ELSYS

ПРОФЕССИОНАЛЬНАЯ СИСТЕМА
КОНТРОЛЯ И УПРАВЛЕНИЯ ДОСТУПОМ

ТВИНПРО
группа компаний

Программный сервис Elsys-SDK II

Версия 1.3.1

Руководство администратора

Самара, 2026

Оглавление

1 Общие сведения....3
2 Условия применения....4
3 Установка сервиса SDK....5
3.1 Установка в ОС Microsoft Windows....5
3.2 Установка в ОС Linux....6
4 Управление сервисом SDK....7
5 Настройка сервиса SDK программой с графическим интерфейсом....8
5.1 Настройка основных параметров работы сервиса....9
5.2 Настройка параметров протоколирования работы сервиса....11
5.3 Настройка параметров защищенного обмена....13
5.4 Настройка параметров взаимодействия с хранилищем секретов....14
5.5 Настройка параметров сертификатов....16
6 Настройка сервиса SDK консольной утилитой....17

1 Общие сведения

Программный сервис Elsys-SDK II (далее, сервис SDK) предназначен для осуществления информационного обмена клиентского программного обеспечения с оборудованием СКУД Elsys. Сервис реализован как программа, способная функционировать на компьютере под управлением операционных систем (ОС) семейства Microsoft Windows и Linux, независимо от пользователя данного компьютера. Для ОС семейства Microsoft Windows сервис реализован в виде программной службы с возможностью запуска в автоматическом либо ручном режиме. В ОС семейства Linux для запуска сервиса SDK используется подсистема инициализации и управления службами systemd.

Сервис SDK обеспечивает:

- взаимодействие клиентского программного обеспечения с оборудованием СКУД Elsys, в том числе, по защищенным каналам связи;
- опрос контроллеров, подключенных в линию связи RS485 (до 63 контроллеров в линии);
- опрос коммуникационных сетевых контроллеров (КСК) Elsys (до 254 КСК);
- опрос контроллеров, подключаемых в сеть Ethernet;
- мониторинг событий устройств и управление ими;
- удаленное обновление микропрограммного обеспечения КСК, контроллеров и адресных расширителей АДЛС;
- централизованное хранение файла конфигурации системы;
- взаимодействие с сервисами хранения секретов с программным интерфейсом, совместимым с Vault HTTP API, в части загрузки SSL сертификатов.

К устройствам относятся КСК, линии связи, контроллеры, точки доступа (двери, турникеты, ворота), считыватели, охранные зоны и входы контроллеров, охранные разделы и группы разделов, выходы и группы выходов.

Обмен данными между клиентским ПО и сервисом SDK осуществляется по протоколу HTTP путём передачи POST-запросов и анализа ответных посылок. Данные в запросных и ответных посылках передаются в формате XML. Для работы сервиса хранения конфигурации используется отдельный TCP-канал.

Для защиты сетевого обмена по всем каналам взаимодействия с клиентами, а также по каналу обмена с контроллерами, используется протокол TLS. Минимальная поддерживаемая версия протокола TLS – 1.2.

2 Условия применения

Сервис SDK функционирует в ОС Microsoft Windows и Linux. Для работы сервиса требуется наличие модулей библиотек Qt версии 5.15 и OpenSSL версии 3.0. Дополнительно, для работы Windows версии сервиса SDK требуется наличие распространяемых библиотек Microsoft Visual C++ 2019 для платформы x64.

Для семейства ОС Microsoft Windows минимальная поддерживаемая версия – Windows 7 SP1 x64, все необходимые для работы библиотеки поставляются в составе установочного комплекта сервиса. Установочные комплекты для ОС семейства Linux представлены бинарными пакетами формата deb и rpm. Поддерживаются установка и работа в Astra Linux SE версий 1.7 и 1.8 базового уровня защищенности, РЕД ОС версий 7.3 и 8 и SberLinux версии 8.8.

Минимальная аппаратная конфигурация компьютера, на котором планируется функционирование сервиса SDK, зависит от используемой ОС и общего количества обслуживаемых устройств. Также, необходимо учитывать настройки протоколирования работы сервиса, а именно, максимальный размер файла журнала и количество хранимых копий.

Минимальная аппаратная конфигурация компьютера, работающего под управлением ОС Windows 7 SP1 x64:

- четырёхядерный CPU с тактовой частотой каждого ядра не менее 2 ГГц;
- объем свободной оперативной памяти не менее 4 Гб;
- свободное место на накопителе не менее 300 Мб (при отключенном отладочном режиме);
- последовательный коммуникационный интерфейс для работы с линией RS-485.

Подключение внешних приложений (сетевых клиентов) к сервису SDK осуществляется по сети Ethernet. Сетевой протокол – TCP/IP. Сервис может обслуживать сетевых клиентов как на всех активных сетевых интерфейсах компьютера, так и только на одном интерфейсе.

> ***Внимание!*** *Для обеспечения доступа внешних приложений через ЛВС к программному сервису SDK необходимо разрешить запуск сервиса в брандмауэре ОС (или другом аналогичном решении, используемом на компьютере с установленным сервисом), либо настроить разрешающие правила доступа к портам сервиса HTTP SDK и сервиса хранения конфигурации, а также к UDP портам опроса сетевых групп и поиска.*

Для управления и настройки сервиса SDK программой с графическим интерфейсом требуются полномочия и права администратора ОС.

3 Установка сервиса SDK

3.1 Установка в ОС Microsoft Windows

Для установки сервиса SDK необходимо запустить программу инсталляции ***SetupElsysAppService_vX.X.X.X.exe***, где X.X.X.X – номер версии сервиса. Запуск программы инсталляции должен быть выполнен пользователем с полномочиями и правами администратора ОС.

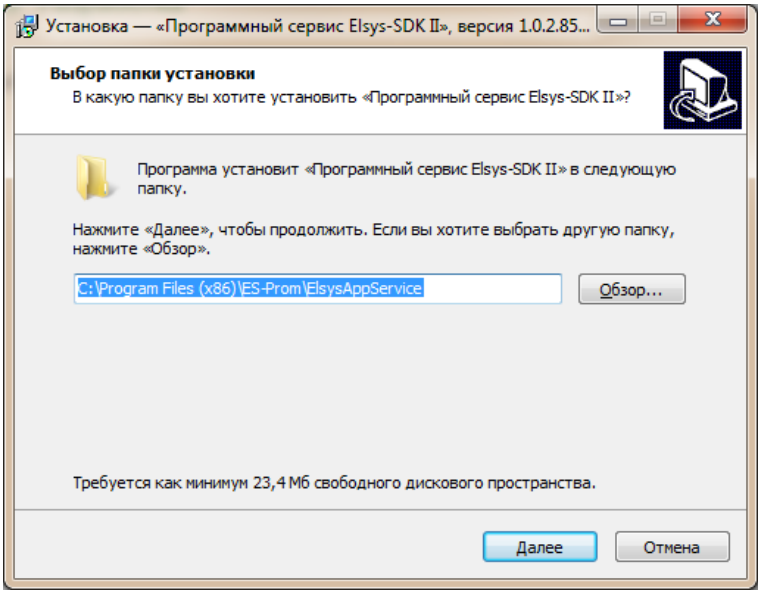

Рисунок 1 – Окно настройки папки установки

После подтверждения полномочий пользователя программа инсталляции предложит выбрать папку установки сервиса SDK. Обязательным требованием при выборе места размещения файлов является наличие неограниченного доступа для системной учетной записи, от имени которой в дальнейшем будет функционировать сервис SDK.

