



КОД БЕЗОПАСНОСТИ

Средство криптографической защиты информации

**Континент-АП**

**Версия 4 (исполнение 8)**

**Руководство администратора**

Android



## КОД БЕЗОПАСНОСТИ

© Компания "Код Безопасности", 2020. Все права защищены.

Все авторские права на эксплуатационную документацию защищены.

Этот документ входит в комплект поставки изделия. На него распространяются все условия лицензионного соглашения. Без специального письменного разрешения компании "Код Безопасности" этот документ или его часть в печатном или электронном виде не могут быть подвергнуты копированию и передаче третьим лицам с коммерческой целью.

Информация, содержащаяся в этом документе, может быть изменена разработчиком без специального уведомления, что не является нарушением обязательств по отношению к пользователю со стороны компании "Код Безопасности".

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

# Оглавление

|  |           |
|--|-----------|
| <b>Список сокращений</b> .....             | <b>4</b>  |
| <b>Введение</b> .....                      | <b>5</b>  |
| <b>Общие сведения</b> .....                | <b>6</b>  |
| Назначение абонентского пункта .....       | 6         |
| Сертификаты .....                          | 6         |
| Профили .....                              | 7         |
| Настройки подключения .....                | 9         |
| <b>Ввод в эксплуатацию</b> .....           | <b>11</b> |
| Установка и первый запуск приложения ..... | 11        |
| Регистрация приложения .....               | 12        |
| Настройка приложения .....                 | 14        |
| Подключение к серверу доступа .....        | 14        |
| <b>Эксплуатация</b> .....                  | <b>17</b> |
| Главное окно приложения .....              | 17        |
| Окно "Профили" .....                       | 18        |
| Список профилей .....                      | 18        |
| Окно "Сертификаты" .....                   | 21        |
| Описание окна .....                        | 21        |
| Меню окна "Сертификаты" .....              | 24        |
| Окно "CDP" .....                           | 28        |
| Окно "CRL" .....                           | 29        |
| Окно "Настройки подключения" .....         | 31        |
| Импорт конфигурации .....                  | 31        |
| Экспорт настроек .....                     | 34        |
| Импорт настроек .....                      | 35        |
| <b>Служебные операции</b> .....            | <b>36</b> |
| Обновление .....                           | 36        |
| Контроль целостности .....                 | 36        |
| Журнал .....                               | 37        |
| Журнал работы приложения .....             | 37        |
| Отладочный журнал .....                    | 39        |
| Управление режимом работы .....            | 40        |

## Список сокращений

|      |  |
|------|--|
| АП   | Абонентский пункт                            |
| АПКШ | Аппаратно-программный комплекс шифрования    |
| ОС   | Операционная система                         |
| СД   | Сервер доступа                               |
| СКЗИ | Средство криптографической защиты информации |
| CDP  | CRL Distribution Point                       |
| CRL  | Certificate Revocation List                  |
| DNS  | Domain Name System                           |
| IP   | Internet Protocol                            |
| MTU  | Maximum Transmission Unit                    |
| NTLM | NT LAN Manager                               |
| TCP  | Transmission Control Protocol                |
| UDP  | User Datagram Protocol                       |

## Введение

Документ предназначен для администраторов изделия "Средство криптографической защиты информации "Континент-АП". Версия 4 (исполнение 8) RU.АМБС.58.29.12.006. В нем содержатся сведения, необходимые для настройки и эксплуатации СКЗИ "Континент-АП" на платформе ОС Android.

**Служба технической поддержки.** Связаться со службой технической поддержки можно по телефону 8-800-505-30-20 или по электронной почте [support@securitycode.ru](mailto:support@securitycode.ru). Страница службы технической поддержки на сайте компании — <https://www.securitycode.ru/services/tech-support/>.

**Сайт в интернете.** Информация о продуктах компании "Код Безопасности" представлена на сайте <https://www.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 <https://www.securitycode.ru/company/education/training-courses/>.

Связаться с представителем компании по вопросам организации обучения можно по электронной почте [education@securitycode.ru](mailto:education@securitycode.ru).

# Глава 1

## Общие сведения

### Назначение абонентского пункта

СКЗИ "Континент-АП" (далее — "Континент-АП", приложение) входит в состав АПКШ "Континент" и обеспечивает доступ удаленных пользователей, использующих мобильные устройства (планшетные компьютеры, смартфоны), 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, функционирующие под управлением ОС Android от версии 5.0 до версии 10.x.

Абонентский пункт реализует следующие основные функции:

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

Поддерживаемые мобильным устройством сетевые интерфейсы:

- подключение через беспроводные сети Wi-Fi (802.11 a/b/g/n);
- подключение через беспроводные сети GPRS/3G/4G.

"Континент-АП" имеет следующие технические характеристики:

- алгоритм шифрования — соответствует ГОСТ 28147-89, длина ключа 256 бит;
- защита передаваемых данных от искажения — соответствует ГОСТ 28147-89 в режиме выработки имитовставки.

### Сертификаты

Для создания защищенного соединения между "Континент-АП" и сервером доступа пользователь "Континент-АП" получает у администратора безопасности и устанавливает на своем мобильном устройстве следующие сертификаты:

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

В зависимости от указаний администратора пользователь "Континент- АП" получает сертификаты двумя способами:

- Администратор безопасности передает пользователю "Континент- АП" корневой и пользовательский сертификаты вместе с закрытым ключом пользователя, записанным на карте памяти или внешнем носителе.
- По требованию администратора безопасности пользователь "Континент-АП" создает на своем мобильном устройстве запрос на получение сертификата пользователя.

**Примечание.** Передача файлов запроса на получение сертификата пользователя может выполняться по открытым каналам связи. Передача файлов сертификатов должна выполняться по защищенным каналам связи.

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

## Профили

Чтобы установить соединение с СД, необходимо выполнить настройку параметров подключения. Так как параметры подключения изменяются (например, подключение к разным СД, использование разных сертификатов и т. д.), для каждого подключения предварительно устанавливаются конкретные значения параметров и сохраняются в виде профиля настроек с присвоенным ему именем. Назначение параметров подключения приведено в таблице ниже:

|   |
|---|
| <b>Имя профиля</b>  |
| Название профиля для подключения к СД   |
| <b>Версия сервера доступа</b>   |
| Номер версии СД, к которому будет подключаться пользователь. Версия СД заполняется автоматически. Если был выбран пользовательский сертификат для СД версии 3.x, версию СД можно изменить на 4  |
| <b>Сервер доступа</b>   |
| IP-адрес или имя сервера доступа  |
| <b>Режим защищенного соединения</b>   |
| Способ подключения абонентского пункта к СД.<br>Может принимать значения: <ul style="list-style-type: none"> <li>• стандартное подключение (TCP);</li> <li>• потоковое подключение (UDP);</li> <li>• подключение через прокси (только для TCP).</li> </ul> Значение по умолчанию — TCP.<br>Для СД 3.x можно установить значение "UDP". Для СД 4.x режим защищенного соединения всегда TCP |
| <b>Прокси-сервер</b>  |
| При нажатии на строку параметра открывается окно настроек подключения к прокси-серверу (см. ниже). Хранит имя или IP-адрес прокси-сервера. Доступен только при режиме защищенного соединения через TCP  |
| <b>Адрес</b>  |
| Сетевое имя или IP-адрес прокси-сервера   |
| <b>Порт</b>   |
| Порт прокси-сервера. Значение по умолчанию — 3128   |
| <b>Аутентификация</b>   |
| Позволяет выбрать тип аутентификации на прокси-сервере. Может принимать значения: <ul style="list-style-type: none"> <li>• без аутентификации;</li> <li>• Basic;</li> <li>• NTML</li> </ul>   |
| <b>Имя пользователя</b>   |
| Имя пользователя для аутентификации на прокси-сервере   |
| <b>Пароль</b>   |
| Пароль пользователя для аутентификации на прокси-сервере  |
| <b>Сертификат</b>   |
| При нажатии на строку параметра открывается окно выбора сертификатов, необходимых для подключения к СД. Список доступных сертификатов представляет собой список импортированных сертификатов  |
| <b>Использовать прокси-сервер</b>   |
| Отвечает за использование прокси-сервера. Может принимать значения: <ul style="list-style-type: none"> <li>• "ВКЛ" — использовать прокси-сервер;</li> <li>• "ВЫКЛ" — не использовать прокси-сервер</li> </ul>   |

|   |
|---|
| <b>Аутентификация по сертификату</b>  |
| <p>Позволяет управлять аутентификацией с использованием сертификата и ключевого контейнера.</p> <p>Может принимать значения:</p> <ul style="list-style-type: none"> <li>• "ВКЛ" — запрашивать пароль от ключевого контейнера;</li> <li>• "ВЫКЛ" — запрашивать учетные данные пользователя (логин и пароль)</li> </ul> |
| <b>Сохранить пароль</b>   |
| Позволяет сохранить пароль для подключения к СД   |
| <b>Порт сервера доступа</b>   |
| <p>Значения по умолчанию:</p> <ul style="list-style-type: none"> <li>• для TCP — 443;</li> <li>• для UDP — 4433</li> </ul>  |
| <b>Порт клиента</b>   |
| Порт мобильного устройства. Значение по умолчанию — 7500  |
| <b>Основной DNS-сервер</b><br><b>Альтернативный DNS-сервер</b>  |
| По умолчанию используются адреса DNS-серверов, получаемые от СД. Если адреса от СД не поступают, их указывают вручную. Адреса, полученные от СД, имеют приоритет над адресами, указанными вручную   |
| <b>Домен</b>  |
| При необходимости можно указать DNS-суффикс, добавляемый автоматически к имени хоста при обращении к защищаемым ресурсам. По умолчанию не используется  |
| <b>MTU</b>  |
| <p>Максимальный размер блока (в байтах) на канальном уровне сети.</p> <p>Значение по умолчанию — 1500</p>   |

Реализована возможность редактирования списка профилей: добавление, удаление и редактирование параметров выбранного профиля.

