Код Безопасности

Средство криптографической защиты информации

Континент-АП

Версия 3.7

Руководство пользователя

iOS

RU.88338853.501430.007 03 91

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

Введение

Документ предназначен для пользователей изделия "Средство криптографической защиты информации "Континент- АП". Версия 3.7" RU.88338853.501430.007 03 (далее — абонентский пункт, СКЗИ "Континент-АП"). В нем содержатся сведения, необходимые пользователю для доступа к ресурсам корпоративной сети с помощью абонентского пункта на платформе iOS.

Сайт в Интернете. Если у вас есть доступ в Интернет, 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).

Общие сведения

Назначение АПКШ "Континент"

Изделие "Аппаратно-программный комплекс шифрования "Континент" (АПКШ "Континент") предназначено для защиты данных, передаваемых по каналам связи сетей общего пользования между сегментами корпоративной сети — локальными вычислительными сетями, отдельными удаленными компьютерами и мобильными устройствами. Защита трафика обеспечивается криптографическими методами, вследствие чего данные в общедоступной сети передаются в зашифрованном виде.

АПКШ "Континент" включает в свой состав средства, обеспечивающие удаленный доступ пользователей к ресурсам защищенной корпоративной сети с мобильных устройств iPad и iPhone. На этих устройствах устанавливается СКЗИ "Континент-АП" (абонентский пункт).

Назначение абонентского пункта

Абонентский пункт обеспечивает доступ удаленных пользователей, использующих мобильные устройства (планшетные компьютеры семейства iPad, смартфоны семейства iPhone), к информационным ресурсам корпоративной сети, защищенной средствами АПКШ "Континент".

Для организации доступа удаленных пользователей к ресурсам защищаемой сети используется сервер доступа, входящий в состав АПКШ "Континент".

Программное обеспечение абонентского пункта реализовано в виде приложения "Континент- АП". Приложение устанавливается на мобильные устройства, поддерживающие беспроводные сети 3G, Wi-Fi (802.11 a/b/g/n) и работающие под управлением операционной системы (ОС) iOS версии 8.0 и выше.

Абонентский пункт реализует следующие основные функции:

- установление защищенного соединения и обмен зашифрованными данными с сервером доступа АПКШ "Континент";
- контроль целостности программного обеспечения абонентского пункта;
- автоматическая регистрация событий, связанных с функционированием абонентского пункта;
- запрет незащищенных соединений.

Абонентский пункт имеет следующие технические характеристики:

- алгоритм шифрования — в соответствии с ГОСТ 28147-89, длина ключа — 256 бит;
- защита передаваемых данных от искажения – в соответствии с ГОСТ 28147-89 в режиме имитовставки;
- увеличение размера IP-пакета — не более 49 байт (с учетом дополнительного заголовка).

Для взаимодействия абонентского пункта и сервера доступа АПКШ "Континент" используются следующие сертификаты:

- сертификат пользователя — для аутентификации пользователя на сервере доступа;
- корневой сертификат — для подтверждения подлинности сертификата пользователя.

Внимание. Запрещается использовать сертификаты, изданные в соответствии с ГОСТ Р 34.10-94.

Описание работы абонентского пункта

Для доступа к ресурсам защищенной корпоративной сети удаленный пользователь средствами абонентского пункта направляет серверу доступа запрос на соединение. Запрос направляется от имени пользователя. По полученному запросу сервер доступа инициирует запуск процедуры взаимной аутентификации с абонентским пунктом. Аутентификация осуществляется на основе сертификатов открытых ключей, и в случае положительного результата между сервером доступа и абонентским пунктом устанавливается защищенное соединение.

Если на сервере доступа установлено программное обеспечение "КриптоПро", проверка подлинности сертификата сервера доступа может осуществляться по списку отозванных сертификатов (CRL), полученному от администратора безопасности и установленному на абонентском пункте.

Установленное соединение абонентского пункта с сервером доступа предоставляет удаленному пользователю доступ к ресурсам сети, защищаемой АПКШ "Континент". Обмен данными с абонентами защищаемой подсети осуществляется через входящий в состав АПКШ "Континент" криптографический шлюз (криптошлюз) в соответствии с правилами фильтрации, задаваемыми администратором, и поддерживается до момента разрыва соединения.

Разорвать соединение может как пользователь, так и администратор безопасности. В некоторых случаях (в зависимости от настроек) разрыв соединения может автоматически выполняться самим сервером доступа. Инициатором соединения абонентского пункта с сервером доступа может быть только удаленный пользователь.

Удаленный пользователь может быть зарегистрирован на нескольких серверах доступа. В этом случае он может подключаться к любому из этих серверов с одного и того же абонентского пункта. Один сервер доступа обслуживает один защищенный сегмент сети.

Сертификаты абонентского пункта

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 подписью удостоверяющего центра сертификации.

Для создания защищенного соединения между абонентским пунктом и сервером доступа пользователю абонентского пункта необходимо получить у администратора безопасности и установить на своем мобильном устройстве следующие сертификаты:

- сертификат пользователя абонентского пункта;
- корневой сертификат, удостоверяющий сертификат пользователя.

В зависимости от указаний администратора пользователь абонентского пункта может получить сертификаты двумя способами:

- Способ 1. Администратор безопасности передает пользователю абонентского пункта корневой и пользовательский сертификаты вместе с ключевым контейнером, записанными на карте памяти или каком-либо внешнем носителе. Администратор также сообщает пользователю пароль доступа к ключевому контейнеру, содержащему закрытый ключ пользователя.
- Способ 2. По требованию администратора безопасности пользователь абонентского пункта создает на своем мобильном устройстве запрос на получение сертификата пользователя. Одновременно с запросом будет создан закрытый ключ пользователя, при этом пользователь самостоятельно назначает пароль доступа к ключевому контейнеру. Для генерации закрытого ключа используется биологический датчик случайных чисел.

