SoftControl

TPS 6.1.398

План пилотного проекта по тестированию СЗИ SoftControl

Содержание

1. Методика проведения пилотного проекта

Этот документ предназначен для Заказчика проекта и содержит сведения, необходимые Заказчику для проведения пилотного проекта.

1.1 Цели проведения пилотного проекта

Целью пилотного проекта является проверка заявленных функциональных и эксплуатационных характеристик СЗИ SoftControl, подготовка к развертыванию решения на рабочей инфраструктуре, приобретение навыков эксплуатации программного продукта.

Задачами проведения пилотного проекта являются:

- Тестирование на совместимость:
  - ❑Совместимость с аппаратной конфигурацией устройств;
  - ❑Совместимость с особыми версиями ОС на устройствах;
  - ❑Сетевая совместимость (проверка работоспособности конфигурации клиент-сервер на сетевом оборудовании и производительности каналов связи).
- Проведение эксплуатационных тестов:
  - ❑Локальная и удаленная инсталляция клиентских компонентов системы;
  - ❑Управление групповыми политиками контроля.

1.2 Требования к тестовому стенду пилотного проекта

Для достижения готовности сторон к проведению пилотного тестирования на инфраструктуре Заказчика необходимо подтвердить выполнение технических условий развертывания компонентов SoftControl: серверного модуля SoftControl Service Center, консоли управления SoftControl Admin Console, клиентского модуля SoftControl SysWatch.

Документ http://kb.safensoft.com/index.php/Файл:Технические_условия _Syswatch.pdf подробно описывает технические условия развертывания компонентов SoftControl.

В стенд для пилотного проекта входят следующие устройства.

- Устройство (или виртуальная машина) для развертывания сервера управления. Системные требования указаны в 1.4, таблица 1 [5] .
- Устройство (или виртуальная машина) для первичного развертывания клиента SoftControl SysWatch, подготовки пакетного инсталлятора и проведения эксплуатационных и функциональных тестов (далее по тексту устройство 1). Системные требования указаны в 1.4, таблица 3 [7].
- Устройство, использующееся в инфраструктуре Заказчика и нуждающееся в реализации мер защиты. Используется для проверки развертывания клиента SoftControl SysWatch с помощью пакетного инсталлятора и проведения эксплуатационных и функциональных тестов (далее по тексту типовое устройство). Системные требования указаны в 1.4, таблица 3 [7].

К сетевой инфраструктуре для проведения пилотного проекта предъявляются следующие требования.

- С устройства 1 и типового устройства должны быть доступны порты 8000, 8088 на сервере управления SoftControl Server.
- Для подключения консоли администрирования SoftControl Admin Console на сервере управления должен быть доступен порт 8080.

1.3 Процесс

Тестирование состоит из следующих последовательных этапов:

1) Согласование внутри Заказчика плана тестирования с определением ответственных лиц из организаций-участников проекта.
2) Установка ПО.
3) Проведение эксплуатационных и функциональных тестов.

4) Подведение итогов, заполнение и подписание контрольного списка проведенного тестирования.

Также на всех этапах тестирования происходит взаимное консультирование и обмен информацией между сторонами, участвующими в проекте.

Результаты представляются в виде заполненного контрольного списка проведения тестирования СЗИ SoftControl, содержащего информацию о результатах каждого из описанных в плане тестов на каждом клиентском компоненте пилотной зоны.

Результаты тестирования необходимо использовать для подтверждения соответствия продукта заявленным функциональным и эксплуатационным характеристикам.

Также созданные в ходе тестирования политики контроля, файлы конфигурации, пакетные инсталляторы и инструкции можно применять для развертывания и эксплуатации программного продукта на сети устройств Заказчика.

1.4 Системные требования

Таблица 1. Минимальные системные требования для сервера управления SoftControl Server

ОС	Частота ЦП	Объем ОЗУ	Объем свободного пространства на жестком диске
Клиентские операционные системы:	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*			
Microsoft® Windows® 11 *64-разрядная*			
Серверные операционные системы:			
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*			
Microsoft® Windows® Server 2022 *64-разрядная*			

Дополнительное ПО:

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

Таблица 2. Минимальные системные требования для консоли управления SoftControl Admin Console

ОС	Частота ЦП	Объем ОЗУ	Объем свободного пространства на жестком диске
Клиентские операционные системы:	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*			
Microsoft® Windows® 11 *64-разрядная*			
Серверные операционные системы:			
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*			
Microsoft® Windows® Server 2022 *64-разрядная*			

Дополнительное ПО:

- Microsoft® .NET Framework 4.5.

- Для серверных операционных систем поддерживаются только варианты установки ОС с рабочим столом.

Таблица 3. Минимальные системные требования для клиентского модуля SoftControl SysWatch

ОС	Частота ЦП	Объем ОЗУ	Объем свободного пространства на жестком диске
Клиентские операционные системы:			150 МБ + дополнительно от 120 МБ для хранения антивирусных баз
Microsoft® Windows® XP (SP2) *32-разрядная*[1,2]	800 МГц	512 МБ	
Microsoft® Windows® XP (SP3) *32-разрядная*[1]	800 МГц	512 МБ	
Microsoft® Windows® XP (SP2) *64-разрядная*[1]	800 МГц	512 МБ	
Microsoft® Windows® XP Embedded (SP2 и выше) *32-разрядная*[1]	800 МГц	256 МБ	
Microsoft® Windows® Embedded for Point of Service 1.0 *32-разрядная*[1]	800 МГц	256 МБ	
Microsoft® Windows® 7 (SP1) *32-разрядная*[3]	1 ГГц	1 ГБ	
Microsoft® Windows® 7 (SP1) *64-разрядная*[3]	1 ГГц	2 ГБ	
Microsoft® Windows® 8 *32-разрядная*	1 ГГц	1 ГБ	
Microsoft® Windows® 8 *64-разрядная*	1 ГГц	2 ГБ	
Microsoft® Windows® 8.1 *32-разрядная*	1 ГГц	1 ГБ	
Microsoft® Windows® 8.1 *64-разрядная*	1 ГГц	2 ГБ	
Microsoft® Windows® 10 *32-разрядная*	1 ГГц	1 ГБ	
Microsoft® Windows® 10 *64-разрядная*	1 ГГц	2 ГБ	
Microsoft® Windows® 10 IoT Enterprise *32-разрядная*	1 ГГц	1 ГБ	
Microsoft® Windows® 10 IoT Enterprise *64-разрядная*	1 ГГц	2 ГБ	
Microsoft® Windows® 11 *64-разрядная*	1 ГГц	4 ГБ	
Серверные операционные системы:			
Microsoft® Windows® Server 2003 (SP2) *32-разрядная*[1,4]	800 МГц	512 МБ	
Microsoft® Windows® Server 2003 (SP2) *64-разрядная*[1,4]	800 МГц	512 МБ	
Microsoft® Windows® Server 2008 R2 *64-разрядная*[3,5]	1,4 ГГц	512 МБ	
Microsoft® Windows® Server 2012 *64-разрядная*[5]	1,4 ГГц	512 МБ	

ОС	Частота ЦП	Объем ОЗУ	Объем свободного пространства на жестком диске
Microsoft® Windows® Server 2012 R2 *64-разрядная*[5]	1,4 ГГц	512 МБ	
Microsoft® Windows® Server 2016 *64-разрядная*[5]	1,4 ГГц	2 ГБ	
Microsoft® Windows® Server 2019 *64-разрядная*[5]	1,4 ГГц	2 ГБ	
Microsoft® Windows® Server 2022 *64-разрядная*[5]	1,4 ГГц	2 ГБ	

Дополнительные требования:

1. Visual C++ 2008 SP1 Redistributable Package x86 (в т. ч. для 64-разрядных ОС).
2. Windows XP SP2 может требовать дополнительных условий эксплуатации (подробнее см. Обновление приложения SoftControl SysWatch и антивирусных баз на Windows XP SP2 (86)).
3. Обновление KB3033929 или любое его замещающее (поддержка алгоритма хэширования SHA-256 при проверке цифровой подписи).
4. Обновление KB968730 или любое его замещающее (поддержка алгоритма хэширования SHA-256 при проверке цифровой подписи).
5. Поддерживаются только варианты установки ОС с рабочим столом.

2. Контрольный список проведения тестирования

2.1 Проверка готовности инфраструктуры Заказчика для развертывания компонент SoftControl TPSecure

2.1.1 Проверка выполнимости технических условий развертывания SoftControl TPSecure

Таблица 4. Проверка выполнимости

№ пп.	Действие	Ожидаемый результат	Комментарий
4.1	Заполнение опросного листа об аппаратно-программных характеристиках устройств пилотной зоны и рабочей станции для развертывания серверного компонента SoftControl Service Center.	❑ Заполнен опросный лист.	Необходимо предоставить сведения об используемом антивирусном и специализированном ПО для выдачи рекомендаций по тонкой настройке совместимости с СЗИ SoftControl. Инструкции по настройке совместимости см. в *SW_4.2_and_higher+KAV+NOD32.docx*.
4.2	Проверка соответствия аппаратно-программных характеристик устройств указанным в опросном листе техническим условиям		
4.2.1	Проверка соответствия аппаратно-программных характеристик рабочей станции для развертывания серверного компонента SoftControl Service Center.	❑ Характеристики соответствуют ТУ.	Для развертывания серверного компонента SoftControl Service Center требуется установка на рабочую станцию компонента Microsoft .Net Framework 4.5.Ссылка на программу установки Microsoft .Net Framework 4.5: https://www.microsoft.com/ru-ru/download/details.aspx?id=42642.
4.2.2	Проверка наличия компонента Filter Manager в операционной системе устройств.	❑ Подтверждено наличие компонента Filter Manager в системе.	Реализуется на устройстве выполнением запроса в командной строке.**

** В командной строке ввести *sc query fltmgr* и нажать **Enter**. В случае, если компонент установлен, появится сообщение о его состоянии; в противном случае – сообщение об ошибке.

2.2 Развертывание тестового стенда SoftControl

2.2.1 Развертывание серверного компонента SoftControl Service Center

Таблица 5. Развертывание SoftControl Service Center

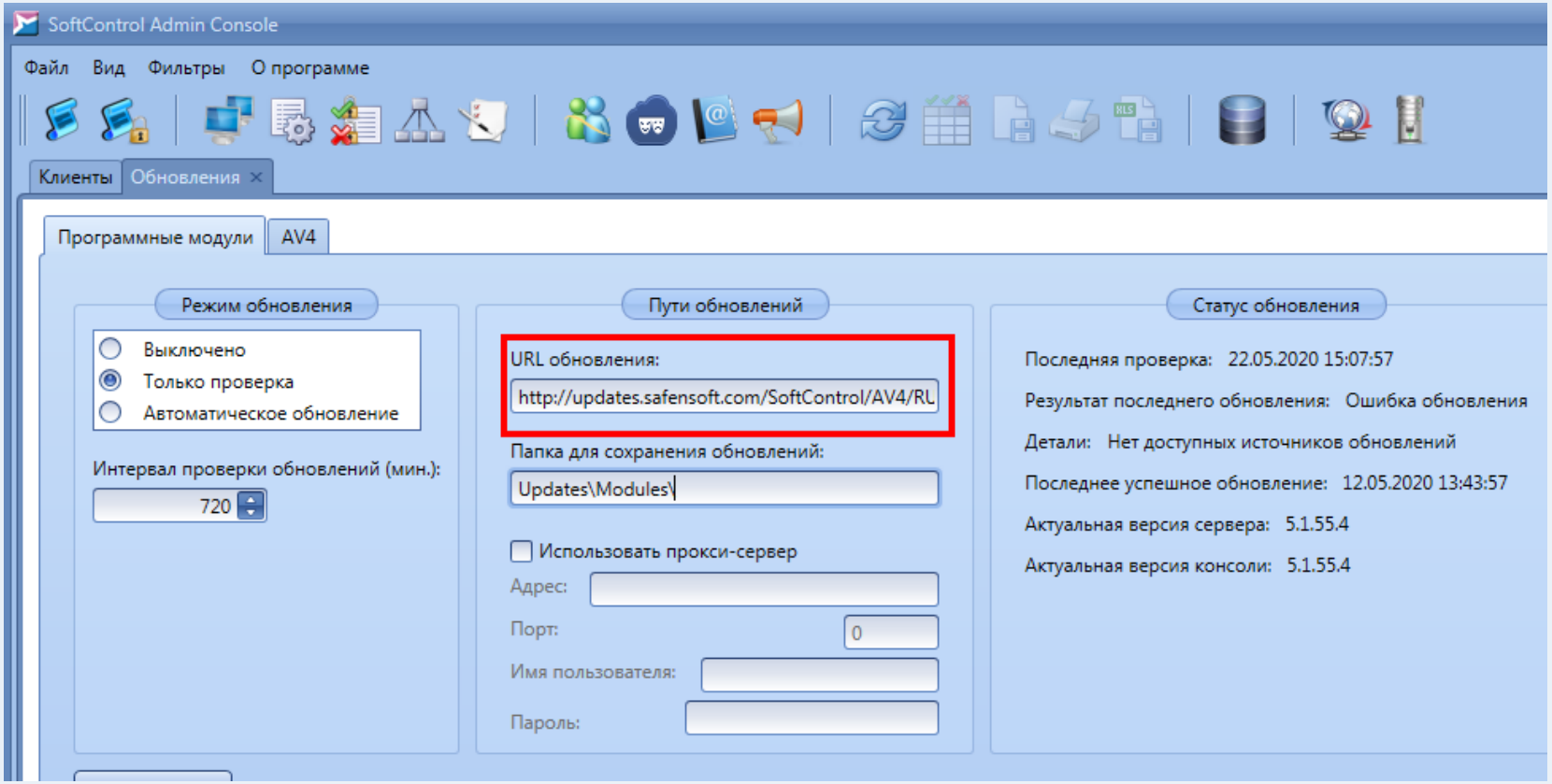
№ пп.	Действие	Ожидаемый результат	Комментарий
5.1	Установлены компоненты SoftControl Server, SoftControl Admin Console, СУБД MS SQL 2014 Express.	❑ Установка и первичное конфигурирование серверного компонента выполнено успешно.	Установка производится силами специалиста Заказчика. Требуются права администратора системы. Установка производится из единого инсталлятора в режиме **Полная***; установятся компоненты: • сервер управления SoftControl Server; • консоль администрирования SoftControl Admin Console; • СУБД Microsoft SQL 2014 Express.
* Возможна установка на промышленную СУБД MSSQL Server, при этом необходимо выбрать тип установки **Выборочная**; в этом случае встроенная в дистрибутив СУБД Microsoft SQL 2014 Express не устанавливается.			
5.2	Конфигурирование серверного компонента SoftControl Service Center		Конфигурирование производится силами Заказчика
5.2.1	Создана учетная запись Администратора SoftControl Service Center, задан пароль Администратора SoftControl Service Center.	❑ Задан пароль Администратора SoftControl Service Center.	Пароль создает специалист Заказчика. Требования к паролю: не менее 7 символов, цифры, буквы латинского алфавита, заглавные и строчные буквы, спецсимволы (см. п. 3.2 «Настройка сервера» документа «Руководство администратора SoftControl Service Center»).
5.2.2	Заданы основной и резервные IP-адреса сервера управления SoftControl Server.	❑ В консоли управления SoftControl Admin Console в области «Хост клиентов» отображаются заданные IP-адреса.	Требуется информация об IP-адресе рабочей станции, доступном для устройств. Требуется информация о возможных резервных IP-адресах (опционально).
5.2.3	Осуществлен вход Администратора в консоль SoftControl Admin Console.	❑ Вход осуществлен успешно.	

5.2.4	Проведена настройка путей обновления антивирусных баз и программных модулей.*	❑ Проведена настройка путей обновления модулей и антивирусных баз.	Предполагается, что у сервера управления SoftControl Service Center есть доступ в сеть интернет для скачивания антивирусных баз и обновлений программных модулей. Если доступа в сеть интернет нет, то имеется возможность скачивать обновления антивирусных баз и программных модулей в ручном режиме.

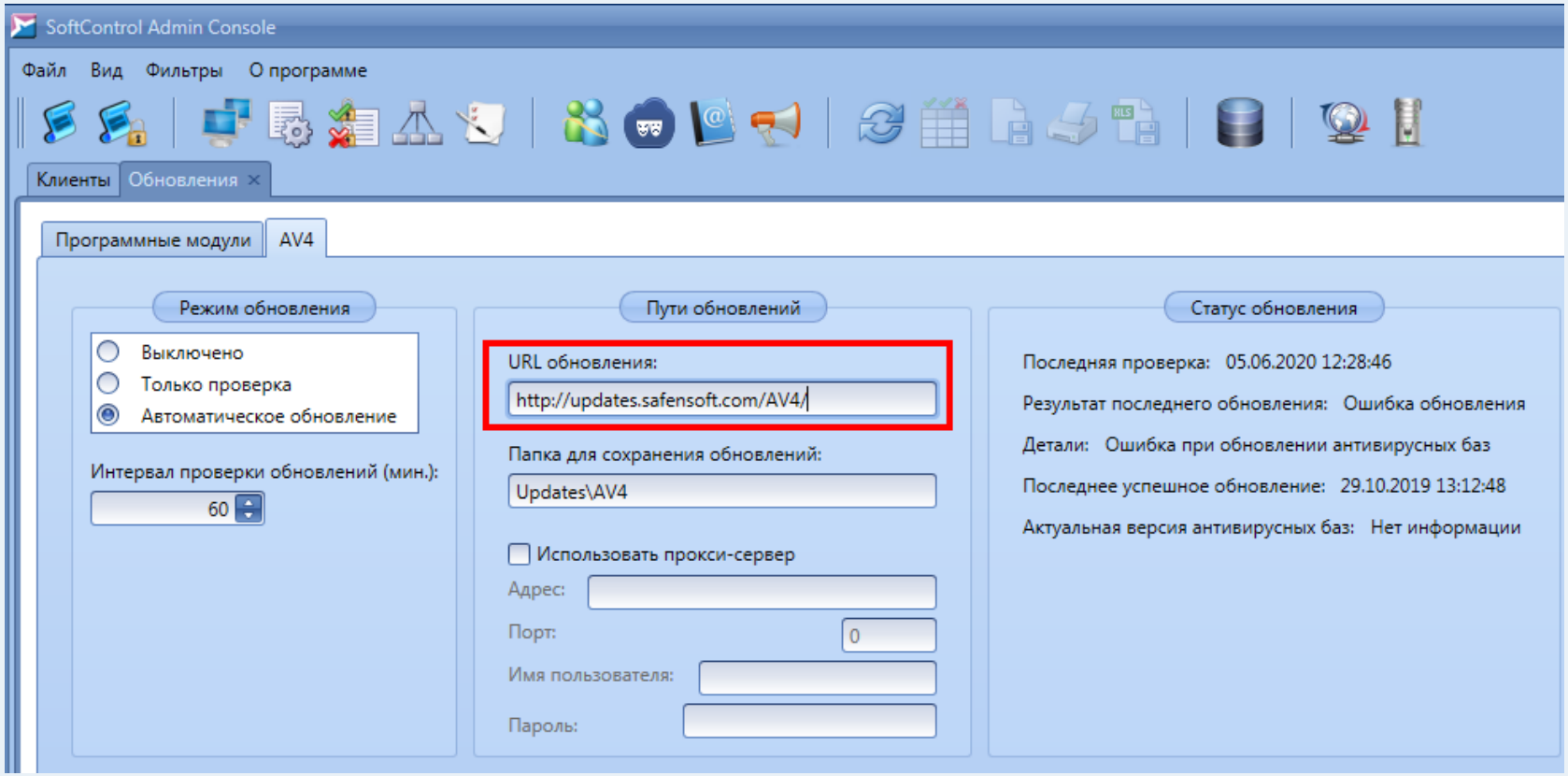
* Для настройки обновления антивирусных баз и программных модулей на сервере управления SoftControl Service Center необходимо:

1) В SoftControl Admin Console щелкнуть левой кнопкой мыши по пиктограмме  (**Обновления**).

2) В открывшемся окне на вкладке **Программные модули** в блоке **Пути обновлений** поле **URL обновления** отредактировать следующим образом. В путь обновления `http://updates.safensoft.com/SoftControl/AV4/RU/` необходимо вставить ваш тестовый (релизный) лицензионный ключ: `http://updates.safensoft.com/<лицензионный ключ>/SoftControl/AV4/RU/`. Для вкладки **Программные модули** рекомендуется **Режим обновления** оставить в положении **Только проверка**.



3) Для настройки обновлений антивирусных баз на вкладке **Антивирусные базы** в блоке **Пути обновлений** поле **URL обновления** отредактировать следующим образом. В путь обновления `http://updates.safensoft.com/AV4/` необходимо вставить ваш тестовый (релизный) лицензионный ключ: `http://updates.safensoft.com/<лицензионный ключ>/AV4/`. Для вкладки **Антивирусные базы** рекомендуется **Режим обновления** оставить в положении **Автоматическое обновление**.



5.3	Скопирован и сохранен файл конфигурации первичного соединения клиентских модулей SoftControl SysWatch к серверу управления SoftControl Server – *ClientSettings.xmlc*.	❑ Выгружен файл настроек *ClientSettings.xmlc*.	Файл *ClientSettings.xmlc* расположен на сервере управления в папке *C:\ProgramData\SafenSoft*.

2.2.2 Развертывание клиентского модуля SoftControl SysWatch на устройстве 1

Таблица 6. Развертывание SoftControl SysWatch

№ пп.	Действие	Ожидаемый результат	Комментарий
6.1	Проведено самотестирование устройства с целью проверки работоспособности и функциональности.	❑ Самотестирование функционирования устройства проведено успешно.	Самотестирование функционирования устройства проводится специалистом Заказчика.
6.2	Установка и первичное конфигурирование клиентского компонента SoftControl SysWatch		
6.2.1	Проведена установка клиентского компонента SoftControl SysWatch в режиме логирования.* В зависимости от наличия установленного антивируса выбран дистрибутив клиентского модуля: • *SysWatch.msi* со встроенным антивирусом; • *SysWatch_Patch.msi* без антивируса.	❑ Установка прошла успешно, журнал установки не содержит ошибок.	Требуются права администратора системы. Если производится установка *SysWatch_Patch.msi* без антивируса, то в установленном на устройстве антивирусе необходимо провести настройки совместимости (см. документ *SW_<version_number_and_higher>+KAV +NOD32.docx*).

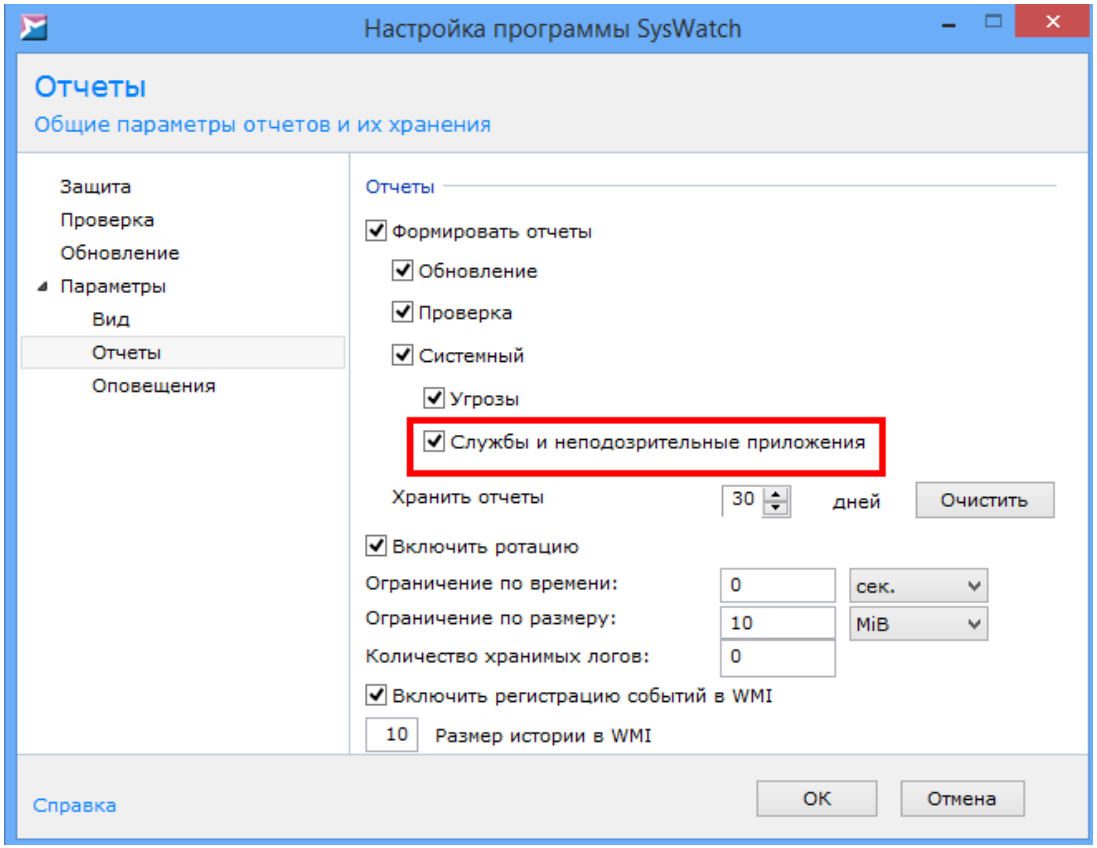
* Установка в режиме логирования производится из командной строки:

- `msiexec /i "C:\Installers\SysWatch.msi" /log C:\Installers\installlog.txt`
- `msiexec /i "C:\Installers\SysWatch_Patch.msi" /log C:\Installers\installlog.txt`

При установке клиентского модуля SoftControl SysWatch на этапе пилотного проекта снимите галочку **Включить сбор профиля после установки**. В связи с тем, что сбор профиля – операция продолжительная, сравнимая по времени выполнения с антивирусным сканированием, при развертывании на слабых устройствах (устройствах самообслуживания, банкоматах, консолях АСУ ТП) возможна установка клиентского модуля SoftControl SysWatch без сбора профиля. Сбор профиля в этом случае можно сделать удаленно с помощью задачи с сервера управления SoftControl Service Center. Вариант с установкой клиентского модуля SoftControl SysWatch с помощью пакетного инсталлятора без сбора профиля, с последующим обновлением антивирусных баз и сбором профиля с помощью задачи с сервера рассмотрен в пункте Удаленное развертывание клиентского компонента SoftControl SysWatch из пакетного инсталлятора на типовом устройстве 36.

6.2.2	Создание предустановленных параметров политик контроля SoftControl SysWatch		В частных случаях задаются рекомендуемые параметры для конкретных устройств (см. документ *TPS_<version_number>-Deployment_Guide-RU.pdf*).
6.2.2.1	Включено логирование служб и неподозрительных приложений.*	❑ В журнале *system_.txt* содержатся события активности процессов в системе.	Для целей получения подробного журнала событий активности процессов в системе устройства и возможности определения конфликтов и создания исключений в правилах контроля.

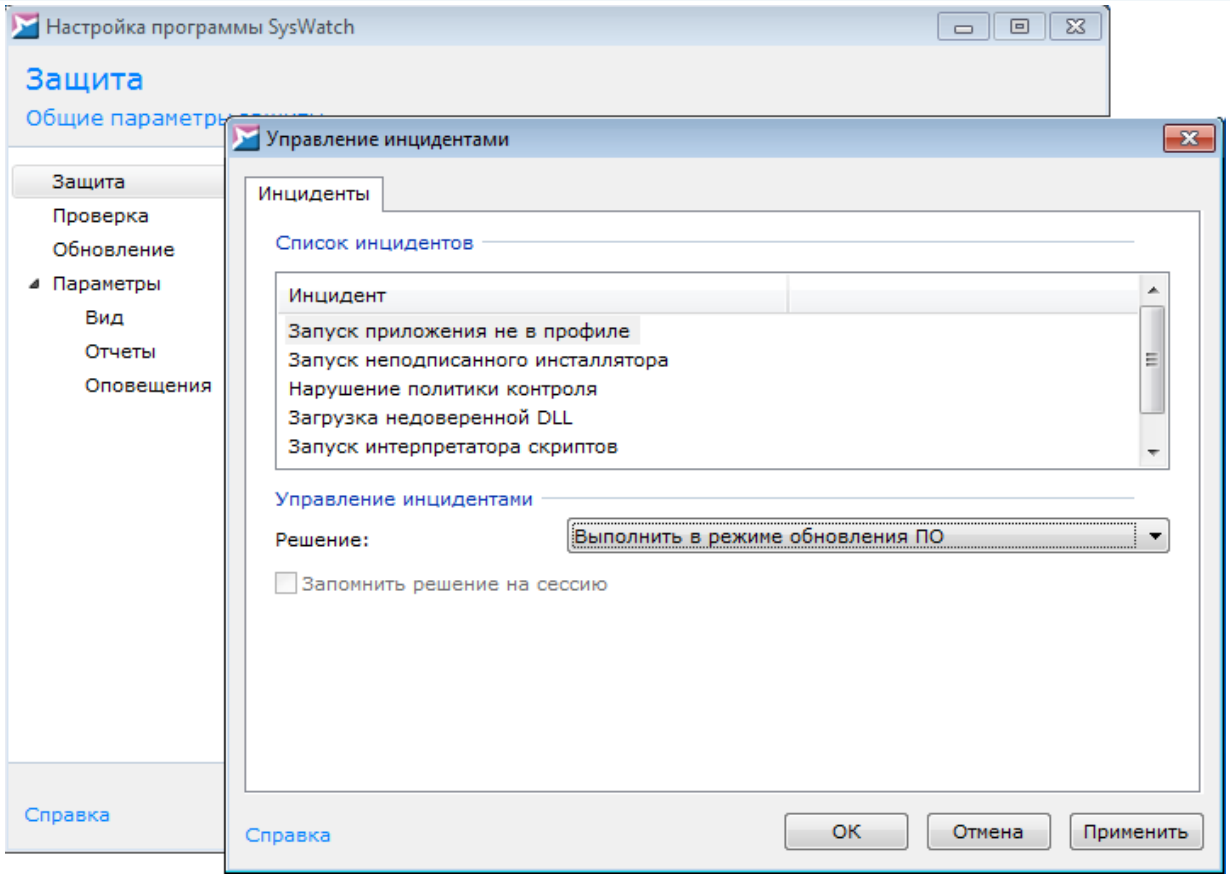
* Для включения **Логирования служб и неподозрительных приложений** необходимо в области системных уведомлений (system tray) щелкнуть правой кнопкой мыши по значку SoftControl SysWatch и выбрать во всплывающем меню пункт **Настройка**. Далее в левой области выбрать пункт **Отчеты** и убедиться, что выставлена галочка **Службы и неподозрительные приложения**; если не выставлена, то выставить ее и нажать на кнопку **ОК** для применения настроек.

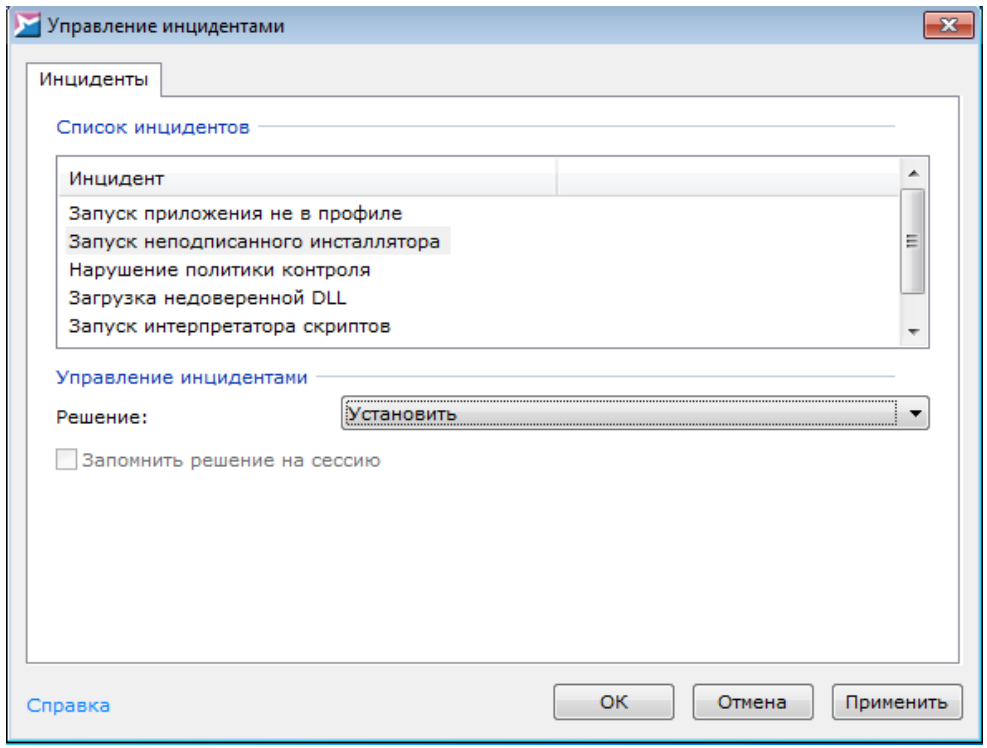


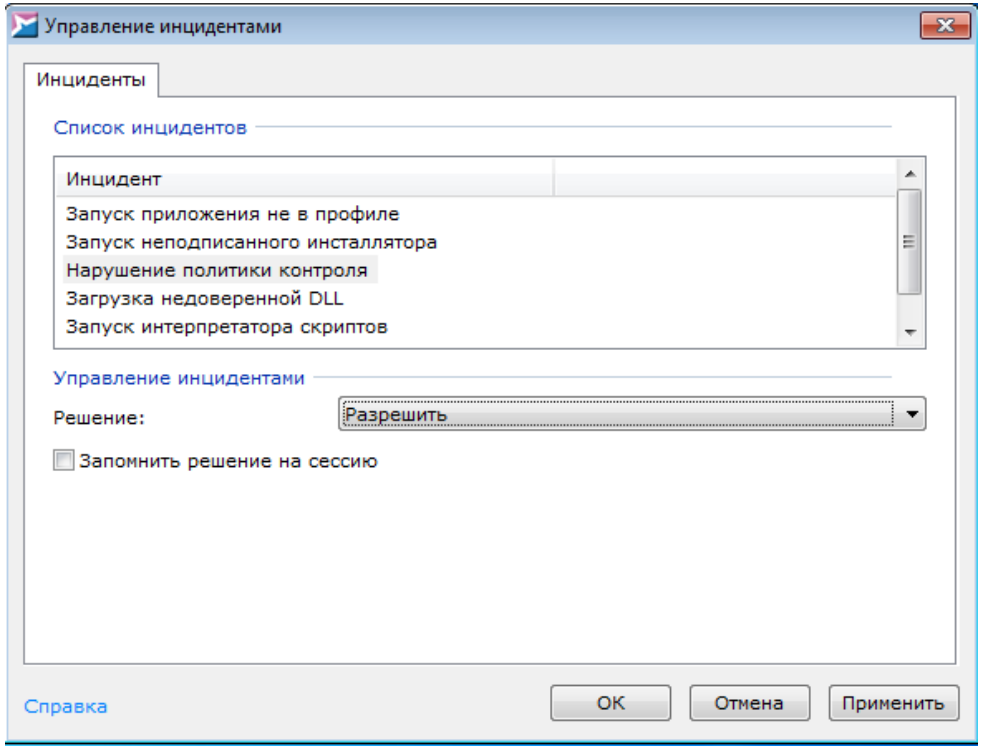
6.2.2.2	Включен режим аудита.*	❑ Режим аудита включен.	В данном режиме клиентский модуль SoftControl SysWatch не производит блокировку по событиям **Запуск приложения не в профиле**, **Запуск неподписанного инсталлятора**, **Нарушение политики контроля**, **Загрузка недоверенной DLL**, **Запуск интерпретатора скриптов**, **Модификация PE-файла не инсталлятором**, что исключает влияние механизмов контроля модуля защиты на работу системных процессов и приложений.

