КОД БЕЗОПАСНОСТИ

Средство защиты информации

Secret Net Studio

Руководство администратора

Настройка и эксплуатация. Шифрование сетевого трафика

RU.88338853.501400.001 91 8

Почтовый адрес:	**115127, Россия, Москва, а/я 66** **ООО "Код Безопасности"**
Телефон:	**8 495 982-30-20**
E-mail:	**info@securitycode.ru**
Web:	**http://www.securitycode.ru**

Оглавление

Список сокращений

AD	Active Directory
FAT	File Allocation Table
IEEE	Institute of Electrical and Electronics Engineers
LFN	Long File Name
MMC	Microsoft Management Console
NTFS	New Technology File System
PCMCIA	Personal Computer Memory Card International Association
PIN	Personal Identification Number
PKI	Public Key Infrastructure
RPC	Remote Procedure Call
RTF	Rich Text Format
TCP	Transmission Control Protocol
USB	Universal Serial Bus
АРМ	Автоматизированное рабочее место
БД	База данных
ЗПС	Замкнутая программная среда
КЦ	Контроль целостности
ЛБД	Локальная база данных
МД	Модель данных
ОС	Операционная система
ПАК	Программно-аппаратный комплекс
ПО	Программное обеспечение
ЦБД	Центральная база данных

Введение

Данное руководство предназначено для администраторов изделия "Средство защиты информации Secret Net Studio" RU.88338853.501400.001 (далее — Secret Net Studio, система защиты, изделие). В нем содержатся сведения, необходимые администраторам для настройки и управления механизмом шифрования сетевого трафика при совместной работе с аппаратно-программным комплексом шифрования "Континент". Перед изучением данного руководства необходимо ознакомиться с документами [**1**], [**3**].

Условные обозначения

В руководстве для выделения некоторых элементов текста используется ряд условных обозначений.

Внутренние ссылки обычно содержат указание на номер страницы с нужными сведениями.

Важная и дополнительная информация оформлена в виде примечаний. Степень важности содержащихся в них сведений отображают пиктограммы на полях.

- Так обозначается дополнительная информация, которая может содержать примеры, ссылки на другие документы или другие части этого руководства.

- Такой пиктограммой выделяется важная информация, которую необходимо принять во внимание.

- Эта пиктограмма сопровождает информацию предостерегающего характера.

Исключения. Примечания могут не сопровождаться пиктограммами. А на полях, помимо пиктограмм примечаний, могут быть приведены и другие графические элементы, например, изображения кнопок, действия с которыми упомянуты в тексте расположенного рядом абзаца.

Другие источники информации

Сайт в интернете. Вы можете посетить сайт компании "Код Безопасности" (http://www.securitycode.ru/) или связаться с представителями компании по электронной почте (support@securitycode.ru).

Учебные курсы. Освоить аппаратные и программные продукты компании "Код Безопасности" можно в авторизованных учебных центрах. Перечень учебных центров и условия обучения представлены на сайте компании http://www.securitycode.ru/company/education/training-courses/. Связаться с представителем компании по вопросам организации обучения можно по электронной почте (education@securitycode.ru).

Глава 1
Общие сведения

Назначение и основные функции

В состав клиентского ПО системы Secret Net Studio включен VPN клиент, предназначенный для организации доступа удаленных пользователей по защищенному каналу к ресурсам, защищаемым средствами АПКШ "Континент". При подключении к серверу доступа АПКШ "Континент" обеспечивается криптографическая защита канала связи. На стороне сервера доступа VPN клиент системы Secret Net Studio рассматривается как отдельный абонентский пункт (АП).

Основные функции абонентского пункта:

- аутентификация сервера доступа на основе технологии открытых ключей;
- формирование ключевой информации, необходимой для организации сессии;
- установление защищенного соединения между удаленным пользователем и сервером доступа;
- генерация закрытого ключа и формирование на его основе открытого с созданием запроса на получение сертификата стороннего удостоверяющего центра;
- импорт сертификатов;
- регистрация событий, связанных с работой абонентского пункта, в журнале Secret Net Studio.

Сертификаты открытых ключей

Сертификат — это цифровой документ, содержащий информацию о владельце ключа, сведения об открытом ключе, его назначении и области применения, название центра сертификации и т. д. Сертификат заверяется электронной цифровой подписью удостоверяющего центра сертификации.

В зависимости от используемого стандарта существуют различные форматы сертификатов. Абонентский пункт может работать со следующими форматами:

- сертификаты в кодировках Distinguished Encoding Rules (DER) и Base-64 (перевод двоичных данных в читаемый текст). Файл, содержащий один сертификат, обычно имеет расширение *.cer. В файлах с таким расширением хранятся сертификаты пользователя (как правило) и реже — сертификаты корневого центра сертификации;
- сертификаты в формате PKCS 7 (обычно с расширением *.p7b). Могут содержать несколько сертификатов, например, цепочку подтверждающих друг друга сертификатов. В таком формате хранятся сертификаты корневого центра сертификации.

Сертификаты в файлах с расширением *.cer и *.p7b соответствуют стандарту X.509v3 Международного телекоммуникационного союза (ITU-T).

Запрос на получение сертификата создается пользователем средствами абонентского пункта по требованию администратора безопасности. Одновременно с запросом средствами криптопровайдера генерируется закрытый ключ пользователя. Запрос в виде файла сохраняется в указанную пользователем папку, ключевой контейнер с закрытым ключом сохраняется на выбираемом ключевом носителе.

