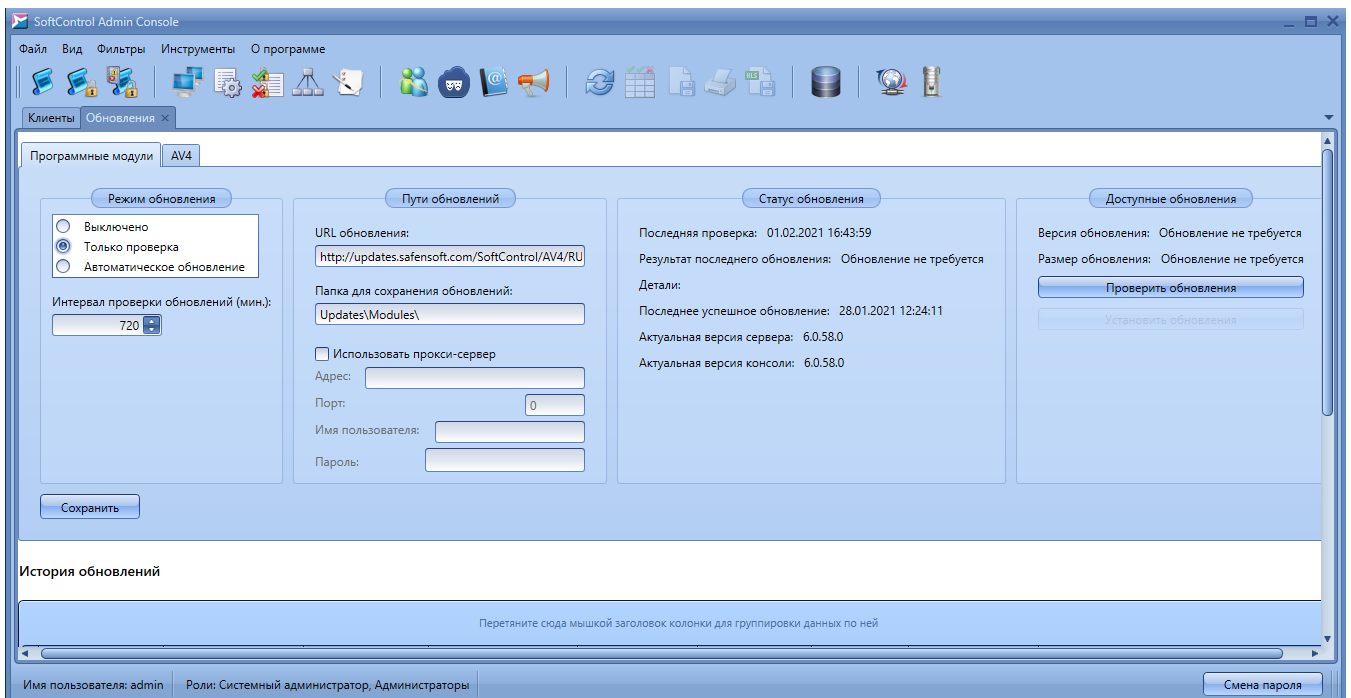


Рисунок 162. Вкладка «Обновления» для программных модулей

#### ▼ Настройка режима обновления

В секции **Режим обновления** возможен выбор трех режимов работы:

- **Выключено:**

Обновление в автоматическом режиме отключено.

- **Только проверка:**

SoftControl Service Center автоматически проверяет наличие обновлений на внешних серверах с периодичностью, указанной в счетчике **Интервал проверки обновлений (мин.)**, но не загружает и не устанавливает их.

- **Автоматическое обновление:**

SoftControl Service Center автоматически проверяет наличие обновлений на внешних серверах с периодичностью, указанной в счетчике **Интервал проверки обновлений (мин.)** и в случае нахождения более новых версий, чем установленные, происходит скачивание пакетов обновлений на сервер. Если найдена новая версия SoftControl Service Center, по окончании загрузки установочных пакетов происходит автоматическое обновление компонентов SoftControl Server и SoftControl Admin Console в фоновом режиме на сервере.

**i** При отсутствии доступа в Интернет или в случае возникновения проблем в процессе автоматического обновления, возможно [обновление SoftControl Service Center в ручном режиме](#)<sup>191</sup> при наличии установочного пакета требуемой версии.

---

[Обновление клиентских компонентов](#)<sup>194</sup> осуществляется с созданного локального «зеркала».

#### ▼ Настройка путей обновления и параметров прокси-сервера

В секции **Пути обновления** задаются следующие параметры:

- **URL обновления:**

Ссылка на внешний сервер, по которой SoftControl Service Center проверяет наличие обновлений. В пути необходимо указать номер текущей лицензии:

`http://updates.safensoft.com/<номер_лицензии>/SoftControl/av/ru`

Примечание. Номер лицензии необходимо указать вручную.

- **Папка для сохранения обновлений:**

Путь сохранения пакетов обновления с внешних серверов относительно директории `C:\ProgramData\SoftControl`. Укажите следующую папку:

`Updates\Modules\`

Установите флажок **Использовать прокси-сервер**, если соединение с внешними серверами требуется осуществлять через прокси-сервер. В этом случае задайте его параметры:

- **Адрес:**

IP-адрес или имя хоста прокси-сервера.

- **Порт:**


Номер порта для связи с прокси-сервером (если не указан – используется порт 80 по умолчанию).

- **Имя пользователя:**

Имя пользователя для аутентификации на прокси-сервере.

- **Пароль:**

Пароль для аутентификации на прокси-сервере.

-  Поддерживается базовый (Basic) тип авторизации. Если аутентификация на прокси-сервере не требуется, то поля **Имя пользователя** и **Пароль** следует оставлять пустыми.

#### ▼ Проверка и обновление по запросу

В секции **Доступные обновления** возможно выполнение операций по запросу с помощью следующих кнопок:

- **Проверить обновления:**

Проверка наличия обновлений программных модулей. В случае обнаружения обновлений отображается **Версия обновления** и **Размер обновления** (в байтах).

- **Установить обновления** (для случая, когда SoftControl Server и SoftControl Admin Console установлены на одном компьютере):


Проверка и, в случае обнаружения, скачивание пакетов обновлений с внешних серверов, установка обновлений SoftControl Server и SoftControl Admin Console.

- **Обновить сервер** (для случая, когда SoftControl Server и SoftControl Admin Console установлены на разных компьютерах):

Проверка и, в случае обнаружения, скачивание пакетов обновлений с внешних серверов, установка обновлений серверного компонента (SoftControl Server).

- **Обновить консоль** (для случая, когда SoftControl Server и SoftControl Admin Console установлены на разных компьютерах):

Проверка и, в случае обнаружения, установка обновлений консоли управления (SoftControl Admin Console).

-  После обновления программных модулей настройки SoftControl Server и SoftControl Admin Console, а также пользовательские фильтры SoftControl Admin Console сохраняются. Накопленные события в SoftControl Admin Console хранятся в БД, поэтому при обновлении не затрагиваются.

В секции **Статус обновления** доступна информация по текущей версии и последним проведенным операциям проверки и установки обновлений.

Для применения измененных установок нажмите на кнопку **Сохранить**.

## 5.2 Настройка обновления антивирусных баз

Данная категория настроек позволяет настраивать и управлять скачиванием антивирусных баз клиентского компонента SoftControl SysWatch с внешних (Интернет) серверов (рис. [Вкладка «Обновления» для антивирусных баз](#)<sup>189</sup>).

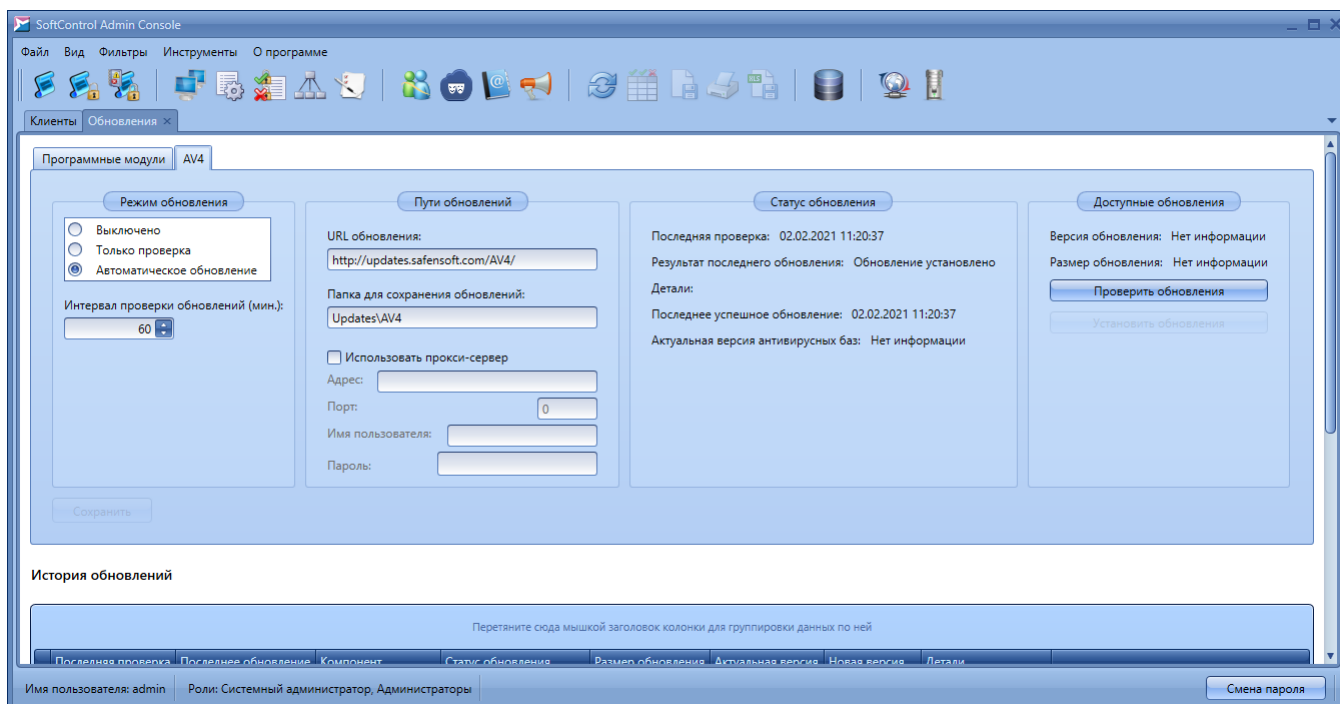


Рисунок 163. Вкладка «Обновления» для антивирусных баз

### ▼ Настройка режима обновления

В секции **Режим обновления** возможен выбор трех режимов работы:

- **Выключено:**

Обновление в автоматическом режиме отключено.

- **Только проверка:**

SoftControl Service Center автоматически проверяет наличие обновлений на внешних серверах с периодичностью, указанной в счетчике **Интервал проверки обновлений (мин.)**, но не загружает их.

- **Автоматическое обновление:**

SoftControl Service Center автоматически проверяет наличие обновлений на внешних серверах с периодичностью, указанной в счетчике **Интервал проверки обновлений (мин.)** и в случае нахождения более новых версий, чем установленные, происходит скачивание обновлений баз на сервер. Обновление антивирусных баз осуществляется в рамках [обновления](#)

[клиентского компонента SoftControl SysWatch<sup>194</sup>](#) с созданного локального «зеркала».

#### ▼ Настройка путей обновления и параметров прокси-сервера

В секции **Пути обновления** задаются следующие параметры:

- **URL обновления:**

Ссылка на внешний сервер, по которой SoftControl Service Center проверяет наличие обновлений. Ссылки для разных антивирусных баз описаны в таблице 37.

**Таблица 37. Адреса обновлений антивирусных баз**

Название	Адрес	Папка для сохранения
Антивирусные базы AV4	http://updates.safensoft.com/ <номер_лицензии>/av4/	Updates\AV4
Антивирусные базы AV5	http://updates.safensoft.com/ <номер_лицензии>/av5/	Updates\AV5

Примечание. Номер лицензии необходимо указать вручную.

- **Папка для сохранения обновлений:**

Путь сохранения пакетов обновления с внешних серверов относительно директории C:\ProgramData\SoftControl. Папки для разных антивирусных баз описаны в табл. 37.

Установите флажок **Использовать прокси-сервер**, если соединение с внешними серверами требуется осуществлять через прокси-сервер. В этом случае задайте его параметры:

- **Адрес:**

IP-адрес или имя хоста прокси-сервера.

- **Порт:**

Номер порта для связи с прокси-сервером (если не указан – используется порт 80 по умолчанию).

- **Имя пользователя:**

Имя пользователя для аутентификации на прокси-сервере.

- **Пароль:**

Пароль для аутентификации на прокси-сервере.



Поддерживается базовый (Basic) тип авторизации. Если аутентификация на

прокси-сервере не требуется, то поля **Имя пользователя** и **Пароль** следует оставлять пустыми.

---

#### ▼ Проверка и обновление по запросу

В секции **Доступные обновления** возможно выполнение операций по запросу с помощью следующих кнопок:

- **Проверить обновления:**

Проверка наличия обновлений антивирусных баз. В случае обнаружения обновлений отображается **Версия обновления** и **Размер обновления** (в байтах).

- **Установить обновления:**

Проверка и, в случае обнаружения, скачивание антивирусных баз с внешних серверов.

В секции **Статус обновления** доступна информация по текущей версии и последним проведенным операциям проверки и установки обновлений.

Для применения измененных установок нажмите на кнопку **Сохранить**.

### 5.3 Обновление SoftControl Server и SoftControl Admin Console в ручном режиме

- 1) Запустите установочный пакет *Service.Center.msi* версии, на которую необходимо произвести обновление.
- 2) В окне **Установка SoftControl Service Center** нажмите на кнопку **Далее** (рис. [Запуск программы обновления](#)<sup>191</sup>).

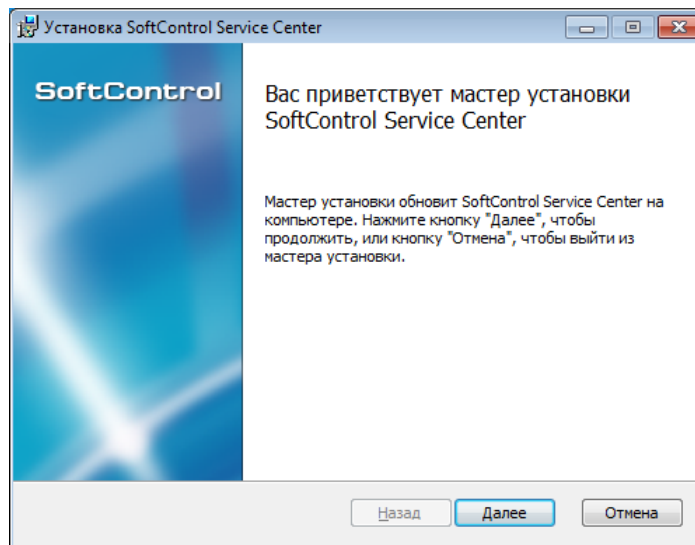


Рисунок 164. Запуск программы обновления

3) В случае вашего согласия, отметьте опцию **Я принимаю условия лицензионного соглашения** и нажмите на кнопку **Далее** (рис. [Лицензионное соглашение](#)<sup>192</sup>).

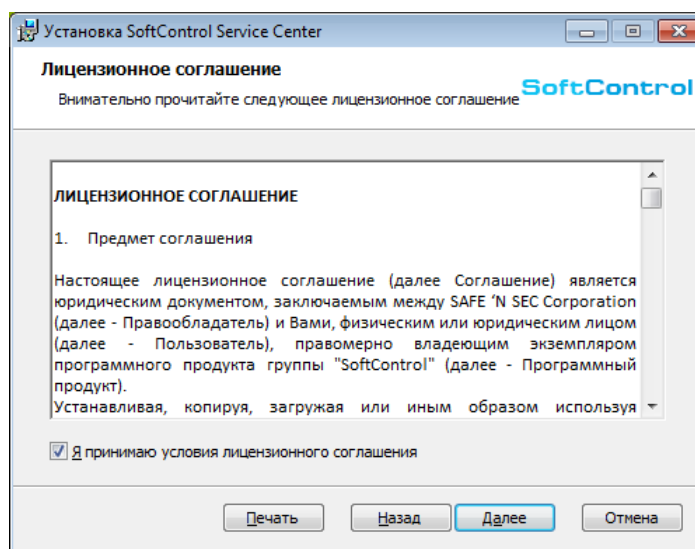


Рисунок 165. Лицензионное соглашение

4) Нажмите на кнопку **Обновить** (рис. [Готовность к обновлению](#)<sup>192</sup>).



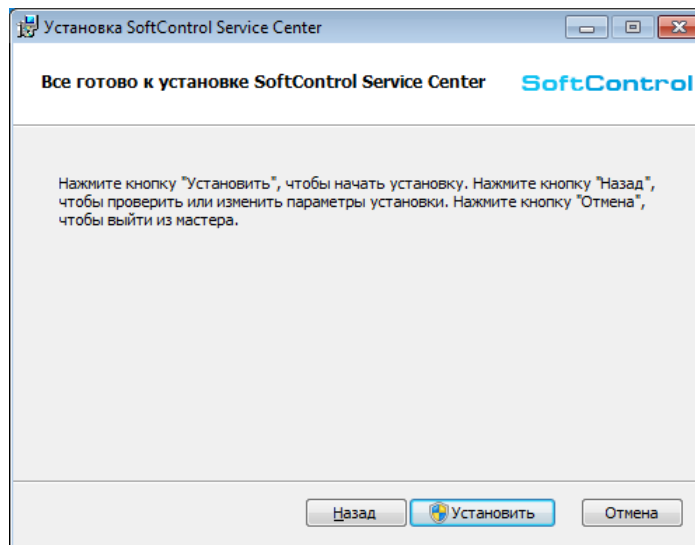


Рисунок 166. Готовность к обновлению

5) Дождитесь окончания процесса обновления (рис. [Процесс обновления](#)<sup>193</sup>).

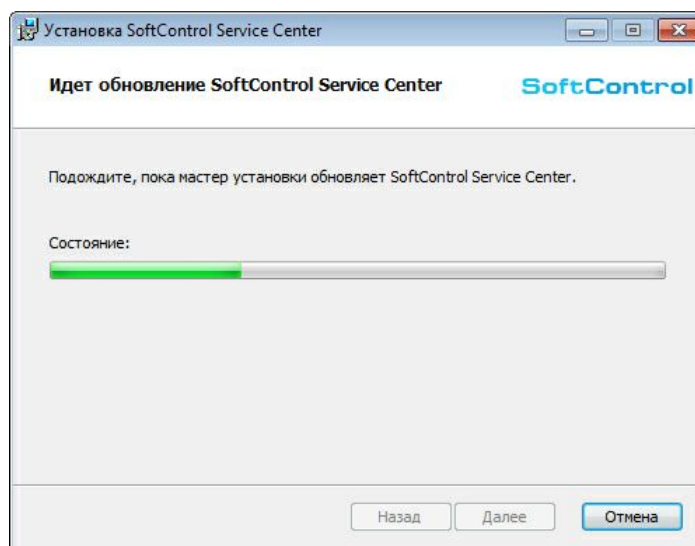


Рисунок 167. Процесс обновления

6) После появления сообщения *Установка SoftControl Service Center завершена* нажмите на кнопку **Готово** (рис. [Завершение обновления](#)<sup>193</sup>).

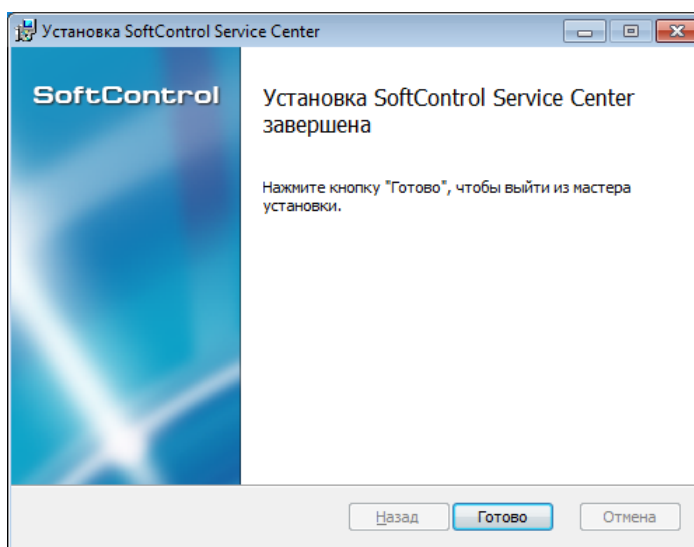


Рисунок 168. Завершение обновления

## 5.4 Обновление клиентских компонентов

После скачивания обновлений с внешних серверов клиентские компоненты могут быть обновлены с SoftControl Service Center следующими способами:

- ❑ После подключения к Сервисному Центру SoftControl SysWatch и SoftControl DLP Client автоматически переключаются в режим обновлений с него. Обновление компонентов производится по запросу посредством создания соответствующей [задачи](#)<sup>(134)</sup> или по расписанию, если оно настроено для [SoftControl SysWatch](#)<sup>(76)</sup> / [SoftControl DLP Client](#)<sup>(123)</sup>.
- ❑ Находясь в автономном режиме работы, SoftControl SysWatch также может быть обновлен с Сервисного Центра. Для этого в настройках источников обновления SoftControl SysWatch через интернет замените предустановленные адреса на соответствующие табл. 38 локальные адреса для необходимых компонентов. Порт связи с сервером по умолчанию – 8088. После применения указанных настроек обновление можно произвести по запросу через ГИП.

