ARUDIT SECURITY LLC.
Novovladykinskiy drive, 8 build 3,
127106, Moscow, Russia
Tel. +7(499) 201-5512
www.safensoft.com
e-mail: sns@safensoft.com

ООО «АРУДИТ СЕКЬЮРИТИ»
127106, Россия, Москва
Нововладыкинский проезд, д. 8, стр. 3
Тел: +7(499) 201-5512
www.safensoft.com
e-mail: sns@safensoft.com

Функциональные характеристики SoftControl 6.1

Table of Contents

Назначение

(«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;

Условные обозначения

Пример обозначения	Описание
	Важная информация.
Условие	Условие выполнения, примечание, пример.
Обновить	заголовки и сокращения; названия экранных кнопок, ссылок, пунктов меню, других элементов программного интерфейса.
Политика контроля	термины (определения); имена файлов и других объектов; тексты сообщений, выводимых пользователю.
C:\Program Files\SoftControl	Пути к файлам, каталогам, ключам системного реестра.
%windir%\system32\msiexec.exe /i	Фрагменты программного кода, командных и конфигурационных файлов.
<каталог установки SoftControl Service Center	Поля для замены функциональных названий фактическими значениями.

Приложение	Ссылки на внутренние ресурсы (разделы документа) или на внешние ресурсы (URL-адреса).

Сокращения

В данном документе употребляются без расшифровки следующие сокращения:
БД – база данных;
ГИП – графический интерфейс пользователя;
ЛВС – локальная вычислительная сеть;
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.

Глоссарий

Глоссарий

Термин	Пояснение
Проактивная защита	Комплекс мер по предотвращению вредоносных воздействий, основанный на превентивных технологиях.
Превентивные технологии	Передовые технологии защиты данных, в основе которых лежит анализ активности на компьютере пользователя: действий любых приложений, служб операционной системы, действий пользователя, активности извне и т.д. В отличие от реактивных технологий, на которых построены такие средства защиты, как антивирусы и персональные сетевые экраны, превентивные технологии анализируют не код объекта, а отслеживают потенциально опасные действия, выполняемые им. Следовательно, инструменты проактивной защиты не

	требуют наличия и постоянного обновления баз вредоносного кода, что является необходимым для традиционных средств защиты.
Реактивные (сигнатурные) технологии	Метод работы антивирусного программного обеспечения и систем обнаружения вторжений, при котором программа в процессе анализа объекта обращается к базе данных известных вирусов и проверяет соответствие какого-либо участка кода просматриваемого объекта известному коду (сигнатуре) вируса в базе данных.
Политика контроля	Целостный набор **правил контроля активности**.
Правило контроля активности	Набор условий, определяющих действие приложения и реакцию на него SoftControl SysWatch.
Профиль системы	База данных, хранящаяся локально на **клиентском хосте** и содержащая контрольные суммы **исполняемых модулей**. Профиль системы создаётся в результате автоматической настройки SoftControl SysWatch (операция сбора профиля).
Приложение в профиле	Приложение, контрольная сумма которого есть в **профиле системы**.
Отслеживаемое приложение	Приложение, факт запуска которого SoftControl SysWatch обнаружил на **клиентском хосте** в процессе работы с момента установки.
Доверенное приложение	**Отслеживаемое приложение** из **доверенной зоны выполнения**.
Ограниченное приложение	**Отслеживаемое приложение** из **ограниченной зоны выполнения**.
Запрещённое приложение	**Отслеживаемое приложение** из **запрещённой зоны выполнения**. SoftControl SysWatch запрещает запуск таких приложений на клиентском хосте.
Зона выполнения (доверенная, ограниченная, запрещённая)	Отдельная **политика контроля**, применяемая к подмножеству **отслеживаемых приложений**. Всего на каждом **клиентском хосте** имеется 3 зоны

	выполнения: доверенная, ограниченная, запрещённая. Любое **отслеживаемое приложение** принадлежит к одной из этих трёх 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 изменённых им PE-файлов. Дочерние процессы данного приложения наследуют режим обновления ПО.
V.I.P.O. (Valid Inside Permitted Operations)	Учётная 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 учётной записи V.I.P.O. можно устанавливать только для **ограниченных приложений**.
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

Требования к аппаратному и программному обеспечению

SoftControl Server (Linux Edition)

Операционная система

- ALT Linux 10.1
- RedOS Linux 7.3.2

СУБД

- PostgreSQL версии 12 и выше (Инструкция по установке на поддерживаемых дистрибутивах Linux в приложении)

Дополнительные требования

- Microsoft .NET 5 (инструкция по установке на поддерживаемых дистрибутивах Linux в приложении)

SoftControl Admin Console

Операционная система

1. Клиентские операционные системы *:
    - 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
2. Серверные операционные системы *:
    - 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

* На данный момент SoftControl Admin Console работает только на ОС Windows.

Дополнительные требования:

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

SoftControl ATM Client

Операционная система

1. Клиентские операционные системы *:
    - Microsoft® Windows® XP (SP2) 32-разрядная/64-разрядная
    - Microsoft® Windows® XP (SP3) 32-разрядная

- 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

2. Серверные операционные системы *:
   - Microsoft® Windows® Server 2003 (SP2) 32-разрядная/64-разрядная
   - Microsoft® Windows® Server 2003 R2 (SP2) 32-разрядная/64-разрядная
   - 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

* На данный момент SoftControl ATM Client работает только на ОС Windows.

SoftControl DLP Client

Операционная система

1. Клиентские операционные системы *:
   - Microsoft® Windows® XP (SP2) 64-разрядная
   - Microsoft® Windows® XP (SP3) 32-разрядная
   - 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
2. Серверные операционные системы *:
   - Microsoft® Windows® Server 2003 (SP2) 32-разрядная/64-разрядная
   - Microsoft® Windows® Server 2003 R2 (SP2) 32-разрядная/64-разрядная
   - 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

* На данный момент SoftControl DLP Client работает только на ОС Windows.

Централизованное управление СИБ

Удалённое централизованное управление клиентскими приложениями SoftControl SysWatch и SoftControl DLP Client 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.

Интерфейс SoftControl Admin Console

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

- Лог событий;
- События безопасности;
- Клиенты;
- Настройки клиентов;
- Профили безопасности;
- Подразделения;
- Задачи;
- Пользователи;
- Роли;
- Контакты;
- Управления нотификациями;
- Обновления;
- Снимки конфигурации;
- Сканнер;
- Измененные настройки.

В верхней части главного окна SoftControl Admin Console под основным меню программы расположен ряд графических кнопок, предназначенных для выполнения базовых операций при работе с SoftControl Admin Console. Кроме того, вкладки Клиенты, Подразделения, Настройки клиентов, Профили безопасности, Задачи, Контакты и Управления нотификациями имеют свои графические кнопки, область действия которых распространяется только на данные вкладки. Функции кнопок общего назначения описаны в табл.

Элементы управления SoftControl Admin Console общего назначения

Название кнопки	Описание	Горячие клавиши
Лог событий	Вызов вкладки **Лог** для всех клиентских компонентов.	
События безопасности	Вызов вкладки **События безопасности**.	
Клиенты	Вызов вкладки **Клиенты**.	F4
Настройки клиентов	Вызов вкладки **Настройки клиентов**.	

Профили безопасности	Вызов вкладки **Профили безопасности**.	
Подразделения	Вызов вкладки **Подразделения**.	
Задачи	Вызов вкладки **Задачи**.	
Пользователи	Вызов вкладки **Пользователи**.	
Роли	Вызов вкладки **Роли**.	
Контакты	Вызов вкладки **Контакты**.	
Управление нотификациями	Вызов вкладки **Нотификации**.	
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 **Лог**.	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 **Снимки конфигурации**	
Обновления	Вызов вкладки **Обновления**.	
Сервер	Вызов настроек соединения с сервером.	

Часть функций, вызываемых с помощью кнопок общего назначения, доступны также из главного меню программы.
В нижней части окна отображается строка с именем текущего пользователя и присущими ему ролями.

В главном окне SoftControl Admin Console дополнительно возможны следующие действия:
Настройка соединения с сервером
Настройка интерфейса

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, открываемому при запуске SoftControl Admin Console.

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:
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** задаётся максимальное количество событий, которое должно отображаться на одной странице вкладки Лог.

Просмотр информации о программе
В главном меню выберите пункт **О программе**.