Система автоматически отслеживает статус сертификата — действителен или недействителен. Недействительным сертификат может быть признан по следующим причинам:

- срок действия сертификата не наступил;

- срок действия сертификата истек;
- сертификат отозван удостоверяющим центром;
- отсутствует сертификат удостоверяющего центра.

Необходимо использовать только действительные сертификаты.

Статус сертификатов, выданных внешним удостоверяющим центром, проверяется по списку отозванных сертификатов этого центра (файл с расширением *.crl). Если список отозванных сертификатов на компьютере отсутствует или просрочен, то проверка сертификатов не выполняется.

Внимание! При использовании сертификатов внешнего удостоверяющего центра необходимо средствами Windows установить на компьютере список отозванных сертификатов этого центра и периодически проводить его обновление.

Привилегия для управления настройками подключений

В системе предусмотрена привилегия управления настройками подключений к серверу доступа. Данная привилегия предоставляет пользователям возможности создания новых подключений к серверу доступа и настройки параметров подключений.

По умолчанию привилегией обладают пользователи, входящие в локальную группу администраторов.

Ниже приводится описание процедуры централизованной настройки при работе с программой управления в централизованном режиме. Локальная настройка выполняется аналогично с использованием программы управления в локальном режиме. Сведения об использовании программы управления см. в документе [**4**].

Для предоставления привилегии:

1. В программе управления откройте панель "Компьютеры" и выберите объект, для которого необходимо настроить параметры. Включите отображение панели свойств с помощью команды в контекстном меню объекта. В панели свойств перейдите на вкладку "Настройки" и загрузите параметры с сервера безопасности.
2. В разделе "Политики" перейдите к группе параметров "Шифрование трафика".
3. Для параметра "Учетные записи с привилегией управления настройками подключений к серверу доступа" отредактируйте список пользователей и групп пользователей, которым предоставлена привилегия.
4. Нажмите кнопку "Применить" в верхней части вкладки "Настройки".

Меню управления абонентским пунктом

Управление абонентским пунктом выполняют с помощью специального меню.

Для вызова меню управления абонентским пунктом:

- Наведите указатель мыши на пиктограмму абонентского пункта, расположенную на панели задач Windows, и нажмите правую кнопку мыши.

  Цвет пиктограммы абонентского пункта указывает на наличие или отсутствие соединения с сервером доступа:

	Серый	Соединение не установлено
	Зеленый	Соединение установлено

  На экране появится меню управления абонентским пунктом.

Табл.1 Команды меню управления абонентским пунктом

Команда	Описание
Подключить	Запускает процедуру установления соединения абонентского пункта с сервером доступа
Разорвать	Запускает процедуру разрыва соединения абонентского пункта с сервером доступа
Настройка > Параметры...	Вызывает на экран окно настройки абонентского пункта для выполнения операций с сертификатами и настройки подключений
Настройка > Запросить новый сертификат...	Запускает процедуру создания запроса сертификата
Настройка > Импорт сертификата...	Запускает процедуру импорта сертификата из файла в хранилище сертификатов на компьютере
Помощь > Справка	Вызывает на экран окно оперативной справочной системы
Помощь > О программе...	Вызывает на экран диалог со сведениями о номере версии программы и авторских правах
Выход	Удаляет пиктограмму абонентского пункта из панели задач Windows

Примечание. Команда "Настройка > Параметры..." доступна только пользователю, обладающему привилегией на управление настройками подключений к серверу доступа. По умолчанию такой привилегией обладает пользователь, входящий в группу локальных администраторов компьютера.

Глава 2
Настройка абонентского пункта

Порядок настройки

Для подготовки абонентского пункта к работе:

1. При необходимости использования криптопровайдера "КриптоПро CSP" установите и настройте его. Процедуры установки и настройки подробно рассматриваются в эксплуатационной документации на данный программный продукт.
2. Установите сертификаты, необходимые для работы. Предусмотрено два варианта получения и установки сертификатов.

   Если сертификаты передаются в составе конфигурационного файла — создайте новое подключение, используя настройки конфигурационного файла (см. стр.**16**).

   Если настройки выполняются без использования конфигурационного файла, выполните следующее:

   - создайте файл запроса на получение сертификата пользователя (см. стр.**9**);
   - установите полученные сертификаты на компьютер (см. стр.**10**);
   - настройте параметры подключения к серверу доступа (см. стр.**13**);
   - настройте аутентификацию сервера доступа (см. стр.**11**).
3. Установите соединение с сервером доступа (см. стр. **19**) и попробуйте подключиться к какому- либо доступному ресурсу, находящемуся в защищенном сегменте корпоративной сети.

   Если пробное соединение с сервером установлено успешно и подключение к ресурсу корпоративной сети возможно — значит, все подготовительные действия выполнены правильно. С этого момента абонентский пункт готов к работе.

Управление сертификатами

Создание запроса на получение сертификата пользователя

Перед тем как приступить к созданию запроса, приготовьте чистый отформатированный ключевой носитель для записи ключевого контейнера.

Для создания запроса:

1. Вызовите контекстное меню пиктограммы абонентского пункта, расположенной на панели задач Windows, и активируйте команду "Настройка > Запросить новый сертификат...".

