

ООО «С-Терра СиЭсПи»
124498, г. Москва, Зеленоград, Георгиевский проспект,
дом 5, помещение I, комната 33
Телефон/Факс: +7 (499) 940 9061
Эл.почта: information@s-terra.com
Сайт: <http://www.s-terra.com>



Программный комплекс С-Терра Клиент-М. Версия 4.1

Руководство администратора

РЛКЕ.00009-04 90 03

06.07.2015

Содержание

1. Комплект поставки	4
1.1. Комплект поставки «Программного комплекса С-Терра Клиент-М», исполнения класса защиты КС1	4
1.2. Комплект поставки «Программного комплекса С-Терра Клиент-М», исполнения класса защиты КС2	5
2. Требования к программно-аппаратным средствам	6
3. Назначение и функции Продукта	7
4. Особенности работы Продукта исполнения класса защиты КС2	8
4.1. Функционирование кнопок устройства при работе модуля доверенной загрузки	8
4.2. Ведение журнала событий модулем доверенной загрузки	9
4.3. Поведение при аварийном завершении работы модуля доверенной загрузки	9
5. Инсталляция «Программного комплекса С-Терра Клиент-М»	10
5.1. Контроль целостности дистрибутива	10
5.2. Инсталляция «С-Терра Клиент-М»	11
6. Инициализация S-Terra Client-M при первом запуске	14
7. Описание интерфейса «Программного комплекса С-Терра Клиент-М»	16
7.1. Регистрация пользователя	17
7.1.1. Интерактивный режим логина в Продукт	17
7.1.2. Автоматический режим логина в Продукт	18
7.2. Главная форма	19
7.2.1. Меню главной формы	19
7.2.2. Элементы интерфейса главной формы	24
7.3. Конфигурация IKE/IPsec	25
7.3.1. Показать конфигурацию	26
7.3.2. Создать конфигурацию	27
7.3.3. Ввести конфигурацию как текст	31
7.3.4. Загрузить конфигурацию из файла	31
7.3.5. Редактировать текущую конфигурацию	32
7.3.6. Остановить защищенное соединение	33
7.3.7. Политика по умолчанию	33
7.4. Сертификаты	35
7.5. Задать общий ключ (preshared key)	40

7.6. Настройки протоколирования	41
8. Деинсталляция «Программного комплекса С-Терра Клиент-М»	42
9. Замечания по использованию «С-Терра Клиент-М»	43
10. Приложение	44
10.1. Получение сертификата пользователя и СА-сертификата	44
10.2. Создание контейнера с ключевой парой на токене	49
10.3. Настройка «С-Терра Клиент-М» с использованием конфигурационного файла	50
10.4. Особенности настройки шлюза при работе с «Программным комплексом С-Терра Клиент-М»	51
10.5. Сообщения об ошибках	52
10.6. Состояние служб IKE/IPsec	56

1. Комплект поставки

1.1. Комплект поставки «Программного комплекса С-Терра Клиент-М», исполнения класса защиты КС1

В комплект поставки «Программного комплекса С-Терра Клиент-М», исполнения класса защиты КС1 входит компакт-диск, на котором находятся:

- Каталог **APK**
 - Каталог **Samsung** – содержит дистрибутив «С-Терра Клиент-М» для мобильных устройств Samsung (Samsung Galaxy S5, Samsung Galaxy S 5 Mini, Samsung Galaxy Tab 10.1, Samsung Galaxy Note 4):
 - s_terra_clientm_esc-4.1.14905.apk – криптографическая библиотека ГОСТ,
 - ap_s_terra_clientm_s_4.1.14905.apk – основное архивное исполняемое приложение, подписанное производителем устройства,
 - файл hashes.
 - Каталог **Yotaphone** – содержит дистрибутив «С-Терра Клиент-М» для мобильных устройств YotaPhone, YotaPhone 2:
 - s_terra_clientm_y-4.1.14905_common_2.apk – архивное исполняемое приложение, подписанное производителем устройства,
 - файл hashes.
 - Каталог **Others** – содержит дистрибутив «С-Терра Клиент-М» для мобильных устройств, работающих под работающими ОС Android 4.x, кроме перечисленных выше:
 - s_terra_clientm-4.1.14905.apk – архивное исполняемое приложение,
 - файл hashes.
 - stverify – утилита для проверки целостности дистрибутива.
- Каталог **Documentation**:
 - «Программный комплекс С-Терра Клиент-М. Руководство администратора» – STerra_ClientM_AdminGuide.pdf,
 - «Программный комплекс С-Терра Клиент-М. Руководство администратора. Создание конфигурационного файла» – Lsp.pdf,
 - «Программно-аппаратный комплекс С-Терра VPN. Версия 4.1. Правила пользования» – Rules-ST.pdf,
 - «Программно-аппаратный комплекс С-Терра VPN. Версия 4.1. Формуляр». (ФСБ России) – Formular_FSB.pdf.
- В печатном виде поставляются:
 - Копия сертификата соответствия ФСБ России.
 - Лицензия на использование «Программного комплекса С-Терра Клиент-М. Версия 4.1».

1.2. Комплект поставки «Программного комплекса С-Терра Клиент-М», исполнения класса защиты КС2

В комплект поставки «Программного комплекса С-Терра Клиент-М», исполнения класса защиты КС2 входит:

- Мобильное устройство (Samsung Galaxy Note 4 или YotaPhone 2), работающее под управлением ОС Android, с предустановленным продуктом «С-Терра Клиент-М» (исполняемое приложение подписано производителем устройства).
- Компакт-диск, содержащий:
 - Каталог **Documentation**:
 - «Программный комплекс С-Терра Клиент-М. Руководство администратора» – STerra_ClientM_AdminGuide.pdf,
 - «Программный комплекс С-Терра Клиент-М. Руководство администратора. Создание конфигурационного файла» – Lsp.pdf,
 - «Программно-аппаратный комплекс С-Терра VPN. Версия 4.1. Правила пользования» – Rules-ST.pdf,
 - «Программно-аппаратный комплекс С-Терра VPN. Версия 4.1. Формуляр». (ФСБ России) – Formular_FSB.pdf.
- В печатном виде поставляются:
 - Копия сертификата соответствия ФСБ России.
 - Лицензия на использование «Программного комплекса С-Терра Клиент-М. Версия 4.1».

2. Требования к программно-аппаратным средствам

«Программный комплекс С-Терра Клиент-М» предназначен для использования на мобильных устройствах Samsung и YotaPhone, работающих под управлением ОС Android 4.x:

- Samsung Galaxy S5,
- Samsung Galaxy S 5 Mini,
- Samsung Galaxy Tab 10.1,
- Samsung Galaxy Note 4,
- YotaPhone,
- YotaPhone 2.

Возможна работа с токенами следующих моделей: "JaCarta MicroSD", "Рутокен ЭЦП" (USB), "Рутокен ЭЦП Bluetooth".

3. Назначение и функции Продукта

Продукт «Программный комплекс С-Терра Клиент-М» (далее Продукт S-Terra Client-M, Продукт, S-Terra Client-M, С-Терра Клиент-М) предназначен для создания защищенных VPN соединений между устройством, на котором он установлен, и другими взаимодействующими с ним доверенными шлюзами VPN и доверенными клиентами VPN.

Продукт S-Terra Client-M выполняет следующие функции:

- обеспечивает защиту трафика на уровне шифрования сетевых пакетов по протоколам IPsec ESP;
- поддерживает метод аутентификации сторон с использованием предопределенных ключей или электронной цифровой подписи в рамках протокола IKE;
- поддерживает формат сертификатов публичных ключей X.509 версии 3.0;
- выполняет генерацию данных аудита и вывод на удаленный или локальный syslog-сервер;
- обеспечивает регулируемую стойкость защиты трафика.

S-Terra Client-M осуществляет защиту трафика протоколов семейства TCP/IP в рамках международных стандартов IKE/IPsec:

- Security Architecture for the Internet Protocol – RFC2401,
- IP Encapsulating Security Payload (ESP) – RFC2406,
- Internet Security Association and Key Management Protocol (ISAKMP) – RFC2408,
- The Internet Key Exchange (IKE) – RFC2409,
- The Internet IP Security Domain of Interpretation for ISAKMP (DOI) – RFC2407.

Продукт S-Terra Client-M использует встроенную криптографическую библиотеку, разработанную компанией «С-Терра СиЭсПи», которая реализует российские криптографические алгоритмы:

- ГОСТ 28147-89 – шифрование/расшифрование данных,
- ГОСТ Р 34.11-94, ГОСТ Р 34.11-2012 – алгоритм хэширования,
- ГОСТ Р 34.10-2001, ГОСТ Р 34.10-2012 – формирование и проверка электронно-цифровой подписи (ЭЦП),
- VKO GOST R 34.10-2001, VKO GOST R 34.10-2012 (256 бит) – выработка общего сессионного ключа,
- а также генерацию случайных чисел.

Продукт S-Terra Client-M работает не только с криптоалгоритмами ГОСТ, но и с международными криптоалгоритмами.

Графический интерфейс S-Terra Client-M представлен как в русском, так и английском варианте и зависит от выбранной настройки мобильного устройства.

Пример сценария, описывающего построение VPN туннеля между шлюзом безопасности S-Terra Gate и мобильным клиентом S-Terra Client-M, можно посмотреть на сайте <http://www.s-terra.com> в разделе «Решения – Типовые сценарии применения продуктов S-Terra» (http://www.s-terra.com/images/Scenarios/text/ver_4_1_scn_1_22.pdf).

4. Особенности работы Продукта исполнения класса защиты КС2

«Программный комплекс С-Терра Клиент-М», исполнения класса защиты КС2 включает в себя модуль доверенной загрузки, проверяющий целостность файлов по заранее заданному списку при старте ОС Android. Целостность контролируется путём вычисления значения хэш-функции (по алгоритму ГОСТ Р 34.11-2012 с размером хэша 256 бит) и сравнения результата вычисления с записанным в файле эталоном.

Модуль доверенной загрузки может работать в двух режимах, отличающихся реакцией на нарушения, обнаруженные при контроле целостности. В обоих случаях будет выдано сообщение об ошибке, далее:

- при нестрогом режиме пользователю предлагается выбор – выключить устройство либо продолжить загрузку ОС Android;
- при строгом режиме загрузка ОС Android блокируется, и устройство можно только выключить.

Если ошибок при контроле целостности обнаружено не будет, то произойдет автоматическая загрузка ОС Android.

Пользователь может заказать установку необходимого режима работы для модуля доверенной загрузки при покупке «Программного комплекса С-Терра Клиент-М». Режим задаётся в конфигурационном файле `st_boot_module.cfg`. Конфигурационный файл может быть расположен либо в памяти устройства `/internal_media_st/S-Terra/st_boot_module.cfg`, либо на внешней microSD карте `/external_media_st/S-Terra/st_boot_module.cfg`.

При работе модуля доверенной загрузки, на экране устройства отображается следующая информация:

- графический логотип S-Terra;
- название продукта и номер версии исполняемого файла модуля доверенной загрузки;
- текущая выполняемая операция;
- подсказка о назначении кнопок устройства (подробнее описание приведено ниже);
- подробные сведения о контроле целостности;
- итоговый результат контроля целостности.

4.1. Функционирование кнопок устройства при работе модуля доверенной загрузки

Назначение кнопок устройства во время работы модуля доверенной загрузки:

- **Home** – загрузить ОС Android при успешном контроле целостности, либо при любом результате контроля целостности при нестрогом режиме работы модуля доверенной загрузки.
При строгом режиме работы модуля доверенной загрузки при обнаружении нарушения целостности, нажатие на кнопку **Home** игнорируется, и дальнейшая загрузка ОС Android блокируется.
- На устройстве Galaxy Tab 10.1 отсутствует кнопка **Home**, вместо нее используется двойное нажатие на кнопку **Power** (Double Power).

- **Power** – выключить устройство.
- **Volume Up / Volume Down** – войти в режим подробного просмотра информации о проверке целостности файлов. Последующее нажатие осуществляет переход на одно более раннее/позднее сообщение в подробном режиме.

Нажатия кнопок запоминаются программой. Однако соответствующее действие может быть осуществлено не сразу (например, при длительной проверке контрольных сумм файлов, ожидаемое действие на нажатие кнопки – продолжение загрузки, выключение, переход в подробный режим – будет осуществлено только после завершения проверки всех файлов).

Назначение кнопок устройства при успешном завершении контроля целостности (доступны в течение 5 секунд после завершения проверки, далее автоматически загрузится ОС Android):

- **Volume Up / Volume Down** – переход в подробный режим просмотра информации о проверке целостности файлов.
- **Power / Home / Double Power** (только для Galaxy Tab 10.1 и YotaPhone 2) – продолжить загрузку ОС Android.

4.2. Ведение журнала событий модулем доверенной загрузки

При работе модуля доверенной загрузки ведётся протоколирование событий и ошибок в файл `/system/st_boot_module.log`. При наличии внешней `microsd`-карты, данный файл копируется в `/external_media_st/S-Terra/st_boot_module.log`, при её отсутствии – в `/internal_media_st/S-Terra/st_boot_module.log`.

В журнал событий записывается следующая информация:

- версия исполняемого файла модуля доверенной загрузки,
- дата и время запуска,
- техническая информация об устройстве (тип, размер экрана),
- какой конфигурационный файл использован (местоположение файла),
- режим работы модуля доверенной загрузки,
- список проверяемых файлов с результатом проверки,
- сообщения об ошибках.

Максимальный размер файла – 32 мегабайта. При переполнении файла удаляются самые старые записи.

4.3. Поведение при аварийном завершении работы модуля доверенной загрузки

В случае непредвиденной ошибки и аварийного завершения работы модуля доверенной загрузки, устройство будет принудительно выключено через 3 секунды. При этом на устройствах с цветным светодиодом будут последовательно гореть синий, зелёный и красный цвета. На устройствах без цветного светодиода дважды загорится светодиод фотовспышки.

Также в файл `/system/st_boot_module.log` будет записан статус выхода (exit code) модуля доверенной загрузки.

5. Установка «Программного комплекса С-Терра Клиент-М»

В случае поставки «Программного комплекса С-Терра Клиент-М», исполнения класса защиты КС2, программный комплекс уже предустановлен на мобильном устройстве.

Поэтому сразу перейдите к разделу «Инициализация S-Terra Client-M при первом запуске».

5.1. Контроль целостности дистрибутива

Перед установкой «Программного комплекса С-Терра Клиент-М» можно убедиться в целостности дистрибутивов, используя утилиту `stverify`, размещенную на поставляемом диске.

Для вычисления контрольной суммы дистрибутива, скопируйте дистрибутив и утилиту на компьютер и выполните команду (указав путь к файлу), например:

```
stverify -mk s_terra_clientm-4.1.14905.apk
```

Полученное значение сравните с эталонным значением контрольной суммы, записанным в файл `hashes` из состава дистрибутива, который содержит строки вида:

```
<hash> <file_name>,
```

где

`<hash>` – эталонное значение контрольной суммы

`<file_name>` – имя файла, для которого подсчитана контрольная сумма.

Для вычисления контрольной суммы для файла дистрибутива и автоматического сравнения с эталонным значением выполните команду (указав путь к файлу), например:

```
stverify s_terra_clientm-4.1.14905.apk hash_from_file,
```

где

`hash_from_file` – эталонное значение контрольной суммы для файла `s_terra_clientm-4.1.14905.apk`, скопированное из файла `hashes`.

5.2. Инсталляция «С-Терра Клиент-М»

Доставьте на мобильное устройство файлы с дистрибутивом «С-Терра Клиент-М».

На мобильном устройстве выберите предложение *Настройки* → *Приложения* и разрешите установку приложений из неизвестных источников.

Для устройств Samsung и YotaPhone установка «Программного комплекса С-Терра Клиент-М» будет немного отличаться, так как в комплект поставки для Samsung кроме основного арк-пакета входит криптографическая библиотека, которая должна быть установлена раньше основного пакета.

Для устройств Samsung сначала установите криптографическую библиотеку – s_terra_clientm_escr-4.1.14905.apk. Установка этого приложения не требует специальных разрешений (Рисунок 1). Версия криптографической библиотеки должна точно совпадать с версией основного пакета.



Рисунок 1

Появится сообщение, что приложение установлено. Для завершения установки нажмите [Готово](#).

