УТВЕРЖДЕНО

BY.РТНК.00003-04.1 34 01-2-ЛУ

Программный продукт «Клиент безопасности мобильный Bel VPN Client-M 4.1»

Руководство администратора

BY.РТНК.00003-04.1 34 01-2

Листов 45

Подп. и дата	
Инв. № дубл.	
Взам. инд. №	
Подп. и дата	
Инд. № подл.	

2016

Содержание

Лицензионное Соглашение

о праве пользования программным продуктом «Bel VPN Client-M 4.1» производства ООО «С-Терра Бел»

Настоящее Лицензионное Соглашение определяет условия использования законно приобретенного программного продукта «Клиент безопасности мобильный Bel VPN Client-M 4.1» (далее – Изделия) Конечным Пользователем (физическим или юридическим лицом, указанным в Лицензии на использование Изделия, являющейся неотъемлемой частью настоящего Лицензионного Соглашения). Предметом настоящего Лицензионного Соглашения является возмездная передача Конечному Пользователю неисключительных непередаваемых прав пользования Изделием.

Под Изделием понимается комплекс материальных объектов (программных средств, носителей информации, кода программных продуктов, документации в печатной и электронной формах), включенных в Спецификацию Комплекта Изделия.

Изделие может использоваться только в качестве персонального Агента защиты (устанавливаться на персональное мобильное устройство (смартфон, планшет, др) пользователя) и не предназначено для использования в других целях. Использование Изделия в прочих системах и/или в иных целях является нарушением настоящего Лицензионного Соглашения.

Изделие может включать компоненты (программные средства, информационные носители и прочее) от третьих поставщиков. Конечный Пользователь получает права на использование этих компонент на основе Лицензий и Лицензионных Соглашений этих поставщиков, которые являются в совокупности неотъемлемой частью настоящего Лицензионного Соглашения.

Изделие в полном комплекте передается Конечному Пользователю на условиях настоящего Лицензионного Соглашения.

Изделие и его компоненты являются интеллектуальной собственностью Производителя и, при наличии третьих поставщиков, интеллектуальной собственностью третьих поставщиков и защищаются законодательством Республики Беларусь об авторском праве на объекты интеллектуальной собственности.

Установка Изделия после предъявления Конечному Пользователю текста Лицензионного Соглашения рассматривается как согласие Конечного Пользователя с условиями Лицензионного Соглашения и вступление его в законную силу, после чего настоящее Лицензионное Соглашение в соответствии со ст. 403 Гражданского кодекса Республики Беларусь имеет силу договора между Конечным Пользователем и Производителем Изделия (ООО «С-Терра Бел»).

При наличии компонент третьих поставщиков Производитель является законным и полномочным представителем третьих поставщиков, если обратное не оговорено в Лицензионных Соглашениях третьих поставщиков или в других документах, регламентирующих отношения между Конечным Пользователем и третьими поставщиками.

Все компоненты третьих поставщиков объединяются в программный комплекс в процессе установки Изделия. Конечный Пользователь имеет право на копирование, установку и эксплуатацию всех компонент третьих поставщиков, поставленных в составе Изделия только в составе работ, связанных с эксплуатацией Изделия. Копирование, распространение, установка и эксплуатация отдельных компонент являются нарушением настоящего Лицензионного Соглашения и авторских прав как Производителя, так и третьих поставщиков (если обратное не оговорено в Лицензиях и Лицензионных Соглашениях третьих поставщиков).

Конечный Пользователь может устанавливать и использовать в рамках настоящего Лицензионного Соглашения только один экземпляр Изделия и не имеет права устанавливать и использовать большее количество экземпляров Изделия.

Конечный Пользователь не имеет права распространять Изделие в формах предоставления доступа третьим лицам к воспроизведению или к воспроизведенным в любой форме компонентам Изделия путем продажи, проката, сдачи внаем, предоставления взаймы или иными другими способами отчуждения.

Конечный Пользователь не имеет права дисассемблировать, декомпилировать (преобразовывать бинарный код в исходный текст) программы и другие компоненты Изделия, вносить какие-либо изменения в бинарный код программ и совершать относительно Изделия другие действия, нарушающие белорусское и международное законодательство по авторскому праву и использованию программных средств.

Настоящее Лицензионное Соглашение вступает в силу с момента установки Изделия и действует на протяжении всего срока использования Изделия.

Неисполнение требований настоящего Лицензионного Соглашения является нарушением Закона Республики Беларусь от 17.05.2011 г. "Об авторском праве и смежных правах" и преследуется по закону.

Настоящее Лицензионное Соглашение предоставляет Конечному Пользователю Ограниченные гарантии, состоящие в том, что

1. В случае, если в ходе эксплуатации Изделия Конечным Пользователем или любым третьим лицом будет обнаружена Критичная Проблема, Производитель Изделия (ООО «С-Терра Бел») обеспечивает:

а) информирование доступными способами Конечного Пользователя о существовании Критичной Проблемы и о способах ее устранения

б) бесплатное предоставление обновлений программного обеспечения Производителя Изделия, в которых устранены Критичные Проблемы.

Примечание 1. Гарантийное обязательство 1 базируется на следующем определении: Критичная Проблема заключается в том, что Изделие, вследствие ошибки в программном обеспечении, не выполняет основные функции безопасности, а именно шифрование трафика и контроль доступа, что приводит к нарушению безопасности сети Конечного Пользователя.

Примечание 2. Обновления программного обеспечения в соответствии с гарантийным обязательством п.1б предоставляются по запросу Конечного Пользователя и по мере разработки обновлений.

2. Если Конечный Пользователь обнаружит в течение 90 (девяноста) дней со дня поставки Изделия дефекты в составе информационных носителей или некомплектность Изделия, то информационные носители будут заменены, а комплектность Изделия восстановлена. По истечении 90 дней претензии Конечного Пользователя по некомплектности изделия и/или дефектам носителей информации рассматриваться не будут.

