УТВЕРЖДЕН

BY.СЮИК.00441-01 34 01-ЛУ

КОМПЛЕКС ПРОГРАММНЫЙ КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ МОБИЛЬНЫХ УСТРОЙСТВ «БАС-А»

Руководство оператора

BY.СЮИК.00441-01 34 01

Листов 43

Подп. и дата	
Инв. № дубл.	
Взам. инв. №	
Подп. и дата	
Инв. № подл.	

2022

№ изм.	*Подп.*	*Дата*

Литера O_1

АННОТАЦИЯ

В настоящем документе описывается последовательность действий по установке, запуску и выполнению «Комплекса программного криптографической защиты информации мобильных устройств «БАС-А» (КП «БАС-А»).

Для понимания изложенного в документе материала необходимы навыки работы в операционной системе Android.

СОДЕРЖАНИЕ

1. НАЗНАЧЕНИЕ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

1.1. КП «БАС-А» предназначен для организации защищенного VPN-подключения устройства, работающего под управлением ОС Android, к «Комплексу программно-аппаратному криптографической защиты информации «БАС» СЮИК.465634.001 (далее – ПАК «БАС») или «Комплексу программному виртуальному криптографической защиты информации «БАС-V» BY.СЮИК.00436-01 (далее – КП «БАС-V»).

1.2. КП «БАС-А» обеспечивают криптографическую защиту передаваемых данных посредством полной инкапсуляции IP-пакетов путем их шифрования с использованием криптографических алгоритмов на основе протоколов IPsec.

1.3. Область применения КП «БАС-А» – системы обработки информации ограниченного распространения.

1.4. КП «БАС-А» реализует следующие функциональные возможности:

а) защиту информации путем ее шифрования с использованием криптографических алгоритмов на основе протоколов IPsec;

б) шифрование передаваемых данных в соответствие с СТБ 34.101.31-2020;

в) контроль целостности пакетов данных (вычисление имитовставки) в соответствие с СТБ 34.101.31, СТБ 34.101.47-2017;

г) согласование ключей шифрования и аутентификация в соответствии с СТБ 34.101.66-2014;

д) поддержка режимов аутентификации как с использованием сертификатов открытых ключей (протоком BSTS), так и с использованием предустановленного секрета (протокол BPACE);

е) генерацию ключей и синхропосылок в соответствии с СТБ 34.101.47;

ж) выработку открытых ключей в соответствии с СТБ 34.101.45-2013;

и) формирование запроса на получение сертификата открытого ключа в соответствии с СТБ 34.101.17-2012 и СТБ 34.101.78-2019;

к) обработку сертификатов открытых ключей и списков отозванных сертификатов в соответствии с СТБ 34.101.19-2012 и СТБ 34.101.78;

л) защиту секретных (личных) ключей от несанкционированного раскрытия, модификации и подмены, открытых – от модификации и подмены;

м) проверку работоспособности при включении и по запросу администратора;

н) тестирование следующих параметров;

– тесты криптографических алгоритмов;

– контроль целостности программного обеспечения;

о) возможность работы через NAT при помощи протокола NAT Traversal (NAT-T);

п) ведение журнала аудита;

р) автоматическую смену ключей шифрования при достижении заданного «времени жизни» ключа;

с) получение IP-адреса из пула сервера;

т) выбор и назначение приложений, трафик от которых должен (или не должен) проходить через VPN;

у) выбор и назначение подсетей, трафик для которых должен (или не должен) проходить через VPN;

ф) возможность блокировки трафика, не предназначенного для VPN.

1.5 КП «БАС-А» не ограничивает функциональные возможности устройства, на котором он установлен и работает.

2. УСЛОВИЯ ВЫПОЛНЕНИЯ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

В табл. 1 приведены минимальные системные требования для выполнения КП «БАС-А».

Таблица 1

ОС	Android версии 4.4 или более новой
Процессор	Intel Atom® Processor Z2520 1.2 ГГц или более быстрый
Устройства хранения данных	от 128 Мбайт
ОЗУ	минимум 512 Мбайт, 2 ГБ рекомендуются

3. ВЫПОЛНЕНИЕ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

3.1. Установка

Примечание. Перед установкой КП «БАС-А» необходимо убедиться в том, что на мобильном устройстве установлена защита от несанкционированного доступа. При ее отсутствии необходимо установить защиту. Необходимо использовать надежные механизмы защиты. Из стандартных методов защиты ОС Android (графический ключ, PIN-код, пароль) надежным является использование сложного пароля (большие и малые буквы, цифры и спецсимволы, увеличение длины пароля). В связи с этим для защиты мобильного устройства необходимо использовать пароль длиной не менее 4 символов, в котором используется хотя бы одна цифра, спецсимвол, а также буквы различных алфавитов или регистров.

Установка КП «БАС-А» осуществляется с помощью apk-файла.

Примечание. В операционных системах, которые являются оболочками Android, расположение меню и названия пунктов могут отличаться от приведенных ниже.

3.1.1. В первую очередь необходимо скопировать apk-файл «strongSwanCont.apk» с компакт-диска на мобильное устройство. Сделать это можно с помощью подключения мобильного устройства к компьютеру следующим образом:

– подключить мобильное устройство для передачи данных к компьютеру с помощью USB-кабеля;

– если при подключении к компьютеру мобильное устройство не предоставляет доступ к файловой системе, то необходимо на мобильном устройстве зайти в «Настройки», перейти в раздел «Для разработчиков» и установить флажок около пункта «Отладка по USB»;

– скопировать apk-файл «strongSwanCont.apk» с компакт-диска на мобильное устройство.

– после этого можно отключить «Отладку по USB» и отключить мобильное устройство от компьютера.

3.1.2. Чтобы иметь возможность устанавливать приложения из apk-файлов, нужно разрешить установку приложений из сторонних источников. Обычно эта опция находится в настройках безопасности устройства («Настройки» – «Безопасность»), либо в настройках приложений («Настройки» – «Приложения»), и обычно называется «Неизвестные источники». Необходимо активировать данный пункт в настройках. У разных производителей мобильных устройств данный пункт может быть запрятан по-разному.

3.1.3. Далее необходимо, собственно, установить КП «БАС-А». Сделать это можно разными способами, например:

– любым файловым менеджером. В файловом менеджере необходимо найти скопированный apk-файл, запустить, выбрать «установить приложение» и принять разрешения приложения;

– специальным приложением-установщиком. Данный тип приложений автоматически ищет apk-файлы на SD-карте и в памяти устройства, строит их список, и предлагает их установить. Далее так же, как и в файловом менеджере: выбрать нужный apk-файл, запустить, выбрать «установить приложение» и принять разрешения приложения;

– через браузер. Для этого необходимо открыть браузер и набрать в адресной строке следующую ссылку: content://com.android.htmlfileprovider/sdcard/«ПутьКФайлу».apk либо file:///sdcard/«ПутьКФайлу».apk (в зависимости от устройства);

3.2. Запуск

3.2.1. Чтобы запустить КП «БАС-А» необходимо нажать на значок приложения, изображенный на рис. 1.

Рис. 1

3.2.2. Приложение «strongSwanCont» поддерживает три языка интерфейса: английский, белорусский и русский. Язык интерфейса устанавливается автоматически в зависимости от выбранного языка системы. Языком по умолчанию является английский, он устанавливается если в качестве системного был выбран английский или любой другой, отличный от белорусского и русского.

3.2.3. Во время первого запуска приложение запросит два разрешения (рис. 2, 3).

Рис. 2

Рис. 3

Первое разрешение (рис. 2) необходимо для возможности чтения приложением файлов сертификатов открытых ключей и ключевых контейнеров, а также сохранения журналов в файлы в доступную пользователю область памяти.

Второе разрешение (рис. 3) необходимо для получения телефонных номеров доступных SIM-карт, при их наличии. Телефонные номера используются только как возможные варианты заполнения поля «Общее имя» во время ввода информации для выпуска запроса на получение сертификата.

3.3. Выполнение

3.3.1. Главное окно приложения

После запуска КП «БАС-А» отображается главное окно (рис. 4), в котором расположены следующие элементы:

1 – кнопка добавления профиля;

2 – кнопка вызова меню;

3 – панель статуса подключения;

4 – список настроенных профилей.

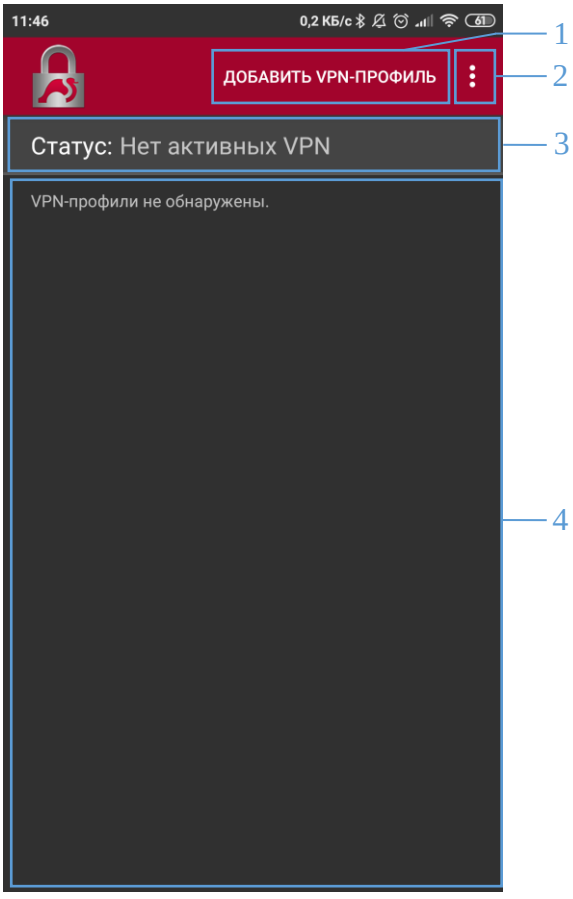


Рис. 4

3.3.2. Самотестирование

3.3.2.1. Самотестирование КП «БАС-А» включает в себя тестирование библиотеки криптографических преобразований и вычисление контрольной характеристики apk-файла приложения.

3.3.2.2. Самотестирование автоматически выполняется при запуске приложения «strongSwanCont» и при возвращении в активное состояние.

Если автоматическое самотестирование завершается успешно, то пользователь может начинать/продолжать работу в приложении. Посмотреть результаты самотестирования можно в журнале (подробнее см. п. 3.3.7).

3.3.2.3. Самотестирование также можно выполнить по запросу оператора. Для это необходимо в главном окне нажать кнопку вызова меню и выбрать пункт «Самотестирование» (рис. 5).