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.
2) На вкладке **Роли** при необходимости создайте дополнительные роли и назначьте учётным записям пользователей роли с выбранными разрешениями. С помощью вкладки **События безопасности** производите учёт действий пользователей через консоль управления.
3) На вкладке **Клиенты** подтвердите или отклоните запросы на регистрацию от клиентских приложений, установленных на конечных точках ЛВС.
4) После формирования рабочей области из необходимых устройств перейдите на вкладку **Настройки клиентов** и создайте необходимые конфигурации, которые будут применяться для клиентских приложений.
5) После создания клиентских настроек перейдите на вкладку **Подразделения** и создайте подразделения (группы) по какому-либо принципу для распределения в них зарегистрированных компонентов на клиентских хостах. При создании подразделений выполните их привязку к определённым конфигурациям.
6) На вкладке **Клиенты** переместите клиентские компоненты в созданные подразделения.

7) На вкладке **Задачи** создайте необходимые задачи для клиентских приложений.
8) Перейдите на вкладку **Лог** и приступите к просмотру отчётов клиентских компонентов.
9) Дополнительно можно настроить оповещения об определённых событиях, которые будут отправляться на электронные почтовые ящики заданных адресатов, а также экспортировать и вывести на печать необходимые данные.

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 к различным функциям Сервисного Центра в зависимости от делегированной им роли.
Через SoftControl Admin Console осуществляется контроль действий пользователей с помощью регистрации событий безопасности сервера.

Роли

Вкладка **Роли** позволяет управлять ролями и настраивать разрешения для них.

Роли на вкладке представлены в виде таблиц, в первой строке которой указано имя роли, а в последующих – права на выполнение определённых 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**. В появившемся окне укажите **Имя роли** и нажмите на кнопку **OK**.
Новая роль будет добавлена в конец списка ролей. Далее задайте разрешения

для неё.

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 **OK**.

Чтобы удалить разрешение, нажмите на ссылку **Удалить разрешение** в соответствующей строке таблицы с ролью.

Пользователи

На вкладке **Пользователи** производится управление учётными записями пользователей и назначение ролей для них.

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

Элементы управления вкладки "Пользователи"

Название кнопки	Описание
Добавить	Создание новой учётной записи.
Редактировать	Редактирование свойств выбранной учётной записи.
Удалить	Удаление выбранных учётных записей.
Переместить	Переместить выбранного пользователя в другое подразделение.

Перечень полей вкладки приведён в табл. 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 учётной записи

Чтобы добавить новую учётную запись, нажмите на кнопку **Добавить**. В появившемся окне укажите **Имя** пользователя, введите **Пароль** учётной записи и его **Подтверждение** (не менее 7 символов). Укажите необходимые **Роли** для

создаваемого пользователя и нажмите на кнопку **Применить**.

Все новые учётные записи автоматически помещаются в подразделение **По умолчанию**. Вы можете переместить выбранную учётную запись в другое подразделение.
В зависимости от роли, 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 учётную запись временной, выставив галочку **Временный пользователь** и указав дату блокировки.

Редактирование учётной записи
Чтобы изменить свойства учётной записи, нажмите на кнопку **Редактировать**. В появившемся окне измените **Имя** пользователя и/или измените **Роли** в соответствующей области, после чего нажмите на кнопку **Применить**. Пароль при этом останется без изменений. Если требуется сменить пароль, то введите новый **Пароль** в одноименном поле и его **Подтверждение** (не менее 7 символов).

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. Кнопка доступна на любой открытой вкладке.

В появившемся окне необходимо ввести старый **Пароль**, **Новый пароль** и его **Подтверждение** (не менее 8 символов) и нажать на кнопку **Применить**.
При смене пароля администратор может ограничить срок его действия. Для этого в файле конфигурации сервера (C:\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 задаётся с помощью параметра *MinPasswordPeriodDays* и не может быть больше значения, установленного для параметра *PasswordValidDays*. Кроме того, можно выставить запрет на использование определённого числа старых паролей (от 1 до 10; параметр *ForbidOldPasswordCount*).
Если учётную запись необходимо заблокировать, выставите галочку **Аккаунт заблокирован**.

Удаление учётной записи
Для удаления учётной записи выберите её, нажмите на кнопку **Удалить** и подтвердите удаление в диалоговом окне.
Примечание. После удаления учётной записи создать новую учётную запись с

таким же именем можно не ранее, чем через 3 года.

Перемещение учётной записи

Для перемещения учётной записи выберите её, нажмите на кнопку **Переместить** и в появившемся окне укажите подразделение, в которое надо переместить данного пользователя.

События безопасности сервера

Консоль управления позволяет фиксировать операции, производимые пользователями, для дальнейшего анализа на вкладке **События безопасности**. Полный перечень полей вкладки приведён в табл.

Поля вкладки «События безопасности»

Поле	Описание
Guid клиента	Уникальный идентификатор клиентского приложения (только для типов событий **Подтверждение клиента**, **Отклонение клиента**, **Удаление клиента**, **Перемещение клиента в другое подразделение**).
Тип события	Тип зарегистрированного события: **Начало сессии**; **Конец сессии**; **Роль создана**; **Роль удалена**; **К роли добавлены разрешения**; **Удалено разрешение у роли**; **Была создана учетная запись**; **Учетная запись была изменена**; **Учетная запись была удалена**; **Подтверждение клиента**; **Отклонение клиента**; **Удаление клиента**; **Запрос на изменение сертификата клиента**; **Новый сертификат назначен клиенту**; **Перемещение объекта в другое подразделение**; **Создано новое подразделение**; **Подразделение было удалено**; **Создание новых настроек**; **Изменение настроек для подразделения**; **Применение частных настроек**; **Удалены настройки**;

	Назначены настройки подразделения; **Создание задачи**; **Отмена задачи**; **Создан контакт**; **Контакт изменен**; **Контакт был удален**; **Была создана нотификация**; **Нотификация была изменена**; **Нотификация была удалена**; **Неавторизованный запрос**; **Недостаточно прав на выполнение запроса**; **Ошибка обработки запроса**.
Тип задачи	Тип задачи (только для типов событий **Создание задачи**, **Отмена задачи**).
Сообщение об ошибке	Сообщение об ошибке во время обработки запроса.
Причина ошибки авторизации	Причина невозможности авторизации на сервере (только для типа события **Неавторизованный запрос**).
ID задачи	Порядковый номер задачи (только для типов событий **Создание задачи**, **Отмена задачи**).
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 перемещён установленный клиентский компонент (только для типов событий **Перемещение клиента в другое подразделение**, **Создано новое подразделение**, **Подразделение было удалено**).
Разрешения роли	Перечисление добавленных (для типа события **К роли добавлены разрешения**) или удаленных (для типа события **Удалено разрешение у роли**) разрешений роли.
ID сессии	Контрольная сумма идентификатора сессии, с которой ассоциировано событие.
Имя аккаунта	Имя учётной записи пользователя (только для типов событий **Была создана учетная запись**, **Учетная запись была изменена**, **Учетная запись была удалена**).
Имя роли	Имя роли (только для типов событий **Роль создана**, **Роль удалена**, **К роли добавлены разрешения**, **Удалено разрешение у роли**).

Имя пользователя	Имя пользователя, с которым ассоциировано данное событие.
Имя нотификации	Имя оповещения (только для типов событий **Была создана нотификация**, **Нотификация была изменена**, **Нотификация была удалена**).
Имя настроек	Имя конфигурации клиентских приложений (только для типов событий **Создание новых настроек**, **Изменение настроек для подразделения**, **Удалены настройки**).
Имя контакта	Имя адресата получателя оповещений (только для типов событий **Создан контакт**, **Контакт был изменен**, **Контакт был удален**).
Время возникновения	Дата и время возникновения события.
Время создания настроек	Время создания настроек клиентских приложений на сервере (только для типа события **Создание новых настроек**).
Имя клиента	Имя клиентского хоста (только для типов событий **Подтверждение клиента**, **Отклонение клиента**, **Удаление клиента**, **Запрос на изменение сертификата клиента**, **Новый сертификат назначен клиенту**, **Перемещение клиента в другое подразделение**).
IP адрес запроса	IP-адрес компьютера с установленной консолью управления SoftControl Admin Console, от которой пришел запрос на сервер.

Дополнительные действия, возможные на данной вкладке:

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** в необходимое место заголовка таблицы. Для удаления существующего поля перетащите его в окно **Выбор колонок**, либо за пределы заголовка таблицы.