Таблица 38. Адреса обновлений с SoftControl Service Center

Компонент	Описание	Адрес
Core	Программные модули	http://<IP-адрес сервера>:<порт связи с сервером>/api/updates/SNS
AV-AV4	Антивирусные базы AV4	http://<IP-адрес сервера>:<порт связи с сервером>/api/updates/AV4
AV-AV5	Антивирусные базы AV5	http://<IP-адрес сервера>:<порт связи с сервером>/api/updates/AV5

## 6. Удаление компонентов SoftControl Service Center

Удаление SoftControl Server и SoftControl Admin Console: в Панели управления Windows в разделе **Программы** (Programs) → **Программы и компоненты** (Programs and Features) выберите *SoftControl Service Center* и нажмите на кнопку **Удалить** (Uninstall).

Удаление одного из компонентов:

- 1) В Панели управления Windows в разделе **Программы** (Programs) → **Программы и компоненты** (Programs and Features) выберите *SoftControl Service Center* и нажмите на кнопку **Изменить** (Change).
- 2) В окне **Установка SoftControl Service Center** нажмите на кнопку **Далее** (рис. [Запуск программы удаления](#)<sup>195</sup>).

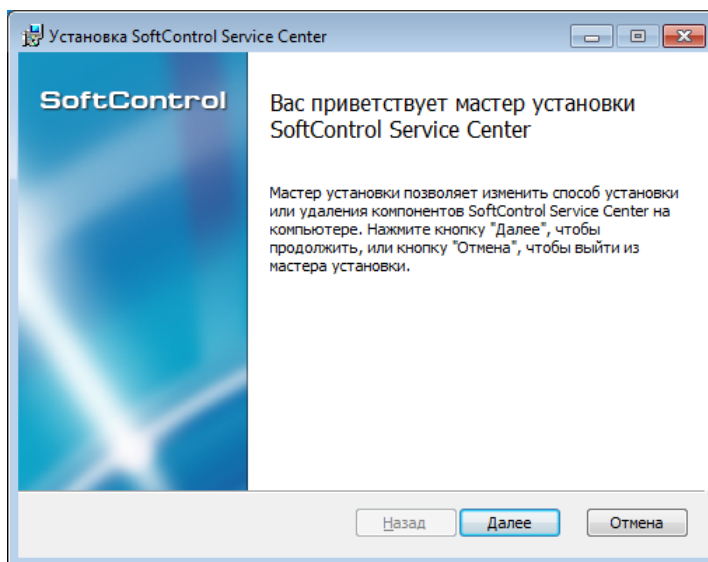


Рисунок 169. Запуск программы удаления

- 3) Выберите операцию **Изменить** (рис. [Типы операций](#)<sup>195</sup>).
- 4) Выберите компонент для удаления (рис. [Выбор компонентов для удаления](#)<sup>196</sup>): нажмите на пиктограмму компонента и в выпадающем меню выберите опцию **Компонент будет полностью недоступен** (рис. [Опции установки компонента](#)<sup>196</sup>). После того как все установки завершены, нажмите на кнопку **Далее**.

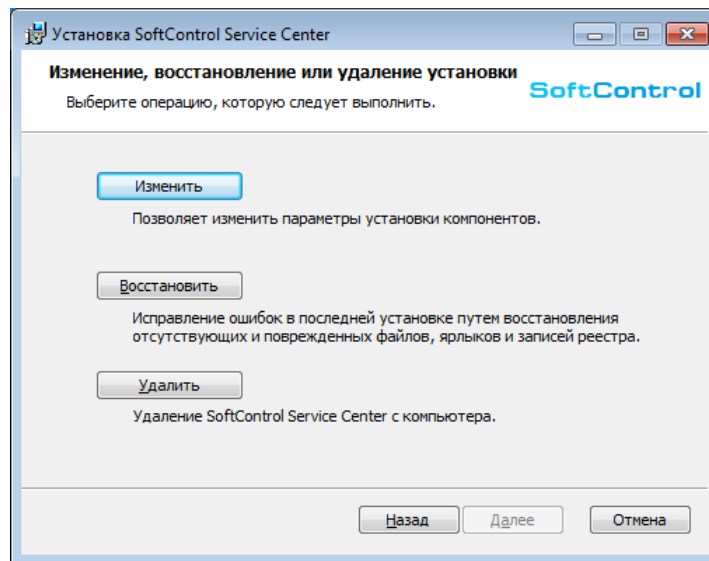


Рисунок 170. Типы операций

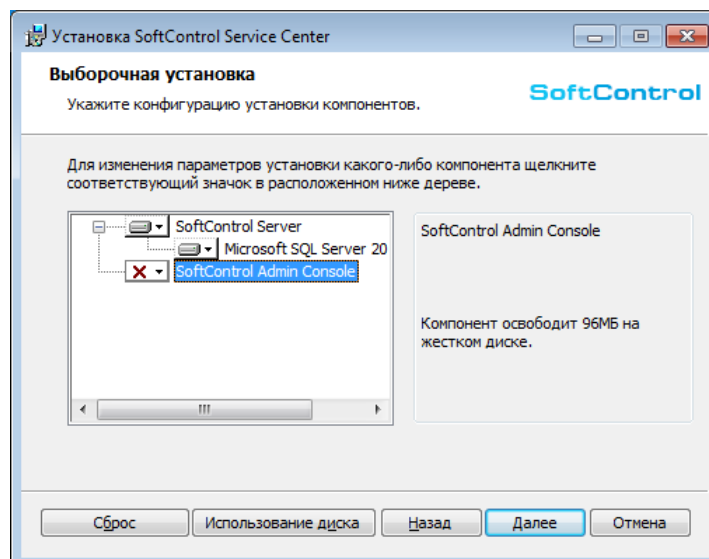


Рисунок 171. Выбор компонентов для удаления

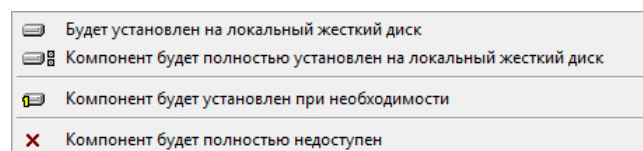


Рисунок 172. Опции установки компонента

5) Нажмите на кнопку **Изменить** (рис. [Готовность к удалению](#)<sup>196</sup>).

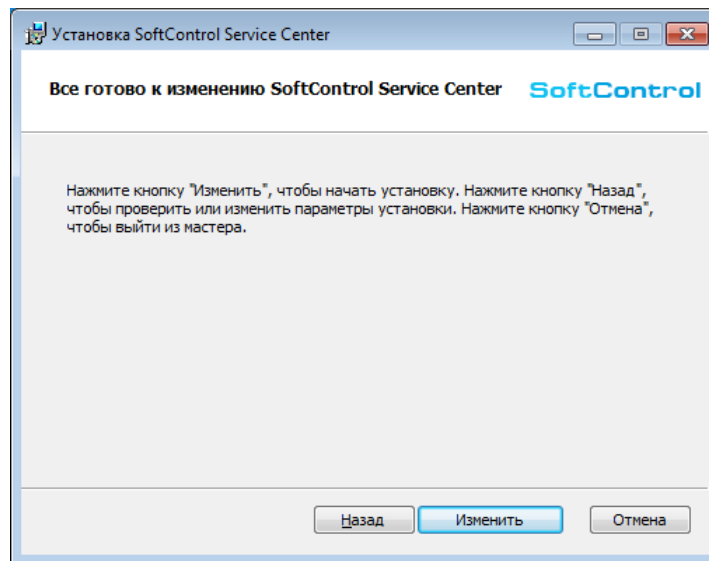


Рисунок 173. Готовность к удалению

6) Дождитесь окончания процесса удаления (рис. [Процесс удаления](#)<sup>197</sup>).

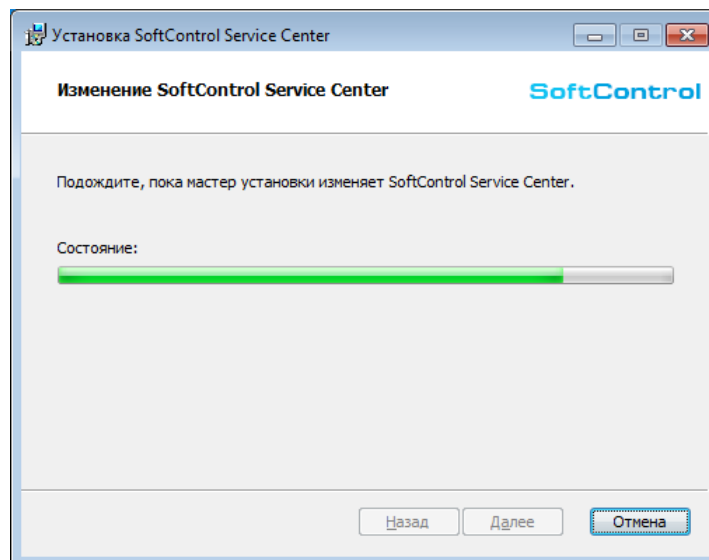


Рисунок 174. Процесс удаления

7) После появления сообщения *Установка SoftControl Service Center завершена* нажмите на кнопку **Готово** (рис. [Завершение удаления](#)<sup>197</sup>).

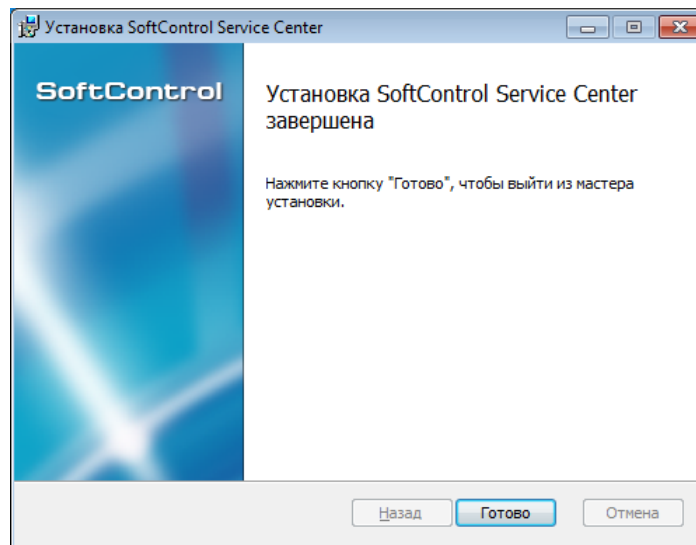


Рисунок 175. Завершение удаления

**i** В случае, если SoftControl Server был установлен со встроенной СУБД (например, была выбрана [полная установка](#)<sup>14</sup>), удаление Microsoft® SQL Server® 2014 Express SP1 необходимо произвести вручную. Для этого выполните удаление следующих элементов СУБД стандартными средствами Windows:

- *Microsoft SQL Server 2014;*
- *Microsoft SQL Server 2012 Native Client;*
- *Microsoft SQL Server 2014 Setup (English);*
- *Microsoft SQL Server 2008 Setup Support Files;*
- *Microsoft SQL Server 2014 Transact-SQL ScriptDom.*

## 7. Диагностика проблем

В случае возникновения проблем при развертывании и функционировании SoftControl Service Center в первую очередь обратитесь к отчету **SafenSoft** в журнале событий Windows. Для этого откройте Панель управления Windows, выберите раздел **Система и безопасность** (System and Security) → **Администрирование** (Administrative Tools), в нем откройте средство **Просмотр событий** (Event Viewer). В открывшемся окне в панели слева разверните категорию **Журналы приложений и служб** (Applications and Services Logs) и в ней выберите журнал **SafenSoft**. При анализе ошибок, предупреждений и уведомлений в данном отчете может быть найдена причина, вызвавшая сбой при установке, запуске и установлении соединения между компонентами. Если определить причину самостоятельно невозможно, приложите файлы текстовых отчетов компонентов к запросу в [техническую поддержку ООО «АРУДИТ СЕКЬЮРИТИ»](#). <sup>203</sup> Список необходимых файлов приведен в табл. 39.

Таблица 39. Текстовые отчеты компонентов SoftControl Service Center

Название	Имя файла	Путь	Краткое описание	Авторотация по умолчанию	Управление авторотацией
<b>Логи Service Center</b>					
Лог Service Center	ServerDetailedLog.txt	C:\Program Files (x86)\SafenSoft\Service Center\Server\logs\	Лог Service Center	При превышении размера 209715200 создается новый файл	Через файл SafenSoft.Enterprise.Server.exe.nlog
Журнал обновлений	checks.log	C:\Program Files(x86)\Safensoft\Service Center\Server\Tools\Updates\Reports\	Лог проверок наличия обновлений	—	—
Журнал обновлений	sns.log	C:\Program Files(x86)\Safensoft\Service Center\Server\Tools\Updates\Reports\	Журнал обновления модулей	—	—
Журнал обновлений	[av_name].log	C:\Program Files(x86)\Safensoft\Service Center\Server\Tools\Updates\Reports\	Лог обновления антивируса, вместо av_name имя антивируса (av4, av5)	—	—
Журнал обновлений	root.log	C:\Program Files(x86)\Safensoft\Service Center\Server\Tools\Updates\Reports\	Сборный лог, в который дублируются записи sns.log и [av_name].log	—	—
<b>Логи Admin Console</b>					
Лог Admin Console	ConsoleDetailedLog.txt	C:\ProgramData\SafenSoft\	Лог Admin Console	—	—

Название	Имя файла	Путь	Краткое описание	Авторотация по умолчанию	Управление авторотацией
<b>Локальные логи клиента SysWatch</b>					
Отчеты о событиях безопасности	system_[date]_[time].txt	C:\Documents and Settings\All Users\Application Data\ (Windows XP) или C:\ProgramData\S.N.Safe&Software\Safe'n'Sec\Reports\ (Windows 7 и новее)	Отчеты о событиях безопасности	30 дней	Через настройки
Отчеты о сборе профиля	profile_[date]_[time].txt	C:\Documents and Settings\All Users\Application Data\ (Windows XP) или C:\ProgramData\S.N.Safe&Software\Safe'n'Sec\Reports\ (Windows 7 и новее)	Лог сбора профиля, список проверенных объектов и результаты сбора профиля	30 дней	Через настройки
Отчеты об антивирусной проверке	scan_[date]_[time].txt	C:\Documents and Settings\All Users\Application Data\ (Windows XP) или C:\ProgramData\S.N.Safe&Software\Safe'n'Sec\Reports\ (Windows 7 и новее)	Лог антивирусной проверки	30 дней	Через настройки
Отчеты об обновлениях	update_[date]_[time].txt	C:\Documents and Settings\All Users\Application Data\ (Windows XP) или C:\ProgramData\S.N.Safe&Software\Safe'n'Sec\Reports\ (Windows 7 и новее)	Отчеты об обновлениях	30 дней	Через настройки
Перечень зараженных файлов	threats.xml	C:\ProgramData\S.N.Safe&Software\Safe'n'Sec	Перечень зараженных файлов	—	—
Общие логи SysWatch	safensec_[date]_[time]_[foobar].txt	C:\ProgramData\S.N.Safe&Software\Safe'n'Sec\Common Logs\	Вывод сообщений и ошибок процессов службы safensec.exe	При превышении числа записей (может не совпадать с числом строк) в один файл больше 50000 создается новый файл	—
Общие логи SysWatch	snscon_[date]_[time]_[foobar].txt	C:\ProgramData\S.N.Safe&Software\Safe'n'Sec\Common Logs\	Вывод сообщений и ошибок графического интерфейса snscon.exe	При превышении числа записей (может не совпадать с числом строк) в один файл больше 50000 создается новый файл	—
Общие логи SysWatch	snsods_[date]_[time]_[foobar].txt	C:\ProgramData\S.N.Safe&Software\Safe'n'Sec\Common Logs\	Вывод сообщений и ошибок антивирусного сканера snsods.exe	При превышении числа записей (может не совпадать с числом строк) в один файл больше 50000 создается новый файл	—



Название	Имя файла	Путь	Краткое описание	Авторотация по умолчанию	Управление авторотацией
Журнал соединения с Service Center	sw_notify_[date]_[time].txt	C:\Documents and Settings\All Users\Application Data\ (Windows XP) или C:\ProgramData\S.N.Safe&Software\Safe'n'Sec\Reports\ (Windows 7 и новее)	Вывод ошибок при подключении к Service Center	—	—
<b>Локальные логи DLP Client</b>					
Журнал соединения с Service Center	dlp_notify_[date]_[time].txt	C:\Documents and Settings\All Users\Application Data\ (Windows XP) или C:\ProgramData\S.N.Safe&Software\Safe'n'Sec\Reports\ (Windows 7 и новее)	Вывод ошибок при подключении к Service Center	—	—
Журнал обновления DLP Client	update_log.txt	C:\Program Files\SafenSoft\DLP Client	Вывод сообщений и ошибок при запуске обновления	—	—
Журнал обновления DLP Client	checks.log	C:\Program Files\SafenSoft\DLP Client\Updater\Reports	Лог проверок наличия обновлений	—	—
Журнал обновления DLP Client	sns.log	C:\Program Files\SafenSoft\DLP Client\Updater\Reports	Журнал обновления модуля	—	—
Журнал обновления DLP Client	root.log	C:\Program Files\SafenSoft\DLP Client\Updater\Reports	Сборный лог, в который дублируются записи sns.log	—	—
<b>Локальные логи SysCmd</b>					
Общие логи SysCmd	SysCmd_[date]_[time]_[foobar].txt	C:\ProgramData\S.N.Safe&Software\Safe'n'Sec\Common Logs\	Вывод сообщений и ошибок процессов службы SysCmd.exe	При превышении числа записей (может не совпадать с числом строк) в один файл больше 50000 создается новый файл	—
Журнал соединения с Service Center	scmd_notify_[date]_[time].txt	C:\Documents and Settings\All Users\Application Data\ (Windows XP) или C:\ProgramData\S.N.Safe&Software\Safe'n'Sec\Reports\ (Windows 7 и новее)	Вывод ошибок при подключении к Service Center	—	—
Журнал обновления SysCmd	update_log.txt	C:\Program Files\SoftControl\SysCmd	Вывод сообщений и ошибок при запуске обновления	—	—
Журнал	checks.log	C:\Program Files	Лог проверок	—	—

Название	Имя файла	Путь	Краткое описание	Авторотация по умолчанию	Управление авторотацией
Обновления SysCmd		\SoftControl\SysCmd\Updater\Reports	наличия обновлений		
Журнал обновления SysCmd	sns.log	C:\Program Files\SoftControl\SysCmd\Updater\Reports	Журнал обновления модуля	–	–
Журнал обновления SysCmd	root.log	C:\Program Files\SoftControl\SysCmd\Updater\Reports	Сборный лог, в который дублируются записи sns.log	–	–
<b>Локальные логи DeCrypt</b>					
Стандартный файл журнала	DecryptLog.log	C:\Windows\	Содержит список устройств и уведомления о событиях	При достижении 100 Мб создается DecryptLog(rotated dd.mm.yyyy).log , где dd.mm.yyyy – дата ротации файла	–
Подробный файл журнала	DeCrypt.log	C:\ProgramData\DeCrypt\	Содержит события системы шифрования и причины неудачного завершения операций	При достижении 100 Мб создается DeCrypt.log_old1, DeCrypt.log_old2 и т.д.	–

**Примечание 1.** Для отчета по работе серверного компонента происходит ротация файлов, позволяющая контролировать размер файлов отчетов. Ротация позволяет формировать отчеты, автоматически разбиваемые на идентичные по своим параметрам части вида

*Log.000, ..., Log.N,*

при этом последний по времени отчет имеет максимальный индекс. Новый файл создается каждый раз, когда размер основного файла с отчетом (*ServerDetailedLog.txt*) превышает 200Мб.

**Примечание 2.** В таблице 39 приведены логи, включенные по умолчанию. Чтобы узнать о выключенных по умолчанию логах, прочитайте статью: [http://kb.safensoft.com/index.php/SoftControl\\_logs](http://kb.safensoft.com/index.php/SoftControl_logs).

Расшифровка сообщений из логов компонентов системы SoftControl описана в статье [http://kb.safensoft.com/index.php/Understanding\\_messages\\_from\\_SoftControl\\_log\\_files](http://kb.safensoft.com/index.php/Understanding_messages_from_SoftControl_log_files).

## 8. Техническая поддержка

При возникновении вопросов по установке, настройке и работе SoftControl Service Center вы можете обращаться в техническую поддержку по электронной почте [support@sns-control.ru](mailto:support@sns-control.ru).

## 9. Приложение

### 9.1 Установка и настройка PostgreSQL 9.5

Программный продукт SoftControl Service Center поддерживает работу с разными версиями SQL-серверов. Ниже приведена инструкция по установке и настройке СУБД PostgreSQL на ОС Windows для ее совместного применения с ОС Windows.

#### ▼ Установка PostgreSQL 9.5

- 1) Запустите установочный файл PostgreSQL 9.5 от администратора.
- 2) Нажмите **Next**.

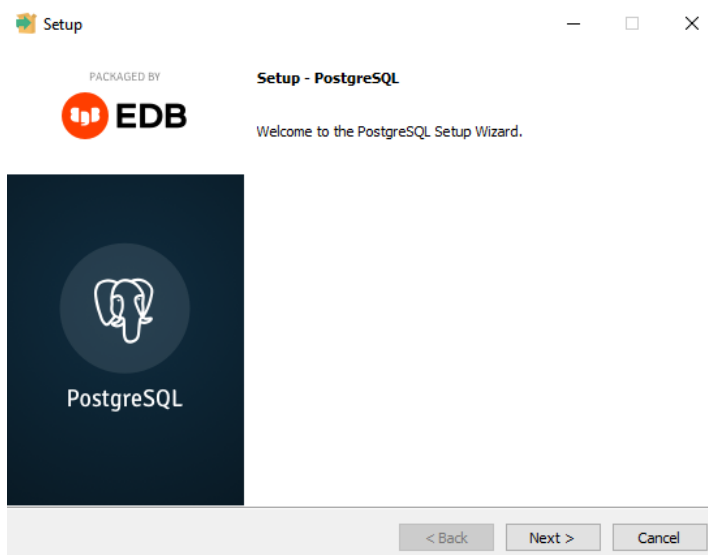


Рисунок 176. Начало установки

- 3) Укажите путь для установки PostgreSQL и нажмите **Next**.