Для использования профиля при подключении к СД необходимо сделать его активным. Активным может быть только профиль с привязанным сертификатом. При подключении активный профиль используется по умолчанию.



## Настройки подключения

Перед установлением соединения с СД необходимо настроить общие параметры, действующие для всех подключений. Назначение общих настроек подключения разъясняется в таблице ниже:

|   |
|---|
| <p><b>Постоянное соединение</b></p> <p>Соединение, отключаемое только средствами настройки общих параметров подключения, автоматически восстанавливается после потери сетевого соединения. Для реализации постоянного соединения с сервером доступа предварительно настройте или активируйте профиль подключения. Может принимать значения:</p> <ul style="list-style-type: none"> <li>• "ВКЛ";</li> <li>• "ВЫКЛ".</li> </ul> <p>Применение параметра делает невозможным управление некоторыми другими параметрами подключения (см. ниже)</p> |
| <p><b>Переподключение</b></p> <p>Автоматическое переподключение при потере сетевого соединения или при разрыве защищенного канала по инициативе сервера доступа АПКШ "Континент". Может принимать значения:</p> <ul style="list-style-type: none"> <li>• "ВКЛ";</li> <li>• "ВЫКЛ".</li> </ul> <p>Недоступно для управления, если установлен параметр "Постоянное соединение"</p>  |
| <p><b>Количество попыток переподключения</b></p> <p>Значение по умолчанию — 3. После последней неудачной попытки выводится сообщение об ошибке подключения. Недоступно для управления, если установлен параметр "Постоянное соединение"</p>   |
| <p><b>Время ожидания переподключения, с</b></p> <p>Пауза между попытками подключения (в секундах). Значение по умолчанию — 30. Недоступно для управления, если установлен параметр "Постоянное соединение"</p>  |
| <p><b>Время ожидания при бездействии, с</b></p> <p>Время неактивности (в секундах), по истечении которого произойдет отключение от СД. Под неактивностью понимается отсутствие трафика в защищенном канале. Значение по умолчанию — 600. Недоступно для управления, если установлен параметр "Постоянное соединение"</p>  |
| <p><b>Проверка по CRL</b></p> <p>Позволяет управлять функцией проверки актуальности сертификата по списку отозванных сертификатов. Может принимать значения:</p> <ul style="list-style-type: none"> <li>• "ВКЛ";</li> <li>• "ВЫКЛ"</li> </ul>   |
| <p><b>Время работы при просроченном CRL, д</b></p> <p>Количество дней, по истечении которых невозможно установить соединение с СД, если список отозванных сертификатов устарел. Значение по умолчанию — 0</p>   |
| <p><b>Автоматическое обновление CRL</b></p> <p>Позволяет управлять функцией автоматического обновления списка отозванных сертификатов в установленный параметром "Период обновления CRL" промежуток времени. Может принимать значения:</p> <ul style="list-style-type: none"> <li>• "ВКЛ" — обновлять CRL автоматически;</li> <li>• "ВЫКЛ" — не обновлять CRL автоматически. Обновление CRL можно выполнить вручную в меню окна "CDP", используя команду "Скачать CRL"</li> </ul>   |

|  |
|--|
| <b>Период обновления CRL, ч</b>  |
| Определяет периодичность обновления списка отозванных сертификатов в часах. Может принимать значения от 1 до 48. Значение по умолчанию — 12  |
| <b>Журнал</b>  |
| Позволяет настроить уровень детализации журнала "Континент-АП" (см. стр. <a href="#">37</a> ).<br>Может принимать значения: <ul style="list-style-type: none"><li>• Базовый;</li><li>• Расширенный</li></ul> |

Предусмотрены операции импорта конфигурации, экспорта и импорта настроек. Операция экспорта применяется при переносе всех настроек приложения, настроенного на конкретном мобильном устройстве, на другое устройство с установленным "Континент-АП". Операция импорта применяется для загрузки на конкретное устройство настроек приложения, экспортированных с другого устройства с установленным "Континент-АП".

## Глава 2

# Ввод в эксплуатацию

### Установка и первый запуск приложения

Установка приложения "Континент-АП" выполняется пользователем из магазина приложений (например, из Google Play) или с использованием установочного файла с расширением "apk".

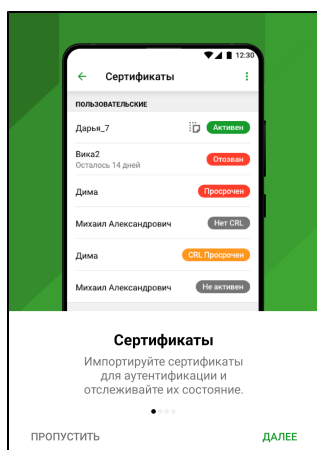
#### Внимание!

- Для работы с Google Play необходимо наличие учетной записи Google.
- Установочный арк-файл хранится на поставляемом диске. Для установки с использованием арк-файла необходимо перенести этот файл на требуемое устройство, разрешить на этом устройстве установку приложений из неизвестных источников и запустить установочный файл.

#### Для установки из магазина приложений и первого запуска:

1. В стандартном магазине приложений найдите приложение "Континент-АП" и загрузите его на свое устройство.
2. Запустите "Континент-АП".

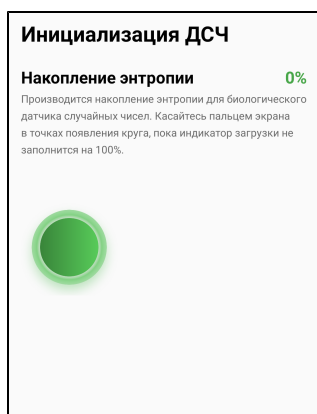
При первом запуске приложения появятся обучающие экраны, подобные следующему.



3. Для просмотра всех обучающих экранов нажимайте "Далее". На последнем экране нажмите "Зарегистрироваться".

**Примечание.** Нажатие кнопки "Пропустить" осуществляет переход к накоплению энтропии.

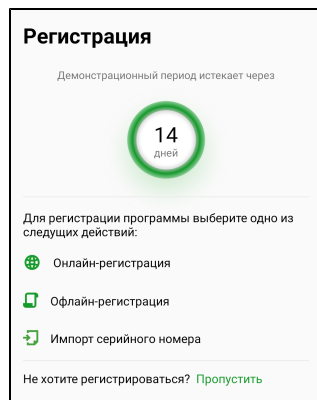
На экране появится сообщение с инструкцией и индикатором накопления энтропии для биологического датчика случайных чисел.



4. Нажимайте на зеленый круг на экране.

**Примечание.** Накопление энтропии используется для создания фиктивного ключевого контейнера. Ключевой контейнер требуется для подключения по анонимному TLS с использованием самоподписанного корневого сертификата. При удалении всех данных приложения и через год с момента последнего накопления энтропии пользователь должен заново накопить энтропию при первом запуске приложения.

Когда индикатор накопления энтропии заполнится на 100%, откроется экран регистрации приложения.



## Регистрация приложения

Сразу после установки "Континент-АП" работает в демонстрационном периоде, который составляет 14 дней. Количество дней, оставшихся до окончания демонстрационного периода, отображается в разделе "О программе".

**Примечание.** Функции приложения в демонстрационном периоде не ограничиваются.

Если по истечении срока демонстрационного периода приложение не зарегистрировано, при каждом запуске будет открываться экран регистрации с соответствующим сообщением. Пропустить регистрацию будет невозможно. "Континент-АП" можно зарегистрировать, выполнив онлайн- или офлайн-регистрацию.

### Для онлайн-регистрации "Континент-АП":

1. На экране регистрации приложения нажмите "Онлайн-регистрация".

**Примечание.** Экран регистрации появляется при каждом запуске "Континент-АП" до тех пор, пока приложение не зарегистрировано. Также экран регистрации можно вызвать в разделе "О программе", нажав на строку "Демонстрационный период".

Появится окно, подобное следующему.

2. Введите требуемые параметры и нажмите "Подтвердить".

Начнется процесс регистрации и подключения к указанному серверу регистрации. При успешном завершении операции на экране появится соответствующее сообщение.

3. Нажмите "ОК".

### Для офлайн-регистрации "Континент-АП":

1. На экране регистрации (стр. 12) нажмите "Офлайн-регистрация".

**Примечание.** Экран регистрации появляется при каждом запуске "Континент-АП" до тех пор, пока приложение не зарегистрировано. Также экран регистрации можно вызвать в разделе "О программе", нажав на строку "Демонстрационный период".

На экране появится окно ввода данных для регистрации.

2. Введите требуемые параметры и нажмите "Сохранить файл".

Приложение предложит выбрать папку для сохранения файла.

3. Выберите нужную папку и нажмите "Выбрать".

Файл будет сохранен в указанной папке на мобильном устройстве.

4. Передайте файл на сервер регистрации для получения файла с серийным номером.

5. После получения файла с серийным номером перенесите его на мобильное устройство.