Настоящее Лицензионное Соглашение не содержит никаких гарантий по поставке, функциональности и соответствию Изделия любым техническим требованиям, стандартам и условиям. Эти вопросы относятся к области лицензирования деятельности поставщика, сертификации Изделия и его компонент в установленном порядке, договоров о поставке, техническом сопровождении и технической поддержке и регламентируются в рамках отдельных документов.

Настоящее Лицензионное Соглашение (в рамках законодательства Республики Беларусь и если противное не оговорено в виде отдельного дополнительного соглашения с Конечным Пользователем) не регламентирует вопросы технических, организационных и прочих возможных проблем, связанных с эксплуатацией Изделия и возможных материальных, финансовых и прочих потерь Конечного Пользователя в результате эксплуатации Изделия.

Срок действия настоящего Лицензионного Соглашения распространяется на весь период эксплуатации Изделия Конечным Пользователем. Действие настоящего Лицензионного Соглашения может быть прекращено по решению Конечного Пользователя. В этом случае Конечный Пользователь должен уничтожить все информационные носители, содержащие код и прочие информационные компоненты Изделия, включая информацию на внутренних носителях Изделия. Прекращение действия Лицензионного Соглашения по инициативе Конечного Пользователя является односторонней добровольной акцией Конечного Пользователя и не является предметом для взаиморасчетов и других хозяйственных операций.

Программный продукт Системная Библиотека GNU libc является свободно распространяемым продуктом и используется в составе Изделия без каких либо модификаций в соответствии с лицензией "The GNU General Public License" (http://www.gnu.org/licenses/licenses.html).

Android является торговой маркой компании Google в США и в других странах.

Изделие включает в себя программное обеспечение, написанное Эриком Янгом (Eric Young. eay@cryptsoft.com).

Java является торговой маркой корпорации Oracle.

Другие названия компаний и продуктов, упомянутые в настоящем Лицензионном Соглашении и в составе информационных источников Изделия могут являться зарегистрированными торговыми марками соответствующих им компаний. Упоминание наименований, продуктов, торговых марок третьих организаций исключительно неформально и не является ни поддержкой, рекомендацией либо рекламой. ООО «С-Терра Бел» не несет какой-либо ответственности в отношении работоспособности и использования этих продуктов.

Напечатано в Республике Беларусь

ООО «С-Терра Бел»

220012, г. Минск ул. Чернышевского, д. 10А, офис 702Б1

Телефон: (+375 17) 280 6000

Факс: (+375 17) 280 78 67

Эл.почта: info@s-terra.by

http://www.s-terra.by

1. Комплект поставки

В комплект поставки программного продукта «Клиент безопасности мобильный Bel VPN Client-M 4.1» входит компакт-диск, на котором находятся:

- Каталог **Soft**:
  - s_terra_clientm-4.1.15981.apk – архивное исполняемое приложение,
  - avverify – утилита для проверки целостности дистрибутива.
  - файл hashes.
- Каталог **Documentation**:
  - BelVPN_Client-M-4-1_AdminGuide.pdf – «Программный продукт «Клиент безопасности мобильный Bel VPN Client-M 4.1». Руководство администратора» –.

В печатном виде поставляются:

- Копия сертификата соответствия техническому регламенту Республики Беларусь ТР 2013/027/BY.
- Лицензия на использование «Программного продукта «Клиент безопасности мобильный Bel VPN Client-M 4.1».

2. Требования к программно-аппаратным средствам

Программный продукт «Клиент безопасности мобильный Bel VPN Client-M 4.1» предназначен для использования на мобильных устройствах, работающих под управлением ОС Android 4.x.

Перечень устройств, протестированных на совместимость с программным продуктом «Клиент безопасности мобильный Bel VPN Client-M 4.1»:

- Samsung Galaxy S5,
- Samsung Galaxy S 5 Mini,
- Samsung Galaxy Tab 10.1,
- Samsung Galaxy Note 4,
- Samsung Galaxy S6,
- Samsung Galaxy S6 Edge,
- Samsung Galaxy S6 Edge Plus,
- Samsung Galaxy S3,
- Samsung Galaxy J5,
- Samsung Galaxy J7,
- Samsung Galaxy S5 Duos.

3. Назначение и функции Продукта

Программный продукт "Клиент безопасности мобильный Bel VPN Client-M 4.1 (далее Bel VPN Client-M) предназначен для создания защищенных VPN соединений между устройством, на котором он установлен, и другими взаимодействующими с ним доверенными шлюзами VPN и доверенными клиентами VPN.

Bel VPN 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;
- выполняет генерацию данных аудита и вывод на удаленный или локальный syslog-сервер;
- обеспечивает регулируемую стойкость защиты трафика.

Bel VPN 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 Bel VPN Client использует встроенную криптографическую библиотеку, разработанную ЗАО «Авест».

Bel VPN Client соответствует требованиям Технического регламента Республики Беларусь «Информационные технологии. Средства защиты информации. Информационная безопасность» – ТР 2013/027/BY (взаимосвязанные ТНПА:

- хэширование –СТБ 34.101.31-2011 (подраздел 6.9 раздела 6);
- электронная цифровая подпись –СТБ 34.101.45-2013 (подраздел 6.2 раздела 6; подраздел 7.1 раздела 7; таблица Б1 приложения Б; приложение Д)
- шифрование и контроль целостности – СТБ 34.101.31-2011 (подраздел 6.4 раздела 6);
- генерация случайных данных – СТБ 34.101.47-2012 (подраздел 6.2 раздела 6);
- управление ключами – СТБ 34.101.66-2014 (приложение А), управление криптографическими ключами, рекомендованное ОАЦ;
- формат сертификатов и списков отозванных сертификатов – СТБ 34.101.19-2012 (разделы 6, 7, 8);
- требования безопасности – СТБ 34.101.27-2011 (класс 1).