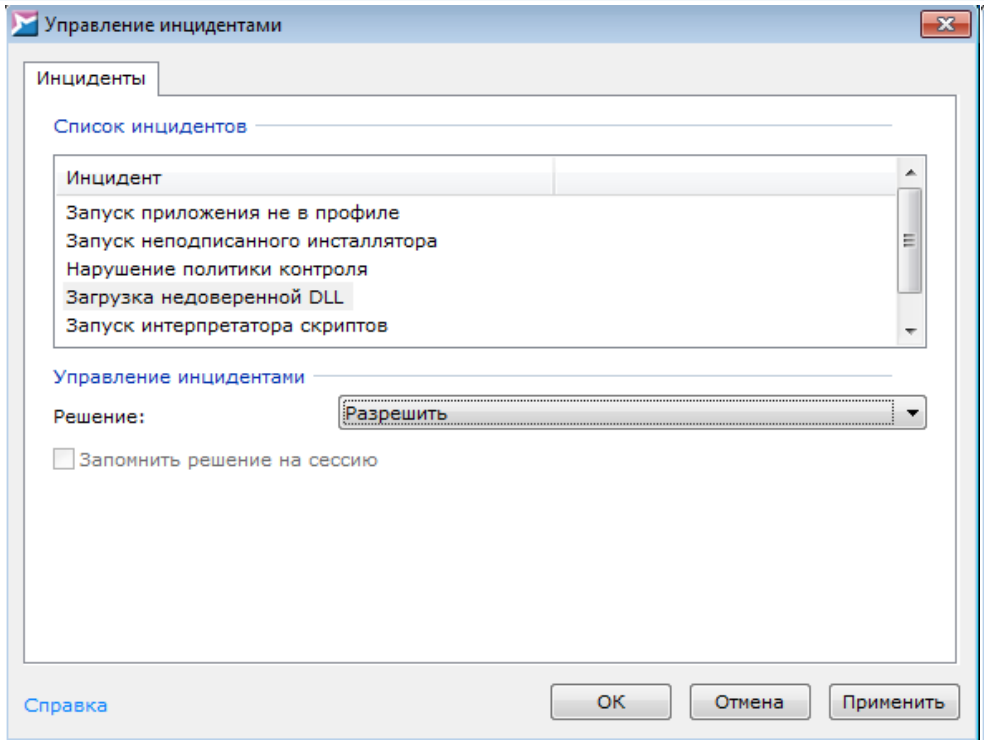
* Для включения режима аудита необходимо в области системных уведомлений (system tray) щелкнуть правой кнопкой мыши по значку SoftControl SysWatch и выбрать во всплывающем меню пункт **Настройка**. Далее в левой области выбрать пункт **Защита**, в области **Управление инцидентами** убедиться, что выставлена галочка **Включить автоматическую обработку инцидентов**, и нажать на кнопку **Настроить**. В настройках **Управление инцидентами** выбрать следующие настройки:

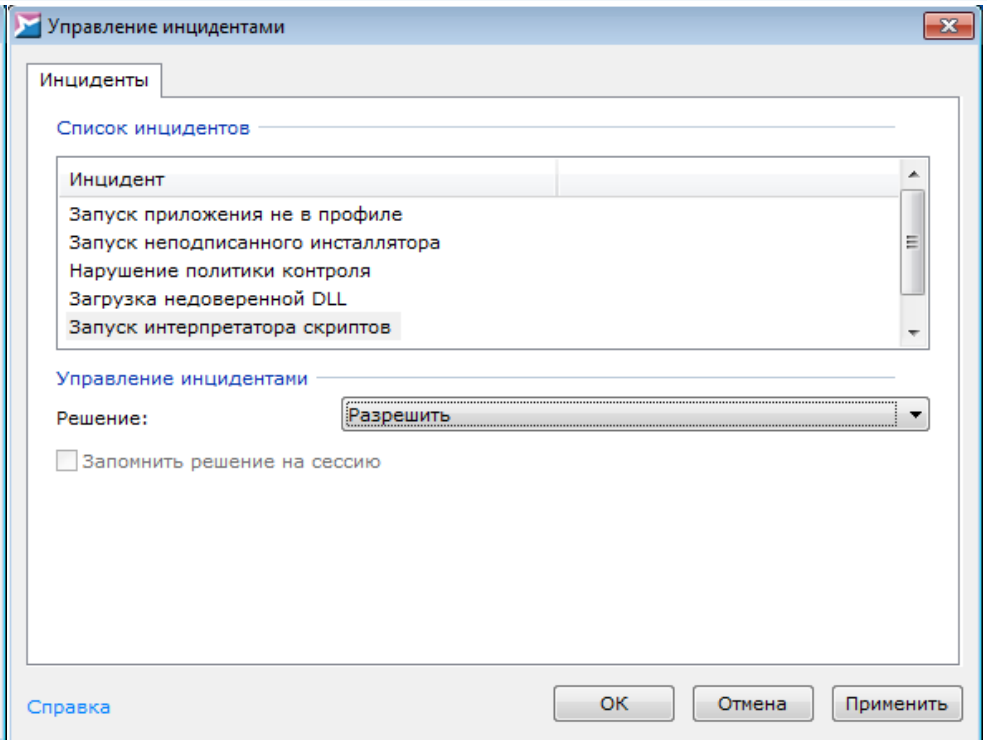
- Запуск приложения не в профиле – Выполнить в режиме обновления ПО;
- Запуск неподписанного инсталлятора – Установить;
- Нарушение политики контроля – Разрешить;
- Загрузка недоверенной DLL – Разрешить;
- Запуск интерпретатора скриптов – Разрешить;
- Модификация PE-файла не инсталлятором – Разрешить.

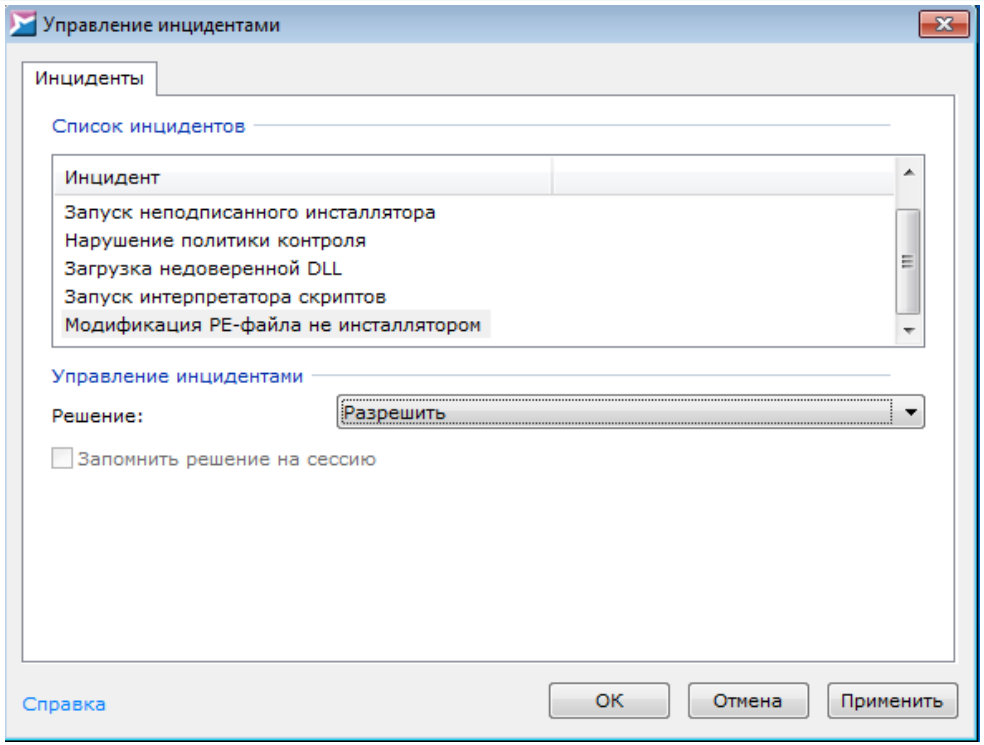

Настройка программы SysWatch
Защита
Общие параметры
Защита
Проверка
Обновление
Параметры
Вид
Отчеты
Оповещения
Справка
Управление инцидентами
Инциденты
Список инцидентов
Инцидент
Запуск приложения не в профиле
Запуск неподписанного инсталлятора
Нарушение политики контроля
Загрузка недоверенной DLL
Запуск интерпретатора скриптов
Управление инцидентами
Решение:
Выполнить в режиме обновления ПО
Запомнить решение на сессию
Справка
OK
Отмена
Применить


Управление инцидентами
Инциденты
Список инцидентов
Инцидент
Запуск приложения не в профиле
Запуск неподписанного инсталлятора
Нарушение политики контроля
Загрузка недоверенной DLL
Запуск интерпретатора скриптов
Управление инцидентами
Решение:
Установить
Запомнить решение на сессию
Справка
OK
Отмена
Применить


Управление инцидентами
Инциденты
Список инцидентов
Инцидент
Запуск приложения не в профиле
Запуск неподписанного инсталлятора
Нарушение политики контроля
Загрузка недоверенной DLL
Запуск интерпретатора скриптов
Управление инцидентами
Решение:
Разрешить
Запомнить решение на сессию
Справка
OK
Отмена
Применить


Управление инцидентами
Инциденты
Список инцидентов
Инцидент
Запуск приложения не в профиле
Запуск неподписанного инсталлятора
Нарушение политики контроля
Загрузка недоверенной DLL
Запуск интерпретатора скриптов
Управление инцидентами
Решение:
Разрешить
Запомнить решение на сессию
Справка
OK
Отмена
Применить

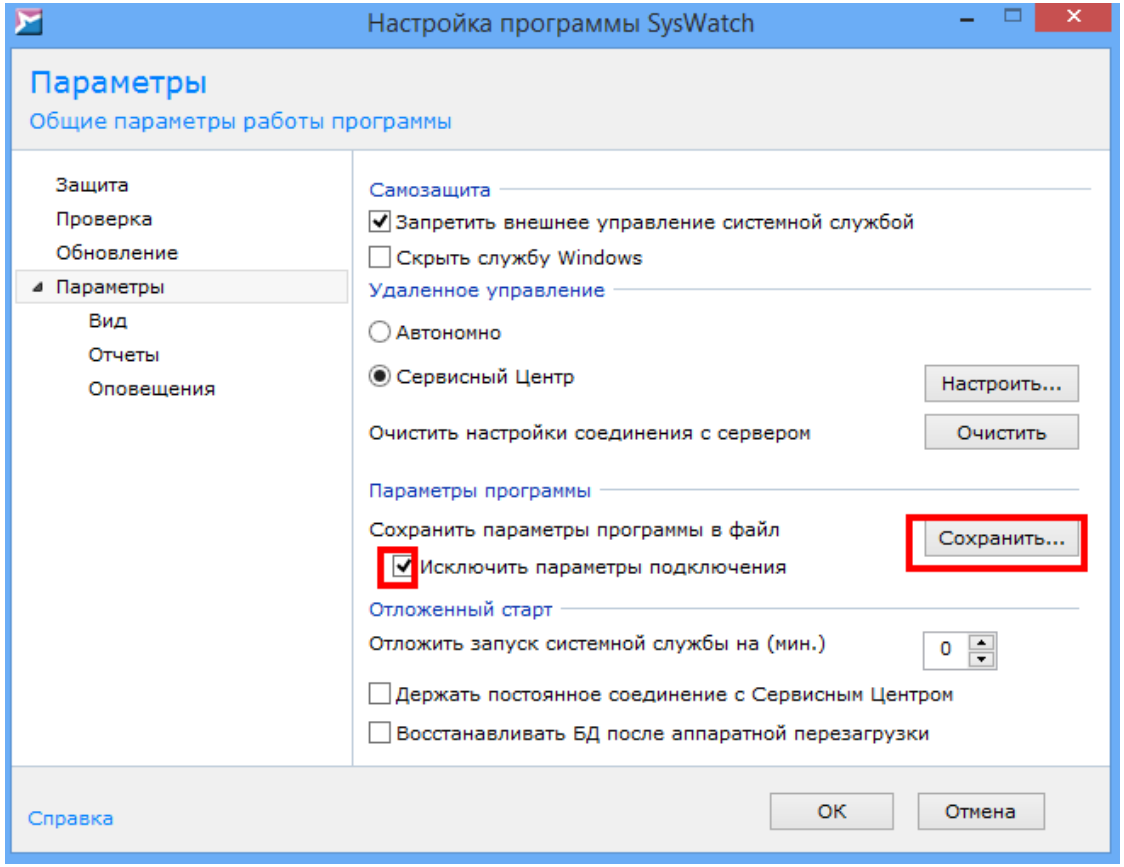

Управление инцидентами
Инциденты
Список инцидентов
Инцидент
Запуск приложения не в профиле
Запуск неподписанного инсталлятора
Нарушение политики контроля
Загрузка недоверенной DLL
Запуск интерпретатора скриптов
Управление инцидентами
Решение:
Разрешить
Запомнить решение на сессию
Справка
OK
Отмена
Применить

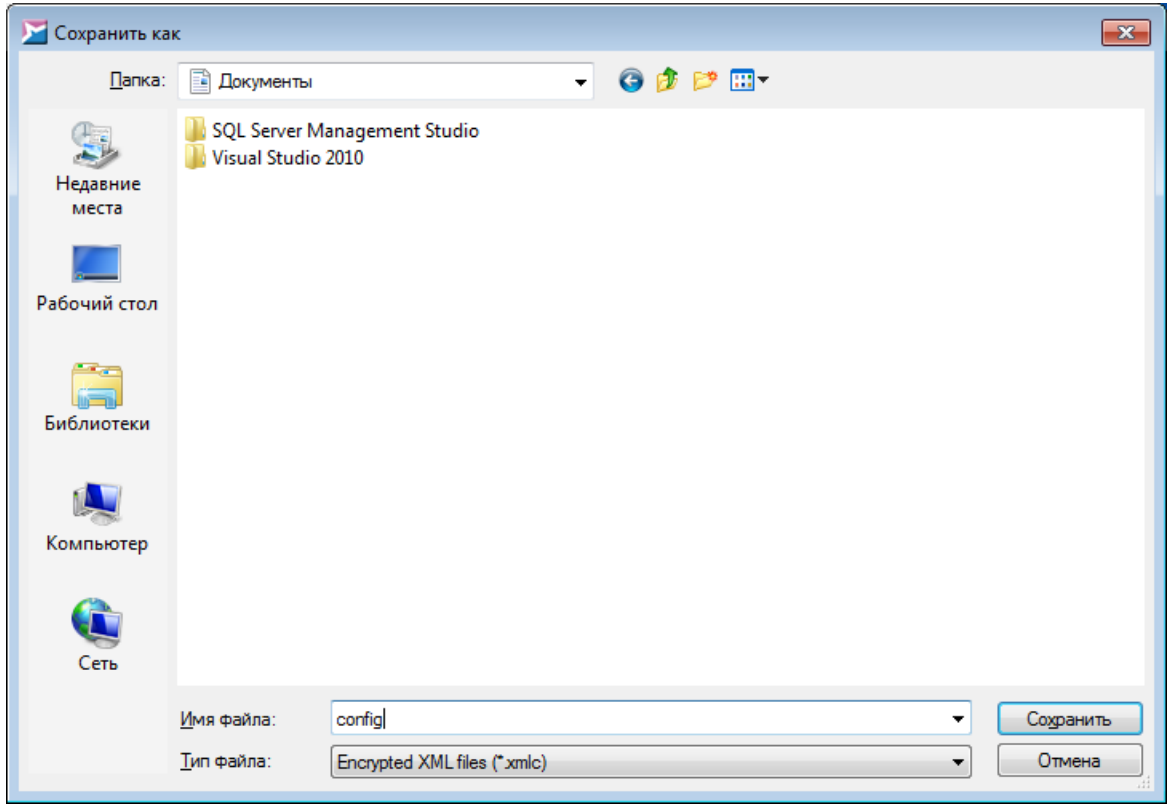


После изменения настроек нажать на кнопку **Применить**.

6.2.3	Выгружен *Config.xmlc*, конфигурационный файл клиентского модуля SoftControl SysWatch на устройстве, содержащий предустановленные настройки совместимости и исключения политик контроля.*	❑ Выгружен и сохранен файл *Config.xmlc*.	Конфигурационный файл будет использован для создания пакетного инсталлятора.

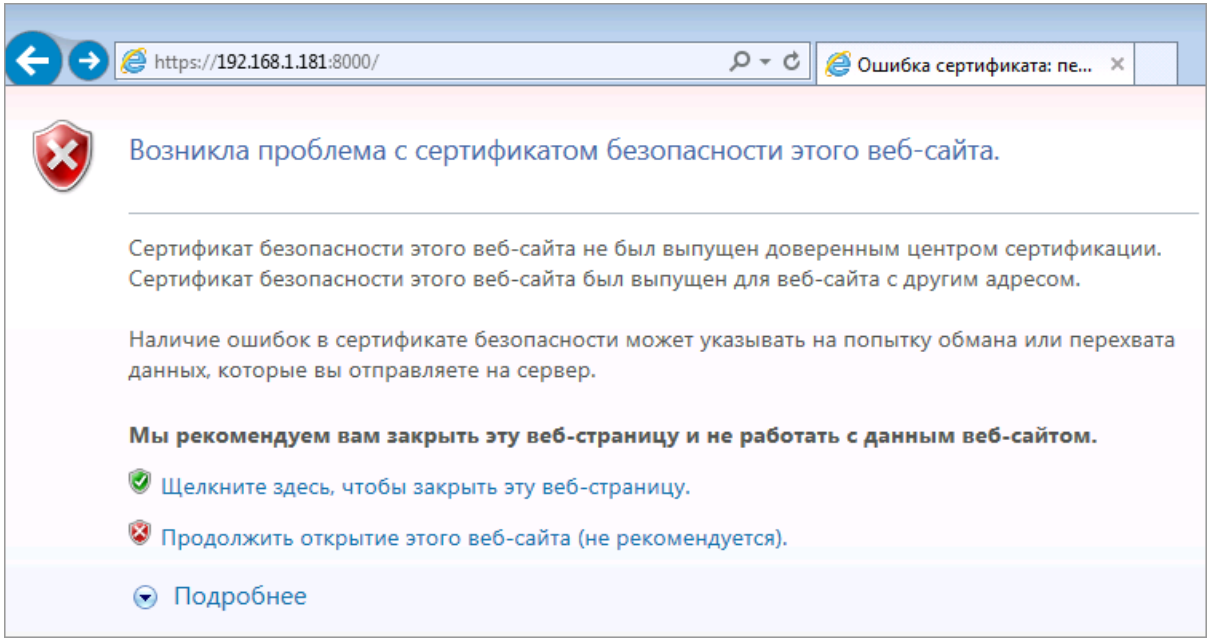
* Для выгрузки конфигурационного файла *Config.xmlc* необходимо в области системных уведомлений (system tray) щелкнуть правой кнопкой мыши по значку SoftControl SysWatch и выбрать во всплывающем меню пункт **Настройка**. В левой области выбрать пункт меню **Параметры**, в пункте **Параметры программы** выставить галочку в поле **Исключить параметры подключения** и нажать на кнопку **Сохранить**. В открывшемся окне выбрать какую-либо папку (например, **Мои документы**) и сохранить файл под именем *Config.xmlc*.





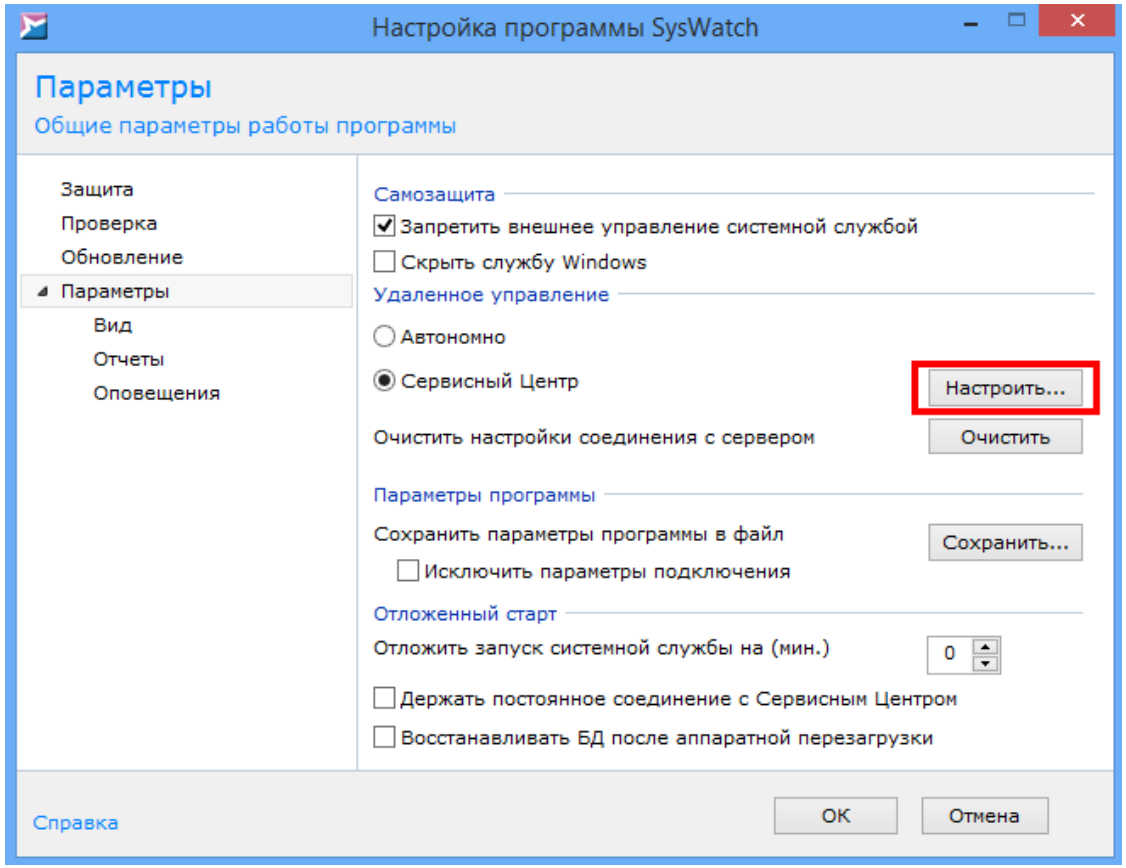
6.3	Произведена проверка сетевой конфигурации устройств в части доступности связи по портам 8000 и 8088 между устройствами и сервером управления.*	❑ Подтверждено наличие связи по портам.	В случае если рабочая станция для развертывания серверного компонента SoftControl Service Center находится в домене, требуется добавить сертификат сервера в доверенные в настройках политик домена.

* С клиентского устройства в браузере Internet Explorer ввести адрес сервера управления SoftControl Service Center и порт подключения клиента (по умолчанию 8000), например, https://192.168.1.181:8000. Если сервер доступен, браузер должен вывести сообщение про неизвестный сертификат. Если SoftControl Admin Console установлена на отдельном от SoftControl Server компьютере, то для проверки связи с SoftControl Service Center необходимо в браузере Internet Explorer ввести адрес сервера и порт подключения SoftControl Admin Console (по умолчанию 8088), например, http://192.168.1.181:8088. Если сервер доступен, браузер должен вывести сообщение про неизвестный сертификат:

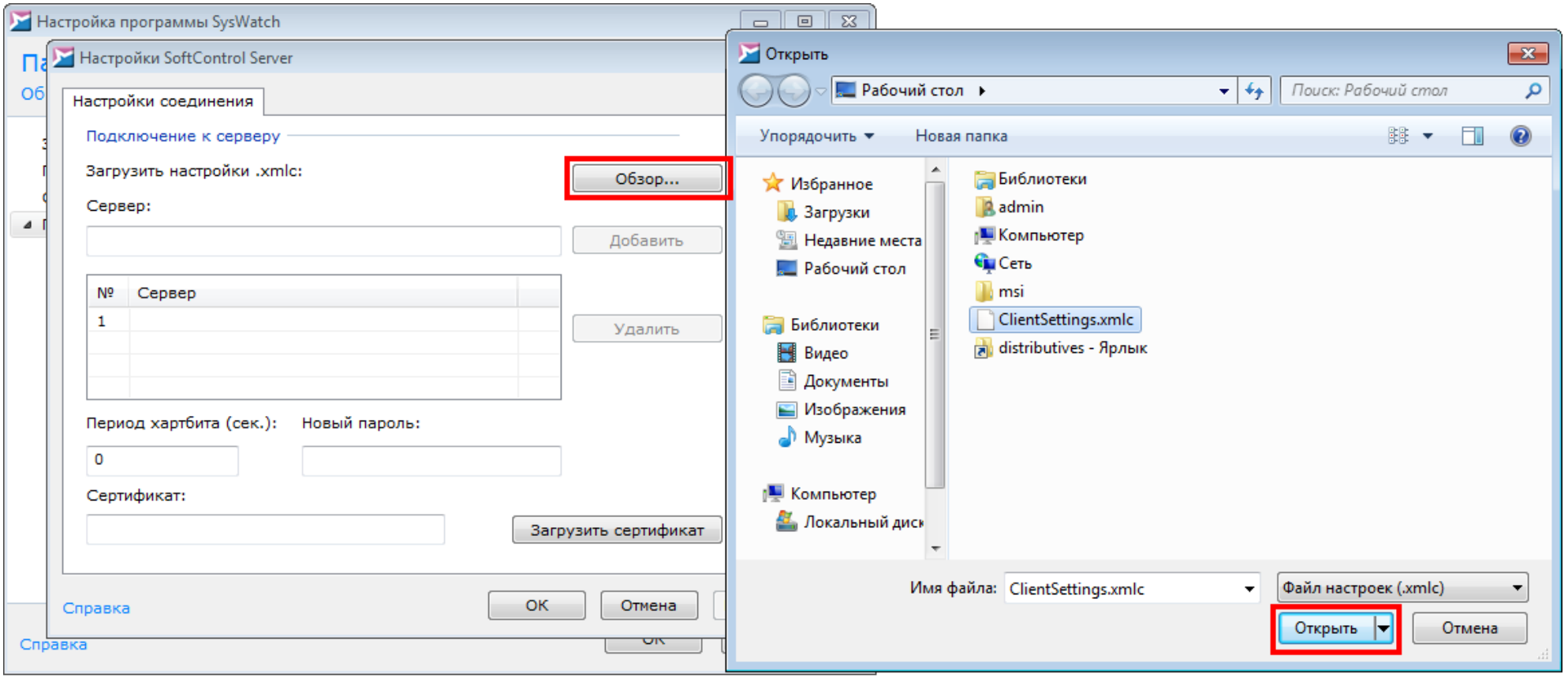


6.4	Проведено подключение клиентского модуля SoftControl SysWatch к серверу управления SoftControl Service Center.*	❑ Запрос на подключение к серверу отправлен.	

* Для подключения клиентского модуля к серверу управления SoftControl Service Center необходимо в области системных уведомлений (system tray) щелкнуть правой кнопкой мыши по значку SoftControl SysWatch и выбрать во всплывающем меню пункт **Настройка**. В левой области выбрать пункт меню **Параметры**, в пункте **Удаленное управление** поставить переключатель в положение **Сервисный Центр** и нажать на кнопку **Настроить**.



В появившемся окне нажать на кнопку **Обзор** и открыть файл *ClientSettings.xmlc*, полученный в п. 5.3 [14] настоящей методики и предварительно скопированный на клиентское устройство:



Далее в окне **Настройка SoftControl Server** необходимо нажать на кнопку **Применить** для отправки запроса на подключение к серверу управления SoftControl Service Center.

6.5	Проведена перезагрузка клиентского устройства.	❑ Клиентское устройство перезагружено.	

6.6	Проведено самотестирование устройства с целью проверки работоспособности и функциональности.	❑ Самотестирование функционирования устройства проведено успешно.	Самотестирование функционирования устройства проводится специалистом Заказчика.
6.7	Проведен сбор логов SNSDumpTool.*	❑ Сбор логов проведен успешно. Сформирован файл *C:\SNS\SnsDump.zip*.	Для сбора логов необходимы права администратора.
* Для сбора логов SNSDumpTool необходимо скачать утилиту для соответствующей версии ОС: • `http://updates.safensoft.com/<номер_лицензии>/39/TOOLS/Setup_SnsDumpTool_x64.exe`, • `http://updates.safensoft.com/<номер_лицензии>/39/TOOLS/Setup_SnsDumpTool_x86.exe` и запустить скачанный файл от имени администратора.			
6.8	В ООО "АРУДИТ СЕКЬЮРИТИ" предоставлены выгруженный конфигурационный файл из предыдущего раздела (5.3 [14]) и логи SNSDumpTool (*C:\SNS\SnsDump.zip*).	❑ Файлы *ClientSettings.xmlc* и *SnsDump.zip* отправлены по адресу support@safensoft.com.	Необходимо для диагностики в случае проблем с развертыванием.

2.3 Эксплуатационные и функциональные тесты SoftControl

2.3.1 Создание пакетного инсталлятора клиентского компонента SoftControl SysWatch

Таблица 7. Создание пакетного инсталлятора

№ пп.	Действие	Ожидаемый результат	Комментарий
7.1	Создан пакетный инсталлятор клиентского компонента SoftControl SysWatch,[1] содержащий: • дистрибутив клиентского компонента SoftControl SysWatch (*SysWatch.msi* или *SysWatch_Patch.msi*); • файл конфигурации первичного подключения к серверу управления SoftControl Service Center (*ClientSettings.xmlc*);[2] • файл конфигурации предустановленных настроек (*Config.xmlc*) в режиме	❑ Создан cmd-скрипт или sfx-архив с расширением *.exe* с перечисленным содержимым.	Пакетный инсталлятор собирается специалистом Заказчика. Для установки необходимы права администратора.

	аудита;[3] • сертификат VeriSign Class 3 Public Primary Certification Authority – *G5.cer*;[4] • скрипт установки, помещающий сертификат клиентского модуля SoftControl SysWatch в хранилище Windows;[5] • скрипт-сценарий запуска пакетного инсталлятора в тихом режиме с логированием процесса установки.		