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. Если группировка производится по нескольким категориям, то приоритет (вложенность категорий) уменьшается слева направо в зависимости от расположения на панели.

Клиенты

Вкладка **Клиенты** служит для управления регистрацией клиентских приложений, перемещением их в подразделения, отслеживания статуса и получения информации о хостах, на которых они установлены.
Основные операции с клиентскими компонентами осуществляются с помощью графических кнопок вкладки, предназначение которых приведено в табл. 9.

Таблица 9. Элементы управления вкладки "Клиенты"

Название кнопки	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 **Лог** для выбранных компонентов.	

Полный перечень полей вкладки приведён в табл.

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: **SysWatch** – компонент проактивной защиты (SoftControl ATM Client / Endpoint Client / SClient);

	DLP – компонент сбора данных (SoftControl DLP Client).
Тип настроек	Тип конфигурации клиентского компонента: **Настройки подразделения** – настройки, общие для подразделения, которому принадлежит клиентский компонент; **Частные настройки** – настройки, индивидуальные для клиентского компонента, независимо от подразделения; **Локальные настройки** – настройки, изменённые локально для клиентского компонента типа SysWatch.
Версия продукта	Версия установленного клиентского компонента. Если версия компонента ниже версии SoftControl Admin Console, данная ячейка подсвечивается красным цветом, если выше – оранжевым.
Статус	Возможные статусы, отражающие текущее состояние клиентского компонента: **Ожидает решения**: от клиентского приложения получен запрос на регистрацию, ожидается решение администратора. **Одобрен**: запрос на регистрацию от клиентского приложения одобрен администратором. **Отклонен**: запрос на регистрацию от клиентского приложения отклонен администратором. **Активен**: за последний отрезок времени, равный удвоенному значению интервала обращения клиента к серверу, зафиксирован факт установки связи зарегистрированного клиентского приложения с сервером. **Остановлен**: за последний отрезок времени, равный удвоенному значению интервала обращения клиента к серверу, не зафиксирован факт установки связи зарегистрированного клиентского приложения с сервером.
Информация	Дополнительная информация по состоянию клиентского компонента. Для компонента типа **SysWatch** имеет следующие показатели: **Защита** – статус проактивной защиты. **Включено**: защита включена по всем областям контроля; **Отключено**: защита отключена по всем областям контроля;

	Частично: защита включена по части областей контроля. • **Сканирование** – статус последней по времени задачи антивирусного сканирования. • **Профиль** – статус последней по времени задачи сбора профиля (автоматической настройки). **Выполняется**: задача находится в процессе выполнения; **Остановлено**: задача остановлена пользователем; **Завершено**: задача успешно завершена; **Ошибка**: возникла ошибка в процессе запуска или завершения задачи. • **Обновление** – статус последнего по времени обновления компонента. **Установлено**: обновление было успешно установлено; **Не найдено**: обновления для компонента не найдены; **Перезагрузить**: необходима перезагрузка клиентского хоста для завершения обновления. Статус **Нет информации** для операций **Сканирование**, **Профиль** и **Обновление** означает, что указанные действия не производились с момента регистрации клиентского приложения на сервере. Для компонента типа **DLP** имеет следующие показатели: • **Наблюдение** – статус активности наблюдения. **Включено**: наблюдение включено по всем областям сбора данных (не включает в себя подкатегорию съёмных носителей); **Отключено**: наблюдение отключено по всем областям сбора данных; **Частично**: наблюдение включено по части областей сбора данных.
Изменён	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: • **применены успешно**; • **ожидание ответа**; • **ошибка применения**; • **локальные настройки**; • **нет информации**.
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 **Держать постоянное соединение с Сервисным Центром** (см. раздел Общие настройки): • **Активен**: постоянное соединение с SoftControl Service Center включено; • **Остановлен**: постоянное соединение с SoftControl Service Center отключено.
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 Настройки SoftControl SysWatch).

Основные действия, выполняемые на данной вкладке:

- управление процессом регистрации;
- перемещение в подразделения;
- управление списком файлов, разрешённых к запуску.

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: зажмите клавишу **Ctrl** на клавиатуре и выделите требуемые компоненты;

- выберите первый компонент диапазона, зажмите клавишу **Shift** на клавиатуре и выберите последний компонент диапазона.

Группировка данных

Информация на вкладке может группироваться по определённым 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. 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 со списком событий выделите требуемые компоненты и выполните одно из следующих действий:

- нажмите на кнопку **Лог событий** в группе кнопок вкладки;
- вызовите контекстное меню нажатием правой кнопки мыши на списке компонентов и выберите команду **Показать события**.

При открытии списка событий в заголовке вкладки Лог отображается количество выбранных компонентов.

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**.

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

При следующем получении запроса от клиентского компонента происходит проверка его сертификата: 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 введённым 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**.

Поле **Статус** после отклонения регистрации выбранных клиентов изменяет своё 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.

Обновление клиентского сертификата

Выберите в списке требуемые клиентские компоненты, находящиеся в состоянии **Активен** или **Остановлен**, и нажмите на кнопку **Сертификат**.

Поле **Срок действия сертификата** обновляется после следующего обращения клиентского компонента с новым индивидуальным сертификатом. При этом использование предыдущего сертификата становится невозможным в связи с его помещением в чёрный список.

Удаление клиентского компонента из БД

Выберите в списке требуемые клиентские компоненты и нажмите на кнопку **Удалить**. При этом не происходит отзыва клиентского сертификата и через интервал обращения клиента к серверу в консоли управления SoftControl Admin Console вновь отобразятся удалённые компоненты в статусе **Ожидает решения**. Для полного вывода клиентских компонентов из эксплуатации необходима следующая последовательность действий:

1) Поместите индивидуальный сертификат клиентского компонента в чёрный список с помощью кнопки **Отклонить**.
2) Удалите клиентские компоненты из БД с помощью кнопки **Удалить**.

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.

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

Управление списком разрешённых файлов

SoftControl Admin Console позволяет получить список файлов, разрешённых к

запуску на компьютере с установленным клиентским приложением SoftControl SysWatch, и при необходимости отозвать разрешения для выбранных файлов.
Для получения списка файлов щёлкните 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>**. 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**).

Для просмотра списка файлов за определённый 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**.

Подразделения

Вкладка **Подразделения** предназначена для группирования клиентских компонентов по территориальному, административному или иному признаку. Кроме того, на вкладке производится привязка подразделений к определённым наборам настроек и генерация одноразовых паролей.

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

Элементы управления вкладки "Подразделения"

Название	Описание
Добавить	Создание нового подразделения.

Редактировать	Редактирование свойств выбранного подразделения.
Удалить	Удаление выбранных подразделений.
Переместить	Переместить выбранное подразделение в другое. Нельзя перемещать подразделение **По умолчанию**, а также родительское подразделение в дочернее.
Одноразовый пароль для SysWatch	Открытие окна генератора одноразовых паролей.
Одноразовый пароль для разблокировки клавиатуры	Открытие окна генератора паролей для разблокировки клавиатуры на клиентском хосте.

Перечень полей вкладки приведён в табл.

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;
- генерация одноразовых паролей.

Управление подразделениями

Управление подразделениями включает в себя следующие действия:

Создание подразделения

Чтобы добавить новое подразделение, нажмите на кнопку **Создать**. В появившемся окне укажите **Имя** подразделения и выберите **Имя настроек** в выпадающем списке, после чего нажмите на кнопку **Применить**.

Изменение свойств подразделения

Чтобы изменить свойства подразделения, нажмите на кнопку **Правка**.

В появившемся окне измените **Имя** подразделения и/или выберите другое **Имя настроек** в выпадающем списке, после чего нажмите на кнопку **Применить**. Если данное подразделение содержит компоненты, их перечень отображается в списке **Клиенты**.

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 определённого 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.

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. 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 счётчике **Осталось времени** в формате *дд:чч:мм:сс*. По истечении интервала времени жизни нажмите на кнопку ещё раз, чтобы сгенерировать новый пароль.

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. При запросе пароля в ГИП SoftControl SysWatch необходимо установить флажок **Использовать одноразовый пароль**.

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.

Настройка клиентских приложений

Вкладка **Настройки клиентов** содержит список конфигураций (наборов настроек) клиентских приложений.
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 определённого клиентского компонента конфигурацию, отличную от конфигурации подразделения. На вкладке отображается список всех конфигураций, включая частные. Информация по работе с частными настройками приведена ниже.
Основные операции с конфигурациями осуществляются с помощью графических кнопок вкладки, предназначение которых приведено в табл

Элементы управления вкладки "Настройки клиентов"

Название кнопки	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 приведён в табл.