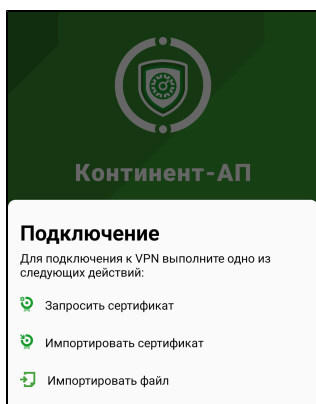
6. Вызовите экран регистрации приложения и нажмите "Импорт серийного номера".

На экране появится директория внутренней памяти устройства.

7. Выберите папку, содержащую файл с серийным номером, и нажмите "Выбрать".

При успешном завершении операции на экране появится соответствующее сообщение.

Если регистрация выполнена сразу после установки приложения, на экране появится окно загрузки "Континент-АП".



После регистрации приложения в разделе "О программе" вместо информации о сроке действия демонстрационной версии появится раздел, содержащий регистрационные данные "Континент-АП".

## Настройка приложения

Для создания защищенного соединения между "Континент-АП" и СД пользователь "Континент- АП" получает у администратора безопасности и устанавливает на своем мобильном устройстве следующие сертификаты:

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

В зависимости от указаний администратора пользователь настраивает приложение двумя способами:

- администратор безопасности передает пользователю "Континент-АП" файл конфигурации, пользователь выполняет импорт полученной конфигурации (см стр. 32);
- по требованию администратора безопасности пользователь "Континент-АП" создает на своем мобильном устройстве запрос на сертификат пользователя (см. стр. 24). Администратор безопасности передает пользователю корневой и пользовательский сертификаты, записанные на карте памяти или внешнем носителе. Пользователь выполняет импорт полученных сертификатов на экране загрузки (см. стр. 13) и настройку параметров профиля (см. стр. 7).

**Примечание.** Передача файлов запроса на получение сертификата пользователя может выполняться по открытым каналам связи. Передача файлов сертификатов должна выполняться по защищенным каналам связи.

Второй способ является предпочтительным, так как позволяет пользователю сохранить в тайне ключевой контейнер и пароль.

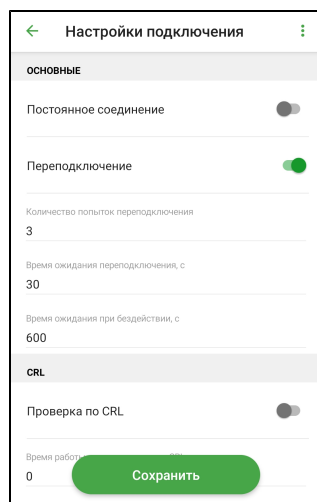
## Подключение к серверу доступа

Перед подключением к СД необходимо настроить общие параметры подключения.

### Для настройки общих параметров подключения:

1. Вызовите меню главного окна приложения (см. стр. 17) и нажмите "Настройки подключения".

На экране появится окно настройки общих параметров подключения.

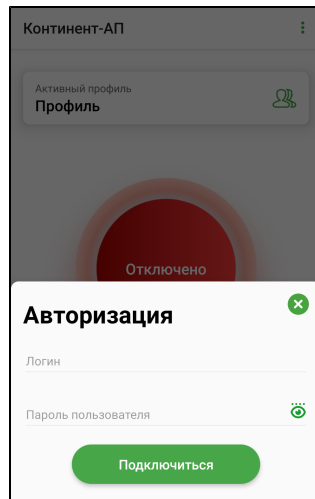


2. Установите значения параметров (см. стр. 9) и нажмите кнопку "Сохранить".

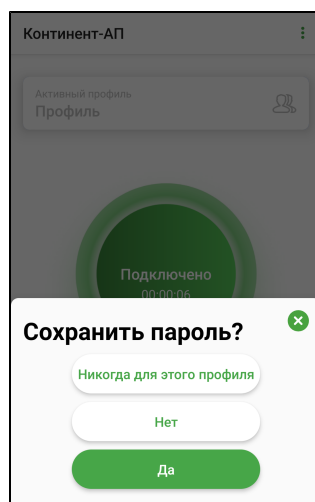
**Для подключения к серверу доступа:**

1. В главном окне приложения (см. стр. 17) нажмите индикатор подключения. На экране появится окно авторизации. В зависимости от типа аутентификации, указанного в настройках профиля, приложение будет запрашивать логин и пароль или пароль для доступа к ключевому контейнеру.

**Примечание.** В данном примере рассматривается вариант ввода логина и пароля.

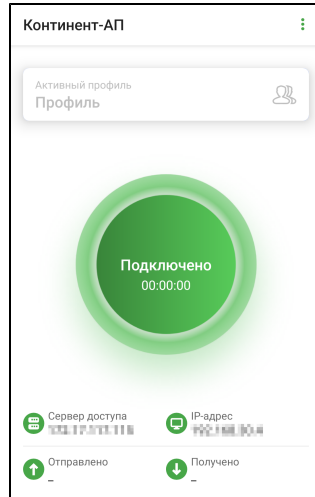


2. Введите логин и пароль. Нажмите "Подключиться". Если в настройках профиля опция "Сохранить пароль" деактивирована, на экране появится окно, подобное следующему.



3. Выполните одно из следующих действий:
  - нажмите "Да".  
Пароль будет сохранен;
  - нажмите "Нет".  
Окно закрывается, но при следующем подключении появится снова;
  - нажмите "Никогда для этого профиля".  
Уведомление закрывается и больше появляться не будет.

Если логин и пароль введены правильно, главное окно "Континент-АП" примет вид, подобный следующему.



При активном подключении нельзя переходить в разделы "Сертификаты", "CDP", "CRL" и "Настройки подключения".

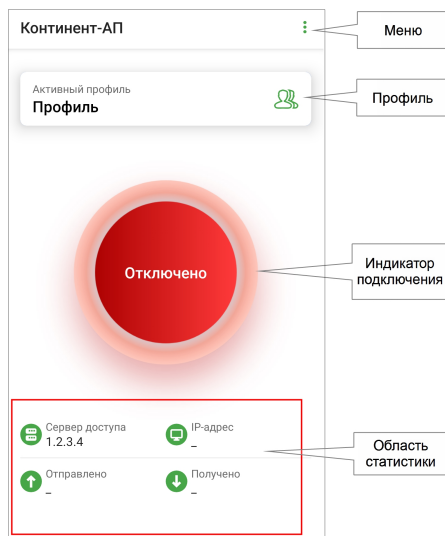
**Примечание.** Раз в полгода пользователь должен менять пароль ключевого контейнера. При подключении к серверу доступа пользователь аутентифицируется и вводит пароль, происходит проверка и, если срок действия пароля истек, появляется окно, в котором пользователь должен ввести и подтвердить новый пароль.



## Глава 3

# Эксплуатация

### Главное окно приложения



#### Описание

Главное окно состоит из четырех объектов:

| Объект                       | Описание   |
|------------------------------|--|
| <b>Меню</b>                  | Меню содержит разделы для работы с сертификатами, CDP и CRL, настройки подключения, просмотра журналов, сведений о программе и смены режима работы |
| <b>Профиль</b>               | Просмотр, создание, удаление и настройка профилей подключения  |
| <b>Индикатор подключения</b> | Подключение/отключение к/от СД   |
| <b>Область статистики</b>    | Просмотр статистики текущей сессии   |

Меню главного окна содержит следующие разделы:

| Пункт меню                   | Описание  |
|------------------------------|---|
| <b>Сертификаты</b>           | Открывает окно с установленными сертификатами (см. стр. 21). Раздел предназначен для удаления, запроса и импорта сертификатов и ключа, для сокрытия сертификатов и ключевых контейнеров во внутренней памяти устройства, просмотра информации о сертификате |
| <b>CDP</b>                   | Открывает окно для управления CDP. Окно предназначено для добавления и удаления CDP, а также загрузки CRL   |
| <b>CRL</b>                   | Открывает окно для управления CRL. Окно предназначено для просмотра и редактирования списка CRL, а также импорта CRL  |
| <b>Настройки подключения</b> | Открывает окно просмотра и настройки общих параметров подключения (см. стр. 31)   |

| Пункт меню                  | Описание   |
|-----------------------------|--|
| <b>Сменить режим работы</b> | Включает и выключает режим ограниченного доступа к управлению настройкой "Континент-АП" — частный режим (см. стр. 40). Основной режим устанавливается по умолчанию |
| <b>Журнал</b>               | Открывает окно просмотра журнала (см. стр. 37)   |
| <b>О программе</b>          | Выводит на экран сведения о текущей версии программного обеспечения, регистрационные данные и контрольные суммы динамических библиотек абонентского пункта         |

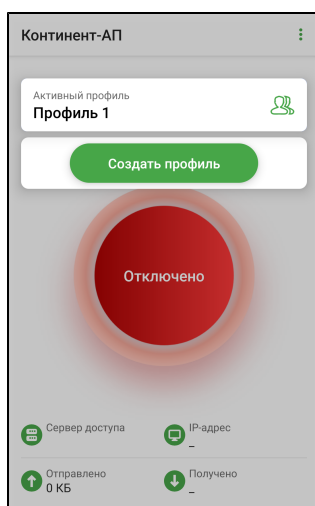
## Окно "Профили"

### Список профилей

**Примечание.** "Континент-АП" поддерживает возможность создания профиля без привязки к сертификату. Такой профиль нельзя активировать, и в списке профилей он обозначается восклицательным знаком ⚠.