4. Контроль целостности дистрибутива

Перед инсталляцией «Клиента безопасности мобильный Bel VPN Client-M 4.1» можно убедиться в целостности дистрибутивов, используя утилиту avverify, размещенную на поставляемом диске.

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

avverify –mk belvpn_clientm_4.1.15981.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:

avverify –mk belvpn_clientm_4.1.15981.apk hash_from_file,

где

hash_from_file – эталонное значение контрольной суммы для файла belvpn_clientm_4.1.15981.apk, скопированное из файла hashes.

4.1. Инсталляция «Bel VPN Client-M»

Доставьте на мобильное устройство файлы с дистрибутивом «Bel VPN Client-M».

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

Затем выполните установку приложения belvpn_clientm_4.1.15981.apk.

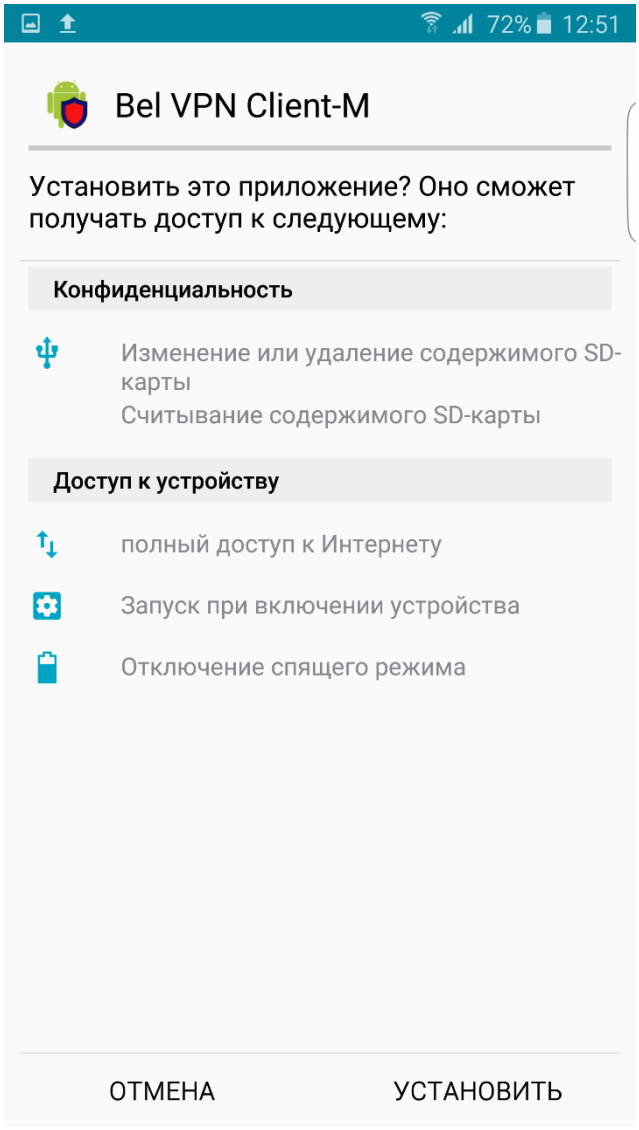

Рисунок 1

Продукту необходимы следующие разрешения:

- 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.).
- NETWORK COMMUNICATION – неограниченный доступ в интернет (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.
- AFFECTS BATTERY – отключение спящего режими

Нажимайте Далее, пока не появится кнопка Установить. После нажатия кнопки Установить, выполнится установка Bel VPN Client-M (Рисунок 2).

