



КОД БЕЗОПАСНОСТИ

Средство криптографической защиты информации

"Континент-АП"

Версия 3.7 (исполнение 8)

Руководство по эксплуатации

Android



КОД БЕЗОПАСНОСТИ

© Компания "Код Безопасности", 2018. 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:	http://www.securitycode.ru

Оглавление

Введение	4
Общие сведения	5
Назначение абонентского пункта	5
Сертификаты	5
Профили	6
Общий порядок установки и настройки "Континент-АП"	7
Эксплуатация	8
Установка	8
Описание главного окна приложения	9
Настройка "Континент-АП"	10
Импорт настроек	11
Ручная настройка приложения	12
Вкладка "Подключение"	14
Общие параметры подключения	14
Соединение с сервером доступа	16
Просмотр сведений	19
Вкладка "Профили"	20
Список профилей	20
Переименование профиля	22
Редактирование параметров профиля	22
Экспорт профиля	22
Изменение статуса профиля	23
Удаление профиля	23
Вкладка "Сертификаты"	24
Описание вкладки "Сертификаты"	24
Установка списка отозванных сертификатов	25
Служебные операции	26
Обновление	26
Контроль целостности	27
Создание файла журнала	31
Управление режимом работы	31
Приложение	33
Пример xml-файла для настройки параметров "Континент-АП"	33

Введение

Документ предназначен для пользователей изделия "Средство криптографической защиты информации "Континент-АП". Версия 3.7 (исполнение 8) RU.88338853.501430.007 03. В нем содержатся сведения, необходимые пользователю для доступа к защищаемым ресурсам средствами абонентского пункта на платформе Android.

Служба технической поддержки. Связаться со службой технической поддержки можно по телефону 8-495-982-30-20 или по электронной почте support@securitycode.ru. Страница службы технической поддержки на сайте компании "Код Безопасности": <https://www.securitycode.ru/products/technical-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 на курсах Учебного центра "Информзащита". Перечень курсов и условия обучения представлены на сайте <https://www.itsecurity.ru/>. Связаться с представителем Учебного центра можно по электронной почте (edu@itsecurity.ru).

Глава 1

Общие сведения

Назначение абонентского пункта

Средство криптографической защиты информации "Континент-АП" (далее — "Континент-АП", приложение) входит в состав изделия "Аппаратно-программный комплекс шифрования "Континент" (далее — 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 операционной системы (ОС) Android 5.0 и выше.

Абонентский пункт реализует следующие основные функции:

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

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 — 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).

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 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.

Профили

Перед установлением соединения с сервером доступа выполните настройку параметров подключения.

Назначение параметров подключения разъясняется в таблице ниже:

Параметр	Описание
Адрес сервера доступа	IP-адрес или имя сервера доступа
Сертификат для подключения	Необходимый для подключения к серверу доступа сертификат пользователя. Список доступных сертификатов представляет собой список размещенных на мобильном устройстве папок, содержащих сертификаты и ключи. Место размещения папок указано в пункте "Папка хранения сертификатов" меню "Настройки"
Режим защищенного соединения	Способ подключения абонентского пункта к серверу доступа: • стандартное подключение (UDP); • потоковое подключение (TCP); • подключение через прокси (только для TCP)
Прокси	Признак использования прокси-сервера для подключения к серверу доступа. Имеет два значения: • выключено; • включено. При нажатии на строку параметра открывается окно настроек подключения к прокси-серверу
Порт сервера доступа	Порт сервера доступа. По умолчанию устанавливаются значения 443 для TCP и 4433 для UDP
Порт клиента	Порт мобильного устройства. По умолчанию устанавливается значение 7500
Основной DNS, альтернативный DNS	По умолчанию используются адреса DNS-серверов, получаемые от сервера доступа. Если адреса от сервера доступа не поступают, их указывают вручную. Адреса, полученные от сервера доступа, имеют приоритет над адресами, указанными вручную
Домен	DNS-суффикс. По умолчанию не используется. При необходимости можно указать DNS-суффикс, добавляемый автоматически к имени хоста при обращении к защищаемым ресурсам
MTU	Максимальный размер блока (в байтах) на канальном уровне сети. По умолчанию устанавливается значение 1500
Адрес сервера	Сетевое имя или IP-адрес прокси-сервера (только для "Подключение через прокси")
Порт	Порт прокси-сервера (только для "Подключение через прокси"). По умолчанию устанавливается значение 3128

Параметр	Описание
Аутентификация	Тип аутентификации: • без аутентификации; • Basic; • NTLM. Поле доступно, если выбрано подключение через прокси
Имя пользователя	Имя пользователя для аутентификации на прокси-сервере. Поле доступно, если выбрано подключение через прокси
Пароль	Пароль пользователя для аутентификации на прокси-сервере. Поле доступно, если выбрано подключение через прокси

Так как параметры подключения изменяются (например, подключение к разным серверам доступа, использование разных сертификатов и т. д.), для каждого подключения предварительно устанавливаются конкретные значения параметров и сохраняются в виде профиля настроек с присвоенным ему именем.

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

Предусмотрены операции экспорта и импорта профиля. Операция экспорта применяется при переносе профиля, настроенного на конкретном мобильном устройстве, на другое устройство с установленным "Континент-АП". Операция импорта применяется для установки на конкретном устройстве профиля, настроенного на другом устройстве с "Континент-АП".

Для использования нового профиля при подключении к серверу доступа присвойте ему статус "активный". Статус "активный" может быть назначен любому профилю, имеющемуся в списке. При подключении профиль со статусом "активный" используется по умолчанию.

Общий порядок установки и настройки "Континент-АП"

Для установки и настройки СКЗИ "Континент-АП" выполните следующие действия:

1. Установите на мобильное устройство приложение "Континент-АП" (см. стр. **8**).
2. Получите у администратора и установите на абонентском пункте сертификат пользователя и корневой сертификат (см. стр. **12**).
3. Создайте профиль (см. стр. **14**).
4. Настройте параметры подключения к серверу доступа (см. стр. **15**).
5. Выполните подключение к серверу доступа (см. стр. **16**).
6. Перейдите в режим пользователя и передайте устройство (см. стр. **31**).

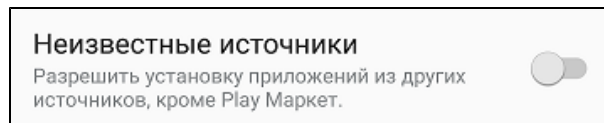
Глава 2

Эксплуатация

Установка

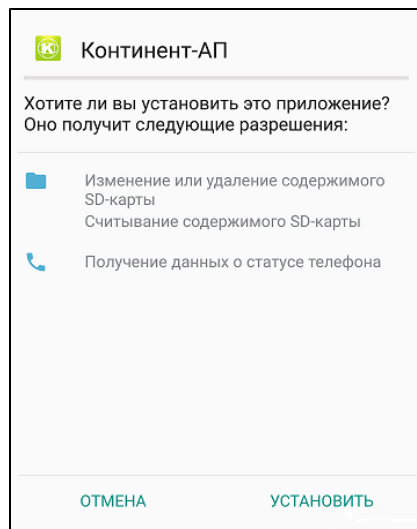
Для установки приложения:

1. Разрешите установку приложений из неизвестных источников, передвинув переключатель вправо.



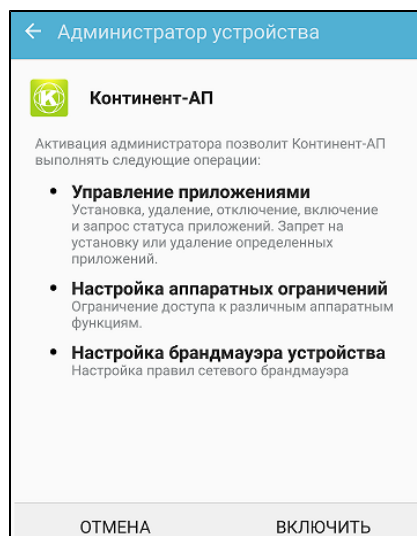
2. Получите от администратора дистрибутив vpncontinent.apk (например, по электронной почте).
3. Скачайте установочный пакет vpncontinent.apk на мобильное устройство.
4. Откройте файловый менеджер, выберите и запустите vpncontinent.apk.