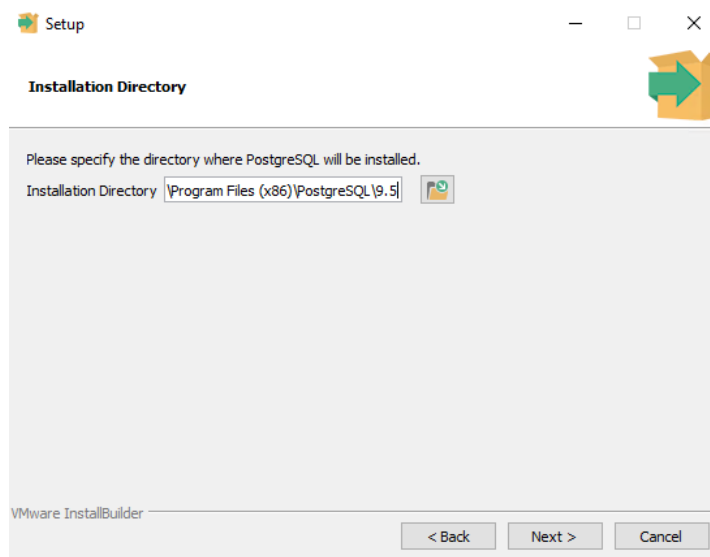


Рисунок 177. Выбор места для установки

4) Укажите путь для хранения данных и нажмите **Next**.

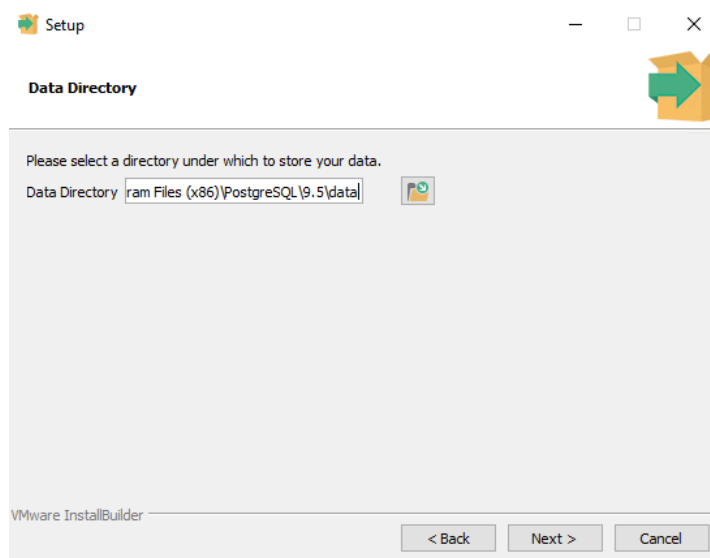


Рисунок 178. Выбор места для хранения данных

5) Задайте пароль для администратора БД по имени postgres. Этот пароль позже потребуется для конфигурирования SoftControl Server для работы с СУБД PostgreSQL. Нажмите **Next**.

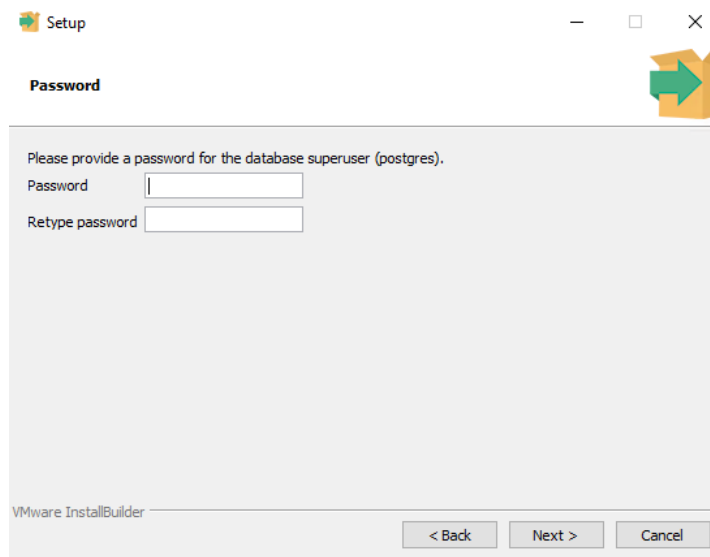


Рисунок 179. Ввод пароля

- 6) Задайте номер порта для работы сервера PostgreSQL. Этот номер порта позже потребуется для конфигурирования SoftControl Server для работы с СУБД PostgreSQL. Нажмите **Next**.

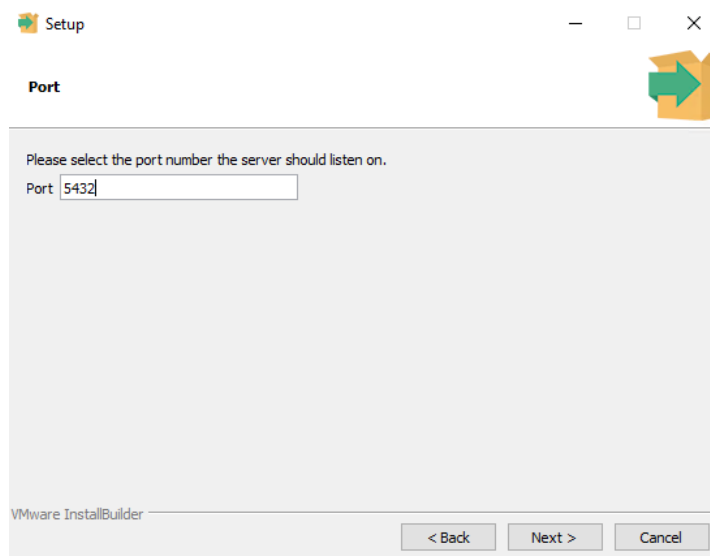


Рисунок 180. Ввод номера порта

- 7) Выберите локаль (можно оставить значение по умолчанию) и нажмите **Next**.

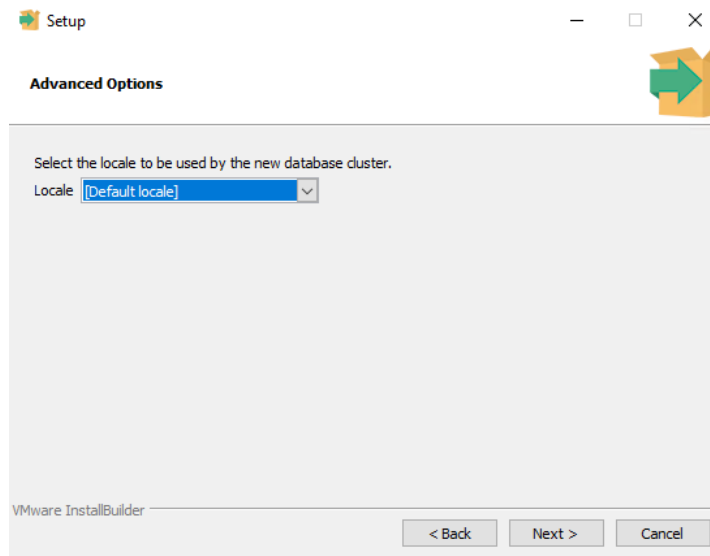


Рисунок 181. Выбор локали

8) Все готово к установке. Нажмите **Next**.

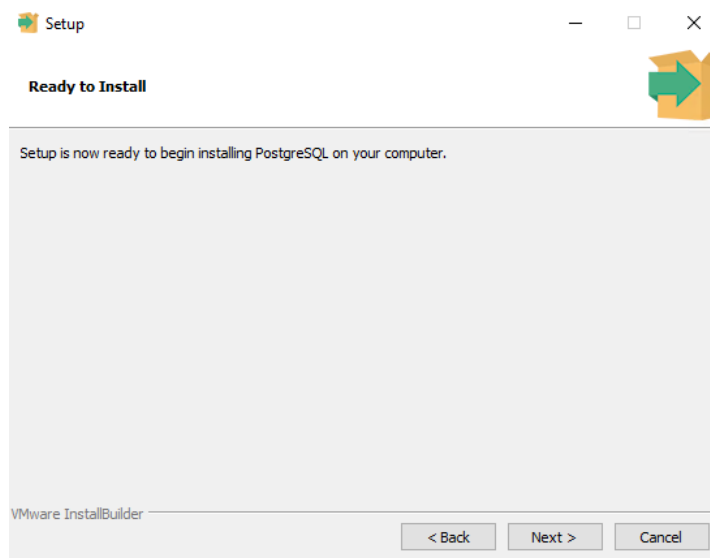


Рисунок 182. Все готово к установке

9) Снимите флажок для установки инструмента Stack Builder и нажмите **Finish**.

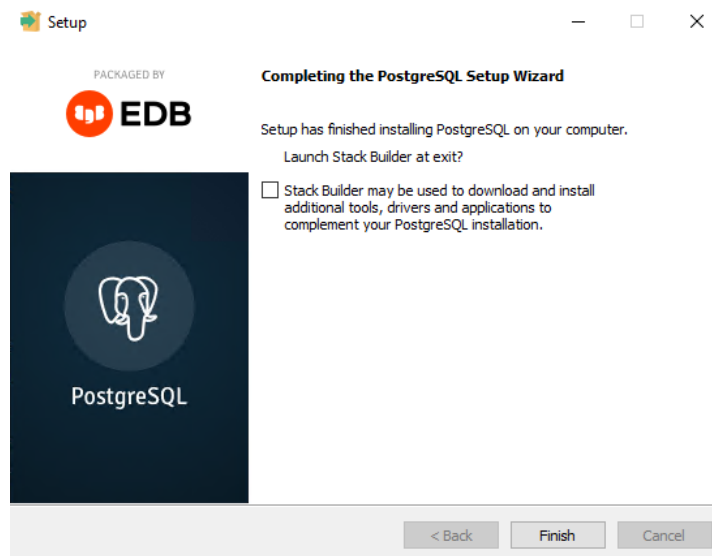


Рисунок 183. Установка завершена

10) Если SoftControl Server устанавливается на тот же компьютер, что и PostgreSQL, никаких дополнительных настроек не требуется. Чтобы установить SoftControl Server на другой компьютер, надо разрешить PostgreSQL принимать соединения с других IP адресов. Для этого необходимо модифицировать файл `pg_hba.conf` (по умолчанию располагается в папке `C:\Program Files\PostgreSQL\9.5\data`). В нем надо найти раздел `# IPv4 local connections` и модифицировать в этом разделе строчку

```
host all all 127.0.0.1/32 md5
```

Вместо `127.0.0.1/32` следует написать `all` (для разрешения соединений со всех IP-адресов), либо указать конкретный IP-адрес, откуда будет подключаться SoftControl Server.

## 9.2 Установка и настройка Microsoft® SQL Server® 2008

Программный продукт SoftControl Service Center поддерживает работу с разными версиями SQL-серверов: SQL Server 2008, SQL Server 2008 R2, SQL Server 2012, SQL Server 2014, SQL Server 2016, SQL Server 2017. Ниже приведена инструкция по установке и настройке СУБД Microsoft® SQL Server® 2008 для ее совместного применения с SoftControl Service Center. Другие версии SQL-серверов устанавливаются аналогично.

### ▼ Подготовка к установке Microsoft® SQL Server® 2008

Перед установкой убедитесь, что система удовлетворяет [МИНИМАЛЬНЫМ](#)



[требованиям к оборудованию и ПО для установки и запуска Microsoft® SQL Server® 2008](#) и, в случае наличия несоответствий заявленным требованиям, устраните их до начала установки.

### ▼ Установка Microsoft® SQL Server® 2008

- 1) Запустите установочный файл Microsoft® SQL Server® 2008.
- 2) В окне Центра установки SQL Server (**SQL Server Installation Server**) откройте раздел **Installation** и выберите тип установки **New SQL Server stand-alone installation or add features to an existing installation** (рис. [Раздел Installation](#)<sup>209</sup>).

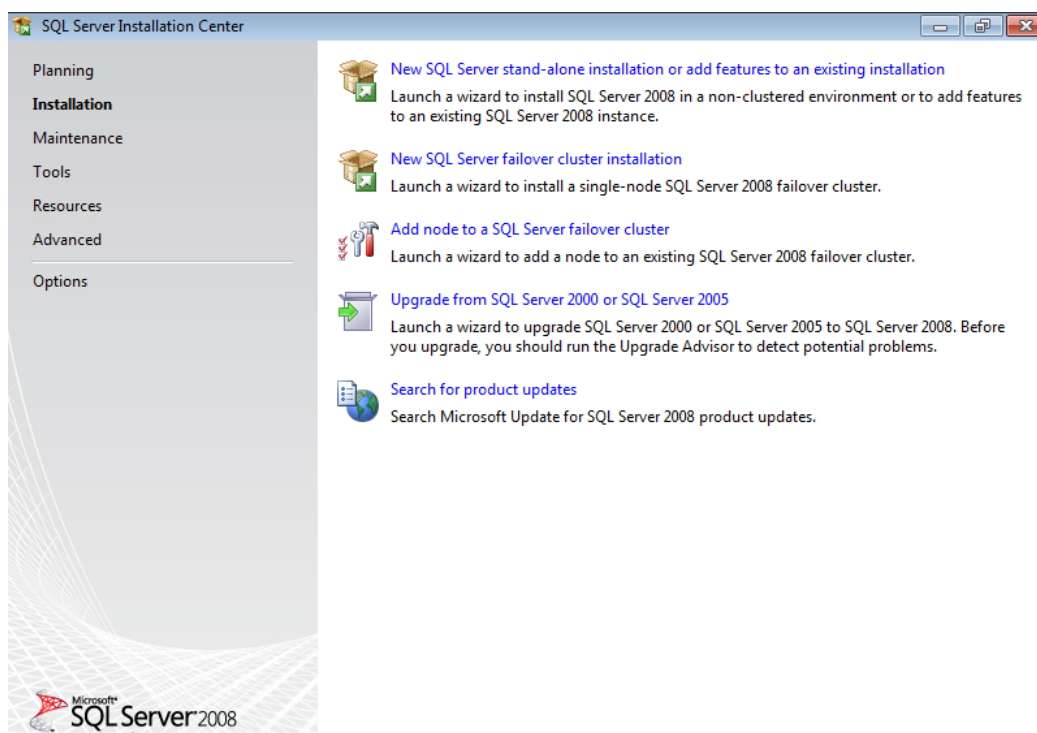


Рисунок 184. Раздел Installation

- 3) В разделе **Setup Support Rules** выполняется проверка на возможные проблемы, которые могут возникнуть при установке вспомогательных файлов установки Microsoft® SQL Server® 2008 (рис. [Проверка проблем при установке вспомогательных файлов](#)<sup>209</sup>). Ошибки должны быть исправлены перед продолжением установки. Если проблем нет, то нажмите на кнопку **ОК**.

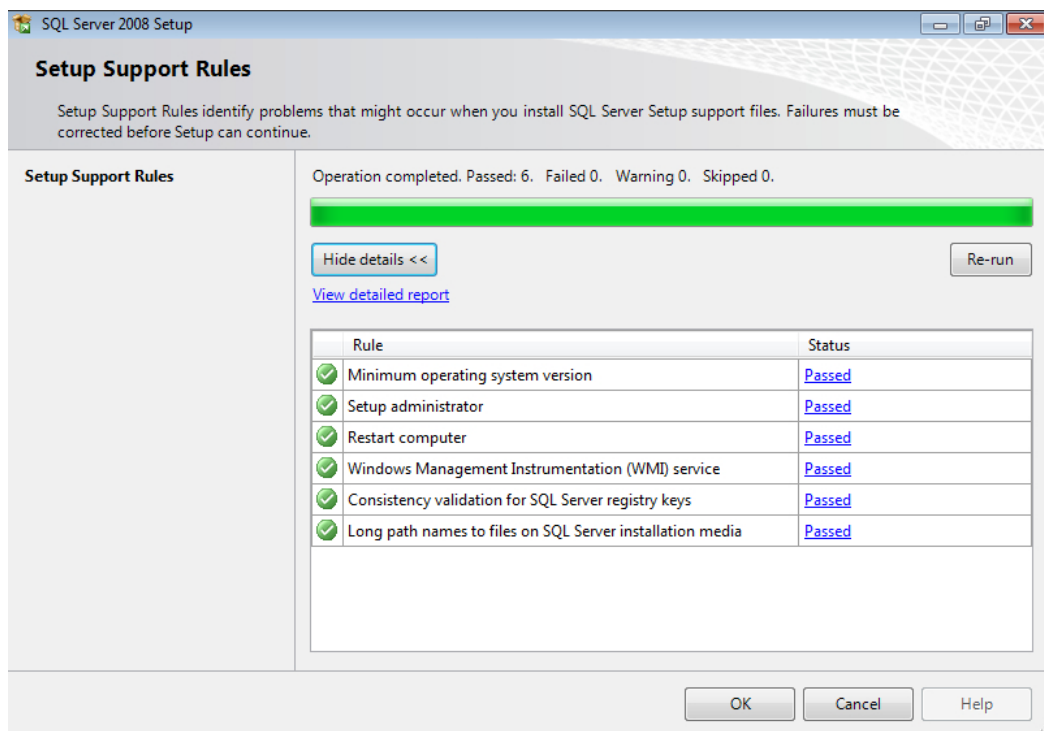


Рисунок 185. Проверка проблем при установке вспомогательных файлов

- 4) В разделе **Product Key** выберите вариант **Enter the product key**, введите лицензионный ключ для Microsoft® SQL Server® 2008 и нажмите на кнопку **Next** (рис. [Раздел Product Key](#)<sup>210</sup>).

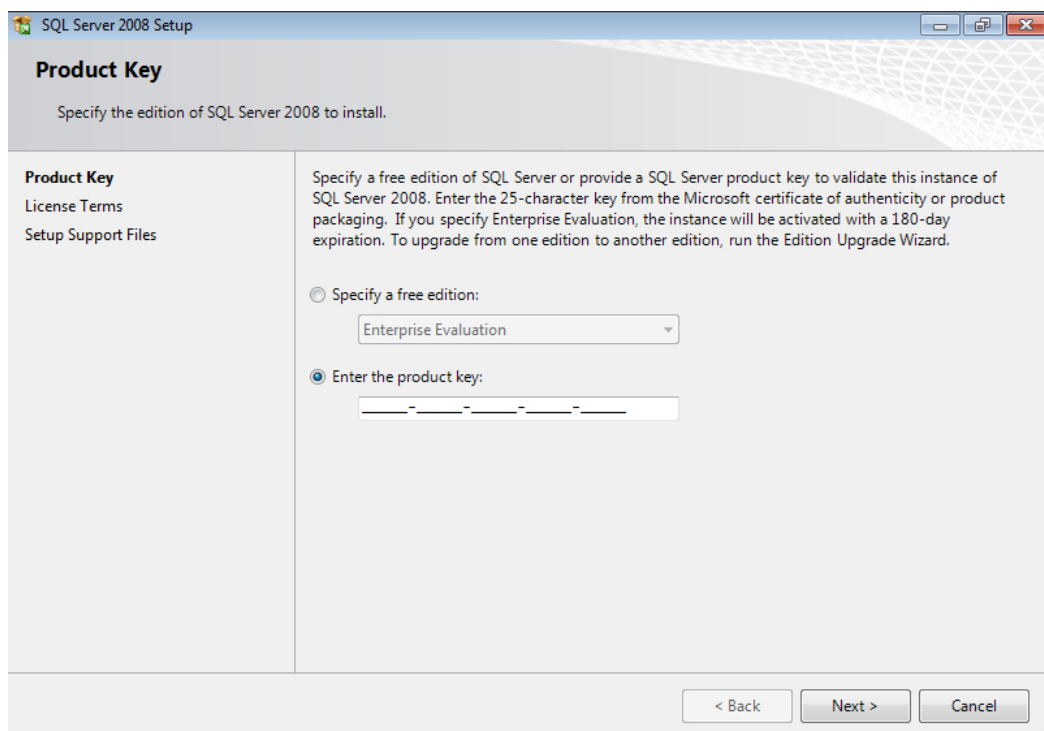


Рисунок 186. Раздел Product Key

5) Прочитайте условия лицензионного соглашения (**License Terms**) и, если Вы с ними согласны, то установите флажок **I accept the license terms** и нажмите на кнопку **Next** (рис. [Раздел License Terms](#)<sup>211</sup>).

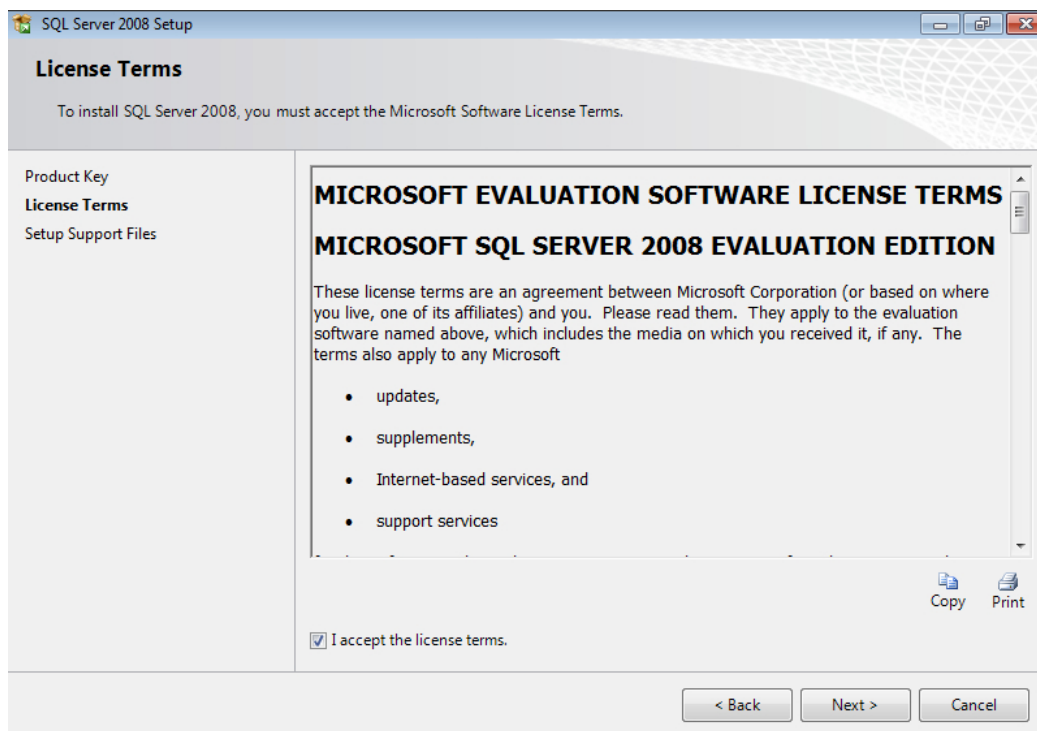


Рисунок 187. Раздел License Terms

6) В разделе **Setup Support Files** нажмите на кнопку **Install** (рис. [Раздел Setup Support Files](#)<sup>211</sup>).