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;
- настройки SoftControl SysWatch;

- настройки SoftControl DLP Client.

Основные действия, выполняемые с клиентскими конфигурациями:

Создание конфигурации подразделения

Чтобы добавить новую конфигурацию подразделения, нажмите на кнопку **Добавить**. В окне **Редактирование настроек клиентов** задайте параметры конфигурации (см. рисунки, начиная с Раздел "Имя и описание" и до Настройки расписания обновления). 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 её и выполните одно из следующих действий:

- нажмите на кнопку **Редактировать** в группе кнопок вкладки;
- 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" и до Настройки расписания обновления). 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, 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 её клиентскому компоненту, перейдите на вкладку Клиенты, 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.
В окне **Редактирование настроек клиентов** задайте параметры конфигурации. 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 её или ранее созданную конфигурацию, после чего нажмите на кнопку **OK** для применения конфигурации к клиентскому компоненту.

Удаление конфигурации

Для удаления конфигурации выберите её, нажмите на кнопку **Удалить** и подтвердите удаление в диалоговом окне.

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 определённого набора настроек, описание конфигурации – для его краткой характеристики.
Чтобы задать **Имя и описание**, в одноимённом разделе категории **Общие настройки** введите **Имя** и **Описание** в соответствующих полях.

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).
Для изменения параметра перейдите в раздел **Хартбит** категории **Общие настройки** и установите значение в поле **Период хартбита (сек.)**.
Выставите 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.

Выставите галочку **Скрыть службу Windows**, если системные службы SoftControl SysWatch (*safensec.exe*) и SoftControl DLP Client (*eventsvc.exe*) не должны показываться в оснастке **Службы** ОС Windows.
Примечание: скрытие системных служб не работает на ОС Windows XP.
Примечание: если системные службы скрыты, то управление ими средствами ОС становится невозможным.

IP-адреса сервера
Задание адресов сервера для подключения со стороны клиентских приложений производится мастером настройки сервера.
Для изменения списка адресов перейдите в раздел **IP адреса сервера** категории **Общие настройки**. 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**

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**), введите ключ в текстовое поле и нажмите на кнопку **Проверить** для проверки лицензии и отображения её параметров в случае корректного ключа.

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:

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

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, всё 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.

Запретить 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 определённых процессов рекомендуется создавать соответствующие Правила политики контроля.

Включить контроль dll-модулей (требуется перезагрузка клиента):

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

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

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

исполняемого кода).

Запретить всем модификацию PE-файлов (кроме инсталляторов):
Запретить изменения исполняемых файлов (exe, dll и т.п.) всеми приложениями, кроме работающих в режиме обновления ПО.

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 отчёт (по умолчанию 60 секунд). События нарушения политики контроля считаются *однотипными* и не вносятся в отчёт, 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 отчёта на клиентском хосте с SoftControl SysWatch добавляется информация о том, сколько однотипных событий было пропущено.

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**

Инцидент	Действие
Запуск приложения не в профиле	• **Выполнить в ограниченном режиме** Выполнение приложения в изолированной среде (песочнице) под учетной записью пользователя «V.I.P.O.» с ограниченными привилегиями. При этом добавления

	в профиль системы не происходит, а приложение помещается в ограниченную зону. Приложение может загружать дочерние модули, которые также не войдут в профиль системы. Даже если такое приложение является вредоносным и выполнит установку каких-либо дополнительных компонентов, то их последующая загрузка будет предотвращена. • **Выполнить в ограниченном режиме после проверки** Запуск приложения в ограниченном режиме, если при антивирусном сканировании приложения не найдено вредоносного кода. В обратном случае запуск будет забло- кирован. • **Выполнить в режиме обновления ПО** Выполнение приложения под текущей учетной записью без ограничений. При этом приложение и все его дочерние модули помещаются в профиль системы и доверен- ную зону. • **Выполнить в режиме обновления ПО после проверки** Запуск приложения в режиме обновления ПО, если при антивирусном сканировании • **Запуск приложе- ния не в профиле** приложения не найдено вредоносного кода. В обратном случае запуск будет забло- кирован. • **Заблокировать** Блокировка запуска приложения.

Запуск неподписанного инсталлятора	• **Установить** Выполнение инсталлятора под текущей учетной записью без ограничений. При этом после установки приложение и все его дочерние модули помещаются в профиль си- стемы и доверенную зону. • **Установить после проверки** Запуск инсталлятора в режиме обновления ПО, если при антивирусном сканирова- нии установщика не найдено вредоносного кода. В обратном случае запуск будет заблокирован. • **Установить в ограниченном режиме** Выполнение инсталлятора в изолированной среде (песочнице) под учетной записью пользователя «V.I.P.O.» с ограниченными привилегиями. При этом добавления в профиль системы не происходит. • **Установить в ограниченном режиме после проверки** Запуск инсталлятора в ограниченном режиме, если при антивирусном сканировании установщика не найдено вредоносного кода. В обратном случае запуск будет за- блокирован. • **Заблокировать** Блокировка запуска инсталлятора.
Нарушение политики контроля	• **Разрешить** Разрешение приложению выполнить действие, совпадающее с условиями правила заданной политики контроля. • **Разрешить после проверки**

	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. • **Запретить** Запрет приложению выполнить действие, совпадающее с условиями правила за- данной политики контроля. • **Запретить и завершить приложение** Запрет приложению выполнить действие, совпадающее с условиями правила за- данной политики контроля, и последующее завершение приложения.
Запуск интерпретатора скриптов	• **Разрешить** Разрешение запуска без ограничений. • **Запретить** Запрет запуска.
Загрузка недоверенной DLL	• **Разрешить** Разрешение загрузки DLL-библиотеки без ограничений. • **Запретить** Запрет загрузки.
Модификация PE-файла не инсталлятором	• **Разрешить** Разрешение модификации PE-файла. • **Запретить** Запрет модификации.

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**.

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.

Выставите флажок **Запретить локальное управление настройками**, если необходимо запретить редактирование настроек SoftControl SysWatch с клиентского хоста. Состояние данной опции будет также отображаться на вкладке Клиенты.

Настройки сканирования

В разделе **Сканирование Общие настройки** категории **SysWatch** настройте опции антивирусной проверки.

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 удаётся.

Выбор действия по окончанию 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 учётные данные, если требуется указать учётную 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.

В счётчике **Частота дней** укажите периодичность, с которой будет выполняться задача, а в поле **Время запуска** – время начала выполнения задачи в формате *чч:мм:сс*.

Настройки обновления

В разделе **Обновление Общие настройки** категории **SysWatch** настройте опции 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 Safe'N'Sec Corporation, доступный посредством сети Интернет.

В области **Источник обновлений** указываются адреса, с которых производится обновление ядра проактивной защиты и баз антивирусных компонентов.

В разделе **Обновление** **Настройки расписания** категории **SysWatch** можно установить расписание обновления, для этого установите флажок **Задать расписание** и настройте параметры. В счётчике **Частота дней** укажите периодичность, с которой будет выполняться задача, а в поле **Время запуска** – время начала выполнения задачи в формате *чч:мм:сс*.

Настройки интерфейса

В разделе **Настройки интерфейса** категории **SysWatch** выберите необходимые опции интерфейса SoftControl SysWatch на клиентских хостах:

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 отчёты и регистрации событий в WMI.
В области **Отчеты** установите флажок **Формировать отчеты**, чтобы включить функцию ведения текстовых отчётов, и выберите виды событий для протоколирования:

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

Выставите галочку **Службы и неподозрительные приложения**, чтобы включить запись событий запуска/остановки служб. Службы, которые были запущены до системной службы *safensec.exe*, будут помечаться в отчётах как *была запущена ранее*.
В счётчике **Формировать отчеты (в днях)** установите количество дней, за которые сохраняется история событий.
В области **Ротация отчётов** при необходимости установите флажок **Включить ротацию** и укажите параметры ротации (один или несколько), ограничивающие количественные характеристики текстовых отчётов:
Ограничение по времени:
введите в данном поле временной лимит одного файла отчёта и выберите

единицы величины в выпадающем списке (секунды, минуты, часы, дни).

Ограничение по размеру:

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

Количество хранимых логов:

введите в данном поле максимальное число хранимых частей файлов отчётов.

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.