[1] Для создания пакетного инсталлятора необходимо поместить дистрибутив SoftControl SysWatch, файлы конфигурации, при необходимости сертификат, которым подписан дистрибутив SoftControl SysWatch, и скрипт установки пакетного инсталлятора в папку.
Ниже приведен пример скрипта пакетной установки *install-sns.cmd*:

```
@echo off
Set folder=C:\SnS-install
set workdir=%~dp0
set config=%folder%config.xmlc
echo making directory
md %folder%
echo copy files
xcopy "%workdir%ClientSettings.xmlc" %folder% /Y
xcopy "%workdir%config.xmlc" %folder% /Y
xcopy "%workdir%SysWatch.msi" %folder% /Y
xcopy "%workdir%VeriSign Class 3 Public Primary Certification Authority - G5.cer" %folder% /Y
echo install cert
certutil -addstore Root "C:\SnS-install\VeriSign Class 3 Public Primary Certification Authority - G5.cer"
echo install syswatch
call %WINDIR%\system32\msiexec.exe /i "C:\SnS-install\SysWatch.msi" configfilename="C:\SnS-install\config.xmlc" tsconfig="C:\SnS-install
\ClientSettings.xmlc" /quiet /norestart /log "C:\SnS-install\install-log.txt"
echo exit
exit
```

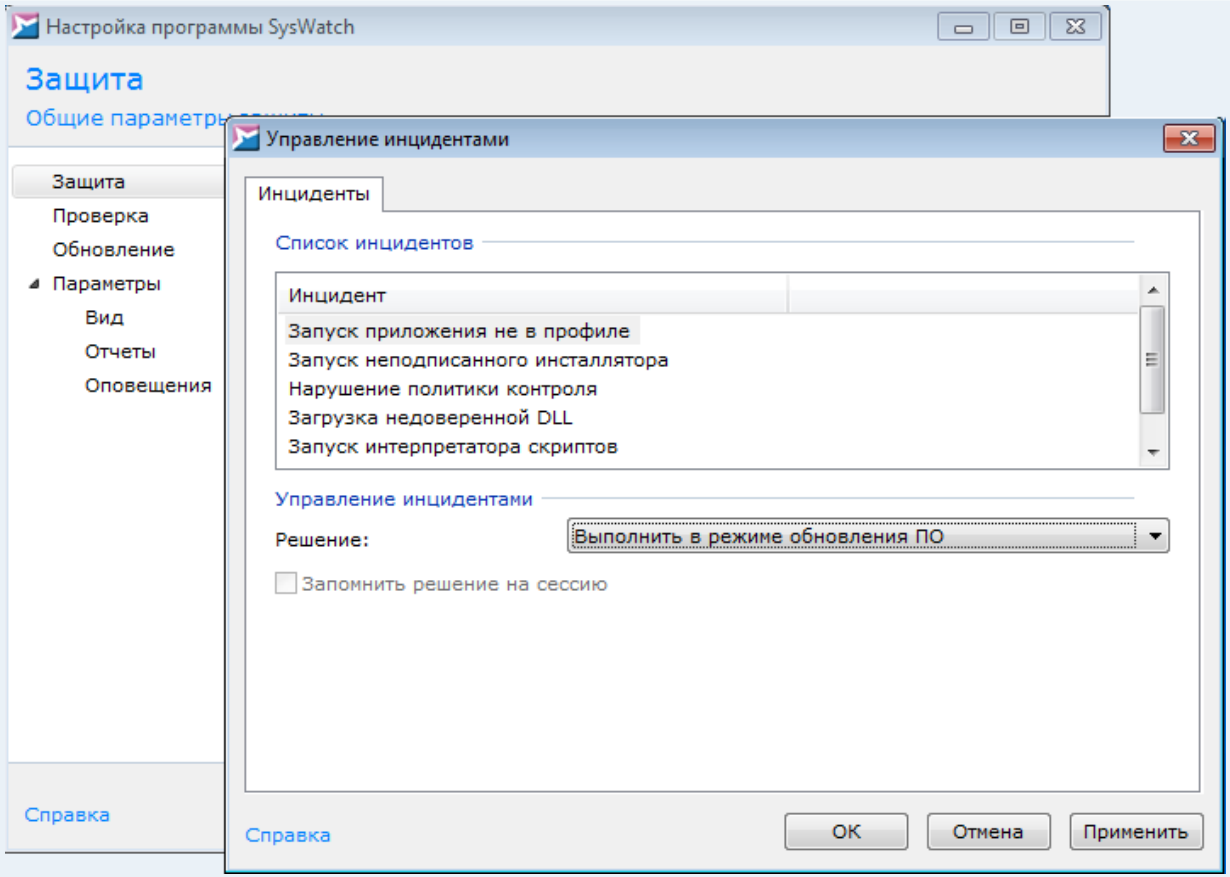
```
@echo off
Set folder=C:\Sns-install
set workdir=%~dp0
set config=%folder%config.xmlc
echo making directory
md %folder%
echo copy files
xcopy "%workdir%ClientSettings.xmlc" %folder% /Y
xcopy "%workdir%config.xmlc" %folder% /Y
xcopy "%workdir%SysWatch.msi" %folder% /Y
xcopy "%workdir%VeriSign Class 3 Public Primary Certification Authority - G5.cer" %folder% /Y
echo install cert
certutil -addstore Root "C:\SnS-install\VeriSign Class 3 Public Primary Certification Authority - G5.cer"
echo install syswatch
call %WINDIR%\system32\msiexec.exe /i "C:\SnS-install\SysWatch.msi" configfilename="C:\SnS-install\config.xmlc" tsconfig="C:\SnS-install
\ClientSettings.xmlc" /quiet /norestart /log "C:\SnS-install\install-log.txt"
echo exit
exit
```

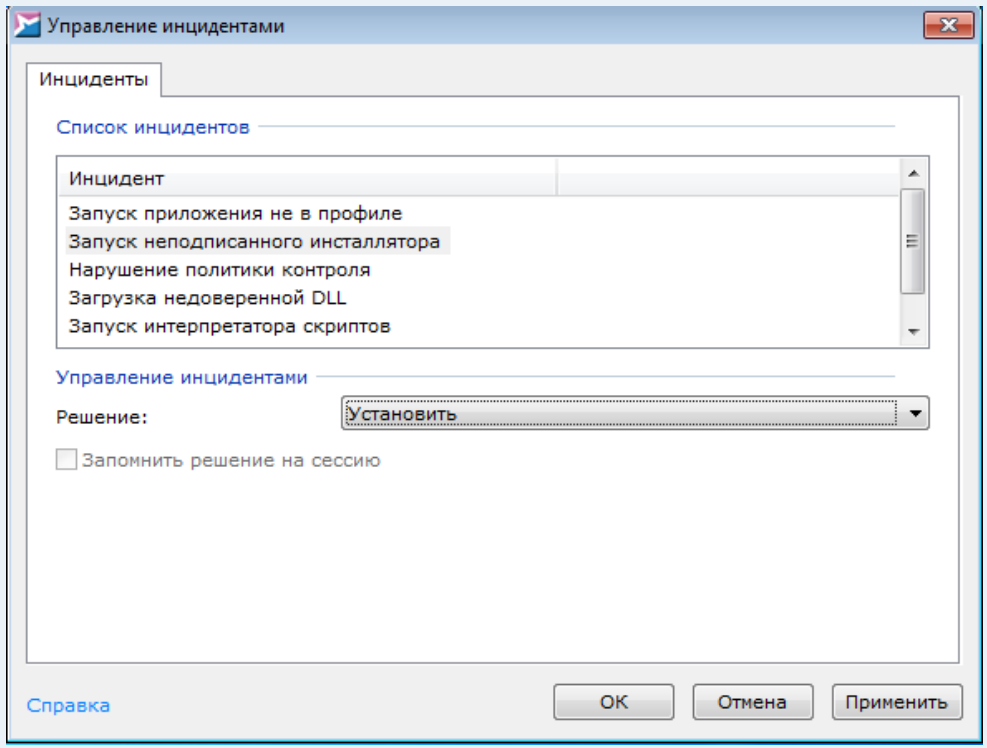
При необходимости данный скрипт может быть преобразован в sfx-архив и подписан сертификатом Заказчика.

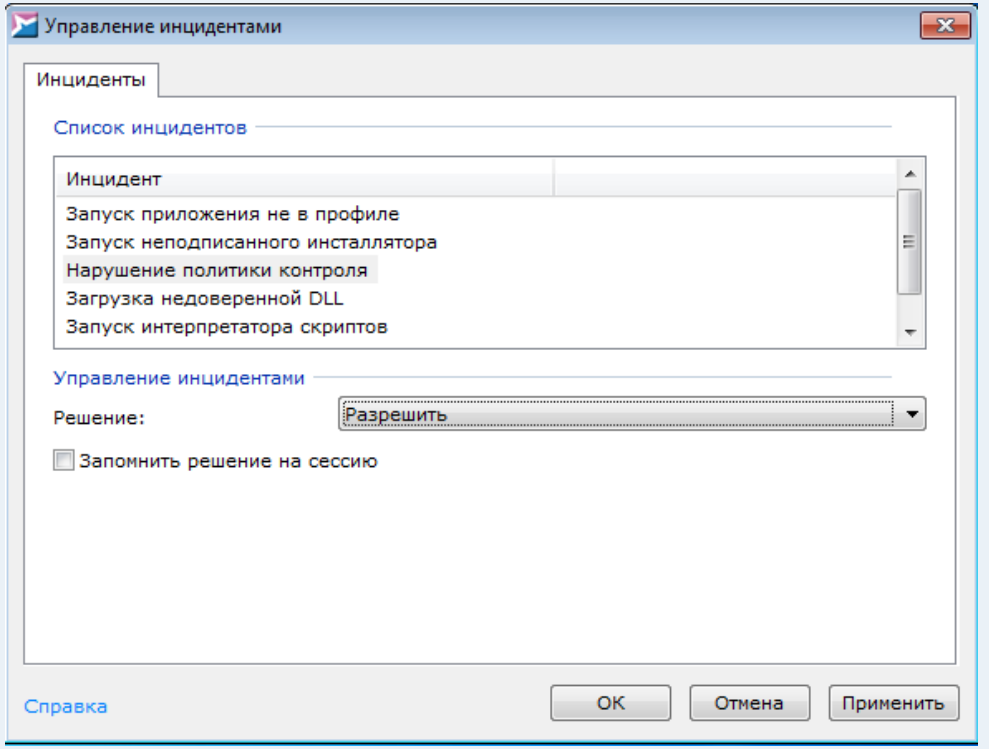
[2] Файл конфигурации первичного подключения к серверу управления SoftControl Service Center (*ClientSettings.xmlc*) расположен на сервере управления в папке *C:\ProgramData\SafenSoft*.

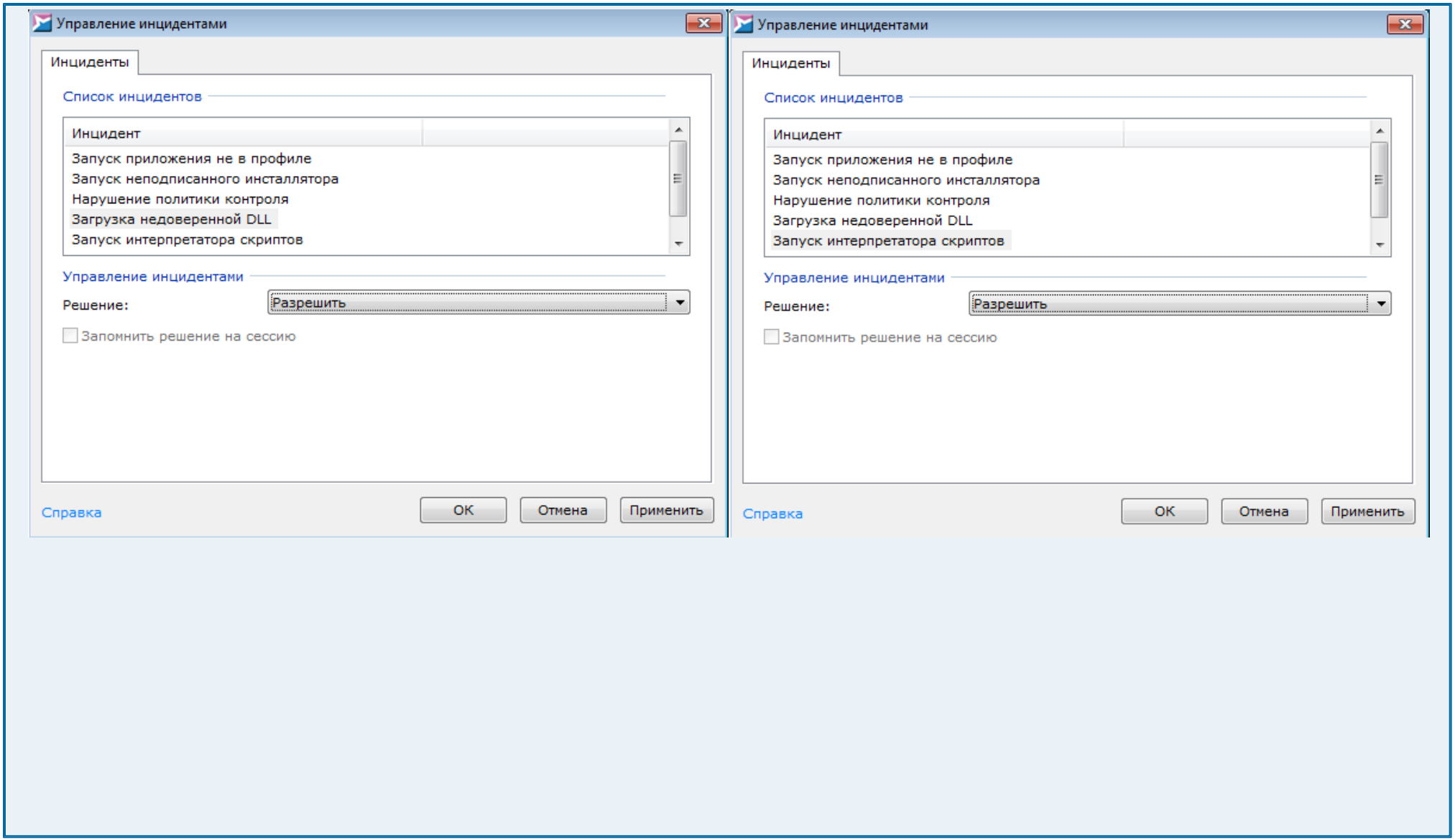
[3] Для включения режима аудита необходимо в области системных уведомлений (system tray) щелкнуть правой кнопкой мыши по значку SoftControl SysWatch и выбрать во всплывающем меню пункт **Настройка**. Далее в левой области выбрать пункт **Защита**, в области **Управление инцидентами** убедиться, что выставлена галочка **Включить автоматическую обработку инцидентов**, и нажать на кнопку **Настроить**. В настройках **Управление инцидентами** выбрать следующие настройки:

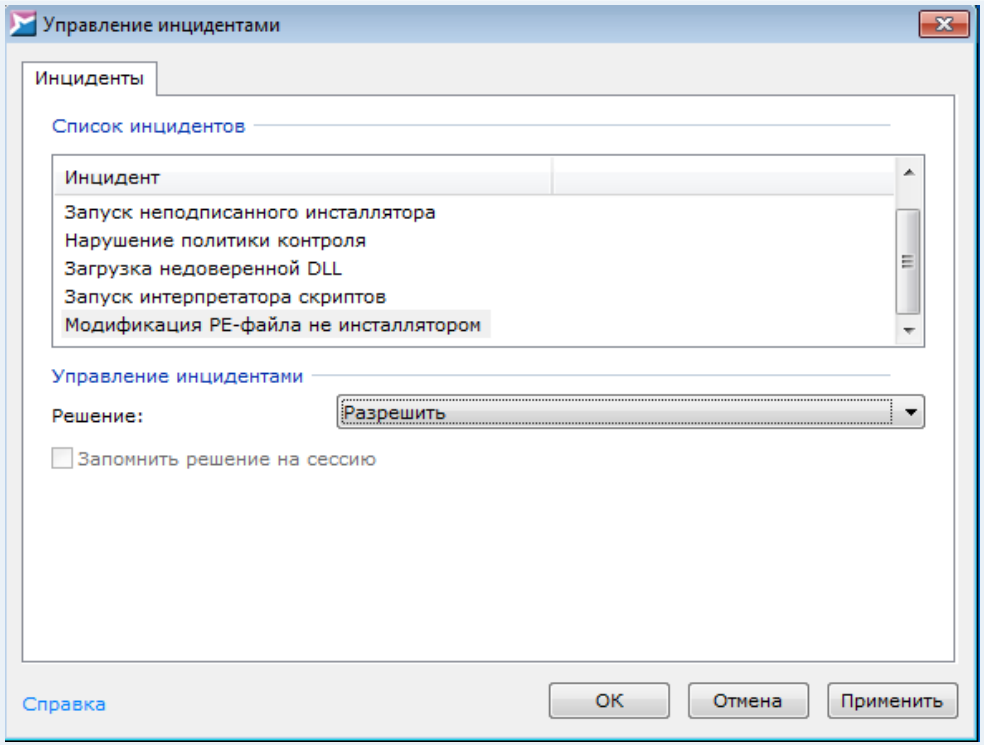
- Запуск приложения не в профиле – Выполнить в режиме обновления ПО;
- Запуск неподписанного инсталлятора – Установить;
- Нарушение политики контроля – Разрешить;
- Загрузка недоверенной DLL – Разрешить;
- Запуск интерпретатора скриптов – Разрешить;
- Модификация PE-файла не инсталлятором – Разрешить.


Настройка программы SysWatch
Защита
Общие параметры
Защита
Проверка
Обновление
Параметры
Вид
Отчеты
Оповещения
Справка
Управление инцидентами
Инциденты
Список инцидентов
Инцидент
Запуск приложения не в профиле
Запуск неподписанного инсталлятора
Нарушение политики контроля
Загрузка недоверенной DLL
Запуск интерпретатора скриптов
Управление инцидентами
Решение:
Выполнить в режиме обновления ПО
Запомнить решение на сессию
Справка
OK
Отмена
Применить


Управление инцидентами
Инциденты
Список инцидентов
Инцидент
Запуск приложения не в профиле
Запуск неподписанного инсталлятора
Нарушение политики контроля
Загрузка недоверенной DLL
Запуск интерпретатора скриптов
Управление инцидентами
Решение:
Установить
Запомнить решение на сессию
Справка
OK
Отмена
Применить

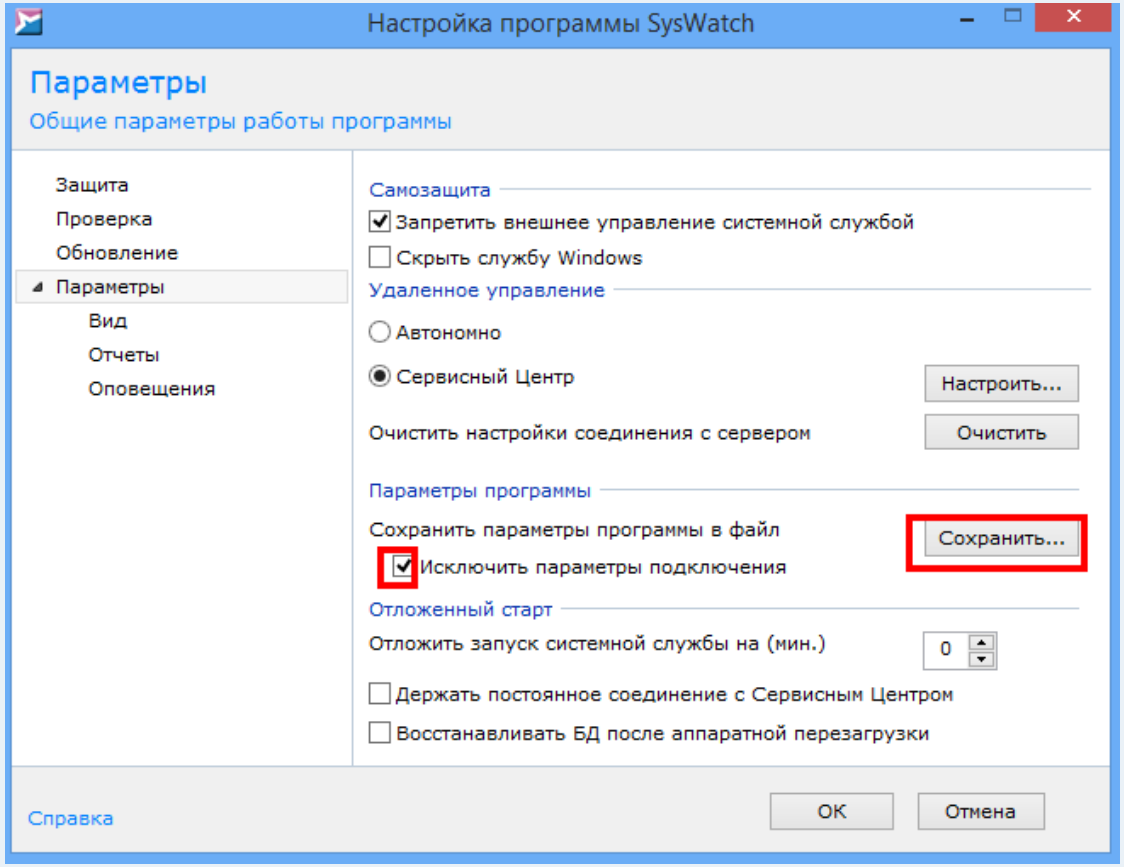

Управление инцидентами
Инциденты
Список инцидентов
Инцидент
Запуск приложения не в профиле
Запуск неподписанного инсталлятора
Нарушение политики контроля
Загрузка недоверенной DLL
Запуск интерпретатора скриптов
Управление инцидентами
Решение:
Разрешить
Запомнить решение на сессию
Справка
OK
Отмена
Применить

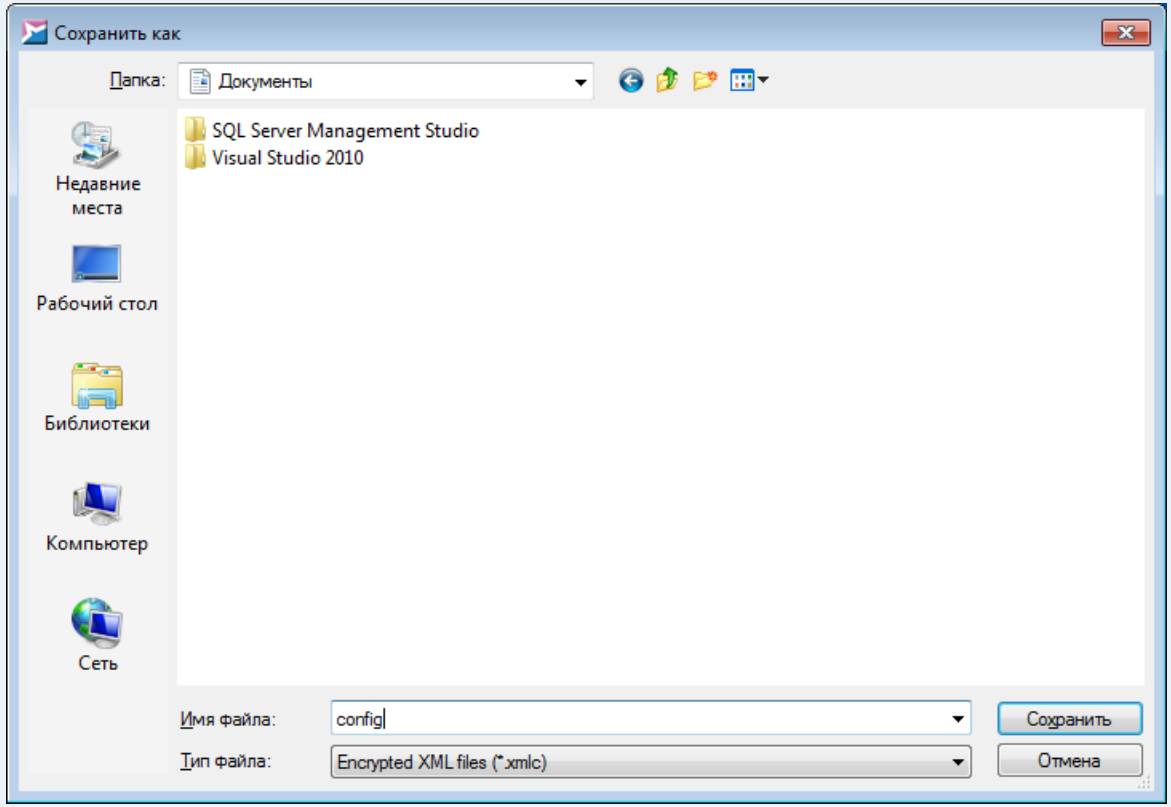

Управление инцидентами
Инциденты
Список инцидентов
Инцидент
Запуск приложения не в профиле
Запуск неподписанного инсталлятора
Нарушение политики контроля
Загрузка недоверенной DLL
Запуск интерпретатора скриптов
Управление инцидентами
Решение:
Разрешить
Запомнить решение на сессию
Справка
OK
Отмена
Применить
Управление инцидентами
Инциденты
Список инцидентов
Инцидент
Запуск приложения не в профиле
Запуск неподписанного инсталлятора
Нарушение политики контроля
Загрузка недоверенной DLL
Запуск интерпретатора скриптов
Управление инцидентами
Решение:
Разрешить
Запомнить решение на сессию
Справка
OK
Отмена
Применить



После изменения настроек нажать на кнопку **Применить**.

Для выгрузки конфигурационного файла *Config.xmlc* необходимо в области системных уведомлений (system tray) щелкнуть правой кнопкой мыши по значку SoftControl SysWatch и выбрать во всплывающем меню пункт **Настройка**. В левой области выбрать пункт меню **Параметры**, в пункте **Параметры программы** выставить галочку в поле **Исключить параметры подключения** и нажать на кнопку **Сохранить**. В открывшемся окне выбрать какую-либо папку (например, **Мои документы**) и сохранить файл под именем *Config.xmlc*.





[4] Сертификат VeriSign Class 3 Public Primary Certification Authority, *G5.cer*, можно выгрузить с клиентского хоста, на котором установлен SoftControl SysWatch, из доверенных корневых центров сертификации.

[5] Для добавления сертификата клиентского модуля SoftControl SysWatch в хранилище Windows необходима утилита *certutil.exe* и ее библиотека *certadm.dll*, которые входят в Windows Server 2003 Administration Tools Pack: https://www.microsoft.com/en-US/Download/details.aspx?id=16770.

2.3.2 Удаленное развертывание клиентского компонента SoftControl SysWatch из пакетного инсталлятора на типовом устройстве

Таблица 8. Удаленное развертывание SoftControl SysWatch

№ пп.	Действие	Ожидаемый результат	Комментарий
8.1	Удаленное развертывание клиентского компонента SoftControl SysWatch из пакетного инсталлятора на типовом устройстве пилотной зоны		Развертывание необходимо проводить на устройстве, повторяющем параметры устройства, на котором были созданы настройки пп. 5.3 (14), 6.2.3 (21).
8.1.1	Доставка пакетного инсталлятора клиентского компонента SoftControl SysWatch на типовое устройство средствами удаленной файлообменной среды.	❑ Пакетный инсталлятор доставлен в файловую систему устройства.	Доставка пакетного инсталлятора в ФС устройства производится силами и средствами удаленной файлообменной среды Заказчика. Замерить и записать время доставки пакетного инсталлятора для нормирования операций развертывания.
8.1.2	Запущен сценарий запуска* пакетного инсталлятора средствами удаленного администрирования.	❑ Лог установки SoftControl SysWatch создан и не содержит ошибок. ❑ В консоли управления SoftControl Admin Console появился новый клиент SoftControl SysWatch в статусе **Ожидает решения**.	Запуск пакетного инсталлятора осуществляется специалистом Заказчика с помощью средств удаленного администрирования, развернутых на типовом устройстве Заказчика.
* Пример сценария запуска, исходя из условия размещения дистрибутива клиентского модуля SoftControl SysWatch, файла конфигурации эталонного образа клиентского модуля SoftControl SysWatch *config.xmlc* и файла настроек подключения к серверу управления *ClientSettings.xmlc* в папке *C:\SnS-install*: `call %WINDIR%\system32\msiexec.exe /i "C:\SnS-install\SysWatch.msi" configfilename="C:\SnS-install\config.xmlc" tsconfig="C:\SnS-install\ClientSettings.xmlc" /quiet /norestart /log "C:\SnS-install\install-log.txt"`			
8.1.3	Администратором наблюдается новый клиент в консоли управления SoftControl Admin Console.	❑ В консоли управления SoftControl Admin Console наблюдается новый клиент SoftControl SysWatch в статусе **Ожидает решения**.	

2.3.3 Создание и применение наборов настроек групповых политик контроля с сервера управления SoftControl Service Center

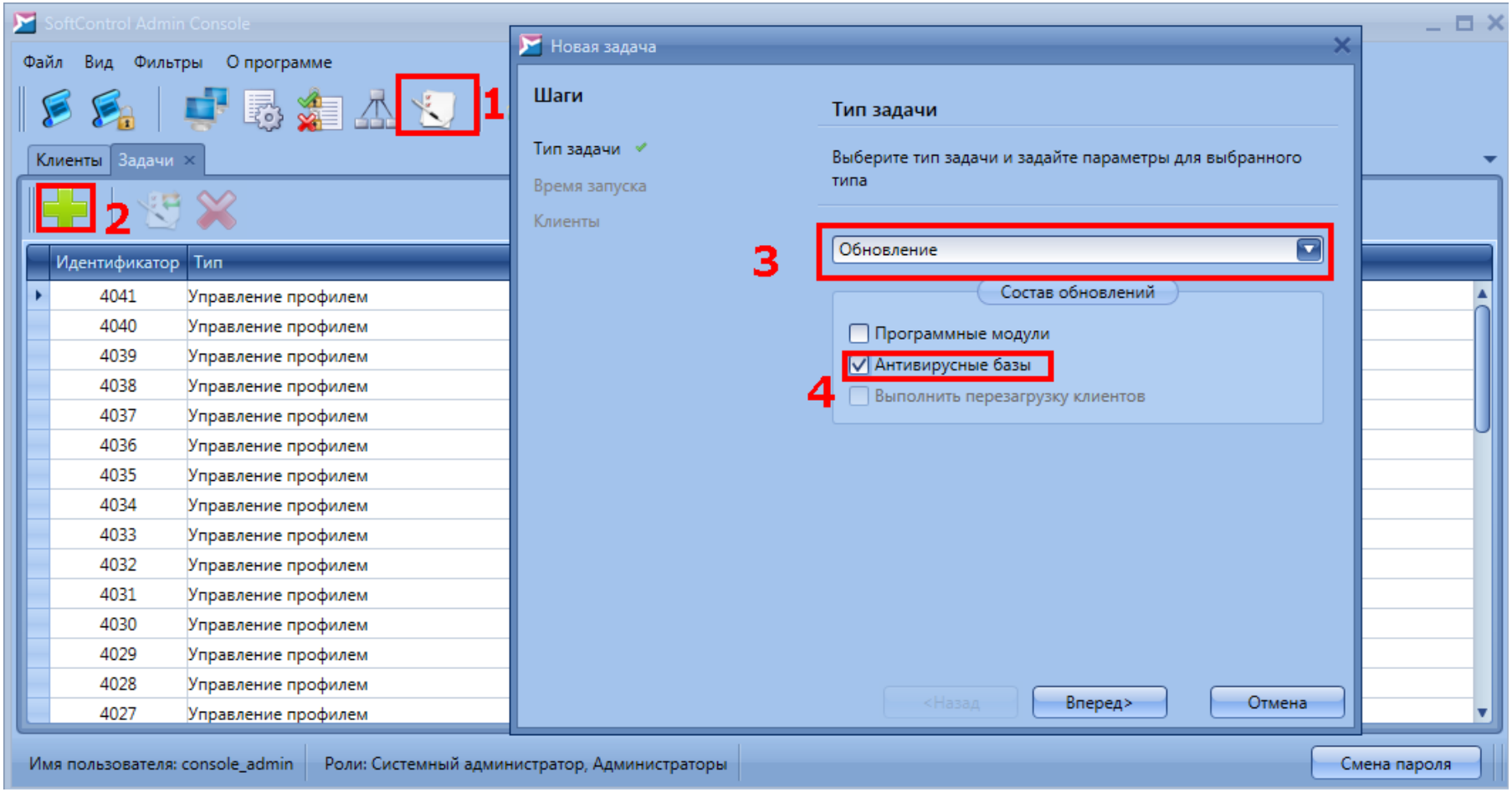
Таблица 9. Создание и применение наборов настроек с SoftControl Service Center

№ пп.	Действие	Ожидаемый результат	Комментарий
9.1	Создание и применение наборов настроек групповых политик контроля с сервера управления SoftControl Service Center		Задаются несколько наборов политик контроля для разных ситуаций эксплуатации: • Production – наиболее жесткий набор политик контроля, предназначенный обеспечить защиту ПО устройства от попыток любых изменений. Применяется на устройствах в состоянии обслуживания клиентов Банка и не подразумевает проведения сервисных работ на устройстве. • For Services – набор настроек политик контроля, обеспечивающий возможность совершения санкционированных сервисных воздействий на ПО устройства при включенной защите.
9.1.1	Создание наборов групповых политик контроля		
9.1.1.1	Создан набор политик контроля Production и Production-Audit на его основе.	❑ Создан набор настроек Production, Production-Audit.	Настройки политик контроля создаются специалистом-представителем Заказчика и могут корректироваться согласно политике ИБ Заказчика. Типовые наборы политик контроля для устройств описаны в файле *Политики_контроля_SoftControl_ATM.xlsx*. Для создания политик контроля в отношении белого списка USB-носителей необходим USB-носитель для тестов.
9.1.2	Создание подразделений		Подразделение – группа устройств с общими групповыми политиками контроля.