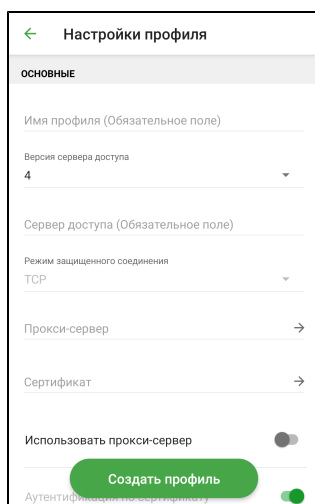
#### Для перехода к списку профилей:

- В главном окне приложения выберите панель "Профиль".  
На экране появится список профилей, подобный следующему.



#### Для создания профиля:

- В списке профилей нажмите "Создать профиль".  
На экране появится окно, подобное следующему.



**2. Активируйте поле "Сертификат".**

В появившемся окне появятся списки корневых и пользовательских сертификатов.

**3. Выберите сертификат.**

В зависимости от выбранного типа сертификата версия СД заполняется автоматически и устанавливается переключатель "Аутентификация по сертификату". Если был выбран пользовательский сертификат для СД версии 3.x, версию СД можно изменить на 4.

**Примечание.** Настройки параметров профиля в зависимости от выбранного типа сертификата различаются следующим образом:

- если выбран пользовательский сертификат для СД 4.x, то активируется переключатель "Аутентификация по сертификату". Если деактивировать переключатель "Аутентификация по сертификату", то в поле "Сертификаты" отобразится название корневого сертификата и аутентификация будет производиться по логину и паролю;
- если выбран пользовательский сертификат для СД 3.x, то переключатель "Аутентификация по сертификату" активируется и блокируется. Деактивировать его нельзя, доступна аутентификация только по сертификату;
- если выбран самоподписанный корневой сертификат для СД 4.x, то переключатель "Аутентификация по сертификату" деактивируется и блокируется. Активировать его нельзя, доступна аутентификация только по логину и паролю. Логин и пароль администратор передает пользователю по защищенному каналу.

**4. Для настройки подключения через прокси-сервер:**

- для параметра "Режим защищенного соединения" укажите значение "TCP";

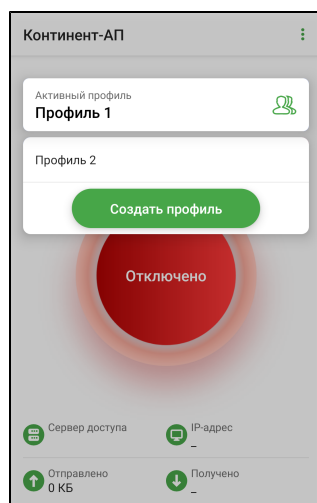
**Примечание.**

- Для СД 4.x значение "TCP" указано по умолчанию и не может быть изменено.
- Для СД 3.x значение параметра можно изменить на "UDP".
- При выборе значения "UDP" строка "Прокси-сервер" и переключатель "Использовать прокси-сервер" становятся скрытыми.

- активируйте строку "Прокси-сервер";
- в открывшейся группе параметров введите их значения;
- нажмите кнопку "Сохранить";
- в настройках профиля для параметра "Использовать прокси-сервер" укажите значение "ВКЛ".

**5. Если необходимо, задайте значения параметрам в группе параметров "Дополнительные настройки".****6. Заполните оставшиеся пустыми поля.****7. Нажмите кнопку "Создать профиль".**

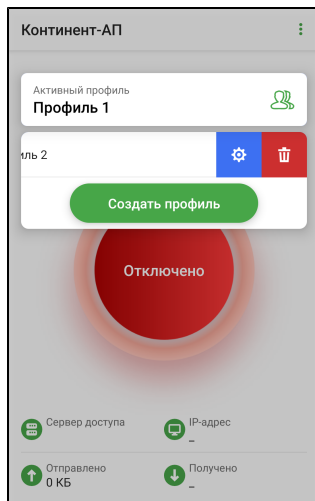
Профиль появится в списке.




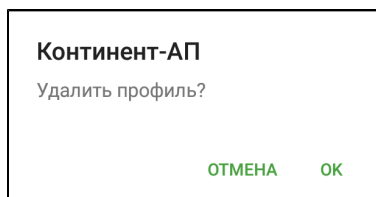
**Для удаления профиля:**

**Примечание.** Активный профиль удалить нельзя!

1. В списке профилей проведите пальцем справа налево по удаляемому профилю.  
Окно примет вид, подобный следующему.



2. Нажмите .  
На экране появится сообщение, подобное следующему.

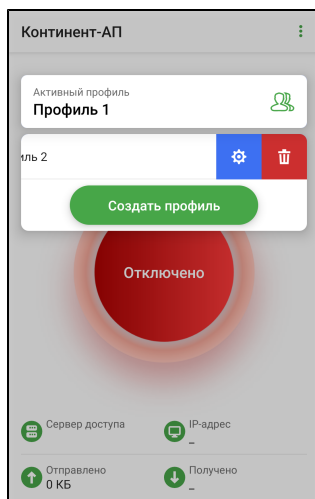


3. Нажмите "ОК".  
Профиль будет удален.

**Для настройки профиля:**

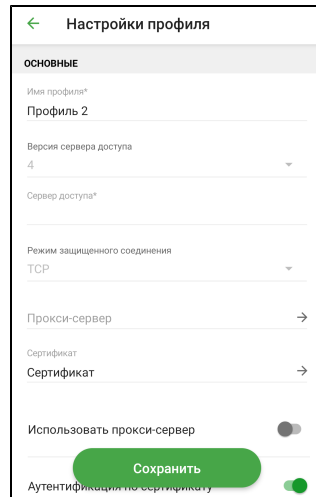
**Примечание.** Редактирование профиля запрещено при установленном соединении с СД.

1. В списке профилей проведите пальцем справа налево по выбранному профилю.  
Окно примет вид, подобный следующему.



## 2. Нажмите .

На экране появится окно, подобное следующему.




## 3. Внесите исправления в доступные для редактирования строки.

## 4. Нажмите "Сохранить".

### Для смены активного профиля в приложении:

- В списке профилей нажатием выберите нужный профиль. Выбранный профиль отобразится на панели "Активный профиль".

**Примечание.** Активировать профиль без сертификата нельзя. Профиль без сертификата отмечается знаком .

## Окно "Сертификаты"

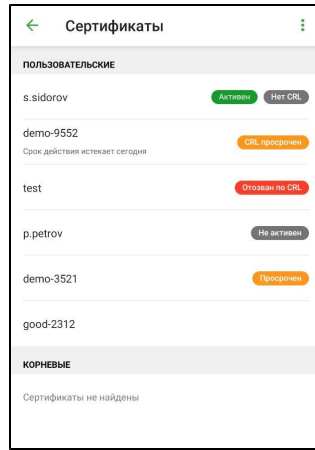
### Описание окна

Окно содержит список всех импортированных на устройство пользовательских и корневых сертификатов. Актуальное состояние сертификатов отображается на экране рядом с названием сертификата. Для отображения состояния используются следующие отметки:

| Отметка                                    | Значение   |
|--|--|
| <b>Активен</b>                             | Статус присваивается, если пользовательский сертификат актуален и используется устройством в данный момент                 |
| <b>Срок действия истекает через n дней</b> | Предупреждение появляется за 14 дней до окончания срока действия сертификата, n — переменная, обозначающая количество дней |
| <b>Отозван по CRL</b>                      | Сертификат находится в списке недействительных сертификатов  |
| <b>Просрочен</b>                           | Срок действия сертификата истек  |
| <b>Нет CRL</b>                             | Данный сертификат не прошел проверку по CRL  |
| <b>CRL просрочен</b>                       | Срок действия CRL истек или еще не начался   |
| <b>Не активен</b>                          | Срок действия сертификата еще не начался   |

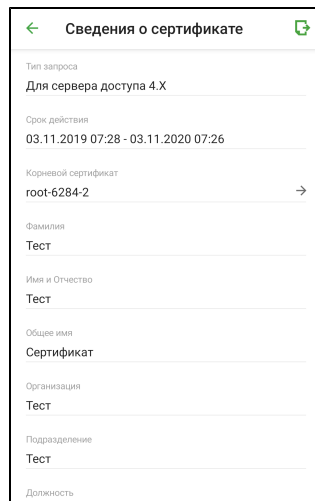
### Для работы с сертификатами:

- В главном окне приложения откройте меню и выберите "Сертификаты". Откроется окно "Сертификаты".



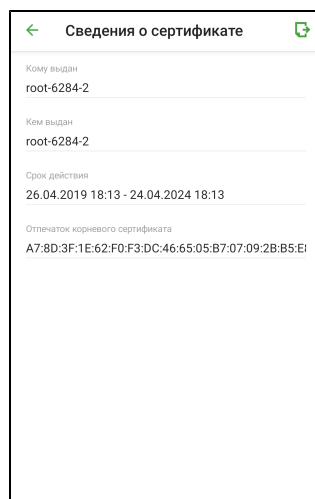
### Для просмотра сведений о пользовательском сертификате:

- Выберите его в списке.  
Окно примет вид, подобный следующему.



### Для просмотра сведений о корневом сертификате:

- Выберите его в списке.  
Окно примет вид, подобный следующему.




**Примечание.** Корневые сертификаты бывают двух видов:

- из полного набора, связанные с пользовательским сертификатом;
- самоподписанные.


В окне "Сертификаты" отображаются пользовательские и самоподписанные корневые сертификаты. Для просмотра информации о корневом сертификате, который связан с пользовательским, в окне "Сведения о сертификате" нажмите "Корневой сертификат".