Созданный запрос на получение сертификата пользователь передает администратору. На основании полученного от пользователя запроса администратор создает сертификат и передает его пользователю вместе с корневым сертификатом.

Примечание. Передача файлов запроса на получение сертификата и сертификата пользователя может выполняться по открытым каналам связи. Передача файла корневого сертификата должна выполняться по защищенным каналам связи.

Второй способ является предпочтительным, так как позволяет пользователю сохранить в тайне закрытый ключ и пароль. Кроме того, при создании запроса на сертификат пользователь самостоятельно указывает информацию о себе, что обеспечивает максимальную точность данных.

Общий порядок установки и настройки абонентского пункта

1. Установите на мобильное устройство приложение "Континент-АП" (см. стр.**9**).
2. Получите у администратора и установите на абонентском пункте сертификат пользователя и корневой сертификат.
   - Если администратор передает пользователю оба сертификата вместе с ключевым контейнером и паролем, выполните процедуру установки сертификатов с закрытым ключом (см. стр.**11**).
   - Если для получения сертификатов пользователь должен отправить администратору запрос, выполните процедуру установки сертификатов по запросу (см. стр.**13**).
3. При необходимости установите список отозванных сертификатов (см. стр.**16**).
4. Настройте параметры подключения к серверу доступа (см. стр.**17**).
5. Установите профиль OpenVPN for SecurityCode (см. стр.**17**).
6. Выполните подключение к серверу доступа (см. стр.**19**).

Установка, обновление и запуск приложения "Континент-АП"

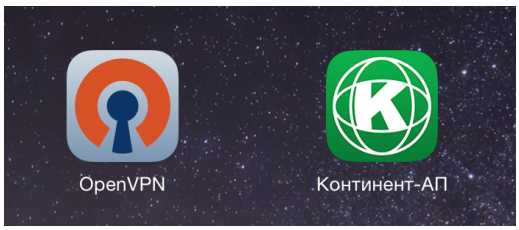
Установка

Программное обеспечение приложения "Континент-АП" устанавливается на мобильное устройство посредством инсталляционного пакета vpncontinent.ipa.

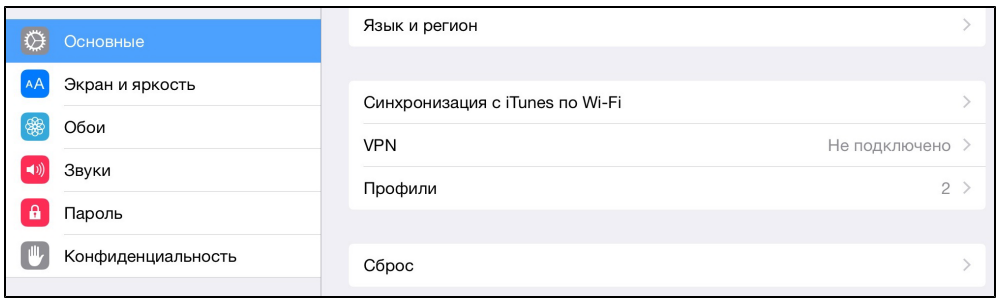
Внимание. Инсталляция файла vpncontinent.ipa осуществляется средствами программного обеспечения, реализующего протокол Apple MDM. При его отсутствии следует использовать приложение Apple iTunes (для Windows и MacOS) или Apple Configurator (для MacOS).

После успешного завершения установки появятся:

- на рабочем столе — значки приложений OpenVPN и "Континент-АП":



- в меню "Настройки" I "Основные" — поля VPN и "Профили":



Обновление

Обновление программного обеспечения абонентского пункта выполняется с помощью приложения iTunes. Оно заключается в удалении текущей и установке новой версии инсталляционного пакета vpncontinent.ipa.

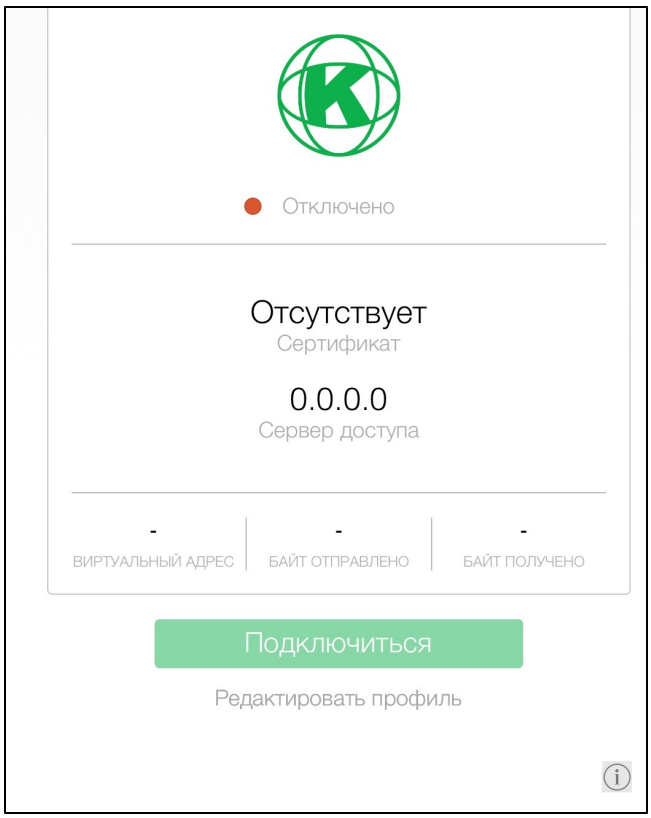
Запуск

Для запуска приложения:

1. Перейдите на рабочий стол мобильного устройства путем нажатия кнопки "Домой", расположенной в нижней части устройства.
2. Нажмите значок "Континент-АП" на рабочем столе.

Внимание. При первом запуске приложения на экране мобильного устройства появится сообщение "Ненадежный корпоративный источник". Средствами операционной системы iOS подтвердите надежность приложения "Континент-АП".