Появится окно установщика приложений Android.



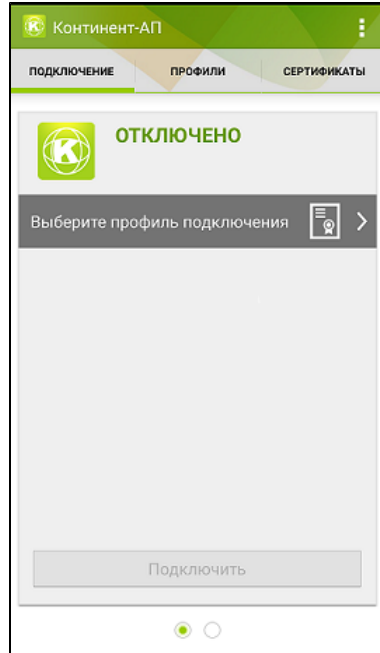
5. Нажмите кнопку "Установить". Начнется установка "Континент-АП"

После окончания установки появится окно с запросом административных прав.



6. Нажмите кнопку "Включить".

Приложение запустится, и откроется окно.

**Описание главного окна приложения**

Центральная часть окна состоит из трех вкладок:

Вкладка	Описание
Подключение	Подключение и отключение от сервера доступа. Просмотр статистики текущей сессии
Профили	Просмотр, создание и настройка профилей подключения
Сертификаты	Работа с сертификатами и импорт ключевого контейнера

Вкладка "Подключение" состоит из двух секций – управления подключением и просмотра статистики. В зависимости от модели мобильного устройства или разрешения экрана секции могут отображаться одновременно или быть разнесены на соседние страницы. Во втором варианте для перехода между страницами проведите пальцем по экрану влево/вправо или используйте переключатель, расположенный в нижней части экрана:



В правом верхнем углу главного окна расположена кнопка вызова дополнительного меню .

В зависимости от модели используемого мобильного устройства кнопка вызова дополнительного меню может отсутствовать. Вместо нее используется кнопка устройства , расположенная ниже главного окна приложения.

Состав пунктов дополнительного меню зависит от активной в данный момент вкладки ("Подключение", "Профили", "Сертификаты").

Ниже в таблице приводится полный список пунктов дополнительного меню:

Пункт меню	Описание
Заблокировать	Включает режим ограниченного доступа к управлению настройкой "Континент-АП" — режим пользователя (см. стр. 31)
Разблокировать	Включает режим полного доступа к управлению настройкой "Континент-АП" — режим администратора (см. стр. 31). Режим администратора устанавливается по умолчанию
Скрыть	Сохраняет сертификаты и ключевой контейнер во внутренней памяти устройства, недоступной для пользователя. Параметр недоступен в режиме пользователя
Показать	Перемещает сертификаты и ключевой контейнер из недоступной для пользователя внутренней памяти устройства в доступную. Параметр недоступен в режиме пользователя
Переименовать	Запускает процедуру переименования выбранного в списке профиля подключения (см. стр. 22). Параметр недоступен в режиме пользователя
Импорт ключа	Запускает процедуру импорта закрытого ключа (см. стр. 12). Параметр недоступен в режиме пользователя
Импорт настроек	Осуществляет автоматическую настройку всех параметров "Континент-АП" (см. стр. 11). Параметр недоступен в режиме пользователя
Импорт	Запускает процедуру импорта профиля (см. стр. 11). Параметр недоступен в режиме администратора
Экспорт	Запускает процедуру экспорта профиля (см. стр. 22). Параметр недоступен в режиме пользователя
Удалить	Запускает процедуру удаления выбранного в списке профиля (см. стр. 23). Активный профиль удалить невозможно. Параметр недоступен в режиме пользователя
Настройки	Открывает окно просмотра и настройки общих параметров подключения (см. стр. 14). Параметр недоступен в режиме пользователя
Журнал	Открывает стандартное окно выбора папки для сохранения журнала (см. стр. 31)
Обновление ПО	Запускает процедуру обновления программного обеспечения "Континент-АП" (см. стр. 26). Параметр недоступен в режиме пользователя
О программе	Выводит на экран сведения о текущей версии программного обеспечения и контрольные суммы динамических библиотек абонентского пункта (см. стр. 19)

Настройка "Континент-АП"

Перед началом работы пользователь должен установить сертификаты безопасности и зарегистрировать профиль.

Если пользователь получил сформированный пользовательский профиль со всеми настройками в формате .xml файла, он должен выполнить операцию импорта.

Импорт настроек

Внимание. Операцию нельзя выполнить в следующих случаях:

- включен общий параметр "Постоянное соединение" (см. таблицу на стр. 14);
- включен режим пользователя (см. стр. 31);
- абонентский пункт находится в одном из режимов: "Инициализация", "Поиск сервера", "Авторизация", "Конфигурация", "Подключено", "Отключено", "Переключено" (см. вкладку "Подключение" главного окна абонентского пункта).

Перед выполнением импорта создайте папку и разместите в ней следующие файлы:

- profile.xml — файл с параметрами подключения. Пример реализации xml-файла с именем profile.xml представлен в приложении на стр. 33;
- user.cer — сертификат пользователя;
- root.p7b — корневой сертификат;
- ключ формата программы управления сервером доступом (hex-строка) или user.key.

В дополнительном меню "Континент-АП" на папке с размещенными в ней файлами для импортирования появится значок шестеренки:

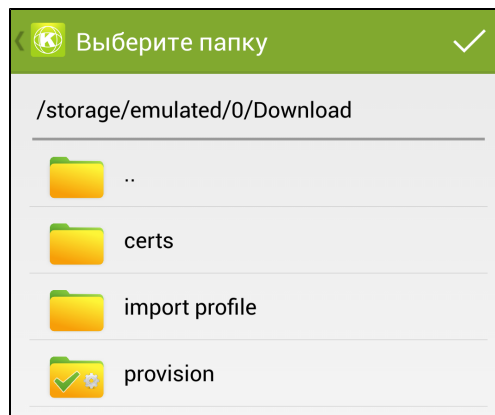


Если значок отсутствует, значит — процедура копирования файлов выполнена с ошибкой.

Для импорта настроек:

1. Вызовите дополнительное меню приложения "Континент-АП".
2. В появившемся меню выберите пункт "Импорт настроек".

На экране появится окно "Выберите папку".



3. Выберите папку со значком шестеренки. На пиктограмме папки появится галочка.
4. На планшетном компьютере нажмите кнопку "Выбрать", на смартфоне — кнопку , расположенную в правом верхнем углу окна.

На экране появится сообщение о процессе выполнения импорта настроек.

По окончании успешного импорта появится соответствующее сообщение, в противном случае — сообщение об ошибке.

Когда импорт настроек будет успешно завершен, перейдите на вкладку "Подключение" для соединения с сервером доступа (см. стр. 14).

Примечание. Для импорта профиля пользователь должен выполнить вышеуказанные инструкции только для файла profile.xml.

Ручная настройка приложения

Если сформированный пользовательский профиль отсутствует, выполните ручную настройку "Континент-АП".

Получение и установка сертификатов доступа

В "Континент-АП" реализованы два способа получения сертификатов: с помощью загрузки файлов на мобильное устройство и оформления запроса на получение сертификата и ключевого контейнера.

Шаг 1. Загрузка файлов на мобильное устройство

Существуют два варианта загрузки файлов:

- Непосредственная передача файлов сертификатов и ключевого контейнера на мобильное устройство по электронной почте.

Сохраните файлы в папку хранения сертификатов пользователя (см. параметр "Папка хранения сертификатов" в таблице на стр. 14).