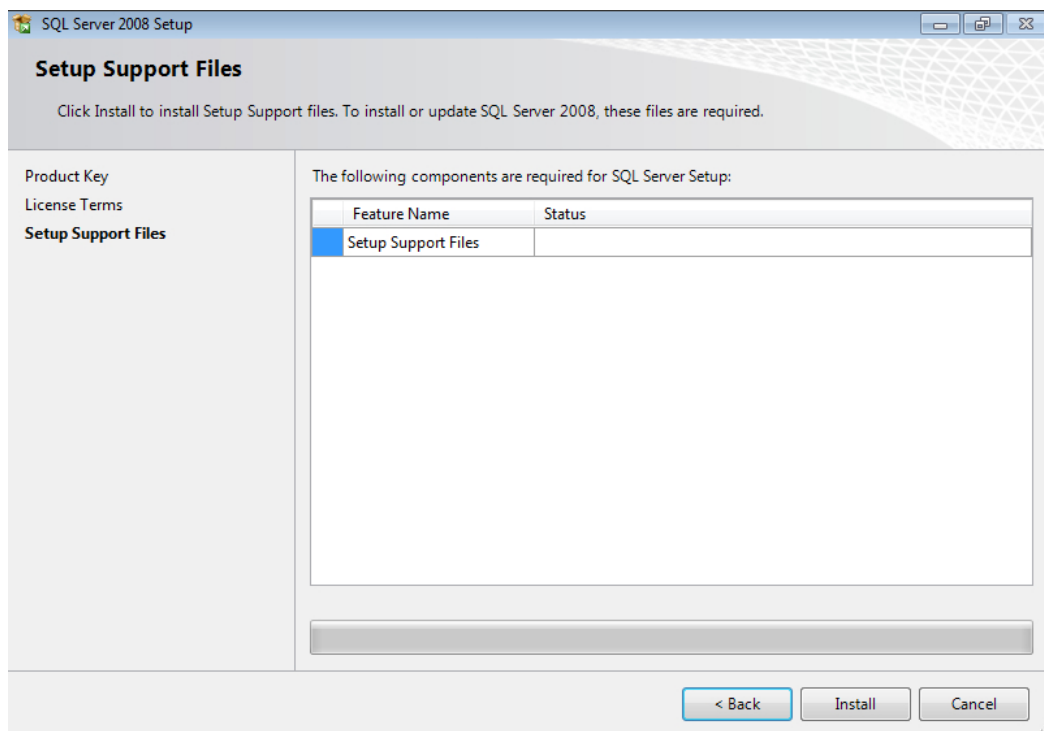


Рисунок 188. Раздел Setup Support Files

- 7) В разделе **Setup Support Rules** выполняется проверка на возможные проблемы, которые могут возникнуть при установке вспомогательных файлов установки Microsoft® SQL Server® 2008 (рис. [Раздел Setup Support Rules. Подробные данные](#)<sup>212</sup>). Ошибки должны быть исправлены перед продолжением установки. Если проблем нет, то нажмите на кнопку **Next**.

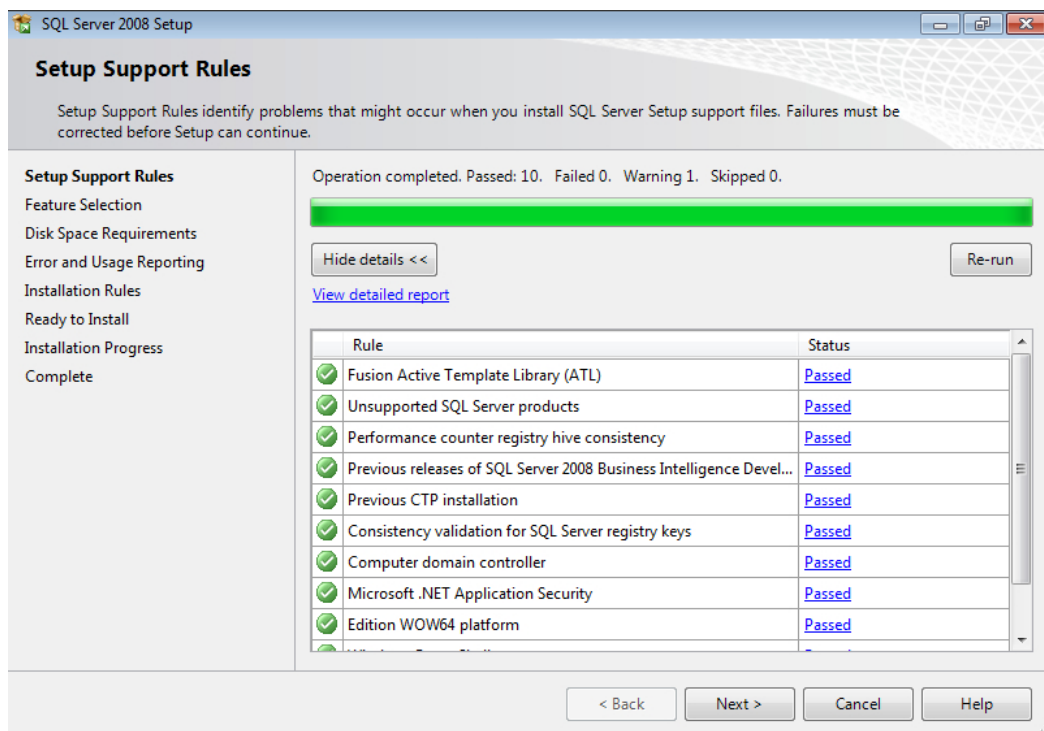


Рисунок 189. Раздел Setup Support Rules. Подробные данные

- 8) В разделе **Feature Selection** выделите компонент **Database Engine Services**, укажите путь для установки в поле **Shared feature directory** и нажмите на кнопку **Next** (рис. [Раздел Feature Selection](#)<sup>213</sup>).

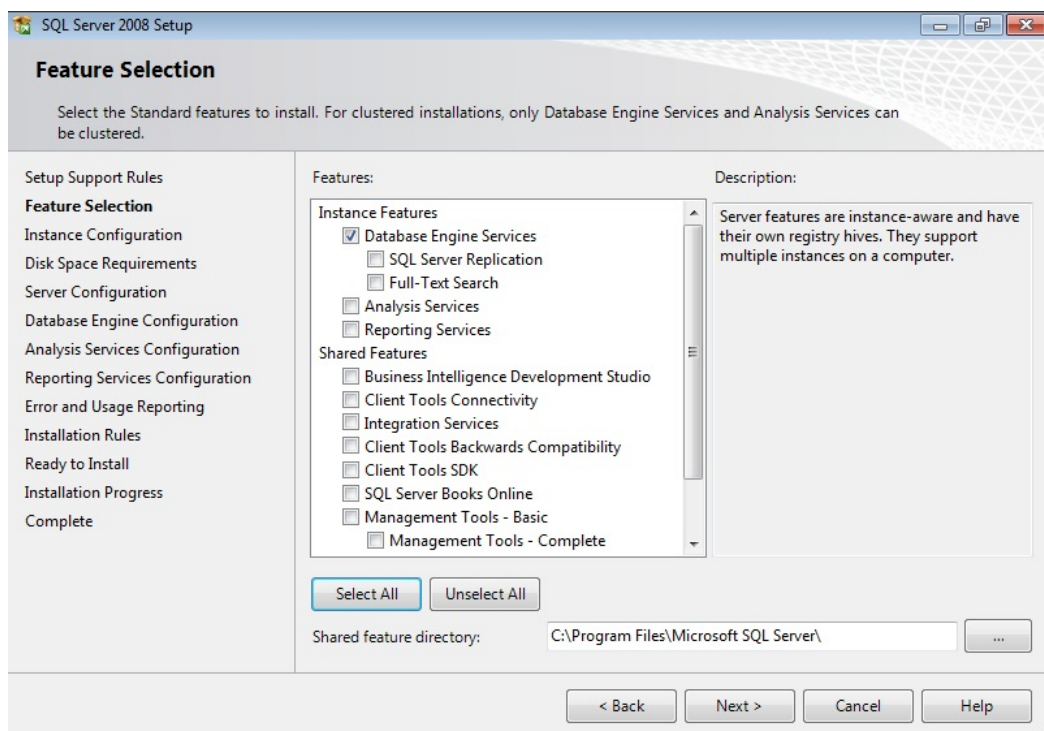


Рисунок 190. Раздел Feature Selection

- 9) В разделе **Instant Configuration** выберите параметр **Default Instance** и нажмите на кнопку **Next** (рис. [Раздел Instance Configuration](#)<sup>214</sup>).

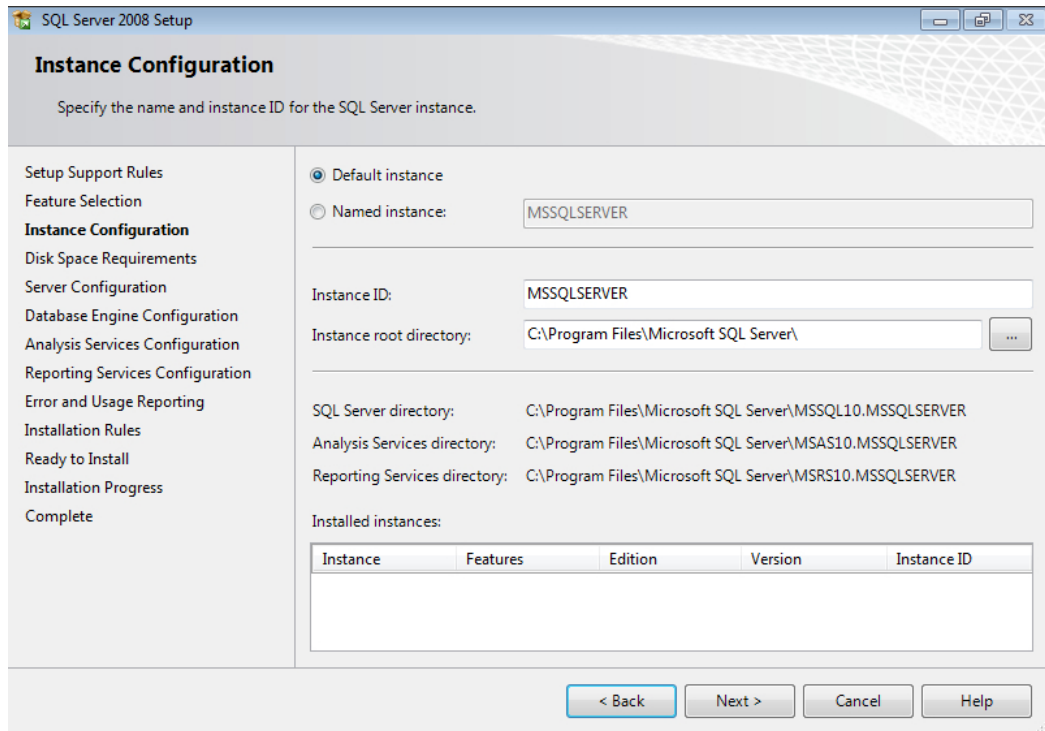


Рисунок 191. Раздел Instance Configuration

- 10) В разделе **Disc Space Requirements** нажмите на кнопку **Next** (рис. [Раздел Disc Space Requirements](#)<sup>214</sup>).

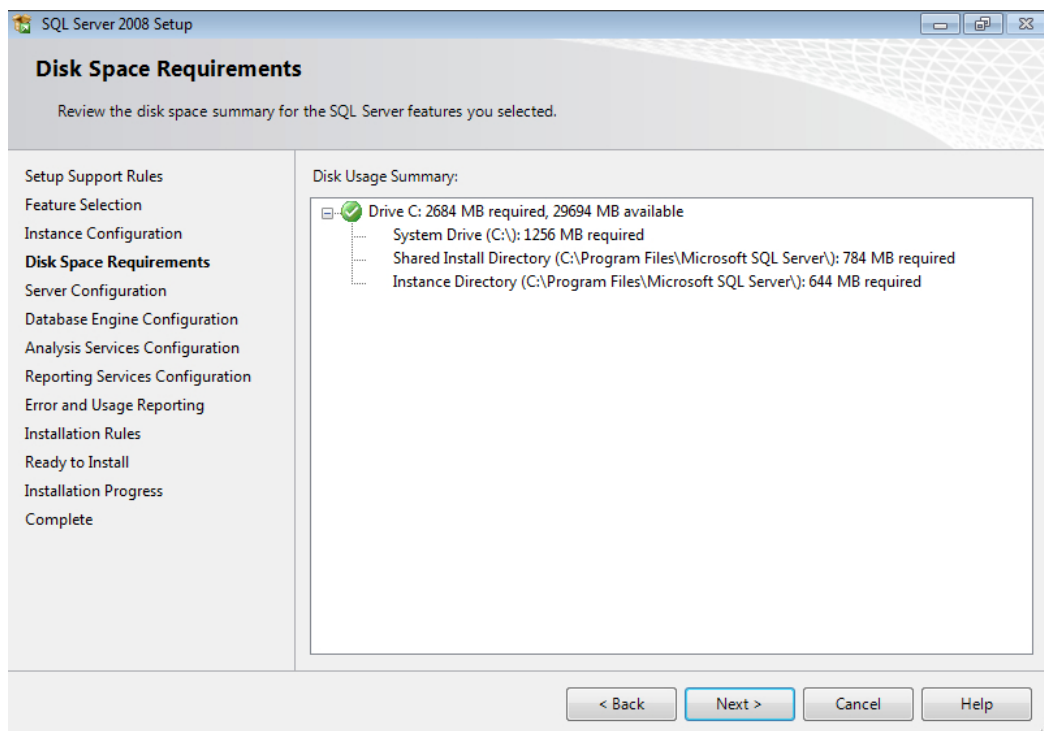


Рисунок 192. Раздел Disc Space Requirements

11) В разделе **Server Configuration** на вкладке **Service Accounts** нажмите на кнопку **Use the same account for all SQL Server services** (рис. [Вкладка Service Accounts раздела Server Configuration](#)<sup>215</sup>).

В открывшемся окне выберите учетную запись **NETWORK SERVICE** и нажмите на кнопку **OK** (рис. [Учетная запись](#)<sup>216</sup>).

На вкладке **Collation** для компонентов **Database Engine** и **Analysis Services** установите параметр **Cyrillic\_General\_CI\_AS** (рис. [Вкладка Collation раздела Server Configuration](#)<sup>216</sup>).

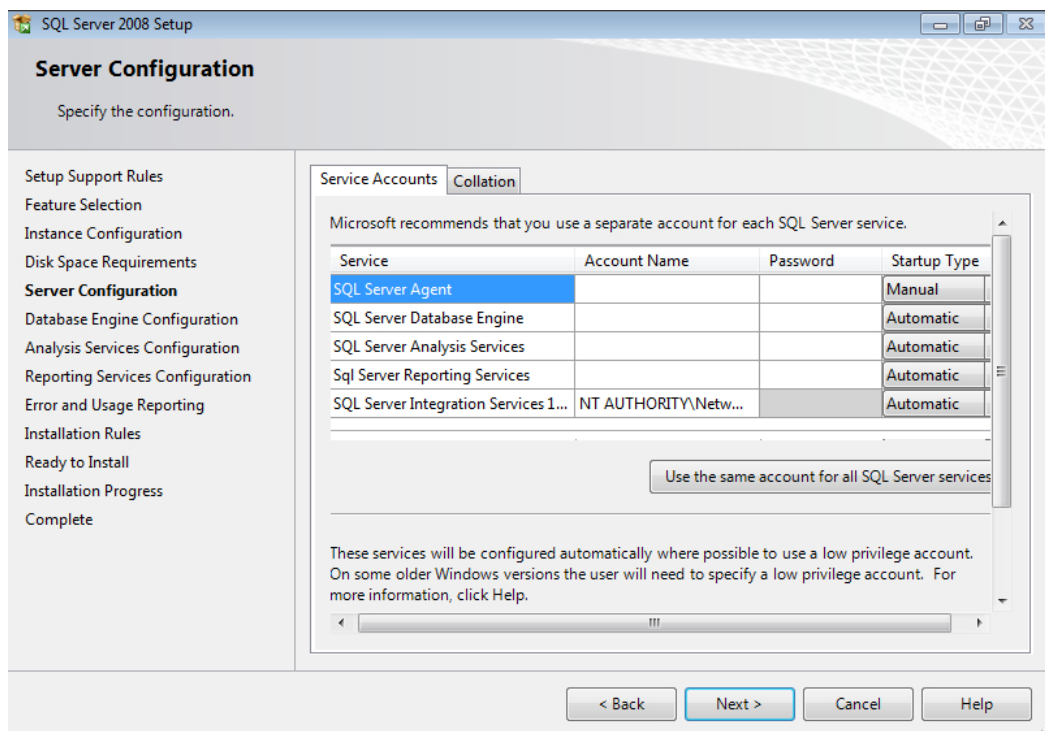


Рисунок 193. Вкладка Service Accounts раздела Server Configuration

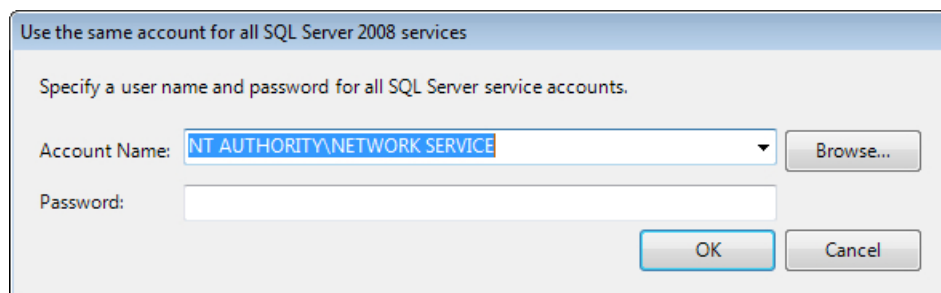


Рисунок 194. Учетная запись



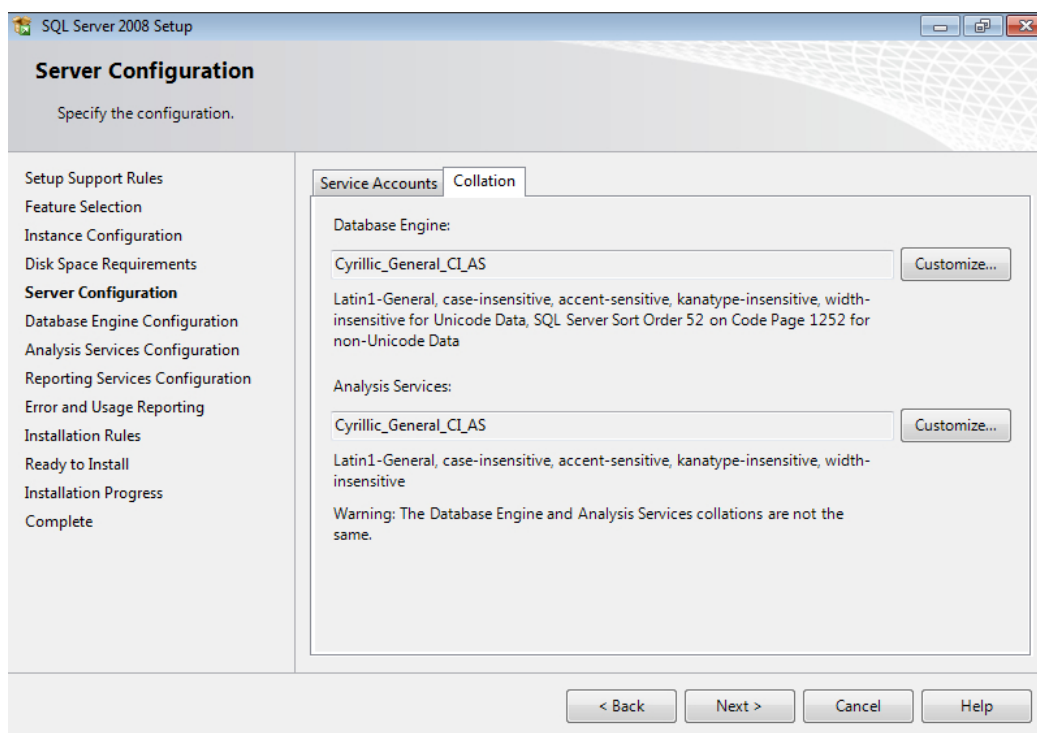


Рисунок 195. Вкладка Collation раздела Server Configuration

Для этого нажмите на кнопку **Customize** для компонента **Database Engine**, в открывшемся окне установите переключатель в положение **Windows collation designator and sort order**, в выпадающем списке **Collation designator** выберите параметр **Cyrillic\_General**, установите флажок **Accent-sensitive** и нажмите на кнопку **ОК** (рис. [Установка параметров Collation для Database Engine](#)<sup>217</sup>).