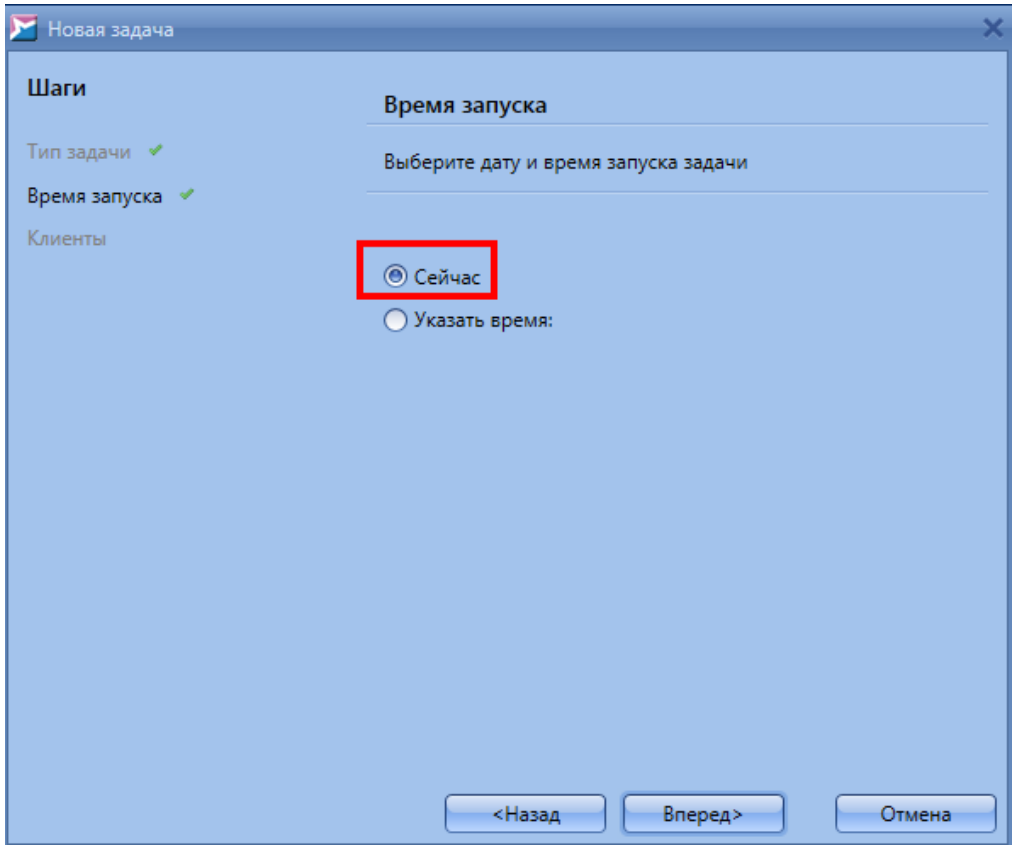
9.1.2.1	Создано подразделения Production, подразделению присвоен набор настроек Production-Audit.	❑ Создано подразделение Production. Подразделению присвоен набор настроек Production-Audit.	
9.1.3	Перемещение клиентов в подразделения с наборами групповых политик		
9.1.3.1	Клиенты SoftControl SysWatch перемещены в подразделение Production.	❑ В консоли SoftControl Admin Console отобразилось состояние настроек клиента SoftControl SysWatch **Применены успешно** и подразделение Production ❑ В консоли SoftControl Admin Console в журнале событий клиента SoftControl SysWatch есть запись *Настройки изменены с сервера*. Доступна к просмотру дополнительная информация об изменении настроек.	
9.2	Запущена задача по обновлению антивирусных баз на устройстве 1.* (Данная операция опциональна в случае необходимости экономии трафика на конечном устройстве).	❑ В консоли SoftControl Admin Console в колонке **Информация** отобразилось состояние клиента SoftControl SysWatch **Обновление - Установлено**.	Для работы обновления антивирусных баз AV4 на устройстве с Windows XP **обязательно** должен быть установлен «Распространяемый пакет Microsoft Visual C++ 2008» (*vcredis t_x86_2008.exe*).

* Для запуска задачи по обновлению антивирусных баз необходимо в консоли SoftControl Admin Console нажать на пиктограмму  (**Задачи**). В открывшемся окне **Задачи** нажать на кнопку  (**Создать**).

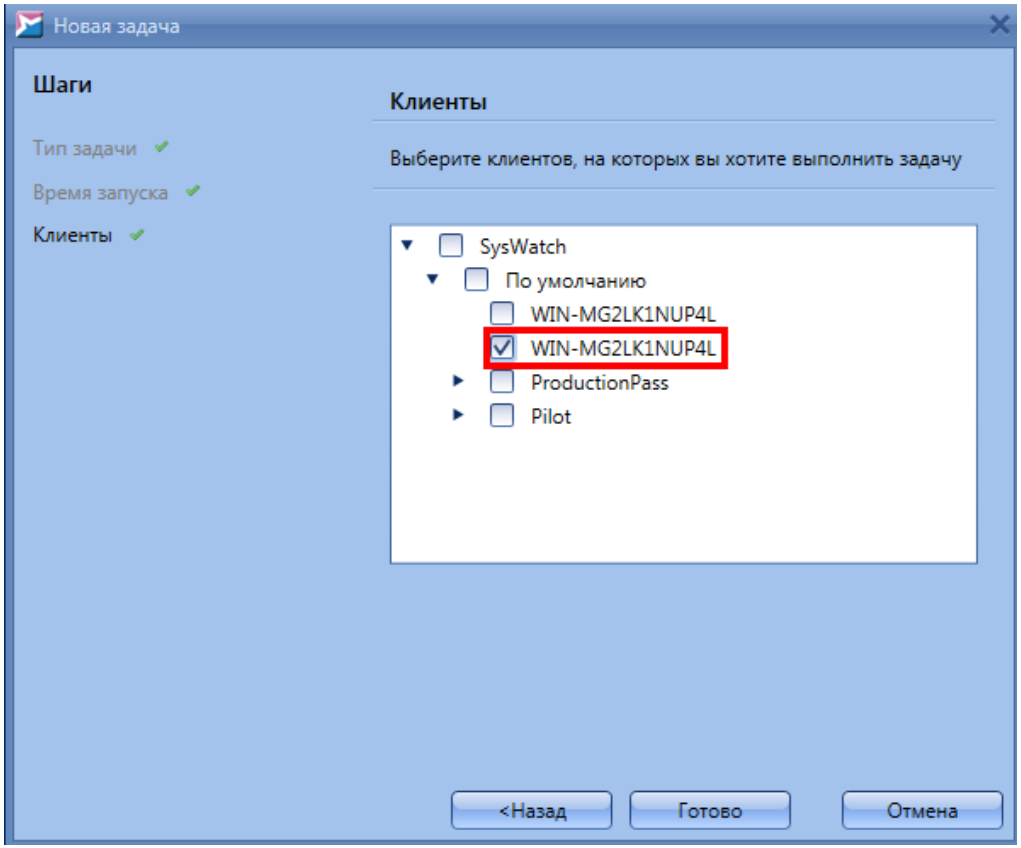
В открывшемся окне **Новая задача** выбрать **Тип задачи** - **Обновление**, выставить галочку **Антивирусные базы** и нажать на кнопку **Вперед**:


SoftControl Admin Console
Файл Вид Фильтры О программе
1
Клиенты
Задачи
2
Идентификатор
Тип
4041 Управление профилем
4040 Управление профилем
4039 Управление профилем
4038 Управление профилем
4037 Управление профилем
4036 Управление профилем
4035 Управление профилем
4034 Управление профилем
4033 Управление профилем
4032 Управление профилем
4031 Управление профилем
4030 Управление профилем
4029 Управление профилем
4028 Управление профилем
4027 Управление профилем
Новая задача
Шаги
Тип задачи
Время запуска
Клиенты
Тип задачи
Выберите тип задачи и задайте параметры для выбранного типа
3
Обновление
Состав обновлений
Программные модули
Антивирусные базы
4
Выполнить перезагрузку клиентов
<Назад
Вперед>
Отмена
Имя пользователя: console_admin
Роли: Системный администратор, Администраторы
Смена пароля

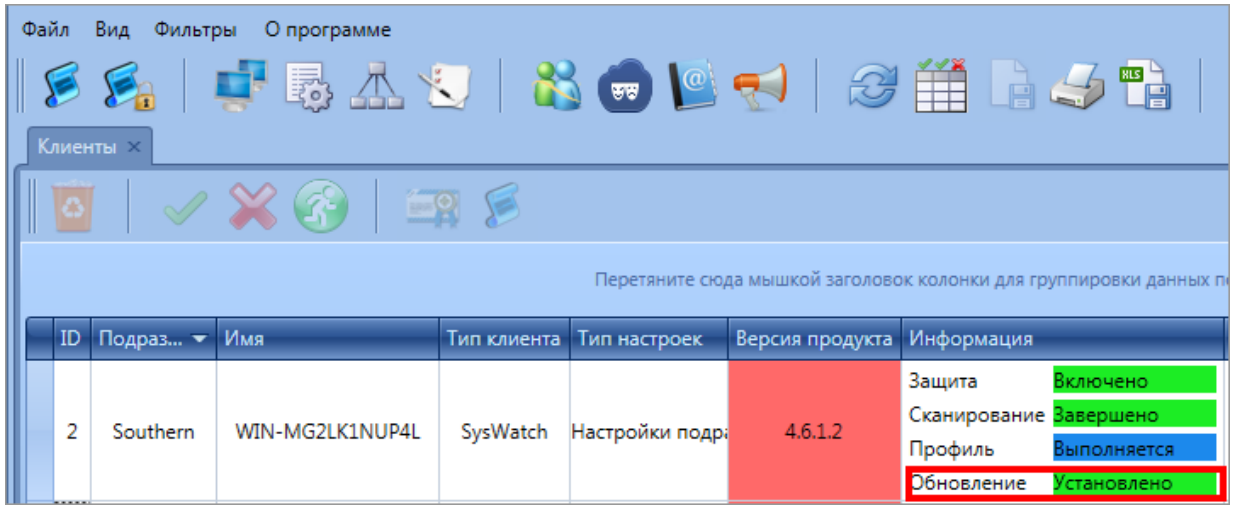
В следующем окне **Время запуска** выбрать время выполнения задачи (в нашем случае – **Сейчас**), и нажать на кнопку **Вперед**:



В следующем окне **Клиенты** необходимо выбрать клиентов, на которых будет запущена задача по обновлению антивирусных баз, и нажать на кнопку **Готово**:

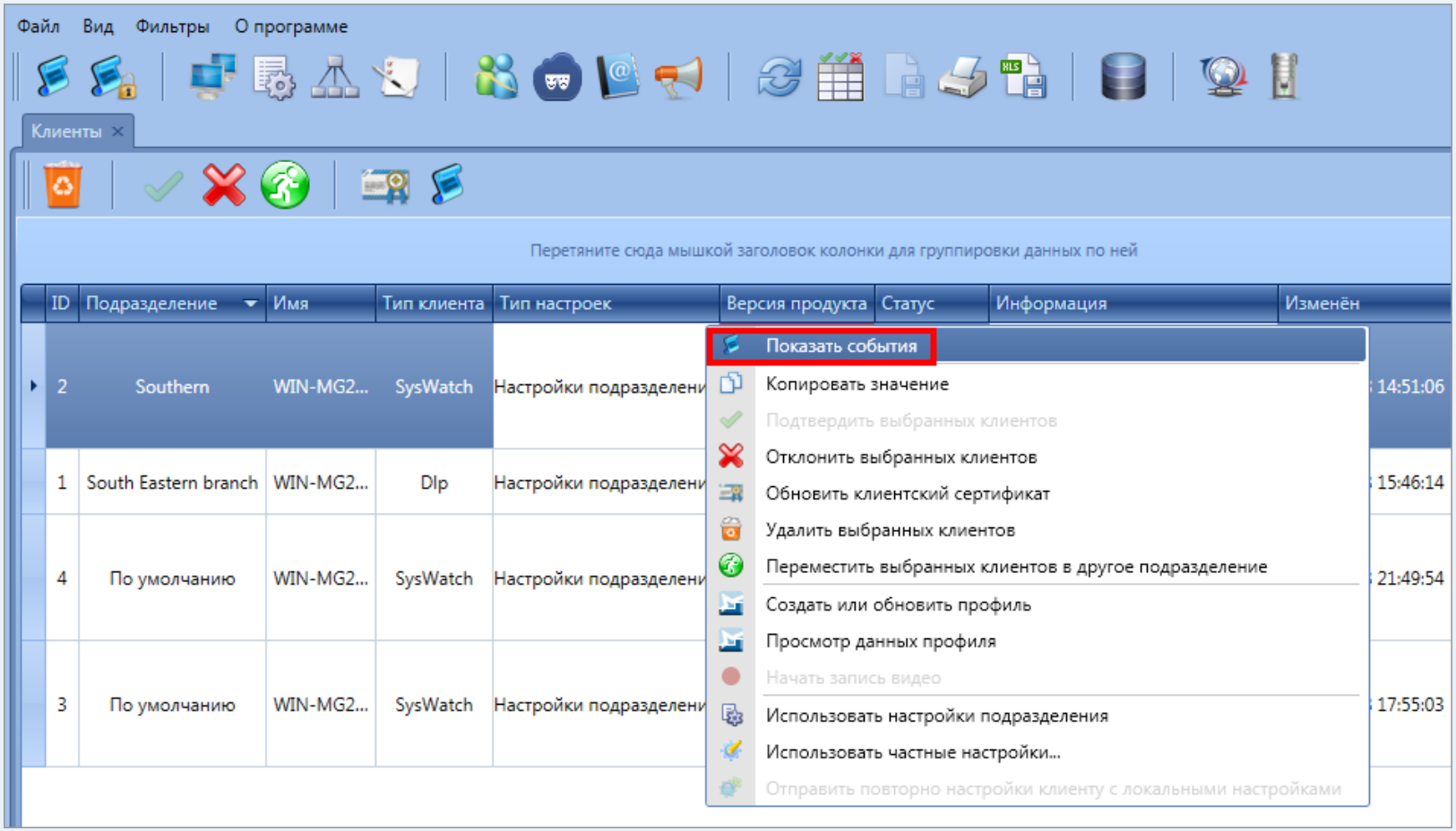


После выполнения обновления на вкладке **Клиенты** у клиента SoftControl SysWatch в поле **Информация** - **Обновление** появится статус **Установлено**.

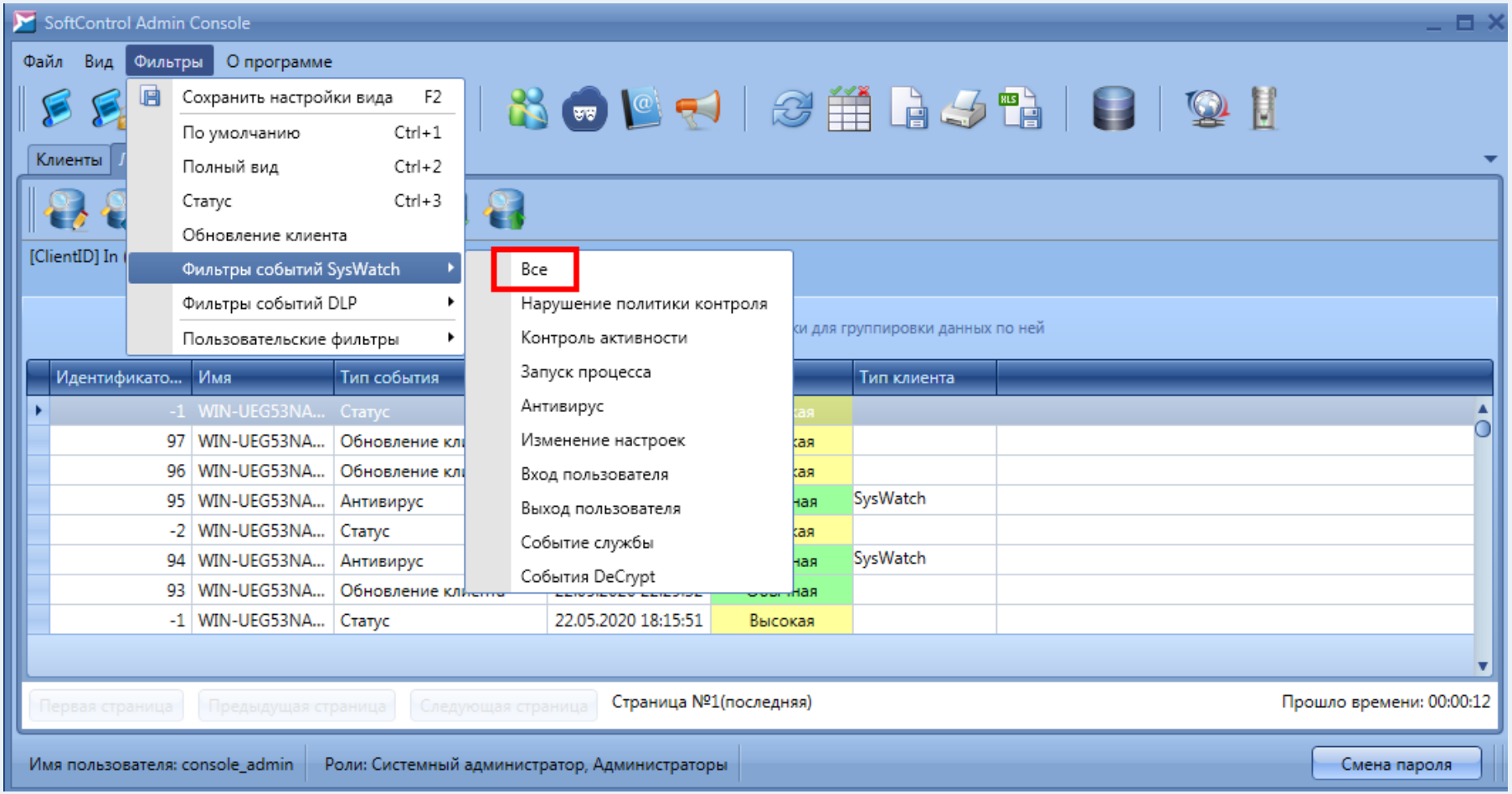


9.3	Создана и выполнена задача по антивирусному сканированию на устройстве 1. (Данная операция опциональна в случае необходимости экономии трафика на конечном устройстве).	❑ В консоли управления SoftControl Admin Console в колонке **Информация** отобразилось состояние клиента SoftControl SysWatch **Сканирование** - **Завершено**.	Задача по антивирусному сканированию создается и выполняется аналогично обновлению антивирусных баз.
9.4	Создана и выполнена задача по сбору профиля на устройстве 1.	❑ В консоли управления SoftControl Admin Console в колонке **Информация** отобразилось состояние клиента SoftControl SysWatch **Профиль** - **Завершено**.	Задача по сбору профиля создается и выполняется аналогично обновлению антивирусных баз.
9.5	Сбор логов по работе устройства 1 на сервере управления.	❑ Собраны логи.	Крайне желательно провести перезагрузку устройства 1 в процессе наблюдения. Срок наблюдения – рабочий день.
9.6	Выгружен в файл *.xls* лог* работы устройства 1. Лог отправлен в техническую поддержку по адресу support@safesoft.com.	❑ Отправлен лог работы устройства 1.	В ответ вы получите рекомендации по дополнительным настройкам совместимости, если таковые требуются.

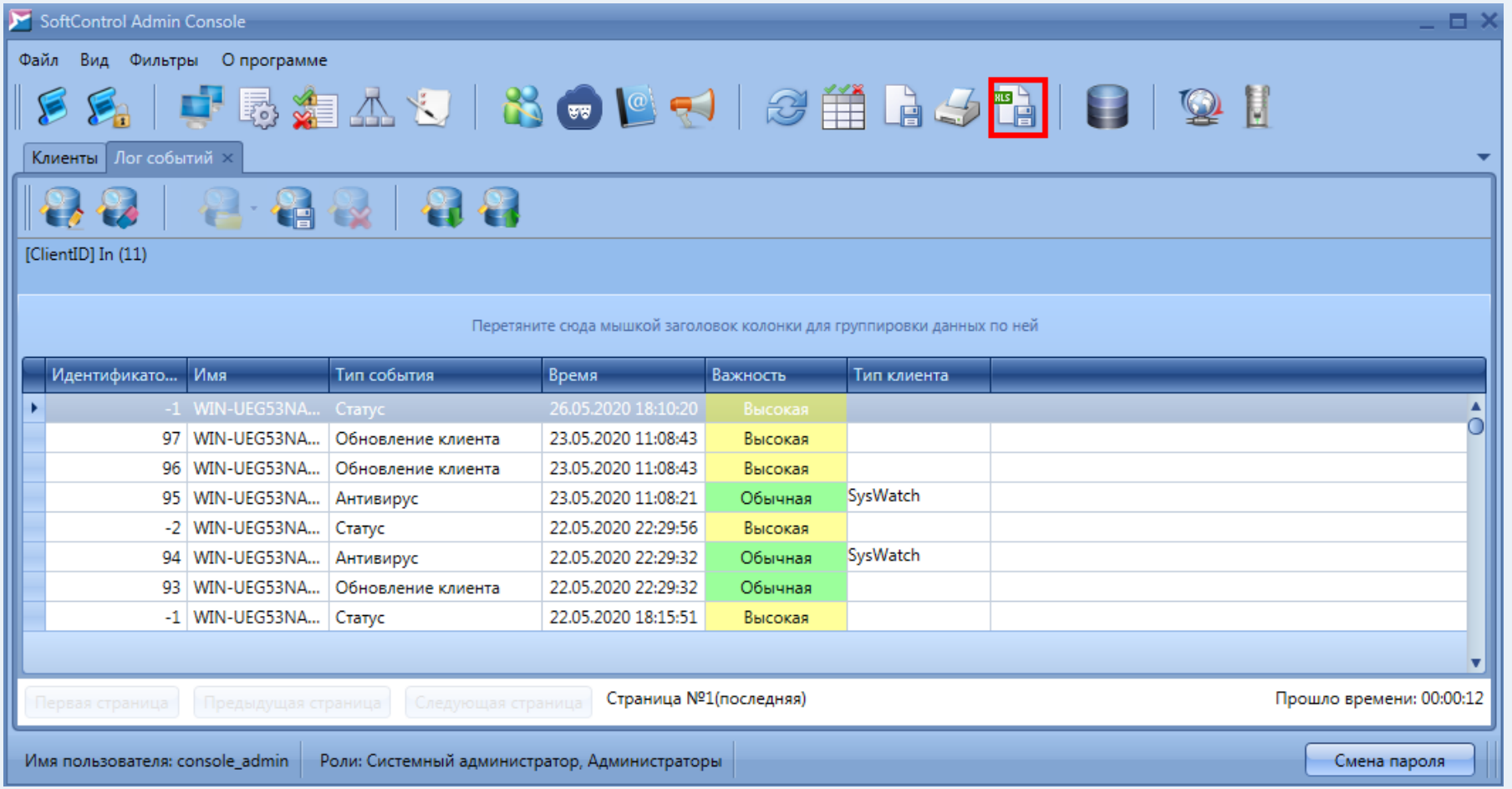
*Для выгрузки лог-файлов в файл *.xls* необходимо на сервере управления на вкладке **Клиенты** щелкнуть правой кнопкой мыши по устройству 1 и во всплывающем меню выбрать пункт **Показать события**.



В открывшейся вкладке **Лог** щелкнуть левой кнопкой мыши по меню **Фильтры** и в пункте **Фильтры событий SysWatch** выбрать пункт **Все**.



Затем щелкнуть левой кнопкой мыши по пиктограмме **Экспорт в Excel**  и сохранить файл выгрузки.

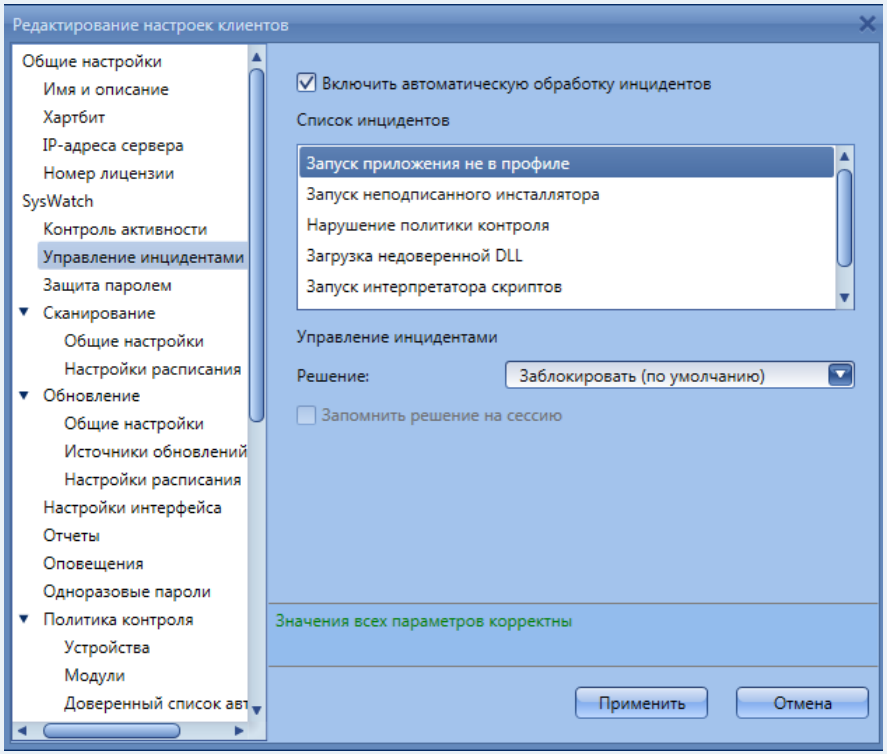


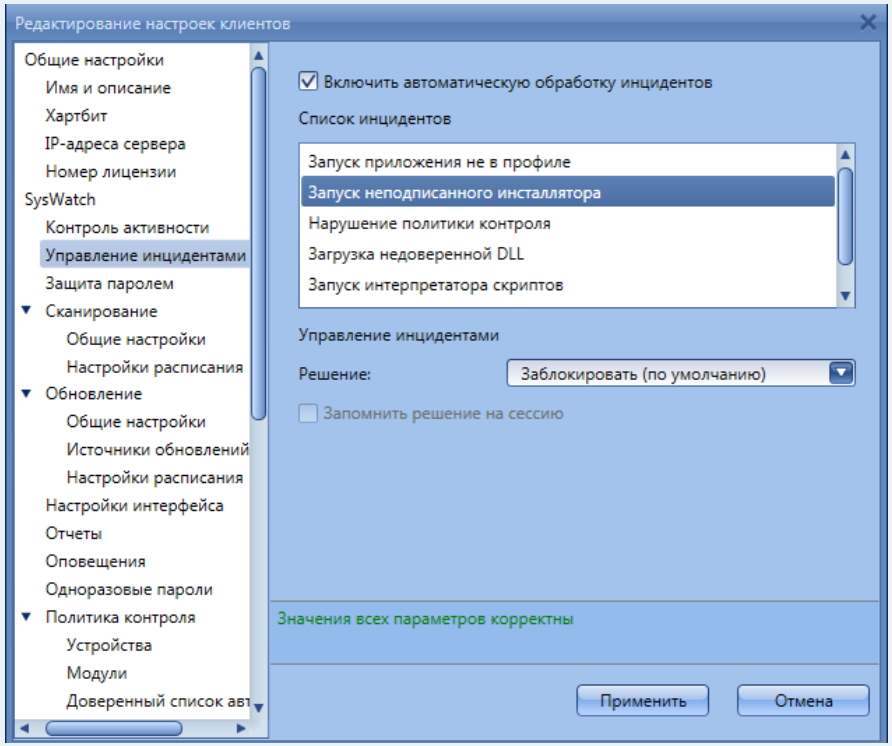
2.3.4 Создание групповых политик контроля. Примеры

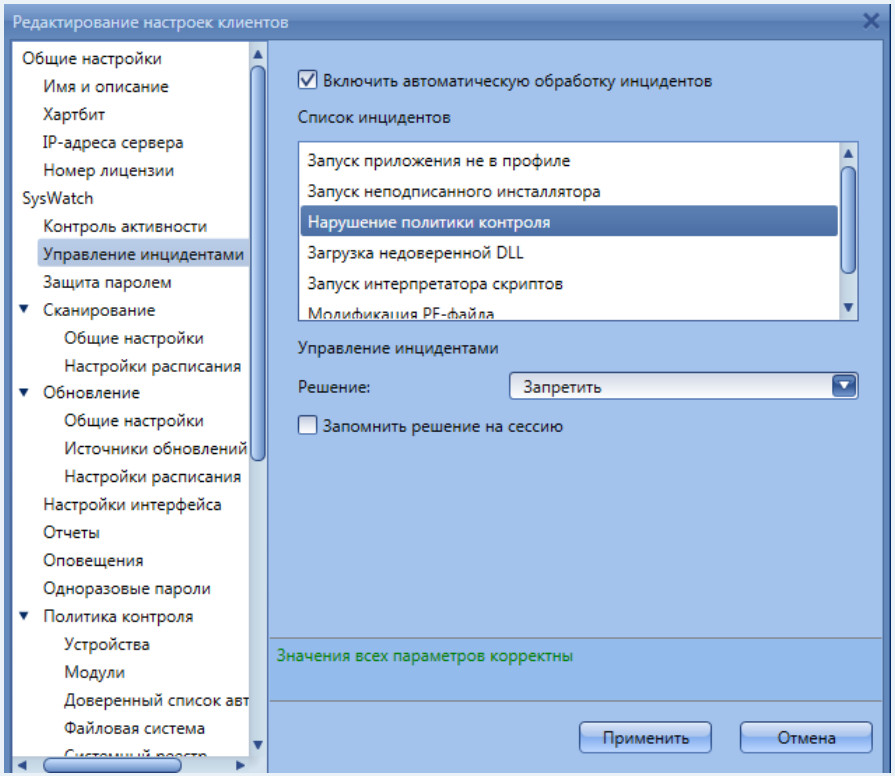
Таблица 10. Примеры создания групповых политик контроля

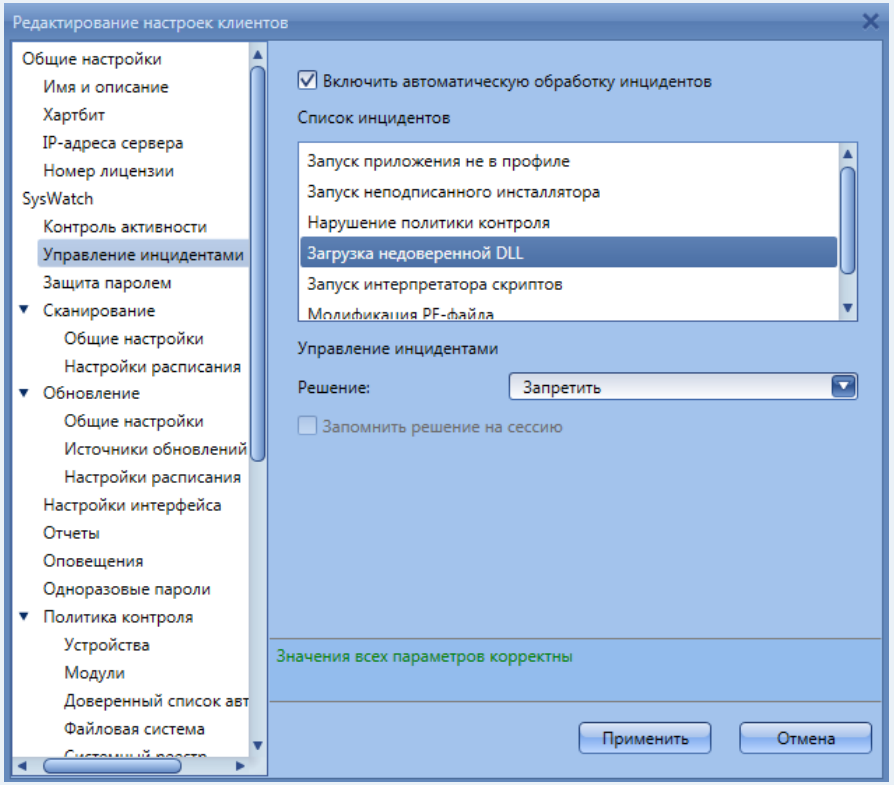
№ пп.	Действие	Ожидаемый результат	Комментарий
10.1	Клиентское устройство переведено из режима аудита в рабочий режим.*	❑ Устройство в рабочем режиме.	Для перевода клиентского устройства из режима аудита в рабочий режим необходимо отредактировать клиентские настройки на сервере управления SoftControl Service Center и применить их к тому подразделению, в котором находится клиентское устройство.