#### Для удаления сертификата:

1. В окне "Сертификаты" проведите пальцем справа налево по строке удаляемого сертификата.
2. Нажмите .
3. Нажмите "ОК".  
Сертификат будет удален.

#### Для экспорта сертификата:

**Примечание.** Операция "Экспорт сертификата" предназначена для передачи сертификата в техническую поддержку в случае ошибки подключения пользователя к серверу доступа.

1. Перейдите в окно сведений о сертификате.
2. Нажмите .  
"Континент-АП" предложит выбрать приложение для отправки сертификата.
3. Выберите почтовый клиент.  
Автоматически будут заполнены строки "От", "Тема" и вложен файл сертификата.
4. Введите адрес получателя и отправьте письмо.

#### Скрытие сертификатов

Процедура предназначена для защиты файлов от несанкционированного изменения, удаления или передачи. После выполнения процедуры при открытии папки файлы user.cer, root.p7b и user.key будут невидимы для пользователя, в том числе и при подключении к компьютеру. Чтобы отменить процедуру скрытия файлов, повторите ее еще раз.


**Примечание.** Если удалить приложение со скрытыми файлами, то все скрытые файлы будут удалены вместе с приложением.

#### Для скрытия файлов:

1. Откройте окно "Сертификаты".
2. Проведите пальцем справа налево по строке требуемого сертификата.



3. Нажмите .

Рядом со скрытыми сертификатами появится значок .

## Меню окна "Сертификаты"

### Запрос на сертификат

Для создания запроса на сертификат:

1. В меню окна "Сертификаты" нажмите "Запросить сертификат".

В зависимости от выбранного типа субъекта внешний вид страницы запроса будет различаться.

2. Введите сведения о пользователе.

Для ввода сведений активируйте поле нажатием и используйте экранную клавиатуру.

**Примечание.** Тип запроса зависит от версии СД.

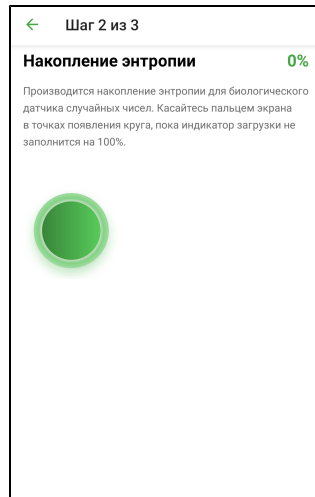
В зависимости от выбранного типа субъекта обязательными являются следующие поля:

| Атрибут           | Произвольный тип | ФЛ | ФЛ (ЮЛ) | ИП | ЮЛ |
|-------------------|------------------|----|---------|----|----|
| Тип запроса       | +                | +  | +       | +  | +  |
| Фамилия           |                  | +  | +       | +  |    |
| Имя и Отчество    |                  | +  | +       | +  |    |
| Общее имя         | +                |    | +       |    | +  |
| Организация       |                  | +  |         |    |    |
| Подразделение     |                  |    |         |    |    |
| Должность         |                  |    | +       |    |    |
| Страна            | +                | +  | +       | +  | +  |
| Область           |                  |    | +       |    | +  |
| Населенный пункт  |                  |    | +       |    | +  |
| Адрес             |                  |    | +       |    | +  |
| Электронная почта |                  |    |         |    |    |
| ИНН               |                  |    | +       |    | +  |
| СНИЛС             |                  | +  |         | +  |    |
| ОГРН              |                  |    | +       |    | +  |
| ОГРНИП            |                  |    |         | +  |    |

3. Нажмите "Далее".



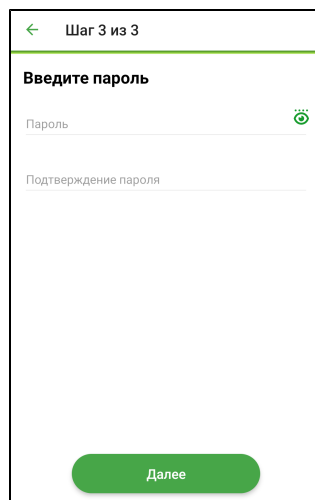
На экране появится окно, подобное следующему.



4. Нажимайте на мишени, пока индикатор прогресса не заполнится целиком.

**Примечание.** Непопадание в круг может привести к снижению уровня накопленной энтропии и повторному выполнению операции.

Когда индикатор покажет 100%, откроется диалог задания пароля для доступа к ключевому контейнеру.



5. Введите и подтвердите пароль.

**Примечание.** Минимальные требования к паролю:

- длина пароля должна быть не менее 6 символов;
- пароль должен содержать буквы латинского алфавита (A–Z, a–z), арабские цифры (0–9), а также специальные символы (., : ; ? ! \* + % - < > @ [ ] { } / \ \_ { } \$ # ~ ^ & = ' " " ` | №);
- буквенная часть пароля должна содержать как строчные, так и прописные (заглавные) буквы.

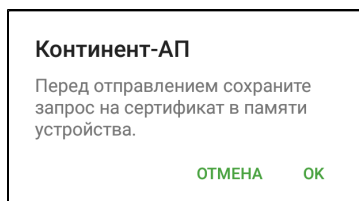
6. Нажмите "Далее".

В нижней части экрана появится меню, подобное следующему.



7. Нажмите "Отправить".

На экране появится сообщение, подобное следующему.

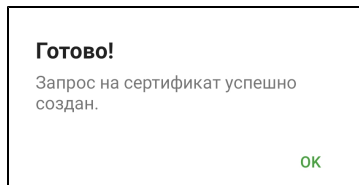


**8.** Нажмите "ОК".

На экране появится директория внутренней памяти устройства.

**9.** Выберите папку для сохранения и нажмите кнопку "Выбрать".

Файл запроса и ключевой контейнер будут сохранены в указанной папке. На экране появится сообщение, подобное следующему.



**10.** В появившемся окне выберите почтовый клиент для отправки письма.

**11.** В окне почтового клиента впишите адрес и отправьте письмо администратору. Автоматически будут заполнены строки "От", "Тема" и вложен файл запроса на сертификат.

**Примечание.** Администратор передает один из наборов файлов:

- полный набор — пользовательский и корневой сертификаты;
- самоподписанный корневой сертификат.

## Импорт сертификата

### Для импорта сертификата:

**Примечание.** При импорте архива с сертификатами из почты убедитесь, что внутри архива нет других папок.

**1.** Откройте меню окна "Сертификаты" и выберите пункт "Импортировать сертификат".

На экране появится директория внутренней памяти устройства.

**2.** Выберите нужную папку и нажмите кнопку "Выбрать".

**Примечание.** При импорте сертификатов из архива отдельная папка не создается, файлы сертификатов распакуются в директорию, в которой находится архив.

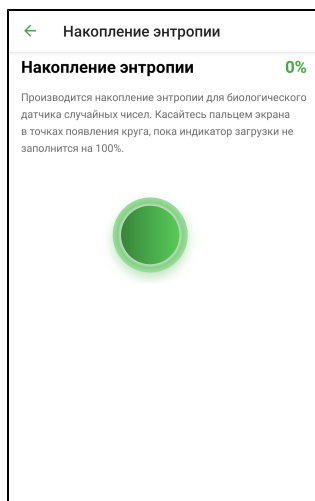
На экране появится окно "Сертификаты". В списке сертификатов появятся новые пользовательские и корневые сертификаты. Количество и тип сертификатов зависит от набора, переданного администратором.

## Импорт ключа

Операция предназначена для случая, когда администратор сформировывает файлы, включая ключ, без запроса на сертификат. Тогда для корректной работы приложения пользователь должен конвертировать ключ в формат для мобильного "Континент-АП". Если ключ не конвертировать, то подключение к СД осуществляться не будет.

### Для импорта ключа:

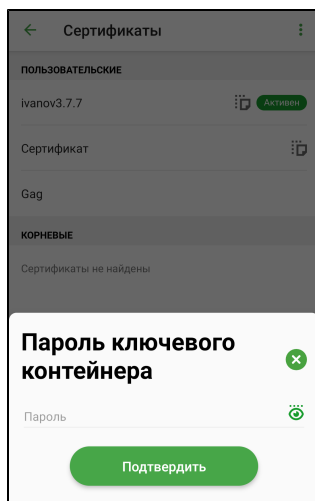
1. В меню окна "Сертификаты" выберите пункт "Импортировать ключ".  
На экране появится директория внутренней памяти устройства.
2. Выберите папку и нажмите кнопку "Выбрать".  
На экране появится окно, подобное следующему.



3. Нажимайте на мишени, пока индикатор прогресса не заполнится целиком.

**Пояснение.** Непопадание в круг может привести к снижению уровня накопленной энтропии и повторному выполнению операции.

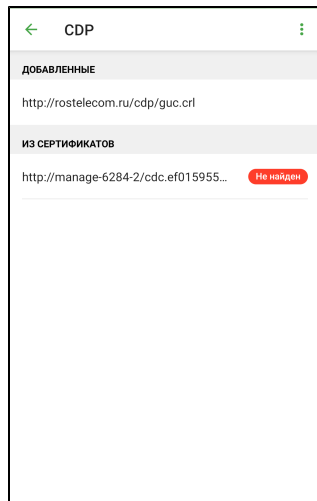
Когда индикатор покажет 100%, откроется запрос на ввод пароля для доступа к ключевому контейнеру.



4. Введите пароль, полученный от администратора, и нажмите "Подтвердить".  
Операция будет завершена, и появится сообщение об успешном импорте.
5. Нажмите "ОК".  
В папке сохранится ключ в формате user.key.