Затем выполните установку приложения ap_s_terra_clientm_s-4.1.14905.apk (для устройств Samsung) или s_terra_clientm_y-4.1.14905_common_2.apk (для устройств YotaPhone).

При установке этих приложений запрашивается длинный список требуемых разрешений. Среди них встречаются достаточно специфичные, связанные с платными услугами, отсылкой SMS, доступом к телефонной книге, запросом местоположения пользователя и т.п. (Рисунок 2). Этот список связан с особенностью работы системных приложений в среде Android. Выдается список не только тех разрешений, которые требуются непосредственно для работы «Программного комплекса С-Терра Клиент-М», а выдается суммарный список разрешений, необходимый для всех системных приложений, установленных на данный момент на устройстве.

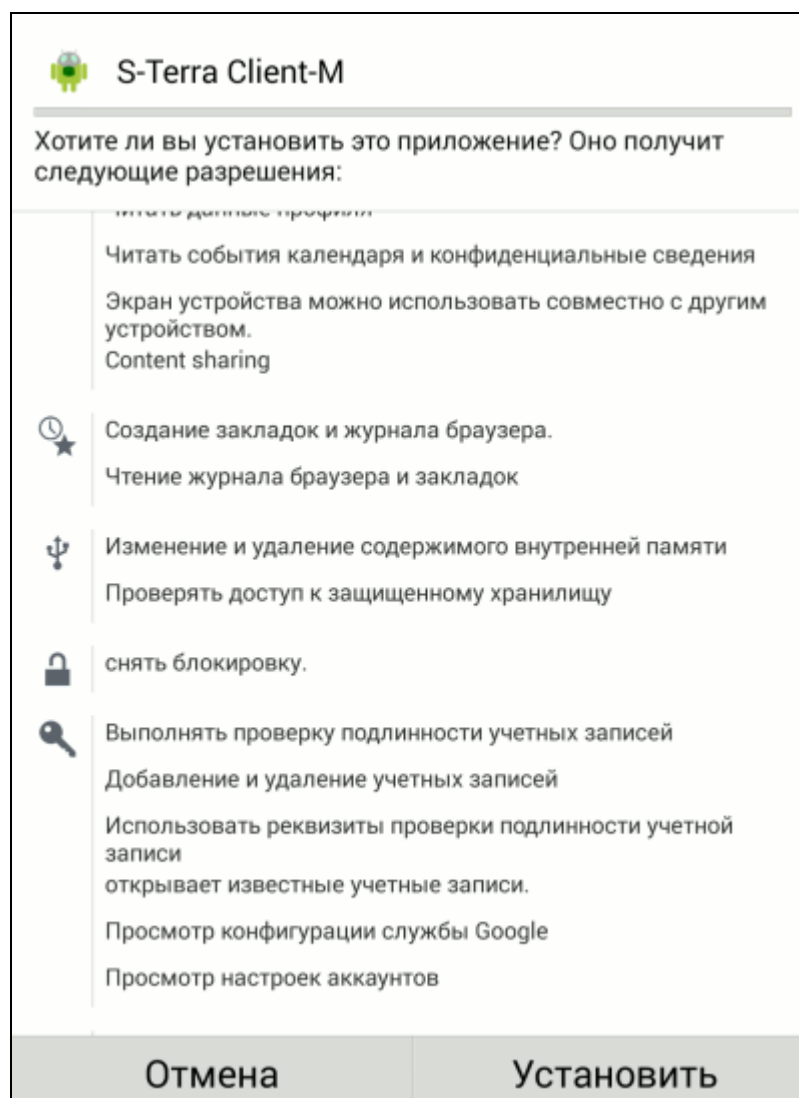


Рисунок 2

Реально продукту необходимы следующие разрешения:

- WRITE_EXTERNAL_STORAGE – изменение или удаление содержимого SD-карты (на SD-карте может создаваться каталог S-Terra, где могут сохраняться и читаться файлы с локальной политикой безопасности, сертификатными запросами, лицензией на продукт и т.п.).
- INTERNET – неограниченный доступ в интернет (для установления защищенного соединения).
- BIND_VPN_SERVICE – проверка доступа к защищенному хранилищу (в реальности речь идет о возможности создания виртуального сетевого интерфейса (только с явного разрешения пользователя), который необходим для установления защищенного соединения).

- RECEIVE_BOOT_COMPLETED – для выполнения действий на старте системы: загрузки политики безопасности по умолчанию и запуска утилиты, следящей за правилами firewall продукта.
- NET_ADMIN и SAMSUNG_MODIFY_IPTABLES – для управления firewall.

Нажимайте [Далее](#), пока не появится кнопка [Установить](#). После нажатия кнопки [Установить](#), выполнится установка S-Terra Client-M (Рисунок 3).

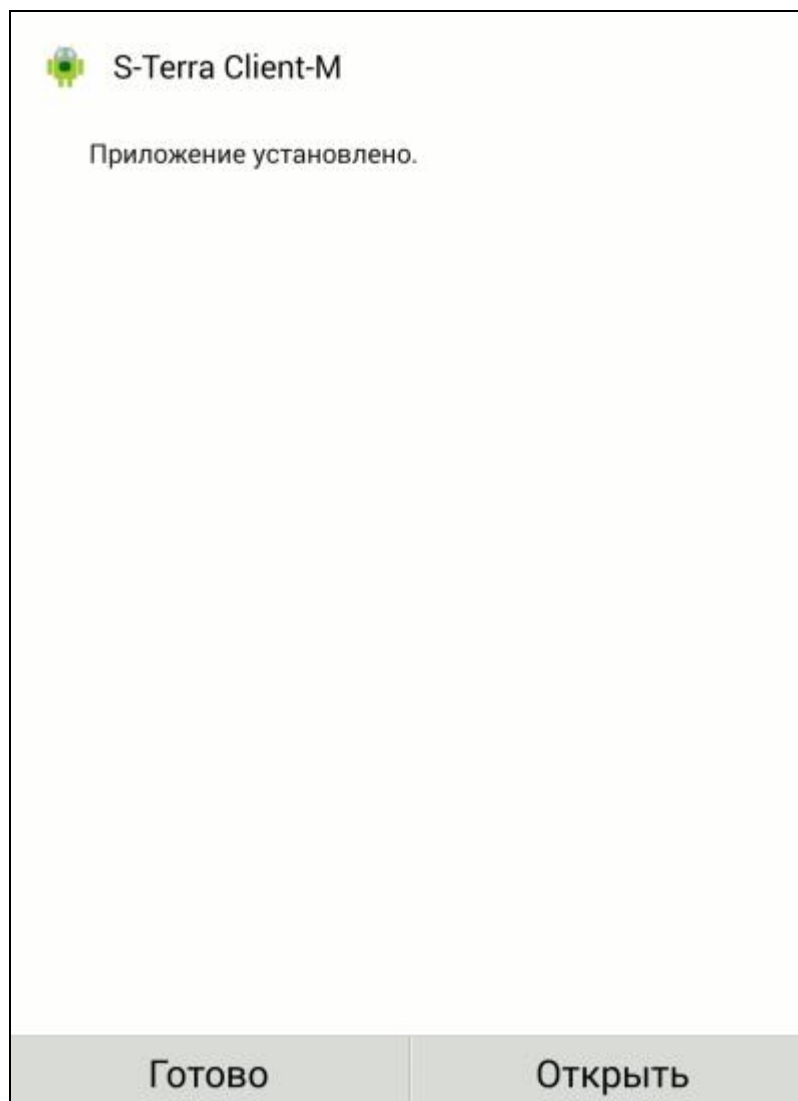


Рисунок 3

Для завершения установки нажмите [Готово](#), в этом случае дальнейшая инициализация Продукта будет выполнена при первом запуске приложения, или нажмите [Открыть](#), чтобы сразу запустить S-Terra Client-M после завершения установки.

6. Инициализация S-Terra Client-M при первом запуске

При первом запуске S-Terra Client-M будет выполнена «биологическая» инициализация генератора случайных чисел, а также запрошена дополнительная информация из лицензии на Продукт, которую нужно взять из лицензии на использование «Программного комплекса С-Терра Клиент-М», входящей в печатном виде в комплект поставки.

Примечание: иногда удобнее заранее подготовить файл с лицензионной информацией agent.lic, тогда при инициализации S-Terra Client-M необходимые данные будут автоматически получены из этого файла.

Пример файла agent.lic (недопустимы пробелы между названием поля, знаком "=" и значением поля):

```
[license]
CustomerCode=test
ProductCode=CLIENTM
LicenseNumber=1
LicenseCode=1234567890AACDDF
```

Файл agent.lic должен быть размещен в папке S-Terra, вложенной в Android External Storage Directory. Путь к Android External Storage Directory строго не регламентируется, но на практике обычно бывает /sdcard/S-Terra либо /mnt/sdcard/S-Terra.

Под термином "External Storage" понимается диск, который будет доступен как внешнее хранилище для компьютера, если к нему подключить, например, мобильное устройство по USB, работающее под управлением ОС Android.

Вначале инициализации S-Terra Client-M на дисплей будет выведено лицензионное соглашение о праве пользования Продуктом (Рисунок 4).

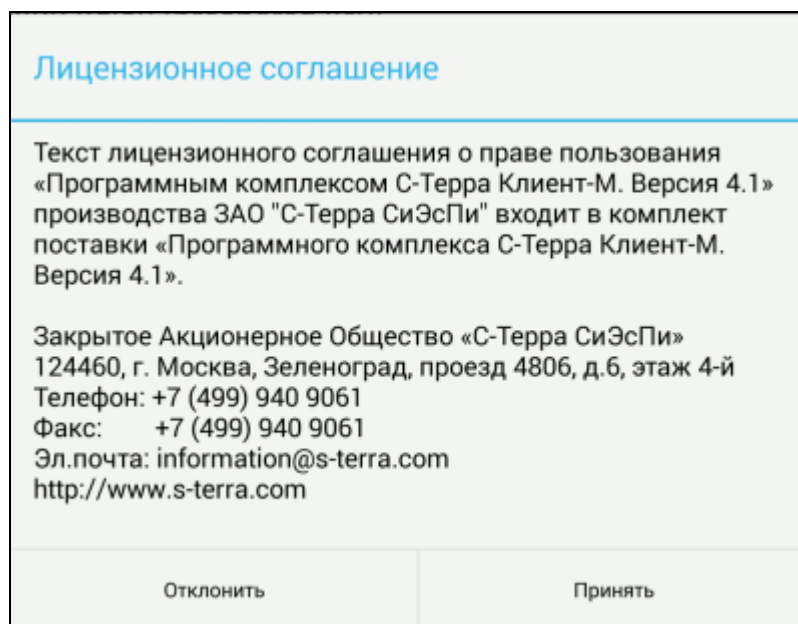
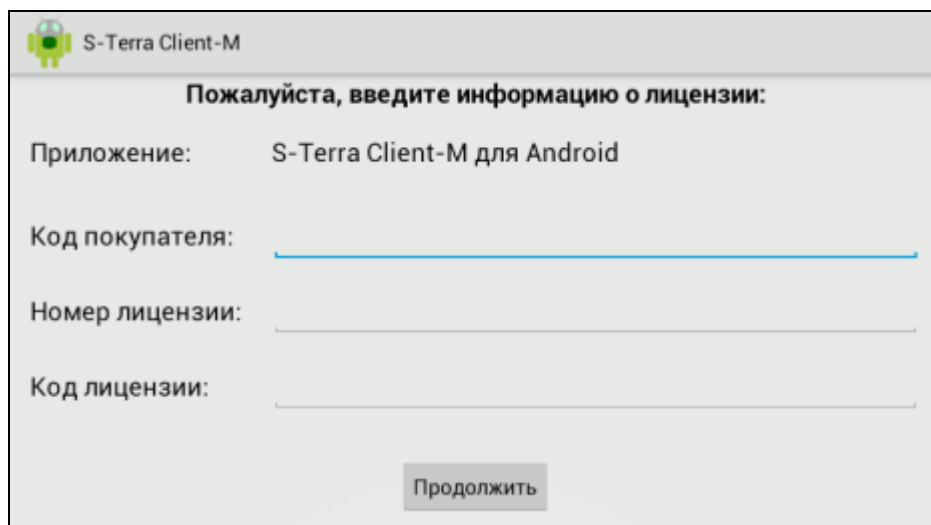


Рисунок 4

В случае принятия условий лицензионного соглашения, будет запрошена информация о лицензии на Продукт (Рисунок 5). Введите данные и нажмите [Продолжить](#).



The screenshot shows the 'S-Terra Client-M' application window. At the top, there is a title bar with the application name and an Android icon. Below the title bar, the text 'Пожалуйста, введите информацию о лицензии:' (Please enter license information:) is displayed. The form contains four labeled input fields: 'Приложение: S-Terra Client-M для Android' (Application: S-Terra Client-M for Android), 'Код покупателя:' (Buyer code:), 'Номер лицензии:' (License number:), and 'Код лицензии:' (License code:). Each field has a corresponding text input area. At the bottom right of the form, there is a button labeled 'Продолжить' (Continue).

Рисунок 5

Далее инициализируется генератор случайных чисел. Понажимайте на круг, меняющий свое местоположение на экране, пока выполняется инициализация (Рисунок 6).

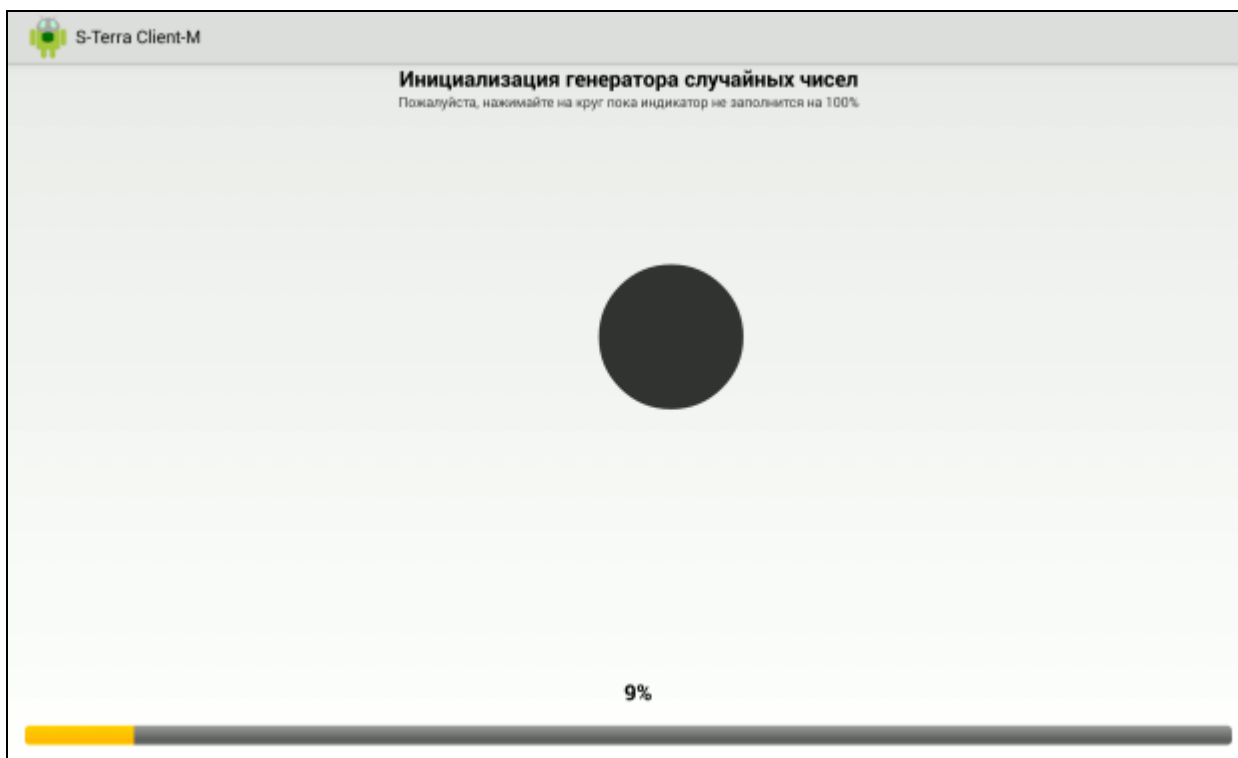


Рисунок 6

После этого S-Terra Client-M готов к эксплуатации. Используя графический интерфейс Продукта, выполните необходимые настройки.