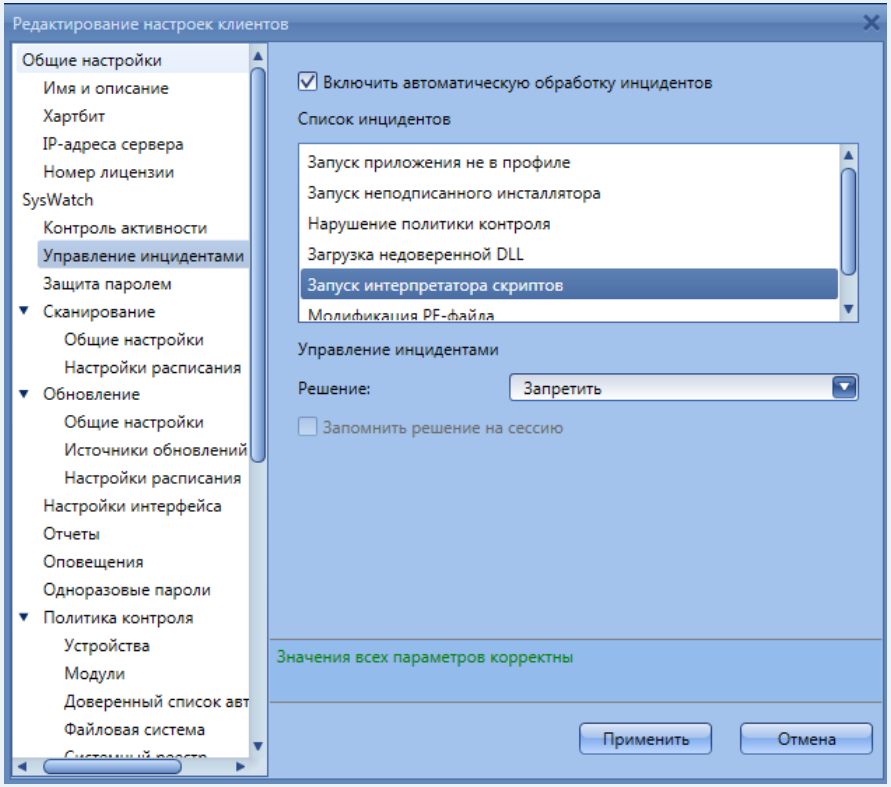
* Для изменения режима необходимо отредактировать клиентские настройки на сервере управления SoftControl Server:

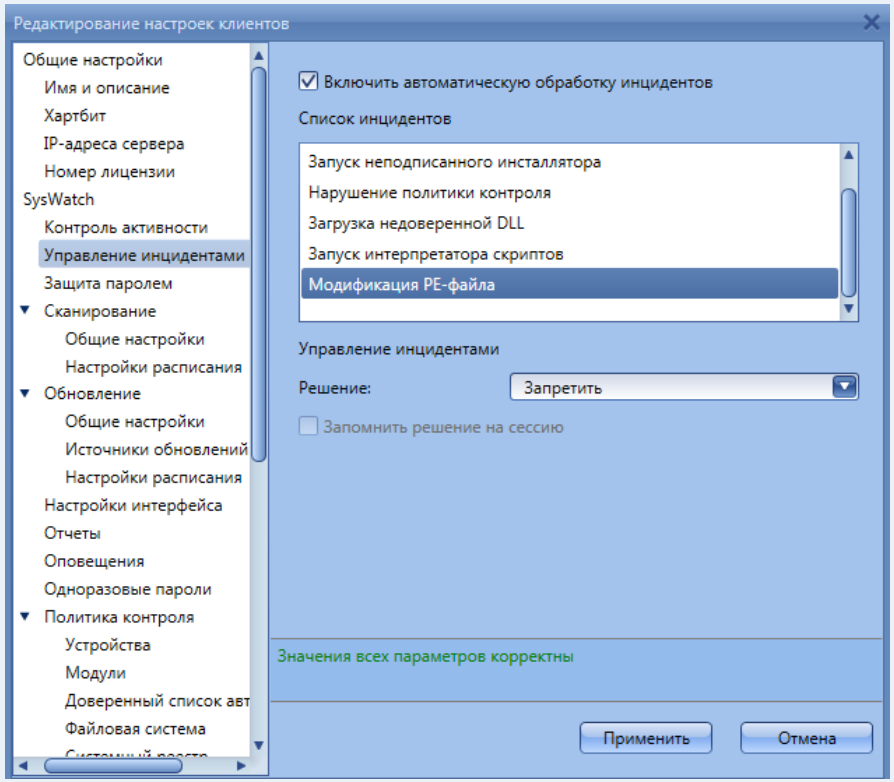





Редактирование настроек клиентов
Общие настройки
Имя и описание
Хартбит
IP-адреса сервера
Номер лицензии
SysWatch
Контроль активности
Управление инцидентами
Защита паролем
Сканирование
Общие настройки
Настройки расписания
Обновление
Общие настройки
Источники обновлений
Настройки расписания
Настройки интерфейса
Отчеты
Оповещения
Одноразовые пароли
Политика контроля
Устройства
Модули
Доверенный список авт
Файловая система
Включить автоматическую обработку инцидентов
Список инцидентов
Запуск приложения не в профиле
Запуск неподписанного инсталлятора
Нарушение политики контроля
Загрузка недоверенной DLL
Запуск интерпретатора скриптов
Управление инцидентами
Решение:
Запретить
Запомнить решение на сессию
Значения всех параметров корректны
Применить
Отмена


Редактирование настроек клиентов
Общие настройки
Имя и описание
Хартбит
IP-адреса сервера
Номер лицензии
SysWatch
Контроль активности
Управление инцидентами
Защита паролем
Сканирование
Общие настройки
Настройки расписания
Обновление
Общие настройки
Источники обновлений
Настройки расписания
Настройки интерфейса
Отчеты
Оповещения
Одноразовые пароли
Политика контроля
Устройства
Модули
Доверенный список авт
Файловая система
Включить автоматическую обработку инцидентов
Список инцидентов
Запуск приложения не в профиле
Запуск неподписанного инсталлятора
Нарушение политики контроля
Загрузка недоверенной DLL
Запуск интерпретатора скриптов
Управление инцидентами
Решение:
Запретить
Запомнить решение на сессию
Значения всех параметров корректны
Применить
Отмена

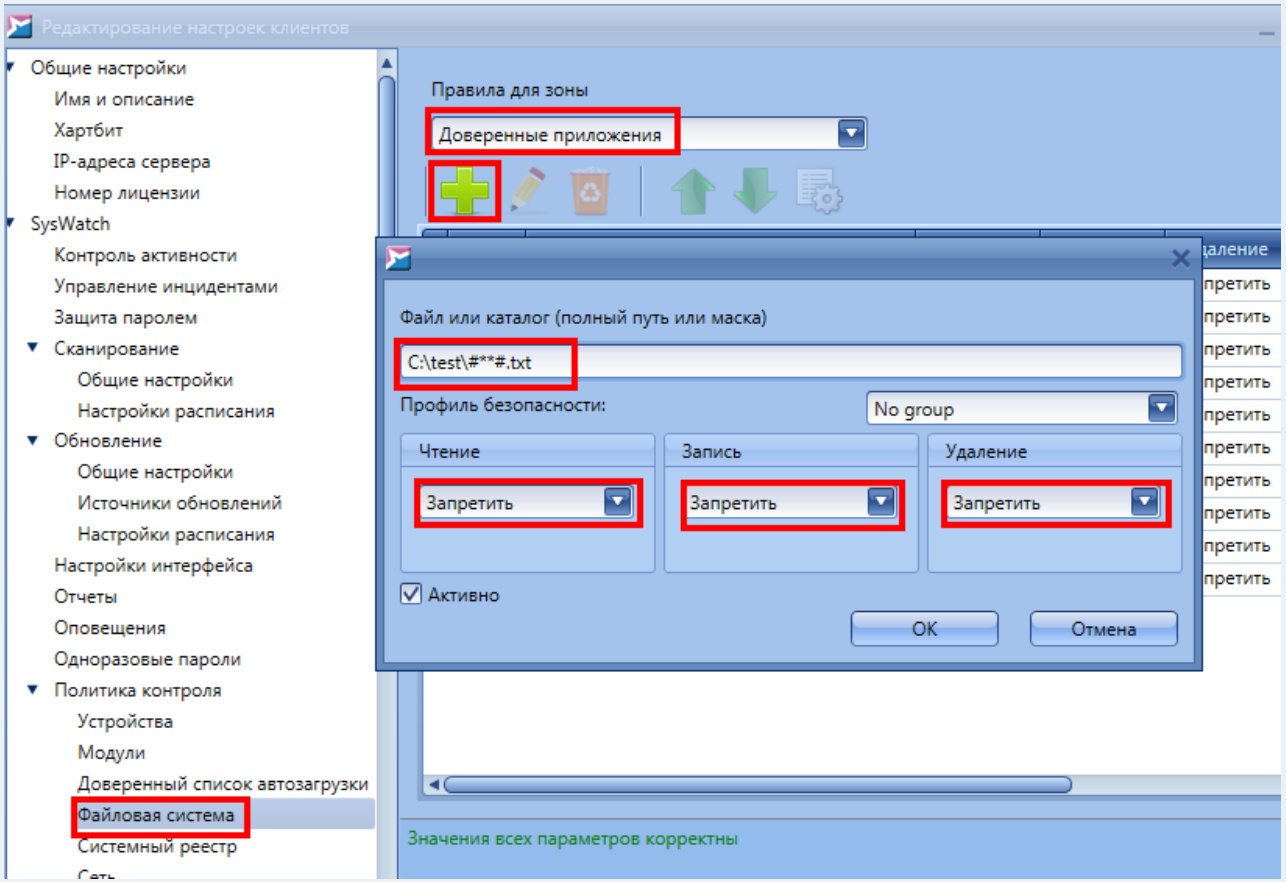


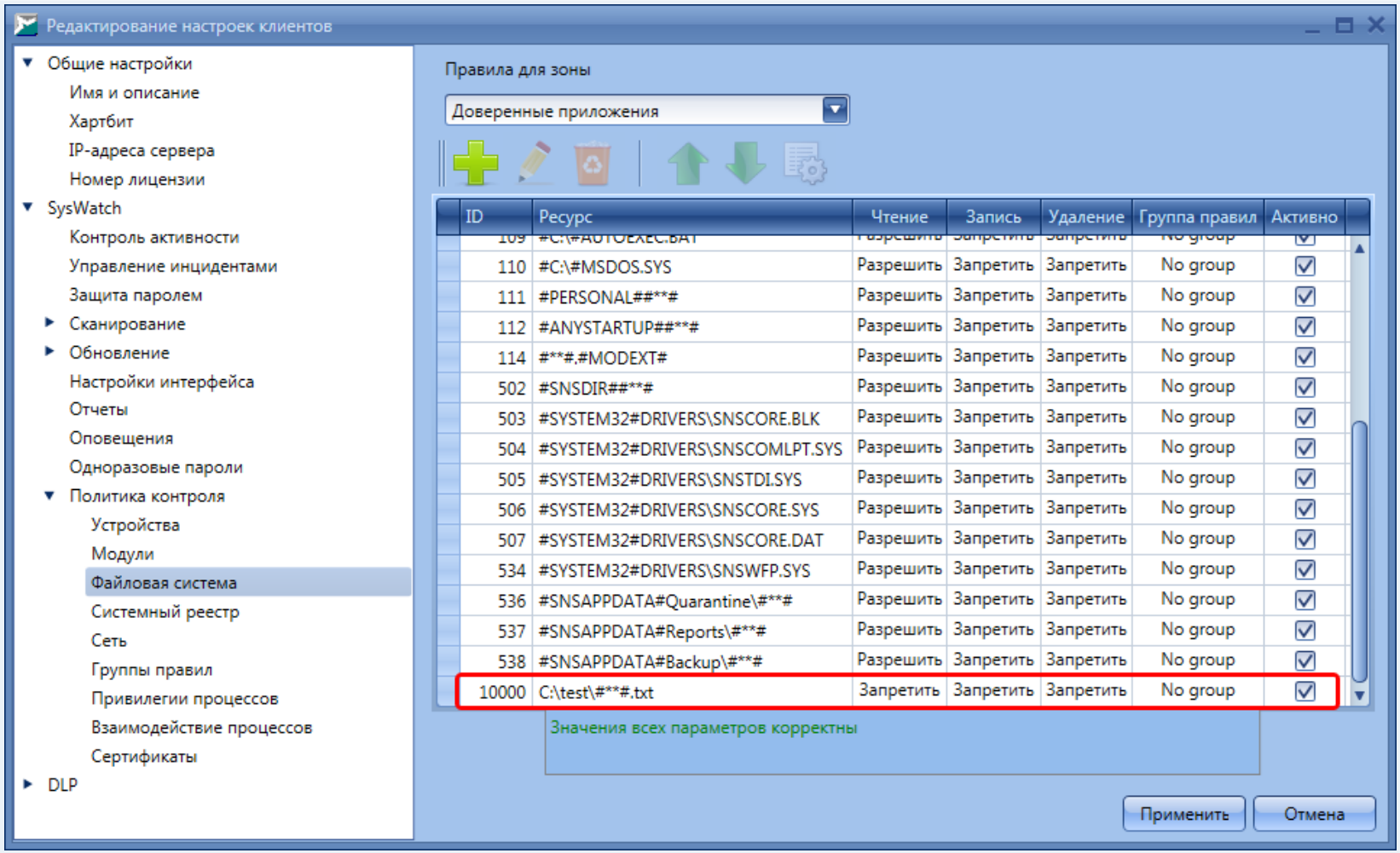


После редактирования настроек клиентов необходимо сохранить настройки под новым именем и применить к тому подразделению, в котором находится клиентское устройство.

10.2	Создание и проверка действия правил политик контроля по каждой области контроля		
10.2.1	Проверка правил политик контроля для файловой системы		
10.2.1.1	Создано правило запрета чтения, записи, удаления текстовых файлов в папке *C:\test* для всех доверенных процессов.*	❑ Создано правило запрета чтения, удаления, записи файлового ресурса *C:\test*.txt* для доверенных приложений.	

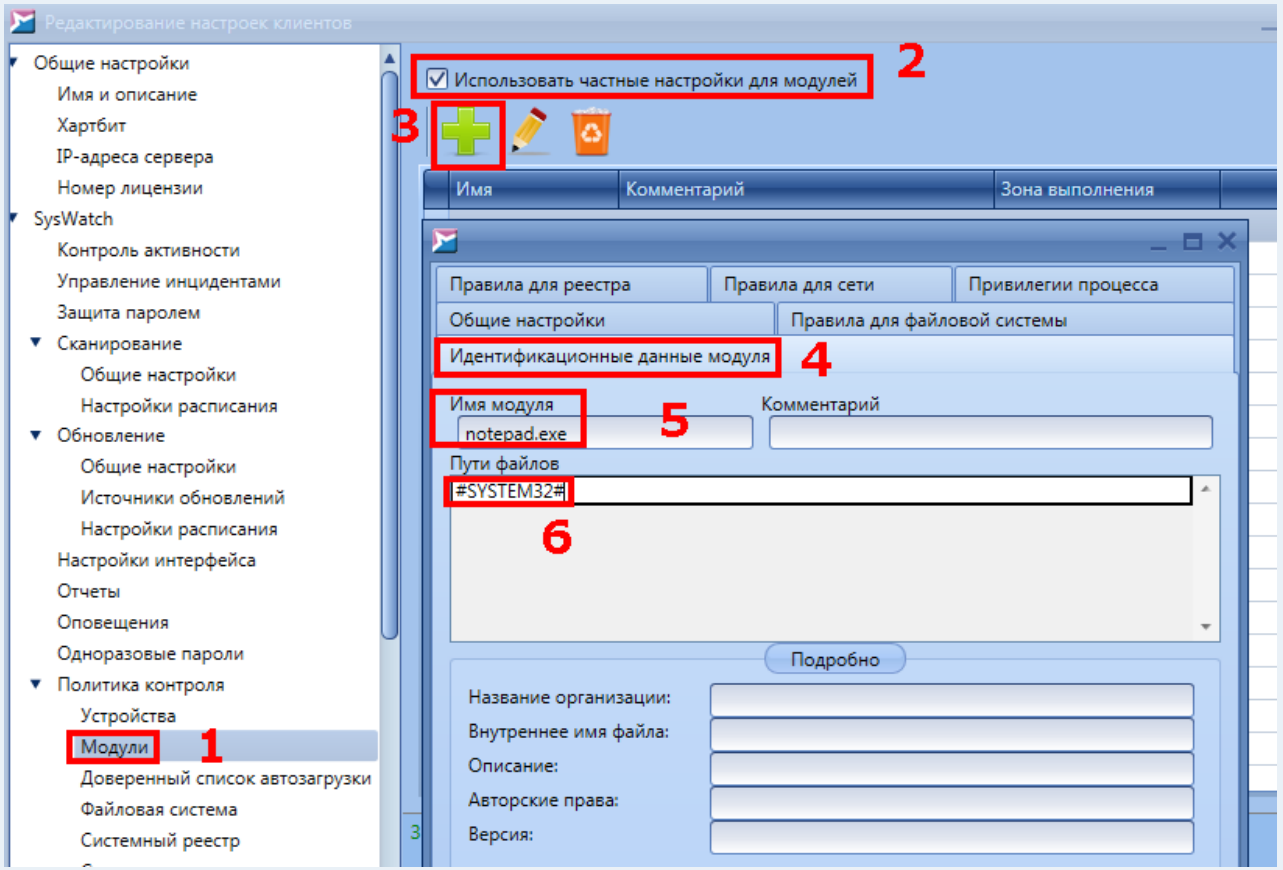
* Для создания правила необходимо отредактировать настройки клиентов:

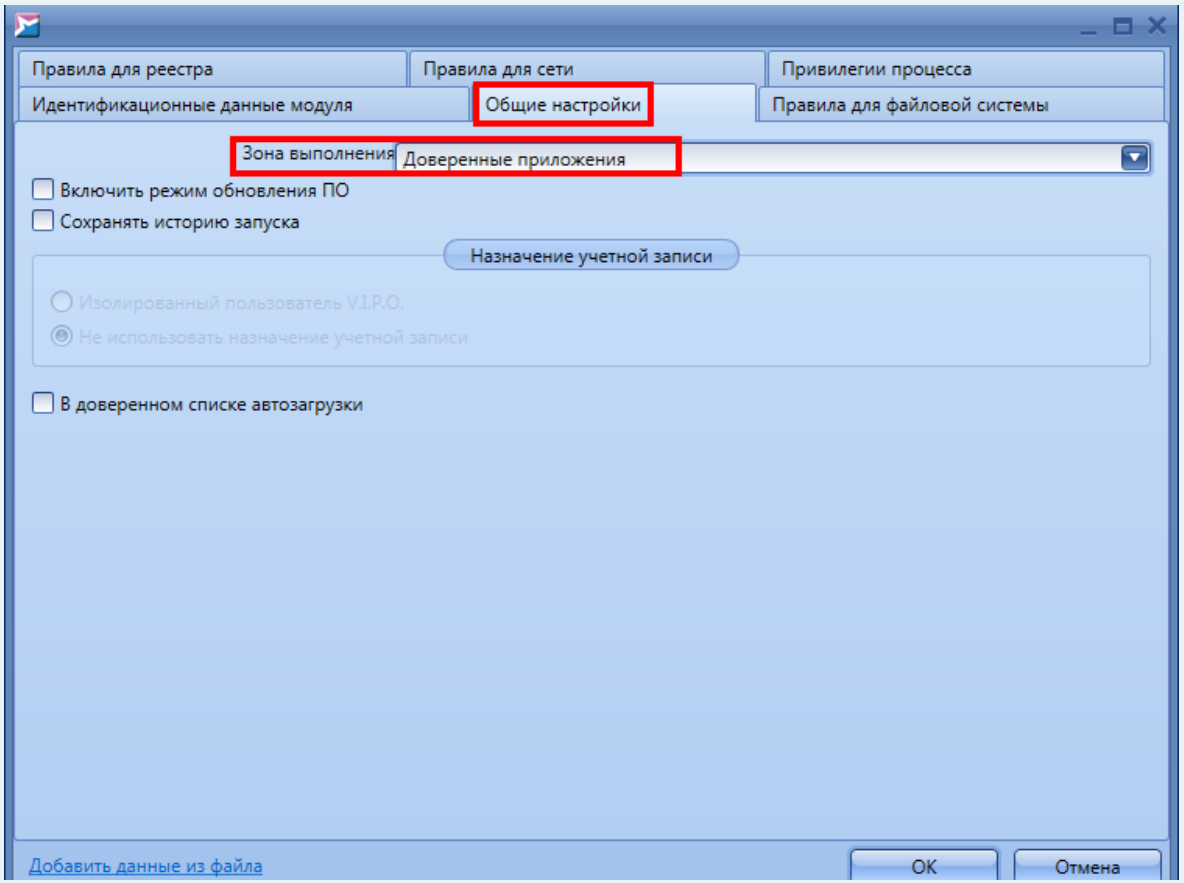


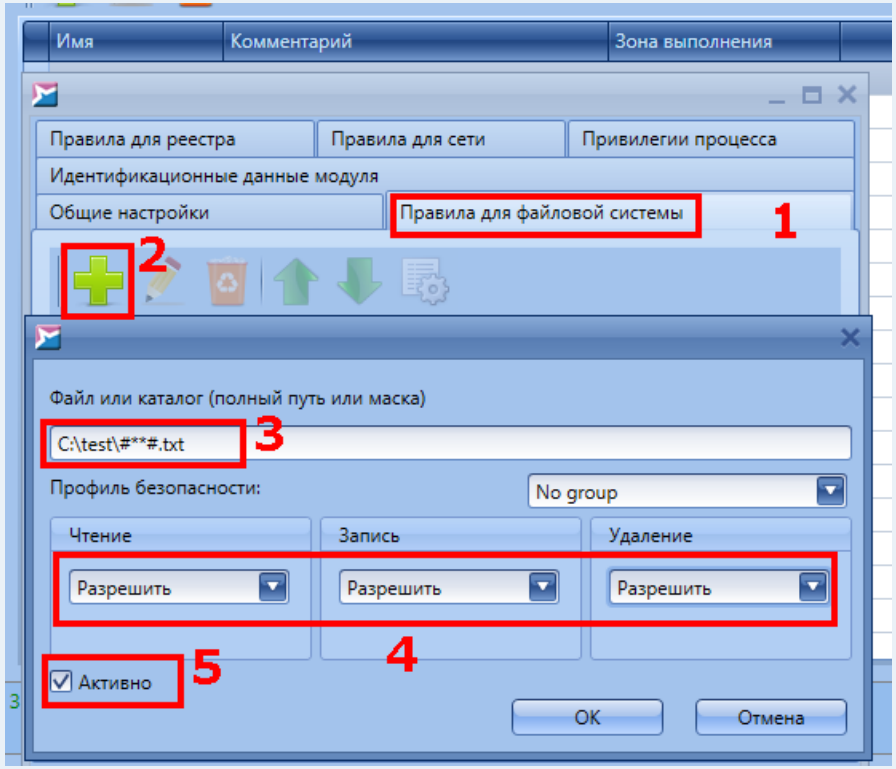

Редактирование настроек клиентов
Общие настройки
Имя и описание
Хартбит
IP-адреса сервера
Номер лицензии
SysWatch
Контроль активности
Управление инцидентами
Защита паролем
Сканирование
Обновление
Настройки интерфейса
Отчеты
Оповещения
Одноразовые пароли
Политика контроля
Устройства
Модули
Файловая система
Системный реестр
Сеть
Группы правил
Привилегии процессов
Взаимодействие процессов
Сертификаты
DLP
Правила для зоны
Доверенные приложения
ID
Ресурс
Чтение
Запись
Удаление
Группа правил
Активно
110 #C:\#MSDOS.SYS Разрешить Запретить Запретить No group
111 #PERSONAL##**# Разрешить Запретить Запретить No group
112 #ANYSTARTUP##**# Разрешить Запретить Запретить No group
114 #**#.#MODEXT# Разрешить Запретить Запретить No group
502 #SNSDIR##**# Разрешить Запретить Запретить No group
503 #SYSTEM32#DRIVERS\SNSCORE.BLK Разрешить Запретить Запретить No group
504 #SYSTEM32#DRIVERS\SNSCOMLPT.SYS Разрешить Запретить Запретить No group
505 #SYSTEM32#DRIVERS\SNSTDI.SYS Разрешить Запретить Запретить No group
506 #SYSTEM32#DRIVERS\SNSCORE.SYS Разрешить Запретить Запретить No group
507 #SYSTEM32#DRIVERS\SNSCORE.DAT Разрешить Запретить Запретить No group
534 #SYSTEM32#DRIVERS\SNSWFP.SYS Разрешить Запретить Запретить No group
536 #SNSAPPDATA#Quarantine\#**# Разрешить Запретить Запретить No group
537 #SNSAPPDATA#Reports\#**# Разрешить Запретить Запретить No group
538 #SNSAPPDATA#Backup\#**# Разрешить Запретить Запретить No group
10000 C:\test\#**#.txt Запретить Запретить Запретить No group
Значения всех параметров корректны
Применить
Отмена

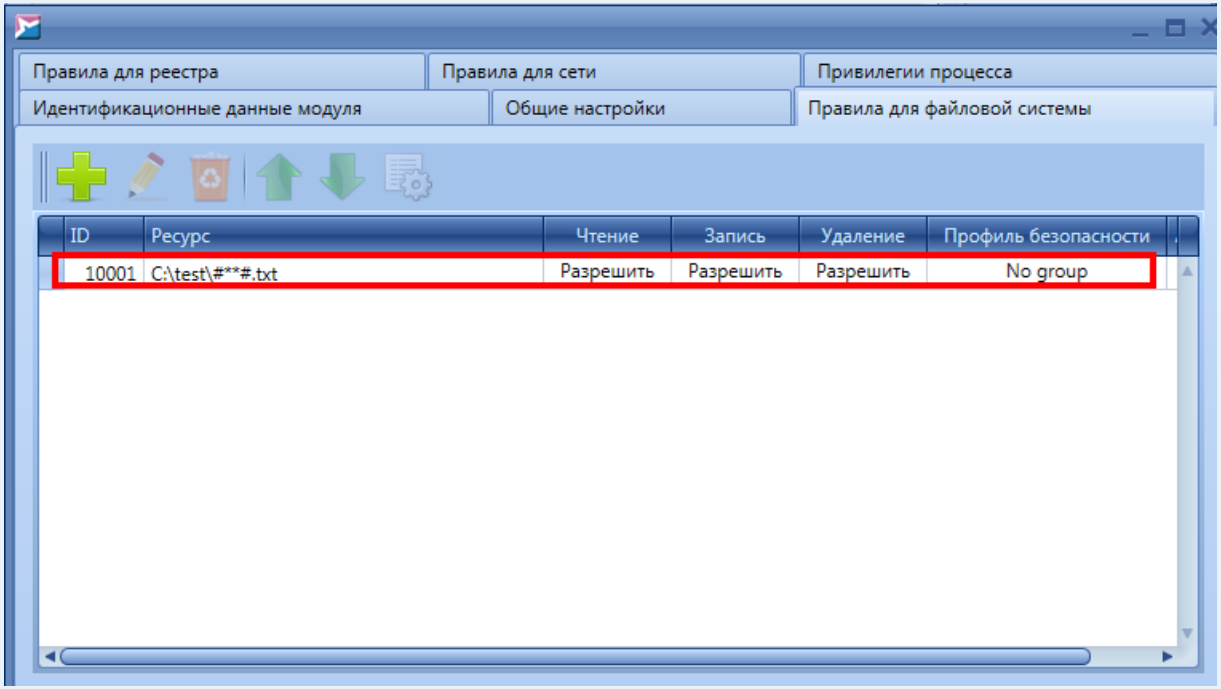
10.2.1.2	Создано правило в разделе **Модули** для приложения *Notepad.exe* (блокнота Windows) на разрешение чтения, записи, удаления текстовых файлов в папке *C:\test\.**	❑ Создано правило разрешения чтения, удаления, записи файлового ресурса *C:\test\[любой_путь\имя].txt* для приложения *Notepad.exe*.	

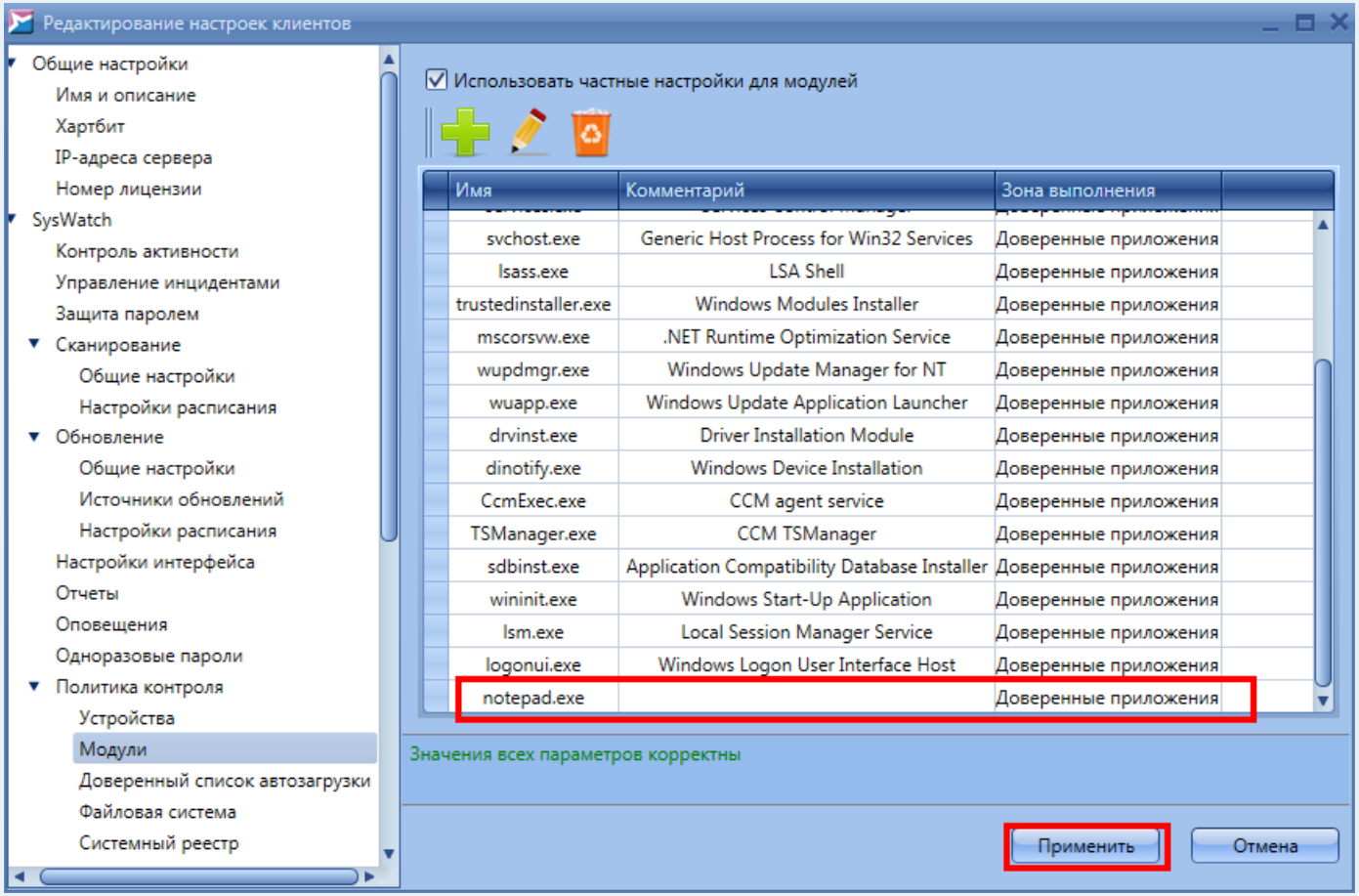
* Для создания правила необходимо отредактировать настройки клиентов:




Правила для реестра
Правила для сети
Привилегии процесса
Идентификационные данные модуля
Общие настройки
Правила для файловой системы
Зона выполнения
Доверенные приложения
Включить режим обновления ПО
Сохранять историю запуска
Назначение учетной записи
Изолированный пользователь V.I.P.O.
Не использовать назначение учетной записи
В доверенном списке автозагрузки
Добавить данные из файла
OK
Отмена

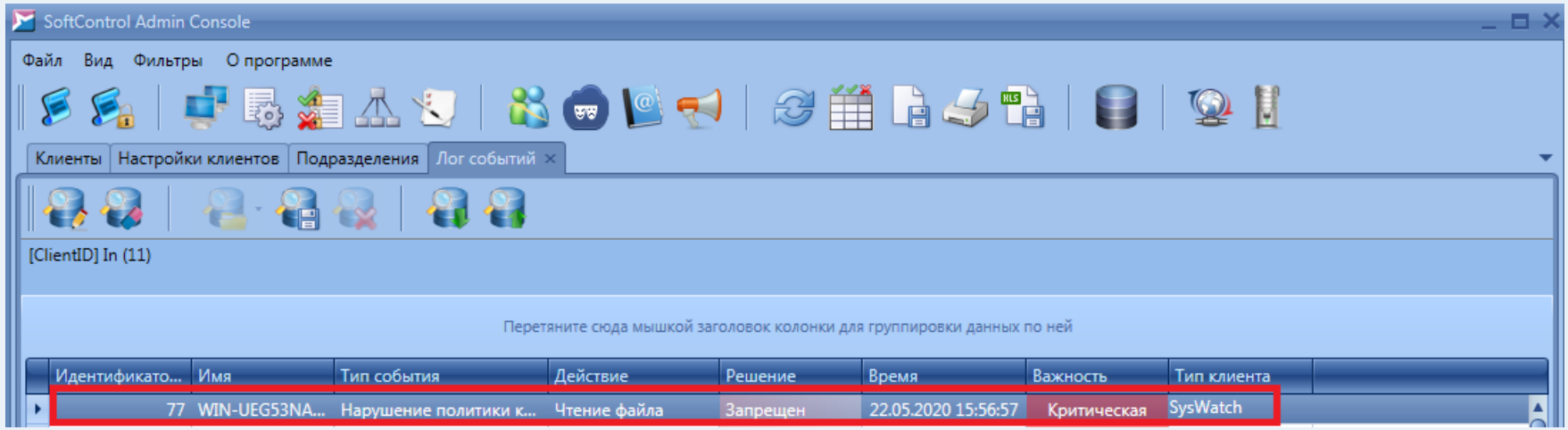

Имя
Комментарий
Зона выполнения
Правила для реестра
Правила для сети
Привилегии процесса
Идентификационные данные модуля
Общие настройки
Правила для файловой системы
1
2
Файл или каталог (полный путь или маска)
C:\test\#**#.txt
3
Профиль безопасности:
No group
Чтение
Запись
Удаление
Разрешить
Разрешить
Разрешить
4
Активно
5
OK
Отмена