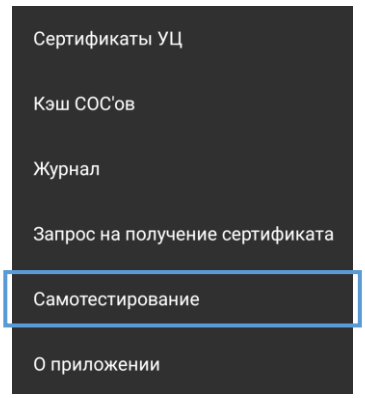


Рис. 5

После этого откроется окно «Самотестирование», в котором во время выполнения самотестирования работает индикатор загрузки.

Если самотестирование по запросу оператора завершается успешно, то в окне «Самотестирование» пропадает индикатор загрузки и отображается надпись: «Успешно» (рис. 6).

После небольшой паузы окно «Самотестирование» автоматически закрывается, и пользователь возвращается в главное окно. Посмотреть результаты самотестирования можно в журнале (подробнее см. п. 3.3.7).

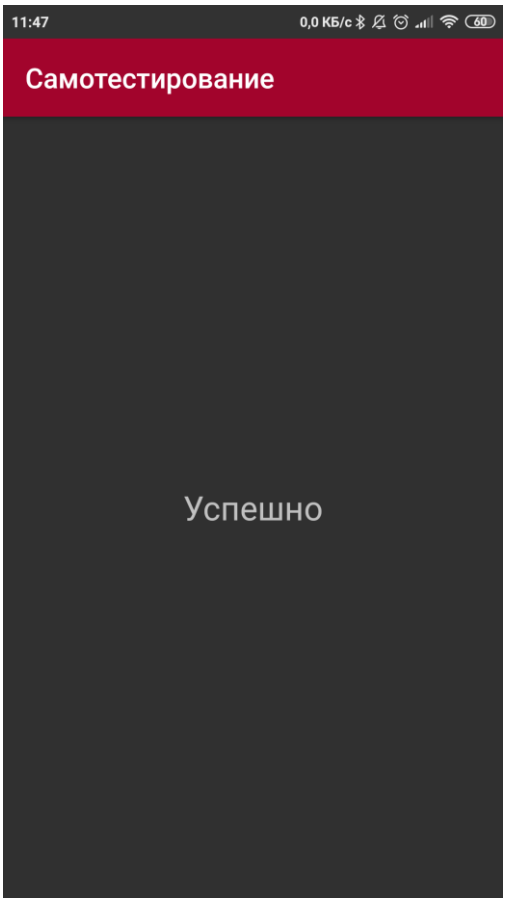


Рис. 6

3.3.2.4. Если самотестирование завершается ошибкой, приложение блокируется и на экране отображается сообщение, представленное на рис. 7. После того, как пользователь нажмет на кнопку «ОК» в окне сообщения приложение будет закрыто.

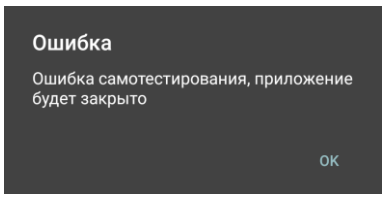


Рис. 7

3.3.2.5. Если пользователь пытается запустить приложение после блокировки, то на экране устройства отображается сообщение, представленное на рис. 8. После нажатия пользователем на кнопку «ОК» в окне сообщения приложение закроется.

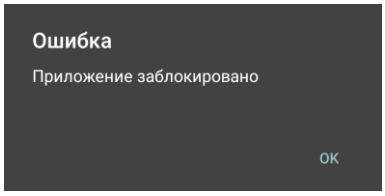


Рис. 8

Для снятия блокировки приложение необходимо переустановить.

3.3.3. Запрос на получение сертификата

3.3.3.1. В КП «БАС-А» есть возможность сгенерировать ключевую пару для аутентификации, сформировать контейнер защищенного личного ключа и запрос на получение сертификата. Для этого необходимо в главном окне нажать кнопку вызова меню и выбрать пункт «Запрос на получение сертификата» (рис. 9).

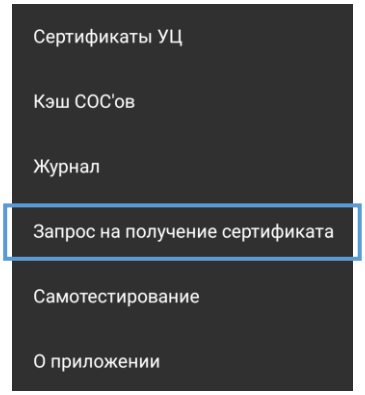


Рис. 9

Откроется окно, отображенное на рис. 10.

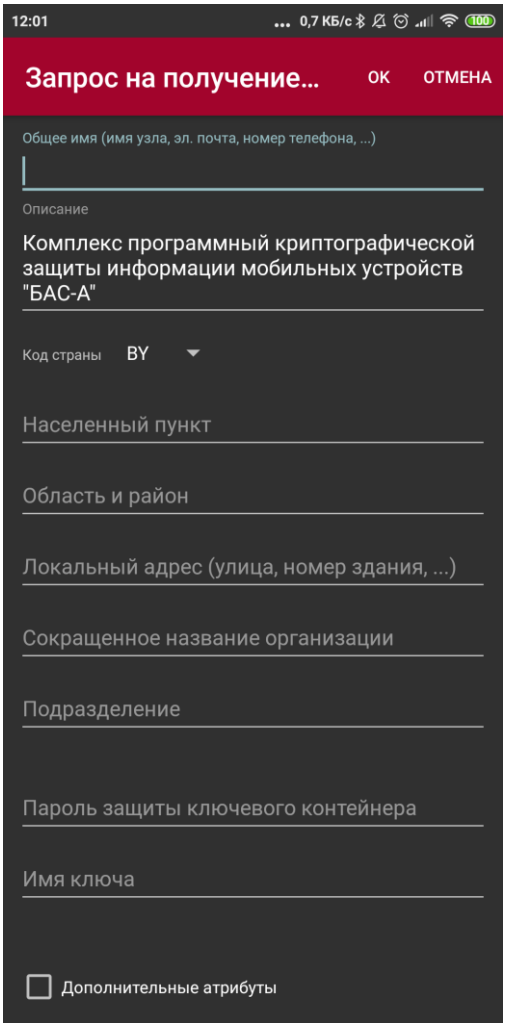


Рис. 10

Необходимо заполнить поля. Обязательными являются «Общее имя», «Населенный пункт», «Сокращенное название организации», «Пароль защиты ключевого контейнера» и «Имя ключа». Пример заполнения полей представлен на рис. 11.

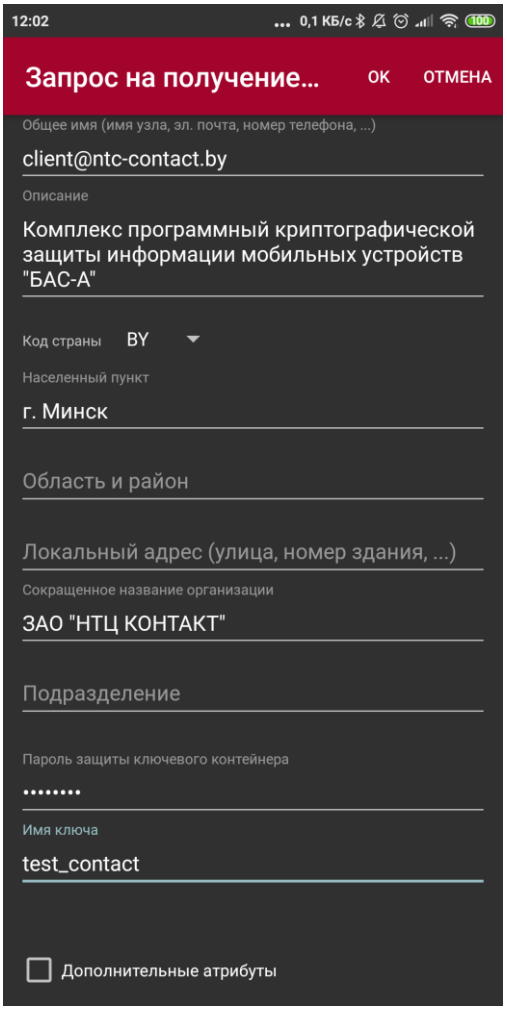


Рис. 11

Значение поля «Имя ключа» будет частью названия файлов ключевых контейнеров и запроса на получение сертификата, а в сам запрос эта информация не будет включена. Имя ключа должно быть уникальным.

3.3.3.2. В нижней части окна есть галочка «Дополнительные атрибуты». Если ее выбрать, отобразятся дополнительные поля (рис. 12).

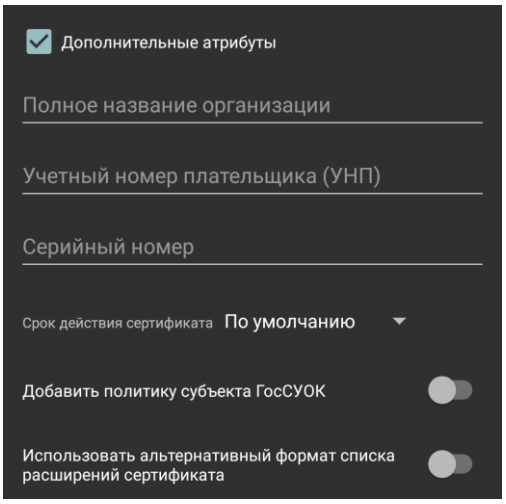


Рис. 12

Дополнительные атрибуты могут понадобиться для специфических требований Удостоверяющего центра, который будет выпускать сертификат. Так, например, для Удостоверяющего центра ГосСУОК необходимо установить переключатель «Добавить политику субъекта ГосСУОК».

3.3.3.3. Чтобы выйти из окна «Запрос на получение сертификата» без формирования ключевых контейнеров и запроса необходимо нажать на кнопку «Отмена» в верхнем правом углу окна.

3.3.3.4. Для продолжения формирования ключевых контейнеров и запроса после заполнения полей необходимо нажать на кнопку «ОК» в верхнем правом углу окна. Если какие-то из обязательных полей не будут заполнены или заполнены некорректно, то сообщения от этом отобразятся в виде подсказки под полем (например, рис. 13, 14).

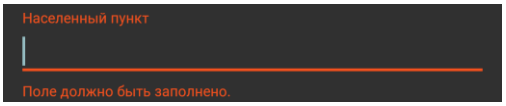


Рис. 13

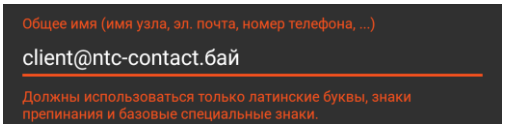


Рис. 14

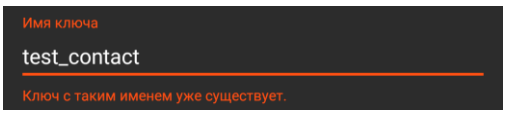


Рис. 15

3.3.3.5. Если поля корректно заполнены, после нажатия на кнопку «ОК» откроется окно «Генерация ключевой пары». В нем необходимо поводить пальцем по экрану для накопления случайности для инициализации криптографического генератора псевдослучайных чисел. По мере накопления случайности будет заполняться индикатор (рис. 16).