Оповещения

В разделе **Оповещения** категории **SysWatch** установите флажок **Показывать оповещения** для отображения локальных оповещений SoftControl SysWatch на клиентских хостах и выберите необходимые типы сообщений:

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

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.

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 введённые пользователем последовательности символов, и как только dswdjwjjраспознает 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.

Политика контроля: Устройства

В разделе Политика контроля Устройства категории SysWatch настройте правила использования следующих внешних устройств и портов системы на клиентских хостах:

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

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). 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 ИД 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 и добавьте пользователей с

помощью кнопки Добавить. Чтобы изменения вступили в силу, нажмите на кнопку Применить.

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).

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. По умолчанию данная возможность отключена; для включения выставите флажок Использовать частные настройки для модулей.

По умолчанию окно содержит ряд модулей ОС Windows. Чтобы добавить в список новый модуль, нажмите на кнопку (Добавить). Появившееся окно содержит ряд вкладок для добавления информации о модуле и задания правил для него.

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 приведён синтаксис масок:

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

В области Подробно можно указать следующую дополнительную информацию по модулю (поля могут быть пустыми):

- Название организации;
- Внутреннее имя файла;
- Описание;
- Авторские права;
- Версия.

Также вы можете выбрать модуль, щёлкнув по ссылке Добавить данные из

файла 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.

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.

Выставите 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 учётной записью запускать данное приложение (только для Ограниченных приложений):

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

Выставите галочку В доверенном списке автозагрузки, если необходимо разрешить автоматический запуск данного модуля на клиентских хостах. Перечень модулей в данной категории можно посмотреть в разделе Политика контроля Доверенный список автозагрузки (см. ниже).

На вкладке Правила для файловой системы задаются правила для доступа приложения к объектам файловой системе (аналогично настройкам в разделе Политика контроля: Файловая система).
На вкладке Правила для реестра задаются правила для доступа приложения к объектам системного реестра (аналогично настройкам в разделе Политика контроля: Системный реестр).
На вкладке Правила для сети задаются правила контроля сетевой активности для приложения (аналогично настройкам в разделе Политика контроля: Сеть).
На вкладке Привилегии процесса задаются ограничения на использование процессом привилегий Windows на клиентских хостах (аналогично

настройкам в разделе Политика контроля: Привилегии процессов).

Чтобы изменить данные модуля, нажмите на кнопку (Изменить) или дважды щёлкните 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

В разделе Политика контроля - Доверенный список автозагрузки категории SysWatch отображается список модулей, автоматический запуск которых разрешён на клиентских хостах. Добавить модули в список можно в разделе Политика контроля - Модули (см. выше).

Политика контроля: Файловая система

В разделе Политика контроля Файловая система категории SysWatch определите правила доступа приложений к объектам файловой системы на клиентских хостах:

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

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 определённых типов (расширений) файлов.
Ниже приведён 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.
Вы можете указывать как папки на локальном жёстком 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.

Выберите профиль безопасности для правила 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;
- Запрос – выводить запрос при совпадении действия над объектом с

условием правила.
Чтобы включить созданное правило в список и сделать его действующим, установите флажок Активно и нажмите на кнопку OK.
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 и добавьте пользователей с помощью кнопки Добавить. Чтобы изменения вступили в силу, нажмите на кнопку Применить.
Чтобы удалить правило, нажмите на кнопку (Удалить).
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:

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

Выберите профиль безопасности для правила 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;

• Запрос – выводить запрос при совпадении действия над объектом с условием правила.

Чтобы включить созданное правило в список и сделать его действующим, установите флажок Активно и нажмите на кнопку OK.
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 и добавьте пользователей с помощью кнопки Добавить. Чтобы изменения вступили в силу, нажмите на кнопку Применить.
Чтобы удалить правило, нажмите на кнопку (Удалить).

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:

- Приём 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.

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:

Название – наименование правила.

Направление – направление сетевой активности, определяющее инициатора соединения:

- **Входящее** – сетевое соединение, инициируемое удалённым хостом;
- **Исходящее** – сетевое соединение, инициируемое 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 удалённом 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**.

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).

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

Выберите профиль безопасности для правила 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 и добавьте пользователей с помощью кнопки **Добавить**. Чтобы изменения вступили в силу, нажмите на кнопку **Применить**.

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 и Сравнение профилей.

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. Создать профили можно на вкладке 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, Политика контроля системного реестра, Политика контроля сетевой активности и Политика контроля модулей). Правила этого профиля не подлежат редактированию и удалению. Для просмотра информации по профилю дважды нажмите на него или нажмите на кнопку (Просмотр).

Чтобы загрузить профиль из базы данных, нажмите на кнопку (Загрузить). В появившемся окне выберите требуемый профиль.

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

Чтобы добавить правило определённой 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.
4. Нажмите на кнопку ОК.

Чтобы удалить из профиля правило определённой 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.

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; в противном случае нажмите на кнопку Нет – тогда все правила будут удалены.

Политика контроля: Привилегии процессов

В разделе **Политика контроля - Привилегии процессов** категории **SysWatch** настройте ограничения на использование процессами следующих привилегий

Windows на клиентских хостах:

- 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 удалённое 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.

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.

Чтобы задать время действия правила и пользователей (или группы пользователей), к которым оно применяется, нажмите на кнопку (**Дополнительно**). В появившемся окне укажите временные интервалы и добавьте пользователей с помощью кнопки **Добавить**. Чтобы изменения вступили в силу, нажмите на кнопку **Применить**.

Политика контроля: Взаимодействие процессов

В разделе Политика контроля Взаимодействие процессов категории SysWatch настройте разрешения для взаимодействия процессов:

• Доступ приложения к буферу обмена;

• Установка приложением глобальных перехватчиков;

• Доступ к процессу и его потокам извне.
Условие: правила распространяются на все приложения из ограниченной зоны выполнения, запущенные под учётной 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 и добавьте пользователей с помощью кнопки Добавить. Чтобы изменения вступили в силу, нажмите на кнопку Применить.

Политика контроля: Сертификаты

В разделе Политика контроля - Сертификаты категории SysWatch определите белый список сертификатов ЭЦП для дополнительного контроля активности процессов на клиентских хостах.
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.
Изначально SoftControl SysWatch содержит базовый список сертификатов доверенных производителей, в том числе три сертификата 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 OK. Установите флажок в столбце Доверять для добавленных сертификатов.
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.

Политика контроля: Запрещенные службы

В разделе Политика контроля Запрещенные службы категории SysWatch задаётся список служб, выполнение которых на клиентских хостах требуется заблокировать.
По умолчанию запрещены следующие службы: RemoteRegistry, TermService, SSDPSRV, RDSessMgr, Seclogon. 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.

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:

- Время работы с приложением;
- Использование USB-устройств;
- Печать документов;
- Пересылка документов по почте;
- Ввод текста с клавиатуры.

Наблюдение за файловой системой, системным реестром и сетевым трафиком активно при выставленной опции Собирать данные и заданном правиле (правилах) в соответствующих пунктах раздела Наблюдение.

Оптимизация

В разделе Оптимизация категории DLP задаются временные параметры регистрации событий.

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 включённой опции Время работы с приложением 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.

Чтобы добавить объект для наблюдения, нажмите на кнопку (Добавить) и введите полный путь до него в появившемся окне.

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

определённых типов (расширений) файлов. Ниже приведён 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 OK для добавления указанного объекта в список.
Вы можете указывать как папки на локальном жёстком 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 отчётах:

- Чтение;
- Создание;
- Удаление;
- Переименование;
- Изменение.

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 и выставленной галочке

в полях Удаление или Изменение. При установке опции Запись видео будет производиться сохранение снимков экрана клиентского хоста с заданными параметрами в момент возникновения наблюдаемого события.
В разделе Наблюдение HTTP категории DLP осуществляется задание наблюдаемых данных в сетевом трафике.
Чтобы добавить данные для наблюдения, нажмите на кнопку (Добавить) и введите строку в появившемся окне. 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.
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 в момент возникновения наблюдаемого события.

Наблюдение: Теневое копирование
В разделе Наблюдение Теневое копирование категории DLP осуществляется настройка сохранения теневых копий наблюдаемых объектов.

Установите флажок Включить теневое копирование для включения функции сохранения резервных копий наблюдаемых объектов файловой системы и системного реестра в случае их изменения. Индивидуальная настройка по включению данной опции для отдельных объектов задаётся 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.
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, щёлкните правой кнопкой мыши по требуемому клиентскому приложению SoftControl DLP Client на вкладке Клиенты 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.
Выберите тип расписания – По дням или По часам, в счётчике 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.