## Окно "CDP"

"Континент-АП" позволяет в автоматическом или ручном режиме получать CDP, автоматически скачивать CRL для проверки валидности используемых сертификатов, а также импортировать CRL вручную.



### Управление CDP

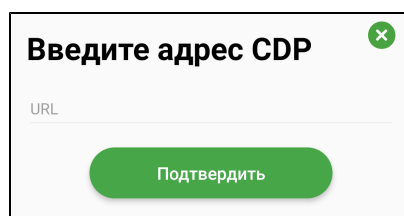
Если используемые сертификаты содержат информацию о CDP, "Континент-АП" получит ее при импорте сертификатов (см. стр. 26).

**Примечание.** Для сертификатов, выпущенных на СД, CRL не требуется. Для подключения к СД отключите проверку CRL (см. стр. 9).

Если импортированные сертификаты не содержат CDP, необходимо вручную добавить CDP в список.

### Для добавления CDP вручную:

1. Вызовите меню окна "CDP" и нажмите "Добавить CDP".  
Появится диалог для ввода URL-адреса, подобный следующему.




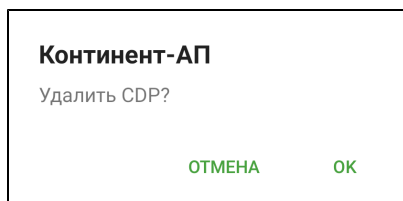
2. В поле "URL" введите адрес CDP в формате:  
`http://[link].crl`  
где [link] — доменное имя требуемого ресурса.
3. Нажмите "Подтвердить".  
Новый CDP будет добавлен в список.

### Для удаления CDP из списка:

#### Примечание.

- CDP, полученные из сертификатов, нельзя удалить вручную. Такие CDP удаляются автоматически после удаления всех сертификатов, из которых они были получены.
- CRL, загруженные из CDP, не будут удалены при удалении этого CDP. CRL можно удалить вручную в окне "CRL".


1. Проведите пальцем справа налево по строке удаляемого CDP и нажмите .  
На экране появится диалог, подобный следующему.



- Нажмите "ОК".  
Выбранный CDP будет удален из списка.

#### Для изменения URL-адреса CDP:

**Примечание.** CDP, полученные из сертификатов, не могут быть изменены.

- Проведите пальцем справа налево по строке изменяемого CDP и нажмите . На экране появится диалог, содержащий URL-адрес выбранного CDP.
- В поле "URL" внесите требуемые изменения.  
URL-адрес CDP должен быть представлен в следующем формате:  
`http://[link].crl`  
где [link] — доменное имя требуемого ресурса.
- Нажмите "Подтвердить".  
Адрес выбранного CDP будет изменен.

#### Загрузка CRL

Автоматическая загрузка CRL происходит следующими способами:

- в результате добавления CDP после импорта сертификатов;
- согласно расписанию в окне "Настройки подключения" (см. стр. 9);
- при каждом запуске приложения "Континент-АП".

#### Внимание!

- Если для CDP не был найден CRL, в строке этого CDP появится отметка "Не найден".
- Если CRL просрочен, в строке соответствующего CDP появится отметка "Устарел".

#### Для загрузки CRL вручную:

**Примечание.** Операция позволяет обновить сразу весь список CRL.

- Вызовите меню окна "CDP" и нажмите "Скачать CRL".  
При успешной загрузке CRL в области уведомлений устройства появится соответствующее сообщение.

## Окно "CRL"

"Континент-АП" позволяет выполнять следующие операции со списками отозванных сертификатов:

- импорт CRL;
- просмотр сведений о CRL;
- экспорт CRL по электронной почте;
- удаление CRL.

#### Для импорта файла CRL:

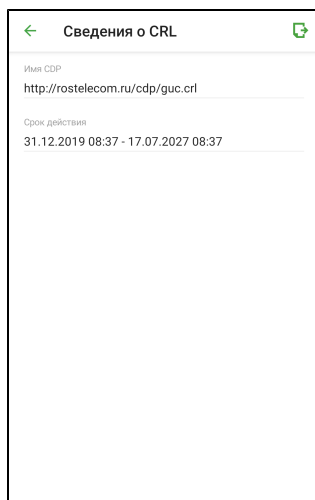
- Вызовите меню окна "CRL" и нажмите "Импортировать CRL".  
На экране появится директория внутренней памяти устройства.
- Выберите нужную папку и нажмите "Выбрать".  
После успешного завершения операции на экране появится соответствующее сообщение.
- Нажмите "ОК".


**Для просмотра сведений о CRL:**

- В окне "CRL" нажатием выберите нужную строку из списка.


**Примечание.** Строка не должна иметь отметок "Не найден" или "Устарел".

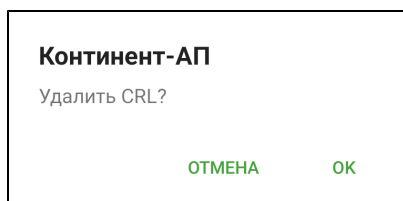
На экране появится окно, подобное следующему.

**Для отправки файла CRL по электронной почте:**

1. В окне "Сведения о CRL" нажмите .
2. "Континент-АП" предложит выбрать приложение для отправки файла. Выберите любой почтовый клиент. Автоматически будут заполнены строки "От", "Тема" и вложен файл CRL.
3. В окне почтового клиента впишите адрес получателя и отправьте письмо.

**Для удаления CRL:**

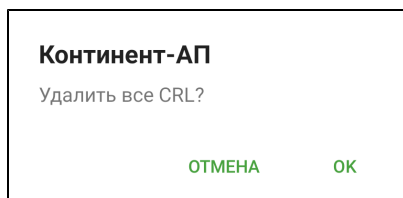
1. В окне "CRL" проведите пальцем справа налево по строке удаляемого CRL.
2. Нажмите . На экране появится диалог, подобный следующему.



3. Нажмите "ОК".  
Выбранный CRL будет удален из списка.

**Для удаления всех CRL:**

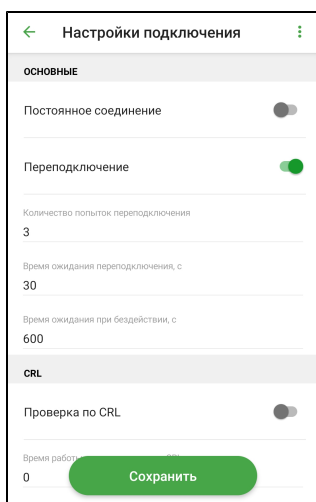
1. В меню окна "CRL" нажмите "Удалить все CRL".  
На экране появится диалог, подобный следующему.



2. Нажмите "ОК".  
Все CRL будут удалены из списка.

## Окно "Настройки подключения"

В окне выполняется настройка параметров подключения к серверу доступа и настройка детализации журналирования. Операции импорта конфигурации, экспорта и импорта настроек выполняются из меню.



## Импорт конфигурации

Файл конфигурации собирается на СД в зашифрованном или незашифрованном виде, в зависимости от версии СД, и содержит следующие компоненты:

| Компонент                  | Параметры   |
|----------------------------|---|
| <b>Версия конфигурации</b> | Номер версии  |
| <b>Профили</b>             | <ol style="list-style-type: none"> <li>1. Название.</li> <li>2. Признак профиля по умолчанию.</li> <li>3. Признак глобального профиля.</li> <li>4. Логин.</li> <li>5. Идентификатор (UUID) пользовательского сертификата.</li> <li>6. Адреса серверов доступа: <ul style="list-style-type: none"> <li>• название;</li> <li>• имя хоста;</li> <li>• порт TCP;</li> <li>• порт UDP</li> </ul> </li> </ol> |
| <b>Ключевые контейнеры</b> | <ol style="list-style-type: none"> <li>1. Идентификатор (UUID).</li> <li>2. Ключевой контейнер.</li> <li>3. Имя ключевого контейнера.</li> <li>4. Случайное число для формирования ключевого контейнера</li> </ol>  |
| <b>Сертификаты</b>         | <ol style="list-style-type: none"> <li>1. Пользовательские.</li> <li>2. Серверные.</li> <li>3. Промежуточные корневые.</li> <li>4. Корневые</li> </ol>  |

Комбинации компонентов файла конфигурации зависят от поставленных задач:

- для быстрого старта — файл конфигурации включает профили, ключевой контейнер и сертификаты;
- для обновления сертификатов — файл конфигурации включает сертификаты и ключевые контейнеры;
- для обновления настроек профиля — файл конфигурации включает профили. Для получения ключевого контейнера и сертификатов пользователь оформляет запрос;

- для ответа на запрос пользователя — файл конфигурации включает профили и сертификаты, ключевой контейнер создается на устройстве пользователя.

Свойства файла конфигурации зависят от СД, на котором он был сформирован:

| Сервер доступа версия 3  | Сервер доступа версия 4                                      |
|--|--|
| Всегда зашифрован  | Шифрование опционально                                       |
| На устройстве всегда набирается энтропия                                   | Энтропия набирается на сервере при формировании файла        |
| При формировании файла доступна комбинация компонентов для быстрого старта | Для формирования файла доступны все перечисленные комбинации |
| Расширение XXX.apcfg   | Расширение XXX.ts4   |

Ниже рассмотрен общий порядок действий при импорте каждой комбинации файла конфигурации.