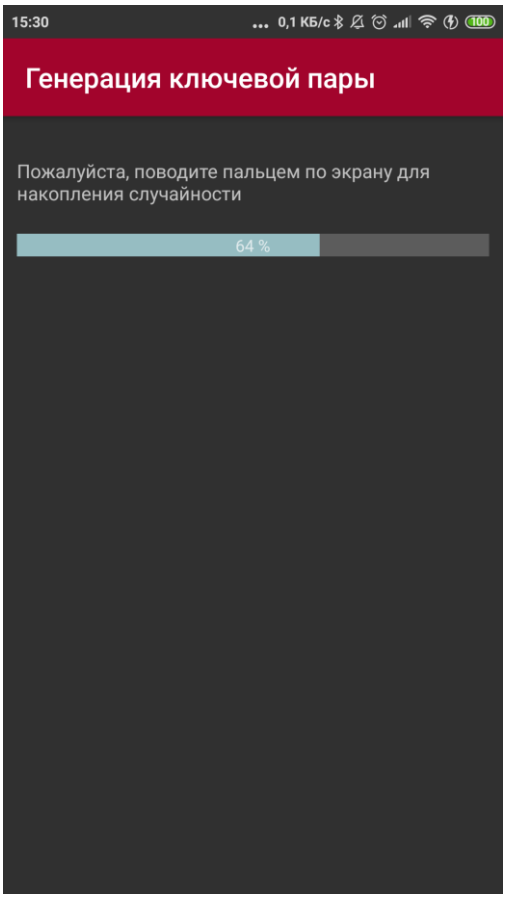


Рис. 16

3.3.3.6. В случае успеха сформируются четыре файла, описанные в табл. 2.

Таблица 2

Содержимое файла	Имя файла	Расположение файла
Запрос на выпуск сертификата	CertReq_*[имя_ключа]*.der	внешнее хранилище, директория «strongSwanCont»
Защищенный контейнер с личным ключом	PrivKey_*[имя_ключа]*.pkc	внутреннее хранилище приложения
Защищенный контейнер с первым частичным секретом	ShareKey1_*[имя_ключа]*.ssc	внутреннее хранилище приложения
Защищенный контейнер со вторым частичным секретом	KeyContainer_*[имя_ключа]*.ssc	внешнее хранилище, директория «strongSwanCont»

[имя_ключа] – это введенное пользователем значение поля «Имя ключа» в окне «Запрос на получение сертификата».

Для защиты личного ключа используется высокоэнтропийный ключ, сгенерированный с помощью криптографического генератора псевдослучайных чисел. Далее этот ключ делится на два частичных секрета с помощью алгоритма разделения секрета, а они в свою очередь защищаются на пароле, введенном пользователем в окне «Запрос на получение сертификата» в поле «Пароль защиты ключевого контейнера». Защищенный контейнер с личным ключом и защищенный контейнер с первым частичным секретом сохраняются во внутреннее хранилище приложения, доступ к которому пользователю и другим приложениям закрыт.

Если ключевые контейнеры и запрос на получение сертификата успешно сформированы, то отобразится сообщение с путями к файлу защищенного контейнера со вторым частичным секретом и к файлу запроса, а также с предложением отправить запрос в УЦ (рис. 17).

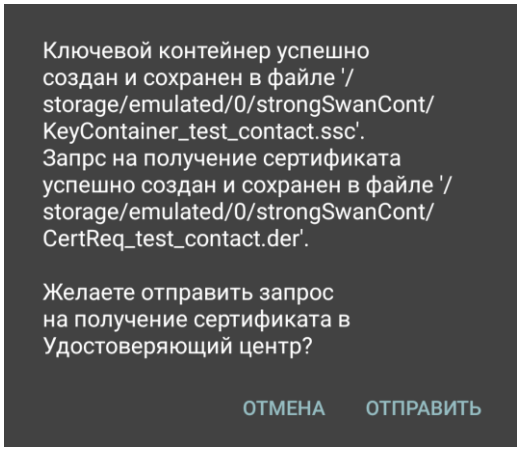


Рис. 17

Если нажать кнопку «Отправить», откроется окно с выбором доступного приложения для отправки файла запроса (например, как на рис. 18).

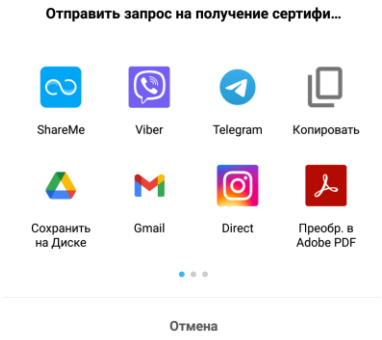


Рис. 18

3.3.3.7. Если во время формирования ключевых контейнеров или запроса на получение сертификата произошла ошибка, то на экране отобразится всплывающее сообщение, а подробности можно посмотреть в файле журнала (подробнее см. п. 3.3.7).

3.3.4. Сертификаты УЦ

В КП «БАС-А» есть возможность просматривать список доверенных сертификатов УЦ, установленных на устройстве Android. Для этого необходимо в главном окне нажать кнопку вызова меню и выбрать пункт «Сертификаты УЦ» (рис. 19).

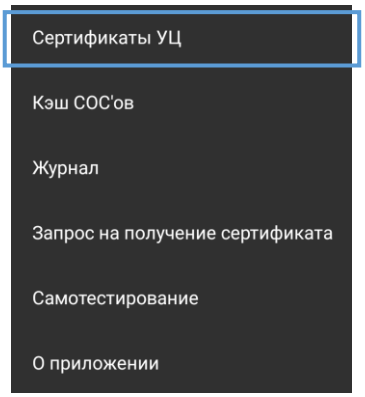


Рис. 19

После этого откроется окно «Сертификаты УЦ», в котором расположены три вкладки: «Система», «Пользователь» и «Импорт» (рис. 20).

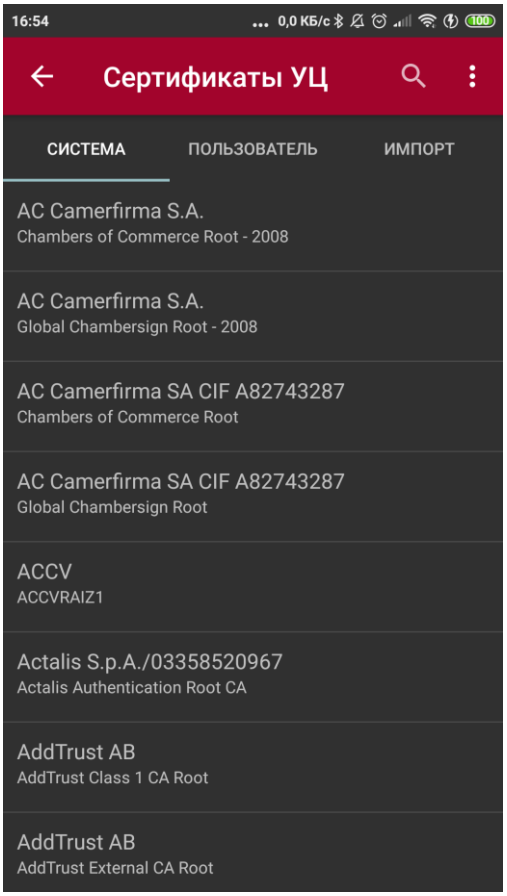


Рис. 20

Вкладка «Система» содержит список системных доверенных сертификатов УЦ.

Вкладка «Пользователь» содержит список сертификатов УЦ, которые пользователь устройства добавил в качестве доверенных через меню системных настроек.

Вкладка «Импорт» содержит список сертификатов УЦ, которые оператор КП «БАС-А» импортировал с помощью функции импорта сертификатов УЦ (п. 3.3.4.1).

3.3.4.1. Импорт сертификата УЦ

Для импорта сертификата УЦ необходимо в окне «Сертификаты УЦ» нажать кнопку вызова меню и выбрать пункт «Импортировать сертификат» (рис. 21).

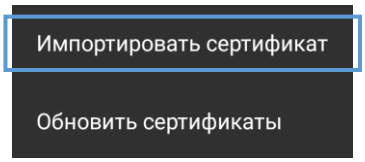


Рис. 21

После этого откроется системное окно выбора файла, в котором необходимо выбрать файл сертификата УЦ.

После выбора файла сертификата в случае успешного разбора сертификата отобразится окно с подтверждением импорта (рис. 22). В сообщении указывается описание субъекта (владельца) сертификата УЦ. После нажатия на кнопку «Импортировать сертификат» поверх окна «Сертификаты УЦ» появится всплывающее уведомление с текстом: «Сертификат успешно импортирован», а в список сертификатов УЦ на вкладке «Импорт» добавится импортированный сертификат (рис. 23).

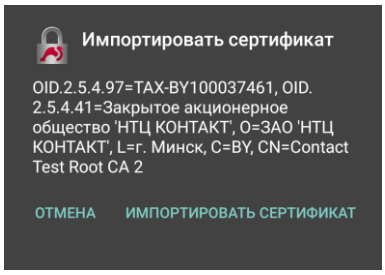


Рис. 22

Рис. 23

Если выбранный файл не удалось разобрать как сертификат, то поверх окна «Сертификаты УЦ» появится всплывающее уведомление с текстом: «Ошибка импорта сертификата».

3.3.4.2. Обновление сертификатов УЦ

Если после построения списков сертификатов УЦ на вкладках «Система» и «Пользователь» были добавлены системные или пользовательские сертификаты УЦ, то для их отображения на вкладках необходимо обновить списки. Для этого в окне «Сертификаты УЦ» следует нажать кнопку вызова меню и выбрать пункт «Обновить сертификаты» (рис. 24).

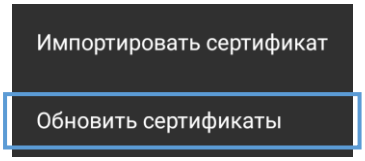


Рис. 24

Список сертификатов УЦ на вкладке «Импорт» обновлять не требуется, т.к. он обновляется автоматически после каждого импорта сертификата.

3.3.4.3. Удаление сертификатов УЦ

В КП «БАС-А» удалять сертификаты УЦ можно только из вкладки «Импорт». Для удаления сертификата необходимо в списке нажатием выбрать необходимый сертификат и в появившемся окне подтверждения (рис. 25) нажать на кнопку «Удалить».

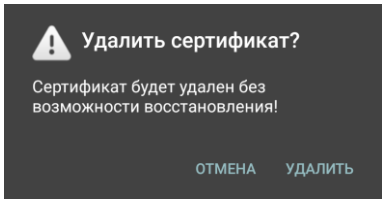


Рис. 25

3.3.5. Работа с VPN-профилями

VPN-профиль – набор параметров и характеристик VPN-подключения, включающий адрес сервера, тип аутентификации, параметры аутентификации, используемые криптографические алгоритмы и др.