7. Описание интерфейса «Программного комплекса С-Терра Клиент-М»

Настройка и управление «Программным комплексом С-Терра Клиент-М» осуществляется с использованием графического интерфейса. При запуске «С-Терра Клиент-М» на экране появляется главная форма (Рисунок 7).

Изначально доступны только следующие элементы: *Службы IKE/IPsec*, *О приложении* и пункты меню: *Автоблокировка*, *Выбрать тип токенов*, *Настройки криптографии*. Остальные настройки будут доступны после запуска служб IKE/IPsec. Чтобы запустить эти службы, надо установить установлен флажок *Службы IKE/IPsec*.

Установить автоблокировку, выбрать тип токенов и настроить криптографию можно как до запуска служб IKE/IPsec, так и позже.

Подробно все элементы формы и меню описаны в разделе [«Главная форма»](#).

Чтобы выполнить процедуру регистрации и получить доступ к остальным настройкам Продукта, позволяющим создать локальную политику безопасности (LSP), запустите службы IKE/IPsec.

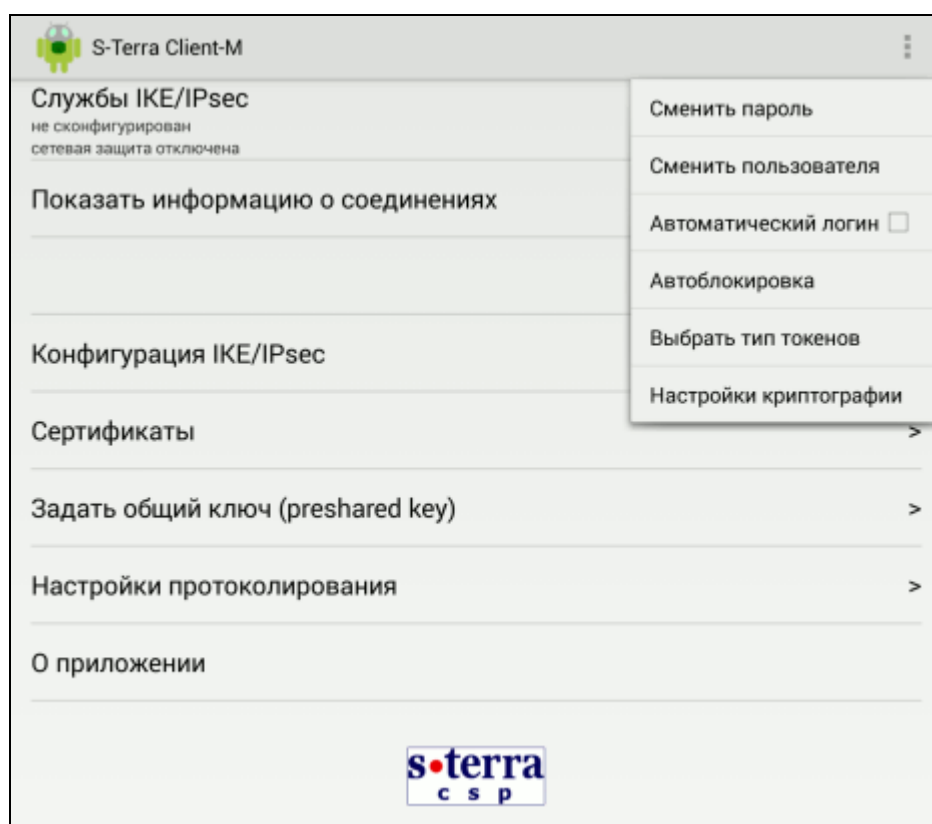


Рисунок 7

7.1. Регистрация пользователя

Режим логина в продукт может быть интерактивным (пользователь должен правильно ввести имя и пароль) и автоматическим (используется сохраненная информация из локальных настроек). Изменить режим логина можно через [меню](#) главной формы.

7.1.1. Интерактивный режим логина в Продукт

После успешного старта служб IKE/IPsec выдается окно логина (Рисунок 8).

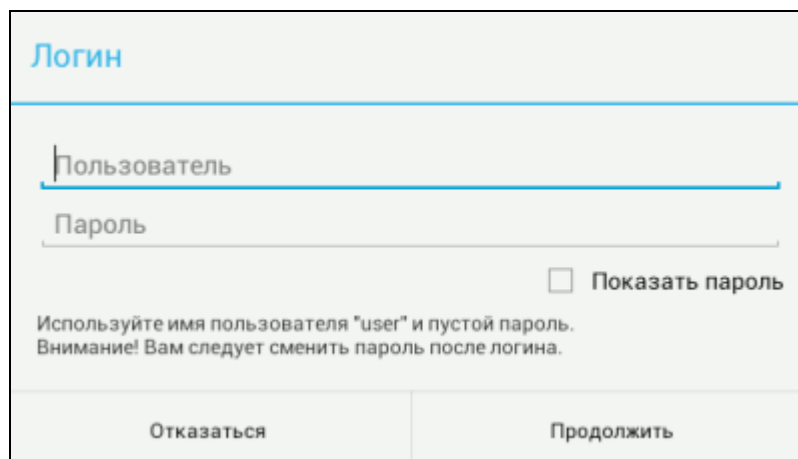


Рисунок 8

По умолчанию пароль частично скрывается. Если установить флажок *Показать пароль*, то пароль будет показан в открытом виде.

Введите имя пользователя, пароль и нажмите [Продолжить](#). Изначально: имя пользователя – user, пароль пустой. Эта подсказка появляется в окне логина, пока не изменится пользователь или пароль.

Если нажать кнопку [Отказаться](#), то регистрация пользователя не выполнится, службы IKE/IPsec будут остановлены. Для последующих попыток логина надо снова запустить службы IKE/IPsec.

При успешном логине будет выдано информационное сообщение, что логин произведен, и пользователь получает доступ ко всем пунктам меню [главной формы](#).

В случае ввода неправильного имени пользователя или пароля будет предложено повторить попытку (Рисунок 9). При нажатии на кнопку [Да](#) повторно выдается окно логина. После успешного логина счетчик допустимых попыток логина устанавливается в исходное значение – 10. При нажатии на кнопку [Нет](#), служба IKE/IPsec будет остановлена.

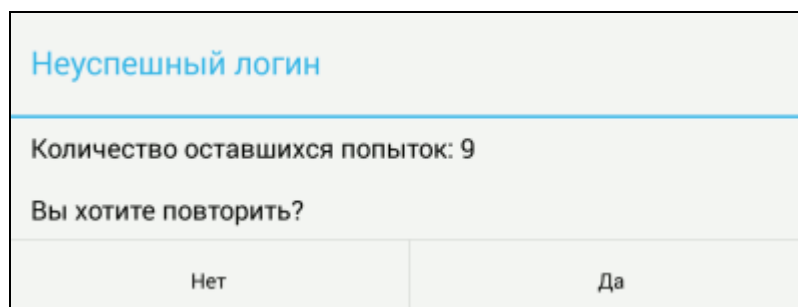


Рисунок 9

Допускаются десять неудачных попыток логина подряд. Затем будет выдано сообщение, что пользователь заблокирован». (Рисунок 10). После нажатия на кнопку [Продолжить](#) служба IKE/IPsec будет остановлена.

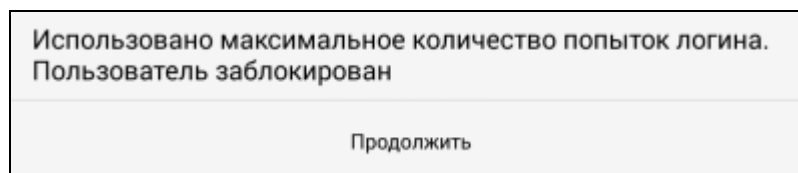


Рисунок 10

При дальнейших попытках логина, даже корректных, будет выдаваться сообщение, приведенное выше. Нормальная работа с продуктом в данной ситуации невозможна.

Решить проблему можно следующим образом:

1. В Настройках устройства войдите в *Диспетчер приложений*.
2. Выберите продукт *S-Terra Client-M*.
3. Нажмите на кнопку [Очистить данные](#). Подтвердите удаление данных.
4. Все действующие настройки продукта (локальная политика безопасности, сертификаты, секретные ключи, начальное значение генератора случайных чисел и т.п.) будут удалены.
5. Далее следует запустить продукт и заново выполнить инициализацию и настройку продукта.

7.1.2. Автоматический режим логина в Продукт

При автоматическом режиме логина в Продукт (без выдачи окна запроса логина) производится попытка логина с именем пользователя и паролем, сохраненными в локальных настройках.

По умолчанию автоматический логин отключен. Установить автоматический режим логина можно при помощи флажка *Автоматический логин*, доступного в соответствующем пункте меню (Рисунок 11).

7.2. Главная форма

После регистрации пользователя становятся доступны все элементы и все пункты меню главной формы (Рисунок 11).

Примечание: при настройке S-Terra Client-M пользователь может использовать свои, ранее созданные сертификаты и конфигурационные файлы, которые должны быть размещены в папке S-Terra, вложенной в [Android External Storage Directory](#).

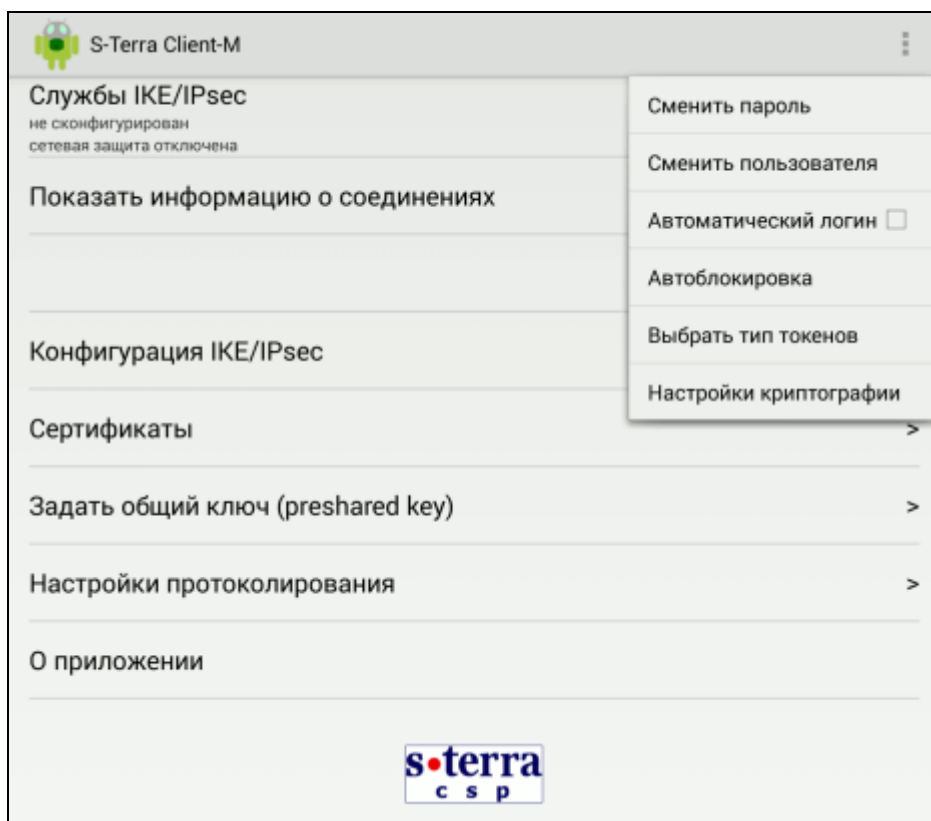


Рисунок 11

7.2.1. Меню главной формы

Сменить пароль

Для смены пароля выберите соответствующий пункт меню (Рисунок 11). Появится окно (Рисунок 12). Введите старый пароль и два раза новый пароль. Нажмите [Продолжить](#).

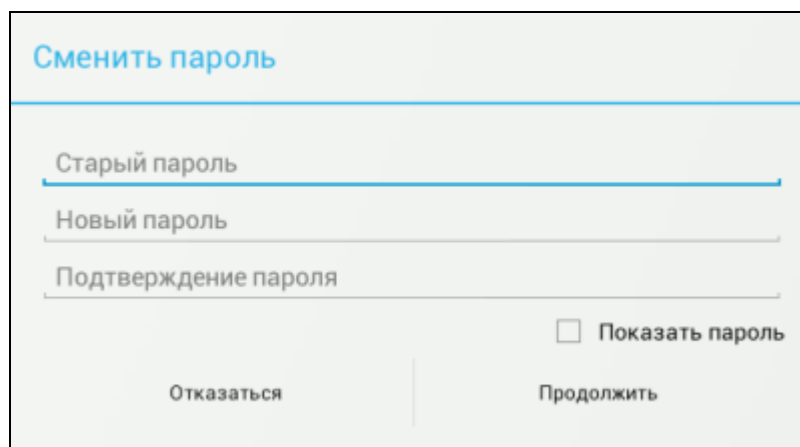


Рисунок 12

В случае успешной смены пароля появится уведомление:

Пароль успешно сменен.

Если перед успешной сменой пароля был задан неинтерактивный логин, то неинтерактивный логин отключается и выдается сообщение:

Пароль успешно сменен. Неинтерактивный логин отключен.

Сменить пользователя

Для смены пользователя выберите соответствующий пункт меню (Рисунок 11).

В появившемся окне (Рисунок 13) надо ввести пароль предыдущего пользователя, имя нового пользователя и два раза новый пароль.

По умолчанию пароли частично скрываются. Если установить флажок *Показать пароль*, пароли будут показаны в открытом виде.

Имя нового пользователя не должно быть пустым.

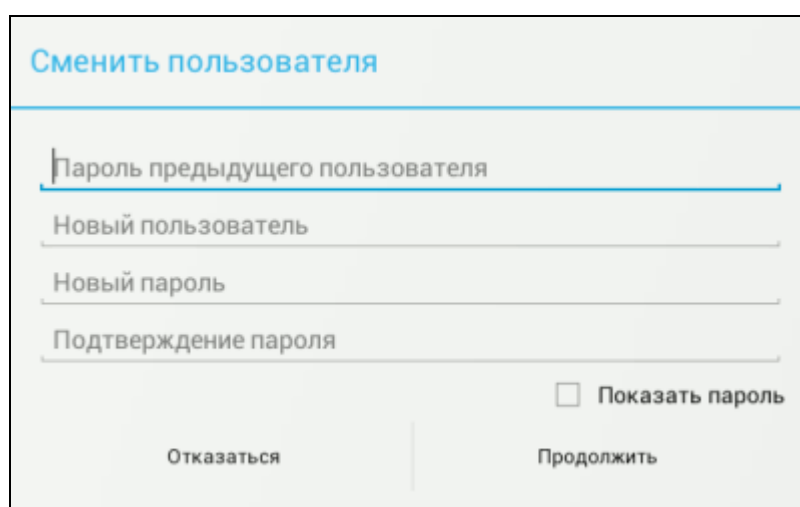


Рисунок 13

Нажмите на [Продолжить](#), чтобы выполнить попытку сменить пользователя.

В случае успеха выдается уведомление:

Пользователь успешно сменен.

Либо, если перед успешной сменой пользователя был задан автоматический логин, то режим автоматического логина отключается и выдается сообщение:

Пользователь успешно сменен. Автоматический логин отключен.

Автоматический логин

Установить автоматический режим логина можно при помощи флажка *Автоматический логин*, доступного в соответствующем пункте меню (Рисунок 11). Флажок по умолчанию сброшен.

После установки флажка появляется окно (Рисунок 14), в котором надо ввести пароль текущего пользователя.

По умолчанию пароль частично скрывается. Если установить флажок *Показать пароль*, то пароль будет показан в открытом виде.

Рисунок 14

При сбросе флажка *Автоматический логин*, необходимо подтвердить использование интерактивного логина (Рисунок 15).

Рисунок 15

Примечание: режим автоматического логина отключается при смене пользователя и при изменении пароля.

Автоблокировка

Включенный режим автоблокировки позволяет автоматически останавливать службы IKE/IPsec после перехода устройства в неинтерактивный (спящий) режим по истечении заранее установленного времени.

Настройки автоблокировки вызывается при выборе пункта меню *Автоблокировка* главной формы.

Для включения автоблокировки нужно выставить флажок *Включить* и ввести время ожидания в секундах (время между переходом устройства в неинтерактивный режим и активацией автоблокировки) (Рисунок 16).