   На экране появится диалог "Параметры сертификата пользователя" мастера запроса сертификата.
2. Заполните поля диалога и нажмите кнопку <Далее>.

   На экране появится диалог "Свойства поставщика служб шифрования".
3. Укажите нужные сведения и нажмите кнопку <Далее>.

Поле	Описание
Криптопровайдер	Наименование поставщика служб шифрования
Менеджер ключевых контейнеров	Хранилище сертификатов, в котором должен храниться сертификат

Поле	Описание
Имя ключевого контейнера	Наименование ключевого контейнера для сохранения закрытого ключа пользователя. По умолчанию формируется из имени пользователя и даты создания запроса

На экране появится диалог "Имя файла".

4. Укажите нужные сведения и нажмите кнопку <Далее>.

Поле	Описание
Имя файла для запроса сертификата	Полное имя файла для запроса сертификата. Для выбора используйте кнопку "Обзор..."
Формат файла	Формат файла запроса
Подготовить бланк запроса на сертификат	При наличии отметки формируется файл HTML для печати запроса в бумажной форме

На экране появится завершающий диалог мастера запроса сертификата, содержащий введенные сведения.

5. Проверьте указанные сведения и нажмите кнопку <Готово>.

Если в качестве криптопровайдера был указан "КриптоПро CSP", на экране появится предложение вставить и затем указать носитель для хранения ключей. Перейдите к п. **6**.

Если в качестве криптопровайдера был указан "Код Безопасности CSP", на экране появится окно, предназначенное для накопления энтропии. Перейдите к п. **9**.

Примечание. Если используемым датчиком случайных чисел является датчик ПАК "Соболь", набор энтропии выполняется автоматически и на экране не отображается.

6. Вставьте приготовленный ключевой носитель и выберите его в списке.

На экране появится окно, предназначенное для накопления энтропии.

7. Следуйте указаниям инструкции на экране и дождитесь завершения накопления энтропии.

На экране появится диалог задания пароля для доступа к ключевому контейнеру.

8. Задайте пароль и нажмите кнопку "OK".

В указанной папке будет сформирован файл запроса сертификата, а на носителе будет записан ключевой контейнер. Перейдите к п. **12**.

9. Следуйте указаниям инструкции и дождитесь завершения накопления энтропии.

На экране появится диалог задания пароля для доступа к ключевому контейнеру.

10. Задайте пароль и нажмите кнопку "OK".

На экране появится диалог выбора носителя.

11. Вставьте приготовленный ключевой носитель, выберите его в списке и нажмите кнопку "OK".

В указанной папке будет сформирован файл запроса сертификата, а на носителе будет записан ключевой контейнер.

Дождитесь сообщения о завершении создания запроса и закройте его.

12. Извлеките ключевой носитель, а файл запроса передайте администратору.

Импорт сертификата

При импорте сертификата в формате PKCS 7 (файл с расширением *.p7b) одновременно осуществляется установка как сертификата пользователя, так и корневого сертификата.

При наличии двух отдельных файлов с сертификатом пользователя (*.cer) и корневым сертификатом (*.p7b) их устанавливают в произвольном порядке.

Процедура импорта используется также в тех случаях, когда сертификат пользователя уже установлен и необходимо отдельно установить только корневой сертификат.

Для импорта сертификата:

1. Вызовите контекстное меню пиктограммы абонентского пункта, расположенной на панели задач Windows, и выберите команду "Настройка > Импорт сертификата...".

   На экране появится диалог "Импортируемый файл" мастера импорта сертификата.

2. Укажите имя файла сертификата и нажмите кнопку <Далее>. Для выбора файла в стандартном диалоге используйте кнопку "Обзор".

   На экране появится диалог "Хранилище сертификатов".

3. Заполните поля диалога и нажмите кнопку <Далее>.

Поле	Описание
Менеджер сертификатов	Хранилище сертификатов, в котором будет храниться сертификат
Автоматически выбрать хранилище на основе типа сертификата	Автоматическое определение хранилища сертификатов
Поместить все сертификаты в следующее хранилище	Ручное определение хранилища сертификатов. Для выбора нужного хранилища используйте кнопку "Обзор"

   На экране появится диалог "Контейнер закрытого ключа сертификата".

4. Выберите нужный ключевой контейнер и нажмите кнопку <Далее>.

   Примечание. Если ключевым носителем является устройство Токен, защищенное PIN-кодом, а в качестве криптопровайдера используется "Код Безопасности CSP", ключевой контейнер может не появиться в списке. Необходимо ввести PIN-код с помощью программы Код Безопасности CSP (см. стр. 20).

   На экране появится завершающий диалог мастера импорта сертификата, содержащий введенные сведения.

5. Проверьте указанные сведения и нажмите кнопку <Готово>.

   На экране появится сообщение об успешной установке сертификата.

6. Закройте окно сообщения.

Настройка аутентификации сервера

Серверный сертификат используется в процедуре взаимной аутентификации абонентского пункта и сервера доступа и подтверждает принадлежность открытого ключа удостоверяющему центру.

Примечание. Открытый ключ используется для проверки электронной подписи удостоверяющего центра в сертификате сервера доступа.

Для подключения к серверу доступа необходимо, чтобы на абонентском пункте были установлены серверный сертификат и удостоверяющий его корневой сертификат, полученные от администратора сервера доступа.

Установка сертификатов (серверного или корневого) выполняется с помощью процедуры импорта, в результате которой импортируемый сертификат помещается в хранилище компьютера.