Правила для реестра
Правила для сети
Привилегии процесса
Идентификационные данные модуля
Общие настройки
Правила для файловой системы
ID
Ресурс
Чтение
Запись
Удаление
Профиль безопасности
10001
C:\test\#**#.txt
Разрешить
Разрешить
Разрешить
No group



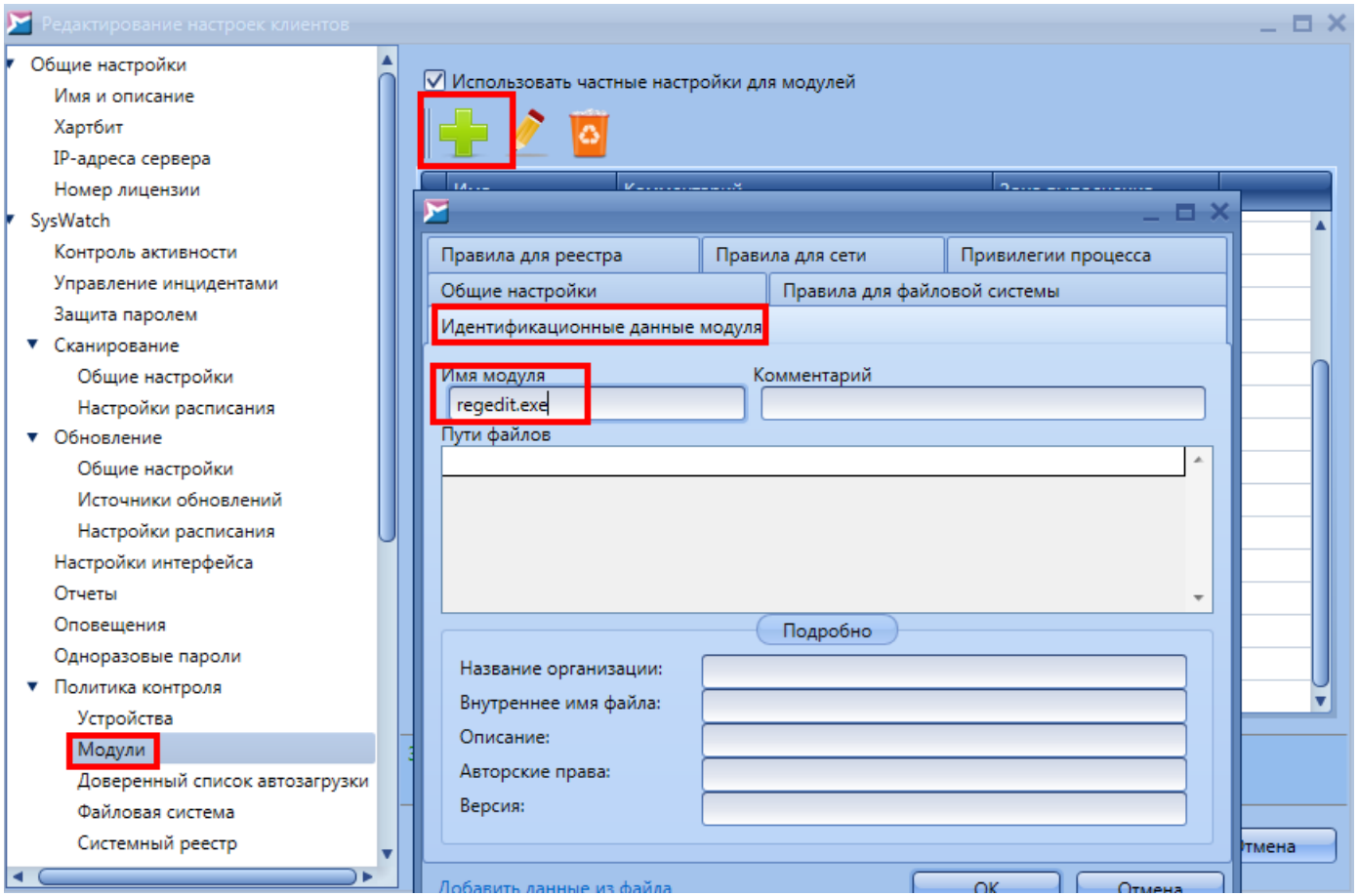
10.2.1.3	Проведена попытка изменить файл *C:\test\1.txt* с помощью *Notepad.exe* и с помощью *Wordpad.exe*.*	❑ С помощью *Notepad.exe* успешное изменение файла; при попытке изменения с помощью *Wordpad.exe* выводится сообщение *Отказано в доступе*.	

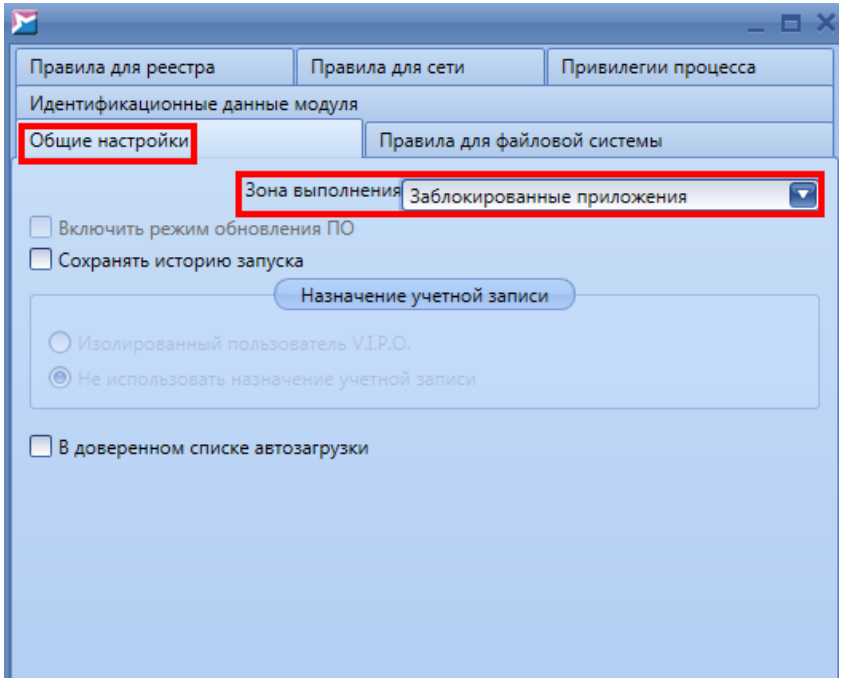
* В консоли администрирования SoftControl Admin Console наблюдается событие **Нарушение политики контроля - Чтение файла**:



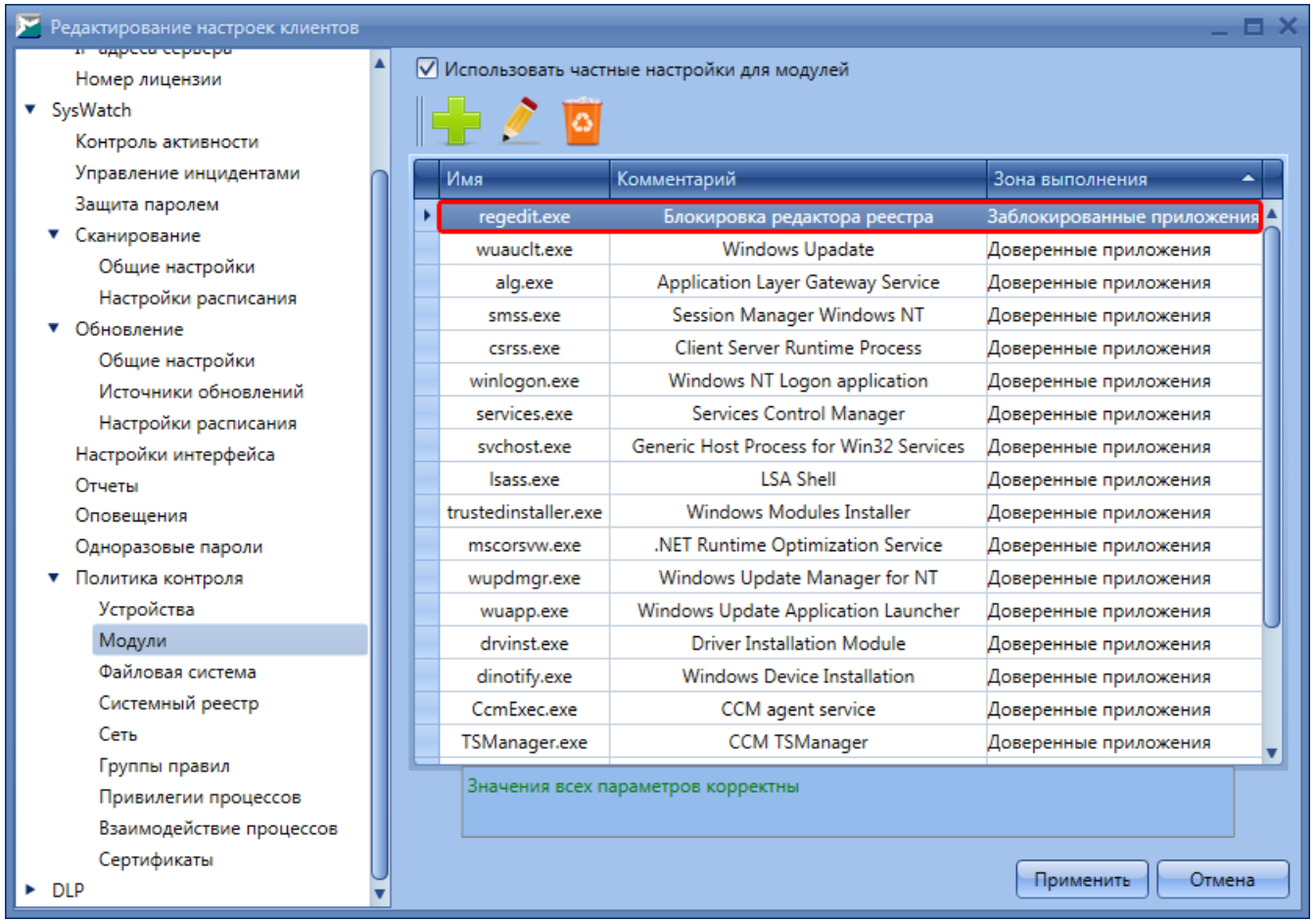
10.2.2	Проверка правил политик контроля для модулей.		
10.2.2.1	Создано правило блокировки запуска редактора реестра Windows через раздел **Модули**.*	❑ Создана настройка блокировки запуска файла *regedit.exe* через раздел **Политика контроля - Модули**.	Создано правило блокировки запуска редактора реестра Windows путем добавления файла *regedit.exe* в список частных настроек для модулей и помещения его в раздел **Зона выполнения - Заблокированные приложения**.

* Для создания правила необходимо отредактировать настройки клиентов:



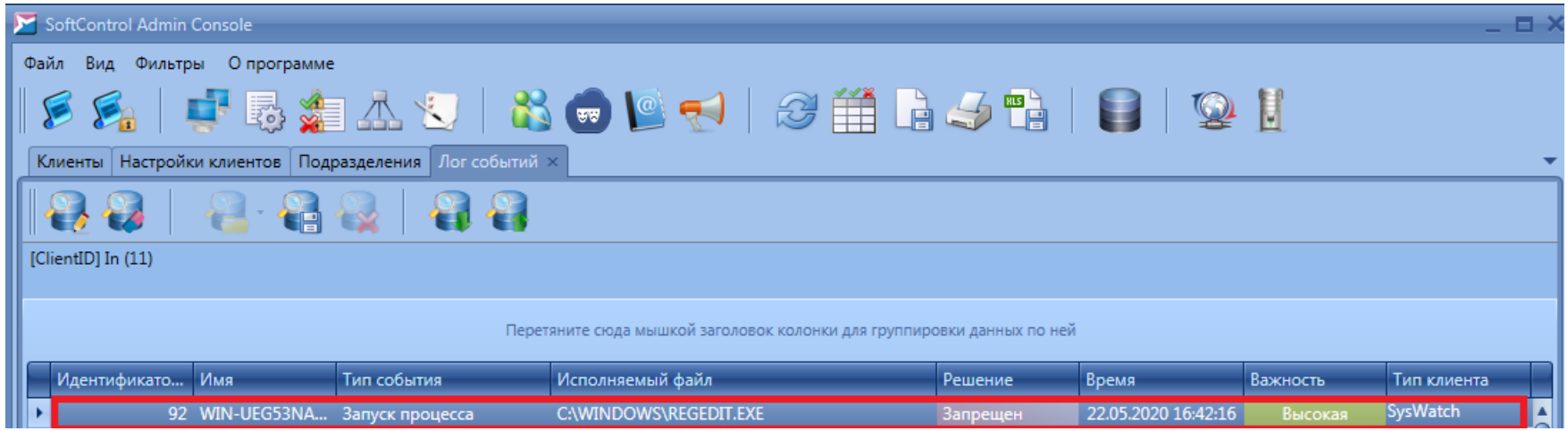

Правила для реестра
Правила для сети
Привилегии процесса
Идентификационные данные модуля
Общие настройки
Правила для файловой системы
Зона выполнения
Заблокированные приложения
Включить режим обновления ПО
Сохранять историю запуска
Назначение учетной записи
Изолированный пользователь V.I.P.O.
Не использовать назначение учетной записи
В доверенном списке автозагрузки

После сохранения настроек в разделе настроек **Политика контроля** - **Модули** появится новая строка:



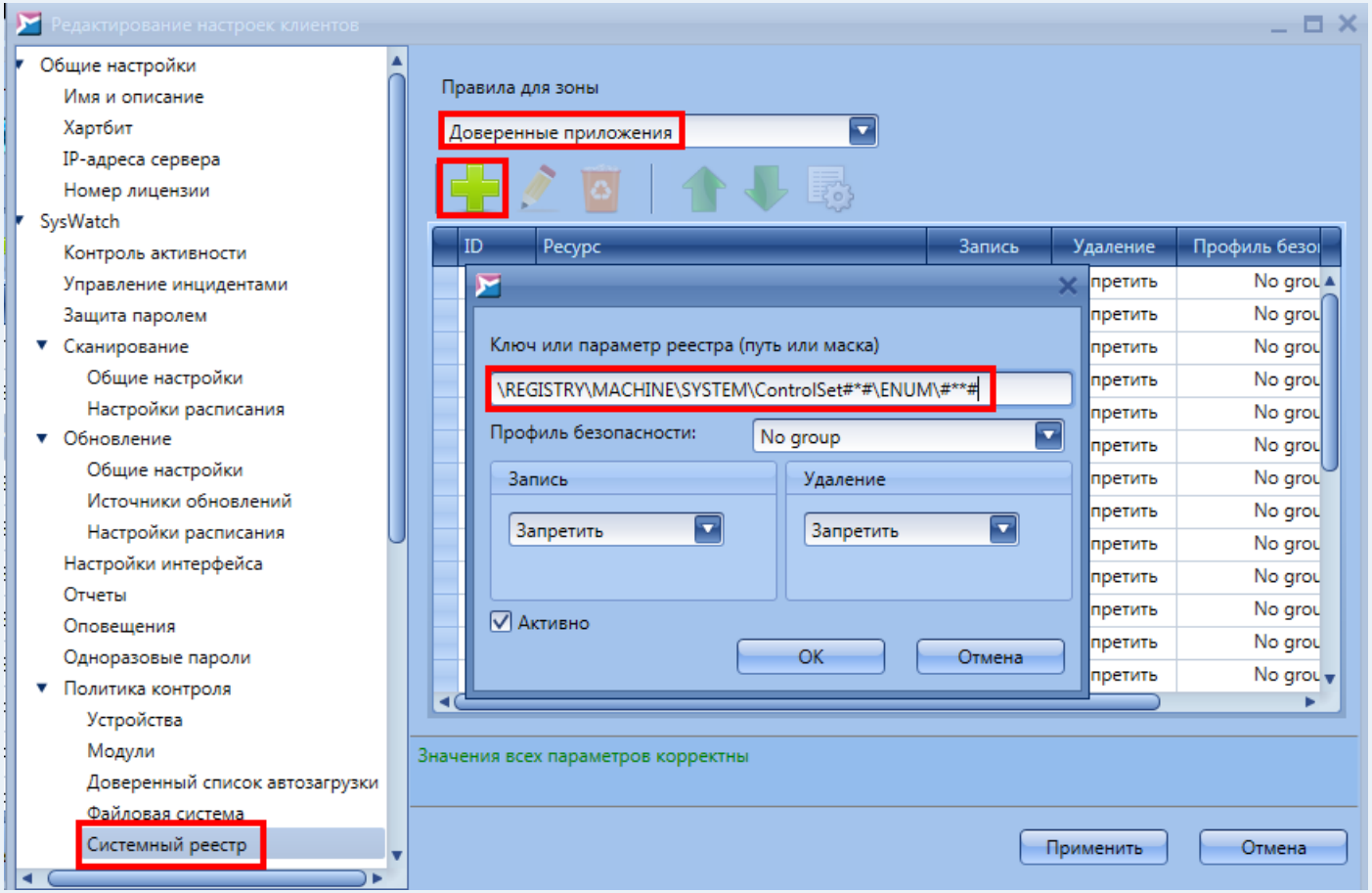
10.2.2.2	Произведена попытка запуска файла *regedit.exe*.	❑ Редактор реестра не запустился, в консоли устройства получено сообщение *Отказано в доступе*.	В логах устройства на сервере управления SoftControl Service Center наблюдается событие **Запуск процесса** *C:\WINDOWS\REGEDIT.EXE* из зоны **Блокированные** с решением по запуску **Запрещен**.*

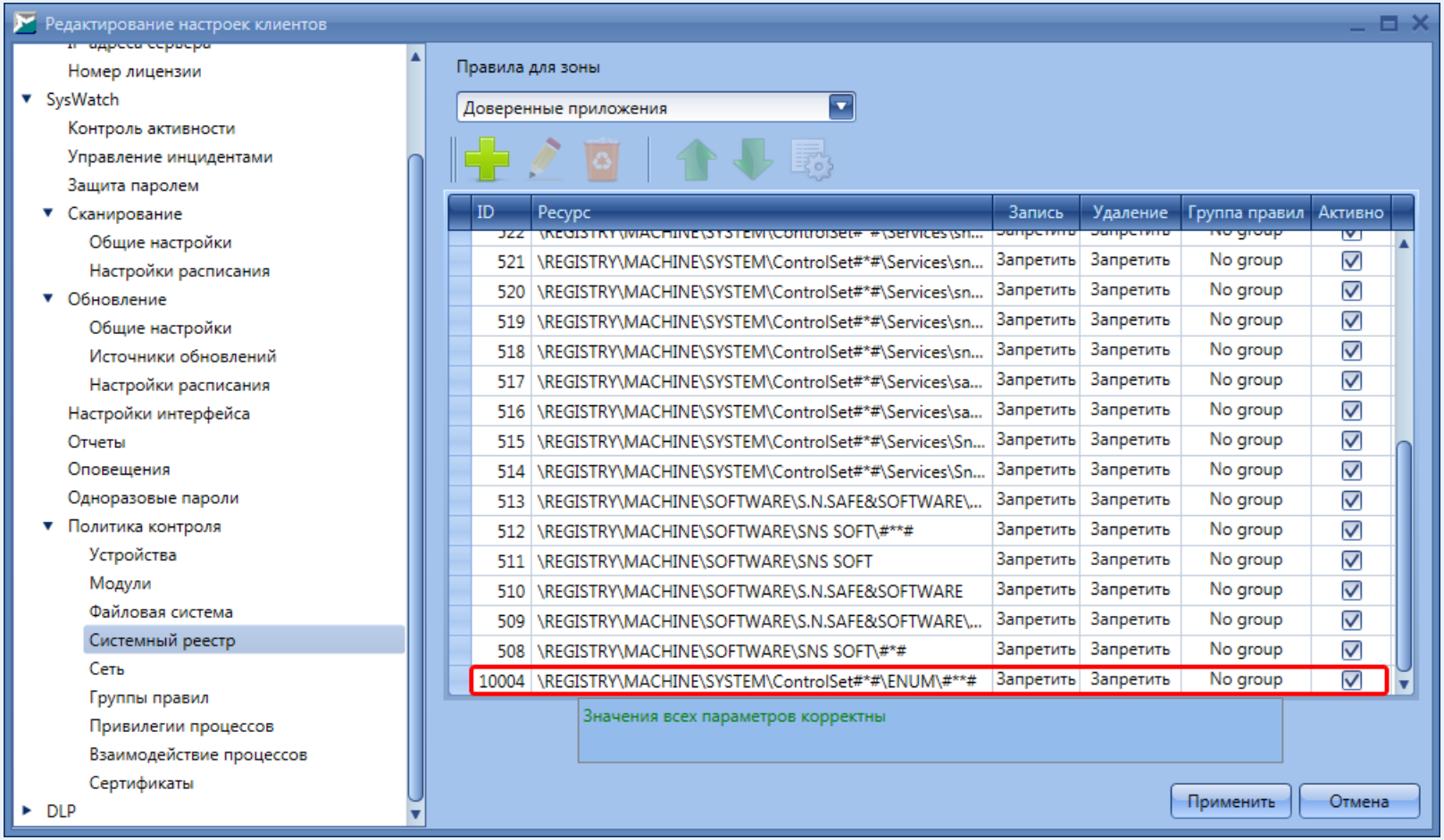
* В консоли администрирования SoftControl Admin Console наблюдается событие **Запуск процесса** из зоны **Блокированные**:



10.2.3	Проверка правил политик контроля для системного реестра		
10.2.3.1	Создано правило блокировки записи в ветку реестра Windows сценариев доступа к функциональным драйверам устройств для PnP-Менеджера (на примере подключения USB-носителя, ранее не подключавшегося к клиентскому устройству).*	❑ Создано правило для зоны **Доверенные приложения** на блокировку записи и удаления.	Ветка реестра для блокировки: *\REGISTRY \MACHINE\SYSTEM\ ControlSet#*#\ENUM\#**#*. Следующее правило для ветки *\REGISTRY \MACHINE\SYSTEM\ CurrentControlSet\ENUM\#**#* необходимо сделать аналогично. Такие правила блокируют работу новых устройств, ранее не подключавшихся к клиентскому устройству.

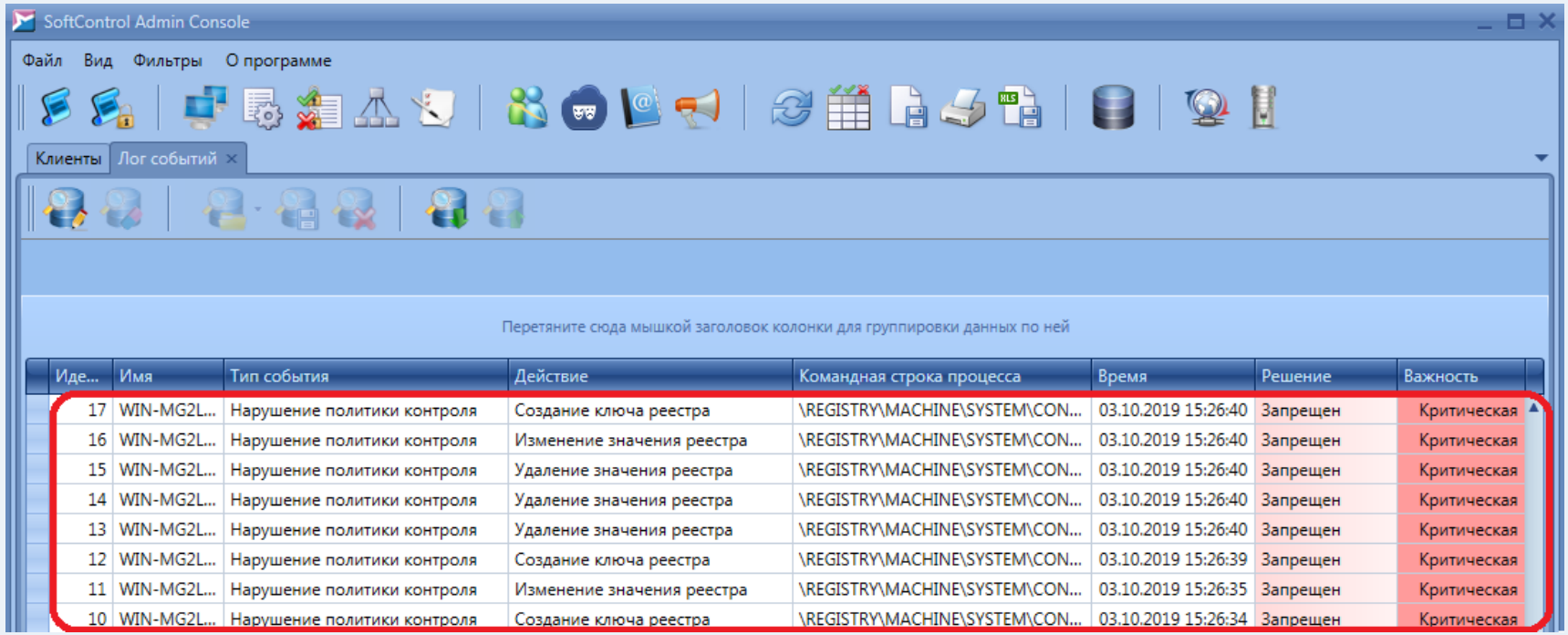
* Для создания правила необходимо отредактировать настройки клиентов, сохранить их под новым именем и применить к подразделению, в котором находится тестируемое устройство.





10.2.3.2	Произведена попытка вставить в тестируемое устройство новый (ранее ни разу не подключавшийся к хосту) USB-носитель.	❑ USB-носитель не подключился к устройству; получено сообщение о том, что драйверы USB-носителя не были установлены.	В логах устройства на сервере управления SoftControl Service Center наблюдается событие **Нарушение политики контроля**; действие – **Создание ключа реестра**, детали – **(ACE_[Номер_правила] =)**, решение – **Запрещен**.*

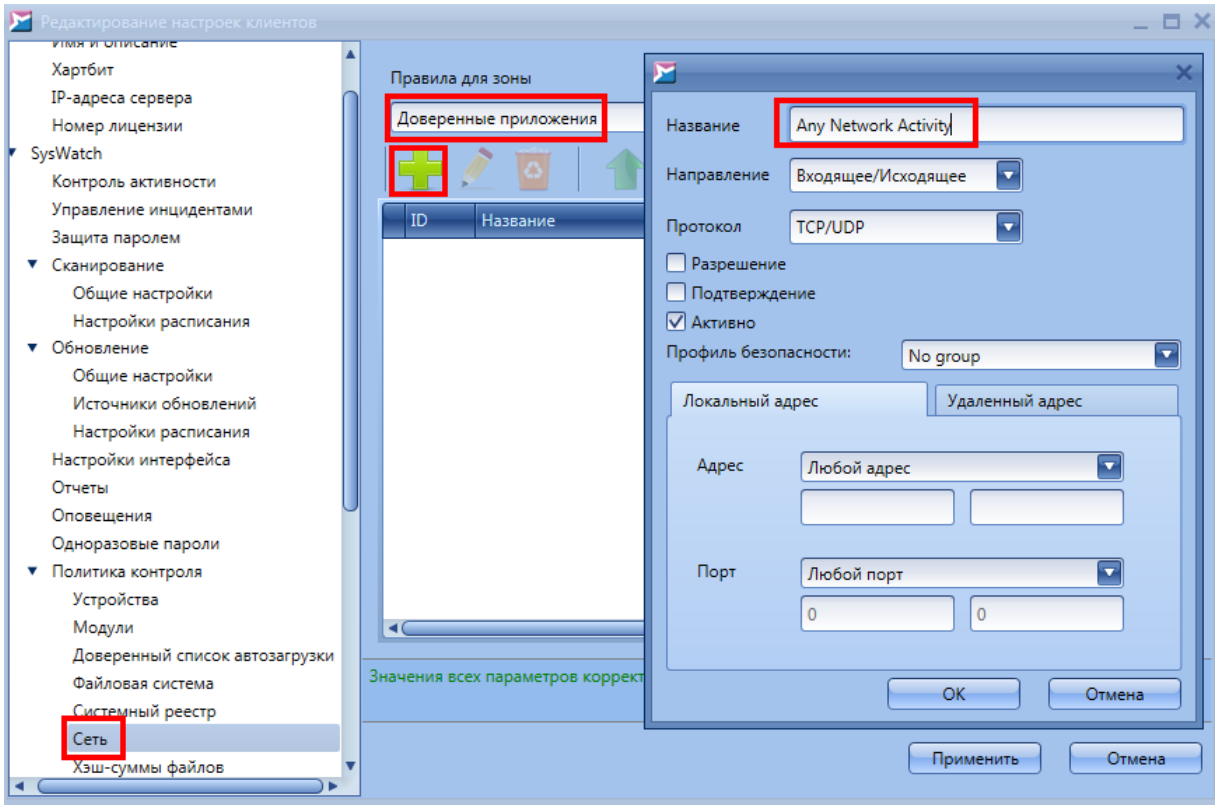
*В консоли администрирования SoftControl Service Center наблюдается событие **Нарушение политики контроля**, действие **Создание ключа реестра**:

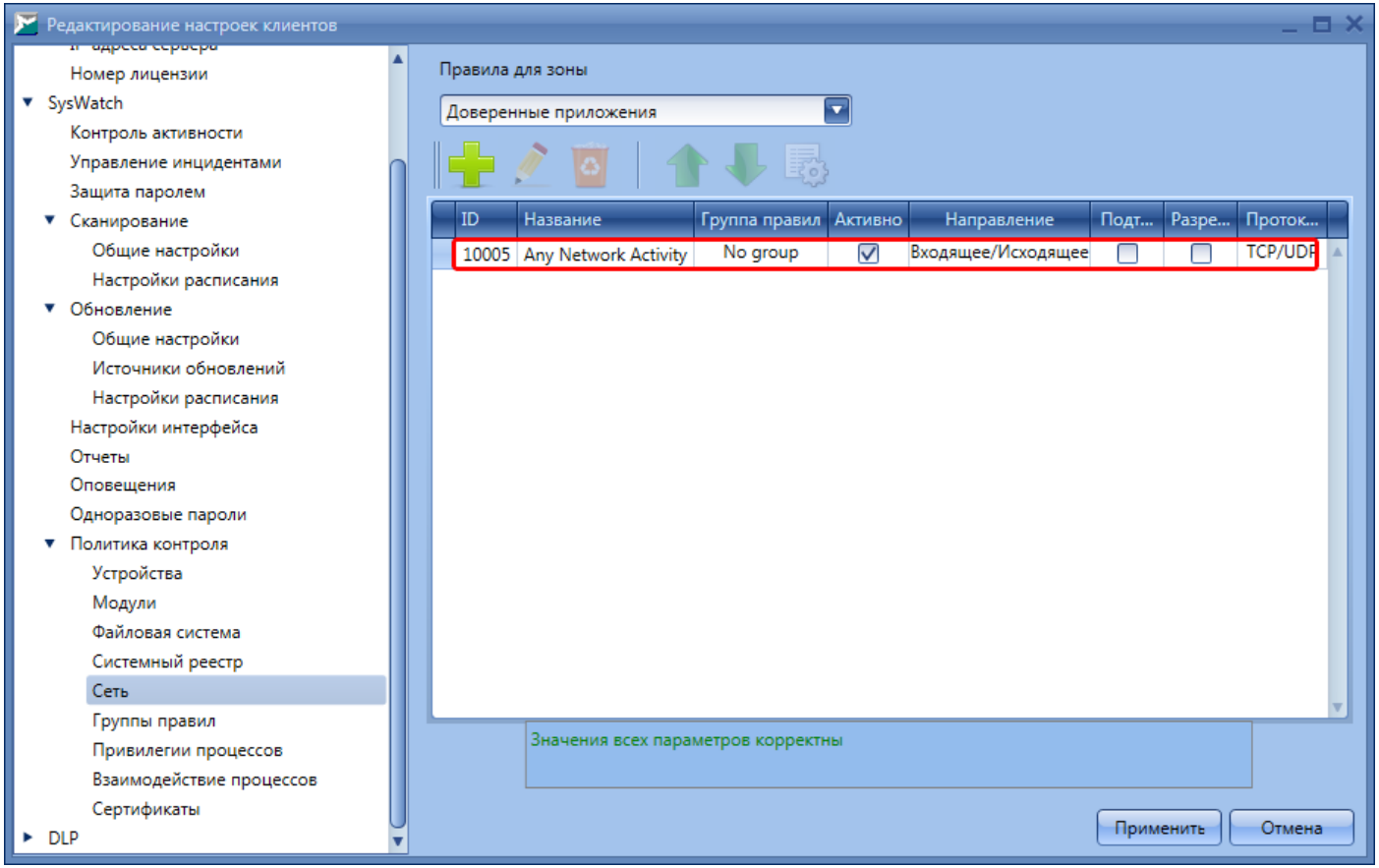


Иде...	Имя	Тип события	Действие	Командная строка процесса	Время	Решение	Важность
17	WIN-MG2L...	Нарушение политики контроля	Создание ключа реестра	\REGISTRY\MACHINE\SYSTEM\CON...	03.10.2019 15:26:40	Запрещен	Критическая
16	WIN-MG2L...	Нарушение политики контроля	Изменение значения реестра	\REGISTRY\MACHINE\SYSTEM\CON...	03.10.2019 15:26:40	Запрещен	Критическая
15	WIN-MG2L...	Нарушение политики контроля	Удаление значения реестра	\REGISTRY\MACHINE\SYSTEM\CON...	03.10.2019 15:26:40	Запрещен	Критическая
14	WIN-MG2L...	Нарушение политики контроля	Удаление значения реестра	\REGISTRY\MACHINE\SYSTEM\CON...	03.10.2019 15:26:40	Запрещен	Критическая
13	WIN-MG2L...	Нарушение политики контроля	Удаление значения реестра	\REGISTRY\MACHINE\SYSTEM\CON...	03.10.2019 15:26:40	Запрещен	Критическая
12	WIN-MG2L...	Нарушение политики контроля	Создание ключа реестра	\REGISTRY\MACHINE\SYSTEM\CON...	03.10.2019 15:26:39	Запрещен	Критическая
11	WIN-MG2L...	Нарушение политики контроля	Изменение значения реестра	\REGISTRY\MACHINE\SYSTEM\CON...	03.10.2019 15:26:35	Запрещен	Критическая
10	WIN-MG2L...	Нарушение политики контроля	Создание ключа реестра	\REGISTRY\MACHINE\SYSTEM\CON...	03.10.2019 15:26:34	Запрещен	Критическая

10.2.4	Проверка правил политики контроля **Сеть**		
10.2.4.1	Создано правило блокировки любой сетевой активности для доверенных приложений.*	❑ Создано правило блокировки любой сетевой активности для доверенных приложений.	