- Передача файлов сертификатов и ключевого контейнера на мобильное устройство при подключении к компьютеру.

Скопируйте файлы сертификатов и ключевого контейнера в папку хранения сертификатов и отключите устройство от компьютера средствами безопасного отключения ОС Windows.

Шаг 2. Импорт ключа

Для импорта ключа:

1. Запустите приложение и перейдите на вкладку "Сертификаты".
2. На вкладке "Сертификаты" нажмите кнопку вызова дополнительного меню  (если кнопка отсутствует, вместо нее используется кнопка устройства , расположенная ниже главного окна приложения) и выберите пункт "Импорт ключа".

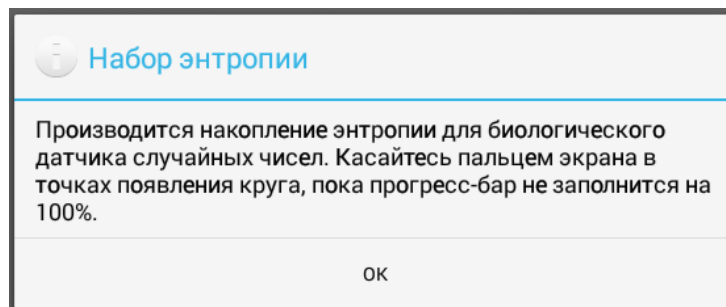
На экране появится стандартный диалог выбора папки.

В абонентском пункте на папку с размещенными в ней файлами сертификатов и ключевого контейнера наносится значок ключа.



3. Выберите папку с изображением ключа и нажмите кнопку "Выбрать".

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



4. Нажмите кнопку "ОК" в окне сообщения и нажимайте круг, перемещающийся по экрану, до завершения процесса накопления энтропии.

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

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

5. Введите пароль, полученный у администратора, и нажмите кнопку "ОК".
Операция будет завершена, и появится сообщение об успешном импорте ключа.

Примечание. Для просмотра сведений о сертификате выберите сертификат в списке. Если установленный сертификат не отобразится в списке, перейдите на любую другую вкладку, после чего вернитесь на вкладку "Сертификаты".

Если сертификат по-прежнему не отображается на экране, перезагрузите устройство и запустите приложение заново.

Шаг 3. Создание запроса на сертификат

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

Для создания запроса:

1. На вкладке "Сертификаты" нажмите кнопку .

На экране появится форма запроса на получение нового сертификата. При

этом кнопка  изменит вид на .

2. Введите сведения о пользователе.

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

- При указании криптопровайдера выберите его на основании сведений, полученных от администратора ("КриптоПро" или "Код Безопасности").
- По умолчанию запрос на получение сертификатов и ключевой контейнер будут сохранены во внутренней памяти устройства в папке с именем, указанным в поле "Имя сотрудника". Путь к папке задается в настройках общих параметров подключения (см. параметр "Папка хранения сертификатов" в таблице на стр. 14).

3. После ввода сведений нажмите кнопку .

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

4. Нажмите кнопку "ОК" в окне сообщения и, следуя инструкции, нажимайте на круг, перемещающийся по экрану, до завершения процесса накопления энтропии.

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

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

5. Введите и подтвердите пароль и нажмите кнопку "ОК".

Файл запроса и ключевой контейнер будут сохранены в указанной папке.

Передайте файл запроса администратору безопасности любым возможным способом (например, подключив устройство к компьютеру).

Примечание. Если папка, содержащая запрос на получение сертификата, не отобразится на экране компьютера, отключите устройство, перезагрузите его и, запустив приложение, подключите устройство к компьютеру.

6. Полученные от администратора файлы сертификатов поместите в папку с хранящимся в ней файлом запроса.

Запустите приложение, перейдите на вкладку "Сертификаты" и убедитесь в наличии установленных сертификатов в списке.

Создание нового профиля

Пользователь импортирует или создает новый профиль. Для импорта профиля воспользуйтесь инструкцией на стр. [11](#).

Для создания нового профиля:

1. Нажмите кнопку , расположенную в верхней части экрана.
На экране появится диалог ввода имени создаваемого профиля.
2. Введите имя профиля и нажмите кнопку "ОК".
В списке появится имя нового профиля и в центральной части экрана отобразятся его параметры. Некоторые значения параметров задаются по умолчанию (описание параметров см. в таблице на стр. [6](#)).
3. Укажите необходимые значения параметров нового профиля:
 - для указания сертификата активируйте поле "Сертификат для подключения", выберите сертификат из списка и нажмите кнопку , расположенную в верхней части экрана;
 - для выбора параметров подключения через прокси, установите значение "Включено", активируйте строку "Прокси" и в открывающейся группе параметров введите их значения. Далее нажмите кнопку "Назад", расположенную в нижней части экрана устройства;
 - для ввода дополнительных параметров установите отметку в поле "Дополнительно" и введите их значения.
4. Для присвоения созданному профилю статуса "активный", после ввода значений параметров нажмите кнопку , расположенную в верхней части экрана.
Новый профиль получит статус "активный" и будет выполнен переход на вкладку "Подключение".

Вкладка "Подключение"

Общие параметры подключения

Перед установлением соединения с сервером доступа выполните настройку общих параметров, действующих для всех подключений.

Назначение общих параметров разъясняется в таблице ниже:

Параметр	Описание
Запрет незащищенных соединений	Параметр принимает одно из трех значений: • "Нет запрета" — разрешаются любые сторонние соединения во время сеанса связи абонентского пункта и сервера доступа. Запрет сторонних соединений, установленный на сервере доступа, имеет более высокий приоритет. • "Запрет после подключения" — запрещаются любые сторонние соединения абонентского пункта после установления связи с сервером доступа. • "Запрет до и после подключения" — всегда запрещаются любые сторонние соединения абонентского пункта как до, так и после установления связи с сервером доступа. Режим поддерживается только в некоторых моделях устройств

Параметр	Описание
Постоянное соединение	Соединение, отключаемое только средствами настройки общих параметров подключения и которое автоматически восстанавливается после потери сетевого соединения. Для реализации постоянного соединения с сервером доступа предварительно настройте или выберите профиль подключения. Параметр имеет одно из двух значений: "Да" (есть отметка) или "Нет" (отметка отсутствует). Для установления постоянного подключения введите пароль. Применение параметра блокирует управление некоторыми другими параметрами подключения
Переподключаться автоматически	Автоматическое переподключение при потере сетевого соединения или при разрыве защищенного канала по инициативе сервера доступа АПКШ "Континент". Параметр может принимать два значения: "Да" (есть отметка) или "Нет" (отметка отсутствует). Недоступно для управления, если установлен параметр "Постоянное соединение"
Количество попыток переподключения	По умолчанию равно 3 (трем). При необходимости может быть изменено. После последней неудачной попытки выводится сообщение об ошибке подключения. Недоступно для управления, если установлены параметры "Переподключаться автоматически" или "Постоянное соединение"
Тайм-аут переподключения	Пауза между попытками подключения (в секундах). По умолчанию устанавливается значение 30. Недоступно для управления, если установлен параметр "Переподключаться автоматически"
Тайм-аут неактивности	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. Недоступно для управления, если установлен параметр "Постоянное соединение"
Папка хранения сертификатов	Имя директории, в которой хранятся папки пользователя с запросом на получение сертификатов, сертификатом пользователя, корневым сертификатом и ключевым контейнером. Каждому профилю подключения должна соответствовать своя папка с сертификатами

Для настройки общих параметров подключения:

1. В главном окне приложения нажмите кнопку вызова дополнительного меню и выберите пункт "Настройки".

На экране появится окно настройки общих параметров подключения.

2. Установите значения параметров и нажмите кнопку "Сохранить" (в смартфоне кнопка располагается в верхней части экрана).

Для отмены выполненных изменений нажмите кнопку "Отменить" (в смартфоне нажмите кнопку "Назад" в нижней части экрана).