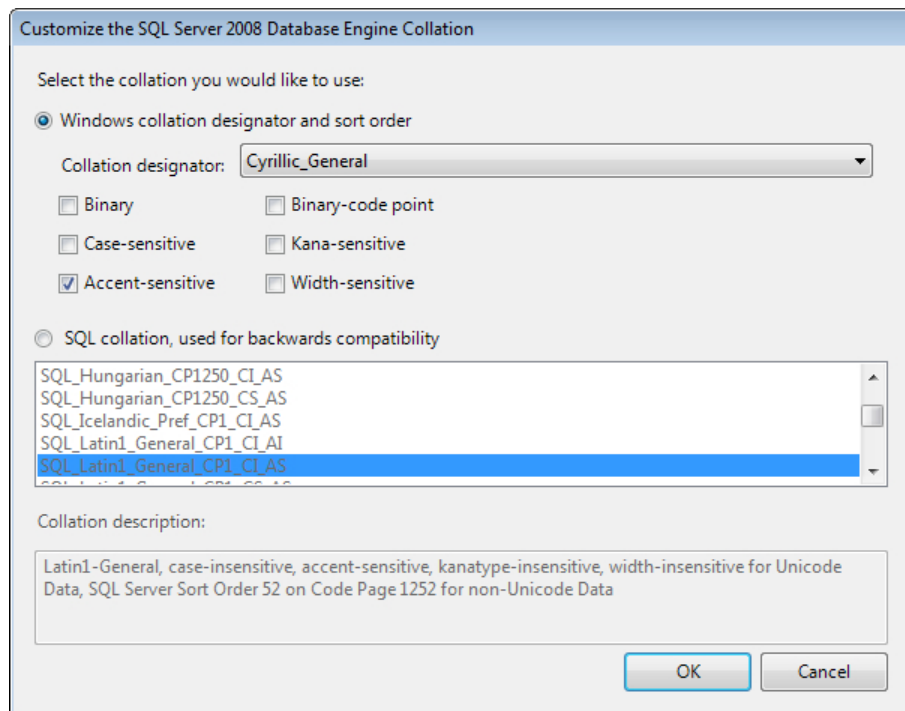


Рисунок 196. Установка параметров Collation для Database Engine

Нажмите на кнопку **Customize** для компонента **Analysis Services**, в открывшемся окне в выпадающем списке **Collation designator** выберите параметр **Cyrillic\_General**, установите флажок **Accent-sensitive** и нажмите на кнопку **OK** (рис. [Установка параметров Collation для Analysis Services](#)<sup>218</sup>).

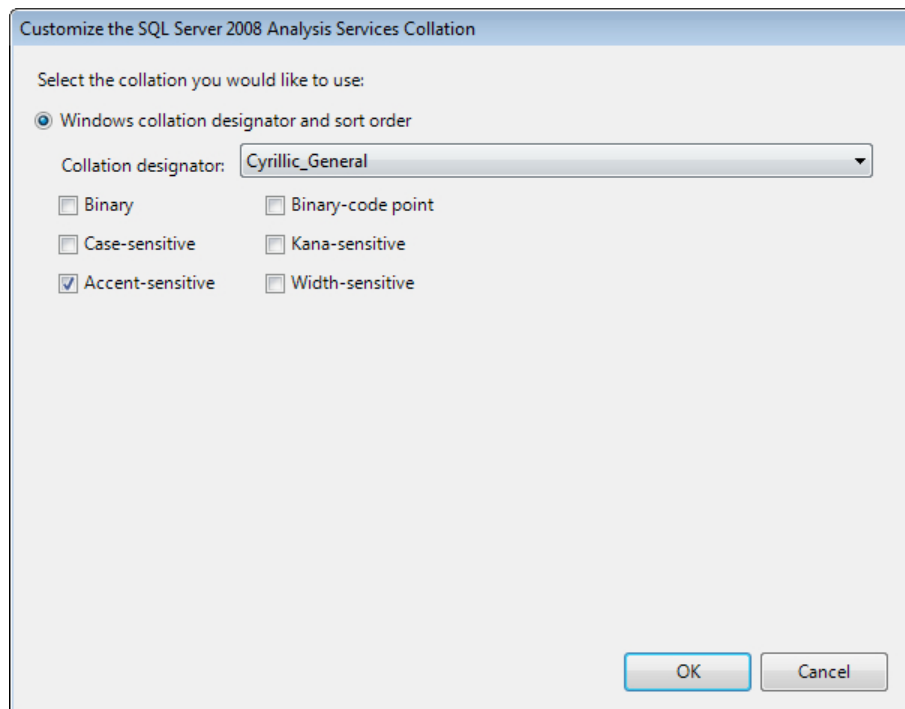


Рисунок 197. Установка параметров Collation для Analysis Services

В разделе **Server Configuration** нажмите на кнопку **Next** для продолжения установки.

- 12) В разделе **Database Engine Configuration** выберите параметр **Mixed Mode** и задайте пароль для учетной записи **Built-in SQL Server system administrator account** в поле **Enter password** и его подтверждение в поле **Confirm password** (рис. [Раздел Database Engine Configuration](#)<sup>219</sup>). Нажмите на кнопку **Add Current User** и убедитесь, что в списке **Specify SQL Server administrators** отображается текущая системная учетная запись, после чего нажмите на кнопку **Next**.

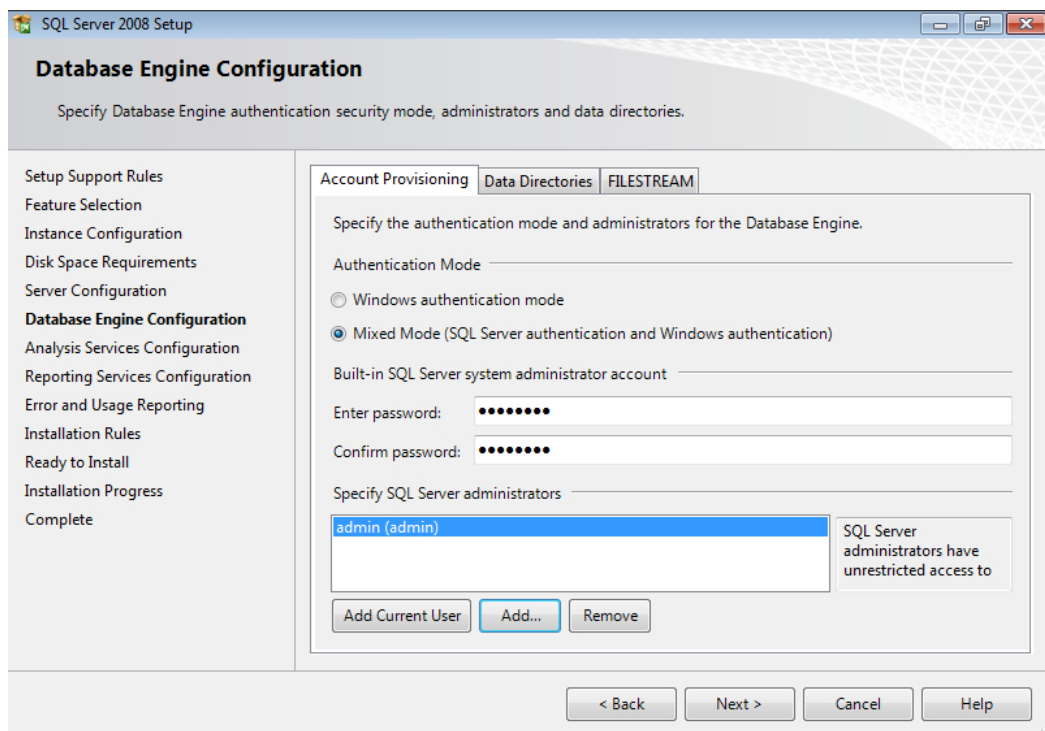


Рисунок 198. Раздел Database Engine Configuration

- 13) В разделе **Analysis Services Configuration** на вкладке **Account Provisioning** нажмите на кнопку **Add Current User** и убедитесь, что в списке **Specify which users have administrative permissions for Analysis Services** отображается текущая учетная запись, после чего нажмите на кнопку **Next** (рис. [Раздел Analysis Services Configuration](#) <sup>220</sup>).

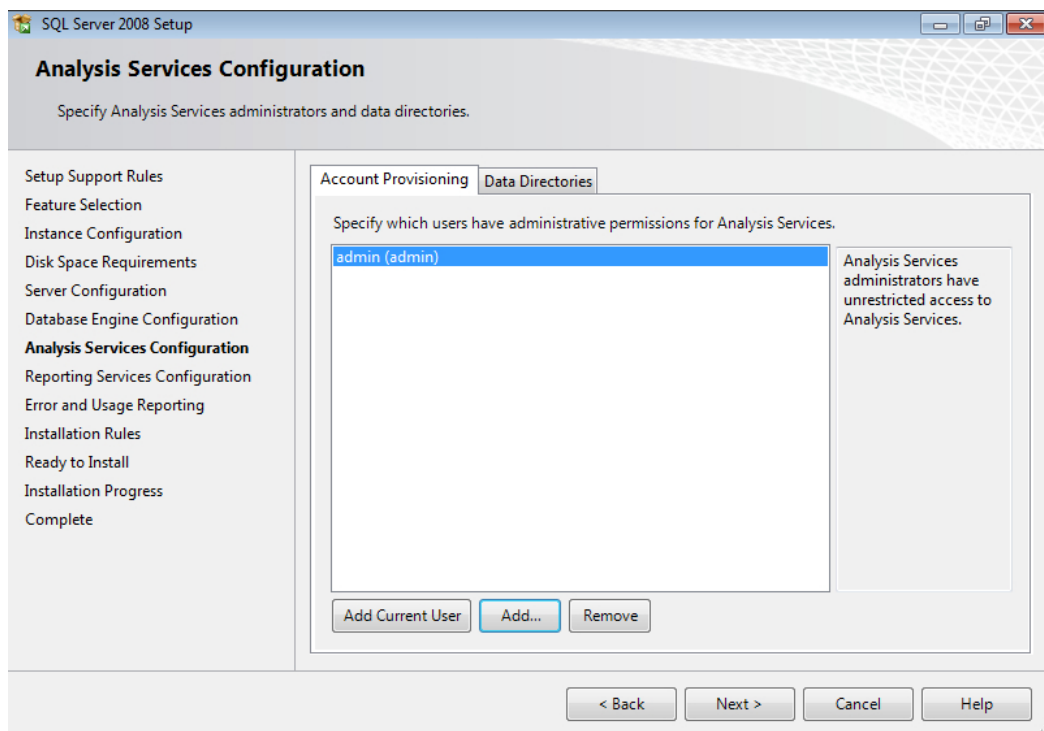


Рисунок 199. Раздел Analysis Services Configuration

- 14) В разделе **Reporting Services Configuration** выберите параметр **Install the native mode default configuration** и нажмите на кнопку **Next** (рис. [Раздел Reporting Services Configuration](#)<sup>221</sup>).

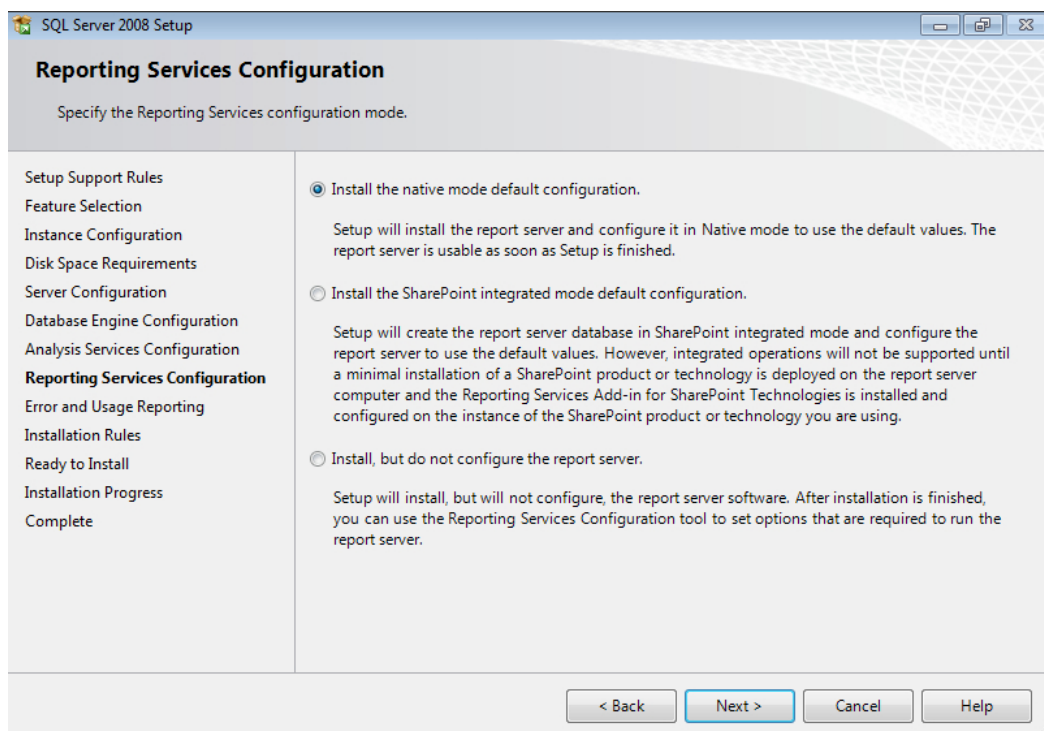


Рисунок 200. Раздел Reporting Services Configuration

- 15) В разделе **Error and Usage Reporting** нажмите на кнопку **Next** (рис. [Раздел Error and Usage Reporting](#)<sup>222</sup>).

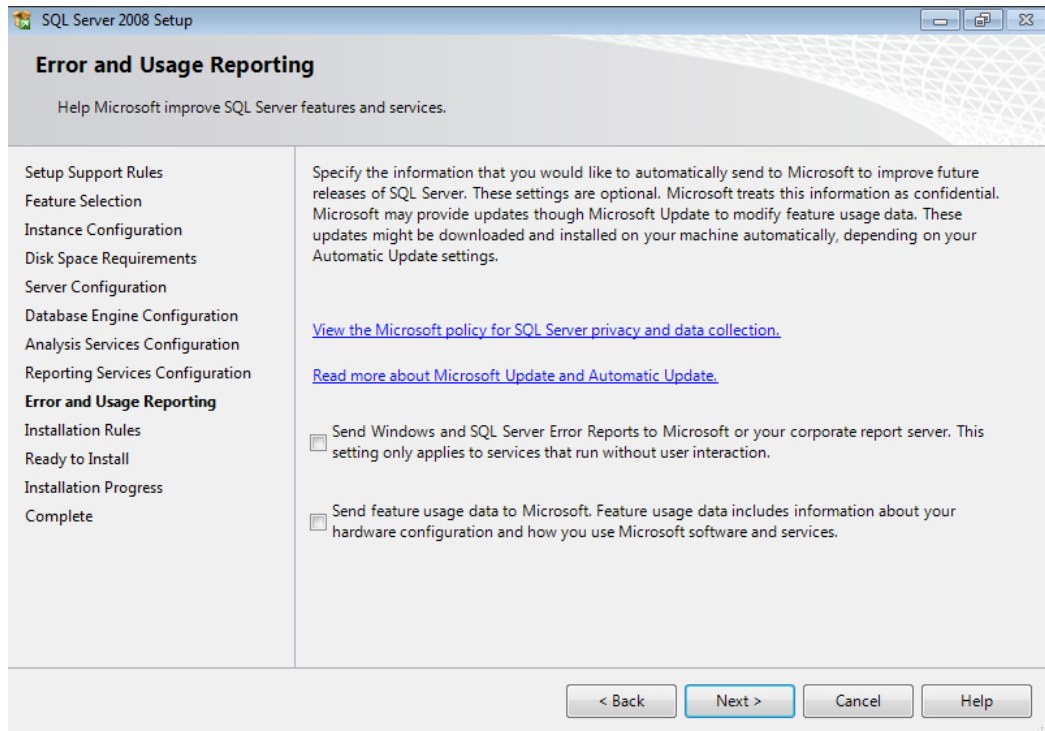


Рисунок 201. Раздел Error and Usage Reporting

- 16) В разделе **Installation Rules** выполняется проверка на возможные проблемы, которые могут возникнуть при установке Microsoft® SQL Server® 2008 (рис. [Раздел Installation Rules](#)<sup>222</sup>). Если ошибок не найдено, то нажмите на кнопку **Next**.

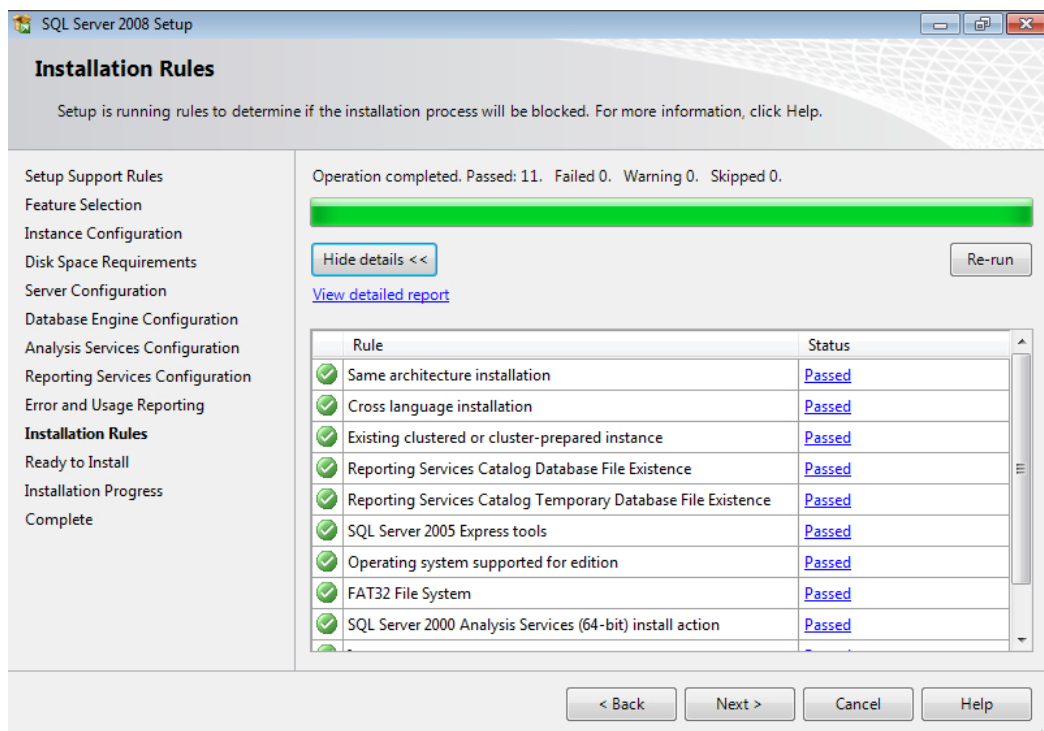


Рисунок 202. Раздел Installation Rules

- 17) В разделе **Ready to Install** проверьте состав устанавливаемых компонентов и нажмите на кнопку **Install** (рис. [Раздел Ready to Install](#)<sup>223</sup>).

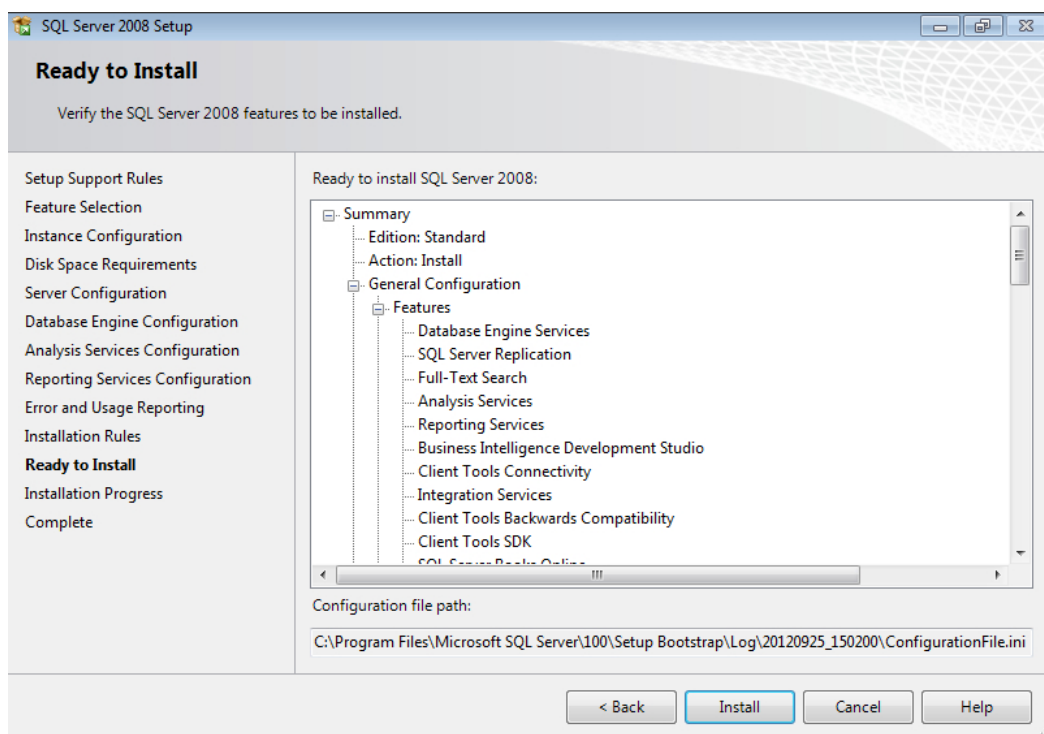


Рисунок 203. Раздел Ready to Install

- 18) В разделе **Installation Progress** отображается процесс установки компонентов Microsoft® SQL Server® 2008 (рис. [Раздел Installation Progress](#)<sup>224</sup>).