На рисунке 1 в строке ввода указано место размещения, предлагаемое программой инсталляции по умолчанию – ***%PROGRAMFILES%\ES-Prom\ElsysAppService***. При самостоятельном выборе папки установки не рекомендуется использовать в качестве места размещения папку, в абсолютном имени которой содержатся символы национальных алфавитов.

Далее, программа инсталляции предложит окончательно подтвердить запуск процесса установки. В процессе установки выполняются следующие частные задачи:

- Копирование исполняемых файлов и библиотек сервиса, вспомогательных утилит, необходимых для его функционирования и справочных руководств в заданную папку установки.
- Проверка наличия установленной версии распространяемых библиотек Microsoft Visual C++ 2019 для платформы x64, выполнение установки библиотек при их отсутствии.
- Создание системного сервиса (службы) Windows со следующими параметрами: имя службы – «***ElsysAppService***», тип запуска – автоматический.
- Создание правила брандмауэра Windows для разрешения сетевого доступа к сервису SDK.

После успешной установки сервиса в системное меню Windows будет добавлена программная группа «ES-Prom» и ярлыки доступа к программе настройки сервиса SDK и руководству администратора.

3.2 Установка в ОС Linux

Установочный комплект представлен следующими пакетами:

- **elsys-app-service_X.X.X.X-astra1.7_amd64.deb** (Astra Linux SE 1.7), **elsys-app-service_X.X.X.X-astra1.8_amd64.deb** (Astra Linux SE 1.8), **elsys-app-service_X.X.X.X-1.el7.x86_64.rpm** (РЕД ОС 7.3), **elsys-app-service_X.X.X.X-1.red80.x86_64.rpm** (РЕД ОС 8) , **elsys-app-service_X.X.X.X-1.el8.x86_64.rpm** (SberLinux 8) – пакет, содержащий бинарные файлы сервиса SDK, консольной утилиты настройки сервиса и руководство администратора, где **X.X.X.X** – версия бинарного пакета;
- **elsys-service-config-gui_X.X.X.X-astra1.7_amd64.deb** (Astra Linux SE 1.7), **elsys-service-config-gui_X.X.X.X-astra1.8_amd64.deb** (Astra Linux SE 1.8), **elsys-service-config-gui_X.X.X.X-1.el7.x86_64.rpm** (РЕД ОС 7.3), **elsys-service-config-gui_X.X.X.X-1.red80.x86_64.rpm** (РЕД ОС 8), **elsys-service-config-gui_X.X.X.X-1.el8.x86_64.rpm** (SberLinux 8) – пакет, содержащий бинарный файл программы настройки сервиса (версия с графическим интерфейсом), где **X.X.X.X** – версия бинарного пакета.

Внимание! *Установка пакетов должна выполняться пользователем с полномочиями и правами администратора ОС.*

Установка пакетов формата **deb** выполняется через систему управления пакетами **apt**. Команда установки имеет следующий вид (на примере пакетов для Astra Linux SE 1.7):

```
apt install ./elsys-app-service_X.X.X.X-astra1.7_amd64.deb
apt install ./elsys-service-config-gui_X.X.X.X-astra1.7_amd64.deb
```

Установка пакетов формата **rpm** выполняется через систему управления пакетами **dnf**. Команда установки имеет следующий вид (на примере пакетов для РЕД ОС 7.3):

```
dnf install elsys-app-service_X.X.X.X-1.el7.x86_64.rpm
dnf install elsys-service-config-gui_X.X.X.X-1.el7.x86_64.rpm
```

Все файлы устанавливаются в папку **/opt/ES-Prom/ElsysAppService**.

В ходе выполнения процедуры установки пакета **elsys-app-service** создается системный пользователь **elsys**, от имени которого выполняется сервис SDK.

Внимание! *Для корректной работы внешних приложений совместно с сервисом SDK необходимо настроить разрешающие правила доступа к портам сервиса HTTP SDK (по умолчанию – 8080/tcp) и сервиса хранения конфигурации (по умолчанию – 5080/tcp). Также, требуется настроить разрешающие правила доступа к UDP портам поиска (4003/udp) и опроса сетевых групп (4096/udp).*

Изменение установленных по умолчанию номеров портов выполняется программой настройки в соответствии с п. 5.1, либо консольной утилитой в соответствии с п. 6. После изменения необходимо внести соответствующие корректировки в разрешающие правила доступа.

4 Управление сервисом SDK

Имя исполняемого файла сервиса SDK в ОС Microsoft Windows – ***sdk2_svc.exe***, в ОС Linux – ***sdk2_svc***.

Для запуска и остановки системной службы Windows, обеспечивающей работы сервиса SDK, может использоваться либо стандартная оснастка «Службы» консоли управления Windows (имя файла оснастки – ***services.msc***, имя системной службы Windows – ***ElsysAppService***), либо программа настройки сервиса с графическим интерфейсом, входящая в установочный комплект. Описание кнопок панели быстрого доступа программы настройки, используемых для управления сервисом SDK, приведено в Таблица 1.

В ОС Microsoft Windows сервис выполняется от имени системной учетной записи, в ОС Linux – от имени пользователя **elsys**. Данный пользователь создается в процессе установки сервиса SDK.

В ОС Linux запуск и остановка сервиса мониторинга должны выполняться либо посредством интерфейса программы настройки сервиса с графическим интерфейсом (кнопки управления размещены на панели быстрого доступа главного окна программы), либо при помощи команд подсистемы systemd.

Запуск сервиса (в подсистеме systemd):

```
systemctl start ElsysAppService
```

Остановка сервиса (в подсистеме systemd):

```
systemctl stop ElsysAppService
```

Внимание! *Запуск и остановка сервиса SDK должны выполняться только в соответствии с данным руководством.*

Для управления сервисом SDK во всех упомянутых случаях пользователь должен иметь полномочия локального администратора.

Инициализационные файлы сервиса SDK (***sdkconfig.xml, apbconfig.xml*** и ***datetimeconfig.xml***) хранятся в рабочей папке данных сервиса, которая в Microsoft Windows располагается по пути «***%PROGRAMDATA%\ES-Prom\ElsysAppService***», в Linux – «***/opt/ES-Prom/ElsysAppService/data***». Системная переменная ***%PROGRAMDATA%*** в ОС Microsoft Windows ссылается на системную папку, предназначенную для хранения общих данных приложений (по умолчанию – ***C:\ProgramData***). Кроме вышеупомянутых файлов в рабочей папке данных сервиса хранится файл ***elsysconfig.xml.gz***, необходимый для работы сервиса централизованного хранения конфигурации системы, и файл буфера сохраненных событий ***membuffer.dat***. Файл настроек сервиса ***elsysappservice.ini*** в Windows-версии также хранится в рабочей папке данных сервиса, в Linux-версии – в каталоге ***/opt/ES-Prom/ElsysAppService/bin***.