Задачи

Вкладка **Задачи** позволяет создавать задачи для клиентских приложений и отслеживать детали их выполнения.
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"

Название кнопки	Описание
Добавить	Создание задачи для клиентских компонентов.
Подробная информация	Просмотр отчёта о выполнении выбранной задачи.
Отменить	Отмена задачи, находящейся в статусе **ожидание**.

Поля вкладки "Задачи"

Поле	Описание
Идентификатор	Порядковый номер задачи.
Тип задачи	Тип задачи: **сбор профиля**; **сканирование**; **обновление**.
Создана	Дата и время создания задачи.
Время запуска	Дата и время запуска задачи.
Статус	Статус завершения задачи: **ожидание** – выполнение задачи не начал ни один клиентский компонент; **отменена** – задача была отменена до начала выполнения; **выполняется** – выполнение задачи начато как минимум одним из клиентских компонентов; **завершена** – задача выполнена всеми клиентскими компонентами.

Основные действия, выполняемые на данной вкладке:

Создание задачи

Чтобы добавить новую задачу, нажмите на кнопку Создать. В окне Новая задача дайте параметры задачи в зависимости от её типа (см. рисунки, начиная с Шаг "Тип задачи" и до Шаг "Клиенты" в разделе Обновление):

- сбор профиля;
- антивирусное сканирование;
- обновление.

Просмотр подробностей выполнения задачи

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

- нажмите на кнопку Подробная информация в группе кнопок вкладки;
- 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.

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

Сбор профиля

1) На шаге Тип задачи выберите Сбор профиля в выпадающем списке и нажмите на кнопку Вперед.
2) На шаге Время запуска выберите опцию Сейчас для немедленного запуска задачи после её добавления, либо выберите опцию Указать время и определите дату и время запуска. Нажмите на кнопку Вперед для продолжения.
3) На шаге Клиенты отметьте клиентские компоненты, для которых необходимо создать задачу. 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.

4.7.2. Антивирусное сканирование

1) На шаге Тип задачи выберите Сканирование в выпадающем списке и отметьте области клиентского хоста для антивирусной проверки:
   - Сканирование памяти;
   - Сканирование загрузочных секторов;
   - Сканирование всех жестких дисков;
   - Сканирование всех съемных носителей.
   - Нажмите на кнопку Вперед для продолжения.
2) На шаге Время запуска выберите опцию Сейчас для немедленного запуска задачи после её добавления, либо выберите опцию Указать время и определите дату и время запуска. Нажмите на кнопку Вперед для продолжения.
3) На шаге Клиенты отметьте клиентские компоненты, для которых необходимо создать задачу.

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.

Обновление

1) На шаге Тип задачи выберите Обновление в выпадающем списке и отметьте необходимые компоненты для обновления и параметры задачи:
Программные модули – обновление программных модулей компонентов типа SysWatch и DLP.
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 и событиях обновления в отчётах.
Нажмите на кнопку Вперед для продолжения.

2) На шаге Время запуска выберите опцию Сейчас для немедленного запуска задачи после её добавления, либо выберите опцию Указать время и определите дату и время запуска. Нажмите на кнопку Вперед для продолжения.

3) На шаге Клиенты отметьте клиентские компоненты, для которых необходимо создать задачу. 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.

Просмотр отчётов

Для просмотра отчётов клиентских приложений в агрегированном виде через консоль управления SoftControl Admin Console предназначена вкладка Лог. Она позволяет в реальном времени отслеживать события на нескольких клиентских хостах одновременно и производить выборку необходимых данных с помощью гибкого механизма фильтрации. На вкладке администратор получает доступ к следующим данным в удобной форме:

- Отчёты SoftControl SysWatch;
- Отчёты SoftControl DLP Client.

Полученные отчёты могут быть выведены на печать или экспортированы в электронный формат.
Кроме того, поддерживается резервное копирование отчётов.

Отчёты SoftControl SysWatch

Вкладка Лог событий предоставляет возможности по детальному мониторингу событий безопасности, регистрируемых SoftControl SysWatch на клиентских хостах.
Полный перечень полей вкладки Лог событий для компонента SoftControl SysWatch приведён в табл.

Поле	Значение
Имя	Имя клиентского хоста.

Идентификатор события	Уникальный идентификатор события. Если происходит приём события с дублированным идентификатором, дублируемая строка помечается красным цветом. В случае нарушения целостности порядка идентификаторов (разрывы в последовательности), в отчёт серверного компонента в журнале Windows вносится соответствующее предупреждение. Исключением являются события типа **Статус**, 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 SysWatch к серверу SoftControl Server.
Тип события	Тип события безопасности (инцидента) • **нарушение политики контроля** • **контроль активности**; • **обновление клиента**; • **запуск процесса**; • **антивирус**; • **изменение настроек**; • **статус** • **вход пользователя**; • **выход пользователя;** • **события DeCrypt**.
Время	Дата и время регистрации события.
Важность	Важность (приоритет) события с точки зрения угрозы информацио безопасности клиентского хоста: • обычная; • высокая; • критическая. Каждому уровню приоритета соответствует свой цвет ячейки.
Действие	Действие в случае события типа **нарушение политики контроля**: • **чтение файла**; • **изменение файла**; • **переименование файла**; • **удаление файла**; • **открытие каталога**; • **удаление каталога**; • **открытие ключа реестра**; • **создание ключа реестра**;

	• **удаление ключа реестра**; • **изменение значения реестра**; • **удаление значения реестра**; • **загрузка DLL-модуля**; • **введен неверный пароль**. Действие в случае события типа **запуск процесса** (данные выводятся в одну строку): • **Инсталлятор**: да/нет; • **В профиле**: да/нет (отсутствует, если на клиентском хосте отключён профиль системы или если в настройках в разделе **Контроль активности** снят флажок **Приложения**); • **Имеет действительную ЭЦП**: да/нет (только для инсталляторов); • **Белый список сертификатов включен**: да/нет (только для инсталляторов); • **Сертификат в белом списке**: да/нет (только для инсталляторов, и если включен белый список); • **Глобальный режим обновления ПО включен**: да/нет (только для инсталляторов); • **Был ли отслеживаемым**: да/нет; • **Запуск в режиме обновления ПО**: да/нет. Действие в случае события типа **антивирус**: • **запуск сканера**; • **запуск сбора профиля**; • **завершение сканирования**; • **профиль собран**; • **сканирование объекта**. Действие в случае события типа **обновление**: • **запуск обновлений**; • **обновление завершено**. Действие в случае события типа **изменение настроек**: • **настройки изменены локально**; • **настройки изменены сервером**. Действие в случае события типа **события DeCrypt**: • **NOTIFY-DEV0;Загрузка, все устройства найдены**; • **NOTIFY-PRETEST;Загрузка с незашифрованным контейнером**; • **NOTIFY-ERROR;Ошибка при загрузке**; • **NOTIFY-PW;Загрузка с паролем**;

	• **NOTIFY-DEV1;Загрузка, одно из устройств не найдено**; • **NOTIFY-DEV2;Загрузка, два устройства не найдены (КРИТИЧНО)**; • **NOTIFY-ACTION: DEV-GET;Запрос списка найденных устройств**; • **NOTIFY-ACTION: DEV-CHANGE;Обновить список устройств**; • **NOTIFY-ACTION: PW-CHANGE;Изменить пароль**; • **NOTIFY-ACTION: DISK-ENC STARTED;Шифрование диска начато**; • **NOTIFY-ACTION: DISK-ENC FINISHED;Шифрование диска завершено**; • **NOTIFY-ACTION: DISK-DEC STARTED;Дешифрование диска начато**; • **NOTIFY-ACTION: DISK-DEC FINISHED;Дешифрование диска завершено**; • **NOTIFY-ACTION: BOOT-PREPARE;Установить системный загрузчик**; • **NOTIFY-ACTION: BOOT-CLEAR;Удалить системный загрузчик**.
Статус действия	Статус действия в случае события типа **антивирус**: • **сканер запущен**; • **ошибка при запуске сканера**; • **сканер был остановлен**; • **успешно**; • **неудачно**. Статус действия в случае события типа **обновление**: • **процесс обновления запущен**; • **ошибка запуска**; • **новых обновлений не найдено**; • **обновление прервано пользователем**; • **обновления успешно установлены**; • **нужна перезагрузка системы**; • **обновление завершено с ошибками**. Статус действия в случае события типа **события DeCrypt**: • **SUCCESS**; • **FAIL**.