Если на абонентском пункте создавалось новое подключение с использованием конфигурационного файла (см. стр. 16), установка серверного сертификата и помещение его в хранилище компьютера выполняются автоматически при создании такого подключения.

Если подключения с использованием конфигурационного файла не создавались, необходимо выполнить процедуру установки серверного и корневого сертификатов.

Для установки сертификата:

1. Вызовите контекстное меню пиктограммы абонентского пункта, расположенной на панели задач Windows, и выберите команду "Настройка > Параметры...".

   На экране появится окно настройки параметров АП.

2. В левой части окна выберите "Аутентификация сервера> Сертификаты" и перейдите к вкладке "Корневые"/"Серверные".

   На вкладке представлен перечень установленных корневых/серверных сертификатов.

3. Для установки сертификата нажмите кнопку "Добавить...".

   На экране появится стандартный диалог выбора файла.

4. Укажите путь к файлу сертификата и нажмите кнопку "ОК".

   Будет выполнен импорт сертификата и установка его в хранилище компьютера.

Для просмотра свойств или удаления выбранного в списке сертификата используйте кнопки "Свойства" и "Удалить".

Работа с корневыми и серверными сертификатами

Корневой и серверный сертификаты используются в процедуре взаимной аутентификации абонентского пункта и сервера доступа и подтверждают принадлежность открытого ключа удостоверяющему центру.

Примечание. Открытый ключ используется для проверки электронной подписи удостоверяющего центра в сертификате сервера доступа.

Работа с сертификатами предусматривает выполнение следующих операций:

- Импорт. Импортируемый сертификат (корневой или серверный) помещается в хранилище и добавляется в список зарегистрированных сертификатов абонентского пункта. Предварительно необходимо получить файл сертификата у администратора сервера доступа и сохранить его на внешнем носителе или на жестком диске компьютера.
- Удаление. Сертификат удаляется из списка зарегистрированных сертификатов и из хранилища.
- Просмотр свойств зарегистрированного сертификата.

Для работы с сертификатами:

1. Вызовите контекстное меню пиктограммы абонентского пункта, расположенной на панели задач Windows, и выберите команду "Настройка > Параметры...".

   На экране появится окно настройки параметров АП.

2. В левой части окна выберите "Аутентификация > Сертификаты" и перейдите к вкладке "Корневые"/"Серверные".

   На вкладке представлен перечень зарегистрированных корневых/серверных сертификатов.

3. Для выполнения нужной операции используйте следующие кнопки.

Добавить...	Запускает процедуру импорта сертификата и открывает стандартный диалог Windows выбора файла
Удалить	Удаляет из списка выбранный сертификат
Свойства	Открывает стандартный диалог свойств выбранного сертификата

Настройка подключений

Настройка параметров подключения

После установки программного обеспечения абонентского пункта автоматически создается подключение к серверу доступа под названием "Континент VPN". Для использования подключения "Континент VPN" требуется настройка его параметров.

Для настройки параметров подключения:

1. Вызовите контекстное меню пиктограммы абонентского пункта, расположенной на панели задач Windows, и выберите команду "Настройка > Параметры...".

   На экране появится окно настройки параметров АП.

2. В левой части окна раскройте группу "Профили подключений".

   В группе "Профили подключений" приведен список всех используемых подключений.

   Примечание. После установки ПО АП, если новые подключения не создавались, в списке будет одно созданное по умолчанию подключение "Континент VPN".

3. Выберите в списке нужное подключение.

   В правой части окна отобразятся параметры выбранного подключения, распределенные по вкладкам.

Табл.2 Параметры подключения

Вкладка/ Параметр	Описание
Общие	
Адрес	Сетевое имя или IP-адрес сервера доступа
Порт	Порт сервера доступа для обмена сообщениями с абонентским пунктом
Имя подключения	Наименование подключения
Протокол	Тип протокола, по которому абонентский пункт должен подключаться к серверу доступа
Пользователь	Имя пользователя или группы пользователей, имеющих доступ к данному подключению
Аутентификация пользователя	
Сертификат	Имя сертификата пользователя, с которым будет осуществляться подключение к серверу доступа. Для выбора сертификата используйте кнопку "Выбрать"
Выдавать предупреждение об окончании срока действия сертификата	За указанное количество дней до окончания срока действия сертификата пользователю будет выводиться соответствующее предупреждение
Ключевой контейнер	Ключевой контейнер сертификата пользователя. Поле заполняется автоматически после выбора сертификата
Параметры	
Подключиться при разрыве связи	Если отметка установлена, то соединение с сервером доступа в случае разрыва связи будет устанавливаться автоматически. Количество попыток соединений в случае разрыва связи указано в поле "Число попыток"

Вкладка/ Параметр	Описание
Число попыток	Количество автоматических попыток подключения к серверу доступа без участия пользователя. Если за указанное число попыток соединение не будет установлено, на экране появится сообщение об ошибке, после чего пользователь может повторить попытку подключения
Интервал между попытками	Интервал времени, по прошествии которого необходимо повторить попытку соединения
Вариант активации подключения	Активация подключения выполняется по требованию пользователя или автоматически после входа пользователя в Windows
Прокси	
Не использовать прокси	Подключение через прокси-сервер не используется
Ручная настройка прокси	Параметры подключения через прокси-сервер задаются вручную
Сервер	Сетевое имя или IP-адрес прокси-сервера
Порт	Порт прокси-сервера
Тип	Тип аутентификации при подключении через прокси-сервер: • без аутентификации; • Basic; • Kerberos; • TLM; • Negotiate
Пользователь	Имя пользователя для аутентификации на прокси-сервере
Пароль	Пароль пользователя для аутентификации на прокси-сервере

4. Установите необходимые значения параметров и нажмите кнопку "Применить".