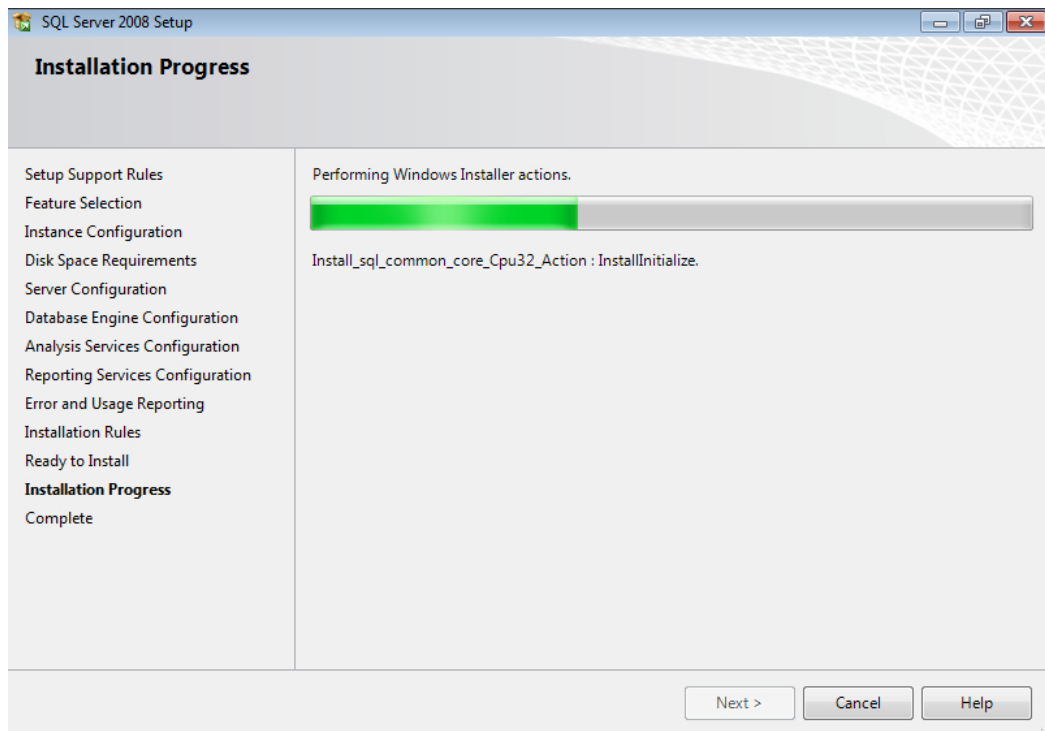


Рисунок 204. Раздел Installation Progress

После окончания установки нажмите на кнопку **Next**.

Для завершения установки в разделе **Complete** нажмите на кнопку **Close** (рис. [Раздел Complete](#)<sup>224</sup>).



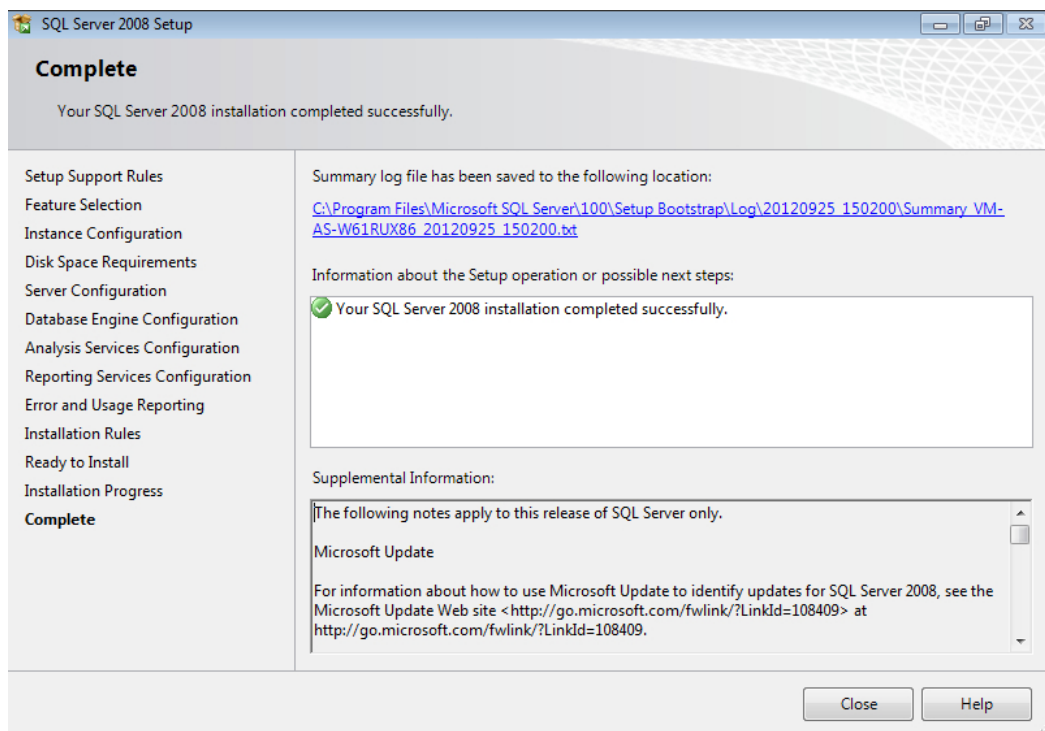


Рисунок 205. Раздел Complete

### 9.3 Добавление компонента Desktop Experience

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

- 1) Откройте оснастку **Server Manager** из раздела **Administrative Tools** меню **Start**. Перейдите в раздел **Features** и в области **Features Summary** нажмите на кнопку **Add Features** (рис. [Оснастка Server Manager](#)<sup>225</sup>).

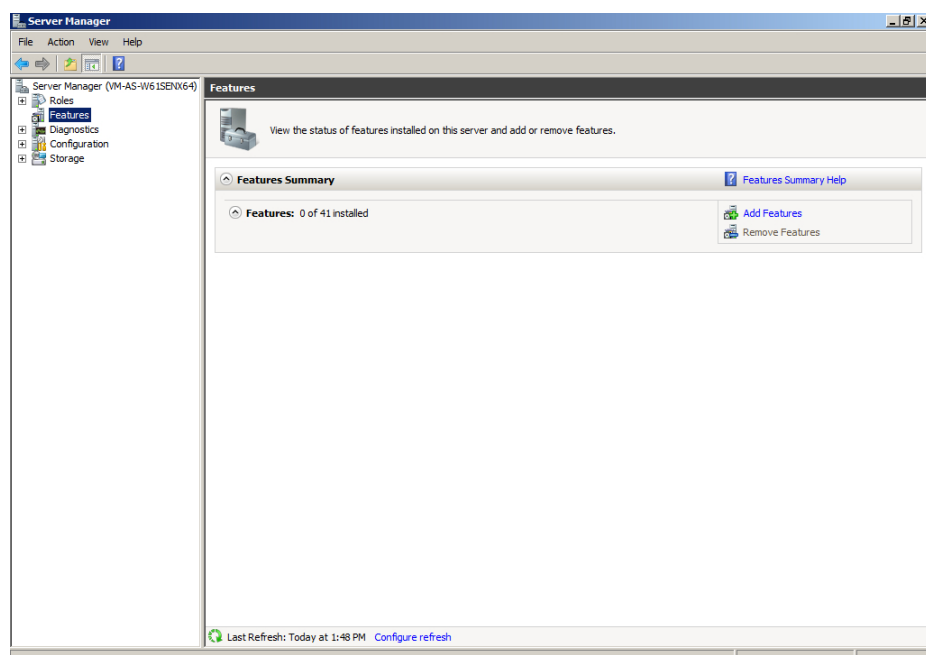


Рисунок 206. Оснастка Server Manager

- 2) В появившемся окне **Add Features Wizard** установите флажок у компонента **Desktop Experience** (рис. [Выбор компонентов для добавления](#)<sup>226</sup>) (в Microsoft® Windows® Server 2012/2012 R2: **User Interfaces and Infrastructure** → **Desktop Experience**).

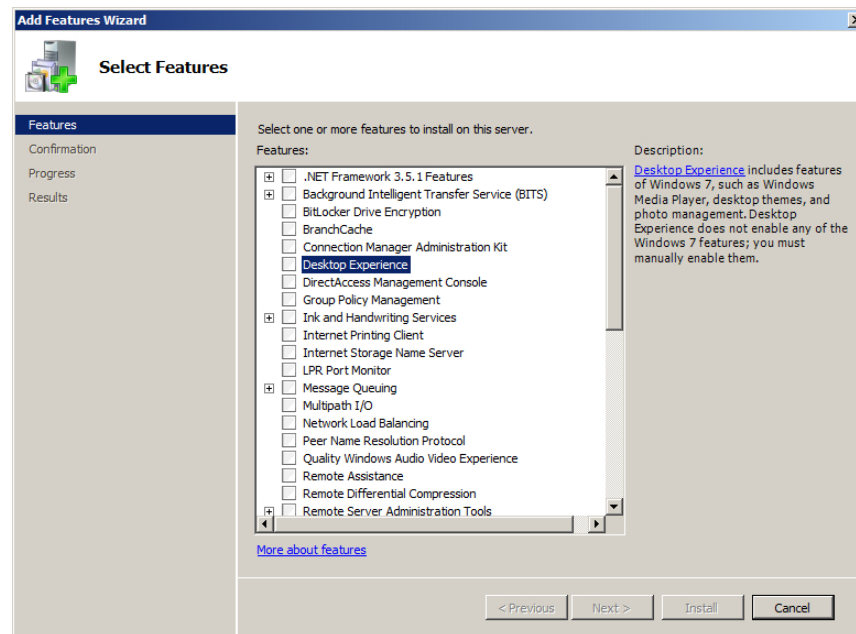


Рисунок 207. Выбор компонентов для добавления

- 3) При появлении диалогового окна с информацией о необходимости добавления связанных компонентов выберите вариант **Add Required Features** (рис. [Запрос добавления связанных компонентов](#)<sup>226</sup>).

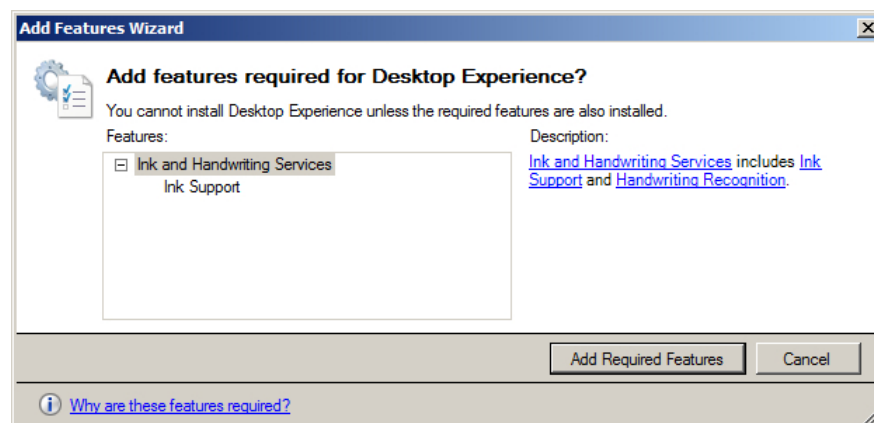


Рисунок 208. Запрос добавления связанных компонентов

- 4) Убедитесь, что компонент **Desktop Experience** выбран и нажмите на кнопку **Next** (рис. [Выбор компонентов для добавления](#)<sup>226</sup>).

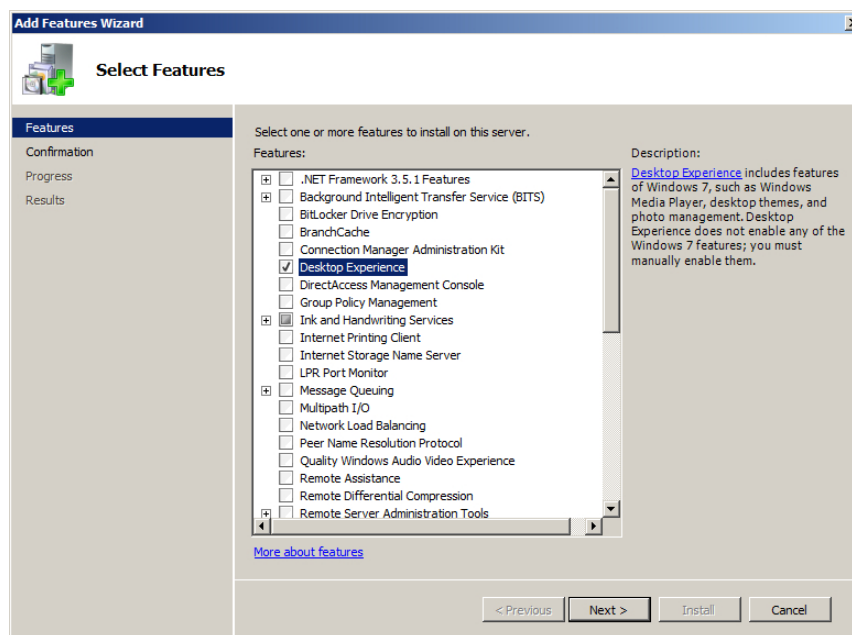


Рисунок 209. Выбор компонентов для добавления

5) На шаге **Confirmation** нажмите на кнопку **Next** (рис. [Подтверждение добавления КОМПОНЕНТОВ](#)<sup>227</sup>).

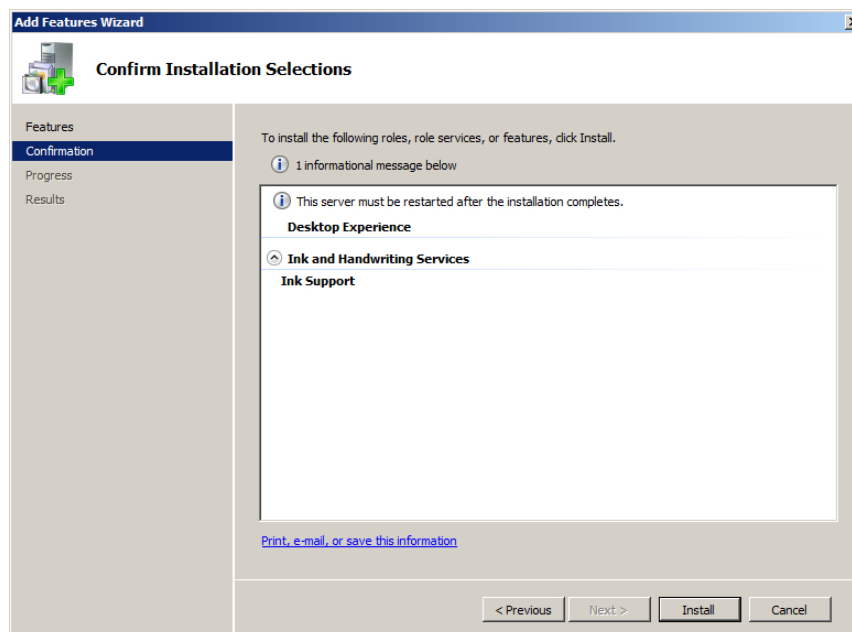


Рисунок 210. Подтверждение добавления компонентов

6) Дождитесь завершения установки (рис. [Процесс установки](#)<sup>227</sup>).

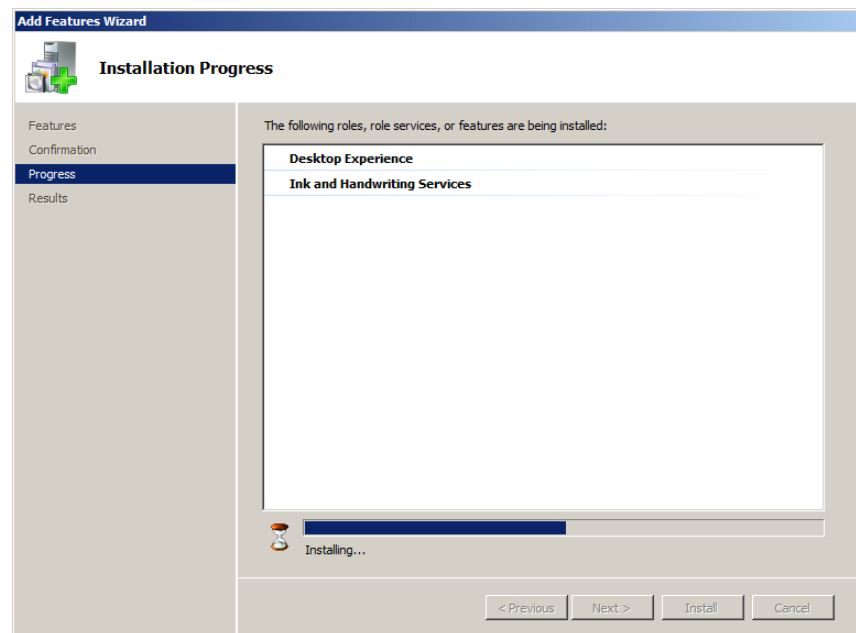


Рисунок 211. Процесс установки

- 7) На шаге **Results** нажмите на кнопку **Close** (рис. [Завершение добавления компонентов](#)<sup>228</sup>).
- 8) В диалоговом окне с предложением перезапуска системы выберите **Yes**, после чего система будет отправлена на перезагрузку для завершения установки (рис. [Запрос перезагрузки](#)<sup>229</sup>).
- 9) После перезапуска системы в появившемся окне **Resume Configuration Wizard** убедитесь, что все требуемые компоненты установлены успешно (**Installation succeeded**) и нажмите на кнопку **Close** (рис. [Результат добавления компонентов](#)<sup>229</sup>).

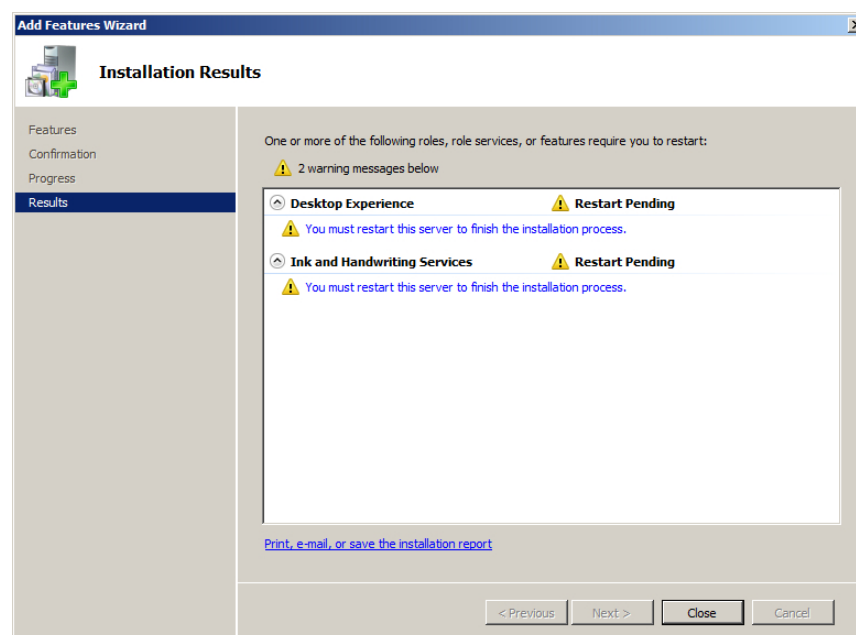


Рисунок 212. Завершение добавления компонентов

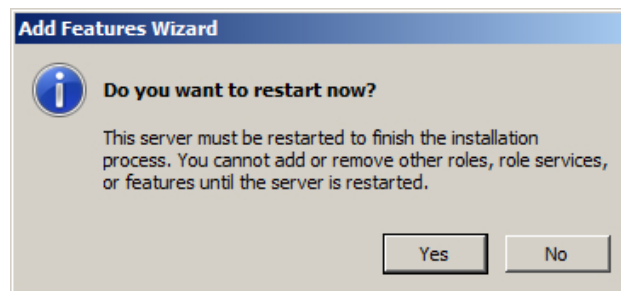


Рисунок 213. Запрос перезагрузки

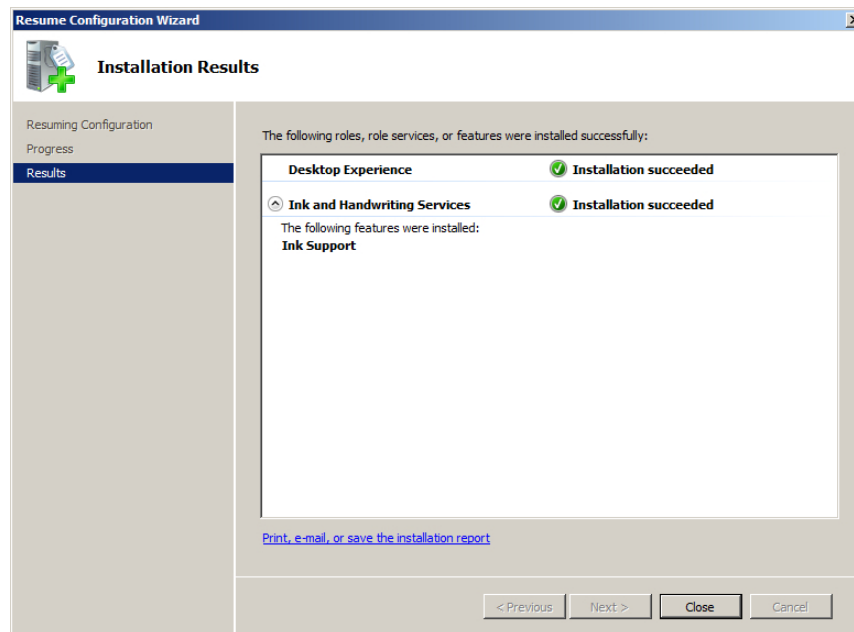


Рисунок 214. Результат добавления компонентов

## 10. Дополнительная информация

### 10.1 О сертификатах

В настоящем разделе рассматриваются некоторые важные аспекты криптографической защиты канала связи между Сервисным Центром и клиентскими приложениями (далее – «клиентами»).