Статус клиента	Статус зарегистрированного клиентского компонент: • **активен**; • **остановлен**; • **работа службы была прервана**; • **ошибка статуса. неверный статус**.
Исполняемый файл	Приложение или инсталлятор, вызвавшая события типов **нарушение политики контроля** или **запуск процесса**.
Командная строка процесса	• Команда, вызвавшая событие типа **запуск процесса**. • Имя объекта файловой системы/реестра, в отношении которог произошло событие типа **нарушение политики контроля**, ил DLL-модуля, загружаемого процессом, вызвавшим событие **нарушение политики контроля** • Неверно введённый пароль.
Пользователь	Учётная запись, под которой произошли события типов **запуск процесса** или **изменение настроек**.
Зона	Зона выполнения приложения: • **доверенные** (разрешённые); • **по умолчанию** (ограниченные); • **блокированные** (запрещенные).
Идентификатор процесса	Уникальный порядковый идентификатор процесса (PID) в ОС для со **процесса**.
Идентификатор родительского процесса	Уникальный порядковый идентификатор родительского процесса (PI типа **запуск процесса**.
Родительский процесс	Наименование родительского процесса для события типа **запуск про**
Решение	Решение по запуску приложения: • **разрешен**; • **запрещен**. Каждому решению соответствует свой цвет ячейки.
Проверено объектов	Количество объектов, проверенных в процессе антивирусного скани
Угроз найдено	Количество найденных угроз в процессе антивирусного сканирования.
Угроз обезврежено	Количество обезвреженных угроз в процессе антивирусного сканиро
Встроенные сертификаты	Количество встроенных сертификатов, обнаруженных в процессе авт настройки (сбора профиля).
Сертификаты каталогов	Количество сертификатов каталогов, обнаруженных в процессе авто настройки (сбора профиля).

Приложения	Статус контроля активности приложений: • **активно**; • **неактивно**.
Файловая система	Статус контроля файловой системы: • **активно**; • **неактивно**
Системный реестр	Статус контроля системного реестра: • **активно;** • **неактивно**
Сеть	Статус контроля сетевой активности: • **активно**; • **неактивно**.
Имя вошедшего пользователя	Учётная запись, под которой произошёл вход в ОС клиентского хост
Имя вышедшего пользователя	Учётная запись, под которой произошёл выход из ОС клиентского хо
Ошибка	Код ошибки в базе данных на сервере.
Тип клиента	Тип клиента, для которого отображается отчёт. Для общих событий (имеет пустое значение.
Детали	Идентификатор (UID) правила, в отношении которого произошло на контроля.
Имя службы	Системное имя службы, которая была запущена/остановлена.
Отображаемое и	Название службы в оснастке **Службы** ОС Windows.
Событие службы	Статус службы: • **ServiceStarted**; • **ServiceFoundRunning**; • **ServiceStopped**.

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
- 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 отчёт 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**.

В появившейся дополнительной вкладке **Измененные настройки** представлен перечень настроек SoftControl SysWatch с указанием их нового состояния.

Отчёты SoftControl DLP Client

Вкладка **Лог событий** предоставляет возможность просмотра отчётов по данным, собираемым SoftControl DLP Client на клиентских хостах.

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

Поля вкладки "Лог событий" для SoftControl DLP Client

Поле	Описание
Имя	Имя клиентского хоста.
Идентификатор события	Уникальный идентификатор события. Если происходит приём события с дублированным идентификатором, дублируемая строка помечается красным цветом. В случае нарушения целостности порядка идентификаторов (разрывы в последовательности), в отчёт серверного компонента в журнале Windows вносится соответствующее предупреждение. Исключением являются события типа **Статус**, 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: • **добавлено устройство**; • **вложение**;

	• **файл**; • **HTTP**; • **монитор клавиатуры**; • **принтер**; • **реестр**; • **устройство отсоединено**; • **время работы**.
Время	Дата и время регистрации события.
Важность	Важность (приоритет) события с точки зрения угрозы информационной безопасности клиентского хоста: • обычная; • высокая; • критическая. Каждому уровню приоритета соответствует свой цвет ячейки.
Статус клиента	Статус зарегистрированного клиентского компонента: • **активен**; • **остановлен**; • **работа службы была прервана**; • **ошибка статуса. неверный статус**.
Путь к процессу	Путь к процессу, вызвавшему событие типов **файл**, **реестр**, **HTTP**, **монитор клавиатуры**, **время работы**, **принтер**, **вложение**.
Описание процесса	Описание процесса, вызвавшего событие типов **файл**, **реестр**, **HTTP**, **монитор клавиатуры**, **время работы**, **принтер**, **вложение**.
Пользователь	Учётная запись пользователя, под которой был запущен процесс, вызвавший событие типов **файл**, **реестр**, **HTTP**, **монитор клавиатуры**, **время работы**, **принтер**, **вложение**.
IP	IP-адрес назначения HTTP-запроса для события типа **HTTP**.
Url	URL назначения HTTP-запроса для события типа **HTTP**.
Заголовок	Заголовок HTTP для события типа **HTTP**.

Маска доступа	Тип операции над наблюдаемым объектом для событий типов **файл** и **реестр**: • **чтение**; • **запись**; • **удаление**; • **переименование**; • **изменение**.
Резервная копия	Локальный путь к теневой копии наблюдаемого объекта с именем вида *<Полное имя оригинального объекта>_<N>.bkp*, где *N* – порядковый номер сохранённой копии, для событий типов **файл** и **реестр**.
Путь к файлу-вложению	Путь к файлу-вложению в почтовом клиенте Microsoft® Outlook® 2003 для события типа **вложение**.
Путь к файлу	Путь к наблюдаемому каталогу или файлу для события типа **файл**.
Тип диска	Тип носителя, на котором располагается наблюдаемый каталог или файл для события типа **файл**: • **локальный носитель**; • **съемный носитель**
Ветка реестра	Путь к наблюдаемому разделу реестра или параметру раздела реестра для события типа **реестр**.
Время записи события	Дата записи ввода с клавиатуры для события типа **монитор клавиатуры**.
Записанные данные	Текст, введенный пользователем с клавиатуры, для события типа **монитор клавиатуры**.
Детали	Описание источника печати для события типа **принтер**.
ID устройства	ID периферийного устройства для событий типов **добавлено устройство** и **устройство отсоединено**.
Класс устройства	Класс периферийного устройства для событий типов **добавлено устройство** и **устройство отсоединено**.
Описание устройства	Описание периферийного устройства для событий типов **добавлено устройство** и

	устройство отсоединено.
Время старта	Время начала работы с приложением для события типа **время работы**.
Время окончания	Время окончания работы с приложением для события типа **время работы**.
Продолжительность	Продолжительность работы с приложением для события типа **время**
Индекс файла	Индекс файла для событии типа **HTTP**.
Тип клиента	Тип клиента, для которого отображается отчёт. 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 отчётах цветом, если содержат в себе дополнительные данные (видеозаписи, теневые копии).

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.
В появившемся окне проигрывателя нажмите на кнопку **Загрузить** и управляйте воспроизведением.
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**.**

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 и в появившемся окне Просмотр теневой копии DLP нажмите на кнопку Открыть, чтобы просмотреть сохранённую копию указанного объекта наблюдения.

Фильтрация событий

Страничное отображение

Информация на вкладке Лог отображается в постраничном режиме. Ограничение максимального количества событий на странице задаётся в настройках интерфейса SoftControl Admin Console (по умолчанию – 10 000 событий).

Записи в таблице вкладки упорядочены по страницам в прямом хронологическом порядке, т.е. странице с наибольшим номером соответствует последняя по времени порция событий. При открытии вкладки загружается первая страница. Для навигации по страницам используйте соответствующие кнопки в нижней части вкладки. Переход осуществляется только на соседние страницы.

Группировка данных

Информация на вкладке Лог может группироваться по всем полям (категориям) для удобства отображения. Полями (категориями), по которым возможно произвести группировку на дополнительной вкладке Сканнер, являются Путь (по умолчанию), Вирус, Результат и Действие. Для группировки по категориям перетащите заголовок колонки на панель, расположенную между заголовком таблицы и группой кнопок вкладки (см. рисунки, начиная с Вкладка "Лог" для компонента SoftControl DLP Client и до Теневая копия объекта наблюдения в разделе выше). 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;
- Вложение;
- Файл;
- HTTP;
- Монитор клавиатуры;
- Принтер;
- Реестр;
- Устройство отсоединено;
- Время работы.