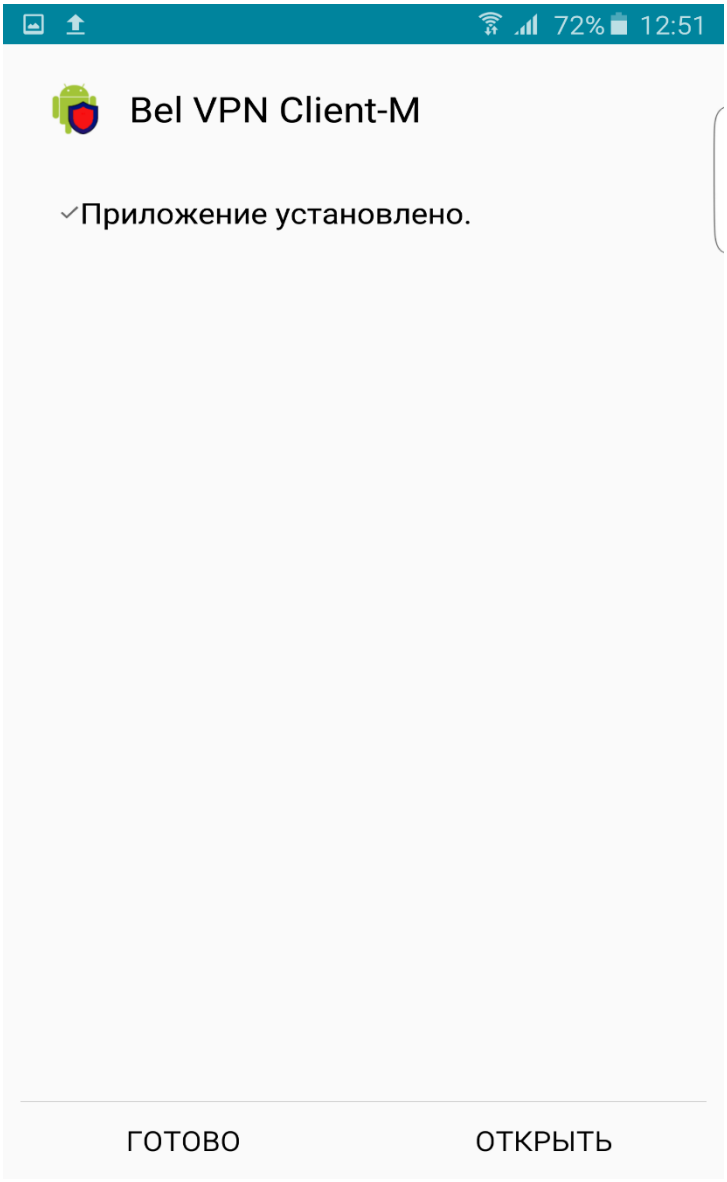

Рисунок 2

Для завершения установки нажмите Готово, в этом случае дальнейшая инициализация Продукта будет выполнена при первом запуске приложения, или нажмите Открыть, чтобы сразу запустить Bel VPN Client-M после завершения установки.

5. Инициализация Bel VPN Client-M при первом запуске

При первом запуске Bel VPN 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 продукта «Клиент безопасности мобильный Bel VPN Client-M 4.1», входящей в печатном виде в комплект поставки.

Примечание: иногда удобнее заранее подготовить файл с лицензионной информацией agent.lic, тогда при инициализации Bel VPN 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 Bel VPN Client-M на дисплей будет выведено лицензионное соглашение о праве пользования Продуктом (Рисунок 3).

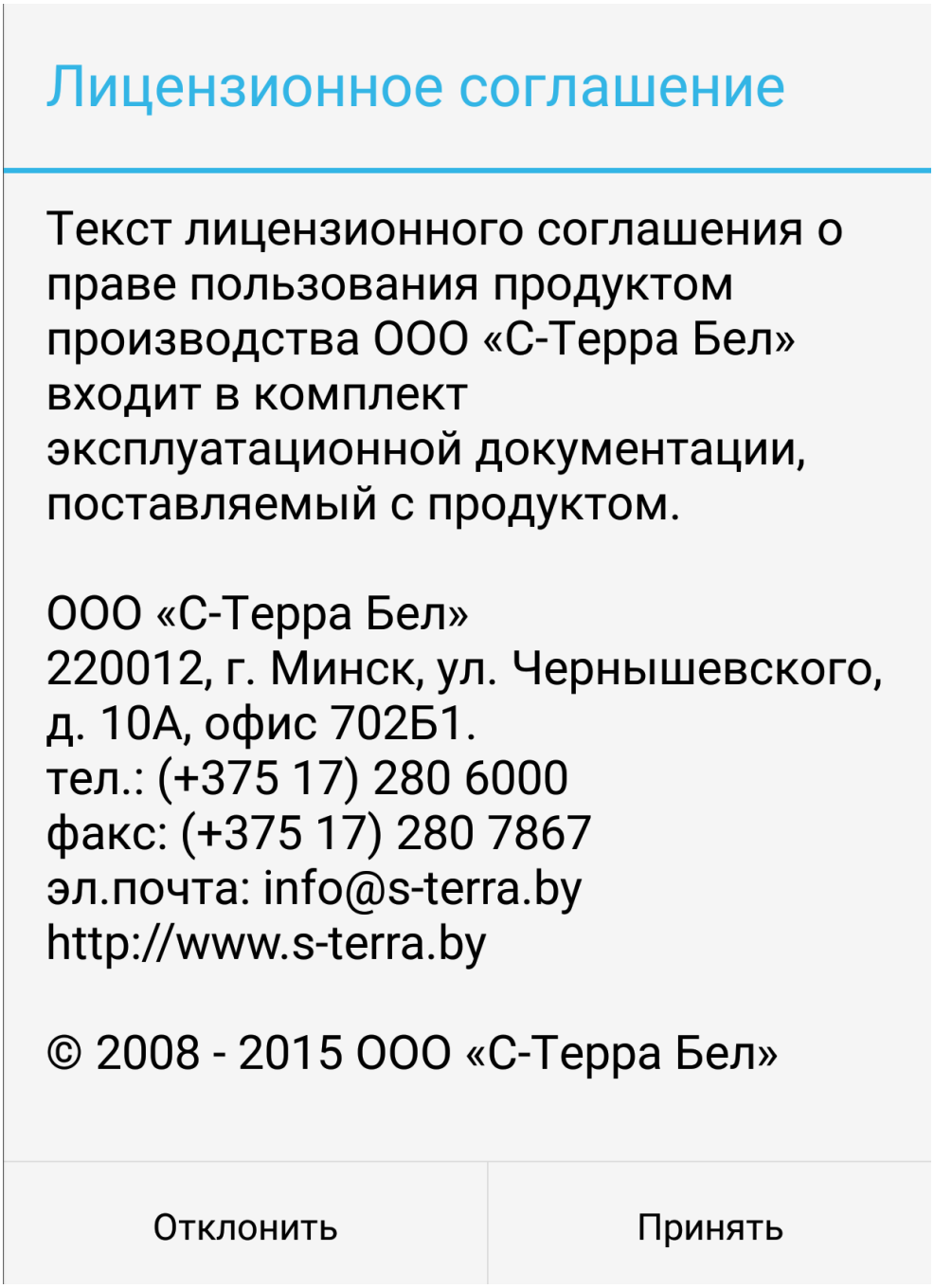

Рисунок 3

В случае принятия условий лицензионного соглашения, будет запрошена информация о лицензии на Продукт (Рисунок 4). Введите данные и нажмите Продолжить.