Откроется главное окно приложения, предназначенное для выполнения основных операций по управлению абонентским пунктом и отображению информации о его настройках и текущем состоянии:



В верхней части окна отображается текущее состояние подключения к серверу доступа — "Отключено" или "Соединение".

Информация о настройках параметров подключения к серверу доступа отображается в полях "Сертификат" и "Сервер доступа":

- "Сертификат" — имя папки, в которой хранится сертификат, используемый для подключения;
- "Сервер доступа" — IP-адрес или имя сервера доступа.

Ниже в полях "Виртуальный адрес", "Байт отправлено", "Байт получено" отображается виртуальный адрес мобильного устройства и объем трафика.

Примечание. Информация в полях отображается при установленном соединении с сервером доступа.

В нижней части окна расположены кнопки:

Подключиться	Запускает процедуру подключения к серверу доступа (см. стр.**19**)
Отключиться	Запускает процедуру отключения от сервера доступа (см. стр.**20**)
Редактировать профиль	Вызывает окно настройки параметров подключения, установки сертификатов и профиля пользователя (см. стр.**12**)
О программе	Вызывает окно со сведениями о компании-разработчике, текущей версии программного обеспечения, контрольной сумме динамической библиотеки абонентского пункта (см. стр.**22**)

Настройка и эксплуатация абонентского пункта

Установка сертификатов

Внимание. Процедуру установки сертификатов рекомендуется выполнять на компьютере с использованием приложения iTunes после подключения к нему мобильного устройства. Установленный сертификат пользователя вместе с корневым сертификатом и ключевым контейнером хранится в приложении "Континент-АП". Имя папки, в которой хранятся сертификаты и ключевой контейнер, задается в ходе процедуры установки сертификата и отображается в главном окне приложения "Континент-АП". Папка доступна только в приложении iTunes, запущенном на компьютере.

Если по каким-либо причинам было установлено несколько сертификатов пользователя, каждый из них будет храниться в отдельной папке. При этом для подключения к серверу доступа будет использоваться сертификат, хранящийся в папке, первой по дате и времени создания.

Установка сертификатов с закрытым ключом

Администратор передает пользователю сертификаты (файлы user.cer, root.p7b) и ключевой контейнер. Кроме того, администратор сообщает пользователю пароль доступа к ключевому контейнеру.

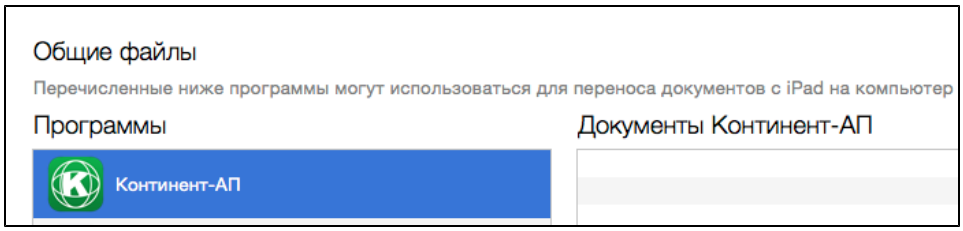
Процедура установки заключается в копировании сертификатов и ключевого контейнера с компьютера на мобильное устройство с последующим импортом ключевого контейнера.

Для установки сертификатов:

1. На компьютере, с которого будет выполняться копирование сертификатов, создайте папку и поместите в нее два файла сертификатов и ключевой контейнер.

   Внимание. Имя созданной папки — это имя папки, в которой будет храниться сертификат пользователя, используемый для подключения к серверу доступа.

2. Подключите к компьютеру мобильное устройство с установленным приложением "Континент-АП".
3. Запустите на компьютере приложение iTunes, откройте подключенное мобильное устройство и в боковом меню в разделе "Настройки" выберите папку "Программы".
4. Прокрутите отображаемый справа список, найдите в нем раздел "Общие файлы" и в подразделе "Программы" выделите пункт "Континент-АП":

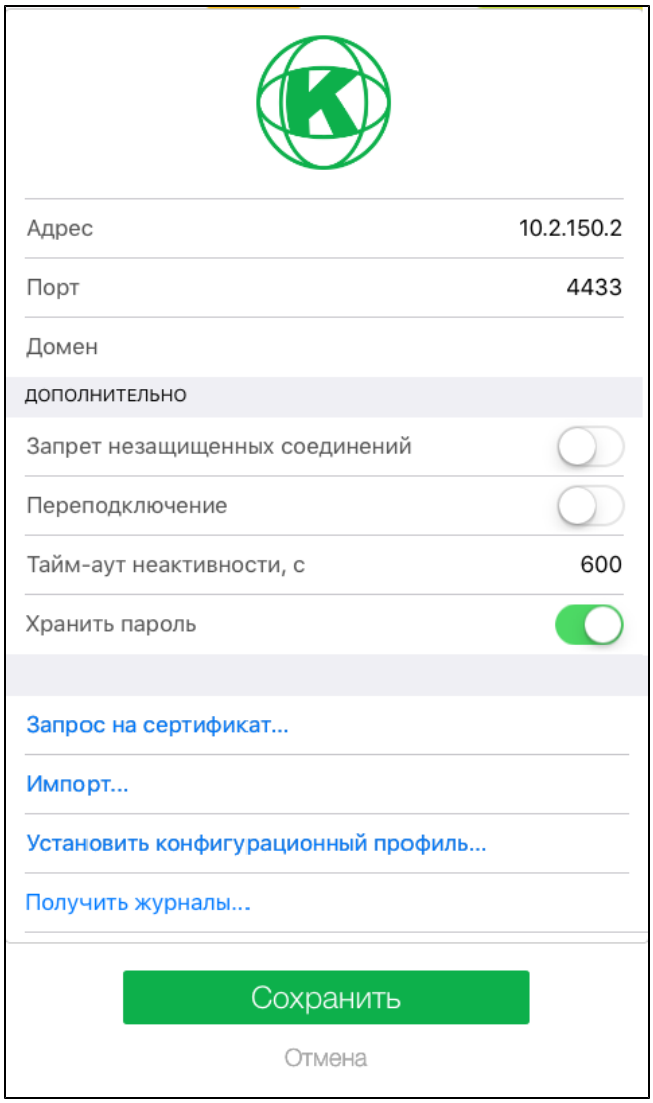


5. Скопируйте путем перемещения в поле "Документы Континент-АП" созданную папку с файлами сертификатов и ключевым контейнером, не меняя ее внутренней структуры.
6. Нажмите кнопку "Синхронизировать".
7. Отключите мобильное устройство от компьютера.