Файлы журнала работы сервиса и отладочных журналов (п. 5.2) по умолчанию хранятся в подкаталоге ***Logs*** рабочей папки сервиса (в Windows-версии) и в каталоге ***/opt/ES-Prom/ElsysAppService/logs*** (в Linux-версии). В процессе эксплуатации размещение файлов журналов может быть переназначено.

5 Настройка сервиса SDK программой с графическим интерфейсом

Имя файла программы настройки в ОС Microsoft Windows – ***sdk2_svc_config.exe***, в ОС Linux – ***sdk2_svc_config***. Исполняемый файл программы находится в каталоге сервиса SDK. В программной группе «ES-Prom» системного меню ОС размещается ярлык быстрого доступа с названием «Настройка сервиса».

> ***Внимание!*** *Для работы программы настройки в ОС Microsoft Windows требуются полномочия и права локального администратора. В ОС Linux полномочия локального администратора требуются только при управлении сервисом SDK.*

Программа настройки требует авторизации пользователя посредством указания пароля доступа к сервису. Пароль по умолчанию – ***ElsysAppService***. При первоначальном запуске программы настройки данный пароль необходимо изменить (п. 5.1).

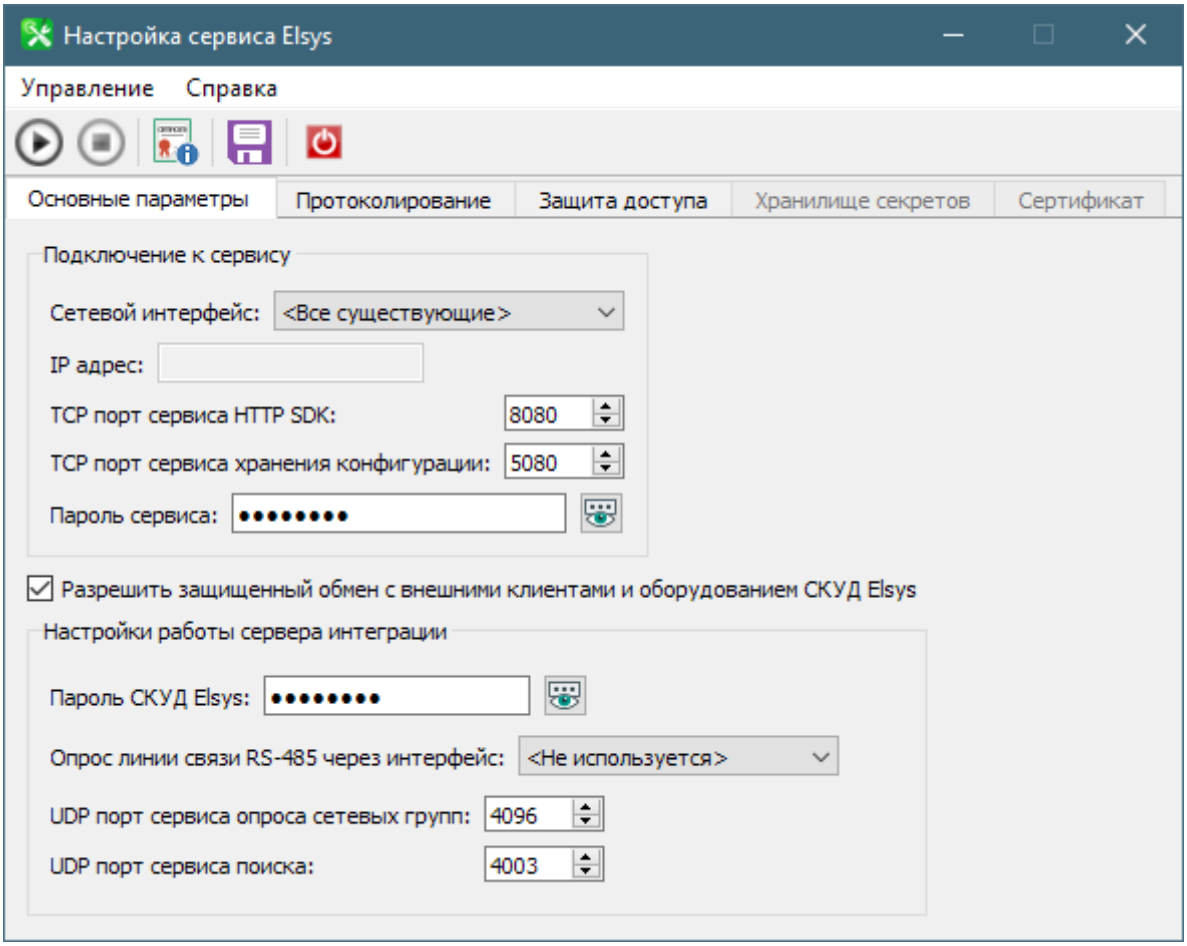

Рисунок 2 – Главное окно программы настройки сервиса SDK

Интерфейс главного окна программы настройки сервиса SDK, изображенный на рисунке 2, позволяет выполнить следующие операции:

- управление сервисом SDK – запуск и остановка;
- настройку параметров сетевого доступа к сервису SDK;
- настройку параметров сервиса SDK, используемых для работы с устройствами;
- настройку протоколирования работы сервиса SDK;
- настройку параметров отладочного режима работы сервера интеграции;

- настройку параметров защиты доступа внешних клиентов к сервису и защищенного обмена с контроллерами;
- отображение основных свойств сертификатов SSL, загружаемых из файловой системы, и проверку корректности настроек защиты доступа.

Команды раздела «Управление» главного меню программы настройки продублированы на панели ярлыков быстрого доступа. Данный раздел главного меню содержит команды для запуска и остановки сервиса SDK, сохранения настроек сервиса SDK в файле конфигурации и завершения работы программы настройки.

Назначение кнопок, расположенных на панели быстрого доступа приведено в таблице 1.

Таблица 1 – Назначение кнопок на панели быстрого доступа

	Отправка команды запуска сервиса SDK.
	Отправка команды остановки сервиса SDK.
	Отображение формы свойств сертификатов SSL, загружаемых из файловой системы.
	Сохранение файла настроек сервиса SDK.
	Завершение работы приложения.

После старта программы настройки в главном окне отображаются текущие параметры, прочитанные из файла настроек сервиса.

Если файл настроек отсутствует в рабочей папке данных сервиса (п. 4), или по какой-либо причине не может быть прочитан программой настройки, то в процессе запуска программы будет сформирован новый файл с настройками по умолчанию. В этом случае будет выполнено уведомление пользователя при помощи окна с соответствующим информационным сообщением.