Создание нового подключения

Если необходимо подключение абонентского пункта к нескольким серверам доступа, для каждого из них должно быть создано и настроено отдельное подключение.

Если средствами абонентского пункта к серверу доступа должны подключаться несколько пользователей и каждый из них должен использовать свой сертификат, для каждого такого пользователя необходимо создать собственное отдельное подключение. При этом должно обеспечиваться разграничение доступа пользователей к подключениям. Разграничение доступа к подключениям осуществляется с помощью параметра "Пользователь" в окне настройки подключения (см. стр.13).

Предусмотрено три варианта создания нового подключения:

- создание подключения, включающее в себя настройку всех его параметров;
- копирование уже имеющегося подключения и последующее редактирование одного или нескольких параметров;
- создание подключения на основе конфигурационного файла, полученного от администратора сервера доступа.

Второй вариант рекомендуется использовать в тех случаях, когда в настройки параметров необходимо внести незначительные изменения. Например, если

необходимо использовать сертификат для подключения к двум серверам доступа. В этом случае достаточно скопировать уже настроенное подключение к первому серверу доступа и в настройках изменить сетевое имя или IP-адрес.

Третий вариант используется в том случае, когда при регистрации нового пользователя на сервере доступа администратор СД сформировал конфигурационный файл. Конфигурационный файл включает в себя основные настройки, необходимые для подключения пользователя абонентского пункта к серверу доступа. Описание создания подключения на основе конфигурационного файла приведено далее (см. стр.**16**).

Для создания нового подключения и настройки его параметров:

1. Вызовите контекстное меню пиктограммы абонентского пункта, расположенной на панели задач Windows, и выберите команду "Настройка > Параметры...".

   На экране появится окно настройки параметров АП.
2. В правой части окна нажмите кнопку "Новое подключение".

   В списке профилей подключений появится новое подключение.
3. В правой части окна на вкладке "Подключение" укажите нужные значения параметров и перейдите на вкладку "Аутентификация пользователя".
4. Укажите сертификат пользователя, который должен использоваться при аутентификации для данного подключения.
   - Для выбора сертификата, находящегося в хранилище личных сертификатов учетной записи, нажмите кнопку "Выбрать".
   - Для выбора сертификата, находящегося в хранилище личных сертификатов компьютера, нажмите на стрелку, расположенную справа от кнопки "Выбрать", и активируйте пункт "Сертификаты компьютера".

     На вкладке "Аутентификация" отобразятся выбранный сертификат и имя связанного с ним ключевого контейнера.
5. Установите отметку, если необходимо выдавать предупреждение об окончании срока действия сертификата, и укажите количество дней.
6. Перейдите на вкладку "Параметры" и введите нужные значения.
7. При необходимости использовать прокси-сервер перейдите на вкладку "Прокси" и выполните настройку.
8. Для сохранения установленных значений параметров нажмите кнопку "Применить".

Примечание. Чтобы сохранить значения параметров и закрыть окно настроек АП, нажмите кнопку "ОК".

Для копирования подключения:

1. Вызовите контекстное меню пиктограммы абонентского пункта, расположенной на панели задач Windows, и выберите команду "Настройка > Параметры...".

   На экране появится окно настройки параметров АП.
2. В левой части окна раскройте группу "Профили подключений", выберите в списке подключение и в правой части окна нажмите кнопку вызова меню, расположенную справа от кнопки "Новое подключение".

   Появится список дополнительных команд.
3. Выберите команду "Копировать подключение".

   В левой части окна в списке появится копия выбранного подключения.
4. Введите в правой части окна на вкладке "Общие" новое имя для данного подключения и далее отредактируйте значение нужного параметра (описание параметров см. стр.**13**).
5. Для сохранения изменений нажмите кнопку "Применить".

Создание подключения на основе конфигурационного файла

Пользователь, имеющий привилегию управления настройками подключений к серверу доступа, может создавать новые подключения на основе конфигурационного файла. Такую привилегию пользователю может предоставить локальный администратор компьютера.

Перед началом создания подключения получите у администратора сервера доступа защищенный паролем конфигурационный файл с сертификатами и ключами пользователя.

> **Примечание.** Если при формировании ключей используется криптопровайдер "Код Безопасности CSP", ключи пользователя сохраняются в конфигурационном файле. Если в качестве криптопровайдера используется "КриптоПРО CSP", ключи сохраняются на внешнем носителе.

Для создания подключения при наличии привилегии:

1. Вызовите контекстное меню пиктограммы абонентского пункта, расположенной на панели задач Windows, и выберите команду "Настройка > Параметры...".

   На экране появится окно настройки параметров АП.

2. В левой части окна раскройте группу "Профили подключений" и в правой части окна нажмите кнопку вызова меню, расположенную справа от кнопки "Новое подключение".

   Появится список дополнительных команд.

3. Выберите команду "Импорт настроек подключения".

   На экране появится стандартный диалог выбора файла.