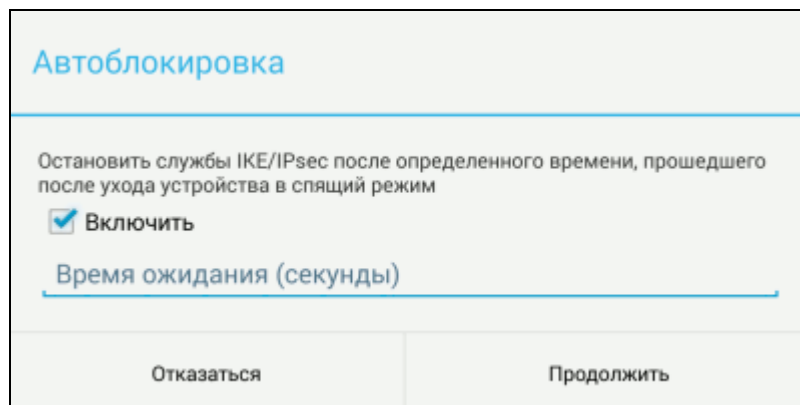


Рисунок 16

Время ожидания должно быть больше или равно 0. Если время ожидания равно 0, то активация автоблокировки происходит сразу после перехода в неинтерактивный режим.

При активации автоблокировки:

- выполняется остановка служб IKE/IPsec;
- пользователю выдается уведомление: "Активирована автоблокировка";
- если нажать на уведомление, происходит вызов графического интерфейса продукта, уведомление при этом удаляется.

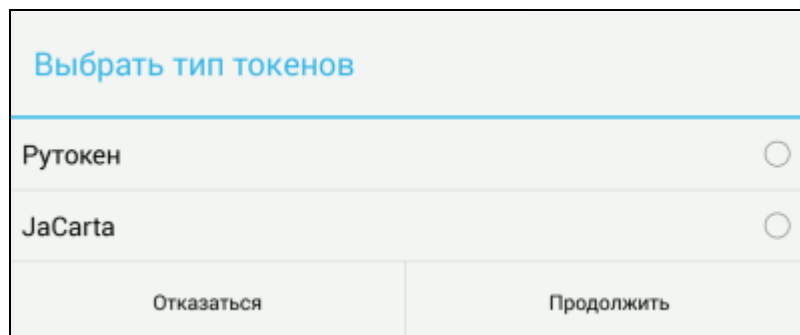
Если после перехода в неинтерактивный режим, но до истечения времени ожидания, устройство перешло в интерактивный режим, никаких специальных действий не делается.

Выбрать тип токенов

Вы можете выполнить эту настройку как до запуска служб IKE/IPsec, так и позже.

Предлагается два провайдера для выбора (Рисунок 17). При нажатии на кнопку [Продолжить](#), СКЗИ будет соответствующим образом настроено. Новая конфигурация СКЗИ будет активирована при старте служб IKE/IPsec.

Если на момент выбора провайдера были запущены службы IKE/IPsec, произойдет перезапуск этих служб с последующей процедурой логина.



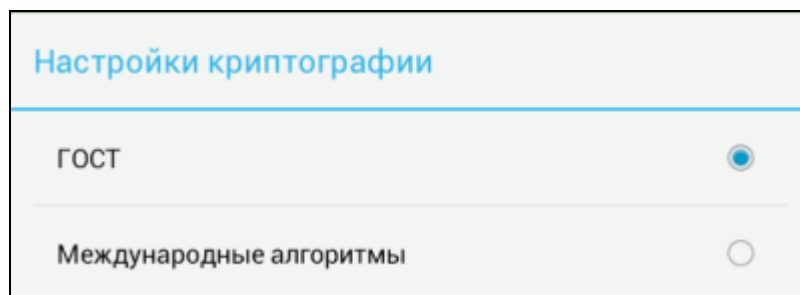
Выбрать тип токенов	
Рутокен	☐
JaCarta	☐
Отказаться	Продолжить

Рисунок 17

Настройка криптографии

Вы можете настроить криптографию как до запуска служб IKE/IPsec, так и позже.

«Программный комплекс С-Терра Клиент-М» может работать, используя либо российские криптографические алгоритмы (ГОСТ), либо международные криптографические алгоритмы (Рисунок 18). По умолчанию используются алгоритмы ГОСТ. Этот пункт меню будет также доступен в разделах «Создать конфигурацию» и «Сертификаты».



Настройки криптографии	
ГОСТ	☒
Международные алгоритмы	☐

Рисунок 18

7.2.2. Элементы интерфейса главной формы

Службы IKE/IPsec – установка или сброс флажка запускает или останавливает службу VPN. При этом будет показано состояние службы.

Если служба включена, то возможны следующие состояния:

- *защищенное соединение установлено,*
- *не соединен,*
- *не сконфигурирован,*
- *сетевая защита отключена.*

Если служба остановлена, то будет выведена соответствующая надпись – *Служба IKE/IPsec остановлена*. После остановки служб все защищенные соединения закрываются. Продукт «С-Терра Клиент-М» деактивируется до следующего старта служб IKE/IPsec. Реальная работа продукта «С-Терра Клиент-М» возможна только после запуска служб IKE/IPsec. Если нужно принудительно удалить защищенное соединение рекомендуется останавливать службы IKE/IPsec. Остановка службы требует подтверждения (Рисунок 19).

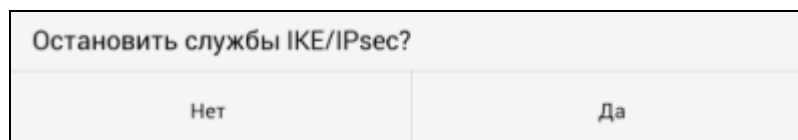


Рисунок 19

Подробное состояние служб IKE/IPsec отражено в Приложении, в разделе [«Состояние служб IKE/IPsec»](#).

Показать информацию о соединениях – раздел содержит информацию о текущих ISAKMP и IPsec сессиях. Для получения подробной информации, нужно установить соответствующий флажок.

Конфигурация IKE/IPsec – в этом разделе задается (редактируется) локальная политика безопасности.

Сертификаты – раздел, в котором можно управлять сертификатами.

Задать общий ключ (preshared key) – раздел, в котором задается общий ключ.

Настройки протоколирования – раздел для настройки протоколирования событий.

О приложении – раздел, в котором содержится информация о Продукте.

Далее рассмотрим более подробно отдельные разделы настроек.

7.3. Конфигурация IKE/IPsec

В разделе **Конфигурация IKE/IPsec** можно создать, посмотреть или отредактировать текущую локальную политику безопасности (конфигурацию), либо вообще отключить сетевую защиту.

Пункт меню *Политика по умолчанию* доступен только в приложениях, подписанных производителем устройств Samsung и YotaPhone. В остальных приложениях этот пункт меню не показывается, для них установлена политика по умолчанию – пропускать все.

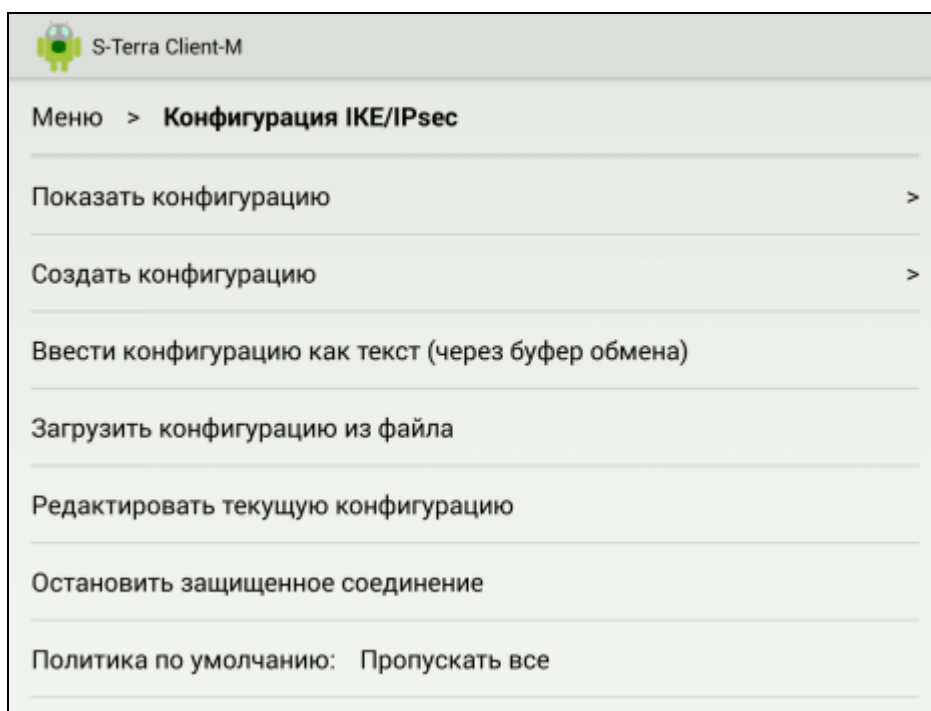


Рисунок 20

Создать локальную политику безопасности можно несколькими способами:

- используя графический интерфейс – пункт меню *Создать конфигурацию*.
- подготовить конфигурацию в текстовом виде и ввести:
 - через буфер обмена – пункт меню *Ввести конфигурацию как текст (через буфер обмена)*,
 - загрузить из файл – пункт меню *Загрузить конфигурацию из файла*.

Настройка «С-Терра Клиент-М» с использованием конфигурационного файла описана в соответствующем разделе [Приложения](#).

Внести исправления в локальную политику безопасности можно, используя графический интерфейс – пункт меню *Создать конфигурацию*, либо редактируя текстовый файл – *Редактировать текущую конфигурацию*.

Опишем действия, которые будут выполняться при выборе отдельных элементов интерфейса данного раздела.

7.3.1. Показать конфигурацию

В текстовом поле отображается текущая локальная политика безопасности. Поле не редактируется.



```

S-Terra Client-M

Меню > Конфигурация IKE/IPsec > Показать

Текущая конфигурация: сгенерирована S-Terra Client-M

#=====
# user-configurable parameters
#=====

# Security gateway address
const SGW_IP = 10.0.1.2

# Remote subnet addresses
const REMOTE_SUBNETS = 192.168.1.0/24

# CRL processing options
const CRL_HANDLING_MODE = BEST_EFFORT

# IKE phase1 options
# values: NORMAL, AGGRESSIVE
const IKE_RULE = NORMAL

# IKE transform set
# values: IKE-GOST-VKO, IKE-AES-SHA1-MODP1024, IKE-AES-SHA1-MODP1536
# IKE-DES3-SHA1-MODP1024, IKE-DES3-MD5-MODP1024
const IKE_TRANSFORMS = IKE-GOST-VKO

# IKE PFS groups
# values: MODP_1024, MODP_1536, VKO_1B, NO_PFS
const PFS_GROUP = VKO_1B

# IKE key lifetime in seconds
const IKE_KEY_LIFETIME = 86400

# Authentication mode.
# values: PRESHARED_KEY, RSA, CERTIFICATE, GOST_CERTIFICATE
# NOTE: GOST_CERTIFICATE requires IKE_TRANSFORMS = IKE-GOST-VKO
const IKE_AUTH = GOST_CERTIFICATE

# IKE ID for preshared key authentication
const PSK_AUTH_ID = ""

# ESP transform set
# values: ESP-DES3-SHA1, ESP-AES-SHA1, ESP-GOST-MAC, ESP-GOST-HMAC,
# ESP-DES3-MD5, ESP-GOST-4M-IMIT
const ESP_TRANSFORMS = ESP-GOST-4M-IMIT

# ESP key lifetime in seconds
const ESP_KEY_LIFETIME = 3600

#=====
# end of user-configurable parameters
#=====

GlobalParameters(
  Title      = "Common LSP for Android Client rev.1"
  Version    = LSP_4_1
  CRLHandlingMode = CRL_HANDLING_MODE
)

IKEParameters(
  LocalPort=0
  NATTLocalPort=0
)

IKETransform IKE-DES3-MD5-MODP1024(
  CipherAlg = "DES3-CBC"
  HashAlg   = "MD5"
  GroupID   = MODP_1024
  LifetimeSeconds = IKE_KEY_LIFETIME
)

```

Рисунок 21

7.3.2. Создать конфигурацию

В данном разделе можно создать или отредактировать локальную политику безопасности, используя графический интерфейс. Можно очистить конфигурацию, воспользовавшись меню в правом верхнем углу (Рисунок 22).

The screenshot shows the 'S-Terra Client-M' application window. The title bar includes the application icon and name. The breadcrumb navigation at the top reads 'Меню > Конфигурация IKE/IPsec > Создать'. The main configuration area is divided into several sections:

- Защищенный шлюз:** A text input field containing 'xxx.xxx.xxx.xxx'.
- Защищаемые подсети:** A text input field containing 'xxx.xxx.xxx.xxx/nn'.
- Параметры IKE phase1**
 - Набор преобразований:** A dropdown menu showing 'ГОСТ VKO'.
 - Параметры обмена:** A dropdown menu showing 'Main'.
 - Режим аутентификации:** A dropdown menu showing 'Сертификат ГОСТ'.
 - IKE ID для аутентификации на общем ключе:** An empty text input field.
 - Ввести IKE ID как текст:** A checked checkbox.
 - Время жизни ключа в секундах:** A text input field containing '86400'.
- Параметры IKE phase2 / IPsec**
 - Группа PFS:** A dropdown menu showing 'VKO_1B'.
 - Набор преобразований:** A dropdown menu showing 'ГОСТ MAC'.
 - Время жизни ключа в секундах:** A text input field containing '3600'.
- Разное**
 - Проверка списков отозванных сертификатов:** A dropdown menu showing 'По возможности'.
- Пакетный фильтр**
 - Режим фильтрации:** A dropdown menu showing 'Стандартный'.

At the bottom of the form is a button labeled 'Применить конфигурацию'.

Рисунок 22

Предлагаемые значения некоторых параметров будут зависеть от того, [какая криптография выбрана](#): российские криптографические алгоритмы или международные.

Защищенный шлюз – задается адрес шлюза, защищающего подсеть, с которой строится защищенное соединение.

Защищаемые подсети – указываются адреса подсетей, к которым необходим удаленный доступ. Вводятся через запятую, с указанием маски подсети. Например:

192.168.101.10, 192.168.102.0/24

Параметры IKE phase1

В этой области задаются параметры для первой фазы IKE.

Набор преобразований – параметры создаваемого защищенного канала, которые будут предложены партнеру для согласования.

Если была выбрана криптография ГОСТ, то предлагается вариант:

- *ГОСТ VKO* – состоит из двух наборов преобразований:
 - алгоритм шифрования – ГОСТ 28147-89 в режиме CBC, алгоритм хэширования – ГОСТ Р 34.11-94, алгоритм для выработки ключевого материала – VKO ГОСТ Р 34.10-2001 (длина ключа 256 бит);
 - алгоритм шифрования – ГОСТ 28147-89 в режиме CBC, алгоритм хэширования – ГОСТ Р 34.11-12, алгоритм для выработки ключевого материала – VKO ГОСТ Р 34.10-2012 (длина ключа 256 бит).

Если была выбрана криптография с использованием международных алгоритмов – предлагаются:

- *AES SHA1 MODP_1024* – используется алгоритм шифрования – AES в режиме CBC, алгоритм хэширования – SHA1, алгоритм для выработки ключевого материала – стандартная Oakley-группа с длиной ключа 1024 бит.
- *AES SHA1 MODP_1536* – используется алгоритм шифрования – AES в режиме CBC, алгоритм хэширования – SHA1, алгоритм для выработки ключевого материала – стандартная Oakley-группа с длиной ключа 1536 бит.
- *DES3 SHA1 MODP_1024* – используется алгоритм шифрования – DES3 в режиме CBC, алгоритм хэширования – SHA1, алгоритм для выработки ключевого материала – стандартная Oakley-группа с длиной ключа 1024 бит.
- *DES3 MD5 MODP_1024* – используется алгоритм шифрования – DES3 в режиме CBC, алгоритм хэширования – MD5, алгоритм для выработки ключевого материала – стандартная Oakley-группа с длиной ключа 1024 бит.

Параметры обмена – режим обмена информацией. Возможно одно из двух значений:

- *Main* – в этом режиме партнеру высылаются все IKE политики для выбора и согласования. Значение по умолчанию.
- *Aggressive* – в этом режиме партнеру высылается только первая IKE политика из списка, имеющая самый высокий приоритет.