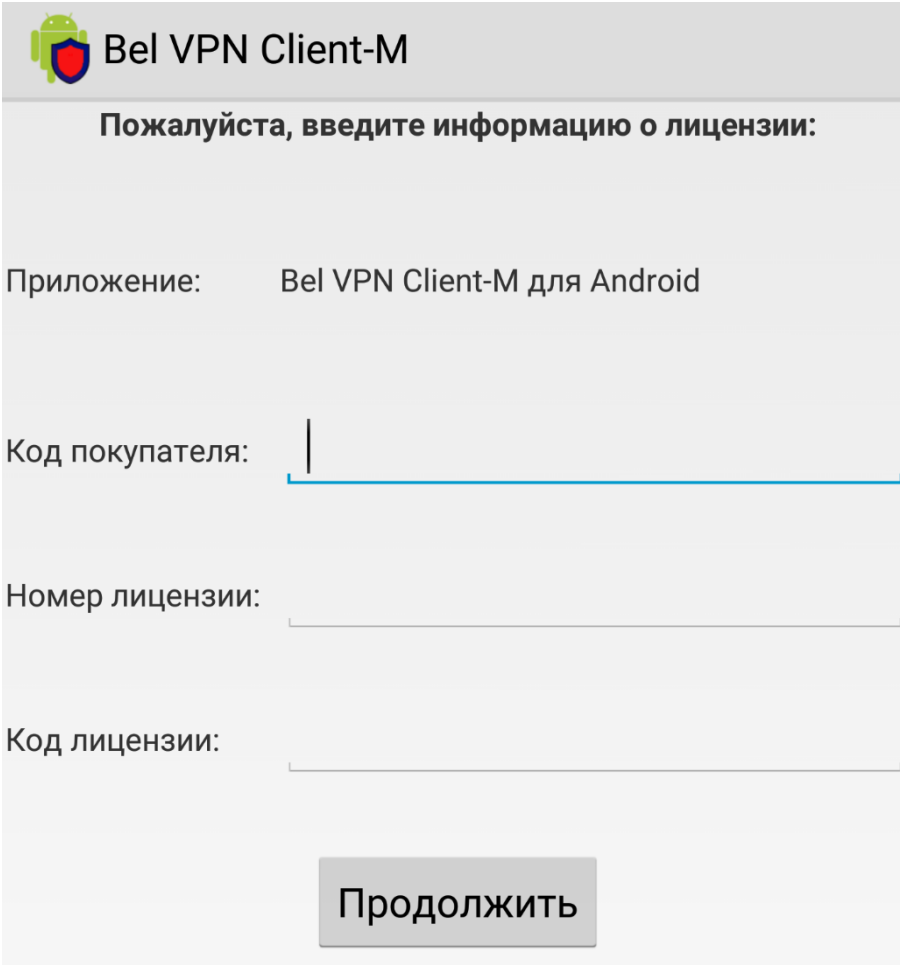

Рисунок 4

Далее инициализируется генератор случайных чисел. Изменяйте положение устройства в пространстве, пока выполняется инициализация (Рисунок 5).

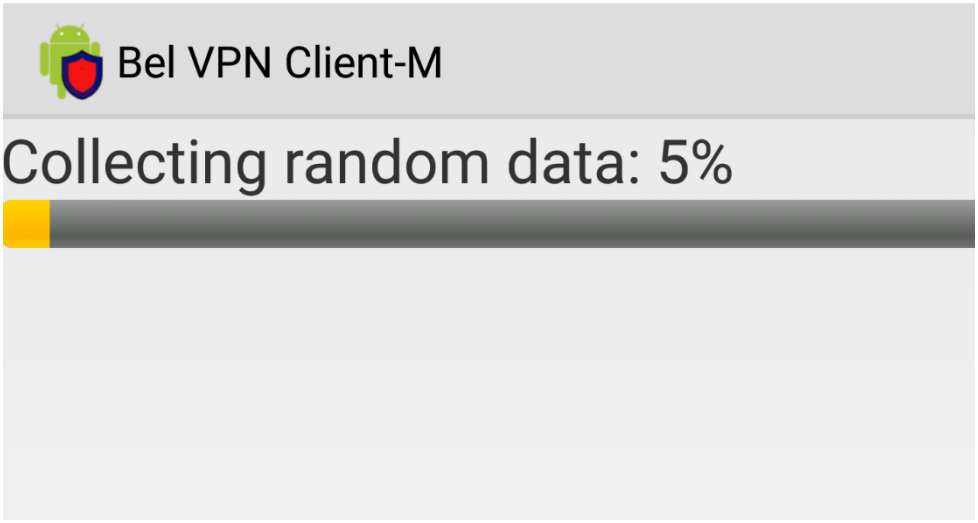

Рисунок 5

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

6. Описание интерфейса «Клиента безопасности мобильного Bel VPN Client-M 4.1»

Настройка и управление «Клиента безопасности мобильного Bel VPN Client-M 4.1» осуществляется с использованием графического интерфейса. При запуске «Bel VPN Client-M» на экране появляется главная форма (Рисунок 6).

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

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.