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.

Для добавления нового поля в таблицу текущей вкладки нажмите кнопку Выбрать колонки и перетащите требуемое поле из окна Выбор колонок в необходимое место заголовка таблицы. Для удаления существующего поля перетащите его в окно Выбор колонок, либо за пределы заголовка таблицы.

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

В SoftControl Admin Console существует возможность тонкой подстройки параметров выборки с помощью средства Редактор фильтра. Если на вкладке Лог производится фильтрация по какому-либо из полей, в нижней части вкладки отображается строка параметров фильтра.
Для вызова окна редактора нажмите кнопку Редактировать фильтр в правой части строки параметров..
В первой строке редактора красным цветом указано логическое условие, по которому объединяются параметры фильтра. Для изменения логического условия нажмите на него левой кнопкой мыши, при этом в выпадающем меню доступны следующие логические операторы:

- И;
- ИЛИ;
- Не И;
- Не ИЛИ.

Для добавления нового параметра фильтра выберите пункт меню Добавить Условие, либо нажмите на значок плюса около логического условия. Для добавления параметра фильтра, состоящего из нескольких параметров, объединённых по своему логическому условию, выберите пункт меню Добавить Группу. Работа с элементами группы аналогична работе с элементами общего списка. Возможно создание вложенных групп. Для очистки фильтра выберите пункт меню Очистить всё. Нажмите OK, чтобы сохранить параметры фильтра.
Синтаксис строки параметра фильтра выглядит следующим образом: <поле, по которому производится фильтрация> <условие> <значение>. Каждый элемент строки параметра можно изменить, нажав на него. Варианты условия автоматически определяются исходя из типа поля.
Для упорядочивания данных в таблицах вкладок по определённым 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 OK.

Печать и экспорт в файлы отчётов

В SoftControl Admin Console существует несколько возможностей экспорта накопленной информации в отчётах клиентских приложений.
Для вывода отчёта на печать произведите выборку с помощью необходимых фильтров и нажмите на кнопку **Печать**. В открывшемся окне предварительного просмотра можно задать **Настройки страницы** и **Масштаб** с помощью соответствующих кнопок.
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 отчёта в таблицу Excel произведите выборку с помощью необходимых фильтров и нажмите на кнопку **Экспорт в Excel**. В диалоговом окне сохранения укажите место для сохранения отчёта и его имя, после чего нажмите на кнопку **Сохранить** (Save).

Резервное копирование отчётов

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 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.
Вы также можете настроить резервное копирование с помощью сторонних средств, без использования инструментов SoftControl Service Center. В этом случае в окне **Настройки сервера** выберите пункт **Я сам настрою резервное копирование**.

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 получателей оповещений, после чего настроить параметры отправки.

Контакты
На вкладке **Контакты** производится задание адресатов – получателей нотификаций.

Перечень полей вкладки приведён в табл. 26.

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**. В появившемся окне укажите данные получателя в полях **Имя** и **Электронная почта** и нажмите на кнопку **Применить**.

Для правки и удаления контактов воспользуйтесь соответствующими кнопками.

Нотификации

Вкладка **Управление нотификациями** предназначена для настройки параметров отправки оповещений о событиях посредством электронной почты.

Снимки конфигурации

Вкладка **Снимки конфигурации** предназначена для создания снимков конфигурации любого подключённого 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.

Обновление компонентов СИБ

SoftControl Service Center предоставляет возможность централизованного обновления всех компонентов системы с сервера обновлений. Это может быть либо сервер SoftControl, либо сервер, развёрнутый на предприятии. Вкладка **Обновления** позволяет произвести настройку и просмотреть историю обновлений.

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

Программные модули;

Антивирусные базы.

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

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: • **Обновление не требуется**; • **Доступно обновление**; • **Обновление загружено**; • **Обновление установлено**; • **Ошибка обновления**.
Размер обновления	Размер обновления в байтах.
Актуальная версия	Текущая версия установленного компонента.
Новая версия	Версия компонента, доступная к обновлению.
Детали	Дополнительная информация.

Настройка обновления программных модулей

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

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 ретрансляция 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. Обновление клиентских компонентов осуществляется с созданного локального «зеркала».

астройка 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.
Папка для сохранения обновлений:
Путь сохранения пакетов обновления с внешних серверов относительно директории C:\ProgramData\SoftControl.

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.

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, ретрансляция 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, ретрансляция 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).
В секции **Статус обновления** доступна информация по текущей версии и последним проведенным операциям проверки и установки обновлений.
Для применения изменённых установок нажмите на кнопку **Сохранить**.

Настройка обновления антивирусных баз
Данная категория настроек позволяет настраивать и управлять ретрансляцией антивирусных баз клиентского компонента SoftControl SysWatch с внешних (Интернет) серверов.

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 ретрансляция обновлений баз на сервер. Обновление антивирусных баз осуществляется в рамках обновления клиентского компонента SoftControl SysWatch с созданного локального «зеркала».

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**.
3) Выберите операцию **Изменить**.

4) Выберите компонент для удаления: нажмите на пиктограмму компонента и в выпадающем меню выберите опцию **Компонент будет полностью недоступен**. После того как все установки завершены, нажмите на кнопку **Далее**.
5) Нажмите на кнопку **Изменить**.
6) Дождитесь окончания процесса удаления.
7) После появления сообщения *Установка SoftControl Service Center завершена* нажмите на кнопку **Готово**.

Дополнительная информация

О сертификатах сервера

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 используется протокол HTTPS. Все данные между сервером и конечной точкой передаются в зашифрованном виде по защищённому каналу, при этом для авторизации клиентов используются сертификаты стандарта X.509.
В процессе работы SoftControl Server генерирует следующие виды сертификатов:
Корневой – данный сертификат является сертификатом удостоверяющего центра в рамках СИБ на основе Сервисного Центра и помещается в хранилище Windows. Все остальные виды сертификатов продукта подписаны корневым сертификатом, что является одним из критериев их достоверности.
Серверный – сертификат серверной стороны, используемый для взаимодействия с клиентами и помещаемый в хранилище Windows.
Общий клиентский – сертификат клиентской стороны, используемый для регистрации клиентов на сервере. 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, применяемый к клиенту на конечной точке, а также выгружается в отдельный файл по следующему пути:

C:\ProgramData\SafenSoft\Client.pem

Индивидуальный клиентский – сертификат клиентской стороны, выдаваемый серверным компонентом после подтверждения регистрации 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 истёк срок его действия, существует возможность выдачи другого сертификата (обновление) или его отзыв (отклонение регистрации).

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 изменён 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
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.

Резервное копирование

В некоторых случаях существует необходимость в создании резервной копии компонентов Сервисного Центра, с целью дальнейшего восстановления полностью работоспособной конфигурации без потери связи с клиентскими приложениями на удалённых хостах. Случаи, к которым применимы данные операции:

необходимость переустановки ОС на компьютере с компонентами ;
необходимость переноса на другой компьютер.

7.3.1. Создание резервной копии

Резервная копия файлов включает в себя необходимые для восстановления файлы конфигурации серверного компонента SoftControl Server и сертификаты. Также могут быть сохранены пользовательские фильтры 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**.
   Введите путь до каталога, куда предполагается сохранить файлы резервной копии, в соответствующее поле. Если требуется сформировать подкаталог с уникальным идентификатором по введённому 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 отображён статус операции.
3) Для сохранения пользовательских фильтров в окне **Резервное копирование** 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), сохранять её копию не требуется. В обратном случае создайте резервную копию текущей БД средствами Microsoft® SQL Server®.

Восстановление из резервной копии

Для восстановления из резервной копии выполните следующую последовательность действий:

1) Убедитесь, что на компьютере установлено правильное время.
2) Установите SoftControl Service Center той же версии, что использовался на компьютере, с которого создавалась резервная копия.
3) Выполните восстановление ранее сохранённой БД. Пропустите этот шаг, если БД находилась на другом компьютере и не удалялась.
4) Произведите первичную настройку сервера. 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**. Введите путь до каталога с ранее сохранёнными файлами резервной копии в соответствующее поле и нажмите на кнопку **Восстановить**. В нижней части окна будет отображён статус операции.
7) При необходимости восстановления пользовательских фильтров в окне **Резервное копирование** повторите действия п. 6 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.
10) Авторизуйтесь в консоли управления SoftControl Admin Console. Проверьте работоспособность компонентов.