> ***Внимание!*** *Любые изменения параметров работы сервиса SDK должны быть сохранены в файле настроек. Сохраненные изменения значений параметров (кроме параметров отладочного режима) вступят в силу только при повторном запуске сервиса SDK. Изменения значений параметров отладочного режима применяются без перезагрузки сервиса SDK в течении 10 секунд после сохранения файла настроек.*

5.1 Настройка основных параметров работы сервиса

Группа интерфейсных элементов управления вкладки «Основные параметры» (рисунок 3) обеспечивает настройку параметров сетевого доступа внешних клиентов к сервису SDK и работы сервера интеграции с оборудованием СКУД Elsys, в том числе, и с использованием защищенных подключений по протоколу TLS. Минимальная поддерживаемая версия протокола TLS – 1.2. При включении режима защищенного обмена требуется дополнительная настройка параметров в соответствии с п.5.3.

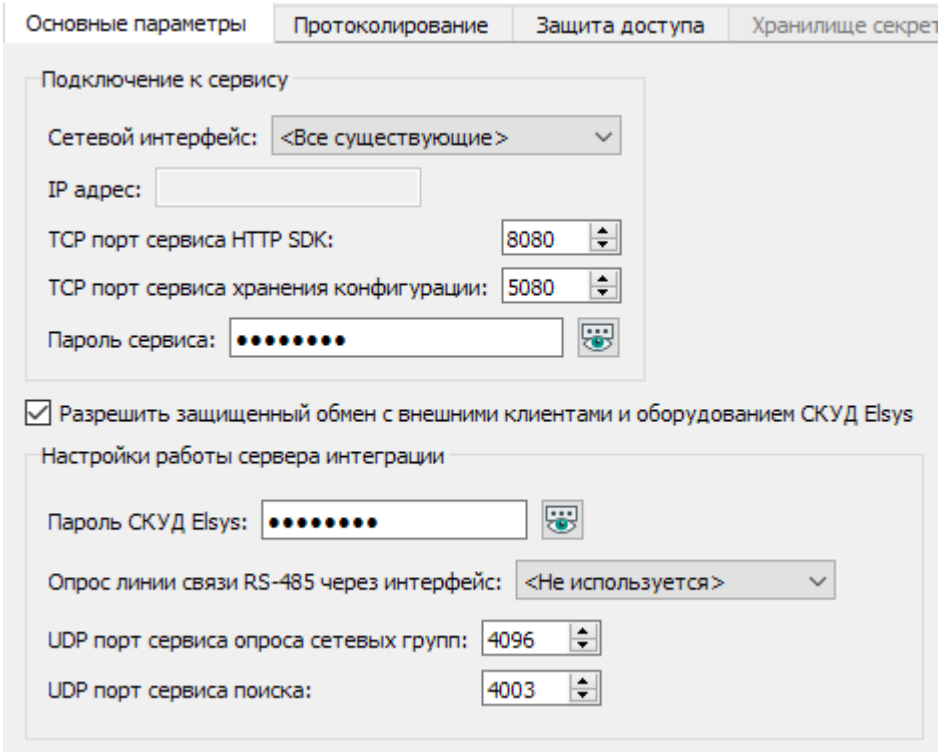

Рисунок 3 – Интерфейс настройки основных параметров

Выпадающий список «Сетевой интерфейс» содержит адреса всех сетевых адаптеров текущего хоста, а также пункты «Все существующие» и «Задано пользователем». При выборе пользователем пункта списка, содержащего адрес, подключение внешних клиентов будет возможно только на том интерфейсе, адрес которого выбран пользователем. При необходимости, пользователь может указать адрес самостоятельно. Для этого надо выбрать пункт списка «Задано пользователем» и указать корректный адрес IPv4 в расположенном ниже поле ввода. При выборе пользователем пункта «Все существующие» сервер интеграции будет обрабатывать клиентские запросы, поступающие с любого из сетевых интерфейсов хоста.

> ***Внимание!*** *После установки сервер интеграции по умолчанию настроен на обработку только локальных запросов (адрес интерфейса – 127.0.0.1). Для разрешения сетевого доступа клиентских приложений к сервисам HTTP SDK и хранения конфигурации требуется выполнение настройки.*

Номера портов, используемых для подключения к сервисам HTTP SDK и хранения конфигурации, задаются в соответствующих поля ввода, расположенных в группе «Подключение к сервису». По умолчанию сервис HTTP SDK использует TCP-порт с номером 8080, сервис хранения конфигурации системы – TCP-порт 5080. В случае наличия конфликтов с другим программным обеспечением необходимо выполнить настройку номеров портов.

Поле «Пароль сервиса» задает пароль, используемый для работы с сервисом HTTP SDK. Также этот пароль используется для доступа к программе настройки параметров сервиса. Поле обязательное, количество символов в пароле – от 4 до 16, кодировка символов – ASCII. Триггерная кнопка управляет режимом отображения символов пароля.

Группа интерфейсных элементов «Настройки работы сервера интеграции» позволяет настроить параметры коммуникационных потоков сервиса SDK, обеспечивающих опрос контроллеров, подклю-

ченных в линию связи RS-485, опрос сетевых групп и функционирование сервиса поиска оборудования. Также, в данной группе элементов можно задать пароль СКУД Elsys, используемый сервисом SDK при обмене сообщениями с КСК и контроллерами в сетевых группах.

> ***Внимание!*** *Связь с КСК и контроллерами в сетевых группах возможна лишь при совпадении паролей в сервисе SDK и устройствах, участвующих в обмене.*

Пароль СКУД Elsys должен содержать 8 алфавитно-цифровых символов в кодировке ASCII (латинские буквы в верхнем или нижнем регистре и цифры). При создании конфигурации сервиса генерируется случайный пароль СКУД. Триггерная кнопка управляет режимом отображения символов пароля.

Имя коммуникационного интерфейса, используемого сервисом SDK для опроса контроллеров в линии связи RS-485, может быть выбрано либо из элементов выпадающего списка имен интерфейсов, обнаруженных на локальном ПК, либо введено пользователем в расположенном справа поле ввода, если выбран элемент списка «Задано пользователем». Вводимое пользователем имя должно соответствовать требованиям к именам коммуникационных интерфейсов операционной системы. По умолчанию опрос контроллеров в линии связи отключен.

> ***Внимание!*** *При задании некорректного имени коммуникационного интерфейса, либо имени интерфейса, несуществующего на момент запуска сервиса SDK, опрос контроллеров в линии RS-485 будет недоступен.*

Номер порта UDP сервиса, используемого для опроса сетевых групп, и номер порта, используемого UDP сервисом поиска КСК и контроллеров в сетевых группах, не должны совпадать. По умолчанию сервис опроса сетевых групп использует порт 4096, а сервис поиска – порт 4003. Изменять заданные по умолчанию номера портов рекомендуется только в случае наличия конфликтов с другим программным обеспечением хоста сервиса SDK.

Измененные значения основных параметров работы сервера интеграции применяются только после сохранения файла настроек и перезапуска сервиса.

5.2 Настройка параметров протоколирования работы сервиса

Для настройки основных параметров протоколирования работы сервиса SDK предназначены интерфейсные элементы управления, расположенные на вкладке «Протоколирование» (рисунок 4). Данная группа элементов позволяет настроить размещение файлов журналов работы сервиса, максимальный размер файла журнала и количество хранимых версий. Также, можно настроить использование расширенной версии журнала работы, содержащей отладочные сообщения для анализа проблем в работе информационных подсистем сервиса SDK, и параметры отладочного протоколирования работы сервера интеграции (информационного обмена коммуникационных потоков сервера оборудования, HTTP сервиса и внутренней работы сервиса SDK). Протоколирование отладочных сообщений и отладочный режим сервера интеграции по умолчанию выключены.