Режим аутентификации

Аутентификация пользователя при создании защищенного соединения может осуществляться при помощи сертификата открытого ключа или [общего ключа \(preshared key\)](#).

Если используется криптография ГОСТ, то предлагается выбрать:

- *Сертификат ГОСТ* – аутентификация с использованием сертификата. Значение по умолчанию.
- *Общий ключ* – аутентификация с использованием общего ключа.

Если была выбрана криптография с использованием международных алгоритмов, то предлагаются:

- *Сертификат RSA* – аутентификация с использованием сертификата. Значение по умолчанию.
- *Общий ключ* – аутентификация с использованием общего ключа.

IKE ID для аутентификации на общем ключе – задается идентификатор ключа, который будет пересылаться партнеру по соединению (строка, содержащая шестнадцатеричное представление идентификатора ключа). Поле доступно, если выбран режим аутентификации *Общий ключ*.

Ввести IKE ID как текст – при установке этого флажка идентификатор ключа вводится как текст, который затем будет преобразован в шестнадцатеричное представление. Поле доступно, если выбран режим аутентификации *Общий ключ*.

Время жизни ключа в секундах – время существования ISAKMP SA. Значение по умолчанию – 86400.

Параметры IKE phase2 / IPsec

В этой области задаются параметры для второй фазы IKE.

Группа PFS – указываются параметры выработки ключевого материала, высылаемые партнеру для согласования при создании SA (Security Association), если используется опция PFS (perfect forward secrecy).

Если была выбрана криптография ГОСТ, предлагаются:

- *VKO_1B* – при согласовании новой SA выполняется новый обмен ключами по алгоритму VKO ГОСТ Р 34.10-2001 [RFC4357] (длина ключа 256 бит). Это значение используется по умолчанию.
- *VKO2_1B* – при согласовании новой SA выполняется новый обмен ключами по алгоритму VKO ГОСТ Р 34.10-2012 (длина ключа 256 бит).
- *NO_PFS* – опция PFS не используется, в этом случае ключевой материал заимствуется из первой фазы IKE.

Если была выбрана криптография с использованием международных алгоритмов – предлагается следующий список:

- *MODP_1024* – при согласовании новой SA выполняется новый обмен ключами по алгоритму Диффи-Хеллмана (1024-битовый вариант).
- *MODP_1536* – при согласовании новой SA выполняется новый обмен ключами по алгоритму Диффи-Хеллмана (1536-битовый вариант).
- *NO_PFS* – опция PFS не используется, в этом случае ключевой материал заимствуется из первой фазы IKE.

Набор преобразований – задается политика IPsec защиты в виде набора преобразований.

Если была выбрана криптография ГОСТ, предлагается список:

- *ГОСТ MAC* – алгоритм шифрования ГОСТ 28147-89 (в режиме простой замены с зацеплением), алгоритм проверки целостности ГОСТ 28147-89 (в режиме выработки имитовставки). Значение по умолчанию.
- *ГОСТ HMAC* – алгоритм шифрования ГОСТ 28147-89 (в режиме простой замены с зацеплением), алгоритм проверки целостности ГОСТ Р 34.11-94.

- *ESP_GOST-4M-IMIT* – алгоритм ESP_GOST-4M-IMIT самостоятельно обеспечивает как защиту конфиденциальности (шифрование), так и контроль целостности данных (имитозащиту).

Если была выбрана криптография с использованием международных алгоритмов, то предлагается следующий список:

- *DES3 SHA1* – алгоритм шифрования DES3, алгоритм проверки целостности SHA1.
- *AES SHA1* – алгоритм шифрования AES, алгоритм проверки целостности SHA1.
- *DES3 MD5* – алгоритм шифрования DES3, алгоритм проверки целостности MD5.

Время жизни ключа в секундах – задается время, в течение которого IPsec SA будет существовать. Значение по умолчанию – 3600.

Разное

В этой области задаются дополнительные настройки.

Проверка списков отозванных сертификатов – задается режим проверки списков отозванных сертификатов (CRL). Возможные значения:

- *По возможности* – список отозванных сертификатов используется при проверке сертификата только в том случае, если он является действующим. Этот режим отличается от режима *Необязательна* тем, что CRL может быть получен посредством протокола LDAP (если он настроен). Это значение используется по умолчанию.
- *Отключена* – при проверке сертификата список отозванных сертификатов не обрабатывается.
- *Необязательна* – список отозванных сертификатов используется только в случае, если он был предустановлен или получен (и обработан) в процессе IKE обмена и является действующим.
- *Включена* – для успешной проверки сертификата обрабатывается список отозванных сертификатов.

Пакетный фильтр

В этой области задаются настройки межсетевого экрана. Настройка этих параметров доступна только в приложениях, подписанных производителем устройств Samsung и YotaPhone. В остальных приложениях этот пункт меню не показывается, для них установлен пакетный фильтр – разрешающий.

Режим фильтрации – предлагается выбрать режим фильтрации трафика. Возможные значения:

- *Стандартный* – запретить прохождение открытого трафика в защищенную подсеть (подсети) и из защищенной подсети (подсетей). Это значение используется по умолчанию.
- *Макс. защита* – запретить прохождение любого открытого трафика.
- *Разрешающий* – разрешить прохождение любого открытого трафика.

Применить конфигурацию – при нажатии на кнопку конфигурация становится активной.

7.3.3. Ввести конфигурацию как текст

При выборе этого пункта меню появляется текстовое поле для ввода локальной политики безопасности из буфера обмена.

The image shows a screenshot of a software interface. At the top, there is a header bar with the text "Введите LSP:" in blue. Below this is a large, empty rectangular area for text input. At the bottom of the interface, there is a horizontal bar containing three buttons: "Отказаться" (Refuse), "Сохранить" (Save), and "Применить" (Apply).

Рисунок 23

Введенную конфигурацию можно сохранить в текстовом файле или сразу применить (загрузить в базу Продукта).

7.3.4. Загрузить конфигурацию из файла

При выборе этого пункта меню предлагается выбрать файл с конфигурацией. Файл с конфигурацией должен быть предварительно размещен в папке S-Terra, вложенной в [Android External Storage Directory](#).

Конфигурация из файла будет загружена в текстовое поле, где ее можно отредактировать, а затем сохранить в текстовом файле или применить.

7.3.5. Редактировать текущую конфигурацию

При выборе этого пункта меню выводится текстовое поле с локальной политикой безопасности (Рисунок 24).

Текущую конфигурацию можно отредактировать и сохранить в текстовом файле или сразу применить.

Введите LSP:

```

# CRL processing options
const CRL_HANDLING_MODE = BEST_EFFORT

# IKE phase1 options
# values: NORMAL, AGGRESSIVE
const IKE_RULE = NORMAL

# IKE transform set
# values: IKE-GOST-VKO, IKE-AES-SHA1-MODP1024, IKE-AES-SHA1-MODP1536
#         IKE-DES3-SHA1-MODP1024, IKE-DES3-MD5-MODP1024, IKE-GOST2012-VKO2
const IKE_TRANSFORMS = IKE-GOST-VKO, IKE-GOST2012-VKO2

# IKE PFS groups
# values: MODP_1024, MODP_1536, VKO_1B, VKO2_1B, NO_PFS
const PFS_GROUP = VKO_1B

# IKE key lifetime in seconds
const IKE_KEY_LIFETIME = 86400

# Authentication mode.
# values: PRESHARED_KEY, RSA_CERTIFICATE, GOST_CERTIFICATE
# NOTE: GOST_CERTIFICATE requires IKE_TRANSFORMS = IKE-GOST-VKO
const IKE_AUTH = GOST_CERTIFICATE

# IKE ID for preshared key authentication
const PSK_AUTH_ID = ""

# ESP transform set
# values: ESP-DES3-SHA1, ESP-AES-SHA1, ESP-GOST-MAC, ESP-GOST-HMAC,
#         ESP-DES3-MD5, ESP_GOST-4M-IMIT
const ESP_TRANSFORMS = ESP_GOST-4M-IMIT

# ESP key lifetime in seconds
const ESP_KEY_LIFETIME = 3600

# Firewall options
# values: FW_PASS, FW_DROP, FW_NO_IPSEC_BYPASS
const FIREWALL_POLICY = FW_NO_IPSEC_BYPASS

#=====
# end of user-configurable parameters
#=====

GlobalParameters(
  Title      = "Common LSP for Android Client rev.1"
  Version    = LSP_4_1
  CRLHandlingMode = CRL_HANDLING_MODE
)

IKEParameters(
  LocalPort=0

```

Отказаться
Сохранить
Применить

Рисунок 24

7.3.6. Остановить защищенное соединение

При выборе этого пункта меню устанавливается политика безопасности по умолчанию.

Службы IKE/IPsec будут работать только в режиме диагностики и настройки.

Остановка защищенного соединения требует подтверждения (Рисунок 25).

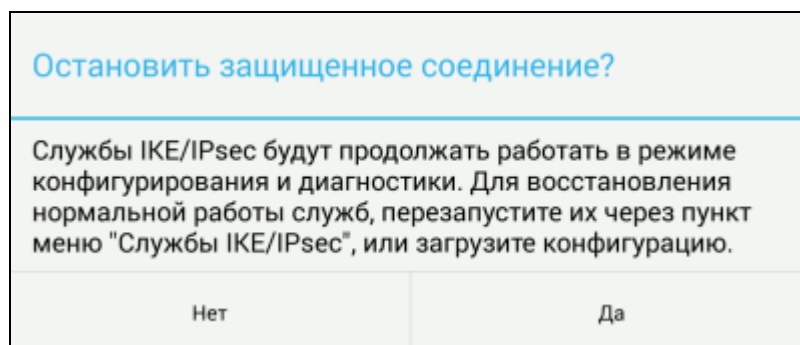


Рисунок 25

Для восстановления нормальной работы служб, перезапустите или загрузите конфигурацию.

7.3.7. Политика по умолчанию

Выбор этого пункта меню вызывает окно (Рисунок 26), в котором предлагается выбрать политику безопасности по умолчанию.

Пункт меню *Политика по умолчанию* доступен только в приложениях, подписанных производителем устройств Samsung и YotaPhone. В остальных приложениях этот пункт меню не показывается, для них установлена политика по умолчанию – пропускать все.

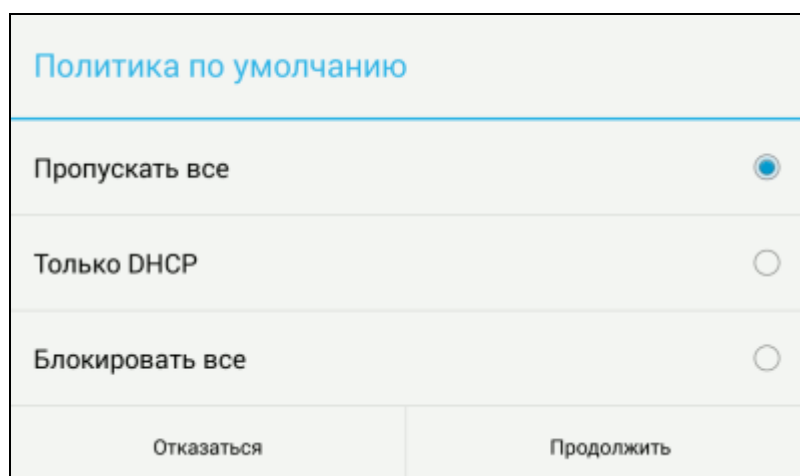


Рисунок 26

Политика по умолчанию действует в следующие моменты:

- Активируется в процессе автостарта.
- Работает до старта служб IKE/IPsec и логина.
- Работает после логина, если отсутствует LSP в базе локальных настроек.
- Активируется после выбора *Конфигурация IKE/IPsec → Остановить защищенное соединение*.
- Активируется после остановки служб IKE/IPsec.

Возможны следующие варианты политики по умолчанию:

- Пропускать все – пропускать все пакеты. Вариант по умолчанию.
- Только DHCP – пропускать пакеты только по протоколу DHCP.
- Блокировать все – не пропускать трафик.

7.4. Сертификаты

В разделе **Сертификаты** задаются локальный сертификат и CA сертификат, сертификаты партнеров, список отозванных сертификатов (CRL). Также в этом разделе можно создать запрос на получение локального сертификата, посмотреть сертификаты, находящиеся в базе Продукта и удалить сертификаты.

Примечание: в случае, если импортируемый сертификат находится в файле, этот файл должен быть предварительно размещен в папке S-Terra, вложенной в [Android External Storage Directory](#).

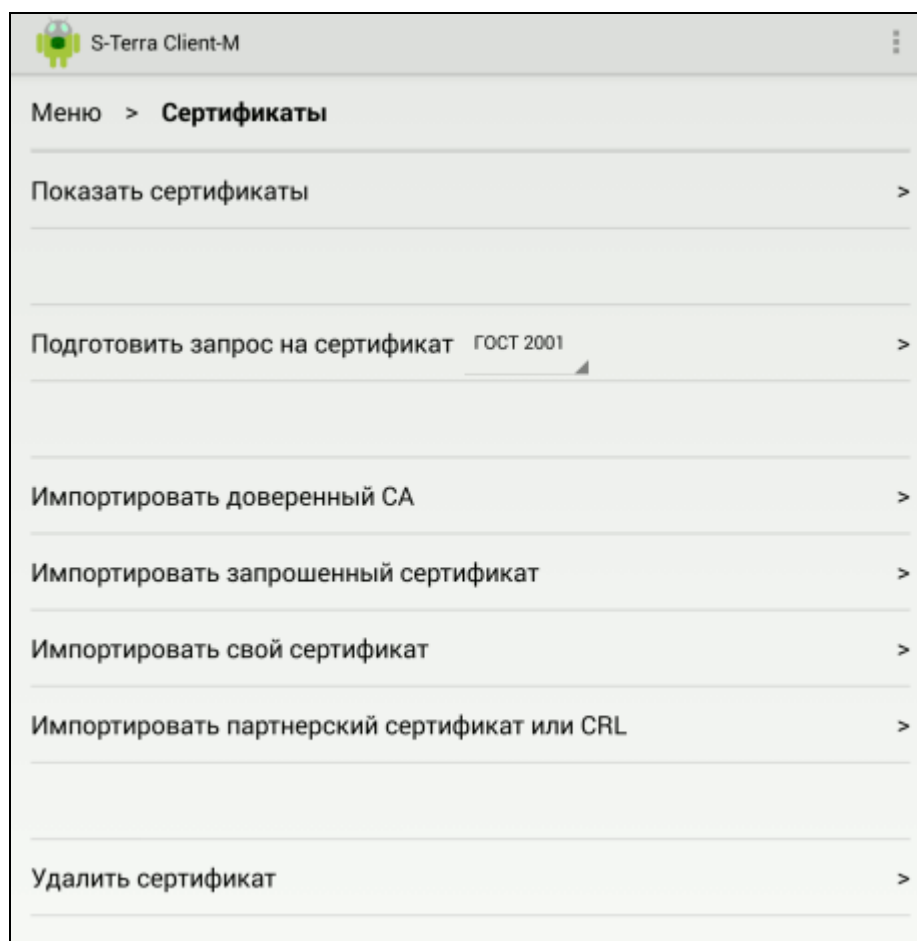


Рисунок 27

Показать сертификаты – выводится информация о сертификатах, находящихся в базе Продукта.

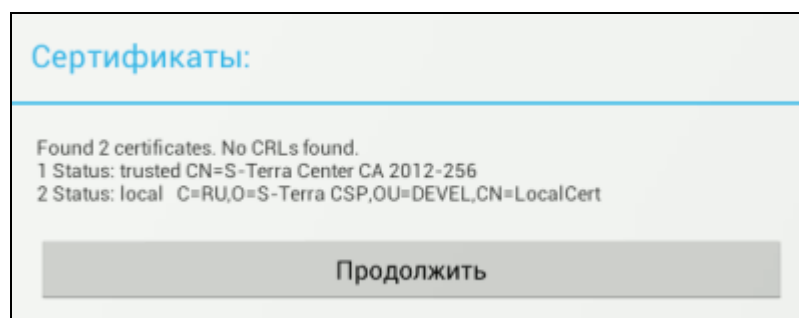


Рисунок 28

Подготовить запрос на сертификат ГОСТ (2001/2012)/RSA – В зависимости от того [какая криптография выбрана](#), будет подготовлен запрос либо ГОСТ сертификата (предлагается для выбора ГОСТ 2001 и ГОСТ 2012), либо RSA сертификата.