КП «БАС-А» выполняет защищенное VPN-подключение к ПАК «БАС» или КП «БАС-V». Поэтому при настройке КП «БАС-А» необходимо учитывать сервера, к которому выполняется VPN-подключение.

3.3.5.1. Создание VPN-профиля

Для создания VPN-профиля необходимо в главном окне нажать кнопку «Добавить VPN-профиль» (рис. 26).

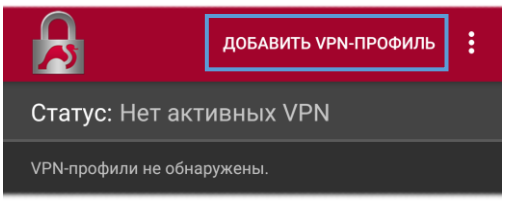


Рис. 26

Все параметры профиля условно делятся на основные и расширенные.

Набор основных характеристик профиля изменяется в зависимости от выбранного типа VPN. Доступно два типа (выпадающий список «Тип VPN»):

– «IKEv2 EAP-BPACE (Логин/Пароль)» – аутентификация EAP протоколом BPACE в соответствии с СТБ 34.101.66, п. 7.6;

– «IKEv2 EAP-BSTS (Сертификат)» – аутентификация EAP протоколом BSTS в соответствии с СТБ 34.101.66, п. 7.5.

3.3.5.1.1. Параметры профиля с аутентификацией протоколом BPACE

Окно добавления профиля с аутентификацией протоколом BPACE представлено на рис. 27.

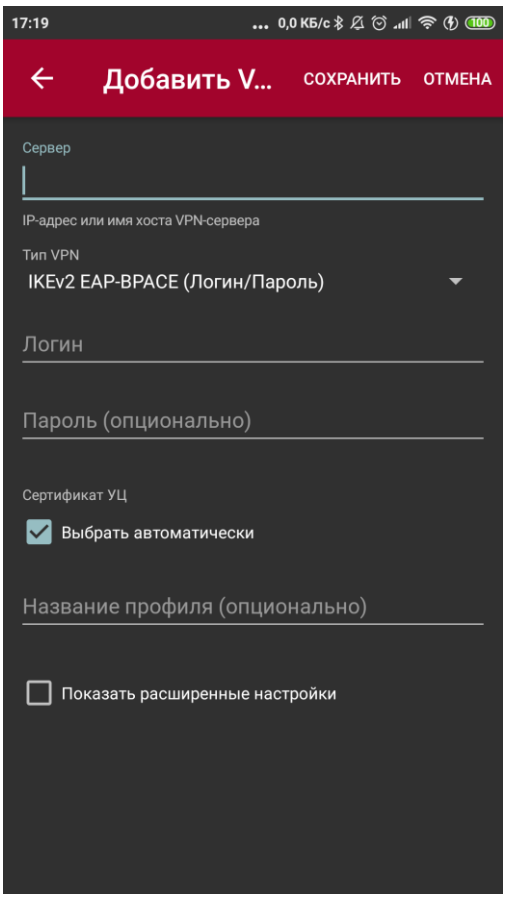


Рис. 27

При выборе типа VPN «IKEv2 EAP-BPACE (Логин/Пароль)» доступны следующие основные поля для настройки:

– поле «Сервер», обязательное для заполнения. Должно содержать IP-адрес и имя хоста VPN-сервера;

– поле «Логин», обязательное для заполнения. Должно содержать имя (логин) пользователя;

– поле «Пароль», необязательное для заполнения. Может содержать пароль для подключения к серверу. Если поле оставить пустым, то программа запросит пароль непосредственно во время подключения;

– область «Сертификат УЦ». Позволяет указать сертификат УЦ, которым должен быть выпущен сертификат сервера. По умолчанию область содержит отмеченную галочку «Выбрать автоматически». Это означает, что во время подключения программа переберет все доступные доверенные сертификаты УЦ на устройстве (см. п. 3.3.4). Если галочку «Выбрать автоматически» снять, появится возможность выбора конкретного сертификата УЦ (рис. 28).

Выбор конкретного сертификата УЦ сократит время перебора сертификатов УЦ до одного, что ускорит аутентификацию и установку защищенного соединения.

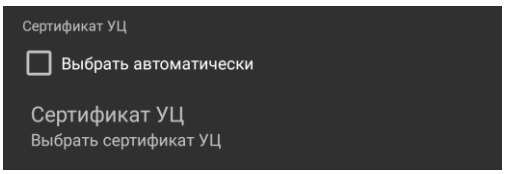


Рис. 28

Если нажать на «Выбрать сертификат УЦ», то откроется окно «Сертификаты УЦ» (рис. 20), в котором на любой из вкладок можно выбрать сертификат УЦ. Если пользователь выберет сертификат, то в области «Сертификат УЦ» отобразятся два поля из выбранного сертификата: «Название организации» и «Общее имя» (например, рис. 29);

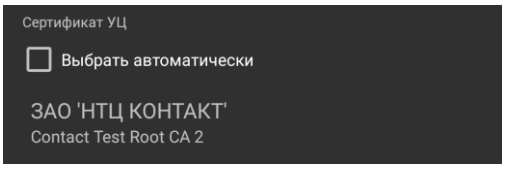


Рис. 29

– поле «Название профиля», необязательное для заполнения. Название будет отображаться в главном окне в списке профилей. Если название не будет задано, по умолчанию названием профиля будет установлено значение, указанное в поле «Сервер».

Пример заполнения основных полей профиля с аутентификацией протоколом BPACE представлен на рис. 30.

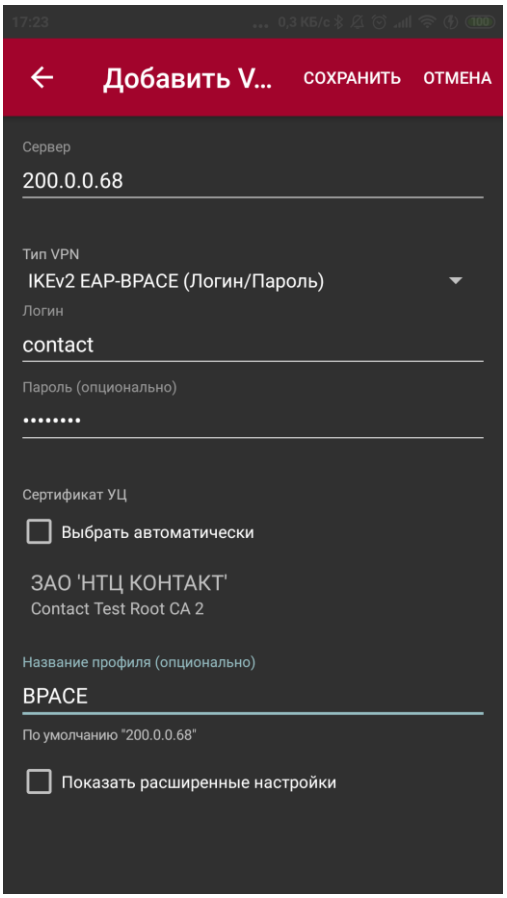


Рис. 30

3.3.5.1.2. Параметры профиля с аутентификацией протоколом BSTS

Окно добавления профиля с аутентификацией протоколом BSTS представлено на рис. 31.

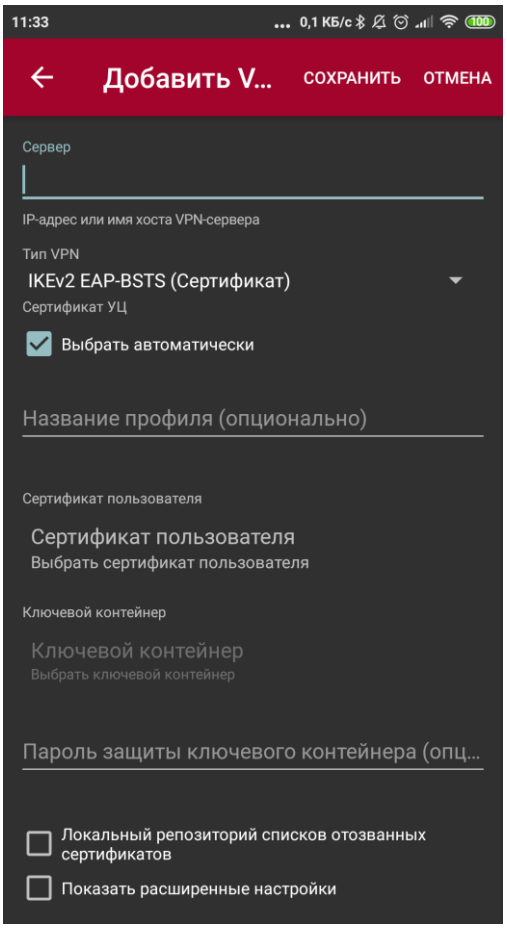


Рис. 31

При выборе типа VPN «IKEv2 EAP-BSTS (Сертификат)» доступны следующие основные поля для настройки:

– поле «Сервер», обязательное для заполнения. Должно содержать IP-адрес и имя хоста VPN-сервера;

– область «Сертификат УЦ». Позволяет указать сертификат УЦ, которым должен быть выпущен сертификат сервера. По умолчанию область содержит отмеченную галочку «Выбрать автоматически». Это означает, что во время подключения программа переберет все доступные доверенные сертификаты УЦ на устройстве (см. п. 3.3.4). Если галочку «Выбрать автоматически» снять, появится возможность выбора конкретного сертификата УЦ (рис. 28).

Выбор конкретного сертификата УЦ сократит время перебора сертификатов УЦ до одного, что ускорит аутентификацию и установку защищенного соединения.