> ***Внимание!*** *Отладочный режим работы сервера интеграции не является основным режимом работы сервиса и должен включаться только для выявления проблем в работе сервиса и оборудования по указанию сотрудников технической поддержки.*

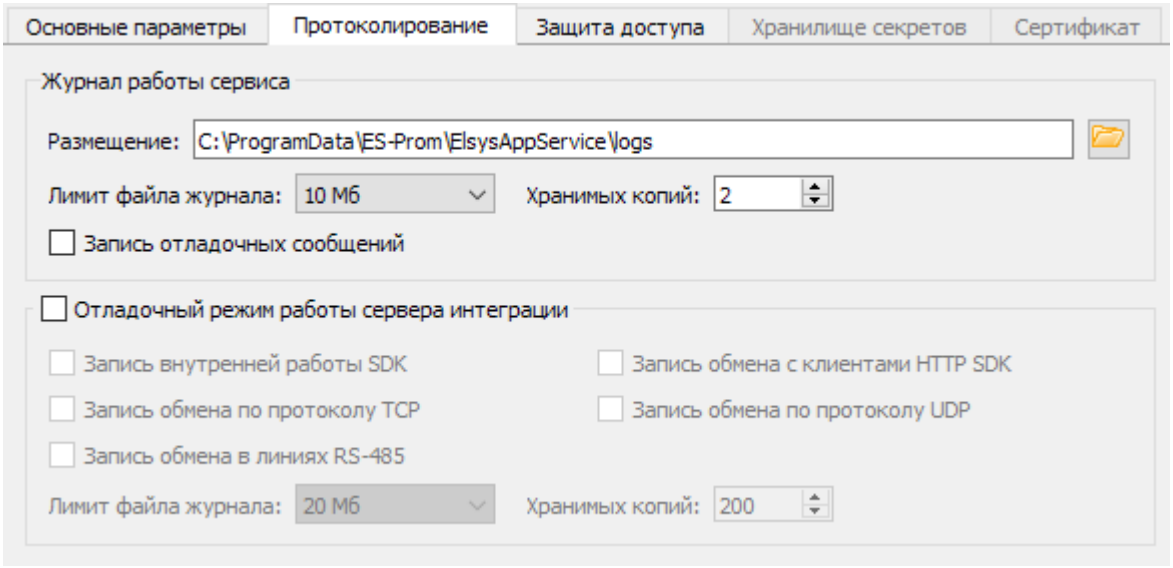

Рисунок 4 – Интерфейс настройки протоколирования работы сервиса

Имя файла журнала работы сервиса – ***elsysappservice.log***, информационного обмена коммуникационных потоков – ***comm_debug_xxx.log***, информационного обмена HTTP сервиса – ***http_debug_xxx.log***, внутренней работы сервиса SDK – ***sdk_debug_xxx.log***, где ***xxx*** – номер версии файла журнала.

Подсистема протоколирования работы сервиса осуществляет контроль размера текущей версии журнала и при достижении заданного предела размера выполняет резервное копирование текущего журнала в файл хранимой копии с последующей очисткой содержимого текущей версии журнала работы. Максимально допустимый размер текущей версии журнала составляет 50 МБ. Максимально допустимое количество хранимых копий – 4.

> ***Внимание!*** *При выборе максимального размера файла журнала и количества хранимых копий необходимо учитывать наличие свободного места на диске.*

Подсистема отладочного протоколирования использует последовательную нумерацию версий файлов журнала с переключением на следующую версию файла при достижении заданного предела размера. После достижения максимального значения номер версии сбрасывается до минимального значения. Максимально допустимый размер текущей версии журнала составляет 50 МБ. Максимально допустимое количество хранимых версий – 200.

По умолчанию файлы журнала работы сервиса и его архивные копии для Windows-версии размещаются в подкаталоге ***Logs*** рабочей папки данных сервиса (п. 4), для Linux-версии – в каталоге ***/opt/ES-Prom/ElsysAppService/logs***. Кнопка отображает окно выбора нового размещения файлов журналов. Файлы журналов отладочного протоколирования размещаются в одном каталоге с журналами работы сервиса.

> ***Внимание!*** *Каталог, назначаемый для хранения файлов журналов работы, должен иметь установленные права полного доступа для учетной записи пользователя, от имени которого запускается сервис (п. 4). При выборе максимального размера файла журнала и количества хранимых копий необходимо учитывать наличие свободного места на диске.*

Измененные значения параметров протоколирования работы применяются только после сохранения файла настроек и перезапуска сервиса. Измененные значения параметров отладочного протоколирования применяются в течении 10 секунд после сохранения файла настроек и не требуют перезапуска сервиса.

5.3 Настройка параметров защищенного обмена

Для настройки параметров защиты доступа внешних клиентов к сервису и информационного обмена сервера интеграции с оборудованием СКУД Elsys, поддерживающим защищенный режим работы, предназначены интерфейсные элементы, расположенные на вкладке «Защита доступа» (рисунок 5). По умолчанию защита доступа отключена. При отключенной защите доступа опрос контроллеров в уже существующих защищенных сетевых группах и КСК с включенной защитой доступа не производится, добавление новых защищенных групп и контроллеров в уже существующие блокируется.

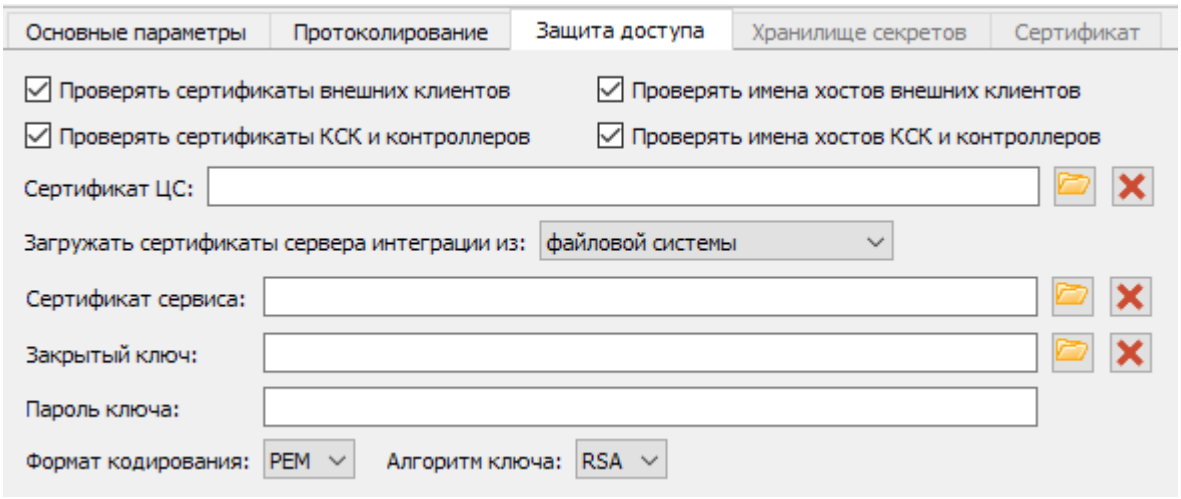

Рисунок 5 – Интерфейс настройки параметров защиты доступа

> ***Внимание!*** *При настройке данного функционала пользователь обязан указать имена файлов SSL сертификата сервиса SDK и закрытого ключа этого сертификата.*

Если установлен флаг «Проверять сертификаты внешних клиентов» или флаг «Проверять сертификаты КСК и контроллеров», то наличие ошибок в сертификате (включая истечение срока действия сертификата) будет вызывать прекращение информационного обмена с клиентом или оборудованием. При отключении флагов проверки имен хостов в случае несоответствия имени субъекта сертификата (CN) или альтернативного имени субъекта (SAN) с адресом клиента или устройства информационный обмен прерываться не будет. Сведения о выявленной ошибке сертификата фиксируются в журнале работы сервиса независимо от состояния флага проверки имени.