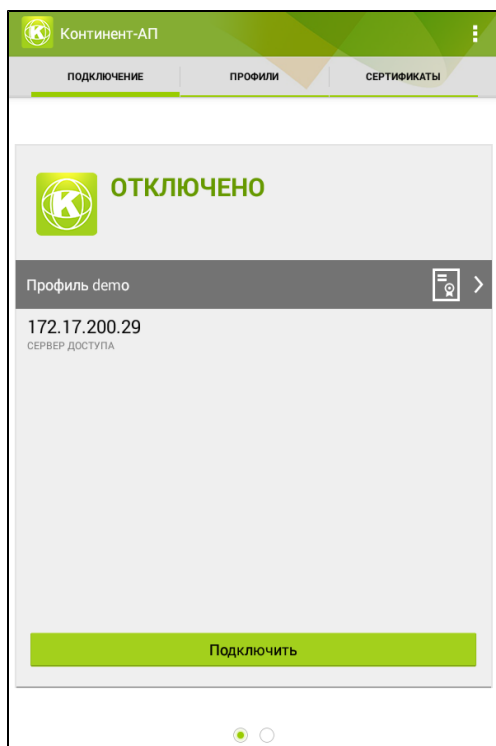
Соединение с сервером доступа

Для подключения к серверу доступа:

Примечание. Перед подключением к серверу доступа:

- на мобильном устройстве установите сертификат пользователя, корневой сертификат, а также ключевой контейнер;
- настройте профиль подключения к серверу доступа;
- настройте общие параметры подключения.

1. В главном окне приложения перейдите на вкладку "Подключение".



На вкладке приводятся следующие сведения:

- состояние подключения ("отключено");
- имя используемого профиля подключения;
- IP-адрес или имя сервера доступа, для подключения к которому используется данный профиль.

Примечание. Для просмотра параметров настройки профиля активируйте строку с его именем. Значения параметров редактируются. После просмотра или редактирования параметров вернитесь на вкладку "Подключение".

Для подключения с помощью другого профиля активируйте строку с его именем, выберите в списке профиль и переведите его статус в "активный" (см. стр. [20](#)).

2. Нажмите кнопку "Подключить".

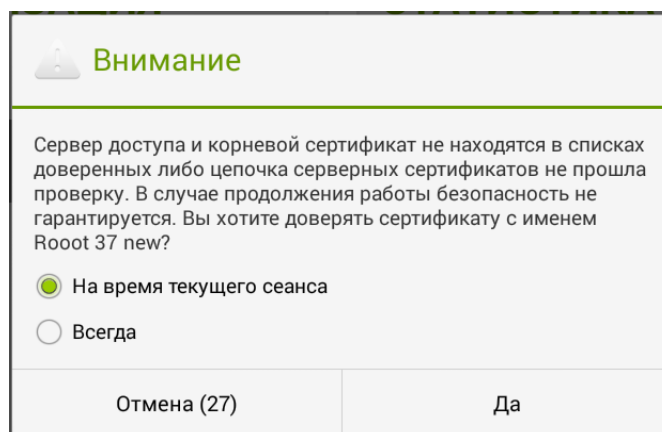
На экране появится запрос на ввод пароля доступа к ключевому контейнеру.

3. Введите пароль и нажмите кнопку "ОК".

Примечание. Если подключение выполняется в первый раз, на экране может появиться системное предупреждение о доверии приложению. Установите отметку в поле "Я доверяю этому приложению" и нажмите кнопку "ОК".

Начнется подключение к серверу доступа.

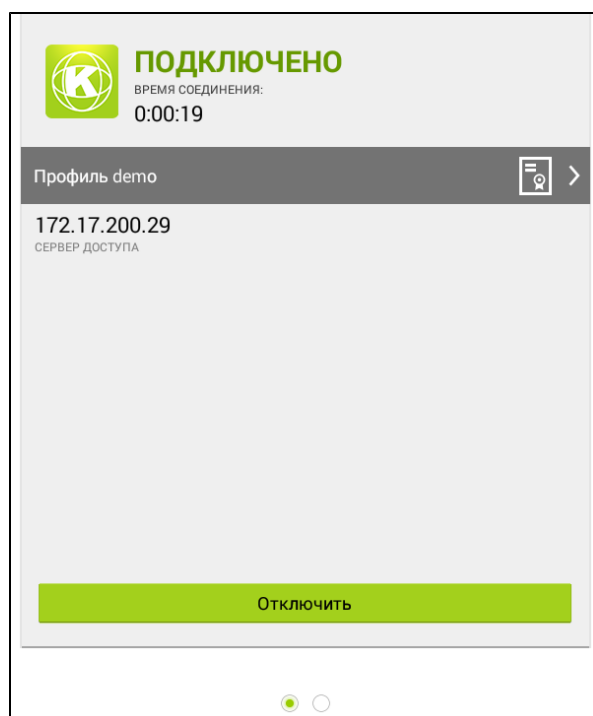
4. Если корневой сертификат, установленный на мобильном устройстве, не соответствует корневому сертификату, присланному сервером доступа в момент подключения, на экране появится сообщение, что сервер доступа и корневой сертификат не находятся в списке доверенных.



Если вы хотите продолжить работу, выберите период доверия и нажмите кнопку "Да". Подключение продолжится.

В ином случае нажмите кнопку "Отмена" и получите новый сертификат (см. стр. 13).

После успешного завершения процедуры аутентификации произойдет подключение "Континент-АП" к серверу доступа и состояние подключения изменится на "подключено" с отображением времени подключения, а кнопка "Подключить" изменит свое название на "Отключить".



Внимание. После подключения к серверу доступа на панели уведомлений, расположенной в верхней части экрана, появится значок . Коснитесь значка и проведите пальцем вниз — откроется окно с информацией о текущем сеансе связи и кнопки "Отмена" (для закрытия окна) и "Разъединить" (для разрыва соединения с сервером доступа).

Для разрыва соединения:

Пояснение. Разрыв соединения невозможен, если абонентский пункт находится в режиме постоянного соединения (см. параметр "Постоянное соединение" в таблице на стр. 14).

1. В главном окне приложения перейдите на вкладку "Подключение".
2. Нажмите кнопку "Отключить".

Произойдет отключение абонентского пункта от сервера доступа.

Внимание. Если разрыв соединения произошел без участия пользователя, на панели уведомлений мобильного устройства появится значок . Коснитесь значка и проведите пальцем вниз — откроется сообщение "Соединение с сервером разорвано".
Значок приложения "Континент-АП" будет отображаться до тех пор, пока пользователь не установит соединение с сервером доступа.

Просмотр сведений

В приложении "Континент- АП" реализован просмотр сведений о текущем состоянии соединения с сервером доступа, о защищенных подсетях, а также о текущей версии программного обеспечения абонентского пункта.

Для просмотра сведений о текущем состоянии соединения:

- При установленном соединении с сервером доступа в главном окне приложения "Континент-АП" перейдите на вкладку "Подключение".

Сведения о текущем состоянии соединения отобразятся в секции просмотра статистики:

СТАТИСТИКА	
Виртуальный IP-адрес	200.1.1.3
Защищенные подсети	126.0.0.0/29 126.0.0.8/29 124.0.0.0/29 Подробнее
Передано, байт	1515
Принято, байт	2939
Отброшено, байт	0
Передано, пакетов	7
Принято, пакетов	5
Отброшено, пакетов	0

Примечание. Если секция просмотра статистики на вкладке не отображается, перейдите на соседний экран (см. пояснение на стр.9).