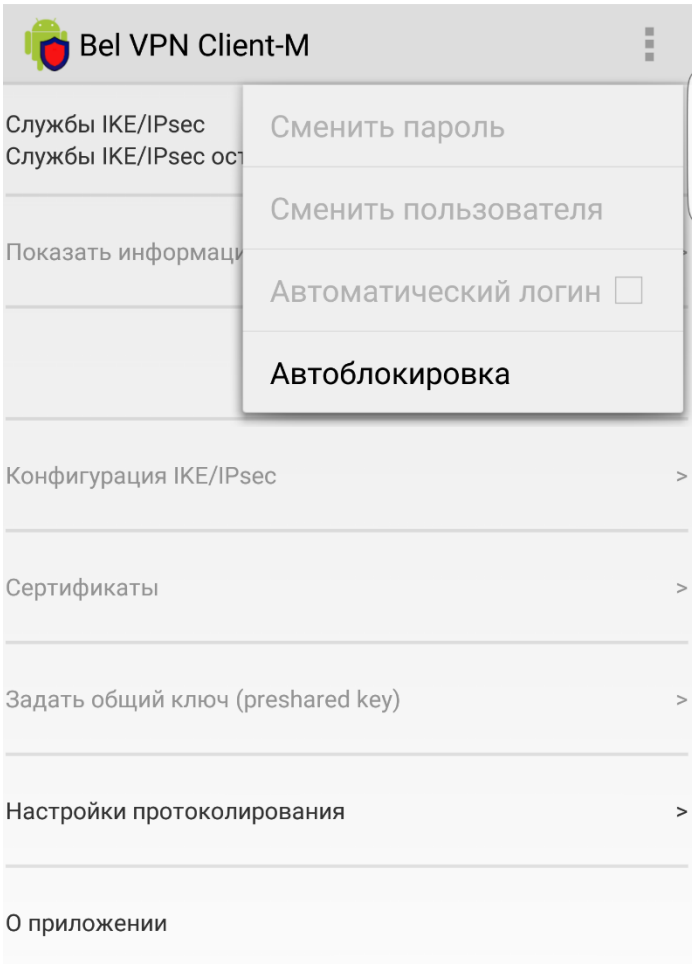

Рисунок 6

6.1. 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.

1.1.1 Интерактивный режим логина в Продукт

После успешного старта служб IKE/IPsec выдается окно логина (Рисунок 7).

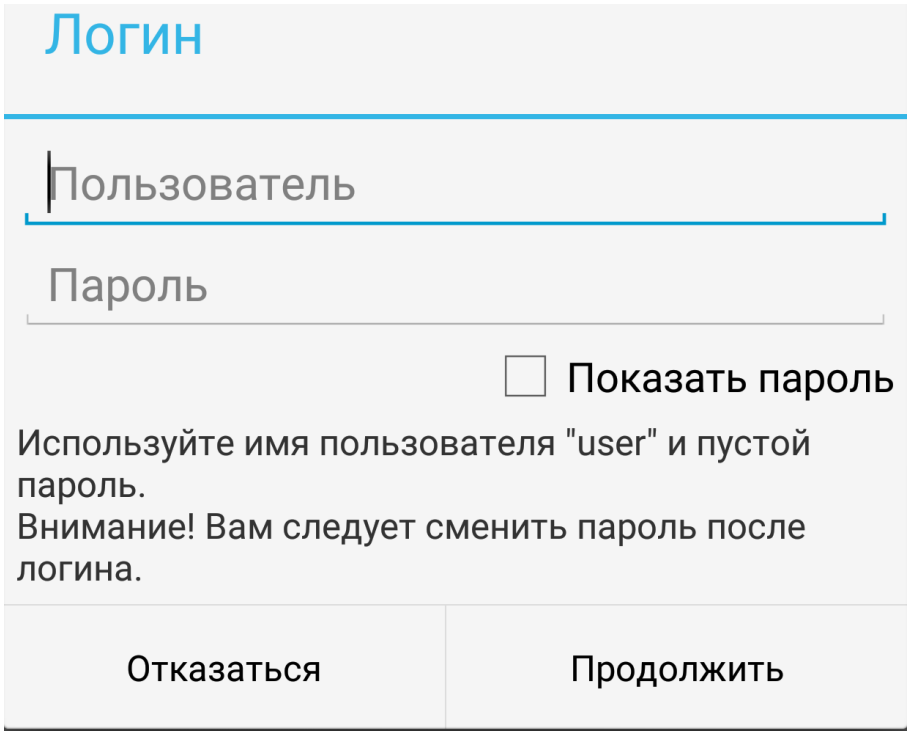

Рисунок 7

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 8). 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.

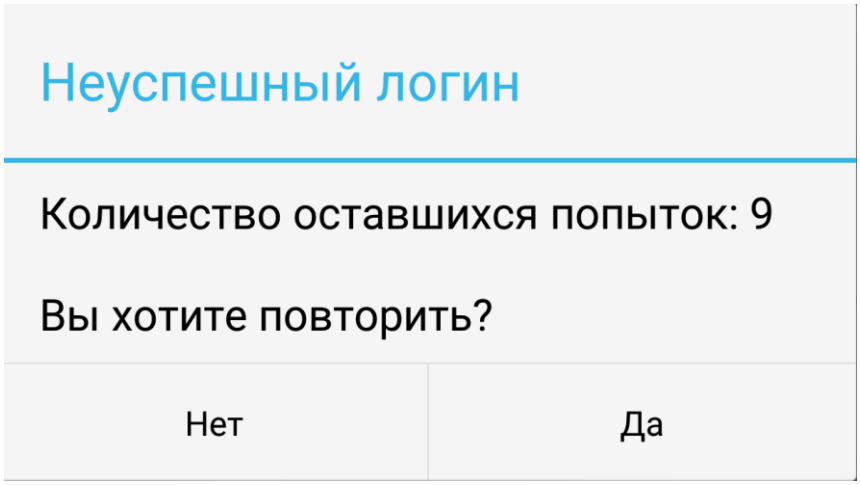

Рисунок 8

Допускаются десять неудачных попыток логина подряд. Затем будет выдано сообщение, что пользователь заблокирован». (Рисунок 9). После нажатия на кнопку Продолжить служба IKE/IPsec будет остановлена.