### Импорт конфигурации для быстрого старта

#### Для импорта конфигурации:

1. Администратор формирует файл конфигурации и передает пользователю по почте или на съемном носителе. Если конфигурация зашифрована, администратор сообщает пользователю пароль от конфигурации и пароли ключевых контейнеров по доверенному каналу.
2. Пользователь переносит полученный файл конфигурации на устройство.
3. Пользователь запускает приложение "Континент-АП", регистрирует свою копию приложения (или пропускает регистрацию и запускает демонстрационный период) и нажимает кнопку "Импортировать файл" на экране загрузки. Пользователь находит файл конфигурации в памяти устройства, выбирает его и нажимает кнопку "Выбрать".
4. Приложение определяет тип конфигурации. Если файл сформирован на СД версии 3, на устройстве появится окно с накоплением энтропии. Если файл сформирован на СД версии 4, шаг с накоплением энтропии пропускается.
5. На этом этапе при необходимости пользователь вводит пароль от конфигурации.
6. Пользователь вводит пароль от ключевого контейнера, так как ключ импортируется из конфигурации и конвертируется в формат для "Континент-АП".

**Примечание.** В состав файла конфигурации может входить несколько ключевых контейнеров. Пользователь должен ввести пароль для каждого ключевого контейнера в наборе.

7. Приложение "Континент-АП" извлекает сертификаты и ключевой контейнер в скрытую папку. В интерфейсе новые сертификаты импортируются в раздел "Сертификаты", создаются новые профили, активным становится профиль с признаком по умолчанию.

Если операция импорта выполнена успешно, приложение "Континент-АП" отобразит главный экран приложения с новым активным профилем.

Если импорт конфигурации для быстрого старта выполняется повторно:

- старые сертификаты, ключевые контейнеры на устройстве и ссылки на сертификаты в приложении не удаляются;
- профиль из конфигурации добавится с именем <имя\_профиля> + 1, а старый профиль останется.

### Импорт конфигурации для обновления сертификатов

#### Для импорта конфигурации:

1. Администратор формирует файл конфигурации и передает пользователю по почте или на съемном носителе. Если конфигурация зашифрована,



администратор сообщает пользователю пароль от конфигурации и пароли ключевых контейнеров по доверенному каналу.

2. Пользователь переносит полученный файл конфигурации на устройство.
3. Пользователь запускает приложение "Континент-АП" и нажимает кнопку "Импортировать конфигурацию" в окне "Настройки подключения".
4. Пользователь находит файл конфигурации в памяти устройства, выбирает его и нажимает кнопку "Выбрать". На этом этапе при необходимости пользователь вводит пароль от конфигурации.
5. Пользователь вводит пароль от ключевого контейнера, так как ключ импортируется из конфигурации и конвертируется в формат для "Континент-АП".

**Примечание.** В состав файла конфигурации может входить несколько ключевых контейнеров. Пользователь должен ввести пароль для каждого ключевого контейнера в наборе.

6. Приложение "Континент-АП" извлекает сертификаты и ключевой контейнер в скрытую папку. В интерфейсе сертификаты импортируются в раздел "Сертификаты".

Если операция импорта выполнена успешно, приложение "Континент-АП" отобразит главный экран приложения.


При совпадении имен существующего и импортируемого сертификата:

- старые сертификаты, ключевые контейнеры на устройстве и ссылки на сертификаты в приложении не удаляются;
- привязка к сертификату в настройках профиля не изменяется.

Если пользователь произведет импорт такой конфигурации из экрана загрузки, для полной настройки приложения необходимо создать профиль. Окно создания профиля отобразится после импорта конфигурации.

## Импорт конфигурации для обновления профиля

### Для импорта конфигурации:

1. Администратор формирует файл конфигурации и передает пользователю по почте или на съемном носителе. Если конфигурация зашифрована, администратор сообщает пользователю пароль от конфигурации по доверенному каналу.
2. Пользователь переносит полученный файл конфигурации на устройство.
3. Пользователь запускает приложение "Континент-АП" и нажимает кнопку "Импортировать конфигурацию" в окне "Настройки подключения".
4. Пользователь находит файл конфигурации в памяти устройства, выбирает его и нажимает кнопку "Выбрать". На этом этапе при необходимости пользователь вводит пароль от конфигурации.
5. Приложение "Континент-АП" извлекает из файла конфигурации информацию о настройках профиля и создает новые профили. Профили импортируются без привязки к сертификату и отмечаются знаком . При попытке активации профиля появится предупреждение: "Не указан сертификат для подключения".
6. Пользователь делает запрос на сертификат и импортирует полученные сертификаты в разделе "Сертификаты".
7. Пользователь редактирует импортированный профиль, привязывает сертификат к новому профилю и нажимает кнопку "Сохранить".

Если операция импорта выполнена успешно, приложение "Континент-АП" отобразит главный экран приложения с новым активным профилем.

Если пользователь произведет импорт конфигурации с помощью экрана загрузки:

- приложение выдаст ошибку "В конфигурации не указан сертификат для подключения. Запросите и импортируйте сертификат".

## Импорт конфигурации после запроса пользователя

### Для импорта конфигурации:

1. Пользователь создает запрос на сертификат с помощью экрана загрузки и отправляет администратору.
2. Администратор на основе запроса формирует файл конфигурации и передает пользователю по почте или на съемном носителе. Если конфигурация зашифрована, администратор сообщает пользователю пароль от конфигурации по доверенному каналу.
3. Пользователь переносит полученный файл конфигурации на устройство.
4. Пользователь запускает приложение "Континент-АП" и нажимает кнопку "Импортировать файл" на экране загрузки.
5. Пользователь находит файл конфигурации в памяти устройства, выбирает его и нажимает кнопку "Выбрать". На этом этапе при необходимости пользователь вводит пароль от конфигурации.
6. Откроется внутренняя директория приложения с предложением выбрать папку для сертификатов. Пользователю необходимо выбрать папку, которая была сформирована при запросе на сертификат.

**Примечание.** Если в папке отсутствует запрос на сертификат и ключевой контейнер, появится сообщение об ошибке: "Не удастся импортировать конфигурацию. Не найден ключевой контейнер".

Приложение "Континент-АП" извлекает из файла конфигурации информацию о сертификате и настройках профиля. В интерфейсе новые сертификаты импортируются в раздел "Сертификаты". В приложении создается новый профиль. Сертификат, соответствующий запросу, и ключевой контейнер привязываются к профилю автоматически. После установки настроек профиль становится активным.

Если операция импорта выполнена успешно, приложение "Континент-АП" отобразит главный экран приложения с новым активным профилем.

Пользователь также может импортировать такую конфигурацию из экрана "Настройки подключения". Предварительно необходимо создать и отправить администратору запрос на сертификат.

### Восстановление настроек

Если в результате действий пользователя или администратора были нарушены настройки профиля или удалены сертификаты, выполните повторный импорт конфигурации. Настройки профиля и сертификаты на устройстве будут восстановлены.

### Экспорт настроек

**Примечание.** Данная функция предназначена для переноса настроек с одного устройства на другое исключительно для одного конкретного пользователя. Нельзя передавать файл с настройками другим пользователям.

Экспорт настроек предназначен для переноса готового набора профилей, сертификатов и ключевых контейнеров на новое устройство. Операция "Экспортировать настройки" предшествует операции "Импортировать настройки". В отличие от файла конфигурации файл настроек формируется на устройстве и имеет формат settings.json.

**Для экспорта настроек:**

1. Вызовите меню окна "Настройки подключения".
2. Нажмите "Экспортировать настройки".  
Приложение предложит выбрать папку для сохранения файла.
3. Отметьте папку и нажмите "Выбрать".  
На экране появится сообщение об успешном сохранении файла. Приложение вернет пользователя в окно "Настройки подключения".

Сохраненный файл извлеките из памяти устройства любым доступным способом и передайте на другое устройство для выполнения операции импорта.

**Импорт настроек**

**Примечание.** Данная функция предназначена для переноса настроек с одного устройства на другое исключительно для одного конкретного пользователя. Нельзя передавать файл с настройками другим пользователям.

Операция предназначена для установки пакета настроек из другого приложения. Перед выполнением импорта создайте папку и разместите в ней файл настроек settings.json.

**Для импорта настроек:**

1. Вызовите меню окна "Настройки подключения".
2. Нажмите "Импортировать настройки".  
Откроется директория внутренней памяти устройства.
3. Выберите в папке файл настроек и нажмите кнопку "Выбрать".

**Примечание.** После импорта настроек все сертификаты импортируются скрытыми (см. стр. 23).

## Глава 4

# Служебные операции

### Обновление

Обновление приложения "Континент-АП" выполняется при переходе на новую версию в стандартном магазине приложений (например, в Google Play).

#### Примечание.

- В зависимости от настроек устройства пользователя, приложения могут обновляться автоматически. Проверить версию "Континент-АП", установленную на устройстве, можно в разделе приложения "О программе".
- Для работы с Google Play необходимо наличие учетной записи Google.

#### Для обновления приложения вручную:

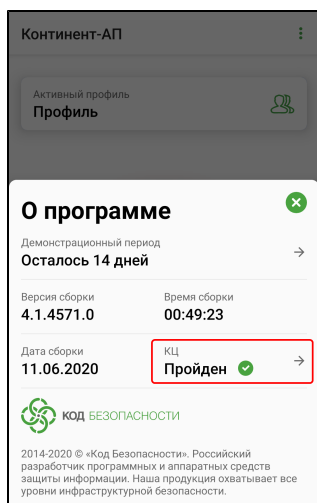
- В стандартном магазине приложений найдите приложение "Континент-АП" и выполните стандартную процедуру обновления.