4. Укажите конфигурационный файл пользователя и нажмите кнопку "Открыть".

   На экране появится диалог ввода пароля для расшифрования конфигурационного файла.

5. Введите пароль и нажмите кнопку "ОК".

   На экране появится диалог ввода пароля для доступа к ключевому контейнеру пользователя.

6. Введите пароль и при необходимости установите отметку в поле "Запомнить пароль".

   Нажмите кнопку "ОК".

   На экране появится диалог смены пароля доступа к ключевому контейнеру.

7. Введите и подтвердите новый пароль и нажмите кнопку "ОК".

   На экране появится диалог выбора ключевого носителя для сохранения ключевого контейнера пользователя.

   > **Примечание.** Ключевой контейнер может храниться на внешнем носителе или в реестре Windows.

8. Выберите ключевой носитель и нажмите кнопку "ОК".

   > **Внимание!** Если ключевой носитель защищен PIN-кодом, введите его.

9. Если корневой сертификат на компьютер не устанавливался, на экране появится запрос на его установку. В этом случае подтвердите необходимость установки в диалоге запроса.

   В списке профилей появится новое подключение с настройками, указанными в конфигурационном файле.

Для создания подключения при отсутствии у пользователя привилегии:

1. Выполните процедуру предоставления пользователю привилегии на управление настройками подключений (см. стр.7).

Примечание. Если привилегию необходимо предоставить в локальном режиме работы программы управления в сеансе пользователя, который не обладает правами локального администратора компьютера, выполните запуск программы следующим образом:

- Вызовите контекстное меню ярлыка запуска "Локальный центр управления" и выберите команду "Запуск от имени администратора".
- При появлении запроса на ввод учетных данных введите имя и пароль администратора.

2. После сохранения изменений в списке учетных записей с привилегией пригласите к компьютеру пользователя, для которого должно быть создано подключение. Выполните совместно с ним процедуру создания подключения (см. выше).
3. Вернитесь к программе управления и удалите пользователя из списка учетных записей, обладающих привилегией.
4. Нажмите кнопку "Применить" в верхней части вкладки "Настройки", после чего закройте программу управления.

Настройка режима подключения до входа в систему

Предусмотрен режим работы абонентского пункта, когда подключение к серверу доступа осуществляется до входа пользователя в операционную систему.

После входа пользователя в систему к компьютеру будут применены параметры групповых политик домена.

Для настройки режима:

1. Поместите сертификат пользователя в хранилище личных сертификатов компьютера. Данную операцию можно выполнить стандартными средствами ОС Windows или импортированием сертификата средствами абонентского пункта (см. стр.**10**).
2. Выполните привязку сертификата пользователя к подключению. Для этого в настройках параметров подключения (см. стр.**13**) на вкладке "Аутентификация пользователя" укажите сертификат пользователя, помещенный в хранилище личных сертификатов компьютера.
3. Выполните контрольное подключение пользователя к серверу доступа (см. стр.**19**). При необходимости при подключении сохраните защитный PIN-код внешнего носителя (если используется) и пароль доступа к ключевому контейнеру.
4. Отключите абонентский пункт от сервера доступа и перезагрузите компьютер.

   После перезагрузки компьютера в окне выбора пользователя для входа в ОС Windows появится кнопка "Вход в сеть".

Примечание. Вид кнопки и ее расположение в окне зависят от используемой операционной системы.

Удаление подключения

Для удаления подключения:

1. Вызовите контекстное меню пиктограммы абонентского пункта, расположенной на панели задач Windows, и выберите команду "Настройка > Параметры...".

   На экране появится окно настройки параметров АП.
2. В левой части окна в группе "Профили подключений" выберите необходимое подключение.
3. В правой части окна нажмите кнопку "Удалить подключение".

   Выбранное подключение будет удалено.
4. Для сохранения изменений нажмите кнопку "Применить" или "ОК".

Проверка настройки аутентификации сервера

Соединение абонентского пункта с сервером доступа осуществляется после успешного завершения процедуры их взаимной аутентификации, в которой используются серверный и пользовательский сертификаты. Поэтому для подключения к серверу доступа необходимо, чтобы на абонентском пункте были установлены серверный сертификат и удостоверяющий его корневой сертификат.

В некоторых случаях, например, при создании нового подключения с использованием конфигурационного файла, корневой и серверный сертификаты устанавливаются автоматически.

Для проверки наличия установленных сертификатов:

1. Вызовите контекстное меню пиктограммы абонентского пункта, расположенной на панели задач Windows, и выберите команду "Настройка > Параметры...".

   На экране появится окно настройки параметров АП.

2. В левой части окна раскройте группу "Аутентификация сервера".

   В правой части окна отобразятся вкладки со списками установленных корневых и серверных сертификатов.

3. Убедитесь, что списки не пустые и содержат нужные сертификаты.

   Если нужные сертификаты отсутствуют, обратитесь к администратору сервера доступа и получите от него файлы сертификатов. Далее выполните установку сертификатов (см. стр.**11**).

Глава 3
Использование абонентского пункта

Подключение к серверу доступа

Перед подключением к серверу доступа подсоедините к считывателю ключевой носитель с закрытым ключом пользователя.

Для подключения к серверу доступа:

1. Вызовите контекстное меню пиктограммы абонентского пункта, расположенной на панели задач Windows, и выберите команду "Подключить".

   На экране появится диалог выбора подключения.