Для импорта ключевого контейнера:

1. Запустите на мобильном устройстве приложение "Континент-АП" и в главном окне выберите пункт меню "Редактировать профиль".

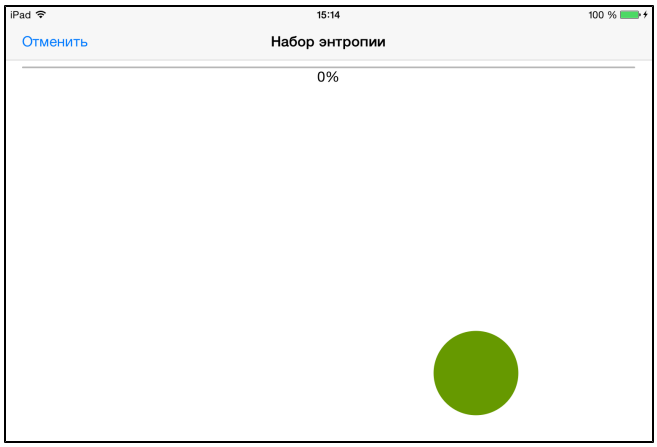
На экране появится окно настройки параметров подключения, подобное следующему:



2. Выберите в нижней части окна пункт "Импорт".

   На экране появится сообщение с инструкцией по накоплению энтропии для биологического датчика случайных чисел.

3. Нажмите кнопку "ОК" в окне сообщения и согласно инструкции нажимайте на мишень, перемещающуюся по экрану, до завершения процесса накопления энтропии, необходимой для генерации закрытого ключа:



Внимание. Непопадание в мишень может привести к снижению уровня накопленной энтропии и необходимости повторного выполнения данной операции.

После завершения операции накопления энтропии на экране появится запрос на ввод пароля для доступа к ключевому контейнеру.

4. Введите пароль, полученный у администратора, и нажмите кнопку "Ввести".

   На экране появится сообщение об успешном импорте ключевого контейнера.

5. Нажмите кнопку "OK" в окне сообщения.

   Будет выполнен возврат в главное окно приложения "Континент-АП". В главном окне отобразится имя папки, в которой хранится сертификат, используемый для подключения к серверу доступа.

Установка сертификатов по запросу

Установку сертификатов по запросу можно выполнить двумя способами — с помощью приложения iTunes и путем использования электронной почты.

Внимание. Перед созданием запроса получите у администратора безопасности сведения об используемом криптопровайдере.

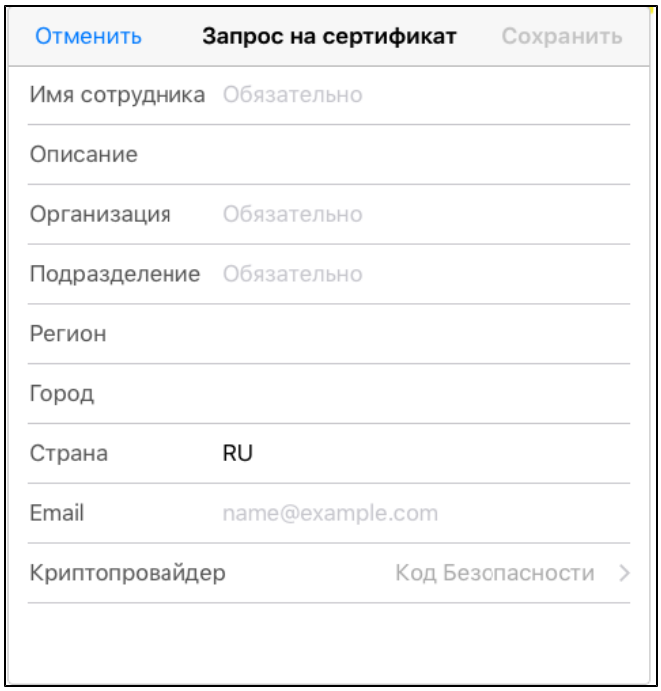
Для установки сертификатов по запросу с использованием приложения iTunes:

1. Запустите на мобильном устройстве приложение "Континент-АП" и в главном окне выберите пункт меню "Редактировать профиль".

   На экране появится окно настройки параметров подключения (см. рисунок выше).

2. Выберите в нижней части окна пункт "Запрос на сертификат".

   На экране появится форма запроса на получение нового сертификата:



3. Введите сведения о пользователе.

   Для ввода сведений выделите поле и затем используйте открывающуюся в нижней части окна экранную клавиатуру.

   - Имя, вводимое в поле "Имя сотрудника", должно быть уникальным.
   - При указании криптопровайдера выберите его на основании сведений, полученных от администратора безопасности ("КриптоПро" или "Код Безопасности").

- По умолчанию запрос на получение сертификатов и ключевой контейнер будут сохранены на мобильном устройстве в папке с именем, указанным в поле "Имя сотрудника".

4. После ввода сведений нажмите кнопку "Сохранить".

   На экране появится сообщение с инструкцией по накоплению энтропии для биологического датчика случайных чисел.

5. Нажмите кнопку "ОК" в окне сообщения и согласно инструкции нажимайте на мишень, перемещающуюся по экрану, до завершения процесса накопления энтропии.

   Внимание. Непопадание в мишень может привести к снижению уровня накопленной энтропии и необходимости повторного выполнения данной операции.