Статистика показывает значения следующих параметров:

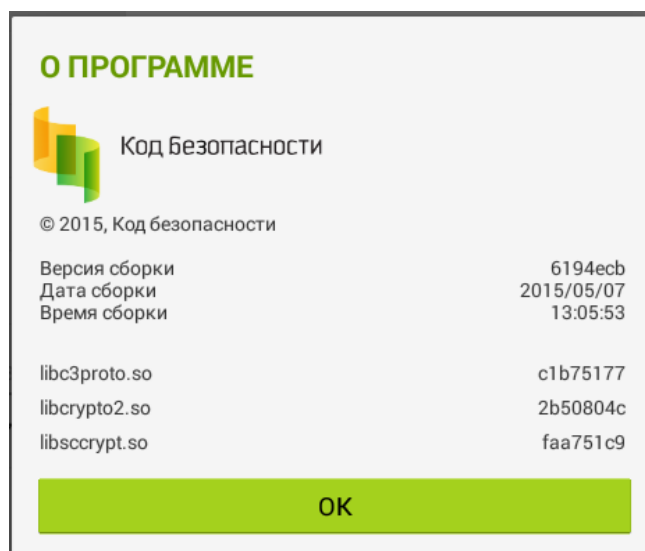
- виртуальный IP-адрес мобильного устройства;
- список защищенных подсетей;
- количество переданных, принятых и отброшенных байт;
- количество переданных, принятых и отброшенных пакетов.

Примечание. Для просмотра полного списка защищенных подсетей используйте ссылку "Подробнее".

Для просмотра сведений о текущей версии приложения:

1. Вызовите дополнительное меню и выберите пункт "О программе".

На экране появятся название компании – разработчика приложения, номер версии сборки программного обеспечения "Континент- АП" , дата и время сборки, а также контрольные суммы используемых библиотек:



- После просмотра сведений нажмите кнопку "OK".

Вкладка "Профили"

Процедуры создания и импорта профиля см. на стр. [14](#) и стр. [11](#) соответственно в разделе "Настройка "Континент-АП" .

Список профилей

Все операции, связанные с профилями подключений, выполняются в главном окне приложения на вкладке "Профили".

Для перехода к списку профилей:

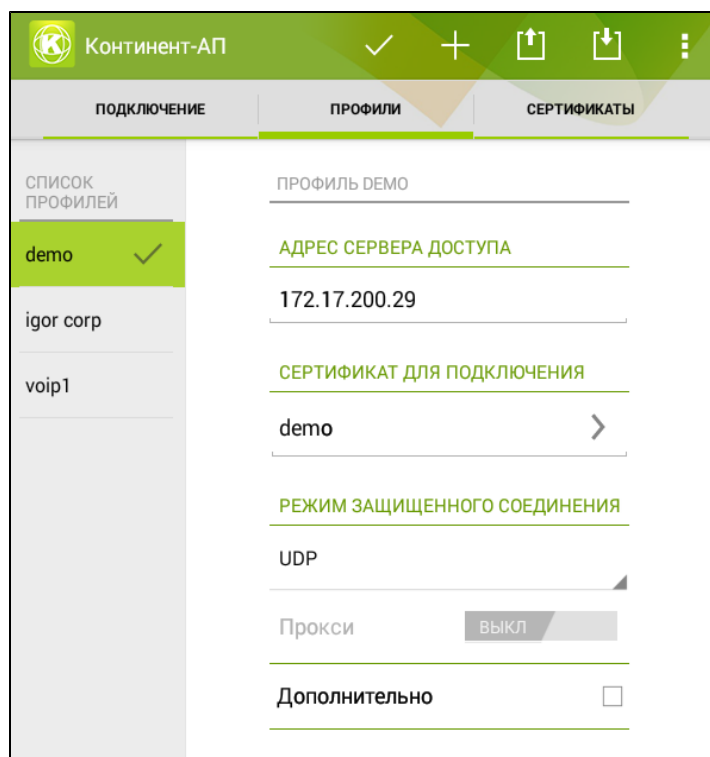
- В главном окне приложения перейдите на вкладку "Профили".
В левой части вкладки появится список созданных профилей подключений.

Примечание. Если профиль подключения не создавался, список будет пустым.

Активный профиль в списке отмечен галочкой, расположенной справа.

Справа от списка отображаются значения параметров профиля, выбранного в списке. При этом дополнительные параметры и параметры настройки прокси скрыты.

Примечание. На смартфонах на вкладке "Профили" отображается только список. Для просмотра параметров профиля необходимо выбрать его в списке.



- Для просмотра параметров настройки прокси-сервера включите "Прокси".
- Для просмотра дополнительных параметров установите отметку в поле "Дополнительно".

В верхней части главного окна расположены дополнительные кнопки, предназначенные для выполнения операций с профилями.

Кнопка	Назначение
	Перевод профиля в статус "активный"
	Создание нового профиля
	Экспорт выбранного в списке профиля. В смартфоне процедура экспорта запускается с помощью пункта дополнительного меню "Экспорт"
	Импорт профиля. В смартфоне процедура импорта запускается с помощью пункта дополнительного меню "Импорт"

Примечание. В зависимости от используемого мобильного устройства некоторые из приведенных выше кнопок могут отсутствовать. Вместо них используют кнопку , расположенную в нижней части экрана устройства.

Посредством команд вкладки "Профили" выполняются следующие операции:

- создание нового профиля и добавление его в список;
- переименование профиля, выбранного в списке;
- редактирование параметров профиля;
- экспорт выбранного в списке профиля;
- импорт профиля;
- удаление выбранного в списке профиля;
- назначение выбранному в списке профилю статуса "активный".

Переименование профиля

Для переименования профиля:

1. Выберите в списке профиль, нажмите кнопку вызова дополнительного меню  (если кнопка отсутствует, вместо нее используется кнопка устройства , расположенная ниже главного окна приложения) и выберите пункт "Переименовать".

На экране появится диалог редактирования имени профиля.

2. Введите новое имя профиля и нажмите кнопку "ОК".

Профиль в списке будет переименован.

Редактирование параметров профиля

Для редактирования профиля:

- Выберите в списке профиль и отредактируйте значения параметров (см. выше процедуру создания нового профиля).

Внимание. При установленном соединении с сервером доступа редактирование профиля запрещается.

Экспорт профиля

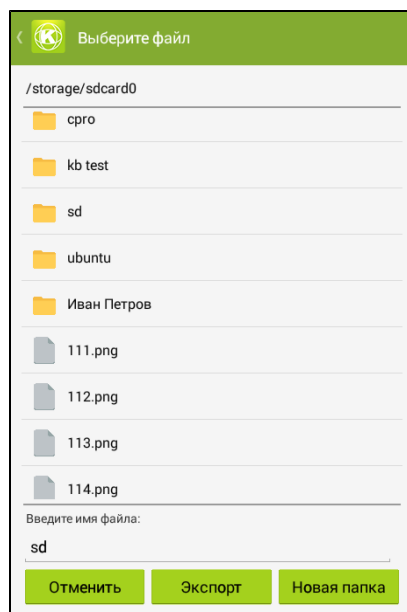
Процедура экспорта выполняется, когда требуется использовать профиль в абонентском пункте другого мобильного устройства.

Для экспорта профиля:

1. Выберите в списке профиль и нажмите кнопку , расположенную в верхней части экрана.

Пояснение. Если указанная кнопка отсутствует, с помощью кнопки , расположенной в нижней части экрана устройства, вызовите дополнительное меню и выберите пункт "Экспорт".

На экране появится диалог выбора папки для сохранения профиля:



По умолчанию предлагается сохранить профиль в папке, отображаемой в верхней части диалога. При этом файлу сохраняемого профиля присваивается имя профиля.

2. Чтобы сохранить профиль в другой папке, выберите ее или создайте новую с помощью кнопки "Новая папка".

Внимание. На смартфоне кнопка, показанная на рисунке выше, отсутствует. Вместо нее используйте кнопку "Новая папка" , расположенную в верхней части экрана.

3. Чтобы изменить имя сохраняемого файла, введите новое имя в нижней части диалога.
4. Нажмите кнопку "Экспорт" (см. рисунок выше) или кнопку , расположенную в верхней части экрана.
Профиль будет сохранен в указанной папке.
5. Скопируйте стандартными средствами файл профиля на внешний носитель.