Если нажать на «Выбрать сертификат УЦ», то откроется окно «Сертификаты УЦ» (рис. 20), в котором на любой из вкладок можно выбрать сертификат УЦ. Если пользователь выберет сертификат, то в области «Сертификат УЦ» отобразятся два поля из выбранного сертификата: «Название организации» и «Общее имя»;

– поле «Название профиля», необязательное для заполнения. Название будет отображаться в главном окне в списке профилей. Если название не будет задано, по умолчанию названием профиля будет установлено значение, указанное в поле «Сервер»;

– область «Сертификат пользователя». В области необходимо нажать на «Выбрать сертификат пользователя» и в открывшемся окне выбрать файл сертификата пользователя. Если пользователь выберет сертификат, то в случае корректности сертификата в области «Сертификат пользователя» отобразятся два поля из выбранного сертификата: «Общее имя» и «Название организации» (рис. 32). Если во врем разбора сертификата произошла ошибка, то отобразится всплывающее сообщение «Невозможно открыть файл сертификата»;

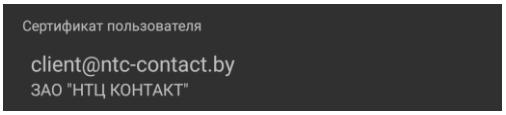


Рис. 32

– область «Ключевой контейнер». В области необходимо нажать на «Выбрать ключевой контейнер» и в открывшемся окне выбрать файл защищенного контейнера второго частичного секрета. Имя файла должно соответствовать шаблону «KeyContainer*_[имя_ключа]*.ssc», где *[имя_ключа]* – это введенное пользователем значение поля «Имя ключа» в окне «Запрос на получение сертификата» при формировании запроса. После выбора в области «Ключевой контейнер» отобразится путь к выбранному файлу (рис. 33);

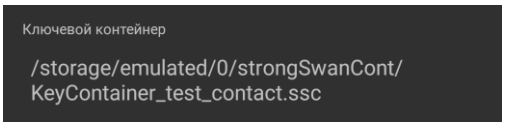


Рис. 33

– поле «Пароль защиты ключевого контейнера», необязательное для заполнения. Может содержать пароль для снятия защиты с контейнера. Если поле оставить пустым, то программа запросит пароль непосредственно во время подключения;

– параметр «Локальный репозиторий списков отозванных сертификатов». По умолчанию репозиторий не задан. Для того, чтобы установить репозиторий необходимо установить галочку «Локальный репозиторий списков отозванных сертификатов» и в появившейся ниже области нажать на «Выбрать репозиторий списков отозванных сертификатов». После этого откроется окно выбора файла, в котором необходимо выбрать файл списка отозванных сертификатов. Директория, из которой был выбран файл, и станет локальным репозиторием. Путь к этой директории отобразится в области под параметром «Локальный репозиторий списков отозванных сертификатов» (рис. 34).

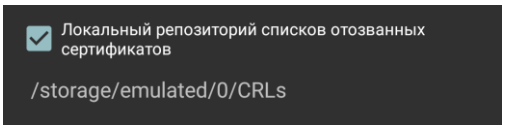


Рис. 34

Подробнее о работе с СОС’ами см. п. 3.3.6.1.

Пример заполнения основных полей профиля с аутентификацией протоколом BSTS представлен на рис. 35.

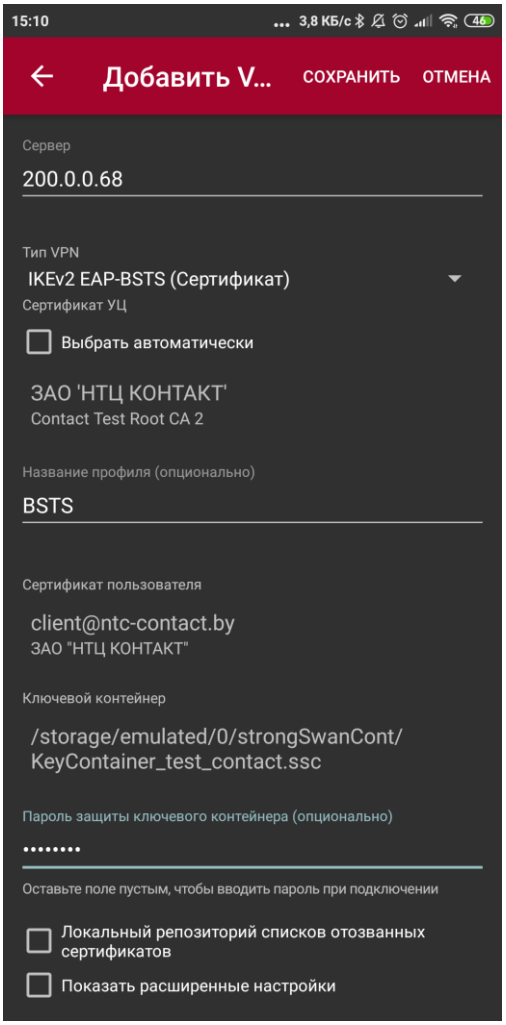


Рис. 35

3.3.5.1.3. Расширенные параметры профиля

Для установки расширенных параметров необходимо установить галочку «Показать расширенные настройки» (рис. 36).

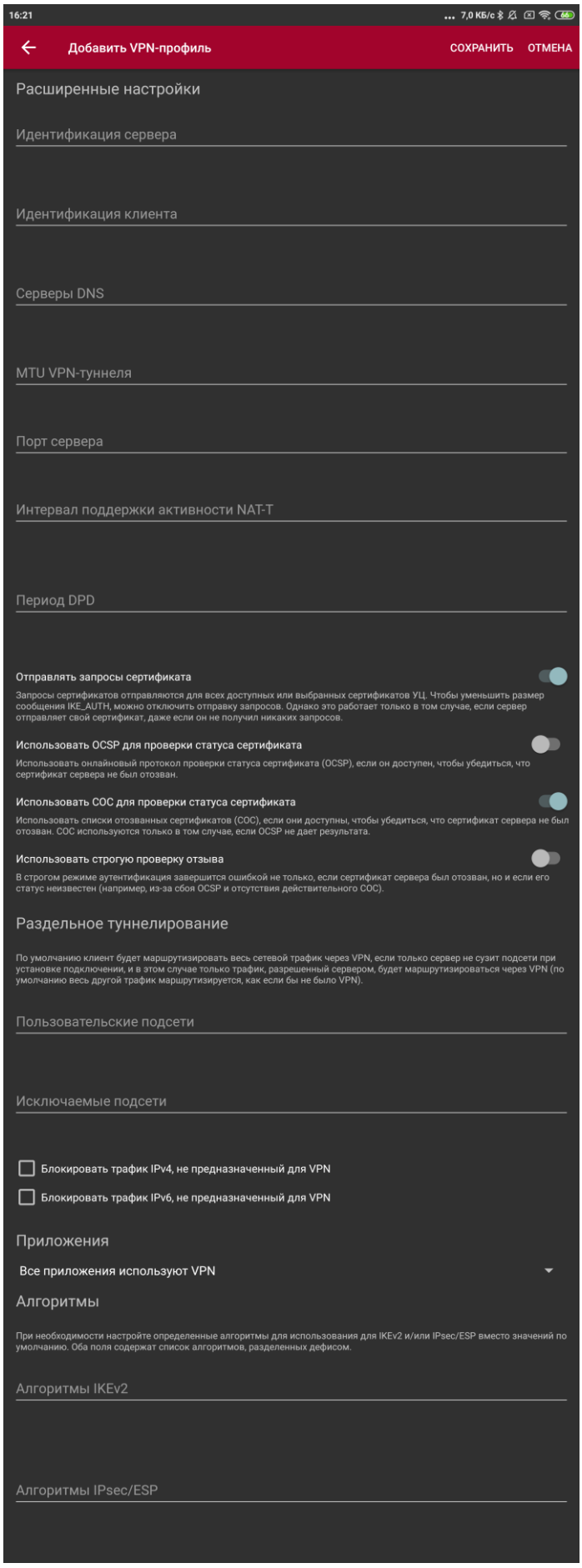

16:21
7,0 КБ/с
Добавить VPN-профиль
СОХРАНИТЬ
ОТМЕНА
Расширенные настройки
Идентификация сервера
Идентификация клиента
Серверы DNS
MTU VPN-туннеля
Порт сервера
Интервал поддержки активности NAT-T
Период DPD
Отправлять запросы сертификата
Запросы сертификатов отправляются для всех доступных или выбранных сертификатов УЦ. Чтобы уменьшить размер сообщения IKE_AUTH, можно отключить отправку запросов. Однако это работает только в том случае, если сервер отправляет свой сертификат, даже если он не получил никаких запросов.
Использовать OCSP для проверки статуса сертификата
Использовать онлайновый протокол проверки статуса сертификата (OCSP), если он доступен, чтобы убедиться, что сертификат сервера не был отозван.
Использовать COC для проверки статуса сертификата
Использовать списки отозванных сертификатов (COC), если они доступны, чтобы убедиться, что сертификат сервера не был отозван. COC используются только в том случае, если OCSP не дает результата.
Использовать строгую проверку отзыва
В строгом режиме аутентификация завершится ошибкой не только, если сертификат сервера был отозван, но и если его статус неизвестен (например, из-за сбоя OCSP и отсутствия действительного COC).
Раздельное туннелирование
По умолчанию клиент будет маршрутизировать весь сетевой трафик через VPN, если только сервер не сузит подсети при установке подключении, и в этом случае только трафик, разрешенный сервером, будет маршрутизироваться через VPN (по умолчанию весь другой трафик маршрутизируется, как если бы не было VPN).
Пользовательские подсети
Исключаемые подсети
Блокировать трафик IPv4, не предназначенный для VPN
Блокировать трафик IPv6, не предназначенный для VPN
Приложения
Все приложения используют VPN
Алгоритмы
При необходимости настройте определенные алгоритмы для использования для IKEv2 и/или IPsec/ESP вместо значений по умолчанию. Оба поля содержат список алгоритмов, разделенных дефисом.
Алгоритмы IKEv2
Алгоритмы IPsec/ESP

Рис. 36

Большинство расширенных параметров содержат подробное описание. Оно отображается при нажатии на поле параметра (например, рис. 37).

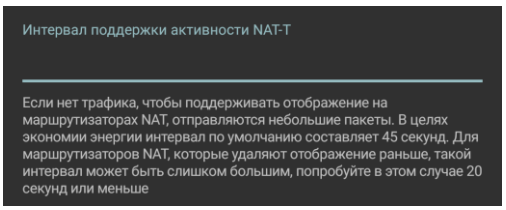


Рис. 37

3.3.5.1.3.1. В расширенных настройках можно указать раздельное туннелирование (секция «Раздельное туннелирование»). По умолчанию весь сетевой трафик будет маршрутизироваться через VPN. Можно указать конкретные подсети, которые будут маршрутизироваться через VPN, а остальной трафик нет. Либо, наоборот, указать те подсети, которые не нужно маршрутизировать через VPN, а весь остальной трафик пройдет через VPN.

3.3.5.1.3.2. Также можно заблокировать трафик, не предназначенный для VPN, установив соответствующие галочки для трафика IPv4 и IPv6. Это позволит повысить безопасность устройства.

3.3.5.1.3.3. Также можно указать приложения, которые будут (или не будут) использовать VPN (секция «Приложения»). Есть три варианта настройки:

– все приложения используют VPN;

– исключить выбранные приложения из VPN;

– только выбранные приложения используют VPN.

3.3.5.1.3.4. В секции «Алгоритмы» можно указать алгоритмы шифрования, контроля целостности, выработки псевдослучайных чисел, Диффи-Хеллмана, преобразования ключа для IKEv2 и IPsec/ESP. Полный перечень допустимых значений для каждой группы алгоритмов приведен в Приложении А.