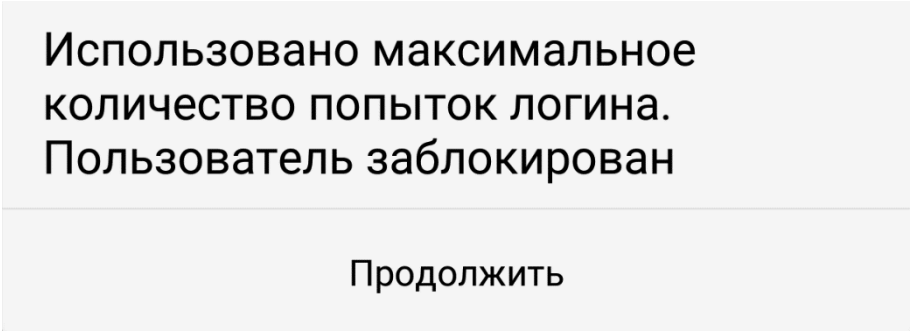

Рисунок 9

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 *Bel VPN Client-M*.
3. Нажмите на кнопку Очистить данные. Подтвердите удаление данных.
4. Все действующие настройки продукта (данные лицензии, 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.

1.1.2 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 10).

6.2. Главная форма

После регистрации пользователя становятся доступны все элементы и все пункты меню главной формы (Рисунок 10).

Примечание: при настройке Bel VPN 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.

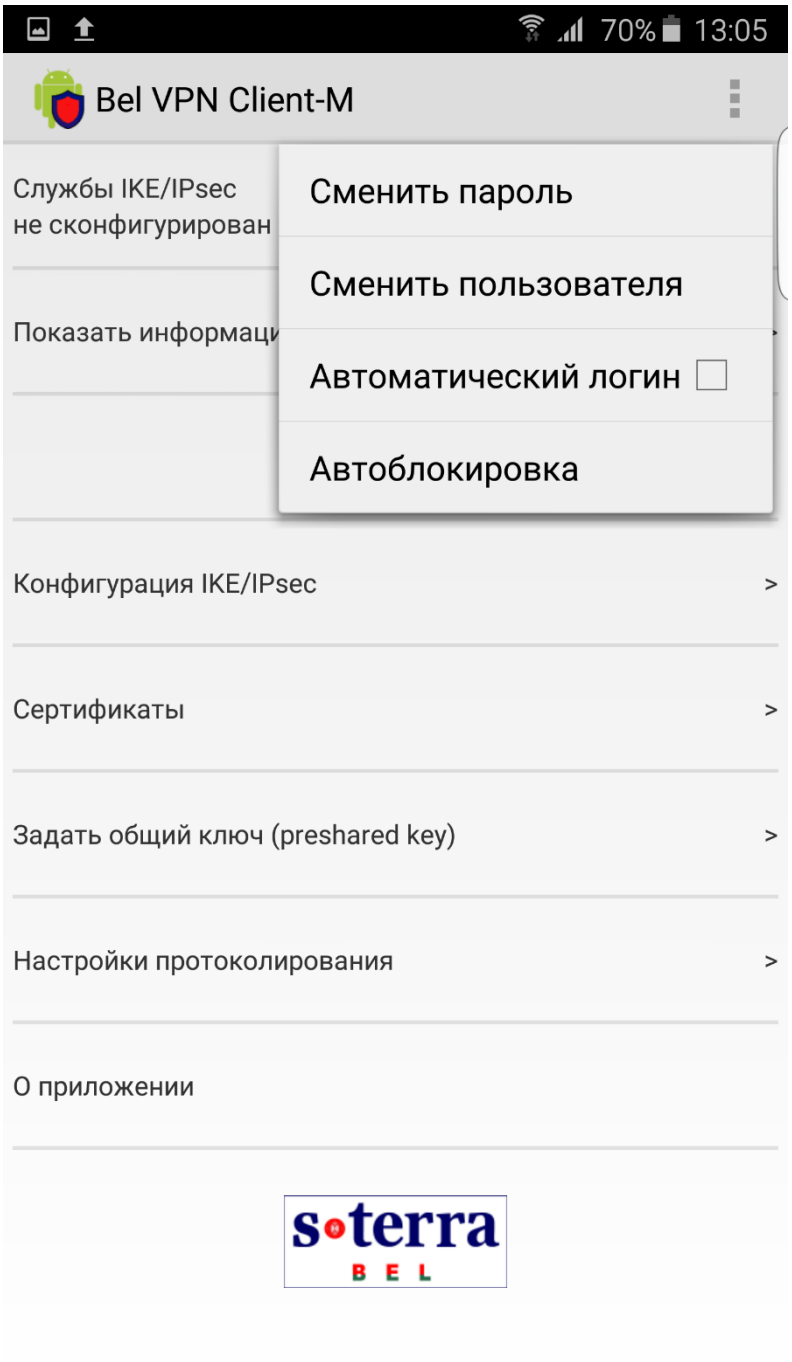

Рисунок 10

1.1.3 Меню главной формы

Сменить пароль

Для смены пароля выберите соответствующий пункт меню (Рисунок 10). Появится окно (Рисунок 11). Введите старый пароль и два раза новый пароль. Нажмите Продолжить.

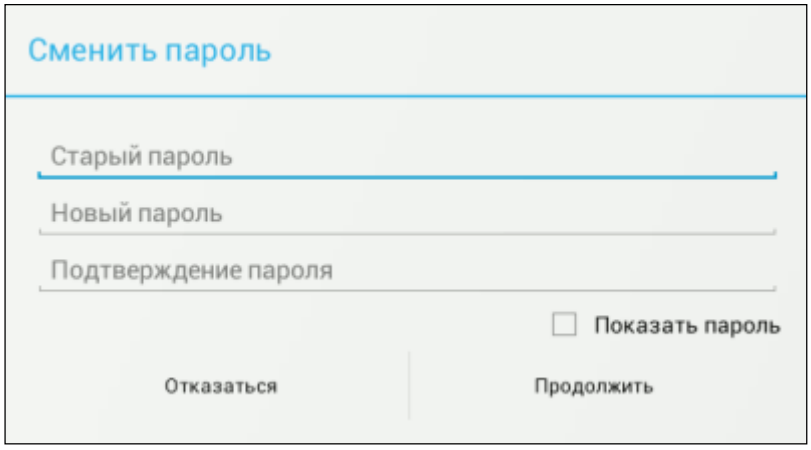

Рисунок 11

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 10).