Изменение статуса профиля

Для изменения статуса профиля:

- Выберите в списке профиль и нажмите кнопку , расположенную в верхней части экрана.
Профиль станет активным и будет выполнен переход на вкладку "Подключение".

Удаление профиля

Внимание. Нельзя удалить профиль со статусом "активный".

Для удаления профиля:

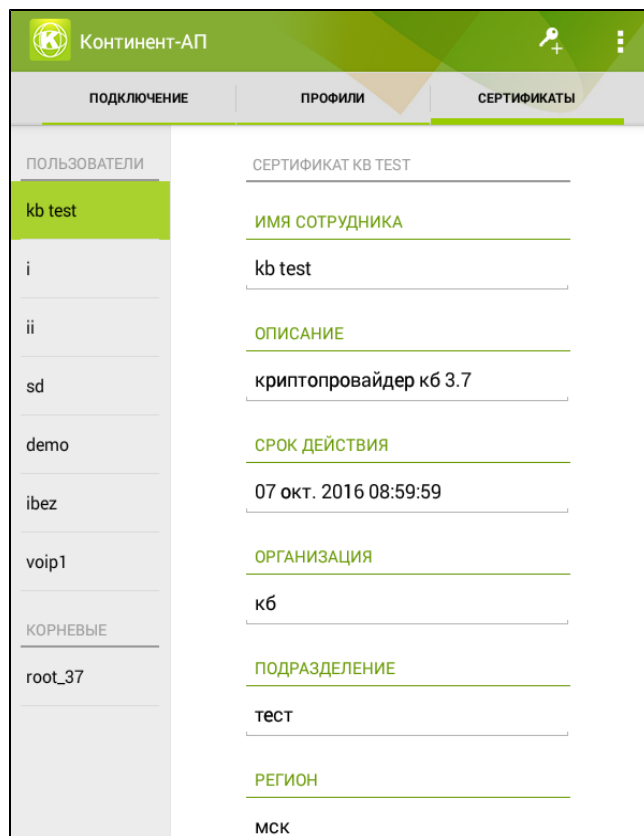
1. Выберите в списке профиль, нажмите кнопку вызова дополнительного меню  (если кнопка отсутствует, вместо нее используется кнопка устройства , расположенная ниже главного окна приложения) и выберите пункт "Удалить".
На экране появится запрос на подтверждение операции удаления.
2. Нажмите кнопку "ОК".
Профиль будет удален из списка.

Вкладка "Сертификаты"

Описание вкладки "Сертификаты"

Для работы с сертификатами:

- В главном окне приложения перейдите на вкладку "Сертификаты".



Внимание. Отображение вкладки зависит от модели используемого мобильного устройства:

- на планшетном компьютере в левой части вкладки отображаются списки установленных на устройстве сертификатов пользователя и корневых сертификатов. В центральной части вкладки отображаются основные поля выбранного в списке сертификата;
- на смартфоне на вкладке отображаются только списки сертификатов. Для просмотра содержимого полей сертификата выберите его в списке.

В верхней части вкладки расположены кнопки:

Кнопка	Описание
	Запускает процедуру формирования запроса на сертификат пользователя
	Вызывает дополнительное меню (описание пунктов меню см. в таблице на стр. 9). Если кнопка отсутствует, вместо нее используется кнопка устройства  , расположенная ниже главного окна приложения

Установка списка отозванных сертификатов

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

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

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

Глава 3

Служебные операции

Обновление

Обновление программного обеспечения абонентского пункта выполняется при переходе на новую версию. Для обновления используется арк-файл, подготовленный компанией-разработчиком.

Предусмотрены два варианта загрузки файла обновления:

- загрузка с карты памяти;
- скачивание файла с HTTP-ресурса компании-разработчика.

В процессе обновления выполняются проверки:

- обновляемой версии абонентского пункта;
- целостности и аутентичности файла обновления.

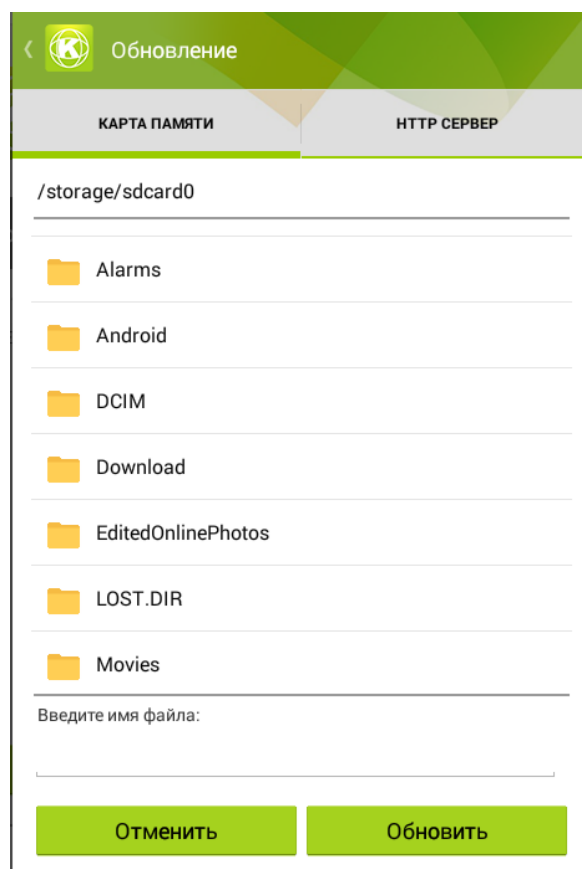
Внимание! Перед выполнением процедуры обновления проверьте уровень заряда аккумулятора мобильного устройства. Уровень заряда должен составлять не менее 50 % от максимального.

Для обновления программного обеспечения:

1. В главном окне приложения нажмите кнопку вызова дополнительного меню и выберите пункт "Обновление ПО".

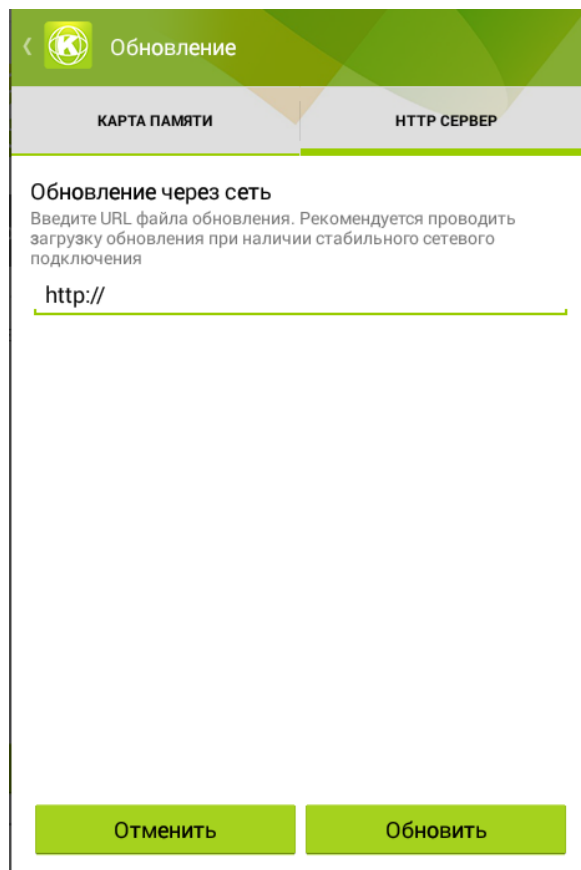
На экране появится окно "Обновление", содержащее две вкладки: "Карта памяти" и "HTTP-сервер".

2. Если обновление выполняется с карты памяти, на вкладке "Карта памяти" раскройте папку с хранящимся в ней файлом обновления, выберите файл и нажмите кнопку "Обновить".



На смартфоне нажмите кнопку , расположенную в верхней части экрана. Начнется процедура обновления приложения. Перейдите к п. 4.