   После завершения операции накопления энтропии на экране появится диалог задания пароля для доступа к ключевому контейнеру.

6. Введите и подтвердите пароль, затем нажмите кнопку "Ввести".

   Файл запроса и ключевой контейнер будут сохранены в папке с именем, указанным при заполнении формы в поле "Имя сотрудника".

   Внимание. Если имя, указанное в поле "Имя сотрудника", повторяется, то файл запроса и ключевой контейнер на мобильном устройстве сохранить не удастся. Необходимо удалить предыдущий запрос и создать запрос с уникальным именем.

7. Подключите к компьютеру мобильное устройство с установленным приложением "Континент-АП".

8. Запустите на компьютере приложение iTunes, откройте подключенное мобильное устройство и в боковом меню в разделе "Настройки" выберите папку "Программы".

9. Прокрутите отображаемый справа список, найдите в нем раздел "Общие файлы" и в подразделе "Программы" выделите пункт "Континент-АП".

   В поле "Документы Континент-АП" отобразится имя папки, в которой были сохранены файл запроса и ключевой контейнер.

10. Выделите папку с файлом запроса и ключевым контейнером, нажмите кнопку "Сохранить в ..." и переместите папку на компьютер.

11. Передайте администратору безопасности файл запроса user.req, сохраненный в папке на компьютере.

12. После получения от администратора файлов user.cer, root.p7b разместите файлы на компьютере в папке, в которой хранится файл запроса и ключевой контейнер.

13. Скопируйте папку с файлами сертификатов из компьютера в приложение "Континент-АП" (см. действия **3**, **4**, **5** процедуры установки сертификатов с закрытым ключом на стр.**11**).

    Пояснение. В случае появления предупреждения системы о перезаписи существующей папки нажмите кнопку "Заменить".

14. На мобильном устройстве откройте главное окно приложения "Континент-АП".

    В главном окне отобразится имя папки, в которой хранится сертификат пользователя, предназначенный для подключения к серверу доступа.

Для установки сертификатов по запросу с использованием электронной почты:

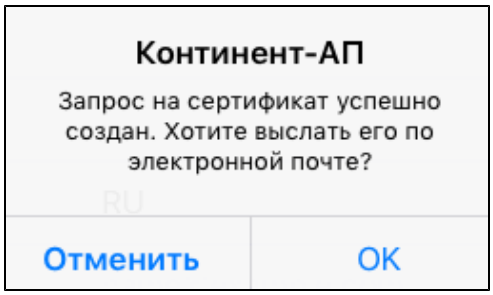
Внимание. Для создания запроса с использованием электронной почты предварительно настройте работу почтового клиента на мобильном устройстве средствами операционной системы iOS.

1. Выполните действия **1-5** вышеописанной процедуры создания запроса с использованием iTunes.

2. Введите и подтвердите пароль, затем нажмите кнопку "Ввести".

Файл запроса и ключевой контейнер будут сохранены в папке с именем, указанным при заполнении формы в поле "Имя сотрудника".

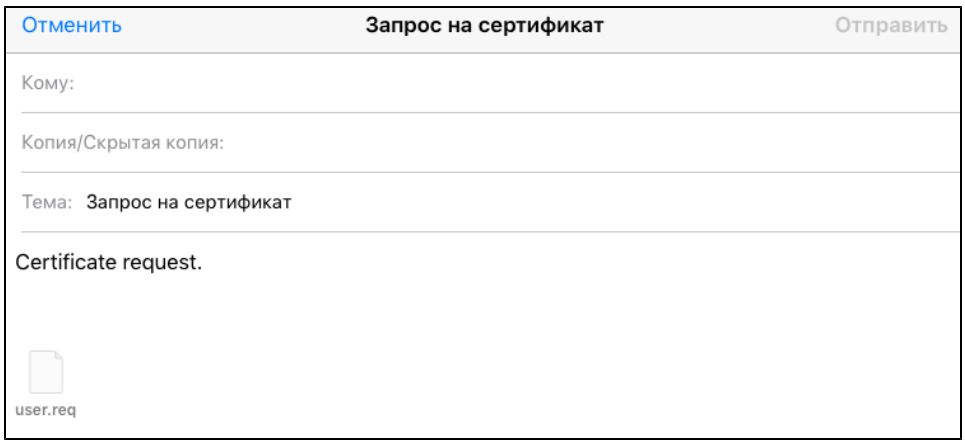
На экране появится сообщение:



3. Нажмите кнопку "OK".

   Файл запроса и ключевой контейнер будут сохранены в папке с именем, указанным при заполнении формы в поле "Имя сотрудника".

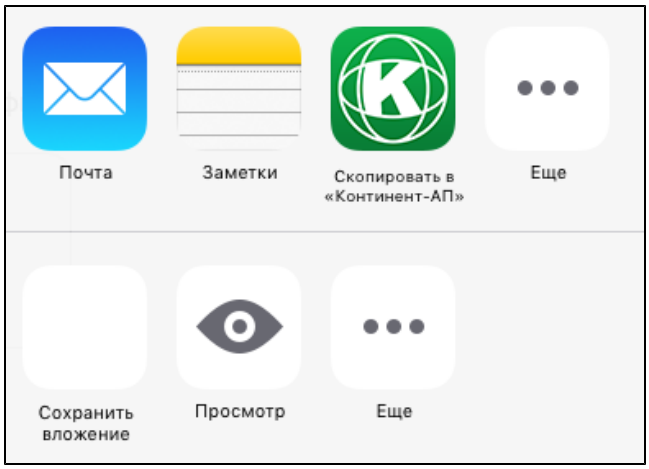
   На экране появится сообщение:



   В поле "Кому:" введите почтовый адрес администратора безопасности и нажмите "Отправить". В ответном письме администратор присылает zip-архив, содержащий файлы сертификатов user.cer, root.p7b.

4. Откройте ответное письмо. Нажмите и удерживайте значок zip-архива.