При выборе этого пункта появляется окно (Рисунок 29) в котором необходимо ввести значение поля Subject Name сертификата (применяется для подготовки запроса на сертификат).

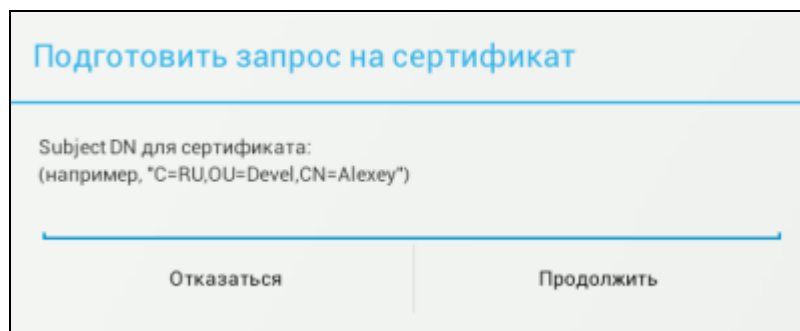


Рисунок 29

Затем инициализируется генератор случайных чисел, создается контейнер с ключевой парой и формируется запрос на сертификат пользователя. После выполнения этих действий, на экране появляется окно, в котором можно выбрать способ сохранения запроса на сертификат (Рисунок 30).

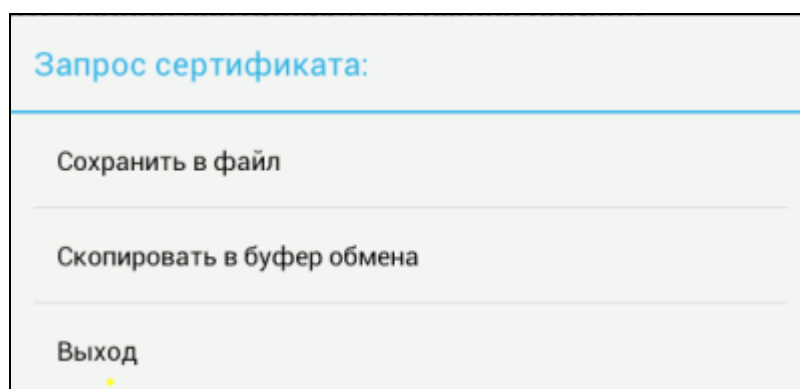


Рисунок 30

Эти же пункты (*Сохранить в файл*, *Скопировать в буфер обмена*) добавятся в раздел **Сертификаты**.

Для получения сертификата нужно отослать запрос в Удостоверяющий Центр. Как это сделать описано в Приложении, в разделе [«Получение сертификата пользователя»](#).

Импортировать доверенный СА – при выборе этого пункта появляется окно (Рисунок 31), в котором надо выбрать способ получения СА сертификата для импорта в базу данных:

- *Ввести доверенный СА как текст (через буфер обмена)* – в поле вводится текст СА сертификата из буфера обмена, для регистрации в базе Продукта.
- *Добавить доверенный СА из файла* – предлагается выбрать файл, содержащий СА сертификат, для регистрации в базе Продукта.

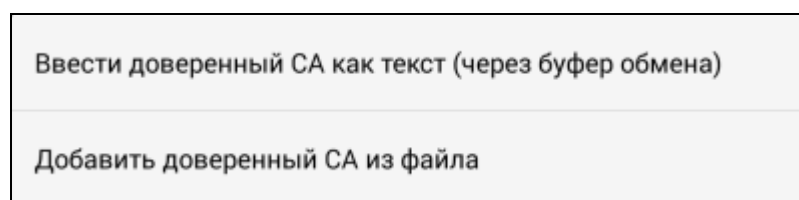


Рисунок 31

Импортировать запрошенный сертификат – выполняется импорт сертификата, полученного из Центра Сертификации. Появляется окно, аналогичное окну, описанному выше (Рисунок 31).

Буфер обмена может использоваться для сертификатов в формате Base64.

Импортировать свой сертификат – этот пункт меню позволяет импортировать свой сертификат, в случае если контейнер с закрытым ключом находится на токене.

Примечание. Программный комплекс «С-Терра Клиент-М» не позволяет создать контейнер на токене, поэтому предлагается воспользоваться сторонними средствами. В [Приложении](#) описано создание контейнера на токене с использованием утилит «Программного комплекса С-Терра Клиент».

Предварительно в меню *Главной формы* нужно выбрать [тип токенов](#). Токен должен быть подключен и доступен.

При выборе этого пункта появляется окно, подобное окну на Рисунок 31, где пользователь выбирает способ ввода своего сертификата.

Затем появляется окно, в котором предлагается указать носитель закрытого ключа (Рисунок 32). Укажите *Контейнер* и нажмите [Продолжить](#).

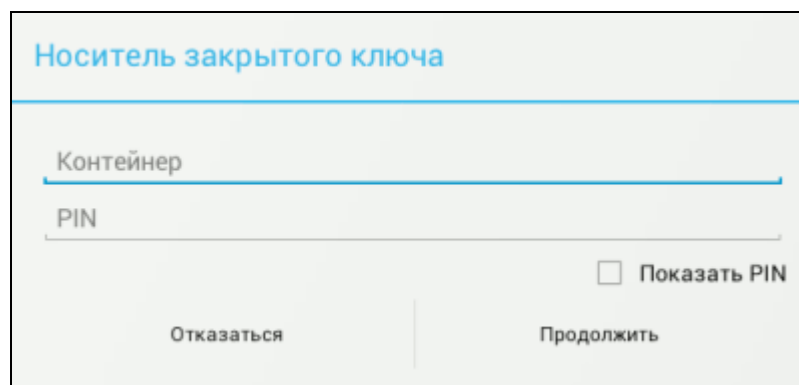


Рисунок 32

Появится список доступных контейнеров (Рисунок 33).

Выберите контейнер	
etoken_p15://rtbt_newp15	☐
etoken://rtbt_one	☐
etoken://conttoken	☒
file://vpn53a0246e	☐
ОтказатьсяПродолжить	

Рисунок 33

Выберите из списка контейнер и нажмите **Продолжить**. Выбранный контейнер отобразится в окне *Носитель закрытого ключа* (Рисунок 32). Введите PIN и нажмите **Продолжить**.

Далее появится окно (Рисунок 34), в котором надо выбрать свой сертификат.

Выберите файл с сертификатом:	
.hashes	☐
certnew(1).p7b	☐
certnew(2).cer	☐
s_terra_clientm-4.1.14703.apk	☐
s_terra_clientm_s-4.1.14689.apk	☐
s_terra_clientm_s-4.1.14703.apk	☐
service.apk	☐
ОтказатьсяПродолжить	

Рисунок 34

Выберите файл с сертификатом и нажмите **Продолжить**. В появившемся окне (Рисунок 35) отобразится Distinguished Name выбранного сертификата. Установите флажок и нажмите **Продолжить**, чтобы импортировать сертификат.

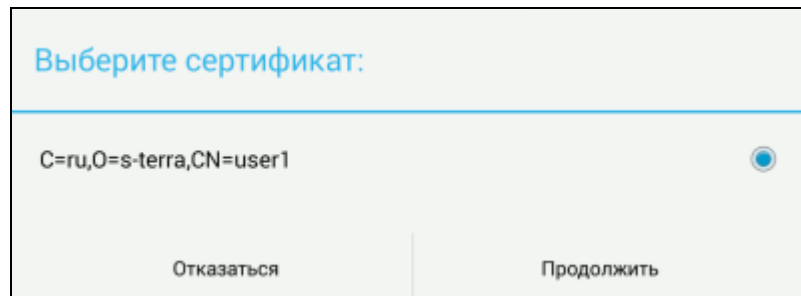


Рисунок 35

Импортировать партнерский сертификат или CRL – предлагается выбрать партнерский сертификат или CRL для регистрации в базе Продукта. Появляется окно, подобное окну на Рисунок 31, в котором предлагается выбрать способ получения сертификата.

Удалить сертификат – в появившемся окне предлагается список сертификатов, которые можно пометить для удаления.

7.5. Задать общий ключ (preshared key)

Альтернативным способом аутентификации при помощи сертификатов является аутентификация с использованием общего ключа (preshared key), но этот способ рекомендуется использовать только в целях тестирования.

В разделе **Задать общий ключ (preshared key)** задается общий ключ.

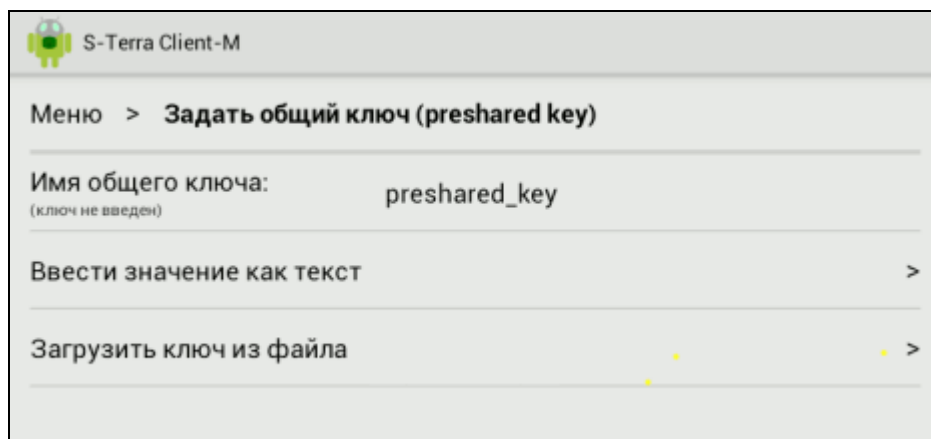


Рисунок 36

Имя общего ключа – *preshared_key* (имя ключа задано и не может изменяться). Подсвечивается состояние ключа – введен/не введен.

Ввести значение как текст – при выборе данного пункта появится поле для ввода значения общего ключа.

Загрузить ключ из файла – предлагается выбрать файл с общим ключом. Файл, содержащий общий ключ, должен быть предварительно размещен в папке S-Terra, вложенной в [Android External Storage Directory](#).

7.6. Настройки протоколирования

В разделе **Настройки протоколирования** можно задать протоколирование событий по протоколу Syslog и указать адрес сервера, куда будут отправляться эти сообщения.

Уровень важности (Severity) протоколируемых событий соответствует уровню debug.

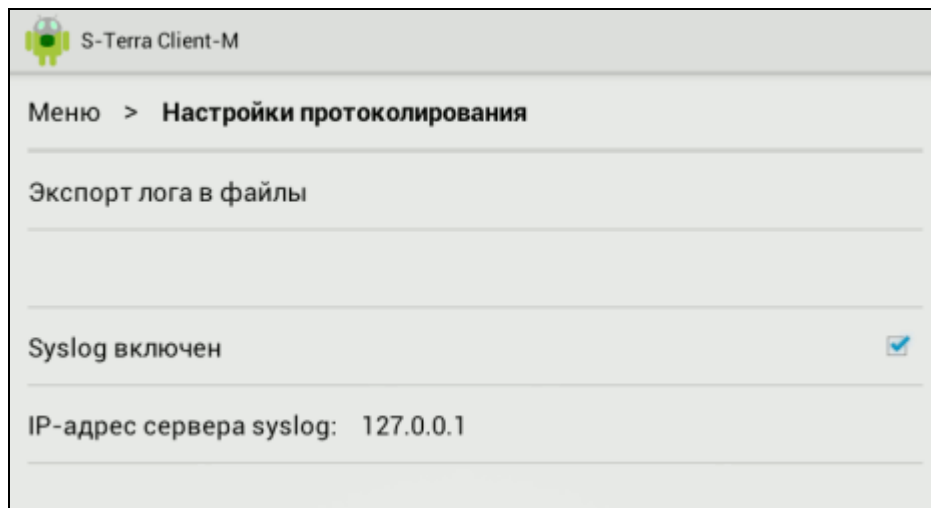


Рисунок 37

Экспорт лога в файлы – при выборе этого пункта, журнал протоколирования будет сохранен в папке S-Terra, вложенной в [Android External Storage Directory](#).

Syslog включен/выключен – флажок установлен – протоколирование ведется, если флажок сброшен, то протоколирование не ведется. По умолчанию протоколирование событий ведется.

IP-адрес сервера syslog – указывается IP-адрес сервера, на который будут посылаться сообщения о протоколируемых событиях. Значение по умолчанию – 127.0.0.1.

8. Деинсталляция «Программного комплекса С-Терра Клиент-М»

Перед деинсталляцией «С-Терра Клиент-М» необходимо остановить службу VPN. Для этого войдите в «С-Терра Клиент-М» и сбросьте флажок **Службы IKE/IPsec**.



Невыполнение этого действия может привести к проблемам при работе с сетевыми приложениями, а также к компрометации сетевой безопасности. В этом случае, для полного удаления компонентов Продукта из системы, необходимо перезагрузить устройство.

Деинсталляция «С-Терра Клиент-М» производится стандартными средствами операционной системы. Войдите в *Настройки*, выберите *Диспетчер приложений* → *Управление приложениями*. Выберите приложение *S-Terra Client-M* и действие *Удалить*. Для приложений, подписанных производителем устройств Samsung, удалите также криптографическую библиотеку *S-Terra Client-M*.

9. Замечания по использованию «С-Терра Клиент-М»

При создании защищенного соединения будет выдан запрос на подтверждение установления VPN-соединения (Рисунок 38).

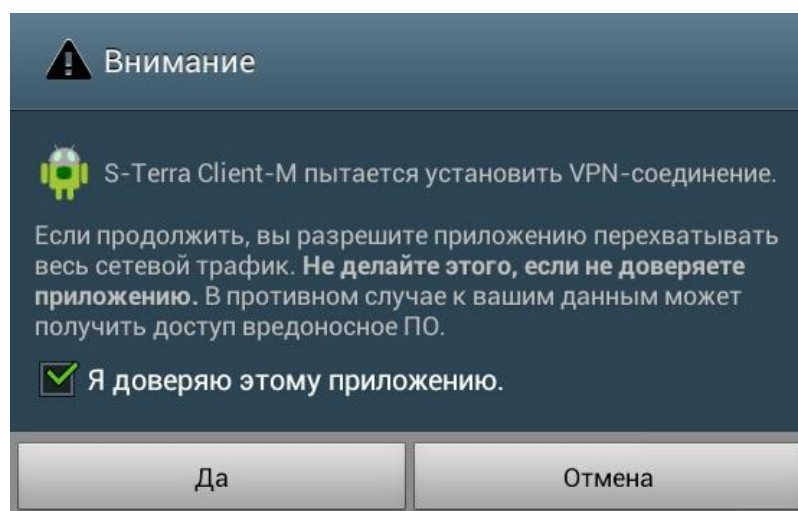


Рисунок 38

Разрешите установление VPN-соединения. В противном случае защищенное соединение не сможет установиться. После получения разрешения установить VPN-соединение, в области системных уведомлений появляется значок ключа. Следует учесть, что появление изображения ключа не гарантирует успешного установления защищенного соединения. Для диагностики надо использовать другие источники информации, например, пункт меню «Показать информацию о соединениях».

Пользовательский интерфейс Android предполагает возможность ручного разъединения VPN-соединения. Однако, такой способ удаления защищенных соединений не рекомендуется, так как он может привести к проблемам с сетевым настройками. Если нужно принудительно удалить защищенное соединение рекомендуется останавливать [службы IKE/IPsec](#).

10. Приложение

10.1. Получение сертификата пользователя и СА-сертификата

В данном разделе рассмотрим один из возможных способов получения сертификата пользователя. В нашем тестовом примере воспользуемся Удостоверяющим Центром – Microsoft Certification Authority, где в качестве криптопровайдера (CSP) используется Crypto-PRO GOST R34.10-2012 Strong Cryptographic Service Provider; Hash algorithm GOST R 34.11-12 512.

Войдите в раздел **Сертификаты** (Рисунок 39). По умолчанию установлена настройка криптографии – *ГОСТ*.