Для взаимодействия между серверным компонентом SoftControl Server и клиентами в SoftControl Service Center используется протокол HTTPS. Все данные между сервером и конечной точкой передаются в зашифрованном виде по защищенному каналу, при этом для авторизации клиентов используются сертификаты стандарта X.509.

В процессе работы SoftControl Server генерирует следующие виды сертификатов:

- **Сертификат УЦ** – самоподписанный корневой сертификат удостоверяющего центра (УЦ) в рамках СИБ SoftControl. В момент конфигурации сервер генерирует этот сертификат и помещает в хранилище Windows. Все остальные виды сертификатов продукта подписаны сертификатом УЦ, что является одним из критериев их достоверности.
- **Серверный сертификат** – сертификат, подписанный сертификатом УЦ и используемый сервером для установки защищенного SSL/TLS-соединения с клиентами. Сервер генерирует этот сертификат в момент конфигурации и помещает в хранилище Windows на серверной машине.
- **Общий клиентский сертификат** – сертификат, подписанный сертификатом УЦ и используемый клиентом для установки защищенного SSL/TLS-соединения с сервером в момент первичного подключения. Данный сертификат является общим для всех новых клиентов и предназначен только для подачи ими первого запроса на сервер. Сертификат встроен в зашифрованный [файл клиентских настроек](#)<sup>(27)</sup>, применяемый к клиенту на конечной точке. Общий клиентский сертификат генерируется сервером в момент конфигурации и хранится на серверной машине по следующему пути:  
C:\ProgramData\SafenSoft\Client.pem
- **Индивидуальный клиентский сертификат** – сертификат, подписанный сертификатом УЦ и используемый клиентом для установки защищенного SSL/TLS-соединения с сервером после [подтверждения регистрации](#)<sup>(50)</sup> администратором через

консоль управления SoftControl Admin Console. Данный сертификат уникален для каждого клиента, что делает невозможным несанкционированный доступ к каналу связи при наличии у злоумышленников украденного индивидуального сертификата другого клиента или общего сертификата. В случае если доверие к индивидуальному сертификату по какой-либо причине утеряно или истек срок его действия, существует возможность выдачи другого сертификата ([обновление](#)<sup>51</sup>) или его отзыв ([отклонение регистрации](#)<sup>51</sup>).

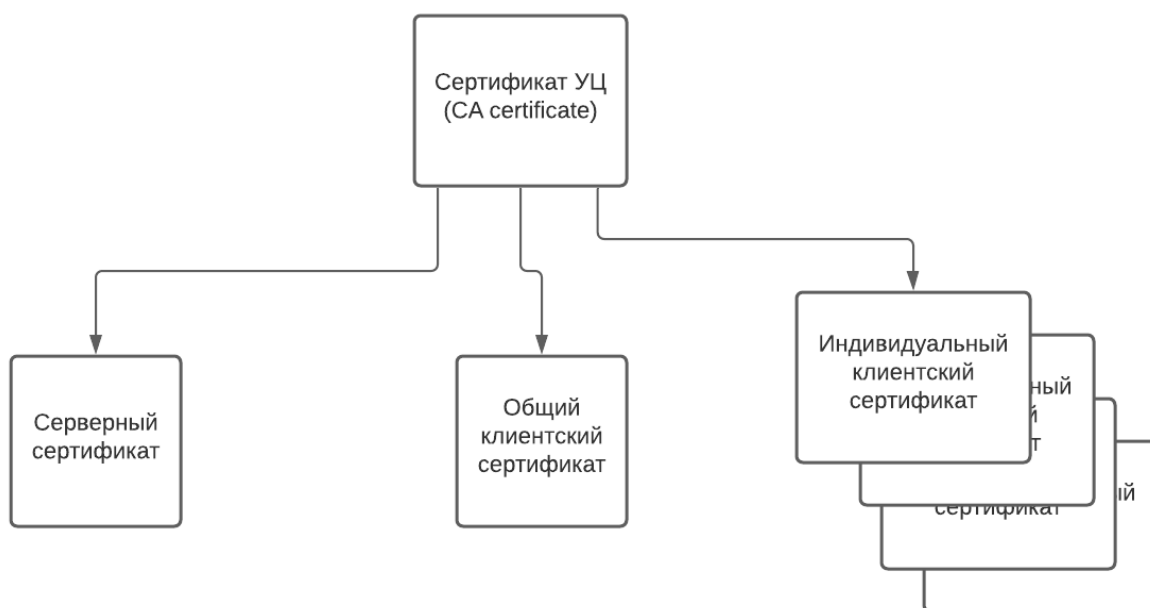


Рисунок 215. Сертификаты в СИБ SoftControl

## 10.2 Управление сертификатами

Чтобы управлять сертификатами УЦ, нажмите на пункт **Инструменты** и выберите **Управление сертификатами УЦ**.

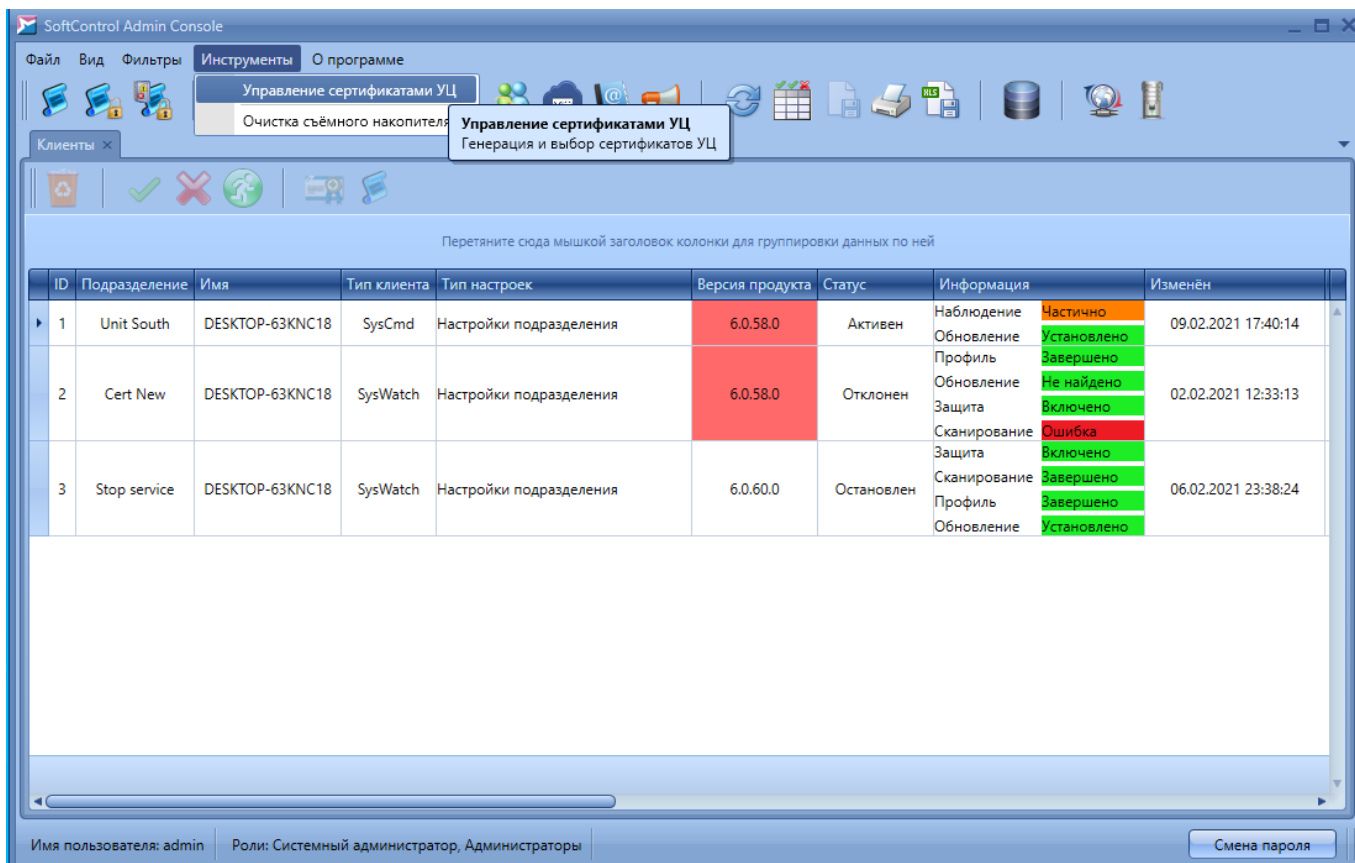


Рисунок 216. Управление сертификатами УЦ

Поля **Текущий сертификат УЦ** и **Новый сертификат УЦ** содержат сведения о действующем сертификате УЦ и сертификате УЦ, который начнет использоваться по истечении действующего. Автоматически новый сертификат УЦ на смену текущему генерируется за три года до конца действия текущего сертификата УЦ. У вас может возникнуть необходимость начать использовать новый сертификат УЦ раньше, если вы обновляете программное обеспечение SoftControl на версию 6.0 или более позднюю (с версий до 6.0). Уже подключенные к серверу SoftControl Server клиенты продолжат работать без изменений, но для регистрации новых клиентов потребуется обновить сертификат УЦ.

Чтобы сгенерировать новый сертификат УЦ, нажмите **Сгенерировать** и подтвердите свое намерение нажатием кнопки **ОК** во всплывающем окне.

Нажмите **Применить** или **ОК**, чтобы активировать сертификат в поле **Текущий**



сертификат УЦ как действующий и сертификат в поле **Новый сертификат УЦ** как сертификат, приготовленный для смены действующего. Подробнее об обновлении сертификатов при переходе на версию 6.0 и более поздние читайте в статье [http://kb.safensoft.com/index.php/Updating\\_SoftControl\\_5\\_to\\_SoftControl\\_6](http://kb.safensoft.com/index.php/Updating_SoftControl_5_to_SoftControl_6).

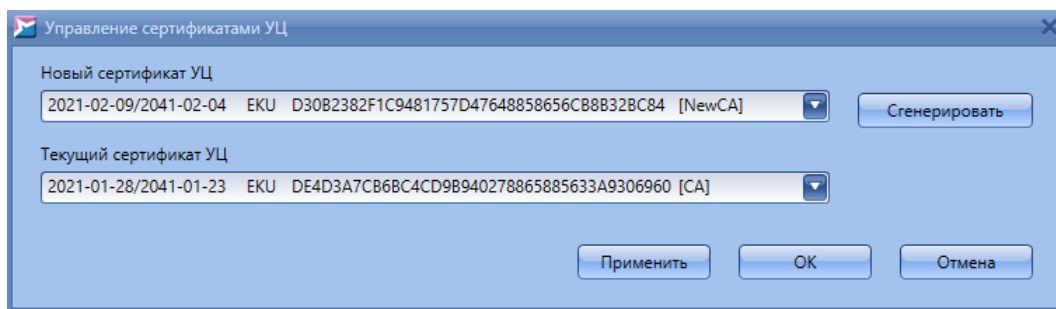


Рисунок 217. Окно управления сертификатами УЦ

Сведения о сертификатах УЦ представлены в следующем формате:

<дата\_генерации\_сертификата>/

<окончание\_срока\_действия\_сертификата><флаг\_EKU\_при\_наличии><имя\_сертификата>.

### 10.3 Восстановление связи с сервером

В системе взаимодействия «клиент-сервер» (в рамках СИБ на основе Сервисного Центра) существует вероятность возникновения ситуаций, при которых IP-адрес сервера может быть изменен автоматически, например, при входе в сеть после перезагрузки. В этом случае клиентские приложения, в конфигурации которых прописаны только IP-адреса компьютера с установленным серверным компонентом SoftControl Server, а не его сетевое имя, теряют связь с ним. Чтобы не корректировать IP-адреса вручную локально в настройках каждого клиентского компонента, предусмотрен функционал резервного сервера восстановления. Для его активации выполните следующие шаги:

1) Откройте файл конфигурации сервера, расположенный по следующему пути:

```
C:\ProgramData\SafenSoft\Server.Config.xml
```

2) В элементе *RescueSettings* замените значение флага *Active* на *True*.

3) Добавьте в элемент *RescueSettings* подэлементы следующего вида:

```
<Address Uri="<новый IP-адрес или имя сервера>" Port="<порт связи>" />
```

4) Сохраните изменения в файле конфигурации.

5) Измените имя компьютера с установленным SoftControl Server на *screstore*.

6) Перезагрузите компьютер с установленным SoftControl Server для применения

новых настроек и изменения сетевого имени хоста.

- 7) После запуска системной службы SoftControl Server порт 8888 для резервного подключения будет автоматически добавлен в брандмауэр Windows.
- 8) По истечении 10 неудачных попыток подключения по списку адресов, заданных в настройках, клиентские компоненты будут предпринимать попытку подключения к резервному серверу с именем *screstore* на порт 8888 (по умолчанию). После успешного подключения по данному адресу, клиентам будет передан заданный в настройках новый список адресов сервера и произведена автоматическая замена старого списка адресов на обновленный в настройках. После того как соединение со всеми подключенными к Сервисному Центру клиентами будет восстановлено, сетевое имя сервера может быть изменено на изначальное.

## 10.4 Резервное копирование SoftControl Service Center

В некоторых случаях существует необходимость в [создании резервной копии](#)<sup>234</sup> компонентов Сервисного Центра, с целью дальнейшего [восстановления](#)<sup>236</sup> полностью работоспособной конфигурации без потери связи с клиентскими приложениями на удаленных хостах. Случаи, к которым применимы данные операции:

- необходимость переустановки ОС на компьютере с компонентами SoftControl Service Center;
- необходимость переноса SoftControl Service Center на другой компьютер.

### 10.4.1 Создание резервной копии

Резервная копия файлов SoftControl Service Center включает в себя необходимые для восстановления файлы конфигурации серверного компонента SoftControl Server и [сертификаты](#)<sup>230</sup>. Также могут быть сохранены [пользовательские фильтры](#)<sup>161</sup> SoftControl Admin Console (опционально). Чтобы создать резервную копию, выполните следующую последовательность действий:

- 1) В основном меню SoftControl Admin Console выберите пункт **Вид** → **Резервное копирование**.
- 2) В появившемся окне установите **Режим копирования** в области **Файлы сервера** (рис. [Создание резервной копии](#)<sup>234</sup>).

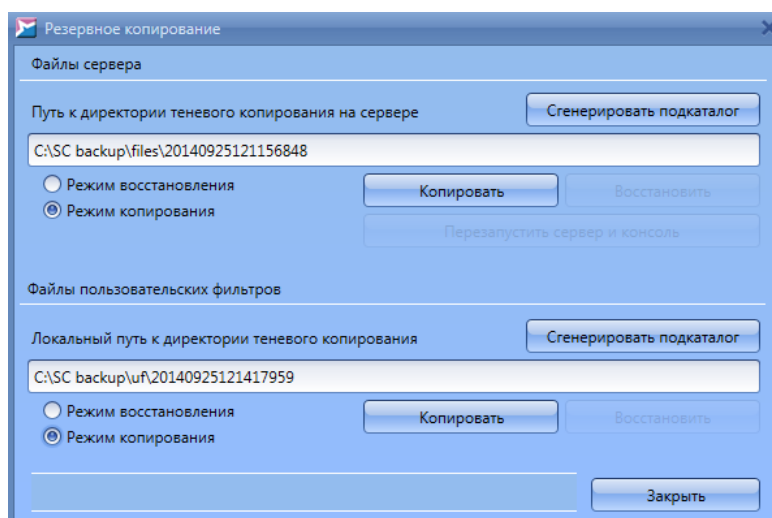


Рисунок 218. Создание резервной копии

Введите путь до каталога, куда предполагается сохранить файлы резервной копии, в соответствующее поле. Если требуется сформировать подкаталог с уникальным идентификатором по введенному пути, нажмите на кнопку **Сгенерировать подкаталог**. Если нажать на указанную кнопку при пустом поле ввода, подкаталог будет по умолчанию располагаться в следующей директории: C:\Windows\System32

Нажмите на кнопку **Копировать**, чтобы создать резервную копию файлов по выбранному пути. В нижней части окна будет отображен статус операции.

- 3) Для сохранения пользовательских фильтров в окне **Резервное копирование** (рис. [Создание резервной копии](#)<sup>234</sup>) повторите действия п. 2 для области **Файлы пользовательских фильтров**.

Если нажать на кнопку **Сгенерировать подкаталог** при пустом поле ввода, подкаталог будет по умолчанию располагаться в директории установки SoftControl Admin Console.

- 4) В случае, если БД Сервисного Центра располагается на внешнем сервере (отличном от компьютера с установленными компонентами SoftControl Service Center), сохранять ее копию не требуется. В обратном случае создайте резервную копию текущей БД средствами Microsoft® SQL Server®.

## 10.4.2 Восстановление из резервной копии

Для восстановления SoftControl Service Center из резервной копии выполните следующую последовательность действий:

- 1) Убедитесь, что на компьютере установлено правильное время.
- 2) [Установите](#)<sup>11</sup> SoftControl Service Center той же версии, что использовался на компьютере, с которого создавалась резервная копия.
- 3) Выполните восстановление ранее сохраненной БД. Пропустите этот шаг, если БД находилась на другом компьютере и не удалялась.
- 4) Произведите [первичную настройку сервера](#)<sup>21</sup>. При настройке укажите новое **Имя базы данных**, отличное от имени старой БД, чтобы не повредить данные в ней. После восстановления из резервной копии сервер автоматически переключится на старую базу данных.
- 5) В основном меню SoftControl Admin Console выберите пункт **Вид** → **Резервное копирование**.
- 6) В появившемся окне установите **Режим восстановления** в области **Файлы сервера** (рис. [Восстановление из резервной копии](#)<sup>236</sup>). Введите путь до каталога с ранее сохраненными файлами резервной копии в соответствующее поле и нажмите на кнопку **Восстановить**. В нижней части окна будет отображен статус операции.

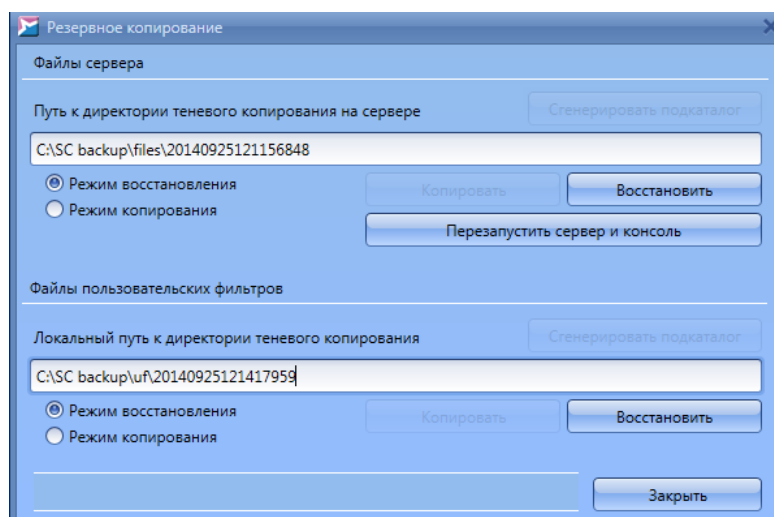


Рисунок 219. Восстановление из резервной копии

- 7) При необходимости восстановления пользовательских фильтров в окне **Резервное копирование** (рис. [Восстановление из резервной копии](#)<sup>236</sup>)

повторите действия п. [6](#)<sup>236</sup> для области **Файлы пользовательских фильтров**.

- 8) Нажмите на кнопку **Перезапустить сервер и консоль** для перезапуска системной службы SoftControl Server и применения восстановленной конфигурации.

Примечание: на некоторых системах может также понадобиться перезагрузка компьютера.

- 9) Удалите временную базу данных, созданную на шаге [4](#)<sup>236</sup>.

- 10) [Авторизуйтесь](#)<sup>27</sup> в консоли управления SoftControl Admin Console. Проверьте работоспособность компонентов.

## 10.5 Привилегии процессов

В табл. 40 представлено описание привилегий Windows, используемых процессами (см. также [https://msdn.microsoft.com/ru-ru/library/windows/desktop/bb530716\(v=vs.85\).aspx](https://msdn.microsoft.com/ru-ru/library/windows/desktop/bb530716(v=vs.85).aspx) и <https://docs.microsoft.com/en-us/windows/device-security/auditing/event-4704>).

**Таблица 40. Описание привилегий процессов**

Привилегия	Описание
Управление аудитом и журналом безопасности	Добавление записей в журнал безопасности.
Архивация файлов и каталогов	Выполнение операций по резервному копированию. Эта привилегия заставляет систему выдать права на чтение любого файла, независимо от того, что указано в списке управления доступом (ACL) для этого файла. Любой другой запрос на доступ, кроме чтения, по-прежнему оценивается с помощью ACL.
Восстановление файлов и каталогов	Выполнение операций восстановления. Эта привилегия заставляет систему выдать права на запись любого файла, независимо от того, что указано в списке управления доступом (ACL) для этого файла. Пользователь с данной привилегией может обходить разрешения файлов, папок, реестра и других постоянных объектов при восстановлении файлов и папок из резервных копий. Дополнительно данная привилегия позволяет назначить любого пользователя или группу с действующим идентификатором безопасности (SID) владельцем файла.
Изменение системного времени	Изменение системного времени. Пользователь с данной привилегией может изменять время и дату на внутренних часах компьютера. Пользователи с такими правами могут влиять на вид журналов событий. Если системное время изменено, события, которые были записаны, будут отображать это новое время, а не реальное время, в которое они произошли.
Завершение работы системы	Завершение работы локальной системы.
Принудительное удаленное завершение работы	Выключение системы с помощью запроса по сети.