Сертификаты центров сертификации (ЦС) загружаются из соответствующих хранилищ операционных систем. Пользователь может добавить свой список сертификатов ЦС. Кнопка отображает окно выбора имени файла, а кнопка – очищает поле с именем файла. Файл сертификата ЦС может содержать несколько сертификатов. Формат загружаемых сертификатов ЦС – PEM.

Сервис может загружать сертификаты как из файловой системы (значение по умолчанию), так и из сервера хранилища секретов, использующего совместимый с HashiCorp Vault HTTP API. Далее рассматривается загрузка сертификатов из файловой системы. Настройка загрузки сертификатов из сервера хранилища секретов рассматривается в п.5.4 и п.5.5.

Сертификаты, загружаемые из файловой системы, могут быть в кодировках PEM или DER, кодировка по умолчанию – PEM. Закрытый ключ может использовать алгоритмы RSA или EC, по умолчанию – RSA. Кроме того, закрытый ключ может храниться в зашифрованном виде с указанием пароля в соответствующем поле ввода данной группы параметров.

Для проверки корректности задания параметров защиты необходимо на панели быстрого доступа главного окна программы нажать кнопку . Пользователю будет отображена форма с результатами проверки и основными свойствами сертификатов сервиса и ЦС.

Измененные значения параметров защиты доступа применяются только после сохранения файла настроек и перезапуска сервиса.

5.4 Настройка параметров взаимодействия с хранилищем секретов

При включенной загрузке сертификатов из сервера хранилища секретов необходимо настроить параметры доступа к серверу. Эти параметры размещены на вкладке «Хранилище секретов» (рисунок 6).

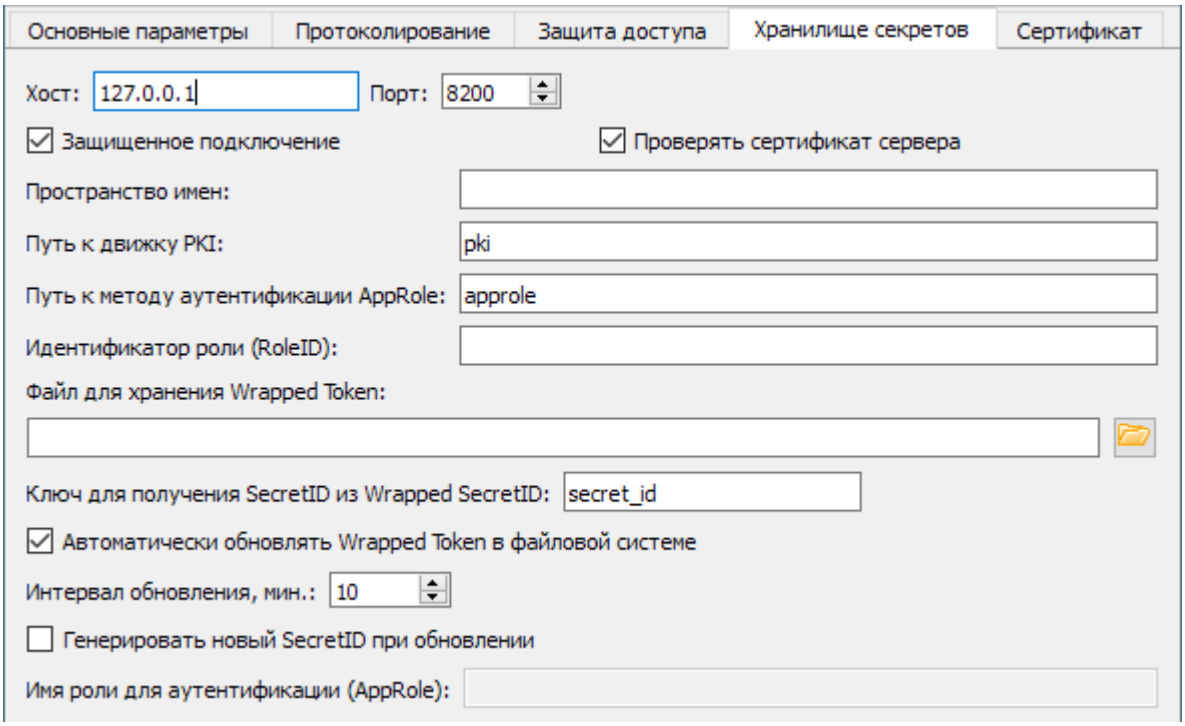

Рисунок 6 – Интерфейс настройки параметров взаимодействия с хранилищем секретов

В поле «Хост» можно указать как IPv4 адрес, так и полное доменное имя хоста с работающим сервером хранилища секретов. По умолчанию настроено подключение к локальному серверу, номер порта – 8200.

Флаг «Защищенное подключение» определяет режим взаимодействия сервиса с сервером хранилища секретов: в обычном (по протоколу http) или в защищенном режиме (по протоколу https). По

умолчанию настроено подключение в защищенном режиме с проверкой сертификата сервера хранилища секретов.

Если сервер хранилища секретов требует защищенное подключение и его сертификат издан ЦС, отсутствующим в хранилище сертификатов ОС, то такой сертификат ЦС (цепочка сертификатов) необходимо указать в программе настройки в соответствии с требованиями п.5.3.

> ***Внимание!*** *Значения параметров, приведенные далее в этом разделе, должны соответствовать конфигурации хранилища секретов. Их значения следует уточнить у администратора сервера хранилища секретов.*

Поле «Пространство имен» необходимо заполнять при подключении к серверу хранилища секретов с включенным функционалом раздельных имен, например, к Enterprise версии Vault. Параметр необязательный, по умолчанию значения нет.

Поле «Путь к движку PKI» содержит URL-путь, по которому по которому будут производиться обращения к движку Public Key Infrastructure в хранилище секретов (используется для получения сертификатов). Параметр обязательный, значение по умолчанию – pki.