### Контроль целостности

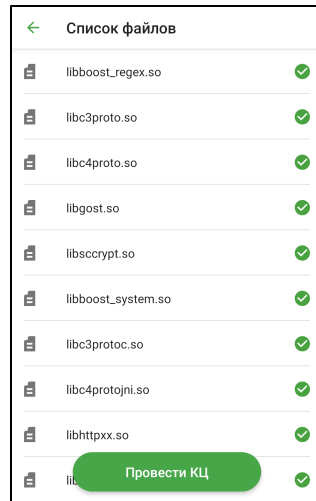
Контроль целостности (далее — КЦ) файлов заключается в сравнении текущих значений контрольных сумм с эталонными значениями контрольных сумм динамических библиотек, заранее вычисленных при установке приложения на устройстве.

#### Для проведения КЦ приложения:

1. В главном окне откройте меню (см. стр. 17) и выберите пункт "О программе".
2. В появившемся окне нажмите на область, указанную на рисунке ниже.



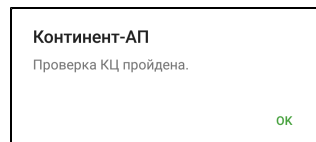
Откроется окно "Список файлов".



### 3. Нажмите кнопку "Провести КЦ".

При обнаружении нарушения КЦ работа приложения блокируется, в журнале записывается соответствующее событие. Для восстановления работы необходимо переустановить приложение.

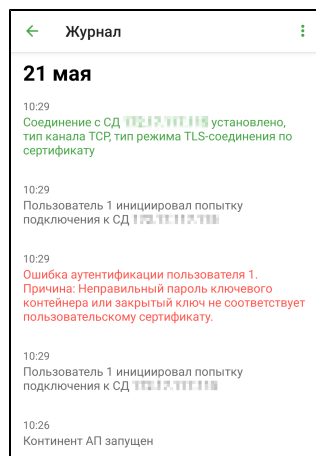
Если КЦ пройден успешно, появится сообщение, подобное следующему.



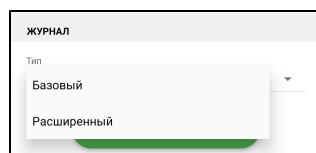
## Журнал

### Журнал работы приложения

В окне "Журнал" содержатся сведения о работе приложения "Континент-АП" за период работы с момента установки приложения.



В журнале предусмотрены два уровня детализации: базовый и расширенный.

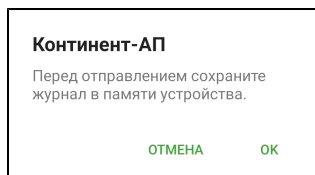


Расширенный уровень детализации включается в разделе "Настройки подключения" (см. стр. 10). Все возможные события, уровень их детализации и цветовое обозначение представлены в таблице ниже.

| Уровень детализации | Цвет    | Событие   |
|---------------------|---------|---|
| Базовый             | Черный  | "Континент-АП" запущен  |
| Базовый             | Черный  | Добавлена ссылка на папку с сертификатом пользователя                                   |
| Базовый             | Черный  | Удалена ссылка на папку с сертификатом пользователя                                     |
| Базовый             | Черный  | Соединение с СД разорвано   |
| Базовый             | Черный  | Пользователь инициировал попытку подключения к СД                                       |
| Базовый             | Черный  | Добавлена ссылка на папку с корневым сертификатом                                       |
| Базовый             | Черный  | Удалена ссылка на папку с корневым сертификатом   |
| Базовый             | Зеленый | Соединение с СД установлено   |
| Базовый             | Зеленый | Пользователь создал запрос на сертификат и ключевой контейнер                           |
| Базовый             | Красный | Произошла системная ошибка  |
| Базовый             | Красный | Ошибка аутентификации пользователя  |
| Расширенный         | Черный  | Пользователь внес изменения в настройки проверки сертификатов                           |
| Расширенный         | Черный  | Пользователь добавил CDP  |
| Расширенный         | Черный  | Пользователь изменил CDP  |
| Расширенный         | Черный  | Загрузка CRL  |
| Расширенный         | Черный  | Пользователь импортировал CRL из файла  |
| Расширенный         | Черный  | Проверка целостности файла выполнена успешно  |
| Расширенный         | Черный  | Выполнен перерасчет контрольной суммы файла   |
| Расширенный         | Черный  | Пользователь изменил параметры подключения к СД   |
| Расширенный         | Зеленый | Запуск процедуры проверки целостности файлов выполнен успешно                           |
| Расширенный         | Красный | СД не ответил на отклик за указанное время  |
| Расширенный         | Красный | СД разорвал соединение с АП   |
| Расширенный         | Красный | Ошибка подключения: использован неподдерживаемый на СД режим организации VPN-соединения |
| Расширенный         | Красный | Нарушена целостность файла. Создание новых сессий запрещено                             |

**Для отправки журнала в техническую поддержку:**

1. В окне "Журнал" откройте меню и нажмите "Отправить журнал".  
Откроется окно, подобное следующему.



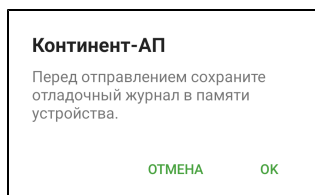
2. Нажмите "ОК".  
Откроется директория внутренней памяти устройства.
3. Выберите папку и нажмите "Выбрать".  
Файл журнала log.json будет создан и сохранен в указанную папку.
4. "Континент-АП" предложит выбрать приложение для отправки журнала.  
Выберите любой почтовый клиент.  
Автоматически будут заполнены строки "От", "Тема" и вложен файл журнала.
5. В окне почтового клиента впишите адрес и отправьте письмо администратору.

**Отладочный журнал**

Отладочный журнал предназначен для проведения детального анализа в случае сбоя в работе приложения.

**Для отправки журнала в техническую поддержку:**

1. В окне "Журнал" откройте меню и нажмите "Отправить отладочный журнал".  
Откроется окно, подобное следующему.



2. Нажмите "ОК".  
Откроется директория внутренней памяти устройства.
3. Выберите папку и нажмите "Выбрать".  
Файл журнала logcat.log будет создан и сохранен в указанную папку.
4. "Континент-АП" предложит выбрать приложение для отправки журнала.  
Выберите любой почтовый клиент.  
Автоматически будут заполнены строки "От", "Тема" и вложен файл журнала.
5. В окне почтового клиента впишите адрес и отправьте письмо администратору.

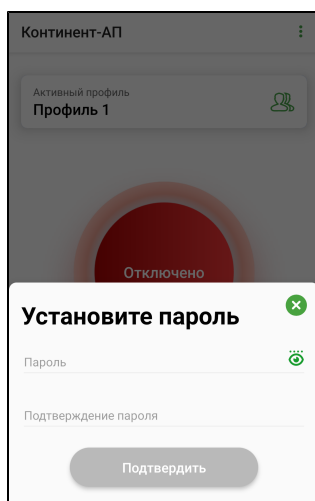
## Управление режимом работы

"Континент-АП" функционирует в двух режимах:

| Основной режим   |
|--|
| <p>Устанавливается по умолчанию. Пользователю предоставляются права полного доступа.</p> <p>Права в основном режиме:</p> <ul style="list-style-type: none"> <li>• подключение и отключение от СД;</li> <li>• просмотр списка профилей;</li> <li>• активация профиля;</li> <li>• просмотр информации о профиле и редактирование;</li> <li>• удаление профиля;</li> <li>• экспорт/импорт настроек;</li> <li>• импорт конфигурации;</li> <li>• создание запроса на сертификат;</li> <li>• импорт сертификата;</li> <li>• просмотр импортированных сертификатов;</li> <li>• просмотр сведений о сертификате;</li> <li>• импорт ключа;</li> <li>• управление CRL;</li> <li>• управление CDP;</li> <li>• удаление сертификата;</li> <li>• скрытие сертификата во внутренней памяти устройства;</li> <li>• просмотр и редактирование настроек подключения;</li> <li>• смена режима работы;</li> <li>• просмотр и сохранение журнала;</li> <li>• просмотр раздела "О программе"</li> </ul> |
| Частный режим  |
| <p>Пользователю предоставляются права ограниченного доступа к управлению настройками приложения. Права в частном режиме:</p> <ul style="list-style-type: none"> <li>• подключение и отключение от СД по заранее активированному профилю;</li> <li>• просмотр и сохранение журнала;</li> <li>• просмотр раздела "О программе"</li> </ul>  |

### Для смены режима работы:

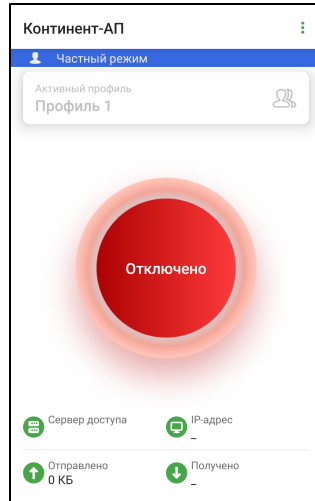
1. Вызовите меню приложения "Континент-АП".
2. В появившемся меню выберите пункт "Сменить режим".  
На экране появится окно "Установите пароль".



3. Введите пароль блокировки в поля "Пароль" и "Подтверждение пароля".
4. Нажмите "Подтвердить".



На главном экране появится надпись "Частный режим" на синем фоне, функции приложения будут ограничены.



Чтобы сменить режим работы, повторите предыдущую операцию еще раз. Если надпись "Частный режим" в главном окне приложения пропала, значит — активирован основной режим.