2. Выберите подключение из раскрывающегося списка.

   Примечание. Раскрывающийся список содержит только те подключения, которые доступны текущему пользователю. Если текущий пользователь входит в группу локальных администраторов, в списке отобразятся все подключения.

   В диалоге отобразится имя сертификата пользователя и срок его действия.

3. Если требуется просмотреть сведения о сертификате или выбрать другой, нажмите кнопку "Выбрать", расположенную справа, и выполните необходимые действия.

4. Нажмите кнопку "Подключение".

   Внимание! В зависимости от настроек подключения может потребоваться ввести защитный PIN-код ключевого носителя и пароль доступа к ключевому контейнеру.

   Начнется подключение к серверу доступа. При этом пиктограмма абонентского пункта на панели задач Windows будет отображаться в анимационном режиме и после установления соединения примет вид "Соединение установлено".

   Примечание. При соединении может возникнуть ошибка, если на компьютере не установлен межсетевой экран Secret Net Studio и для пользователя включен режим запрета незащищенных соединений на сервере доступа. В этом случае для устранения ошибки необходимо либо включить подсистему межсетевого экрана (рекомендуется), либо на сервере доступа разрешить незащищенные соединения для данного пользователя.

Разрыв соединения с сервером доступа

Для разрыва соединения с сервером доступа:

1. Вызовите контекстное меню пиктограммы абонентского пункта, расположенной на панели задач Windows.

2. В контекстном меню активируйте команду "Разорвать".

   Соединение с сервером доступа будет разорвано.

Просмотр событий

Регистрация событий, связанных с работой абонентского пункта, выполняется в журнале Secret Net Studio. События, связанные с работой абонентского пункта, в поле "Источник" имеют значение tsservice.
Сведения о настройке аудита и работе с журналами см. в документах [**3**], [**4**].

Приложение

Управление криптопровайдером "Код Безопасности CSP"

Управление криптопровайдером "Код Безопасности CSP" осуществляется с использованием программы, входящей в состав клиентского ПО Secret Net Studio. Данная программа предназначена для решения следующих задач:

- Выбор датчика случайных чисел, используемого криптопровайдером для генерации ключей.
- Удаление сохраненных на компьютере паролей для ключевых контейнеров, созданных криптопровайдером.
- Управление ключевыми контейнерами, созданными криптопровайдером:
  - определение наличия ключей на ключевых носителях;
  - просмотр информации о ключевых контейнерах;
  - копирование ключевых контейнеров на другой носитель;
  - перемещение ключевого контейнера с одного носителя на другой;
  - изменение пароля на доступ к ключевому контейнеру;
  - ввод защитного PIN-кода ключевого носителя;
  - удаление ключевых контейнеров с носителя.

Запуск программы управления криптопровайдером

Для запуска программы:

- Выполните соответствующее действие в зависимости от версии установленной операционной системы:
  - на компьютере под управлением ОС Windows 8 или Windows Server 2012 загрузите начальный экран "Пуск" и выберите элемент "Код Безопасности CSP" (относится к группе "Код Безопасности");
  - на компьютере под управлением другой ОС — нажмите кнопку "Пуск" и в меню вызова программ выберите команду "Код Безопасности | Secret Net Studio | Код Безопасности CSP".

Выбор датчика случайных чисел

В криптопровайдере "Код Безопасности CSP" могут использоваться следующие средства для генерации ключей:

- встроенный биологический датчик случайных чисел;
- физический датчик случайных чисел ПАК "Соболь".

По умолчанию после установки клиента Secret Net Studio используется встроенный биологический датчик случайных чисел.

Примечание. Если установка клиента выполняется в интерактивном режиме, в программе установки предоставляется возможность выбора нужного датчика случайных чисел.

При необходимости можно сменить датчик случайных чисел с помощью программы управления криптопровайдером. Выполнить процедуру выбора датчика может пользователь с правами локального администратора компьютера.

Для выбора датчика случайных чисел в программе управления:

1. Перейдите на вкладку "Общие" и нажмите кнопку "Сменить тип ДСЧ".
   На экране появится диалог для выбора датчика случайных чисел.
2. Укажите нужное устройство и нажмите кнопку "ОК".
   Появится сообщение о необходимости перезагрузки компьютера.
3. Нажмите кнопку "Да" и перезагрузите компьютер.

Удаление сохраненных паролей

Удалить сохраненные пароли может пользователь с правами локального администратора компьютера.

Для удаления сохраненных паролей:

- Перейдите на вкладку "Общие" и нажмите кнопку "Удалить сохраненные пароли".

Просмотр списка ключевых контейнеров

Программа отображает в иерархическом виде перечень подключенных носителей и хранящихся на них ключевых контейнеров.

Внимание! При подключении защищенного носителя требуется ввод его PIN-кода.

Для просмотра списка:

- Перейдите на вкладку "Ключевые контейнеры". Для управления списком используйте следующие кнопки:

Обновить	Обновляет отображаемый список носителей и ключевых контейнеров
PIN-код	Вызывает на экран окно для ввода PIN-кода выбранного в списке носителя eToken
Информация	Вызывает на экран диалог с информацией о выбранном ключевом контейнере
Копировать...	Запускает процедуру копирования выбранного ключевого контейнера
Переместить...	Запускает процедуру перемещения ключевого контейнера с одного носителя на другой
Изменить пароль...	Вызывает на экран диалог для смены пароля выбранного ключевого контейнера
Удалить	Удаляет выбранный контейнер с носителя

Примечание. В списке отображаются только контейнеры, созданные средствами криптопровайдера "Код Безопасности CSP". Если контейнер носителя, являющегося USB-ключом, не отображается, необходимо ввести PIN-код (см. ниже). Кроме того, процедура ввода PIN-кода выполняется для носителей-USB-ключей перед началом установки пользовательского сертификата криптопровайдера "Код Безопасности CSP".