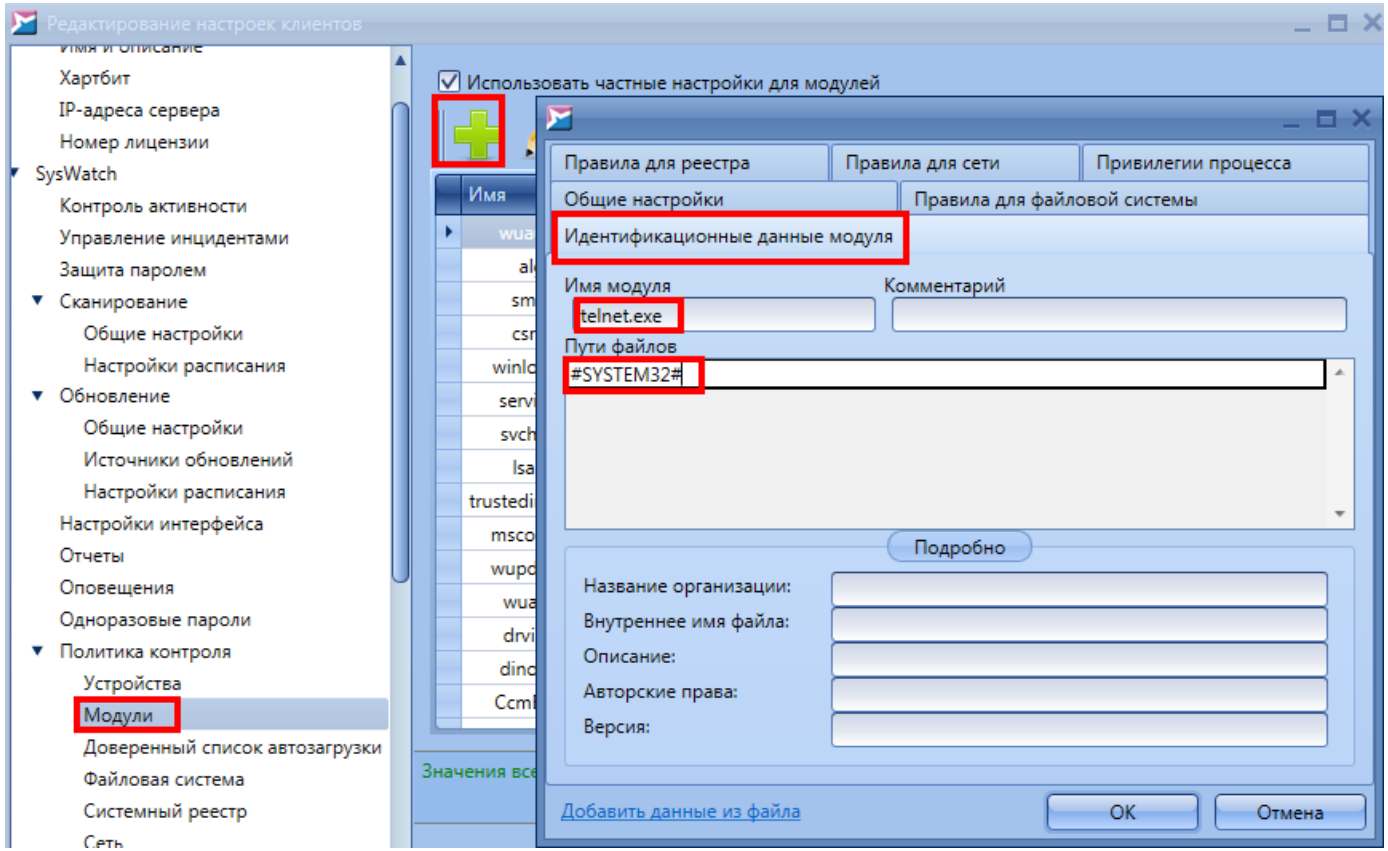
* Для создания правила необходимо отредактировать настройки клиентов, сохранить их под новым именем и применить к подразделению, в котором находится тестируемое устройство. Создание правила **Any Network Activity** блокировки сети для всех приложений из зоны **Доверенные приложения**:

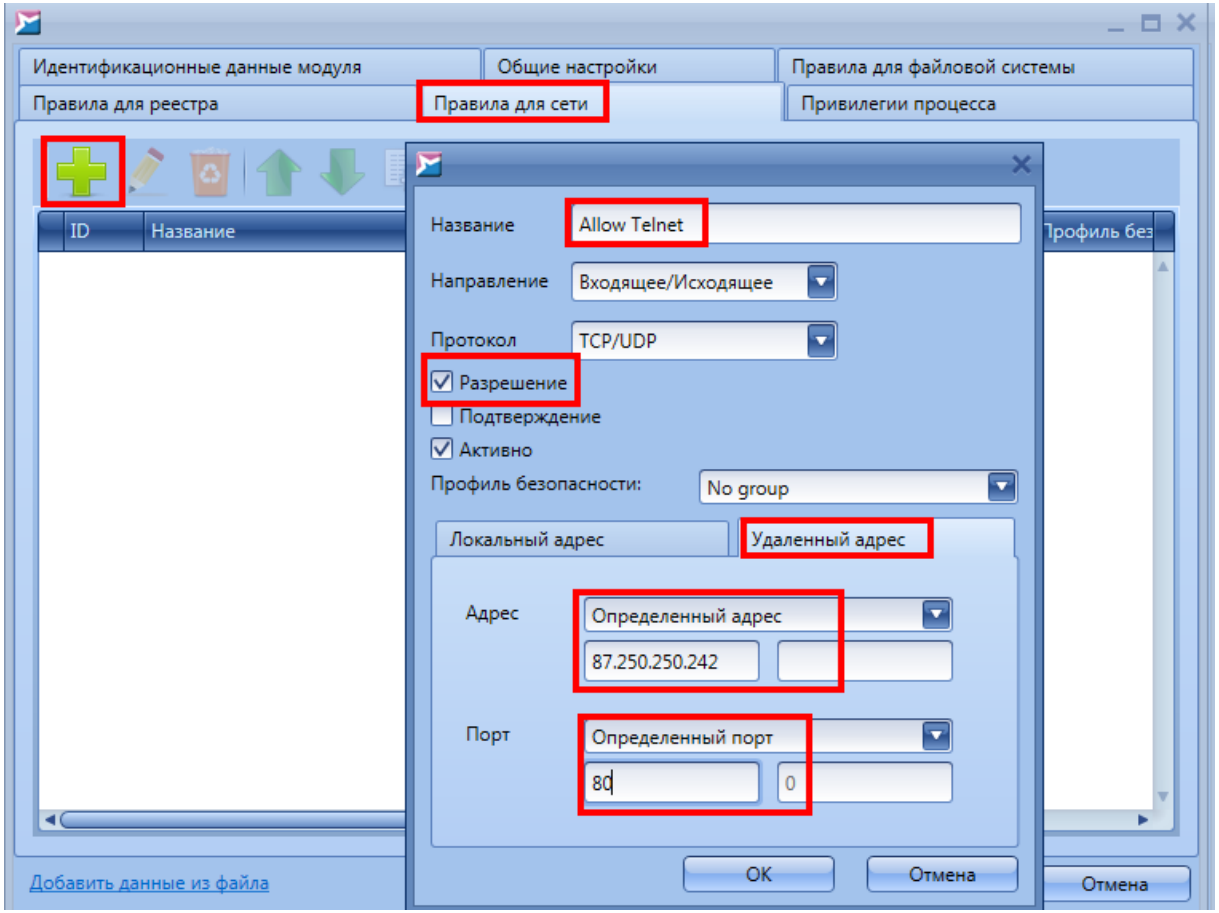


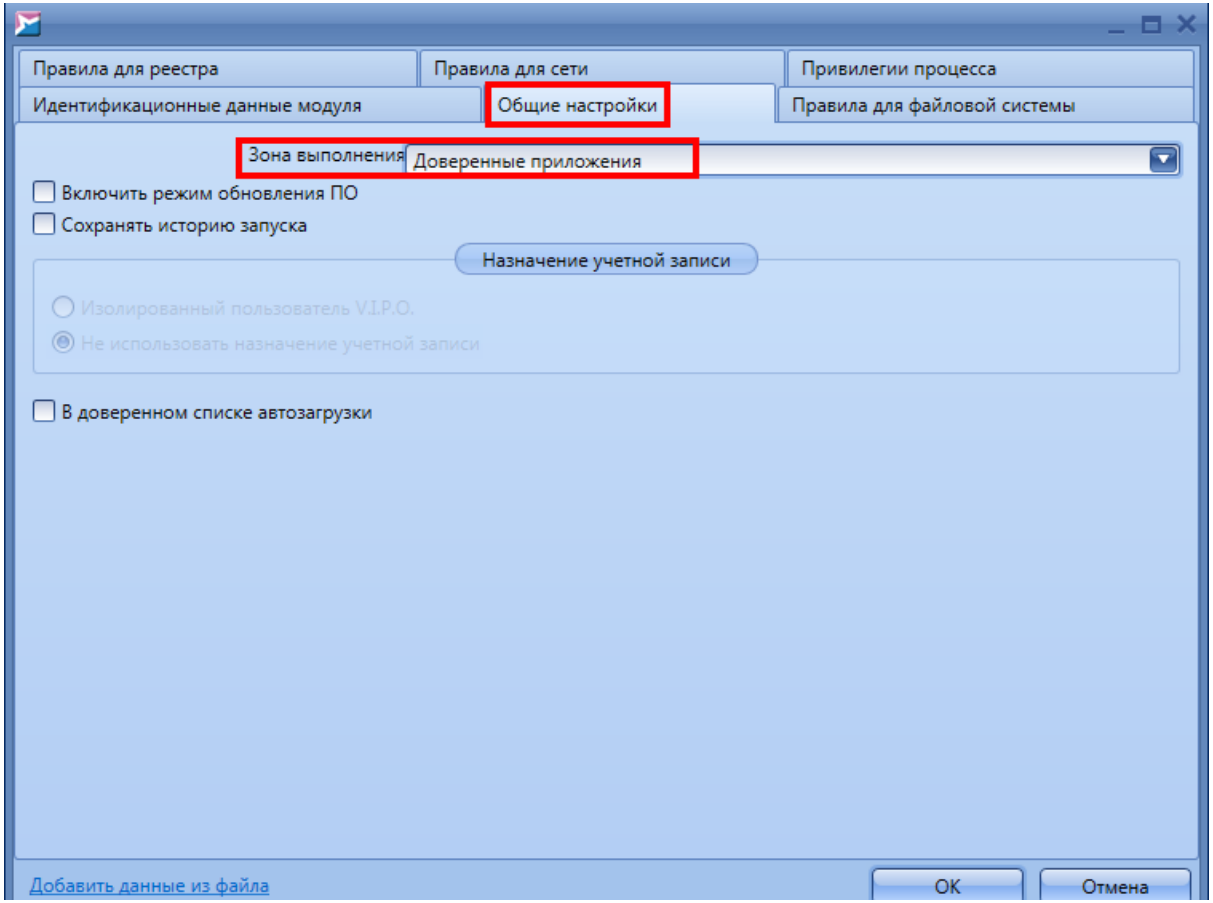


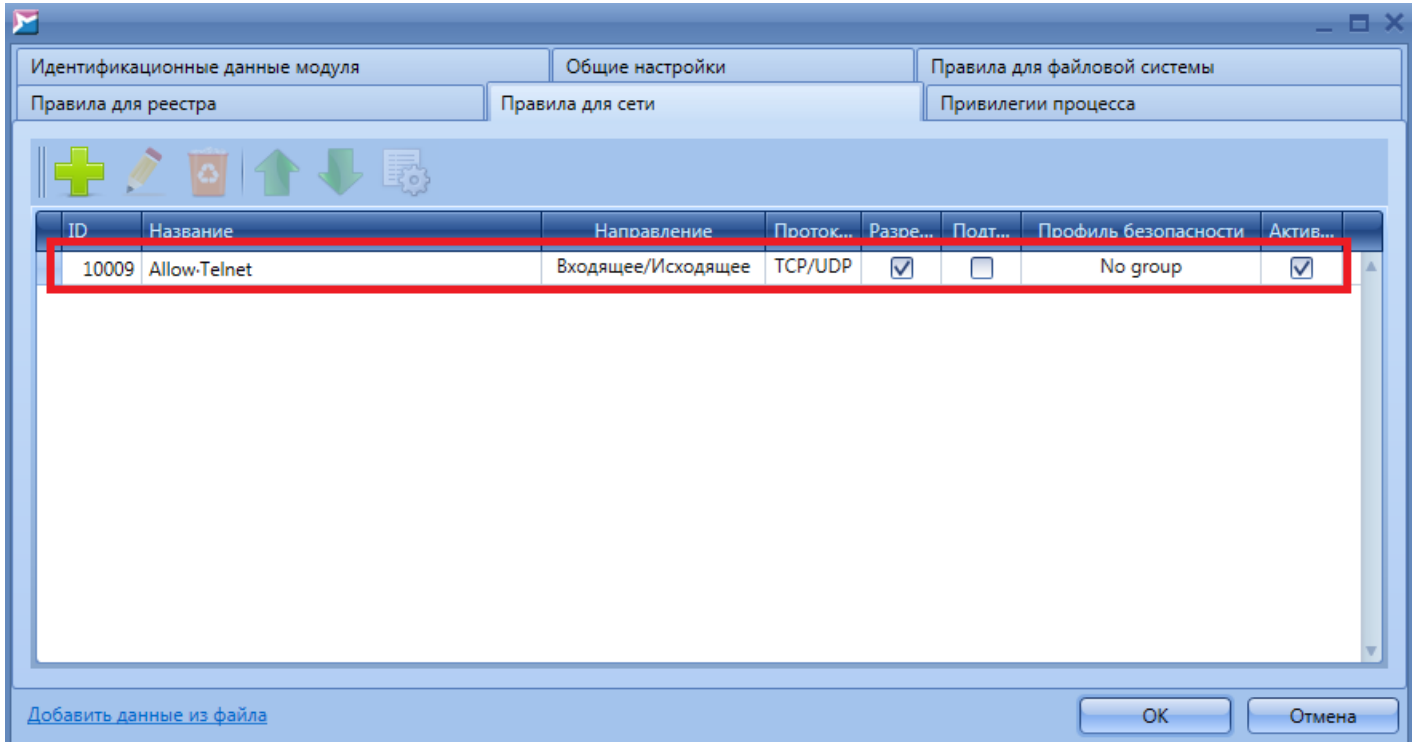
10.2.4.2	Создано правило разрешения доступа для приложения *Telnet* (*C:\windows\system32\telnet.exe*) на адрес *ya.ru* (87.250.250.242:80).*	❑ Создано правило разрешения доступа по сети для *telnet.exe* на адрес *ya.ru* (87.250.250.242:80).	

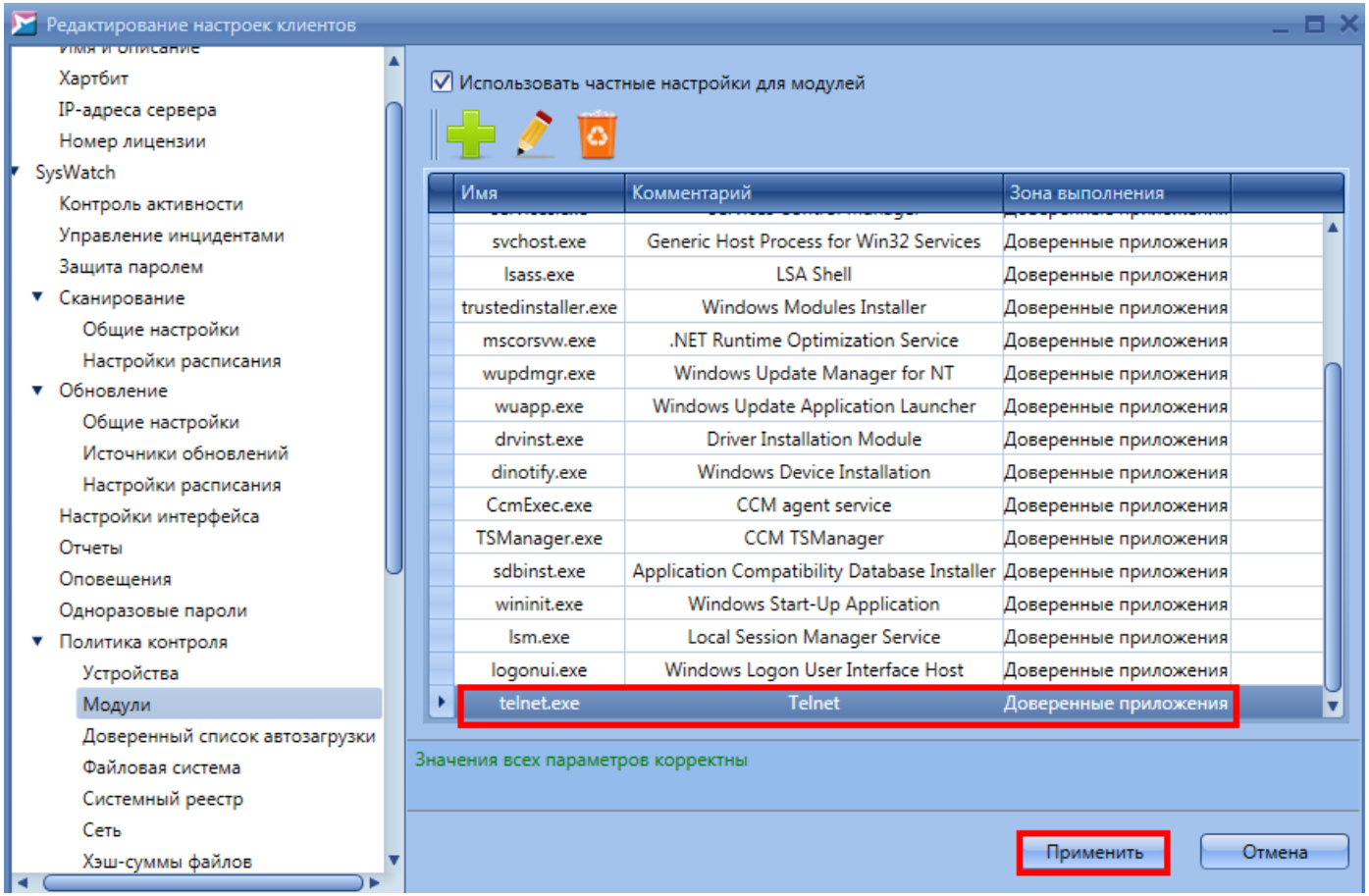
* Для создания правила необходимо отредактировать настройки клиентов, сохранить их под новым именем и применить к подразделению, в котором находится тестируемое устройство. Создание правила для модулей на разрешение доступа по сети приложения *telnet.exe* из папки *#SYSTEM32#* на удаленный адрес *ya.ru* (87.250.250.242:80):




Идентификационные данные модуля
Общие настройки
Правила для файловой системы
Правила для реестра
Правила для сети
Привилегии процесса
ID
Название
Профиль без
Название
Allow Telnet
Направление
Входящее/Исходящее
Протокол
TCP/UDP
Разрешение
Подтверждение
Активно
Профиль безопасности:
No group
Локальный адрес
Удаленный адрес
Адрес
Определенный адрес
87.250.250.242
Порт
Определенный порт
80
0
OK
Отмена
Добавить данные из файла
Отмена


Правила для реестра
Правила для сети
Привилегии процесса
Идентификационные данные модуля
Общие настройки
Правила для файловой системы
Зона выполнения
Доверенные приложения
Включить режим обновления ПО
Сохранять историю запуска
Назначение учетной записи
Изолированный пользователь V.I.P.O.
Не использовать назначение учетной записи
В доверенном списке автозагрузки
Добавить данные из файла
OK
Отмена


Идентификационные данные модуля
Общие настройки
Правила для файловой системы
Правила для реестра
Правила для сети
Привилегии процесса
ID
Название
Направление
Прото...
Разре...
Подт...
Профиль безопасности
Актив...
10009
Allow-Telnet
Входящее/Исходящее
TCP/UDP
No group
Добавить данные из файла
OK
Отмена


Редактирование настроек клиентов
Хартбит
IP-адреса сервера
Номер лицензии
SysWatch
Контроль активности
Управление инцидентами
Защита паролем
Сканирование
Общие настройки
Настройки расписания
Обновление
Общие настройки
Источники обновлений
Настройки расписания
Настройки интерфейса
Отчеты
Оповещения
Одноразовые пароли
Политика контроля
Устройства
Модули
Доверенный список автозагрузки
Файловая система
Системный реестр
Сеть
Хэш-суммы файлов
Использовать частные настройки для модулей
Имя
Комментарий
Зона выполнения
svchost.exe
Generic Host Process for Win32 Services
Доверенные приложения
lsass.exe
LSA Shell
Доверенные приложения
trustedinstaller.exe
Windows Modules Installer
Доверенные приложения
mscorsvw.exe
.NET Runtime Optimization Service
Доверенные приложения
wupdmgr.exe
Windows Update Manager for NT
Доверенные приложения
wuapp.exe
Windows Update Application Launcher
Доверенные приложения
drvinst.exe
Driver Installation Module
Доверенные приложения
dinotify.exe
Windows Device Installation
Доверенные приложения
CcmExec.exe
CCM agent service
Доверенные приложения
TSManager.exe
CCM TSManager
Доверенные приложения
sdbinst.exe
Application Compatibility Database Installer
Доверенные приложения
wininit.exe
Windows Start-Up Application
Доверенные приложения
lsm.exe
Local Session Manager Service
Доверенные приложения
logonui.exe
Windows Logon User Interface Host
Доверенные приложения
telnet.exe
Telnet
Доверенные приложения
Значения всех параметров корректны
Применить
Отмена

10.2.4.3	Произведена попытка доступа *telnet.exe* на адрес *ya.ru* (87.250.250.242:80) и на адрес 192.168.1.180:8000 (указан случайный адрес для примера).	❑ Соединение с адресом 87.250.250.242:80 установлено успешно, с адресом 192.168.1.180:8000 – не установлено.	В логах устройства на сервере управления SoftControl Service Center наблюдается событие **Нарушение политики контроля**; действие – **Попытка установить исходящее соединение**, исполняемый файл – *C:\WINDOWS\SYSTEM32\TELNET.EXE*, детали – **(ACE_[Номер_ правила] =)**, решение – **Запрещен**.*

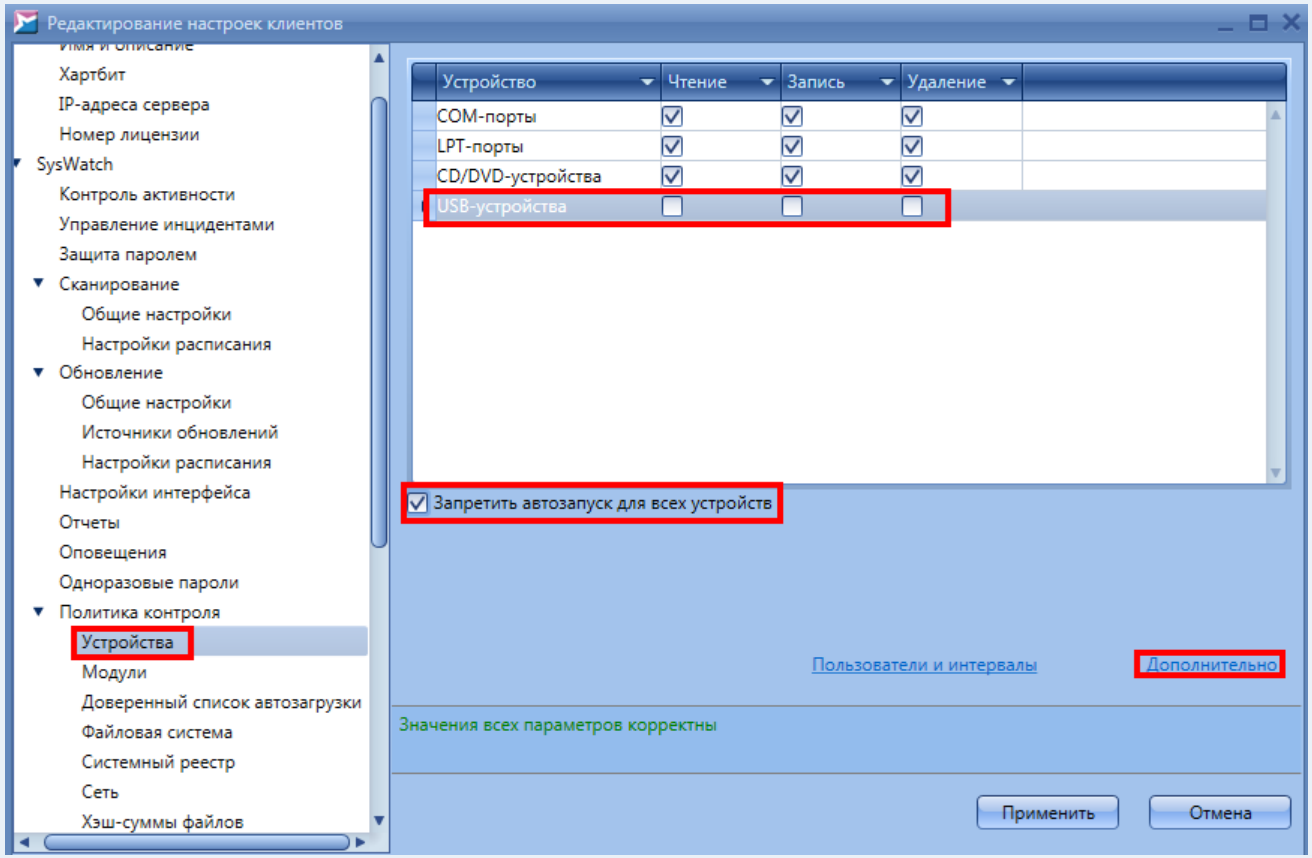
* В консоли администрирования SoftControl Admin Console наблюдается событие **Нарушение политики контроля - Попытка установить исходящее соединение**:

Тип события	Действие	Исполняемый файл	Командная строка процесса	Детали	Решение
Нарушение политики контроля	Попытка принять входящее соединение	SYSTEM	192.168.1.58:137 <- 192.168.1.255:137	(ACE_10005 =...	Запрещен
Нарушение политики контроля	Попытка принять входящее соединение	SYSTEM	192.168.1.89:137 <- 192.168.1.255:137	(ACE_10005 =...	Запрещен
Нарушение политики контроля	Попытка принять входящее соединение	C:\WINDOWS\SYSTEM32...	192.168.1.89:61471 <- 224.0.0.252:5355	(ACE_10005 =...	Запрещен
Нарушение политики контроля	Попытка принять входящее соединение	C:\WINDOWS\SYSTEM32...	192.168.1.89:61849 <- 224.0.0.252:5355	(ACE_10005 =...	Запрещен
Нарушение политики контроля	Попытка принять входящее соединение	C:\WINDOWS\SYSTEM32...	192.168.1.43:56186 <- 224.0.0.252:5355	(ACE_10005 =...	Запрещен
Нарушение политики контроля	Попытка принять входящее соединение	C:\PROGRAM FILES (X86)...	192.168.1.89:5353 <- 224.0.0.251:5353	(ACE_10005 =...	Запрещен
Нарушение политики контроля	Попытка принять входящее соединение	C:\WINDOWS\SYSTEM32...	192.168.1.89:61471 <- 224.0.0.252:5355	(ACE_10005 =...	Запрещен
Нарушение политики контроля	Попытка принять входящее соединение	C:\WINDOWS\SYSTEM32...	192.168.1.89:61849 <- 224.0.0.252:5355	(ACE_10005 =...	Запрещен
Нарушение политики контроля	Попытка принять входящее соединение	SYSTEM	192.168.1.89:137 <- 192.168.1.255:137	(ACE_10005 =...	Запрещен
Нарушение политики контроля	Попытка принять входящее соединение	SYSTEM	192.168.1.7:35161 <- 192.168.1.255:137	(ACE_10005 =...	Запрещен
Нарушение политики контроля	Попытка принять входящее соединение	SYSTEM	192.168.1.7:51319 <- 192.168.1.255:137	(ACE_10005 =...	Запрещен
Нарушение политики контроля	Попытка принять входящее соединение	SYSTEM	192.168.1.7:46941 <- 192.168.1.255:137	(ACE_10005 =...	Запрещен
Нарушение политики контроля	Попытка принять входящее соединение	SYSTEM	192.168.1.11:137 <- 192.168.1.255:137	(ACE_10005 =...	Запрещен
Нарушение политики контроля	Попытка установить исходящее соединение	C:\WINDOWS\SYSTEM32\TELNET.EXE	192.168.1.25:49179 -> 192.168.1.180:8000	(ACE_10005 =...	Запрещен
Запуск процесса	; Инсталлятор: нет; В профиле: да; Был ли...	C:\WINDOWS\SYSTEM32\TELNET.EXE	telnet 192.168.1.180 8000		Разрешен
Нарушение политики контроля	Попытка принять входящее соединение	SYSTEM	192.168.1.11:137 <- 192.168.1.255:137	(ACE_10005 =...	Запрещен
Нарушение политики контроля	Попытка принять входящее соединение	SYSTEM	192.168.1.133:137 <- 192.168.1.255:137	(ACE_10005 =...	Запрещен
Нарушение политики контроля	Попытка принять входящее соединение	SYSTEM	192.168.1.83:138 <- 192.168.1.255:138	(ACE_10005 =...	Запрещен
Нарушение политики контроля	Попытка принять входящее соединение	SYSTEM	192.168.1.83:137 <- 192.168.1.255:137	(ACE_10005 =...	Запрещен
Нарушение политики контроля	Попытка принять входящее соединение	SYSTEM	192.168.1.133:137 <- 192.168.1.255:137	(ACE_10005 =...	Запрещен
Нарушение политики контроля	Попытка принять входящее соединение	SYSTEM	192.168.1.180:138 <- 192.168.1.255:138	(ACE_10005 =...	Запрещен
Нарушение политики контроля	Попытка принять входящее соединение	SYSTEM	192.168.1.7:52628 <- 192.168.1.255:137	(ACE_10005 =...	Запрещен
Нарушение политики контроля	Попытка принять входящее соединение	SYSTEM	192.168.1.7:38307 <- 192.168.1.255:137	(ACE_10005 =...	Запрещен