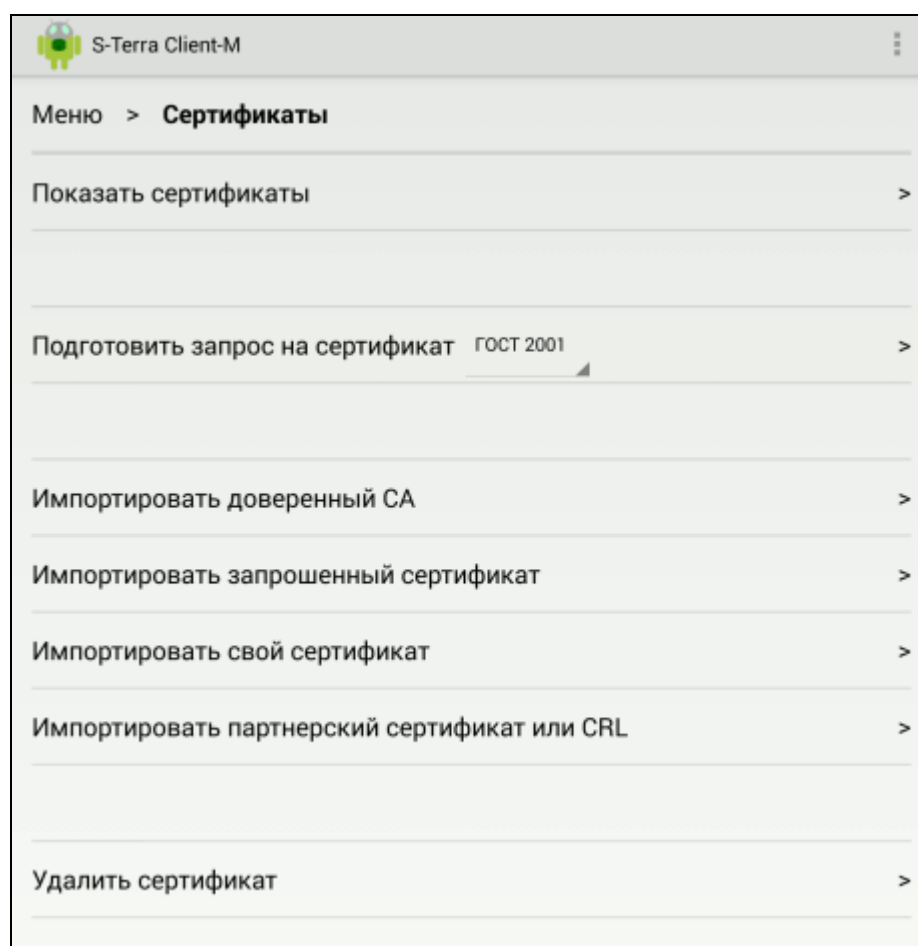


Рисунок 39

Выберите пункт меню *Подготовить запрос на сертификат* (по умолчанию установлен *ГОСТ 2001*).

Появляется окно (Рисунок 40) в котором необходимо ввести значение поля Subject Name сертификата.

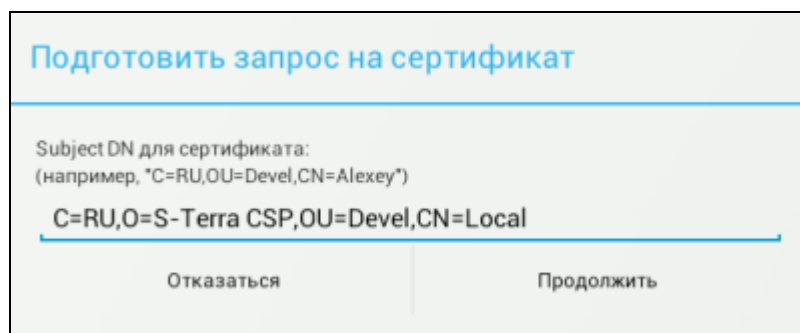


Рисунок 40

Нажмите **Продолжить**.

Инициализируется генератор случайных чисел, создается контейнер с ключевой парой и формируется запрос на сертификат пользователя.

Сохраните запрос сертификата в буфер обмена (Рисунок 41).

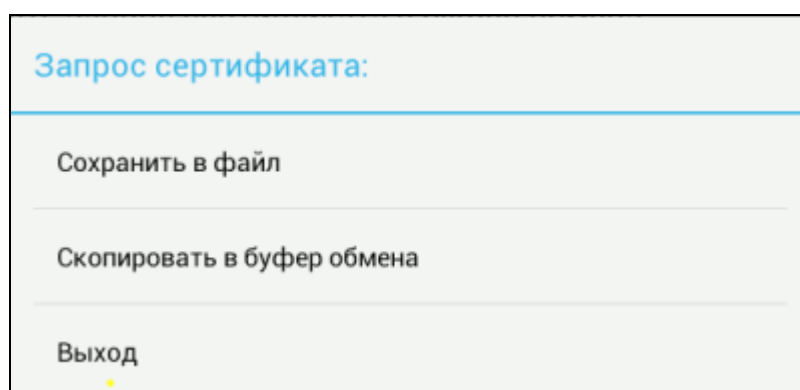


Рисунок 41

Для получения сертификата пользователя нужно отослать запрос на сертификат в Удостоверяющий Центр.

Запустите браузер, укажите IP-адрес Удостоверяющего Центра и утилиту *certsrv*. В приведенном примере адресная строка будет иметь следующий вид:

`http://10.0.251.4/certsrv.`

В появившемся окне Удостоверяющего Центра (Рисунок 42) выберите пункт меню – Request a certificate.

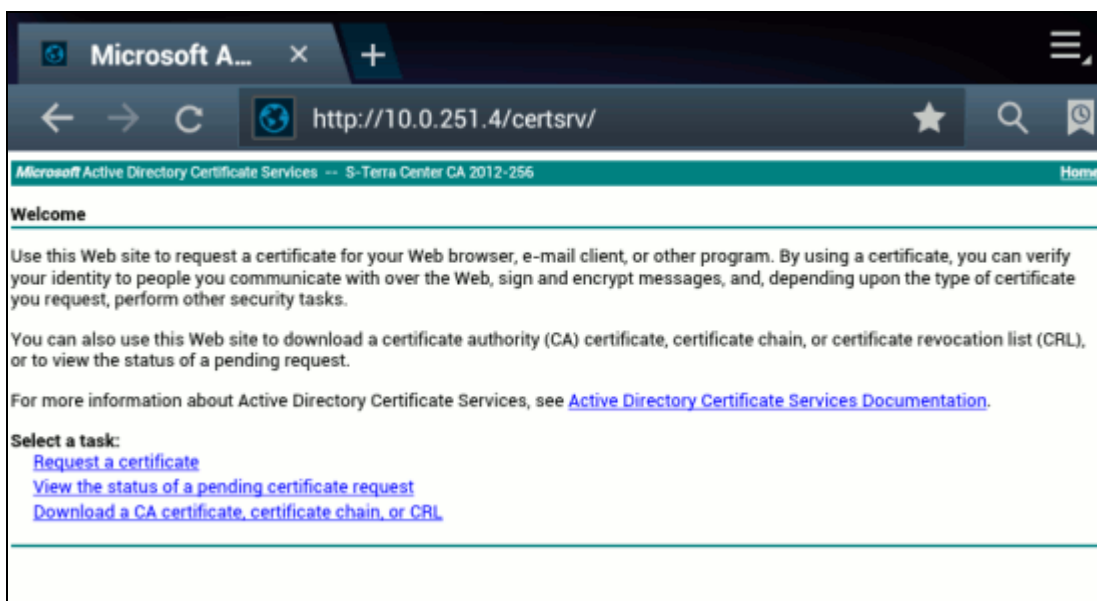


Рисунок 42

В следующем окне (Рисунок 43) выберите `advanced certificate request`.

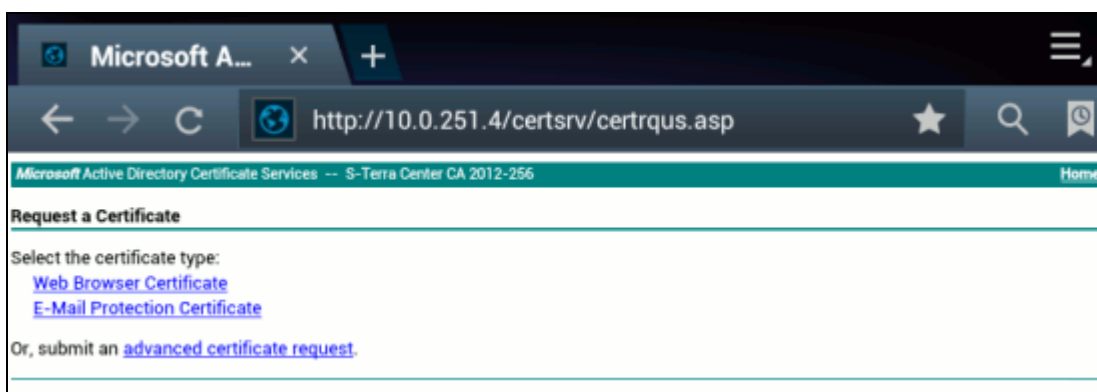


Рисунок 43

Появится окно (Рисунок 44), где в текстовое поле введите запрос на сертификат, подготовленный при помощи S-Terra Client-M в разделе [сертификаты](#), затем нажмите [Submit](#).

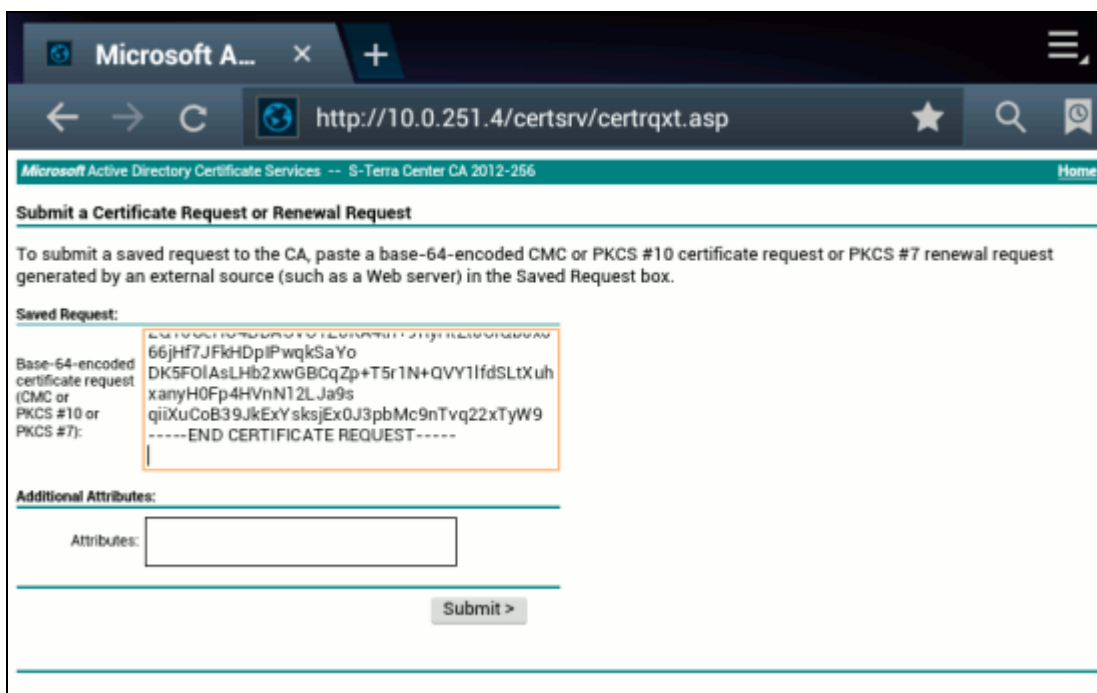


Рисунок 44

Удостоверяющий Центр издаст сертификат пользователя по полученному запросу. Выберите формат для сертификата DER-шифрование и нажмите **Download certificate chain**.

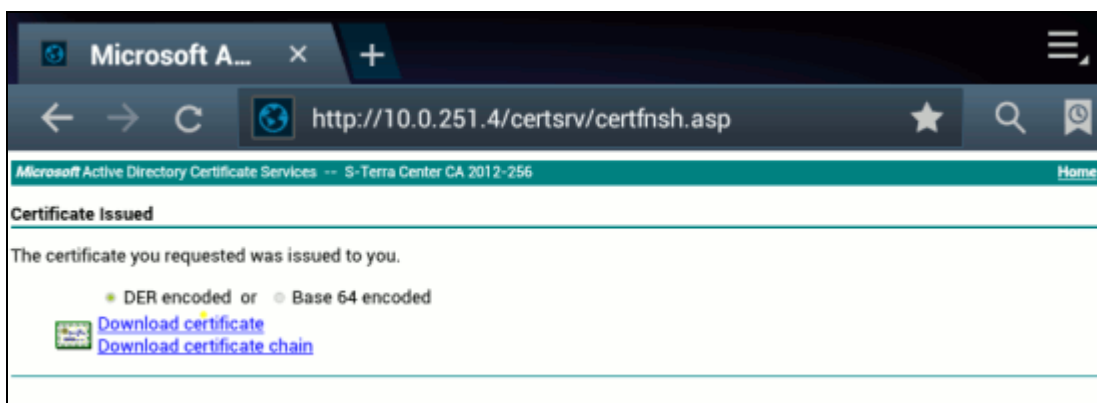


Рисунок 45

Появится окно (Рисунок 46). Выберите *S-Terra Client-M*.

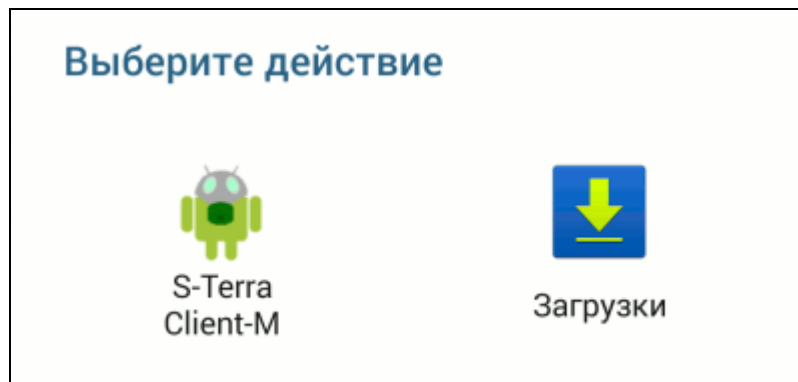


Рисунок 46

Будет предложено импортировать полученные сертификаты (Рисунок 47).

Выберите сертификат Удостоверяющего Центра и нажмите кнопку [Добавить доверенный СА](#). Затем выберите и установите свой сертификат.