Привилегия	Описание
Смена владельцев файлов и других объектов	Привилегия необходима, чтобы стать владельцем объекта без получения избирательного доступа. Пользователь с данной привилегией может стать владельцем любого защищаемого объекта в системе, включая объекты Active Directory, файлы и папки, принтеры, разделы реестра, процессы и потоки.
Отладка программ	Отладка и настройка памяти процесса, который принадлежит другой учетной записи. Пользователь с данной привилегией может присоединять отладчик к любому процессу или ядру. Разработчикам, отлаживающим свои собственные приложения, это пользовательское право не нужно. Разработчикам, отлаживающим новые компоненты системы, это право нужно. Данное право дает полный доступ к чувствительным и критичным компонентам операционной системы.
Изменение параметров среды изготовителя	Изменение энергонезависимой памяти (RAM) систем, которые используют данный тип памяти для хранения информации о конфигурации.
Профилирование производительности системы	Сбор профиля всей системы. Пользователь с данной привилегией может использовать средства наблюдения за производительностью для контроля производительности системных процессов.
Профилирование одного процесса	Сбор профиля по одному процессу. Пользователь с данной привилегией может использовать средства наблюдения за производительностью для контроля производительности несистемных процессов.
Увеличение приоритета выполнения	Увеличение базового приоритета процесса. Пользователь с данной привилегией может использовать процесс с доступом к свойству «запись» другого процесса для увеличения приоритета выполнения, назначенного этому другому процессу. Такой пользователь может изменять запланированный приоритет процесса через пользовательский интерфейс Диспетчера задач.
Загрузка и выгрузка драйверов устройств	Загрузка и выгрузка драйверов устройств. Пользователь с данной привилегией может динамически загружать и выгружать драйвера устройств или другой код в режиме ядра. Это пользовательское право не применяется к драйверам устройств Plug and Play.
Создание файла подкачки	Создание файла подкачки. Пользователь с данной привилегией может создавать и изменять размер файла подкачки.
Настройка квот памяти для процесса	Увеличение квоты, назначенной процессу.
Обход перекрестной проверки	Получение уведомлений об изменениях в файлах и директориях. Привилегия также заставляет систему пропустить все перекрестные проверки на доступ. По умолчанию включена для всех пользователей.
Отключение компьютера от стыковочного узла	Отстыковка ноутбука. Пользователь с данной привилегией может отключить портативный компьютер от стыковочного узла, не выполняя вход в систему.
Выполнение задач по обслуживанию томов	Включение привилегий по обслуживанию томов. Необходима для проведения задач по обслуживанию на томе, например, удаленной дефрагментации.
Имитация клиента после проверки пользователя	Имитация клиента. Пользователь с данной привилегией может имитировать другие учетные записи.
Создание глобальных	Создание именованных объектов сопоставления файлов в глобальном

Привилегия	Описание
объектов	пространстве имен во время удаленных терминальных сессий. Привилегия по умолчанию включена для администраторов, сервисов и учетной записи LocalSystem.

## 10.6 Трафик SoftControl SysWatch

Есть три источника трафика SoftControl SysWatch:

- 1) Оверхеды HTTPS,
- 2) Логи с клиентского устройства,
- 3) Обновления (клиентского модуля и антивирусных баз).

### Оверхеды HTTPS

Трафик оверхедов HTTPS составляет 3,7 КБ за хартбит. (Хартбит – это параметр клиентских компонентов, отвечающий за периодичность установки связи с серверным компонентом SoftControl Server.)

Трафик в месяц от оверхедов HTTPS можно оценить по следующей формуле:  $T1=3,7*30*24*3600/\text{значение хартбита}$  [секунды]. Результат будет выражен в килобайтах в месяц.

### Логи с клиентского устройства

Объем трафика, который генерируется на одно событие, составляет около 500 байт. По количеству событий можно оценить для типового устройства объем трафика, который генерируют логи за сутки, а также заполняемость базы данных.

Чтобы выгрузить сведения о событиях на типовом устройстве за сутки, выполните следующие действия:

1. Откройте в SoftControl Admin Console лог событий для нужного устройства.
2. Выберите в верхней панели меню **Фильтры** → **Фильтры событий SysWatch** → **Все**.

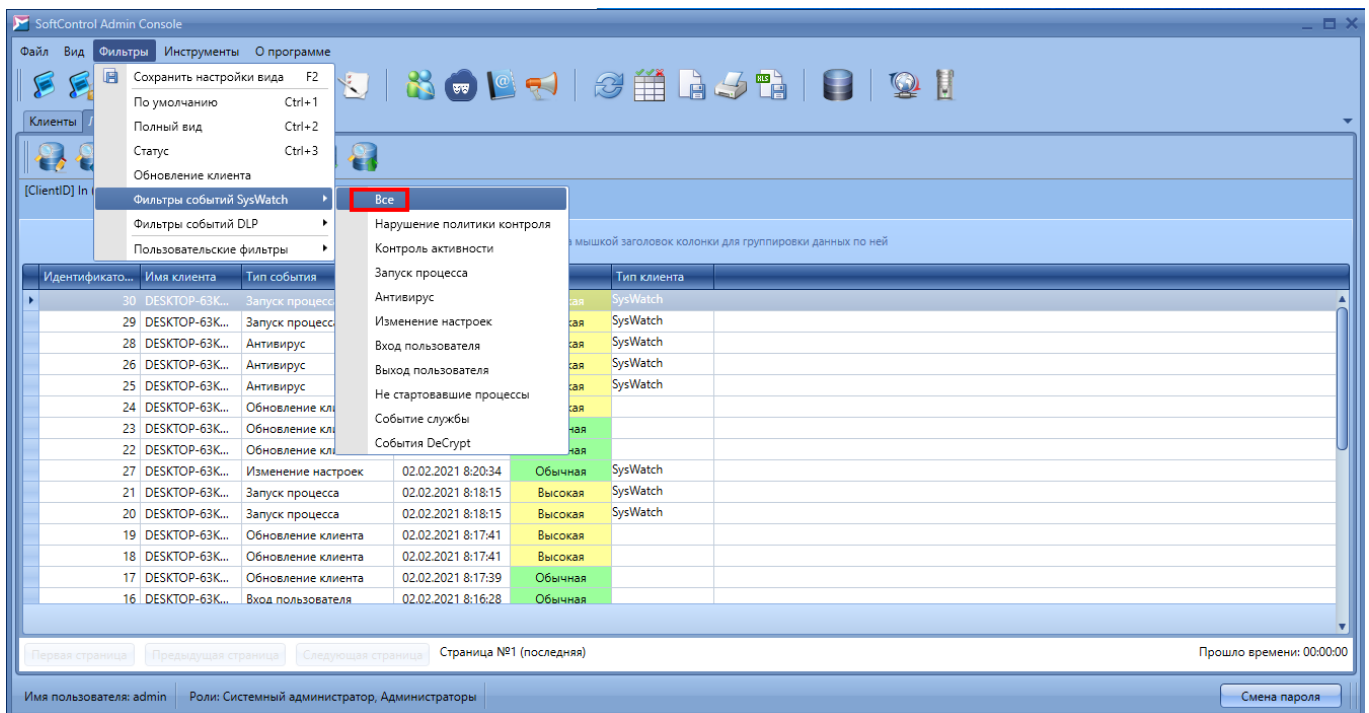



Рисунок 220. Настройка фильтра для лога событий

3. Нажмите на кнопку  (Редактировать запрос). Подробнее см. разделы [Фильтрация событий](#)<sup>159</sup> и [Запросы к базе данных](#)<sup>165</sup>.
4. Чтобы добавить фильтр по времени, нажмите на зеленый кружок со знаком «плюс», затем выберите **Время**, **Между** и задайте интервал в одни сутки.

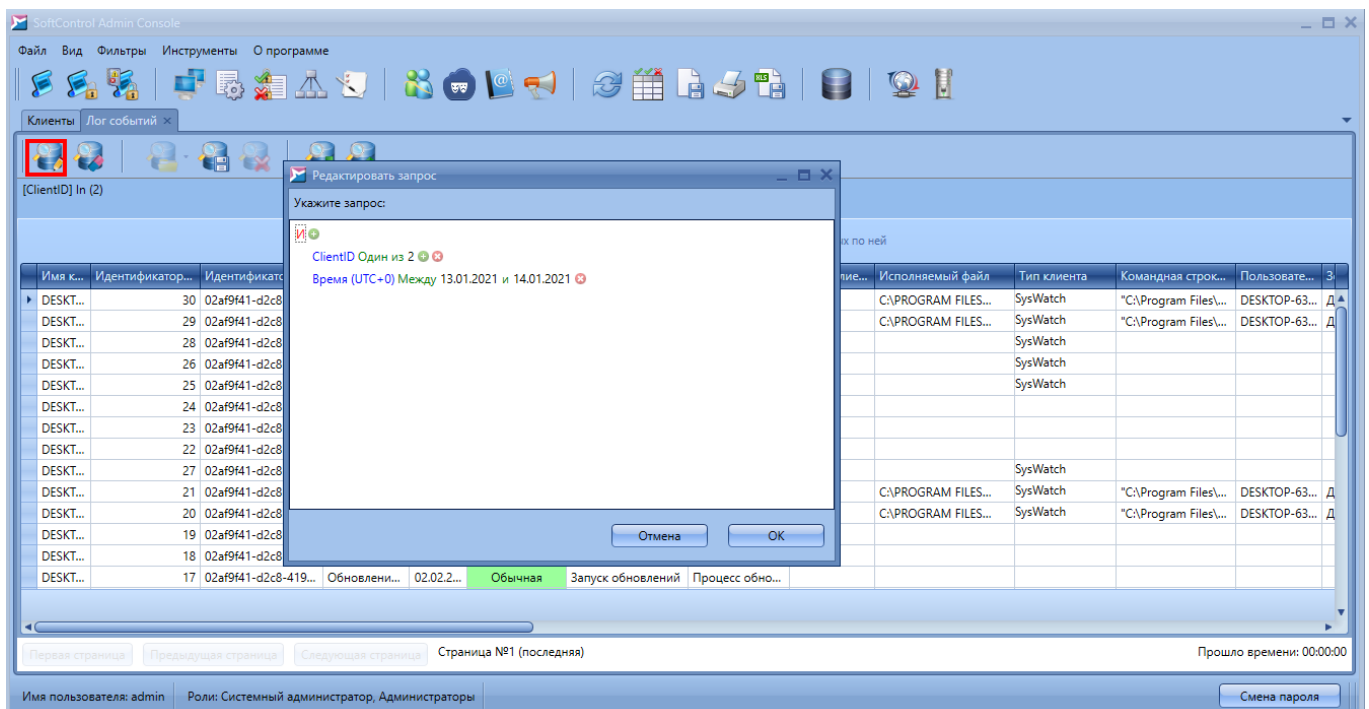


Рисунок 221. Настройка запроса к базе данных. Задание времени



5. На экране появятся записи о событиях, произошедших за указанные сутки. Нажмите на иконку **Экспорт в Excel** и выберите директорию, в которую вы хотите сохранить лог с событиями.

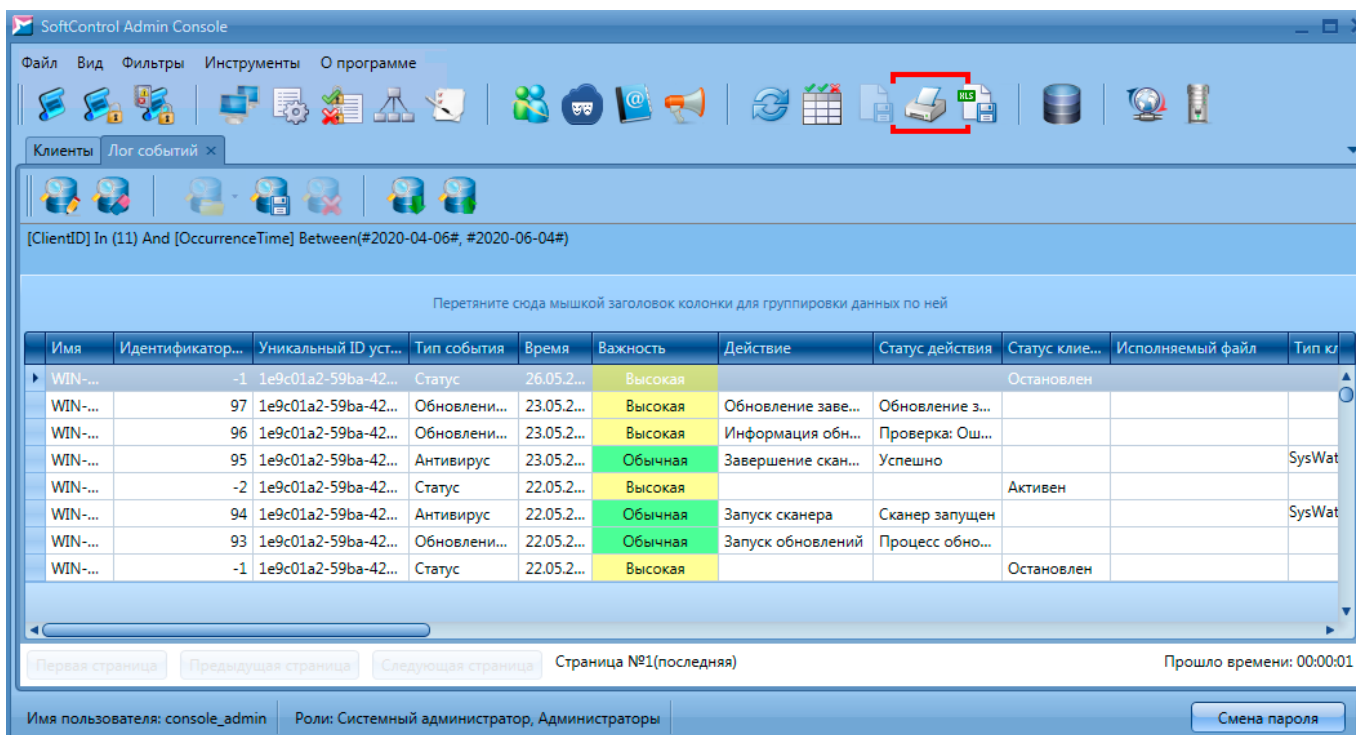


Рисунок 222. Экспорт выборки в файл XLSX

6. В созданном файле посчитайте количество строк. Умножьте это число на 500 байт, и вы получите приблизительный объем трафика за сутки, который приходится на логи от устройства.

## Обновления

### Обновления клиентского модуля

Объем одного обновления составляет 30 МБ. Обновления выходят 3–4 раза в год.

### Обновления антивирусных баз

Объем первого обновления после установки составит 60 МБ. Далее за каждый день объем обновлений может составлять от 400 до 1 300 КБ (по мере выпуска новых антивирусных баз).

## 10.7 Источники

Источники дополнительной информации приведены в табл. 41.

Таблица 41. Вспомогательная документация

Название	Описание
Руководство пользователя SoftControl ATM Client	Руководство по установке, настройке и работе с клиентским компонентом SoftControl ATM Client
Руководство пользователя SoftControl Endpoint Client	Руководство по установке, настройке и работе с клиентским компонентом SoftControl Endpoint Client
Руководство пользователя SoftControl SClient	Руководство по установке, настройке и работе с клиентским компонентом SoftControl SClient
Руководство по установке SoftControl DLP Client	Руководство по установке и настройке клиентского компонента SoftControl DLP Client

## 10.8 Обновление клиентских компонентов и антивирусных баз на Windows XP

Windows XP в зависимости от версии Service Pack может либо вовсе не поддерживать новые сертификаты, либо поддерживать их частично. Это связано с тем, что при их генерации использовались более современные алгоритмы (SHA-256).

Чтобы обновления продуктов SoftControl баз работали корректно, необходимо правильно настроить параметры запуска модулей обновления.

Примечание. Если вы установили приложение SoftControl SysWatch версии 5.1.79 или позднее и при этом ранее это приложение у вас не было установлено, выполнять инструкции из этого раздела не нужно: обновление пройдет корректно. Для SoftControl DLP и SoftControl SysCmd выполнять инструкции из этого раздела не нужно, если у вас версия 6.0.95 или позднее.


1. Откройте в SoftControl Admin Console редактор клиентских настроек.
2. Перейдите в раздел **Модули**.
3. Нажмите на иконку .
4. На вкладке **Идентификационные данные модуля** введите имя модуля (название исполняемого файла) и путь к нему согласно таблице:

Таблица 42. Модули обновления

Обновляемый компонент	Имя модуля	Путь
SoftControl SysWatch	snsupd.exe	C:\PROGRAM FILES\SOFTCONTROL\SYSWATCH\

Обновляемый компонент	Имя модуля	Путь
SoftControl SysCmd	upd.exe	C:\Program Files\SoftControl\SysCmd\Updater
SoftControl DLP Client	upd.exe	C:\Program Files\SafenSoft\DLP Client\Updater

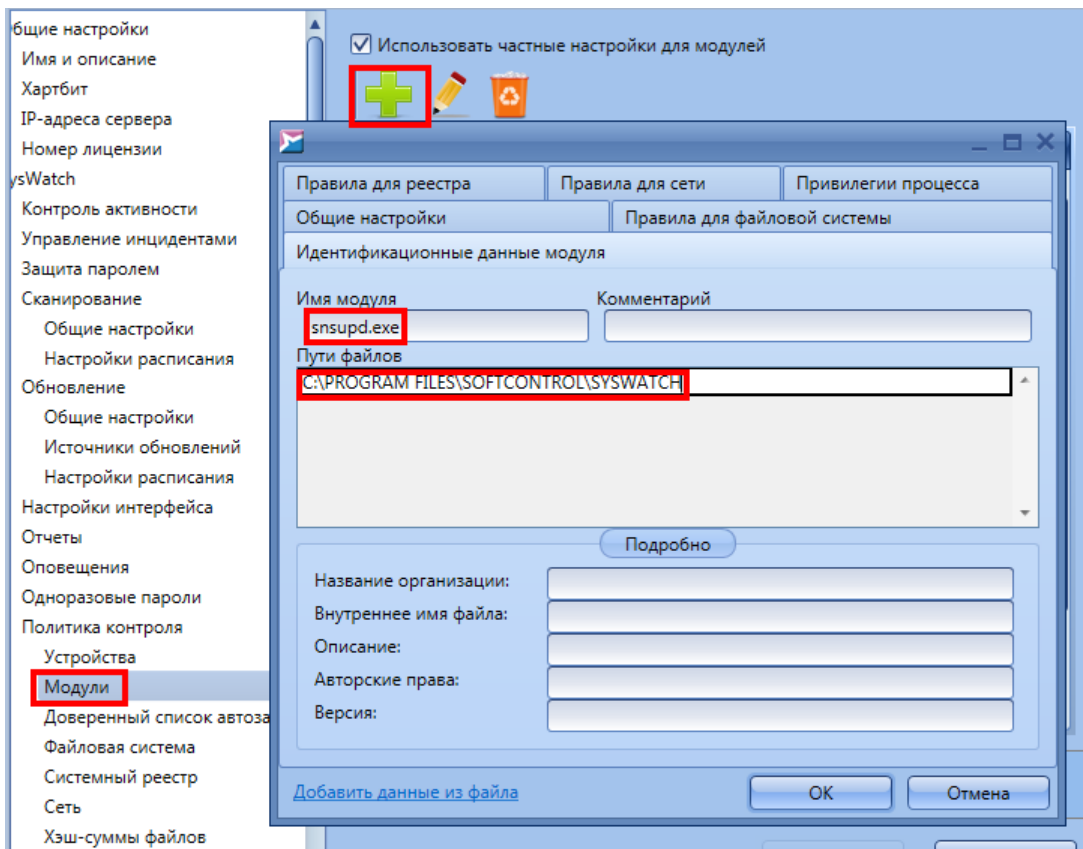


Рисунок 223. Настройка модуля обновления на примере SoftControl SysWatch

5. На вкладке **Общие настройки** выберите зону выполнения **Доверенные приложения** и отметьте флажком **Включить режим обновления ПО**.

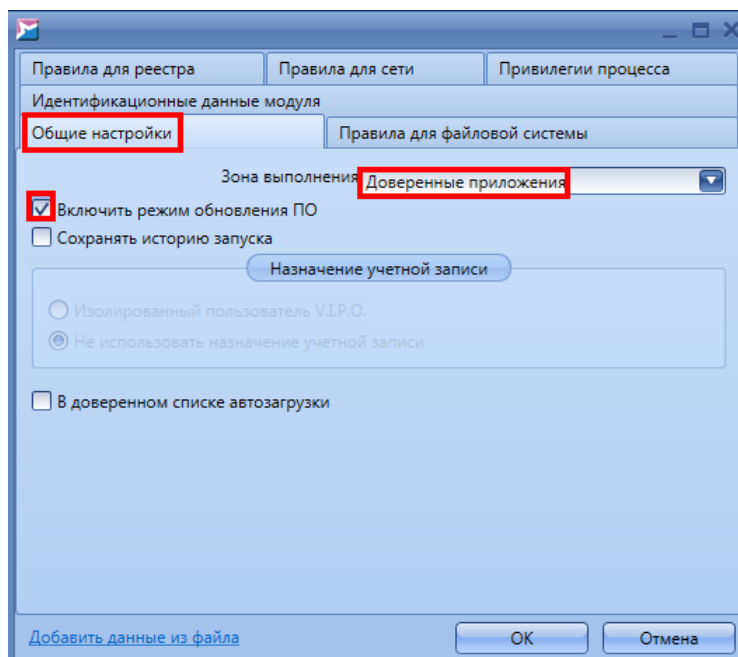


Рисунок 224. Добавление модуля в доверенные приложения

6. Нажмите **ОК**.

7. Сохраните клиентские настройки под новым именем и примените их к подразделению, в котором находятся клиенты, которые необходимо обновить

Если вы настраиваете обновление для SoftControl SysWatch, далее вы можете создать задачу для обновления антивирусных баз или дождаться запуска обновления по расписанию.