Для ввода PIN-кода:

1. Выделите в списке USB-ключ и нажмите кнопку "PIN-код".

   На экране появится окно для ввода PIN-кода.
2. Введите PIN-код.
3. Если необходимо отменить запрос PIN-кода при последующих обращениях к ключевому контейнеру, установите отметку в поле "Запомнить PIN".
4. Нажмите кнопку "OK".

   Окно ввода PIN-кода закроется.
5. Нажмите кнопку "Обновить".

   В списке появится контейнер с указанием его имени.

Копирование ключевого контейнера

Для копирования контейнера:

1. Выберите в списке нужный ключевой контейнер и нажмите кнопку "Копировать".

   На экране появится запрос пароля на доступ к ключевому контейнеру.

2. Введите пароль и нажмите кнопку "OK".

   На экране появится диалог для ввода нового имени, которое будет присвоено копии ключевого контейнера.

3. Введите имя для присвоения копии ключевого контейнера и нажмите кнопку "OK".

   На экране появится диалог для назначения пароля на доступ к ключевому контейнеру.

4. Заполните поля диалога и нажмите кнопку "OK".

   На экране появится диалог для выбора ключевого носителя.

5. Укажите носитель, на который должен быть скопирован ключевой контейнер, и нажмите кнопку "OK".

   На экране появится уведомление о завершении процедуры.

6. Нажмите кнопку "OK".

Внимание! Для подключения абонентского пункта к СД с использованием копии ключевого контейнера необходимо повторно установить сертификат пользователя и связать его с новым ключевым контейнером. Для продолжения работы с исходными ключами необходимо также переустановить сертификат пользователя и связать его с исходным ключевым контейнером.

Перемещение ключевого контейнера

Для перемещения контейнера:

1. Выберите в списке нужный ключевой контейнер и нажмите кнопку "Переместить".

   Если ранее пароль на доступ к данному ключевому контейнеру не сохранялся, на экране появится запрос пароля на доступ к ключевому контейнеру. Введите пароль и нажмите кнопку "OK".

   На экране появится диалог для назначения нового пароля на доступ к ключевому контейнеру.

2. Введите и подтвердите новый пароль.

   При необходимости установите отметку в поле "Запомнить пароль".

   Нажмите кнопку "OK".

   На экране появится диалог выбора ключевого носителя.

3. Укажите ключевой носитель, на который должен быть перемещен выбранный ключевой контейнер, и нажмите кнопку "OK".

   На экране появится уведомление о завершении процедуры.

4. Нажмите кнопку "OK".

   В списке ключевых контейнеров выбранный контейнер будет перемещен на указанный носитель.

Изменение пароля на доступ к ключевому контейнеру

Для изменения пароля:

1. Выберите в списке нужный ключевой контейнер и нажмите кнопку "Изменить пароль".

   На экране появится диалог для назначения пароля на доступ к ключевому контейнеру.

2. Заполните поля диалога и нажмите кнопку "OK".

   На экране появится уведомление о смене пароля.

3. Нажмите кнопку "OK".

Примечание. При выполнении каких-либо действий с ключевым контейнером, пароль доступа к которому устаревает, автоматически выводится запрос на смену пароля.

Удаление ключевого контейнера с носителя

Для удаления контейнера:

1. Выберите в списке нужный ключевой контейнер и нажмите кнопку "Удалить".

   На экране появится запрос для подтверждения удаления.

2. Нажмите кнопку "Да".

Примечание. Пользователю, не наделенному правами администратора компьютера, необходимо дополнительно ввести пароль на доступ к ключевому контейнеру.

Документация

1. Средство защиты информации Secret Net Studio. Руководство администратора. Принципы построения	RU.88338853.501400.001 91 1
2. Средство защиты информации Secret Net Studio. Руководство администратора. Установка, обновление, удаление	RU.88338853.501400.001 91 2
3. Средство защиты информации Secret Net Studio. Руководство администратора. Настройка и эксплуатация	RU.88338853.501400.001 91 3
4. Средство защиты информации Secret Net Studio. Руководство администратора. Централизованное управление, мониторинг и аудит	RU.88338853.501400.001 91 4
5. Средство защиты информации Secret Net Studio. Руководство администратора. Настройка и эксплуатация. Локальная защита	RU.88338853.501400.001 91 5
6. Средство защиты информации Secret Net Studio. Руководство администратора. Настройка и эксплуатация. Сетевая защита	RU.88338853.501400.001 91 6
7. Средство защиты информации Secret Net Studio. Руководство администратора. Настройка и эксплуатация. Антивирус и средство обнаружения вторжений	RU.88338853.501400.001 91 7
8. Средство защиты информации Secret Net Studio. Руководство администратора. Настройка и эксплуатация. Шифрование сетевого трафика	RU.88338853.501400.001 91 8
9. Средство защиты информации Secret Net Studio. Руководство пользователя	RU.88338853.501400.001 92