При подключении сервиса к хранилищу секретов используется метод аутентификации AppRole по заранее настроенным на сервере хранилища секретов идентификатору роли (RoleID) и секретному ключу роли (SecretID). Идентификатор роли является обязательным параметром и задается в программе настройки. Для получения секретного ключа роли используется так называемый Wrapped Token, предварительно сформированный в хранилище секретов для данного идентификатора роли и сохраненный в файловой системе. Имя файла, содержащего токен для получения секретного ключа, задается пользователем и является обязательным параметром. На момент запуска сервиса в файле должен содержаться корректный и непросроченный токен для получения секретного ключа роли.

> ***Внимание!*** *Файл, содержащий токен для получения секретного ключа роли, должен иметь установленные права на чтение для учетной записи пользователя, от имени которого запускается сервис (п. 4). При включенной настройке автоматического обновления токена требуются права полного доступа.*

Параметр «Ключ для получения SecretID из Wrapped SecretID» должен содержать название ключа в JSON-данных, возвращаемых сервером хранилища секретов в процессе получения секретного ключа роли. Параметр обязательный, значение по умолчанию – secret_id.

Флаг «Автоматически обновлять Wrapped Token в файловой системе» позволяет поддерживать актуальность токена, используемого для получения секретного ключа, средствами сервиса. Если данная опция не включена, то наличие в каталоге файла с пригодным токеном должно поддерживаться внешними средствами. По умолчанию данная опция включена. Периодичность обновления задается в минутах, значение по умолчанию – 10 минут.

При автоматическом обновлении токена, используемого для получения секретного ключа, опционально возможно генерировать новое значение секретного ключа роли на сервере хранилища секретов. При включении данной опции необходимо указать имя роли, используемой для аутентификации (AppRole). Также на сервере хранилища секретов для данной роли должна быть настроена

политика, позволяющая создавать и изменять значение секретного ключа роли. По умолчанию данная опция отключена.

5.5 Настройка параметров сертификатов

При включенной загрузке сертификатов из сервера хранилища секретов также необходимо настроить параметры выпуска сертификатов. Эти параметры размещены на вкладке «Сертификат» (рисунок 7).

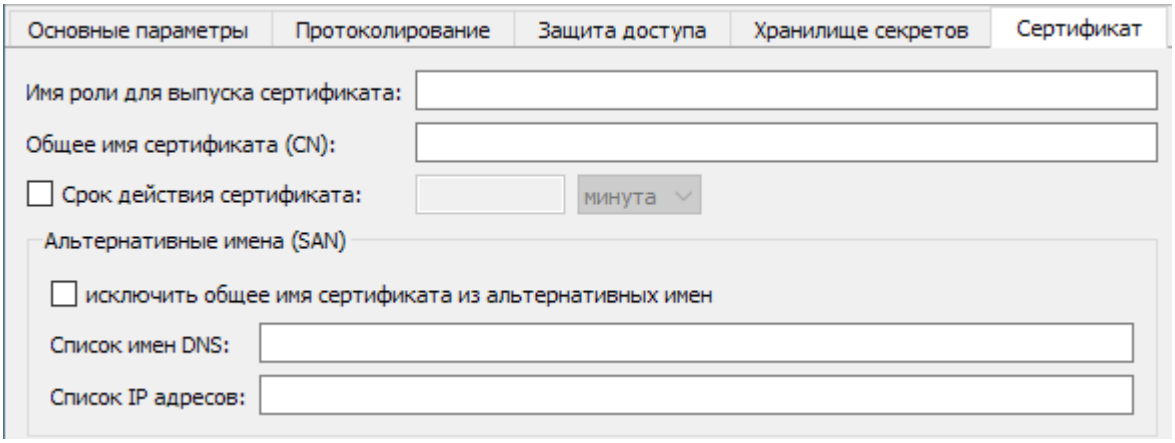

Рисунок 7 – Интерфейс настройки параметров выпуска сертификатов

В поле «Имя роли для выпуска сертификатов» необходимо указать наименование роли, настроенной в движке PKI сервера хранилища секретов и предназначенной для выпуска сертификатов сервера интеграции. Параметр обязательный.

Параметр «Общее имя сертификата» должно содержать значение общего имени (CN). Данное значение является обязательным и должно соответствовать требованиям, заданным в роли для выпуска сертификата. Рекомендуется в качестве общего имени указывать значение полного доменного имени хоста с функционирующим сервером интеграции.

Срок действия выпускаемого сертификата может быть указан явно. При отключенном значении параметра срок действия определяется настройками роли, выпускающей сертификат.

При подключении внешних клиентов к серверу интеграции по IP адресу, а также при наличии в конфигурации системы устройств СКУД Elsys, взаимодействующих с сервером интеграции в защищенном режиме, рекомендуется настроить список IP адресов в группе альтернативных имен (SAN). Данный список может содержать разделенные запятой значения адресов в формате IPv4. Список имен DNS может содержать разделенные запятой полные доменные адреса хоста сервера интеграции.

6 Настройка сервиса SDK консольной утилитой

Имя файла консольной утилиты в ОС Microsoft Windows – ***sdk2_svc_ctl.exe***, в ОС Linux – ***sdk2_svc_ctl***. Исполняемый файл утилиты находится в каталоге сервиса SDK. Для настройки сервиса при помощи консольной утилиты пользователь должен иметь полномочия локального администратора.

Утилита обеспечивает:

- отображение установленных значений основных настраиваемых параметров работы сервиса SDK, пароля СКУД Elsys, а также версии сервиса SDK (действие **SHOW**);
- изменение значений параметров работы сервиса (действие **SET**);
- проверку корректности задания параметров защиты доступа и просмотр основных свойств сертификатов SSL, загружаемых из файловой системы (действие **SSL**).

Каждый из вышеперечисленных пунктов реализуется путем указания соответствующего действия при запуске консольной утилиты. В одном сеансе работы утилиты допускается указывать только одно из вышеперечисленных действий. Для просмотра краткой справки по параметрам вызова утилиты необходимо в командной строке указать опцию ***--help***. Если вместе с опцией помощи указать действие, то будет отображена краткая справка по всем доступным опциям или параметрам данного действия.

Выполнение утилитой любого из действий (кроме выбора просмотра краткой справки) требует авторизации пользователя. Для авторизации необходимо указать пароль доступа к сервису сразу после запуска утилиты. Пароль по умолчанию – ***ElsysAppService***.

```
C:\Program Files (x86)\ES-Prom\ElsysAppService>sdk2_svc_ctl.exe  --help
Использование: sdk2_svc_ctl.exe [параметры] action

Параметры:
  -h, --help  Вывод справки по параметрам командной строки.

Аргументы:
  action      Действие с набором параметров: [SHOW | SET | SSL].
```

Таблица 2 – Параметры режима просмотра

--config	Отображение значений основных параметров работы сервиса.
--devicepass	Отображение пароля СКУД Elsys.
--version	Отображение версии сервиса SDK

Параметры режима просмотра могут указываться в любом сочетании.

Пример указания параметров командной строки для вывода значений основных параметров работы и версии сервиса:

```
sdk2_svc_ctl show --config --version
```

Таблица 3 – Параметры режима установки значений

Основные параметры работы сервиса (п. 5.1)	
--host	IP адрес сетевого сервиса. Для приема входящих пакетов на всех доступных интерфейсах нужно указать адрес 0.0.0.0 или ANY.
--httpport	Номер порта HTTP сервиса.