3. Если обновление выполняется скачиванием файлов с HTTP-ресурса компании-разработчика, перейдите на вкладку "HTTP-сервер", введите полный URL файла обновления, включая имя файла, и нажмите кнопку "Обновить" (см. рисунок ниже) или на смартфоне кнопку , расположенную в верхней части экрана.



Начнется загрузка файла и после ее завершения начнется процесс установки обновления.

4. Дождитесь завершения обновления приложения "Континент-АП".
5. Проведите контроль целостности (см. стр. 27).

Контроль целостности

После установки приложения СКЗИ "Континент- АП" требуется провести контроль целостности приложений ОС устройства. Контроль целостности проводится с помощью специальной утилиты acsum.exe, поставляемой в комплекте с программным обеспечением.

Утилита работает в двух режимах:

- контроль целостности приложений;
- контроль целостности системы.

Утилита работает совместно со следующими файлами:

Name	Date modified	Type	Size
 acsum.exe	6/22/2018 2:44 PM	Application	25,936 KB
 abe.jar	6/22/2018 3:30 PM	Executable Jar File	7,923 KB
 sys.json	5/30/2018 5:28 PM	JSON File	2 KB
 app.json	6/5/2018 12:18 PM	JSON File	1 KB
 acsum.ini	7/2/2018 11:18 AM	Configuration sett...	1 KB
 checksum_sys_SM_J730FM_5200003af48184f5.json	7/2/2018 11:18 AM	JSON File	119 KB

1. Файл известных приложений app.json.

Файл формируется компанией "Код Безопасности" и не редактируется пользователем в процессе работы. Содержит список известных приложений.

Для каждого приложения хранятся следующие данные:

- pack_name — имя пакета приложения;
- app_name — название приложения;
- ver — версия приложения;
- sum — контрольная сумма приложения.

2. Файл контроля системы sys.json.

Файл содержит список рекурсивных путей, по которым контролируется система, с указанием типов файлов. Файл доступен для редактирования пользователем.

3. Файл с контрольными суммами системы checksum_sys_<name>_<ser_num>.json.

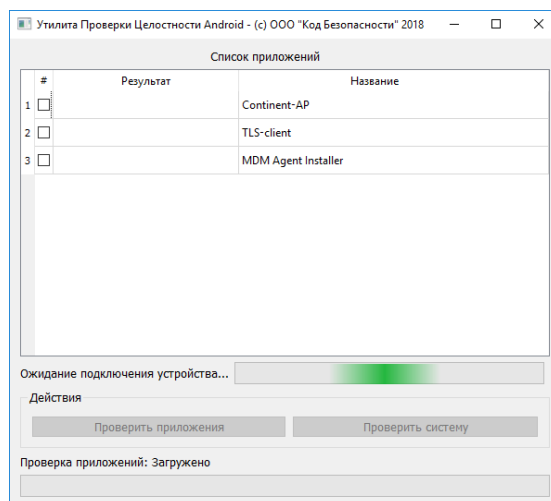
Для каждого подключаемого устройства в процессе работы программы создается отдельный файл. Имя файла checksum_sys_<name>_<ser_num> состоит из <name> — кодовое имя модели устройства, <ser_num> — серийный номер устройства.

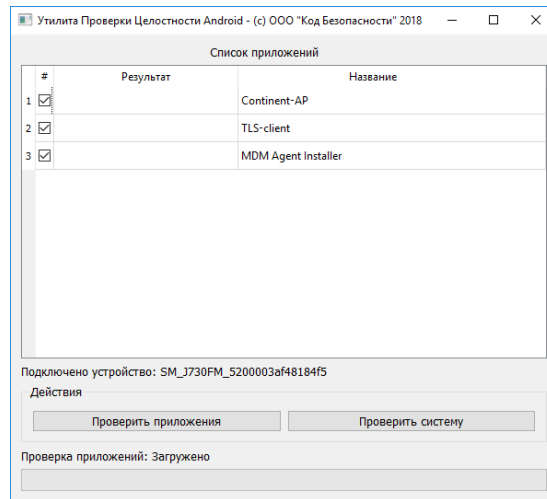
Файл содержит:

- список путей контролируемых файлов, полученных в результате считывания путей файла sys.json;
- рассчитанные контрольные суммы файлов.

Для выполнения операции контроля целостности:

Внимание! Перед началом работы активируйте на устройстве режим разработчика и установите на компьютер последнюю версию драйвера Google USB Driver.

1. Запустите acsum.exe.**2. Подключите устройство с помощью USB-переходника. Окно утилиты примет вид.**

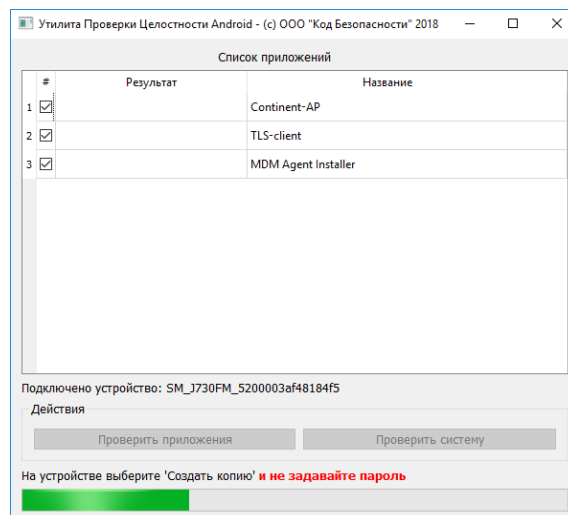


В основном окне отобразятся:

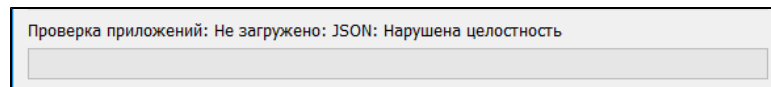
- список известных приложений из файла app.json с возможностью множественного выбора;
- кнопки "Проверить приложения" и "Проверить систему".

3. Нажмите кнопку "Проверить приложения".

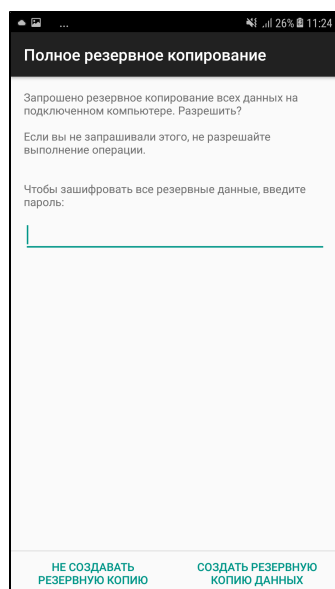
Примечание. Если кнопка заблокирована, отметьте список приложений, которые требуют проверки.



Утилита считывает информацию обо всех версиях выбранных приложений и проверяет целостность файла app.json. Если контрольная сумма не совпадает, система выдает сообщение "Не загружено: JSON: Нарушена целостность" и операция завершается.



Если контрольная сумма совпадает, на устройстве появляется сообщение.



4. Нажмите кнопку "Создать резервную копию данных". Не вводите пароль.
5. После завершения операции в главном окне утилиты будет представлен отчет в табличном виде. В отчете записана следующая информация:

- название приложения;
- результат контроля:
 - Успешно.

1	☒	Приложение: ОК	Continent-AP
---	-------------------------------------	----------------	--------------

- Контрольные суммы не совпадают.

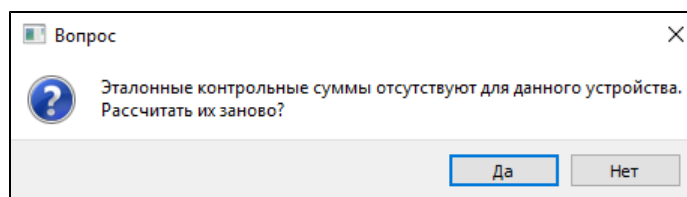
2	☒	Приложение: Ошибка CRC	TLS-client
---	-------------------------------------	------------------------	------------

- Приложение не установлено.