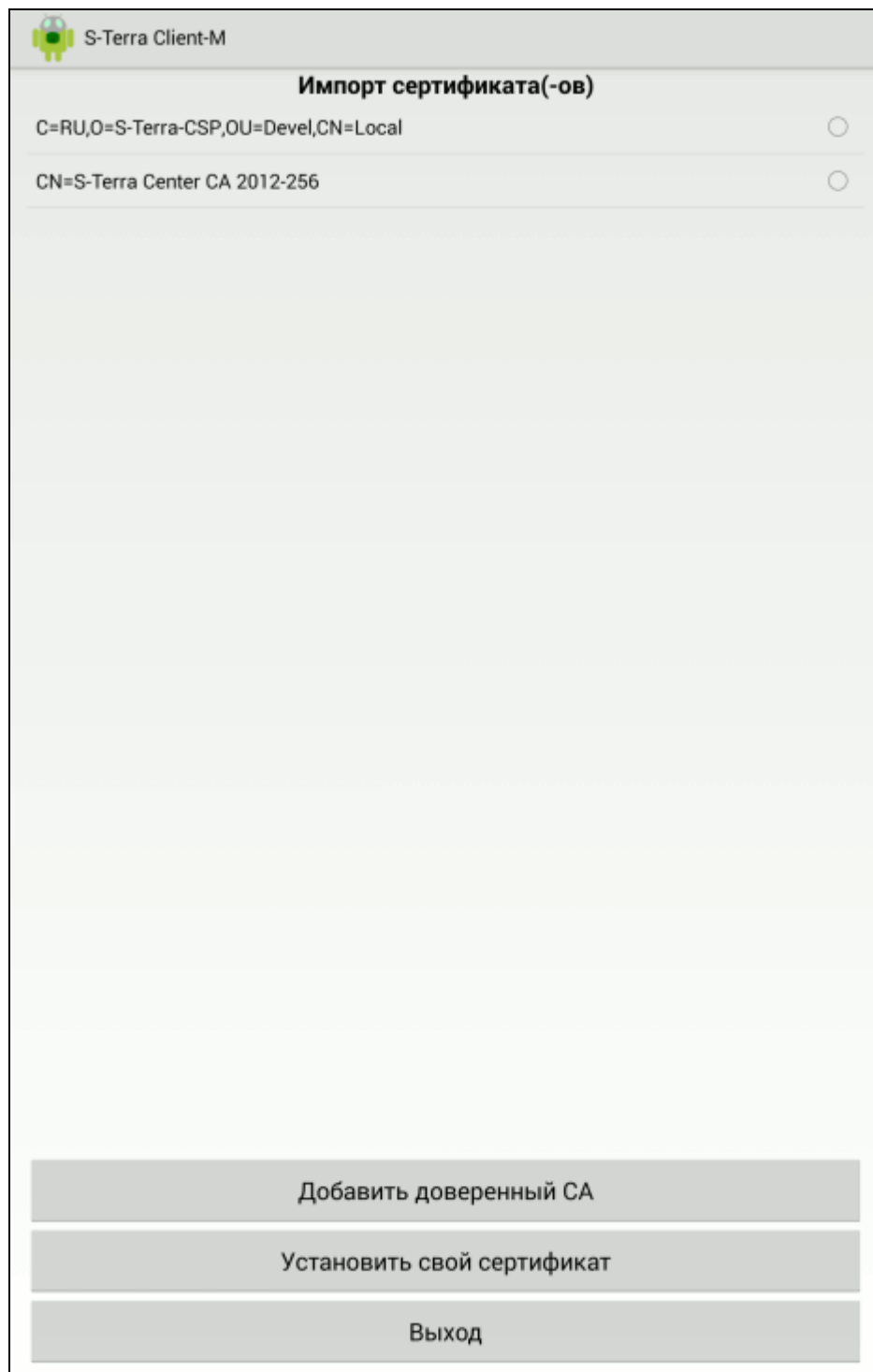


Рисунок 47

В результате выполненных действий сертификаты будут добавлены в базу Продукта.

10.2. Создание контейнера с ключевой парой на токене

«Программный комплекс С-Терра Клиент-М» не позволяет создать контейнер на токене. В данном разделе описывается создание контейнера на токене с помощью утилит «Программного комплекса С-Терра Клиент», с использованием СКЗИ, разработанного компанией S-Terra CSP.

Возможна работа с токенами следующих моделей: "JaCarta MicroSD", "Рутокен ЭЦП" (USB), "Рутокен ЭЦП Bluetooth".

На компьютере администратора должен быть установлен административный пакет продукта «Программный комплекс С-Терра Клиент» или установлен сам программный комплекс. Разница в работе будет лишь в том, что упоминаемые ниже конфигурационный файл `skzi.conf` и утилита `cont_mgr` будут находиться в каталоге `C:\Program Files\S-Terra Client AdminTool` либо в каталоге `C:\Program Files\S-Terra Client`. Также должно быть установлено необходимое ПО для работы с токенами.

1. В файле `skzi.conf`, в котором содержатся настройки СКЗИ, укажите тип токена (`rutoken` или `etoken`), а также местоположение и название модуля для поддержки токена (интерфейс PKCS#11). Для Windows это обычно `%WINDIR%\system32\` (x86) и `%WINDIR%\SysWOW64` (x64).

Например, для функционирования токенов Рутокен в файл `skzi.conf` нужно добавить две строки:

```
TokenLibPath=rtPKCS11ECP.dll
TokenType=rutoken
```

Для функционирования токенов JaCarta в файл `skzi.conf` нужно добавить следующие строки:

```
TokenLibPath=jcPKCS11.dll
TokenType=etoken
```

2. Используя утилиту `cont_mgr create`, создайте контейнер с ключевой парой. Например, создадим контейнер, доступный всем пользователям (уровня компьютера), с именем `conttoken` на внешнем носителе, подключенном по интерфейсу PKCS#11. Пароль (PIN) для доступа к контейнеру `12345678`. PIN токена и пароль контейнера должны совпадать:

```
cont_mgr create -cont system::etoken://conttoken -PIN 12345678
```

3. Создайте запрос на сертификат с помощью утилиты `cont_mgr request`. Запрос создается на основе уже имеющейся в контейнере пары ключей для подписи. Например:

```
cont_mgr request -cont system::etoken://conttoken -PIN 12345678
-o myreq -n "C=ru,CN=user1,O=s-terra" -pem
```

Где параметр `-o` задает выходной файл `myreq` для PKCS#10-запроса, параметр `-n` задает Distinguished Name сертификата, параметр `-pem` указывает выходной формат.

4. Отправьте запрос в Удостоверяющий центр.
5. Полученный сертификат поместите на устройство, работающее под управлением ОС Android в папке S-Terra, вложенной в [Android External Storage Directory](#).
6. Выполните [импорт своего сертификата](#) в разделе *Сертификаты* «Программного комплекса С-Терра Клиент-М».

10.3. Настройка «С-Терра Клиент-М» с использованием конфигурационного файла

Описание конфигурационного файла приведено в документе [«Создание конфигурационного файла»](#) (Lsp.pdf).

Особенности настройки

1. Если в конфигурационном файле S-Terra Client-M включен механизм PathMTUDiscovery (IPsecAction.NoPathMTUDiscovery=FALSE), то значение IPsecAction.MTU должно быть больше 670.
2. Параметр PersistentConnection в структуре IPsecAction всегда должен быть TRUE.
3. Допускается только одна структура NetworkInterface со значением LogicalName по умолчанию.
Для платформ Android, не поддерживающих настройку iptables, фильтры InputFilter и OutputFilter не работают.
Особенности работы с атрибутами InputFilter и OutputFilter для платформ Android, поддерживающих настройку iptables:
 - Фильтры применяются ко всем сетевым интерфейсам кроме виртуального интерфейса ikecfg (tun).
 - Кроме того, присутствие цепочки InputFilter и/или OutputFilter запрещает трафик IPv6 в соответствующих направлениях.
4. Если структура Filter используется в составе NetworkInterface.InputFilter или NetworkInterface.OutputFilter, для нее появляются ограничения, связанные с тем, что такие фильтры преобразуются в правила iptables. Ограничения следующие:
 - Запрещено указание полей Schedule, LogEventID, Log, Label, ExtendedAction, PacketType.
 - Сочетание SourcePort или DestinationPort с ProtocolID кроме TCP и UDP, не допускается.
 - В поле Action можно указывать только PASS или DROP.
5. Структура RoutingTable для S-Terra Client-M не поддерживается.
6. Структура AHProposal для S-Terra Client-M не поддерживается.

10.4. Особенности настройки шлюза при работе с «Программным комплексом С-Терра Клиент-М»

Существуют некоторые особенности при создании политики безопасности для шлюза S-Terra Gate при работе с S-Terra Client-M на платформе Android, что связано как с самой операционной системой, так и использованием беспроводного соединения:

- Получение S-Terra Client-M настроек DNS по IKECFG:
- S-Terra Gate должен быть настроен таким образом, чтобы клиенту выдавался IKECFG-адрес, DNS суффикс и адрес DNS-сервера. Без указания DNS-адреса DNS суффикс на S-Terra Client-M не выставится.

Фрагмент LSP на S-Terra Gate:

```
AddressPool <pool-name>
(
    IPAddresses = ...
    DNSServers = <dns-server-ip>
    DNSSuffixes = "<dns-suffix>"
)
```

- S-Terra Gate может передавать произвольное количество DNS-серверов, но сколько будет реально использоваться, зависит от типа устройства и версии прошивки. Если S-Terra Client-M получит больше четырех адресов DNS-серверов, то все адреса, начиная с пятого, будут проигнорированы. Рекомендуется задавать не более двух адресов в списке адресов серверов DNS, передаваемых по протоколу IKECFG клиенту.
- Существует ограничение на длину DNS суффиксов, получаемых по IKECFG. При превышении ограничения на длину DNS суффиксов защищенное соединение не устанавливается:
 - Если по IKECFG передается один DNS суффикс, то его длина не должна превышать 91 символ.
 - Если по IKECFG передается два и более DNS суффиксов, то их суммарная длина вместе с разделителями не должна превышать 91 символ (длина разделителя – один символ).
- Для версии Gate 3.11 необходимо использовать Dead Peer Detection (DPD). В конфигурационном файле, в структуре IKERule атрибуту DoNotUseDPD должно быть присвоено значение FALSE.
- В конфигурационном файле, в структуре IKEParameters атрибуту IKECFGBindAddress желательно присвоить значение TO_PUBLIC_ADDRESS (для версии Gate 3.x) или в структуре IKERule атрибуту IKECFGBindToPeerAddress присвоить значение TRUE (для версии Gate 4.0). Для S-Terra Gate версии 4.1 это можно не делать.

Описание конфигурационного файла для S-Terra Gate смотрите на сайте <http://www.s-terra.com/support/documents/>.

10.5. Сообщения об ошибках

Возможные сообщения об ошибках, которые могут появиться во время работы Продукта, представлены в нижеследующей таблице.

Таблица 1

Сообщение		Пояснение
Фатальные ошибки		
Please remove S-Terra Client-M using Android application manager	Пожалуйста, удалите S-Terra Client-M, используя стандартные средства управления приложениями Android	Стандартная приписка к остальным сообщениям из этого раздела. Обозначает полную неработоспособность приложения. Возможные причины: Повреждение инсталляционного пакета. Несовместимость с программной или аппаратной платформой. Повреждение ОС. Физическое повреждение устройства.
This device is not supported by S-Terra Client-M	Это устройство не поддерживается S-Terra Client-M	
Failed to load the install configuration	Ошибка загрузки конфигурации инсталлятора	
Failed to parse the install configuration: line <номер_строки>	Ошибка разбора конфигурации инсталлятора: строка <номер_строки>	
Failed to parse the install configuration: line <номер_строки>: Unsupported mode	Ошибка разбора конфигурации инсталлятора: строка <номер_строки>: Неподдерживаемый режим	
File <имя_файла> is not accessible in the package.	Файл <имя_файла> не доступен внутри пакета.	
Failed to extract file <имя_файла>.	Ошибка извлечения файла <имя_файла>.	
Failed to set mode to file <имя_файла>.	Ошибка изменения режима доступа к файлу <имя_файла>.	
Failed to remove file <имя_файла>.	Ошибка удаления файла <имя_файла>.	

Failed to remove directory <имя_файла>.	Ошибка удаления каталога <имя_каталога>.	
Failed to create directory <имя_файла>.	Ошибка создания каталога <имя_каталога>.	
Failed to load the platform aliases	Ошибка загрузки описаний платформ	
Failed to parse the platform aliases: line <номер_строки>	Ошибка разбора описаний платформ: строка <номер_строки>	
Failed to create the file hash list	Ошибка создания списка контрольных сумм файлов	
Failed to obtain text of EULA	Ошибка получения текста лицензионного соглашения	
Стандартные ошибки		
Failed to stop IKE/IPsec services	Ошибка остановки служб IKE/IPsec	
License check failed	Проверка лицензии не прошла	
Failed to load configuration	Ошибка при загрузке конфигурации	
Failed to import pre-shared key	Ошибка добавления общего ключа	
Failed to generate certificate request	Ошибка создания запроса сертификата	
Failed to save certificate request	Ошибка сохранения запроса сертификата	
Failed to import trusted CA	Ошибка добавления CA	
Failed to import local certificate	Ошибка добавления сертификата	
Failed to import remote certificate or CRL	Ошибка добавления сертификата или CRL	
Failed to stop secure connection	Ошибка остановки защищенного соединения	
Cannot connect to the IKE/IPsec services	Ошибка связи со службами IKE/IPsec	
Failed to set syslog parameters	Ошибка настройки параметров syslog	
Failed to read certificates from storage	Ошибка чтения списка сертификатов	
Failed to save text	Ошибка сохранения текста	

Failed to load file <имя_файла>	Ошибка загрузки файла <имя_файла>	
Failed to read current configuration	Ошибка чтения текущей конфигурации	
Failed to construct configuration text	Ошибка формирования текста конфигурации	
Unrecognizable certificate data source	Неизвестный источник данных для сертификата	
Failed to parse certificate storage URL	Ошибка разбора URL хранилища сертификата	
Failed to load certificate storage	Ошибка загрузки хранилища сертификата	
Certificate is not compatible with current request	Сертификат несовместим с текущим запросом	
VPN connection rejected by user	Защищенное соединение отвергнуто пользователем	
Cannot create interface. Probably your device does not support Android VPN Service.	Невозможно создать туннельный интерфейс. Вероятно ваше устройство не поддерживает службу Android VPN.	Как правило фатальная ошибка (свидетельствует о несовместимости устройства)
Login FAILED	Неуспешный логин	
Auto login FAILED	Автоматический логин не выполнен	
IKE/IPsec services start FAILED with exit code <код_возврата>	Ошибка запуска служб IKE/IPsec. Код возврата: <код_возврата>	
Failed to get container list	Ошибка получения списка контейнеров	
Failed to export log to files	Ошибка экспорта лога в файлы	
Failed to get certificate list	Ошибка получения списка сертификатов	
Failed to remove certificate	Ошибка удаления сертификата	
Failed to read token provider list	Ошибка чтения списка провайдеров токенов	
Failed to configure token provider	Ошибка конфигурирования провайдера токенов	
Firewall rules were unexpectedly changed. Security policy can be bypassed. Error code: <код_ошибки>	Правила пакетного фильтра испорчены, возможен обход политики безопасности. Код ошибки: <код_ошибки>	Только в версии для Samsung

Failed to get default policy	Ошибка получения политики по умолчанию	Только в версии для Samsung
Подсказки пользователю		
Please, enter correct security gateway address	Пожалуйста, введите правильный адрес защищенного шлюза	
Please, enter correct remote subnet addresses	Пожалуйста, введите правильные адреса защищаемых подсетей	
Please, enter correct IKE key lifetime	Пожалуйста, введите правильное время жизни ключа IKE	
Please, enter correct ESP key lifetime	Пожалуйста, введите правильное время жизни ключа ESP	
Please, enter correct IKE ID for preshared key authentication	Пожалуйста, введите правильное IKE ID для аутентификации на общем ключе	
Authentication mode GOST certificate requires IKE transform set GOST VKO	Для режима аутентификации Сертификат ГОСТ требуется Набор преобразований ГОСТ VKO	
There is no container found	Не найдено ни одного контейнера	
Passwords do not match	Пароли не совпадают	
Other version of the application (<установленная_версия>) is present. You can install version <устанавливаемая_версия> over it.	Установлена другая версия приложения (<установленная_версия>). Вы можете установить версию <устанавливаемая_версия> поверх.	

10.6. Состояние служб IKE/IPsec

Таблица 2

Политика по умолчанию	Сообщение	Пояснение
Службы IKE/IPsec остановлены		
passdhcpr / dropall / na	Службы IKE/IPsec остановлены	
passall	Службы IKE/IPsec остановлены сетевая защита отключена	
error	Службы IKE/IPsec остановлены сетевая защита может быть нарушена: не удалось получить политику по умолчанию	
Службы IKE/IPsec работают		
	защищенное соединение установлено	Присутствует хотя бы один IPsec SA
	не соединен	LSP загружена, однако IPsec SA отсутствует
passdhcpr / dropall / na	защищенное соединение остановлено	LSP присутствует в базе локальных настроек, однако отгружена ("Остановить защищенное соединение")
passall	сетевая защита отключена	LSP присутствует в базе локальных настроек, однако отгружена ("Остановить защищенное соединение")
error	сетевая защита может быть нарушена: не удалось получить политику по умолчанию	
passdhcpr / dropall / na	не сконфигурирован	LSP отсутствует в базе локальных настроек
passall	не сконфигурирован сетевая защита отключена	LSP отсутствует в базе локальных настроек

Примечание 1: условные обозначения поля "Политика по умолчанию":

- passdhcpr – пропускать пакеты только по протоколу DHCP;
- passall – пропускать все;
- dropall – блокировать все;
- error – неизвестно (аварийная ситуация);
- na – неприменима (в случае APK для прочих устройств – HE Samsung);
- пустая ячейка – не зависит от политики по умолчанию.