   На экране появится окно, подобное следующему:



5. Выберите "Скопировать в "Континент-АП".

   Файлы сертификатов user.cer, root.p7b будут размещены в папке приложения "Континент-АП".

Замена сертификатов на мобильном устройстве

Внимание. Для выполнения замены сертификатов на мобильном устройстве приложение "Континент-АП" должно быть отключено от сервера доступа.

Для замены сертификатов:

1. Подключите мобильное устройство к компьютеру. На компьютере определите место нахождения папки с файлами сертификатов и ключевым контейнером, которую необходимо скопировать в мобильное устройство.
2. Запустите на компьютере приложение iTunes, откройте подключенное мобильное устройство и в боковом меню в разделе "Настройки" выберите папку "Программы".
3. Прокрутите отображаемый справа список, найдите в нем раздел "Общие файлы" и в подразделе "Программы" выделите пункт "Континент-АП".
4. В поле "Документы Континент-АП" удалите папку с файлами сертификатов и ключевым контейнером.
5. Скопируйте путем перемещения в поле "Документы Континент-АП" созданную папку с файлами сертификатов и ключевым контейнером, не меняя ее внутренней структуры.
6. Отключите мобильное устройство от компьютера.

Установка списка отозванных сертификатов

Администратор безопасности передает пользователю абонентского пункта список отозванных сертификатов в виде файла с именем *.crl.

Для установки списка отозванных сертификатов на мобильном устройстве необходимо поместить полученный от администратора файл в папку, в которой хранится сертификат пользователя.

Для установки списка отозванных сертификатов:

1. Подключите к компьютеру мобильное устройство с установленным приложением "Континент-АП".
2. Запустите на компьютере приложение iTunes, откройте подключенное мобильное устройство и в боковом меню в разделе "Настройки" выберите папку "Программы".
3. Прокрутите отображаемый справа список, найдите в нем раздел "Общие файлы" и в подразделе "Программы" выделите пункт "Континент-АП".

   В поле "Документы Континент-АП" отобразится имя папки с сертификатом пользователя.
4. Выделите папку с сертификатом пользователя, нажмите кнопку "Сохранить в ..." и переместите папку на компьютер.
5. На компьютере поместите файл *.crl в папку с сертификатом пользователя.
6. Скопируйте путем перемещения в поле "Документы Континент-АП" папку с сертификатом пользователя и файлом *.crl, не меняя ее внутренней структуры.

   Пояснение. В случае появления предупреждения системы о перезаписи существующей папки нажмите кнопку "Заменить".
7. Отключите мобильное устройство от компьютера.

Механизм проверки по списку отозванных сертификатов начнет действовать при следующем подключении к серверу доступа.

Настройка подключения к серверу доступа

Для настройки подключения:

1. В главном окне приложения нажмите кнопку "Редактировать профиль".

   На экране появится окно настройки параметров подключения (см. стр.**12**).

2. Установите требуемые параметры (см. таблицу ниже) и нажмите кнопку "Сохранить".

Параметр	Описание
Адрес	IP-адрес или имя сервера доступа
Порт	Порт сервера доступа. По умолчанию устанавливается значение 4433
Домен	По умолчанию не используется. Для подключения к ресурсу с использованием доменного имени необходимо ввести его имя в поле "Домен"
Запрет незащищенных соединений	Включает режим запрета любых сторонних соединений абонентского пункта после установки связи с сервером доступа
Переподключение	При значении "Включено" будет выполняться автоматическое переподключение при потере сетевого соединения или разрыве защищенного канала по инициативе сервера доступа. Перед включением параметра убедитесь в назначении вам администратором статического IP-адреса на сервере доступа. По умолчанию установлено значение "Выключено"
Тайм-аут неактивности, с	Время неактивности (в секундах), по истечении которого произойдет отключение от сервера доступа (под неактивностью понимается отсутствие трафика в защищенном канале). По умолчанию установлено значение 600
Хранить пароль	Включает режим запоминания пароля доступа к ключевому контейнеру для подключения к серверу доступа (см. стр.**18**)

Будет выполнен возврат в главное окно приложения. В главном окне будет отображаться адрес сервера доступа.

Установка профиля OpenVPN for SecurityCode

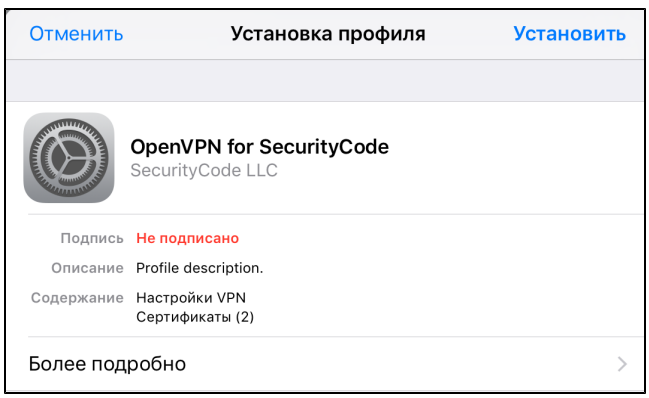
Для установки профиля:

1. В главном окне приложения нажмите кнопку "Редактировать профиль".

   На экране появится окно настройки параметров подключения (см. рисунок п. 7 процедуры импорта сертификатов на стр.**11**).

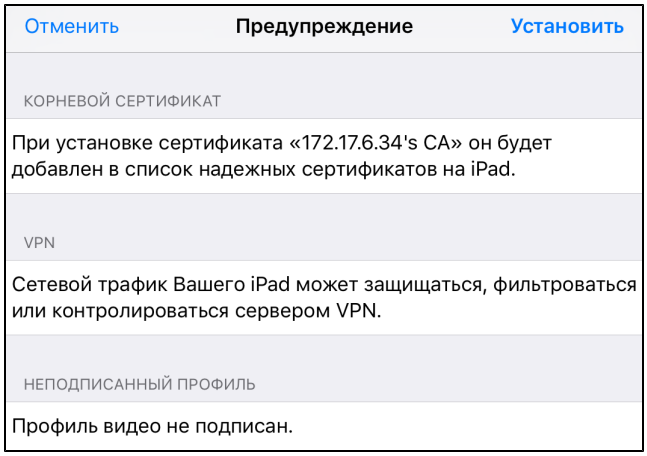
2. В нижней части окна выберите пункт "Установить конфигурационный профиль".