2	☒	Приложение: Не найдено	TLS-client
---	-------------------------------------	------------------------	------------

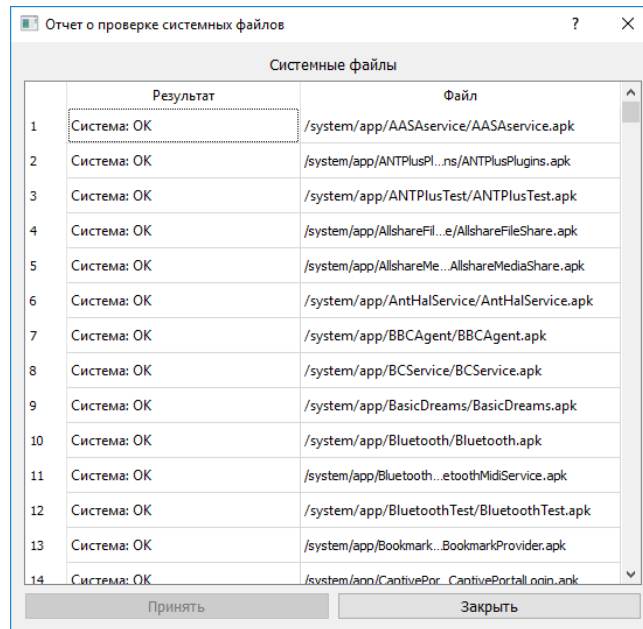
6. Нажмите кнопку "Проверить систему".

Начнется проверка целостности файла с контрольными суммами (далее — КС) системы для данного устройства. Если файла с КС системы нет или нарушена целостность файла, пользователю выдается диагностическое сообщение с запросом на перерасчет КС.



Диагностическое сообщение также выдается в случае, когда подсчитанные КС не совпадают с КС, записанными в файл checksum_sys_<name>_<ser_num>.json. Если пользователь нажимает кнопку "Нет", операция завершается. Если пользователь нажимает кнопку "Да", считаются КС каждого файла с учетом списка рекурсивных путей в файле контроля системы sys.json. Полученные данные сохраняются в файл с контрольными суммами системы для данного устройства.

7. Если КС совпали, на экране появится новое окно.



Если в процессе подсчета КС было выявлено несовпадение, кнопка "Принять" активируется. Нажмите кнопку "Принять", чтобы сохранить новые данные в файле checksum_sys_<name>_<ser_num>.json.

8. Нажмите кнопку "Заккрыть". Операция будет завершена.

Создание файла журнала

В файле журнала содержатся сведения о работе приложения "Континент-АП" за период работы мобильного устройства с момента его последнего включения.

Для создания файла журнала:

1. Нажмите кнопку вызова дополнительного меню  (если кнопка отсутствует, вместо нее используется кнопка устройства , расположенная ниже главного окна приложения) и выберите пункт "Журнал".
На экране появится диалог выбора папки.
2. Задайте параметры сохранения файла журнала.
 - Выберите папку, в которую должен быть сохранен файл журнала.
По умолчанию файл журнала сохраняется в папку, указанную в верхней части диалога. При необходимости создайте новую папку, используя кнопку "Новая папка".
 - Задайте имя файла журнала.
По умолчанию файл сохраняется с именем, содержащим дату и время сохранения.
3. Нажмите кнопку "Сохранить".
Файл журнала будет создан и сохранен в указанную папку.
При необходимости передайте файл журнала администратору безопасности.

Управление режимом работы

"Континент-АП" функционирует в двух режимах:

- режим пользователя — пользователю "Континент-АП" предоставляются права ограниченного доступа к управлению настройками приложения;
- режим администратора (устанавливается по умолчанию) — пользователю предоставляются права полного доступа.

Для включения режима пользователя:

1. Вызовите дополнительное меню приложения "Континент-АП".
2. В появившемся меню выберите пункт "Заблокировать".
На экране появится окно "Введите пароль".
3. Введите пароль блокировки в поля "Пароль", "Подтверждение пароля" и нажмите "Да"/"ОК".
В нижней части главного окна появится сообщение "Включен режим пользователя".
В дополнительном меню приложения вместо пункта "Заблокировать" появится пункт "Разблокировать".

Для включения режима администратора:

1. Вызовите дополнительное меню приложения "Континент-АП".
2. В появившемся меню выберите пункт "Разблокировать".
На экране появится окно "Введите пароль".
3. Введите пароль блокировки в поле "Пароль" и нажмите "Да"/"ОК".
В нижней части главного окна появится сообщение "Включен режим администратора".
В дополнительном меню приложения вместо пункта "Разблокировать" появится пункт "Заблокировать".

Приложение

Пример xml-файла для настройки параметров "Континент-АП"

Ниже представлен пример файла profile.xml. Обязательные поля выделены полужирным шрифтом.

```
<?xml version="1.0" encoding="UTF-8" standalone='yes'?>
```

```
<profile>
```

```
<!--Обязательное поле-->
```

```
<name>имя_профайла</name>
```

```
<!--Обязательное поле-->
```

```
<access_server_address>ip адрес_или_имя_СД</access_server_address>
```

```
<!--Обязательное поле-->
```

```
<connection_certificate>сертификат_подключения</connection_certificate>
```

```
<!--По умолчанию 0-->
```

```
<protected_connection_regime>режим_защищенного_соединения</protected_connection_regime>
```

```
<!--По умолчанию false-->
```

```
<proxy>true - прокси включен, false - прокси отсутствует</proxy>
```

```
<!--Если <proxy>true</proxy>, обязательны <proxy_server_address>, <proxy_port>-->
```

```
<!--Адрес прокси-сервера-->
```

```
<proxy_server_address>ip_адрес</proxy_server_address>
```

```
<!--По умолчанию 3128-->
```

```
<proxy_port>порт_прокси_сервера</proxy_port>
```

```
<!--По умолчанию 0-->
```

```
<proxy_authentication>режим_аутентификации (0 - нет, 1 - Basic, 2 - NTLM)</proxy_authentication>
```

```
<!--Если <proxy_authentication>1 или 2</proxy_authentication>, обязательны <proxy_user_name>, <proxy_password>, <proxy_password_mask>-->
```

```
<proxy_user_name>имя_пользователя</proxy_user_name>
```

```
<!--base64 от замаскированного пароля аутентификации на прокси-->
```

```
<proxy_password>пароль</proxy_password>
```

```
<!--base64 от маски для пароля аутентификации на прокси-->
```

```
<proxy_password_mask>маска_пароля</proxy_password_mask>
```

```

<!--По умолчанию 4433-->
<access_server_port>порт_СД</access_server_port>

<!--По умолчанию 7500-->
<client_port>порт_клиента</client_port>

<prefer_dns_server>DNS_главный (ip адрес)</prefer_dns_server>

<alternative_dns_server>DNS_альтернативный (ip адрес)</alternative_dns_
server>

<domain>домен</domain>

<!--По умолчанию 1500-->
<mtu>значение_MTU (от 0 до 1500)</mtu>

<!-- SHA1 от пароля разблокировки (администратора), преобразованный в
шестнадцатеричный вид-->
<admin_password>пароль</admin_password>

<!--По умолчанию false-->
<persistent>постоянное_соединение true - включить, false -
выключено</persistent>

<!-- - Если <persistent>true</persistent> или ключевой контейнер не
импортирован, обязательны <connection_password>, <connection_password_
mask>-->
<!--base64 от замаскированного пароля для установки соединения-->
<connection_password>пароль</connection_password>

<!--base64 от маски пароля для установки соединения-->
<connection_password_mask>маска_пароля</connection_password_
mask>

<!--Режим запрета незащищенных соединений (0 - нет запрета, 1 - запрет после
подключения, 2 - запрет до и после подключения)-->
<!--По умолчанию 0-->
<protection_mode>режим_запрета_незащищенных_соединений</protection_
mode>

</profile>

```