3.3.5.1.4. Для сохранения параметров профиля необходимо в верхнем правом углу окна нажать кнопку «Сохранить».

В случае корректности заполненных полей окно «Добавить VPN-профиль» закроется, а в главном окне в списке профилей появится запись сохраненного профиля (рис. 38).

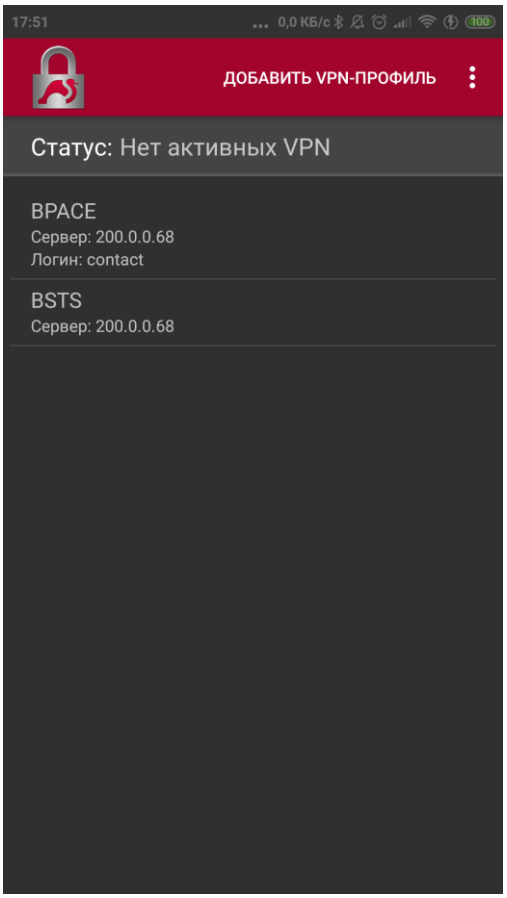


Рис. 38

3.3.5.1.5. Если до сохранения не были заполнены обязательные поля, возле этих полей отобразятся подсказки (рис. 39).

Рис. 39

Для того, чтобы выйти из окна «Добавить VPN-профиль» без сохранения профиля необходимо в верхнем правом углу окна нажать кнопку «Отмена».

3.3.5.2. Редактирование VPN-профиля

Для редактирования профиля необходимо в главном окне в списке сохраненных профилей нажать и удерживать палец на записи с профилем, который нужно отредактировать. Появится дополнительное меню (рис. 40), в котором нужно выбрать «Редактировать». После этого откроется окно, в заголовке которого будет указано название профиля. Содержимое окна аналогично содержимому окна «Добавить VPN-профиль».

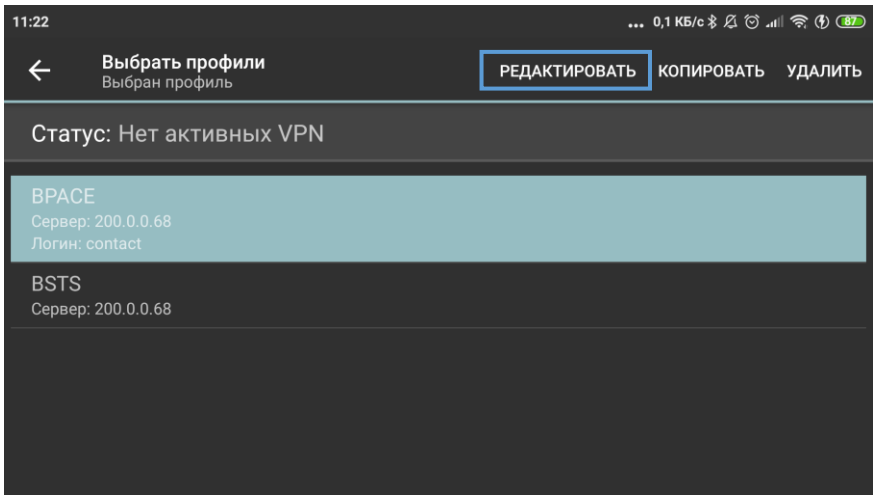


Рис. 40

3.3.5.3. Копирование VPN-профиля

Для копирования профиля необходимо в главном окне в списке сохраненных профилей нажать и удерживать палец на записи с профилем, который нужно скопировать. Появится дополнительное меню (рис. 41), в котором нужно выбрать «Копировать». После этого создастся копия выбранного профиля в списке сохраненных профилей с названием «*имя_копируемого_профиля* (копия)» (рис. 42) и откроется окно, аналогичное окну редактирования профиля.

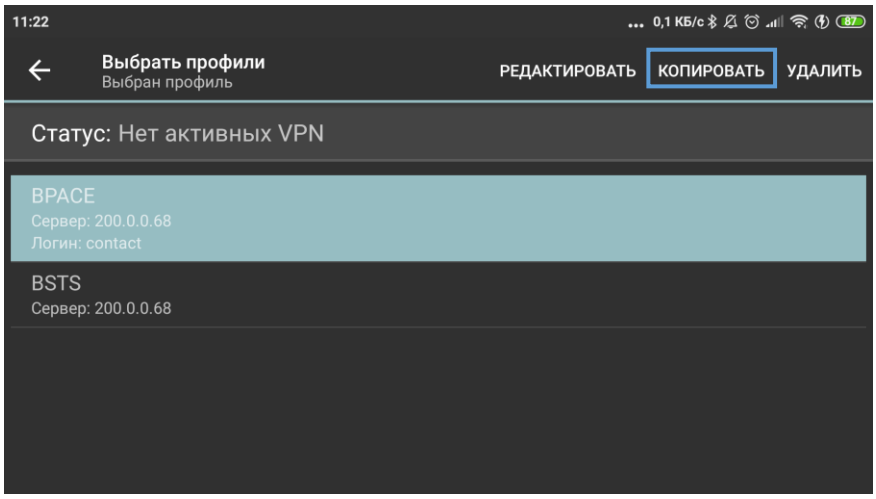


Рис. 41

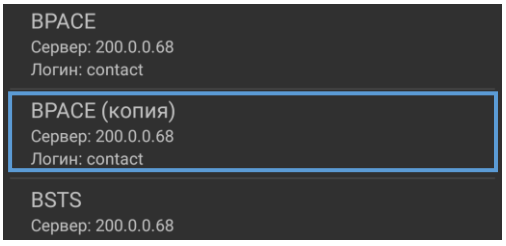


Рис. 42

3.3.5.4. Удаление VPN-профиля

Для удаления профиля необходимо в главном окне в списке сохраненных профилей нажать и удерживать палец на записи с профилем, который нужно удалить. Появится дополнительное меню, в котором нужно выбрать «Удалить». Поддерживается удаление нескольких профилей. Для этого после выделения одного профиля необходимо последовательно выбрать профили, которые необходимо удалить, а затем нажать кнопку «Удалить» (рис. 43).

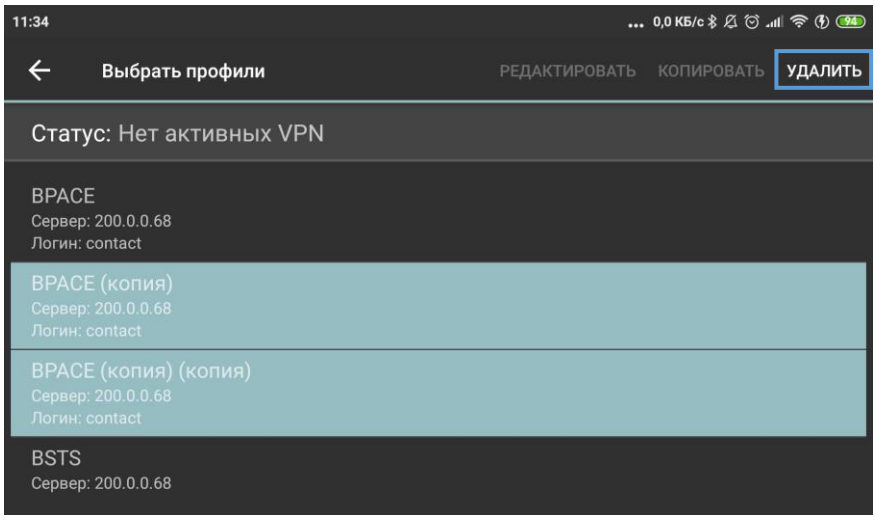


Рис. 43

3.3.5.5. Установка подключения к VPN-серверу

Для того чтобы установить подключение к VPN-серверу необходимо в главном окне в списке сохраненных профилей нажать на запись с нужным профилем.

3.3.5.5.1. При первом подключении КП «БАС-А» запросит разрешение на подключение к сети VPN (рис. 44).

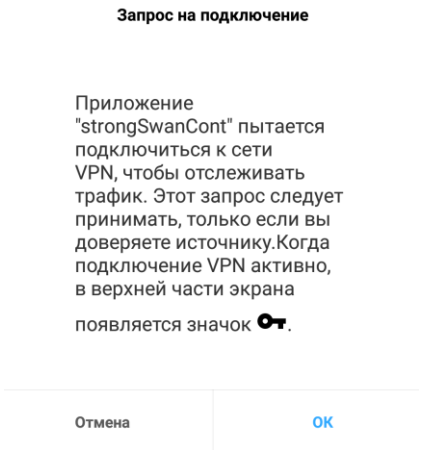


Рис. 44

3.3.5.5.2. Далее отобразится диалоговое окно (рис. 45) с сообщением о внесении КП «БАС-А» в белый список устройства (список приложений, которые игнорируют оптимизацию батареи). После нажатия на кнопку ОК, КП «БАС-А» запросит разрешение на внесение приложения в белый список (рис. 46).

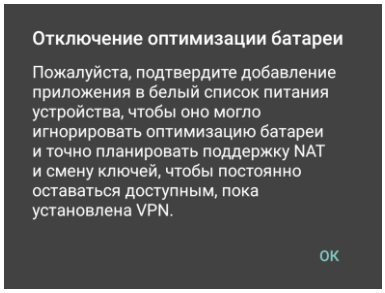


Рис. 45

Рис. 46

3.3.5.5.3. Во время подключения на панели статуса отображается статус «Подключение…», имя подключаемого профиля и индикатор процесса подключения (рис. 47).

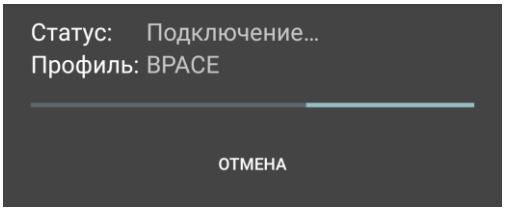


Рис. 47

Для того чтобы прервать подключение необходимо нажать на кнопку «Отмена».

3.3.5.5.4. Если КП «БАС-А» успешно подключился в VPN-серверу на панели статуса отобразится статус «Подключен» (рис. 48).