   На экране появится окно профиля OpenVPN for SecurityCode:



3. Нажмите "Установить".

   Появится окно, подобное следующему:



4. Нажмите "Установить".

   Появится окно "Установка профиля".

5. Нажмите "Установить".

   На экране появится окно профиля OpenVPN for SecurityCode с сообщением "Профиль установлен".

6. Нажмите "Готово".

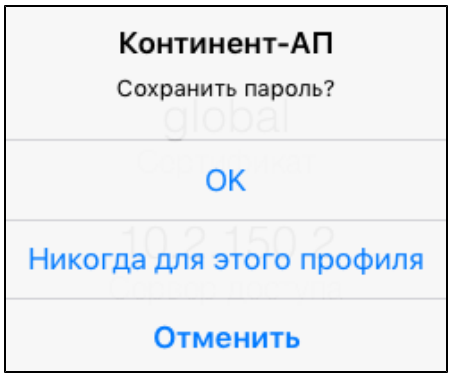
Сохранение пароля доступа

Для соединения с сервером доступа без предъявления пароля в СКЗИ "Континент-АП" реализована функция запоминания пароля доступа к ключевому контейнеру.

Для сохранения пароля доступа:

1. Вызовите главное окно приложения "Континент-АП" и нажмите кнопку "Подключиться".

   В появившемся окне введите пароль доступа. Если он верен, на экране появится диалог сохранения пароля:



2. В зависимости от выбранного варианта действия укажите одно из следующих полей:

Поле	Результат
OK	Пароль будет сохранен. Параметр "Хранить пароль" в окне настройки параметров подключения автоматически включится
Никогда для этого профиля	Пароль не будет сохранен. Параметр "Хранить пароль" будет выключен. При следующем подключении к серверу доступа диалог сохранения пароля не появится

Поле	Результат
Отменить	Пароль не будет сохранен. Параметр "Хранить пароль" будет выключен. Диалог сохранения пароля появится на экране при следующем подключении к серверу доступа

Подключение к серверу доступа

Внимание. Перед первым подключением к серверу доступа должны быть выполнены следующие условия:

- на мобильном устройстве установлены сертификат пользователя и корневой сертификат, а также ключевой контейнер;
- в настройках мобильного устройства активировано беспроводное сетевое подключение;
- настроены параметры подключения к серверу доступа.

Подключение к серверу доступа можно осуществить двумя способами — стандартным (посредством приложения "Континент-АП") и с использованием универсального указателя ресурса URL.

Стандартный способ подключения

Для подключения к серверу доступа:

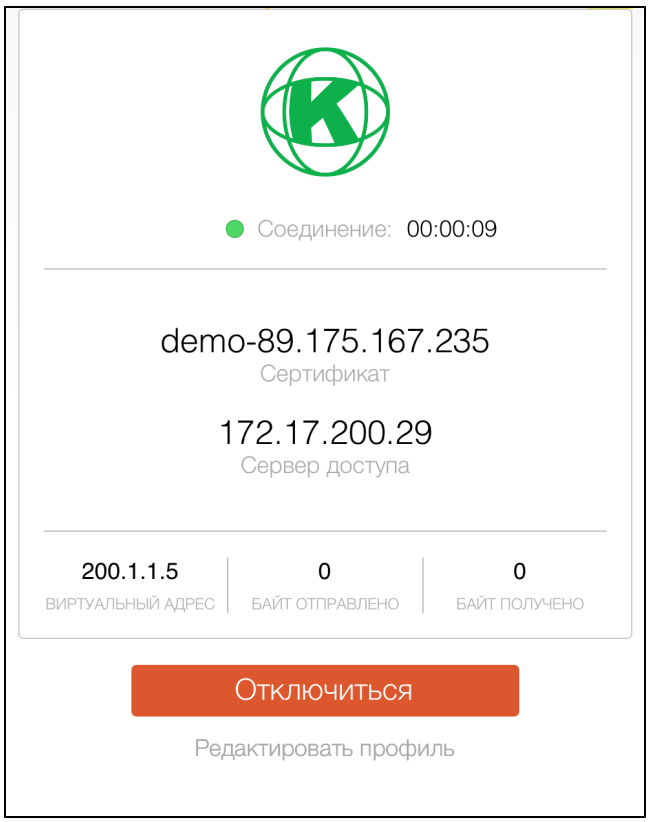
1. Вызовите главное окно приложения "Континент-АП" и нажмите кнопку "Подключиться".

   На экране появится диалог ввода пароля доступа к ключевому контейнеру.

2. Введите пароль и нажмите в диалоге кнопку "Ввести".

   Начнется соединение абонентского пункта с сервером доступа.

   После успешного завершения процедуры аутентификации произойдет подключение к серверу доступа и состояние подключения в главном окне изменится на "Соединение" с отображением времени подключения, а кнопка "Подключиться" изменит свое название на "Отключиться":



В верхнем левом углу экрана появится значок VPN:

Подключение с использованием URL

Внимание. Для выполнения подключения к серверу доступа с использованием URL приложение "Континент-АП" должно быть закрыто или запущено в главном окне.

Для подключения к серверу доступа:

1. Откройте приложение, использующее URL (например, браузер Safari).
2. Наберите в адресной строке приложения

   continent://connect?schema={адрес защищенного ресурса}
3. Нажмите кнопку ввода.

   Откроется главное окно приложения "Континент-АП".
4. Нажмите кнопку "Подключиться".