--cfgport	Номер порта сервиса хранения файла конфигурации.
--netgroupport	Номер порта сервиса опроса сетевых групп.
--searchport	Номер порта сервиса поиска контроллеров.
--comport	Имя последовательного интерфейса ПК, используемого для опроса контроллеров в линии связи RS-485 сервера интеграции.
--disablecom	Отключить опрос контроллеров в линии связи сервера интеграции. При установке данного параметра значение параметра comport игнорируется. Параметр указывается без значения.
--servicepass	Пароль доступа к сервису SDK. Параметр указывается без значения. Новое значение пароля будет запрошено программой настройки.
--devicepass	Пароль СКУД Elsys. Параметр указывается без значения. Новое значение пароля будет запрошено программой настройки.
--usessl	Флаг использования защищенного режима обмена с внешними клиентами и устройствами СКУД Elsys. Допустимые значения – yes/no, true/false или 1/0. При отключении данного параметра игнорируются сохраненные в файле настроек работы сервиса значения параметров защищенного обмена, взаимодействия с хранилищем секретов и загрузки сертификатов из хранилища секретов.
Параметры протоколирования работы сервиса (п. 5.2)	
--logpath	Расположение журналов работы сервиса и отладочных журналов.
--debuglog	Управление записью отладочных сообщений в журнале работы сервиса (общем логе). Допустимые значения – yes/no, true/false или 1/0.
--debugelsys	Управление отладочным режимом сервера оборудования Elsys. Допустимые значения – yes/no, true/false или 1/0.
Общие параметры защищенного обмена (п. 5.3)	
--verifyclientpeer	Флаг проверки сертификатов клиентов. Допустимые значения – yes/no, true/false или 1/0.
--verifyclienthost	Флаг проверки имен хостов в сертификатах клиентов. Допустимые значения – yes/no, true/false или 1/0.
--verifydevicepeer	Флаг проверки сертификатов устройств СКУД Elsys. Допустимые значения – yes/no, true/false или 1/0.
--verifydevicehost	Флаг проверки имен хостов в сертификатах устройств СКУД Elsys. Допустимые значения – yes/no, true/false или 1/0.
--cacert	Имя файла, содержащего сертификат (цепочку сертификатов) ЦС.
--certsource	Источник сертификата сервера интеграции. Допустимые значения – file (файловая система) или vault (хранилище секретов).
--sslcert	Имя файла сертификата сервера при загрузке сертификатов из файловой системы.
--sslkey	Имя файла закрытого ключа сервера при загрузке сертификатов из файловой системы.
--keypass	Пароль шифрования закрытого ключа при загрузке сертификатов из файловой системы. Параметр указывается без значения. Значение пароля будет запрошено программой настройки.
--encoding	Формат кодирования сертификата при загрузке сертификатов из файловой системы.
--algorithm	Алгоритм закрытого ключа при загрузке сертификатов из файловой системы.
Параметры взаимодействия с хранилищем секретов (п. 5.4)	
--vaulthost	Полное доменное имя хоста или IPv4 адрес сервера хранилища секретов.
--vaultport	Номер порта сервера хранилища секретов.
--vaultusessl	Подключение к серверу хранилища секретов по защищенному каналу. Допустимые значения – yes/no, true/false или 1/0.

--verifyvaultpeer	Проверять сертификат сервера при подключении к хранилищу секретов. Допустимые значения – yes/no, true/false или 1/0.
--vaultnamespace	Пространство имен хранилища секретов.
--vaultpkipath	Путь к движку PKI хранилища секретов.
--vaultapprolepath	Путь к методу аутентификации AppRole хранилища секретов.
--authroleid	Идентификатор роли (RoleID).
--wrappedtokenfile	Имя файла для хранения Wrapped Token.
--refreshwrappedtoken	Автоматически обновлять Wrapped Token в файловой системе. Допустимые значения – yes/no, true/false или 1/0.
--tokenrefreshinterval	Интервал обновления Wrapped Token в файловой системе. Задается в минутах, допустимый диапазон значений – 1...7200.
--createsecretid	Генерировать новый SecretID при обновлении Wrapped Token. Допустимые значения – yes/no, true/false или 1/0.
--approlename	Имя роли для аутентификации (AppRole).
Параметры настройки загрузки сертификатов из хранилища секретов (п. 5.5)	
--issuername	Имя роли для выпуска сертификата.
--certcn	Общее имя сертификата (CN).
--excludecommonname	Исключить общее имя сертификата из альтернативных имен. Допустимые значения – yes/no, true/false или 1/0.
--dnssan	Список имен DNS для альтернативного имени субъекта (DNS SAN). Имена в списке разделяются запятыми.
--ipsan	Список IP адресов для альтернативного имени субъекта (IP SAN). Адреса в списке разделяются запятыми.
--certttl	Срок действия сертификата, запрашиваемого в хранилище секретов.
--ttlunit	Единица времени для срока действия сертификата. Допустимые значения – m (минуты), h (часы) или d (дни).

Значения параметров задаются после их имени через пробел, допускается указывать значения параметров сразу после имени и символа =. Значения параметров, содержащие пробелы, должны указываться в кавычках. Имена действий и параметров не являются регистрозависимыми. Имена файлов, коммуникационного интерфейса и каталога размещения журналов, используемые в качестве значений параметров, указываются в соответствии с требованиями ОС. Значения паролей в командной строке не указываются, они будут запрошены в ходе работы утилиты настройки.

Значения параметров должны указываться в соответствии с требованиями в п.5. Параметры работы сервиса, не указанные в командной строке при запуске консольной утилиты, не изменяются.

После изменения параметров необходимо перезапустить сервис SDK.

Пример указания параметров командной строки для установки значений:

```
sdk2_svc_ctl set --host any --disablecom --servicepass
--debuglog yes --debugelsys no –usessl yes –certsource file
--sslcert ssl/server.crt
--sslkey ssl/server.key --keypass --cacert ssl/cacert.crt
--veryfyclientpeer yes --verifydevicepeer yes
```

В этом примере устанавливается режим приема запросов от внешних клиентов на всех доступных сетевых интерфейсах, отключается опрос контроллеров в линии связи RS-485 сервера интеграции, изменяется пароль доступа внешних клиентов к сервису SDK, включается режим расширенного про-

токолирования событий в журнал работы сервиса, отключается отладочный режим сервера оборудования Elsys и включается защита доступа. Файлы сертификатов и закрытого ключа загружаются из файловой системы и расположены в подкаталоге ssl рабочего каталога сервиса SDK. Формат файлов – PEM, закрытый ключ сгенерирован по алгоритму RSA и зашифрован с паролем. Также устанавливается проверка сертификатов внешних клиентов и устройств СКУД Elsys. Новое значение пароля доступа и пароль закрытого ключа будут запрошены у пользователя после успешного прохождения авторизации.

Для проверки корректности задания параметров защиты доступа и просмотра основных свойств сертификатов, загружаемых из файловой системы, необходимо указать при запуске консольной утилиты в командной строке действие **SSL**. Данное действие не имеет дополнительных параметров.