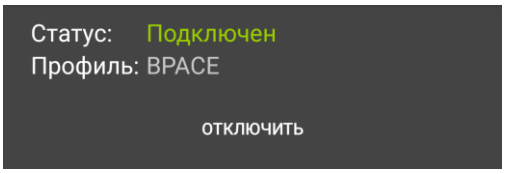


Рис. 48

Для отключения от VPN-сервера необходимо нажать на кнопку «Отключить» на панели статуса подключения.

3.3.5.5.5. Если во время подключения произошла ошибка, то на панели статуса появится дополнительная область, в которой кратко описана ошибка. Также в области есть кнопка для просмотра журнала (кнопка «Журнал») и кнопка для повторного подключения (кнопка «Попробовать снова») (рис. 49).

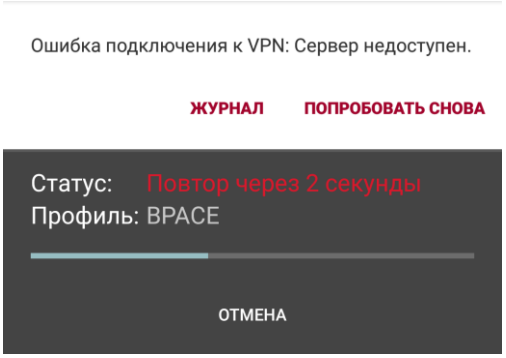


Рис. 49

Также КП «БАС-А» будет пробовать подключиться автоматически через некоторые промежутки времени.

3.3.5.5.6. Если при установленном подключении выбрать в списке настроенных профилей тот профиль, который подключен в текущий момент, отобразится сообщение, представленное на рис. 50.

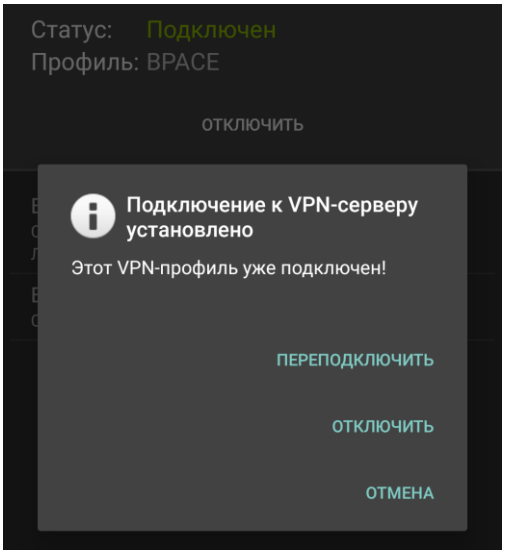


Рис. 50

3.3.5.5.7. Если при установленном подключении выбрать в списке настроенных профилей любой профиль, отличный от того, который подключен в текущий момент, отобразится сообщение, представленное на рис. 51.

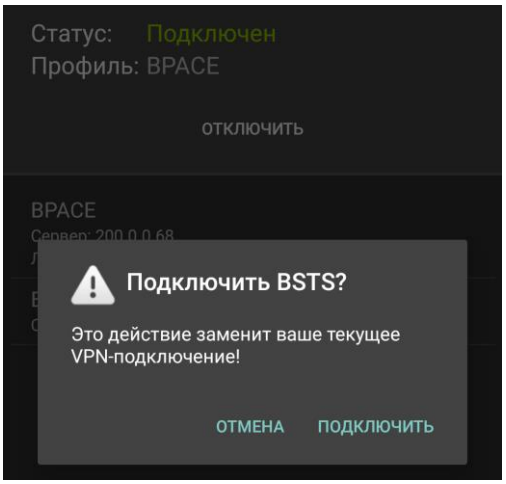


Рис. 51

3.3.6. Обработка COC

В КП «БАС-А» обработка COC выполняется двумя способами:

– из локального репозитория;

– из пунктов распространения COC.

3.3.6.1. Обработка COC из локального репозитория

Во время добавления (или редактирования) VPN-профиля с типом VPN «IKEv2 EAP-BSTS (Сертификат)» есть возможность указать локальный репозиторий COC. Это директория в памяти устройства, в которой хранятся файлы COC. Расширения файлов могут быть любыми.

Во время установки подключения к VPN-серверу КП «БАС-А» обработает файлы COC, находящиеся в локальном репозитории.

Примечание. Файлы, которые не прошли проверку на соответствие формату COC, будут удалены из директории, выбранной в качестве локального репозитория. Рекомендуется создать отдельную директорию в качестве локального репозитория COC и хранить в ней только COC.

3.3.6.2. Обработка COC из пунктов распространения

В расширенных настройках VPN-профиля есть переключатель «Использовать COC для проверки статуса сертификата». Если этот переключатель включен, а сертификат сервера содержит расширение CRLDistributionPoints (пункты распространения списка отозванных сертификатов), то для проверки статуса сертификата сервера будут отправлены запросы COC на указанные пункты распространения. В случае получения COC они сохраняются в кэше COC’ов.

3.3.6.2.1. Для очистки кэша COC’ов необходимо в главном окне нажать кнопку вызова меню и выбрать пункт «Кэш COC’ов» (рис. 52).

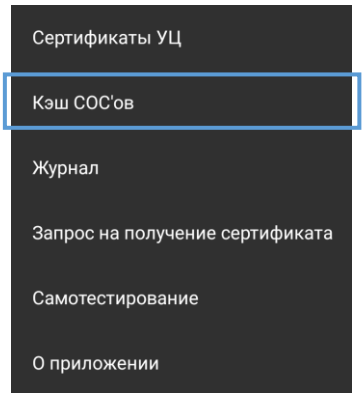


Рис. 52

Если кэш непустой, то отобразится сообщение (рис. 53) с общим количеством файлов и объемом кэша СОС’ов, в котором можно очистить кэш.

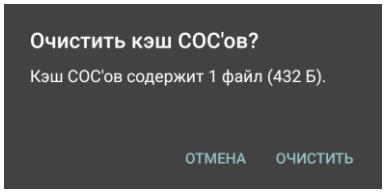


Рис. 53

Если кэш пустой, то это отобразится во всплывающем сообщении.

3.3.7. Журналы

3.3.7.1. КП «БАС-А» ведет три журнала:

– «charon.log», содержит сообщения о подключении к VPN-серверу;

– «certreq.log», содержит сообщения о формировании ключевого контейнера и запроса на получение сертификата;

– «selftest.log», содержит сообщения о выполнении самотестирования.

3.3.7.2. Для просмотра журналов необходимо в главном окне нажать кнопку вызова меню и выбрать пункт «Журнал» (рис. 54).

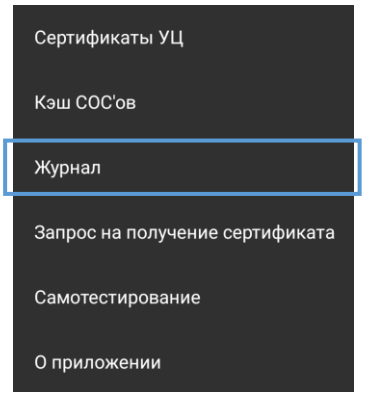


Рис. 54

По умолчанию откроется окно журнала «charon.log» либо последнего открытого журнала.

Для выбора журнала необходимо в окне «Журнал» в правом верхнем углу нажать кнопку вызова меню и выбрать необходимый журнал (рис. 55).

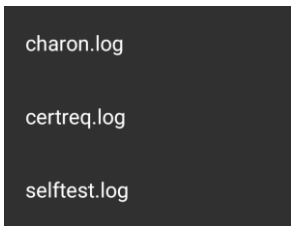


Рис. 55

Примеры журналов приведены в Приложении Б.

3.3.7.3. В КП «БАС-А» есть возможность отправлять файл журнала доступными на устройстве способами (электронная почта, различные мессенджеры и пр.). Для этого необходимо открыть для просмотра нужный журнал и в верхнем правом углу нажать кнопку «Отправить журнал». После этого откроется окно выбора приложения для отправки файла (например, как на рис. 56).

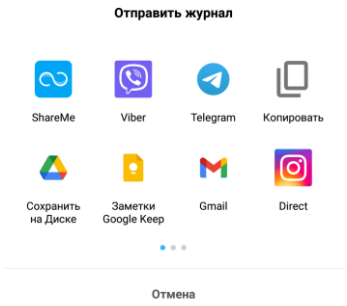


Рис. 56

3.3.8. Просмотр версии

Для просмотра версии необходимо в главном окне нажать кнопку вызова меню и выбрать пункт «О программе» (рис. 57).

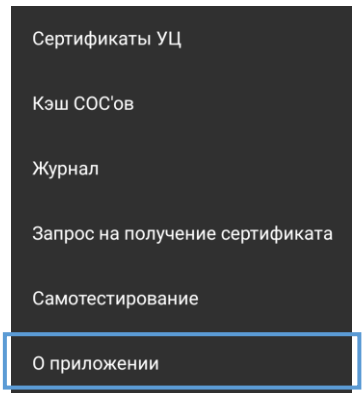


Рис. 57

Отобразится окно, представленное на рис. 58.

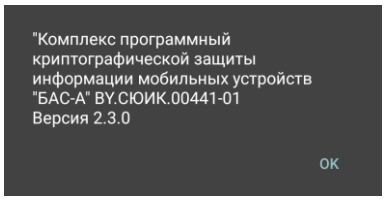


Рис. 58

3.4. Удаление

Удаление КП «БАС-А» с помощью системных настроек.

Примечание. В операционных системах, которые являются оболочками Android, расположение меню и названия пунктов могут отличаться от приведенных ниже.

Для удаления КП «БАС-А» через системные настройки необходимо выполнить шаги:

1) открыть меню устройства;

2) выбрать пункт «Настройки»;

3) выбрать пункт «Приложения» или «Диспетчер приложений» (на старых версиях Android);

4) найти и выбрать приложение «strongSwanCont»;

5) выбрать пункт «Память», если он есть. Если нет, то перейти к шагу 8;

6) нажать кнопку «Очистить данные». Кэш при этом также удалится;

7) нажать назад;

8) нажать кнопку «Удалить», подтвердить свой выбор, нажав «ОК».

4. СООБЩЕНИЯ ОПЕРАТОРУ

КП «БАС-А» выводит сообщения оператору во время выполнения в виде окон с сообщениями и всплывающих сообщений. Сообщения описаны в п. 3.3.

Также КП «БАС-А» выводит сообщения в журналы (см. п. 3.3.7). Сообщения четко описывают причину их появления и не нуждаются в разъяснении.