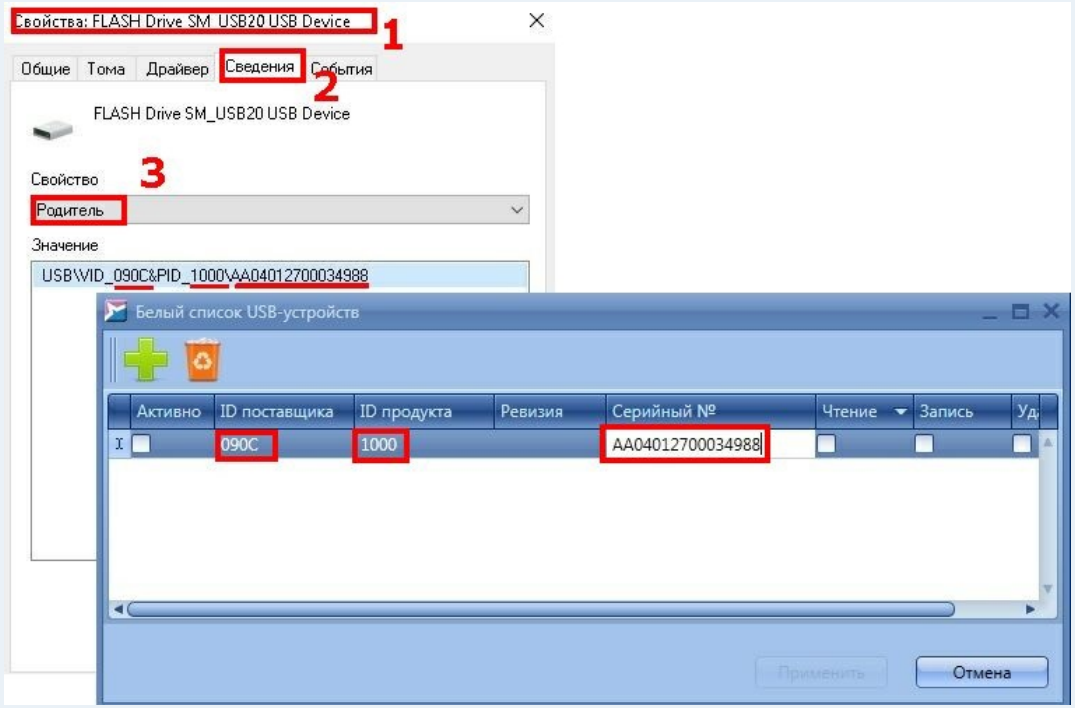
10.2.5	Проверка правил политик контроля для устройств	

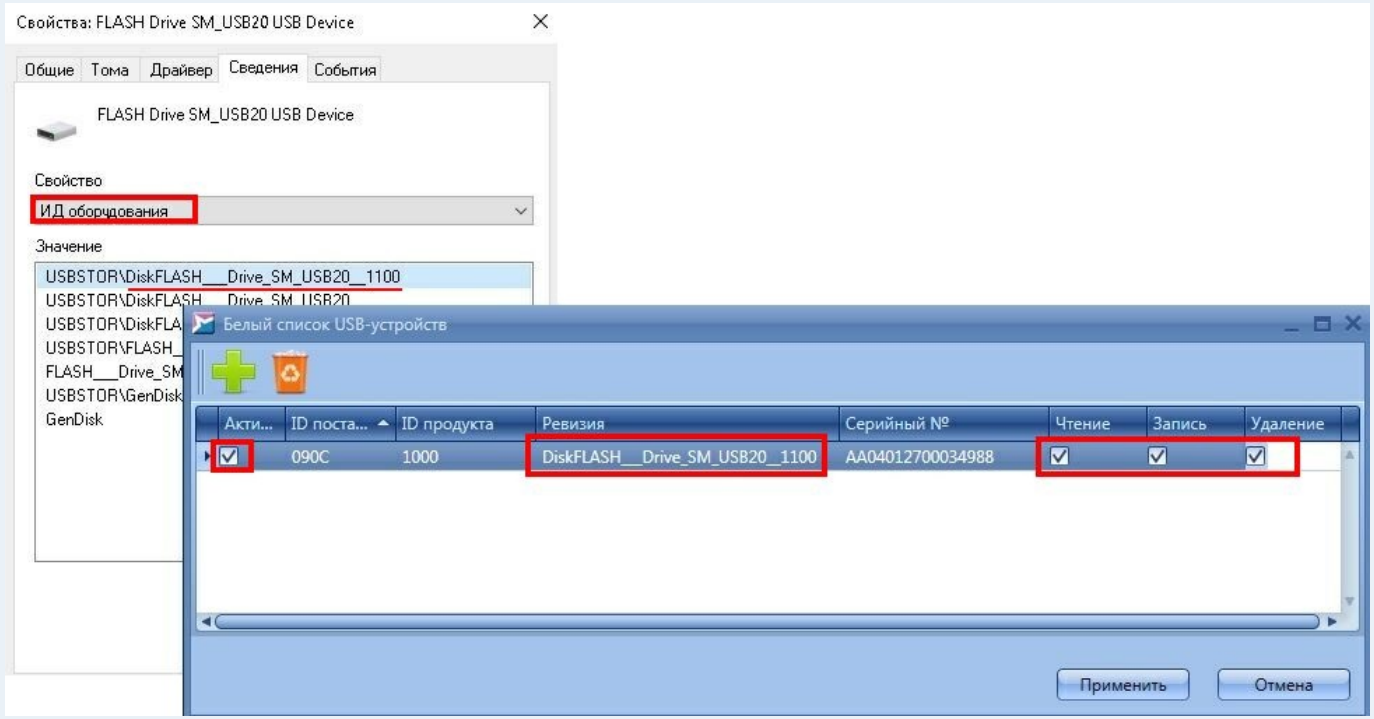
10.2.5.1	Создано правило блокировки доступа к файловой системе USB-носителя, с включением белого списка и добавлением в него доверенного USB-носителя*.	❑ Запрещен доступ к файловой системе USB-носителей, кроме USB-носителей из белого списка.	

* Для создания правила необходимо отредактировать настройки клиентов:



Через диспетчер устройств Windows извлечь данные для формирования правила для доверенного USB-носителя:

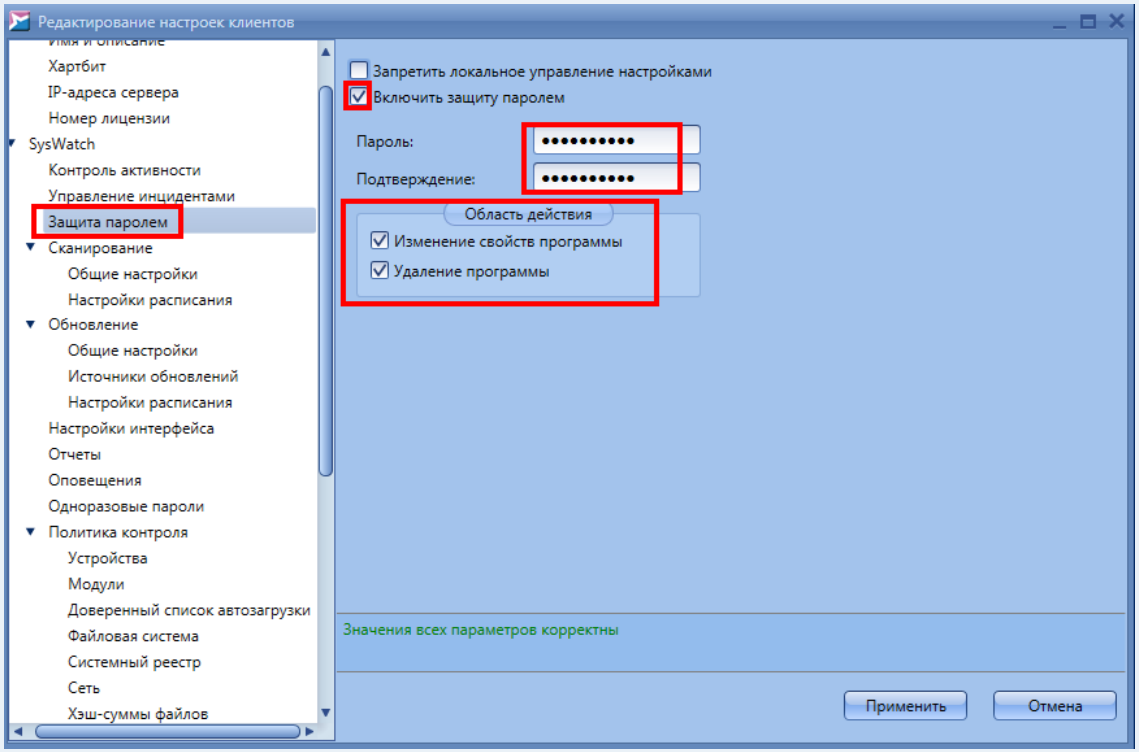




После создания правил необходимо сохранить настройки под новым именем и применить их к подразделению, в котором находится тестируемое устройство.

10.2.5.2	Проведена попытка доступа к файловой системе USB-носителя из белого списка и стороннего USB-носителя.	❑ Доступ к файловой системе USB-носителя из белого списка произведен; при обращении к файловой системе стороннего USB-носителя доступ запрещен с сообщением *Отказано в доступе*.	
10.2.6	Проверка правил политик контроля для функциональности самозащиты **Защита паролем**		
10.2.6.1	Установлен пароль на доступ к графическому интерфейсу (GUI), на изменение свойств и удаление клиентского модуля SoftControl SysWatch.*	❑ Для доступа к графическому интерфейсу (GUI), для изменения свойств и удаления клиентского модуля SoftControl SysWatch требуется ввод пароля.	

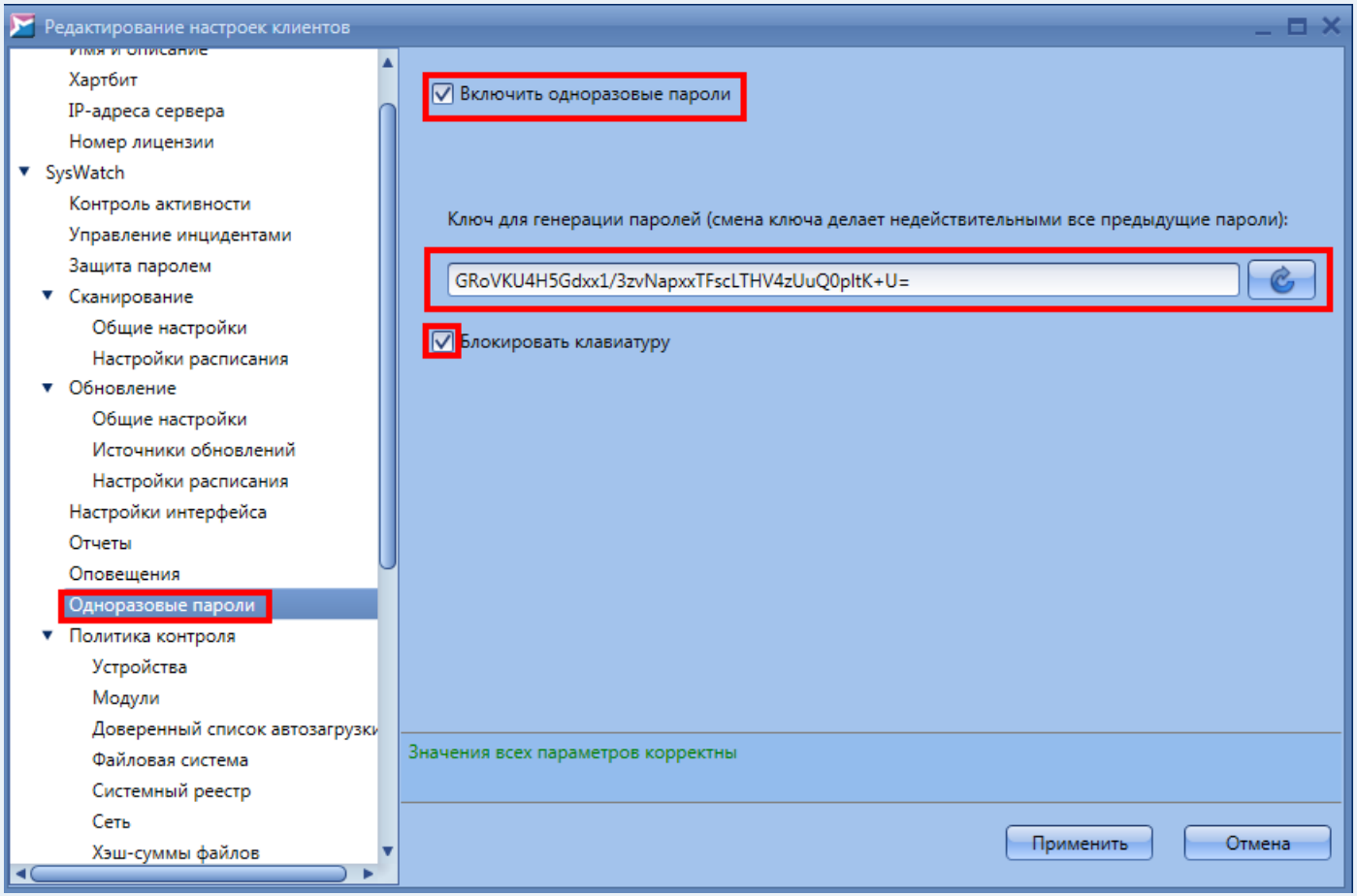
* Для установки пароля необходимо отредактировать настройки клиентов:



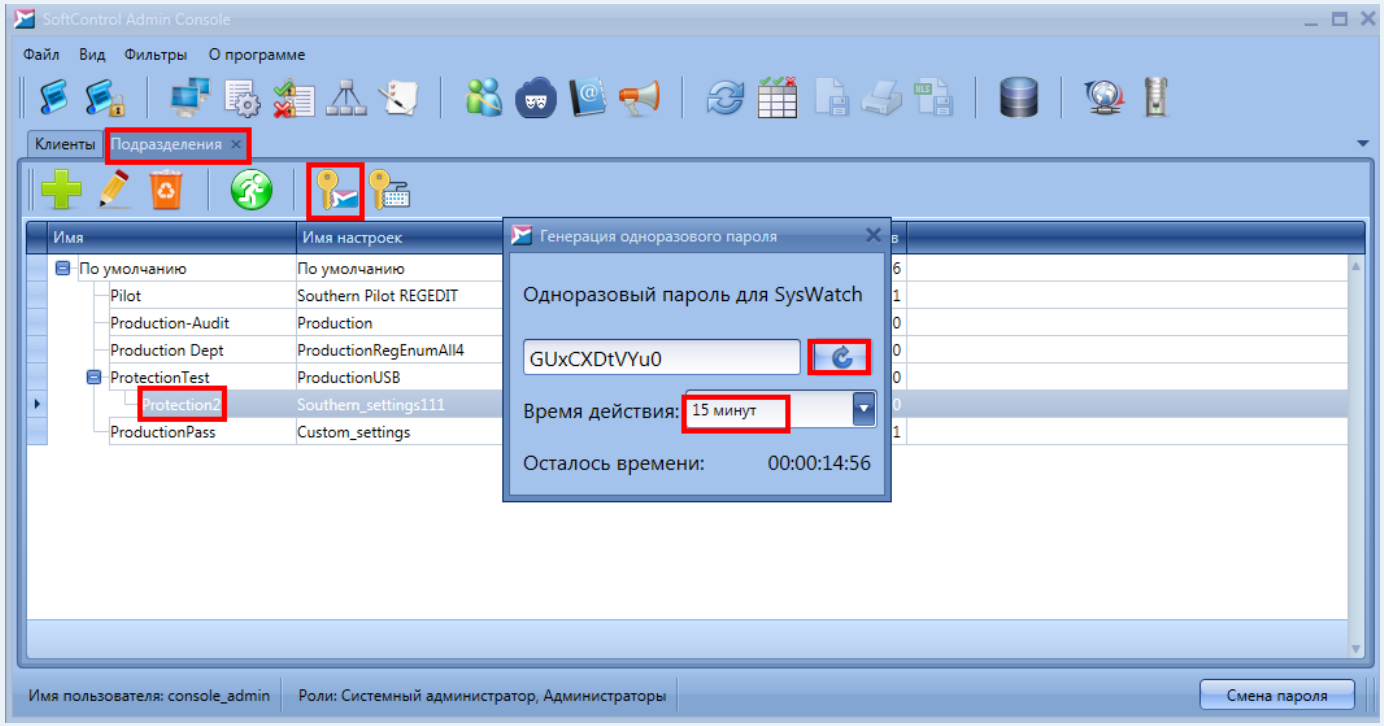
10.2.6.2	Проверен доступ к графическому интерфейсу, произведена попытка удалить клиентский модуль SoftControl SysWatch.	❑ Доступ в GUI без пароля невозможен; при попытке удалить клиентский модуль SoftControl SysWatch запрашивается пароль.	
10.2.7	Проверка правил политик контроля для одноразовых (временных) паролей		

10.2.7.1	Проведено включение одноразовых (временных) паролей на доступ к графическому интерфейсу клиентского модуля SoftControl SysWatch, включена блокировка клавиатуры.*	❑ Включены одноразовые пароли, блокировка клавиатуры.	Одноразовый пароль – это хэш-функция времени по UTC. Для работы одноразового пароля на доступ к графическому интерфейсу клиентского модуля SoftControl SysWatch (разблокировку клавиатуры) время по UTC на клиентском устройстве и SoftControl Admin Console должно совпадать или различаться не более, чем на время действия одноразового пароля.

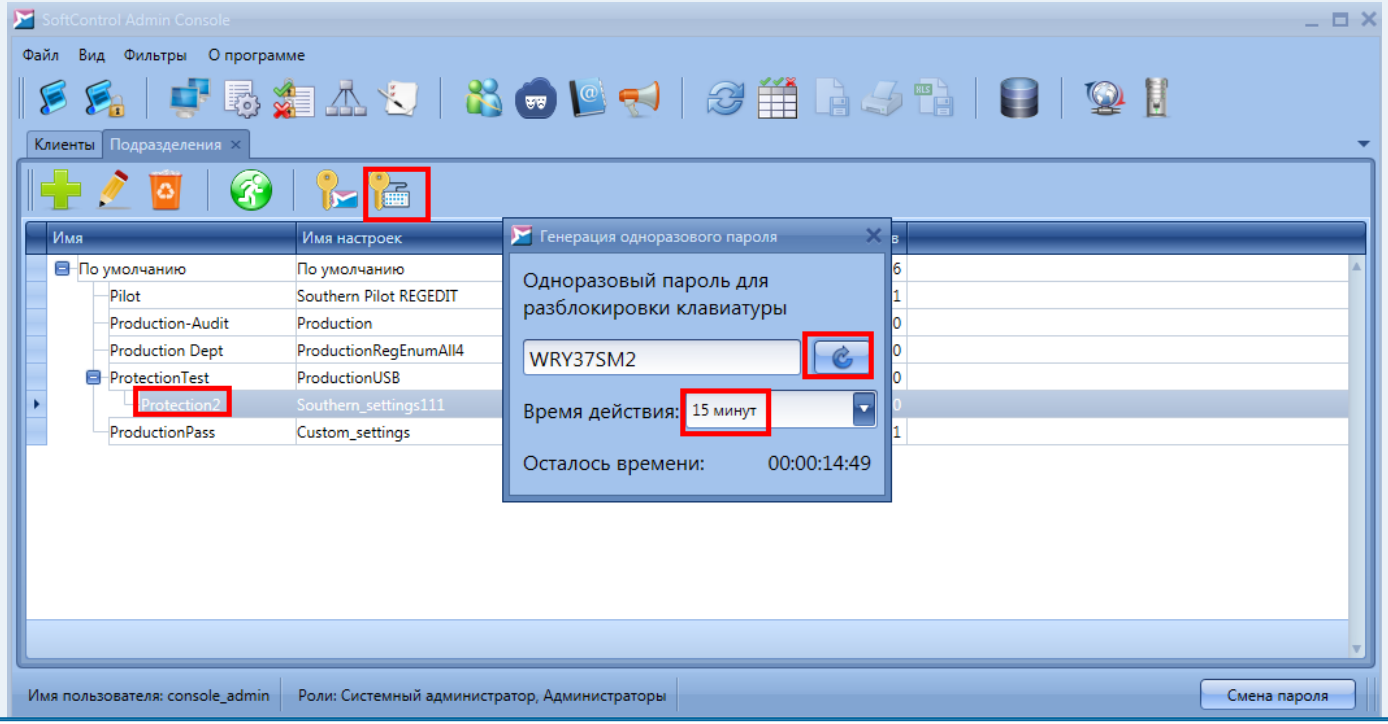
* Для включения одноразовых паролей необходимо изменить клиентские настройки, сохранить их под новым именем и применить к подразделению, в котором находится тестируемое устройство:



Чтобы создать одноразовый парол для доступа к графическому интерфейсу клиентского модуля SoftControl SysWatch, выполните следующие действия:

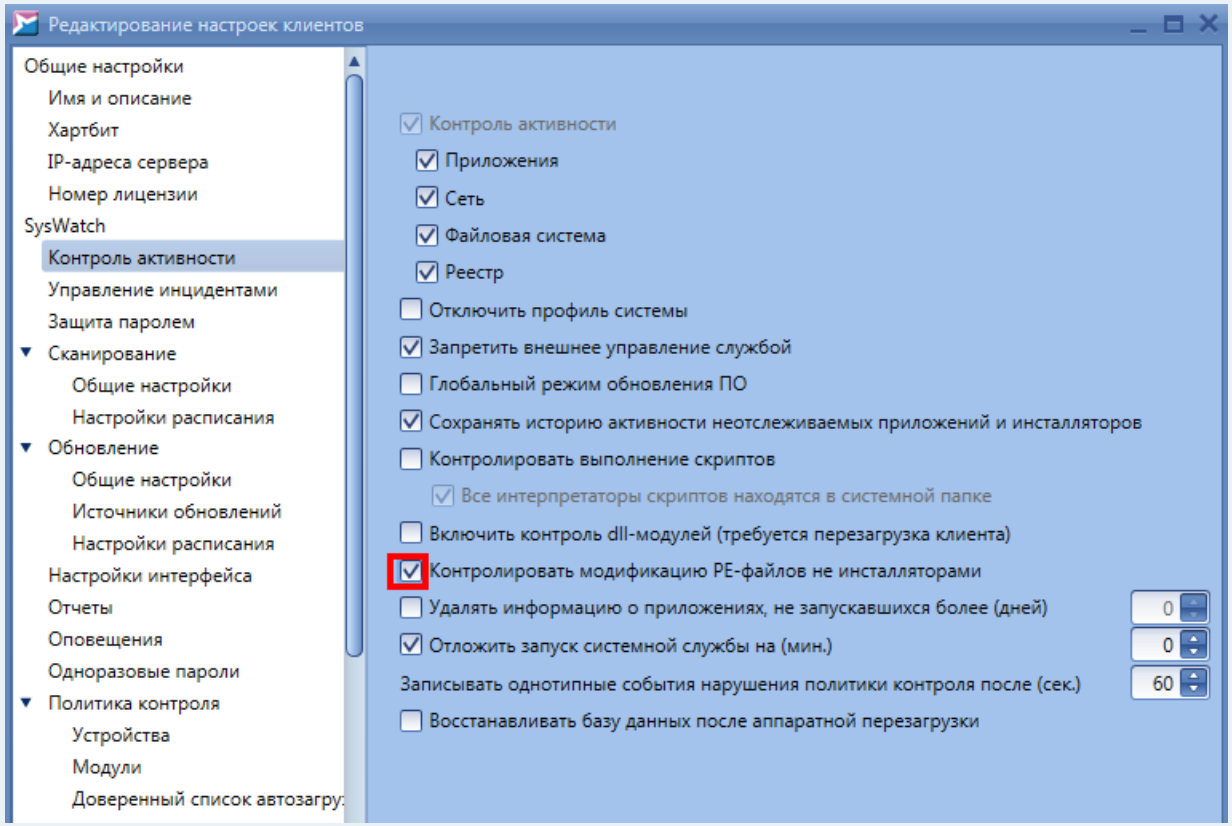


Чтобы создать одноразовый пароль для блокировки клавиатуры клиентского устройства, выполните следующие действия:



10.2.7.2	Проверена работа одноразовых паролей*.	❑ Клавиатура клиентского устройства без ввода пароля не реагирует на нажатия клавиш, доступ к GUI клиентского модуля SoftControl SysWatch возможен при вводе одноразового пароля.	Администратор ИБ выдает инженеру, работающему локально на банкомате, созданные пароли (с актуальным временем действия) на разблокировку клавиатуры и доступ к GUI клиентского модуля SoftControl SysWatch. Инженер с помощью этих паролей производит разблокировку клавиатуры, а затем получает доступ к GUI клиентского модуля SoftControl SysWatch. Следует обратить внимание, что при генерации паролей на разблокировку клавиатуры все буквы ПРОПИСНЫЕ; при вводе пароля на клавиатуре надо вводить строчные буквы.
10.2.8	Проверка правил политик контроля для функции запрета модификации PE-файлов		
10.2.8.1	Установлен запрет на модификацию PE-файлов всем, кроме доверенных инсталляторов.*	❑ Установлен запрет на модификацию PE-файлов.	

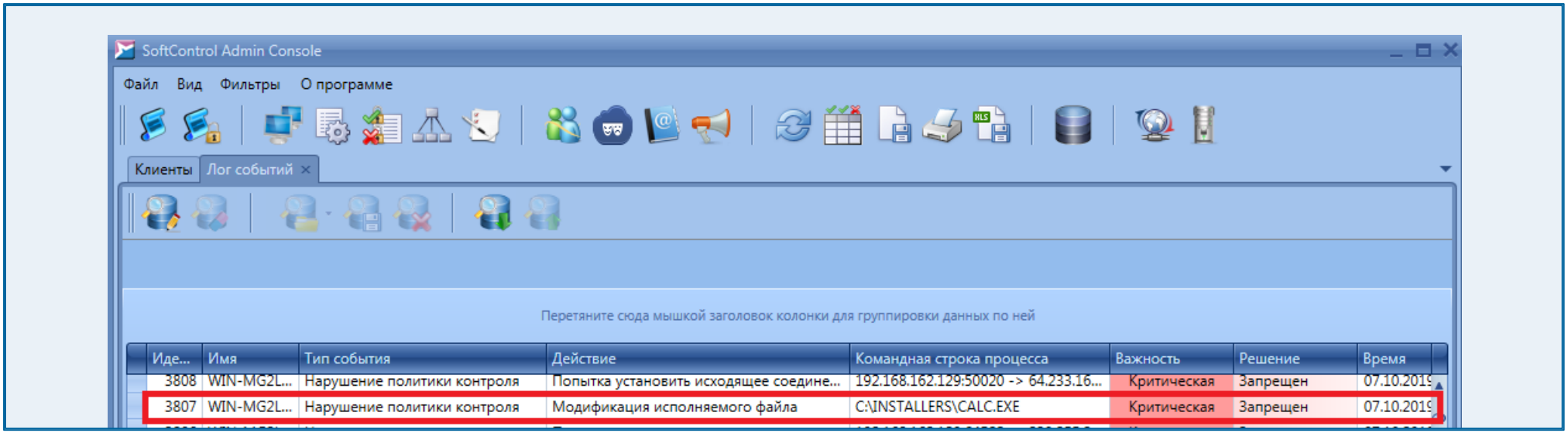
* Для запрета модификации исполняемых файлов необходимо изменить клиентские настройки:



После создания правил необходимо сохранить настройки под новым именем и применить их к подразделению, в котором находится тестируемое устройство.

10.2.8.2	Проведена попытка с помощью блокнота Windows (*notepad.exe*) изменить исполняемый файл Калькулятора (*calc.exe*).*	❑ При попытке изменения исполняемого файла выводится сообщение о невозможности внести изменения в PE-файл.	Файл *calc.exe* предварительно скопирован в папку *C:\installers*.

* На сервере управления в SoftControl Admin Console наблюдается событие **Нарушение политики контроля** - **Модификация исполняемого файла**:


SoftControl Admin Console
Файл Вид Фильтры О программе
Клиенты
Лог событий
Перетяните сюда мышкой заголовок колонки для группировки данных по ней
Иде... Имя Тип события Действие Командная строка процесса Важность Решение Время
3808 WIN-MG2L... Нарушение политики контроля Попытка установить исходящее соедине... 192.168.162.129:50020 -> 64.233.16... Критическая Запрещен 07.10.2019
3807 WIN-MG2L... Нарушение политики контроля Модификация исполняемого файла C:\INSTALLERS\CALC.EXE Критическая Запрещен 07.10.2019

3. Техническая поддержка

При возникновении вопросов по установке, настройке и работе TPSecure 6.1.398 вы можете обращаться в техническую поддержку по электронной почте support@safensoft.com.

4. Дополнительная информация

4.1 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 11. Модули обновления

Обновляемый компонент	Имя модуля	Путь
SoftControl SysWatch	snsupd.exe	C:\PROGRAM FILES\SOFTCONTROL\SYSWATCH\
SoftControl SysCmd	upd.exe	C:\Program Files\SoftControl\SysCmd\Updater

Обновляемый компонент	Имя модуля	Путь
SoftControl DLP Client	upd.exe	C:\Program Files\SafenSoft\DLP Client\Updater

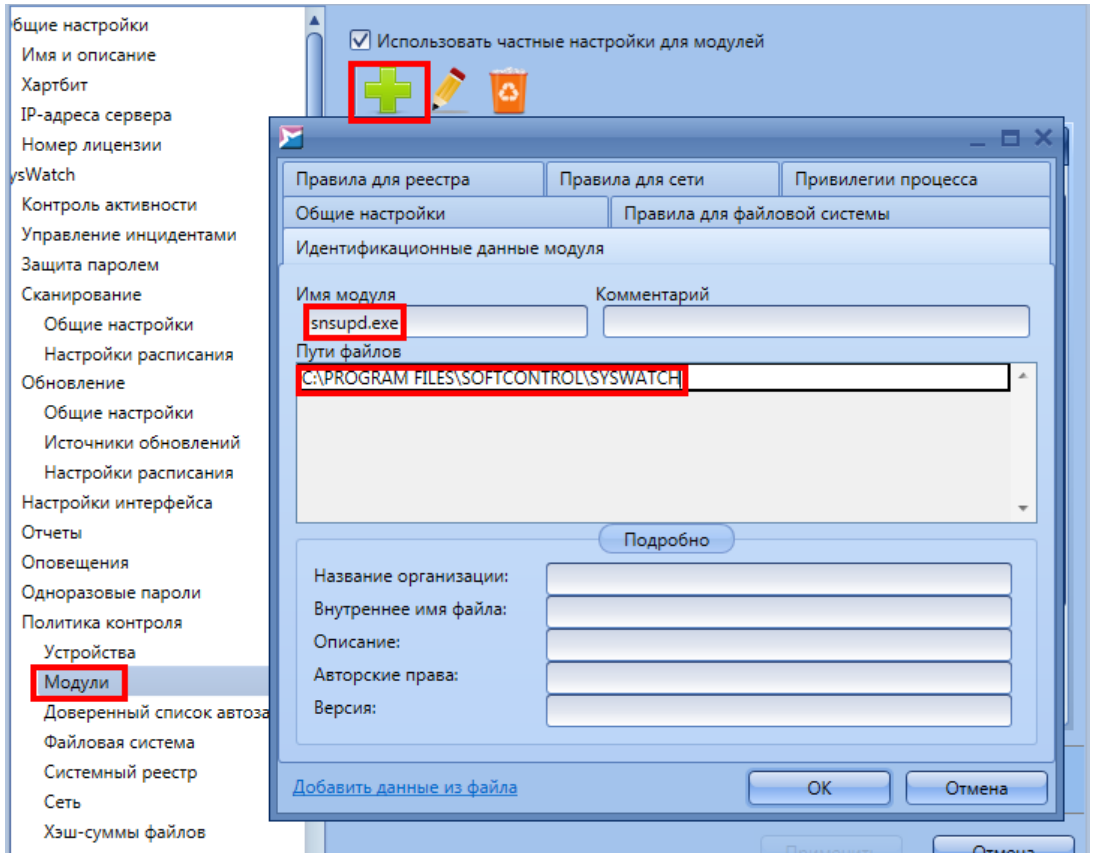


Рисунок 1. Настройка модуля обновления на примере SoftControl SysWatch

5. На вкладке **Общие настройки** выберите зону выполнения **Доверенные приложения** и отметьте флажком **Включить режим обновления ПО**.

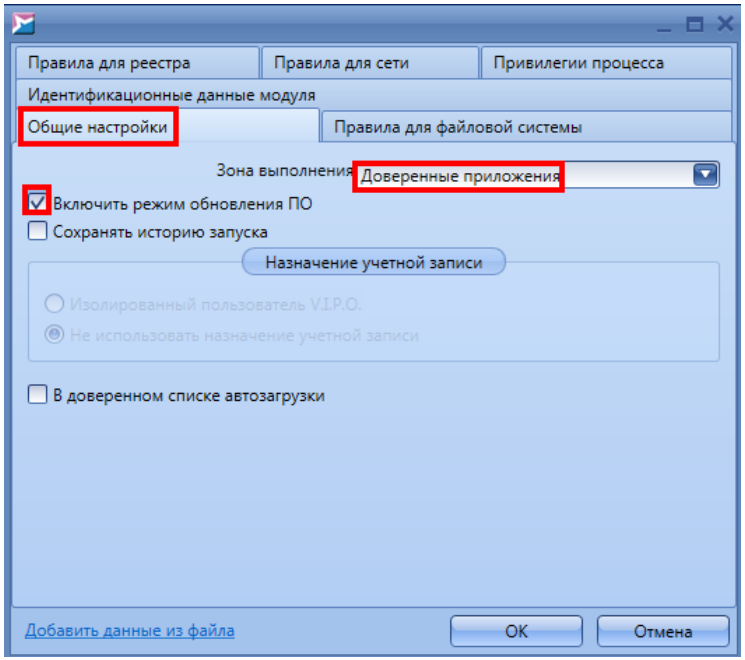


Рисунок 2. Добавление модуля в доверенные приложения

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.