   Если пароль доступа был предварительно сохранен — подключение к серверу произойдет автоматически.

   Если пароль доступа не был сохранен — на экране появится диалог сохранения пароля. Введите пароль и нажмите "ОК" (см. стр.**18**).

После успешного соединения с сервером доступа откроется защищенный ресурс.

Разрыв соединения с сервером доступа

Для разрыва соединения:

- В главном окне приложения "Континент-АП" нажмите кнопку "Отключиться".

  Произойдет отключение абонентского пункта от сервера доступа.

  Состояние подключения в главном окне изменится на "Отключено", а кнопка "Отключиться" изменит свое название на "Подключиться".

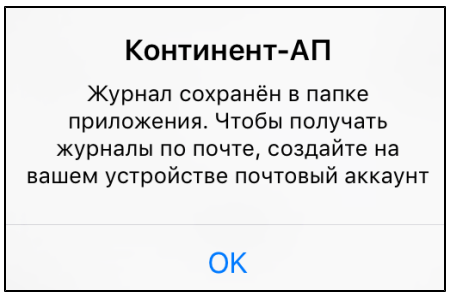
Сохранение журналов работы абонентского пункта

Основные сведения о работе СКЗИ "Континент-АП" размещаются в журналах, представляющих собой log-файлы. Журналы могут храниться на мобильном устройстве, а также быть отправлены по электронной почте.

Для сохранения журнала на мобильном устройстве:

1. Вызовите окно настройки параметров подключения приложения "Континент-АП" (см. стр.**12**). Выберите в нижней части окна пункт "Получить журналы".

   Начнется размещение log-файла в папке приложения "Континент-АП". После успешного сохранения журнала на экране появится сообщение:



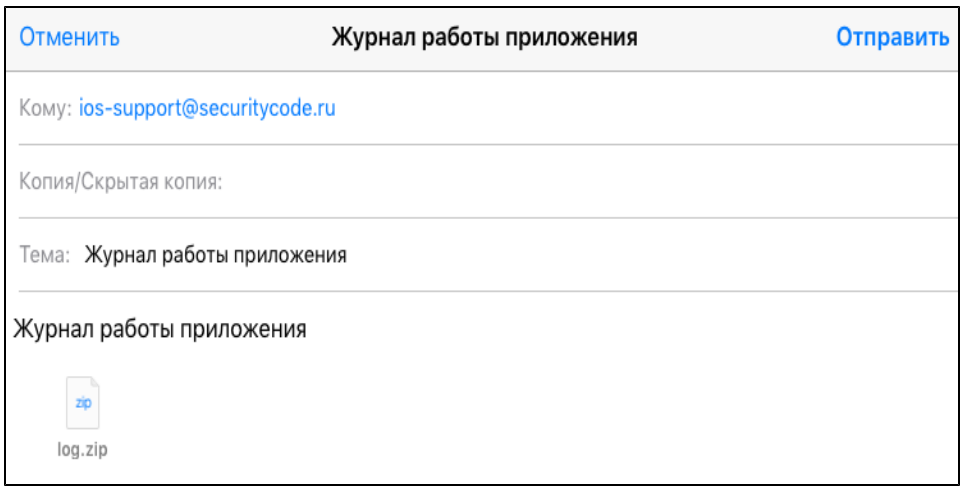
2. Нажмите "ОК".

Для отправки журнала по электронной почте:

Внимание. Для отправки журналов по электронной почте предварительно настройте работу почтового клиента на мобильном устройстве средствами операционной системы iOS.

1. Вызовите окно настройки параметров подключения приложения "Континент-АП". Выберите в нижней части окна пункт "Получить журналы".

   Начнется размещение log-файла в папке приложения "Континент-АП". После успешного сохранения журнала на экране появится окно, подобное следующему:



2. При необходимости заполните атрибуты письма и в верхней части окна нажмите "Отправить".

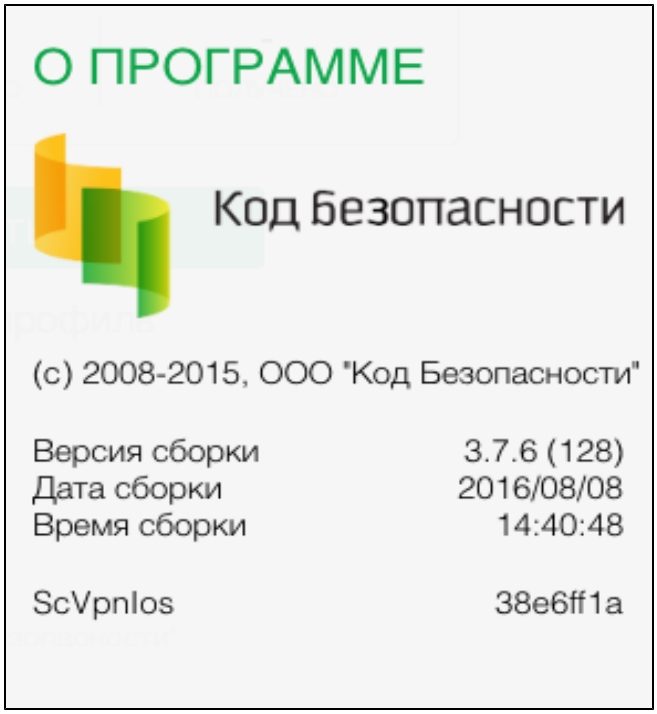
   Для отмены отправки журнала по электронной почте нажмите "Отменить".

Сведения о текущей версии абонентского пункта

В приложении "Континент-АП" имеется возможность просматривать сведения о номере текущей версии программного обеспечения абонентского пункта, дате и времени сборки, контрольной сумме динамической библиотеки ScVpnIos.

Для просмотра сведений о текущей версии приложения:

1. В главном окне приложения нажмите кнопку  "О программе".
   На экране появятся окно "О программе":



2. Для закрытия окна снова нажмите кнопку  "О программе".