ПРИЛОЖЕНИЕ А

СПИСОК ОБОЗНАЧЕНИЙ ДОСТУПНЫХ КРИПТОГРАФИЧЕСКИХ АЛГОРИТМОВ

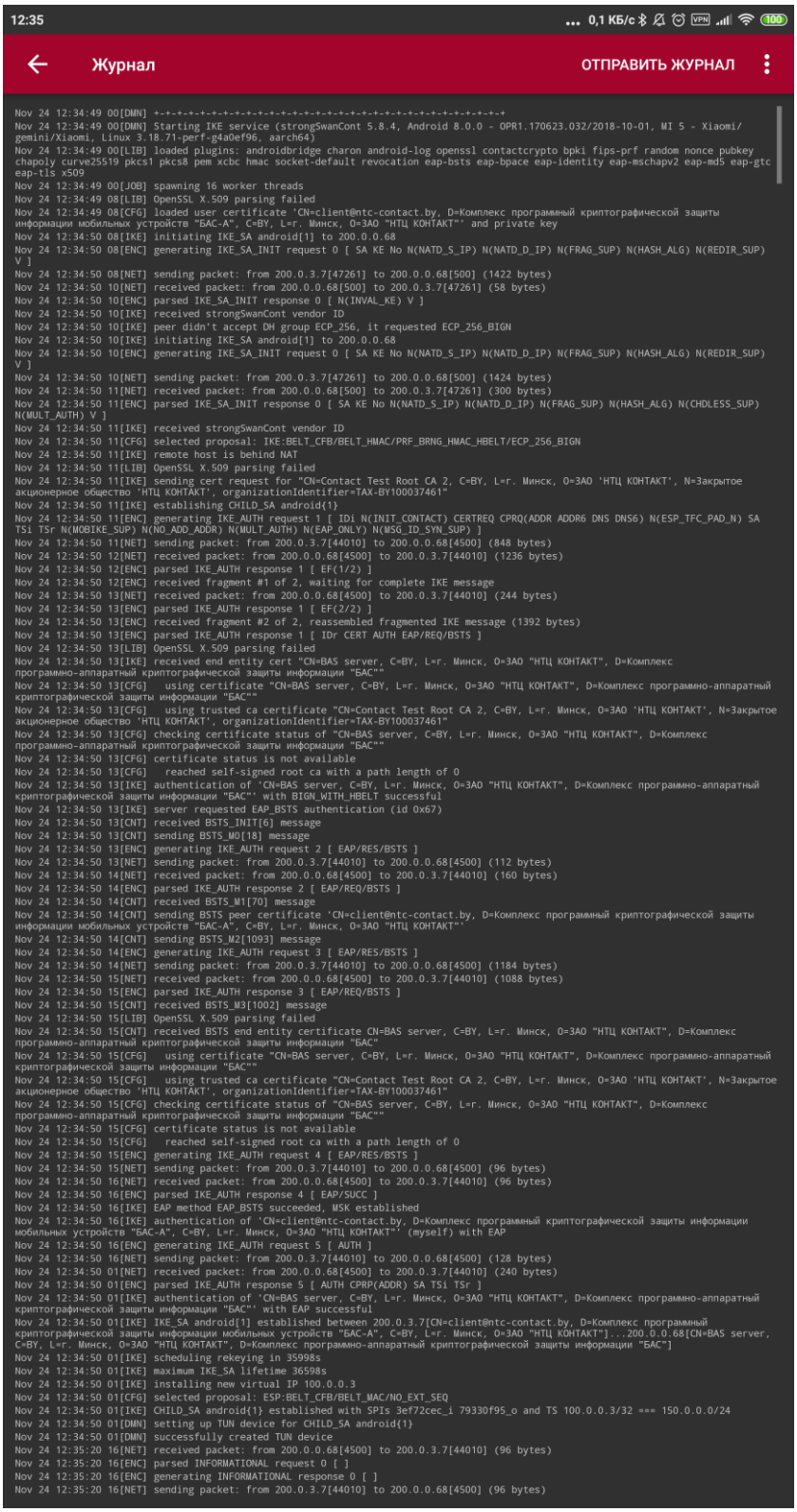
Таблица А.1 – Список обозначений доступных криптографических алгоритмов

EALG	
belt_cbc	алгоритм шифрования СТБ 34.101.31 в режиме сцепления блоков
belt_cfb	алгоритм шифрования СТБ 34.101.31 в режиме гаммирования с обратной связью
belt_ctr	алгоритм шифрования СТБ 34.101.31 в режиме счётчика
belt_cbc_legacy	алгоритм шифрования СТБ 34.101.31 в режиме сцепления блоков (для совместимости с первой версией ПАК «БАС»)
belt_cfb _legacy	алгоритм шифрования СТБ 34.101.31 в режиме гаммирования с обратной связью (для совместимости с первой версией ПАК «БАС»)
belt_ctr legacy	алгоритм шифрования СТБ 34.101.31 в режиме счётчика (для совместимости с первой версией ПАК «БАС»)
IALG	
belt_mac	алгоритм выработки иммитовставки СТБ 34.101.31
belt_hmac	алгоритм ключезависимого хэширования СТБ 34.101.47
belt_mac_legacy	алгоритм выработки иммитовставки СТБ 34.101.31 (для совместимости с первой версией ПАК «БАС»)
belt_hmac_legacy	алгоритм ключезависимого хэширования СТБ 34.101.47 (для совместимости с первой версией ПАК «БАС»)
PRF	
prfbrng_ctr	алгоритм выработки псевдослучайных чисел СТБ 34.101.47 в режиме счётчика
prfbrng_hmac	алгоритм выработки псевдослучайных чисел СТБ 34.101.47 в режиме HMAC
DHGROUP	
ecp256bign	Алгоритм Диффи-Хеллмана с соответствии с СТБ 34.101.66 Приложение А.
modp2048	(для совместимости с первой версией ПАК «БАС»)
KEYREP	
keyrep	алгоритм преобразования ключа СТБ 34.101.31
Примечания: – жирным выделены алгоритмы, используемые по умолчанию; – курсивом выделены первые поддерживаемые значения.	

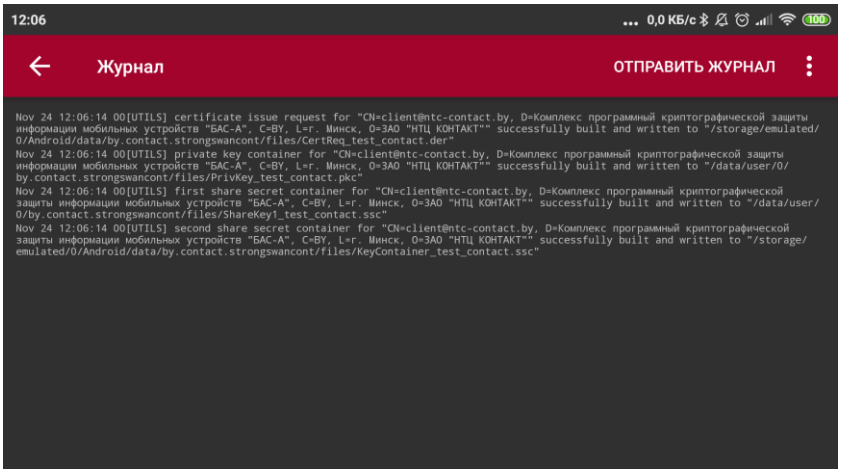
ПРИЛОЖЕНИЕ Б

ПРИМЕРЫ ЖУРНАЛОВ

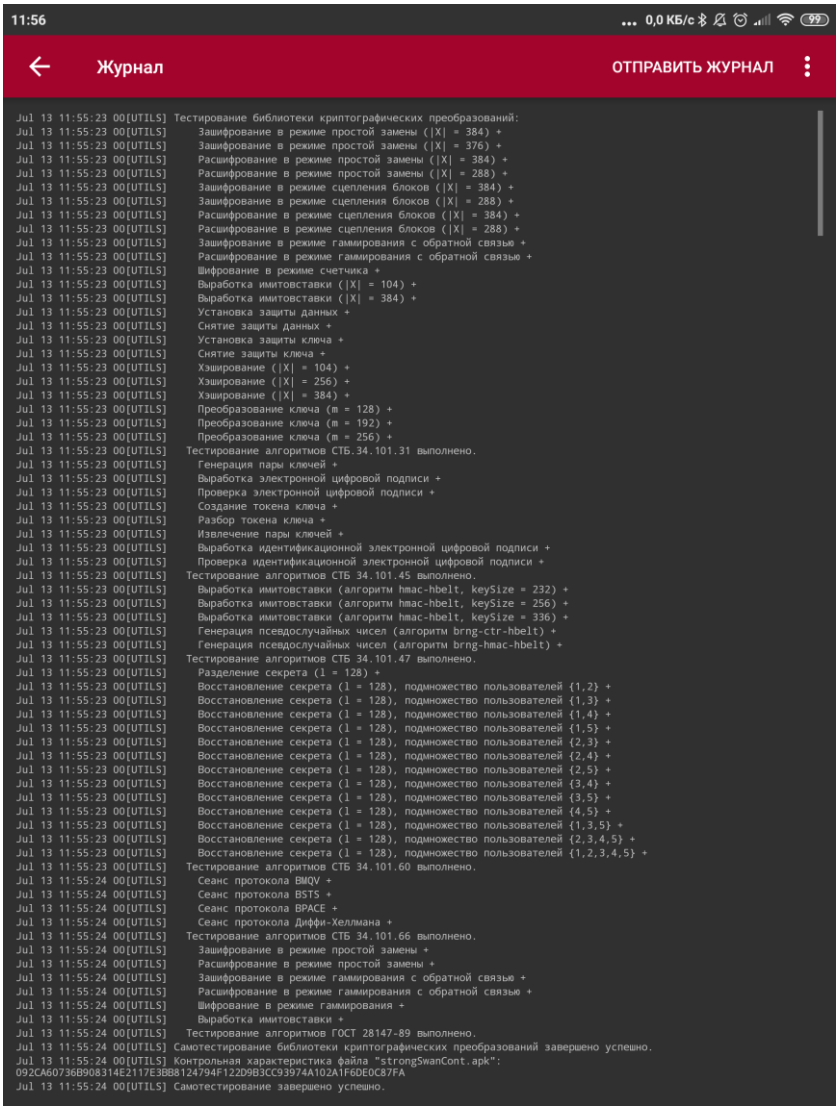
Б.1. Пример журнала «charon.log»



Б.2. Пример журнала «certreq.log»



Б.3. Пример журнала «selftest.log



ПРИЛОЖЕНИЕ В

ПЕРЕЧЕНЬ СОКРАЩЕНИЙ

В настоящем документе приняты следующие сокращения:

ОС – операционная система

ОЗУ – оперативное запоминающее устройство

ПО – программное обеспечение

СОК – сертификат открытого ключа

СОС – список отозванных сертификатов

УЦ – Удостоверяющий центр

Лист регистрации изменений

Изм.	Номера листов (страниц)				Всего листов (страниц) в докум.	№ документа	Входящий № сопроводительного докум. и дата	Подп.	Дата
	измененных	замененных	новых	аннулированных					