В появившемся окне (Рисунок 12) 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.

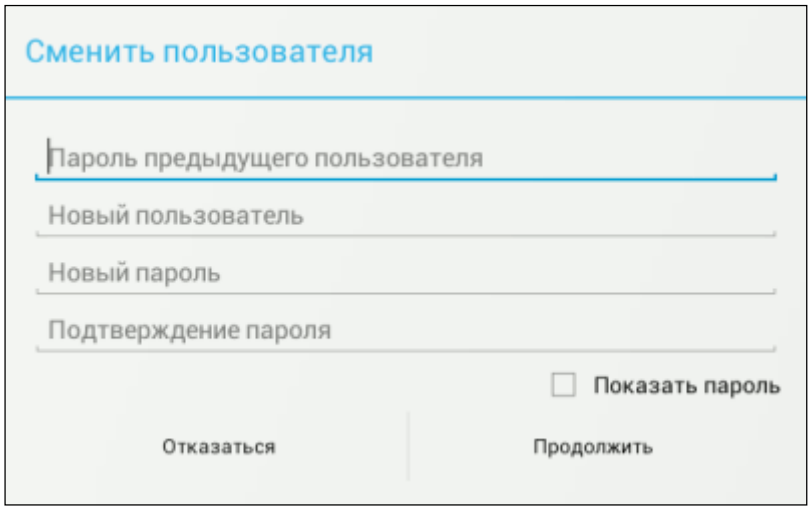

Рисунок 12

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 10). Флажок по умолчанию сброшен.

После установки флажка появляется окно (Рисунок 13), в котором надо ввести пароль текущего пользователя.

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

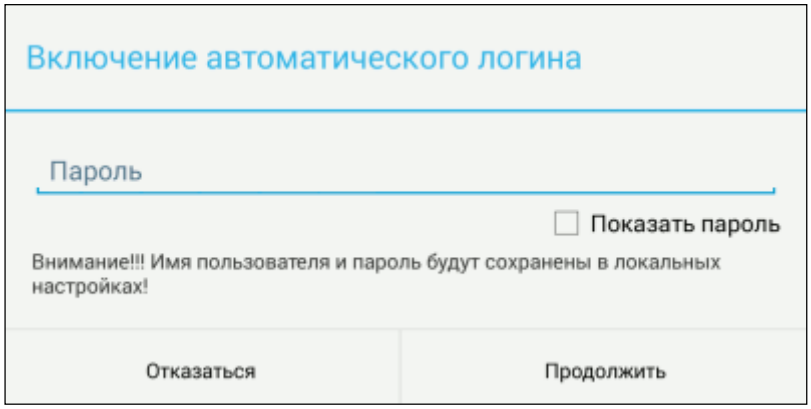

Рисунок 13

При сбросе флажка *Автоматический логин*, необходимо подтвердить использование интерактивного логина (Рисунок 14).

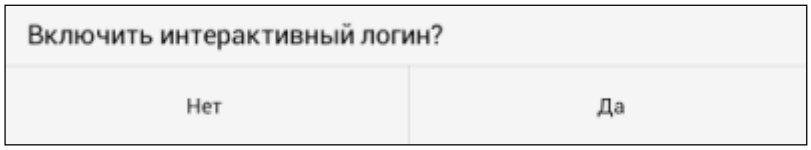

Рисунок 14

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 15).

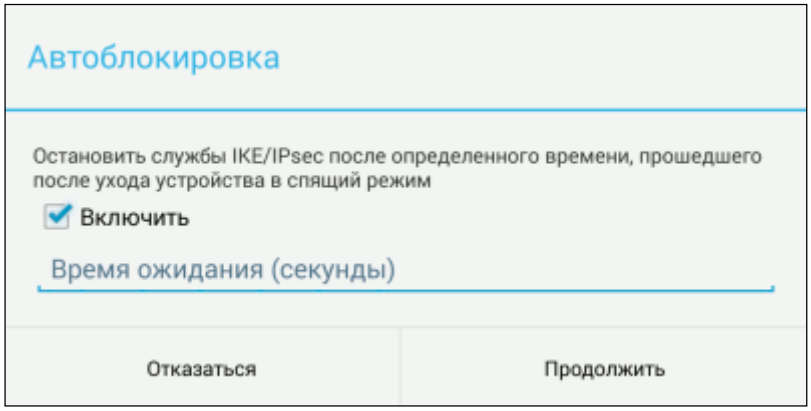

Рисунок 15

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.

1.1.4 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 «Bel VPN Client-M» деактивируется до следующего старта служб IKE/IPsec. Реальная работа продукта «Bel VPN Client-M» возможна только после запуска служб IKE/IPsec. Если нужно принудительно удалить защищенное соединение рекомендуется останавливать службы IKE/IPsec. Остановка службы требует подтверждения (Рисунок 16).

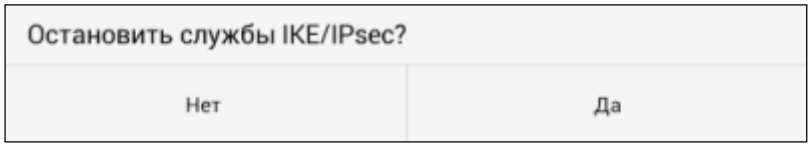

Рисунок 16

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.

6.3. Конфигурация IKE/IPsec

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

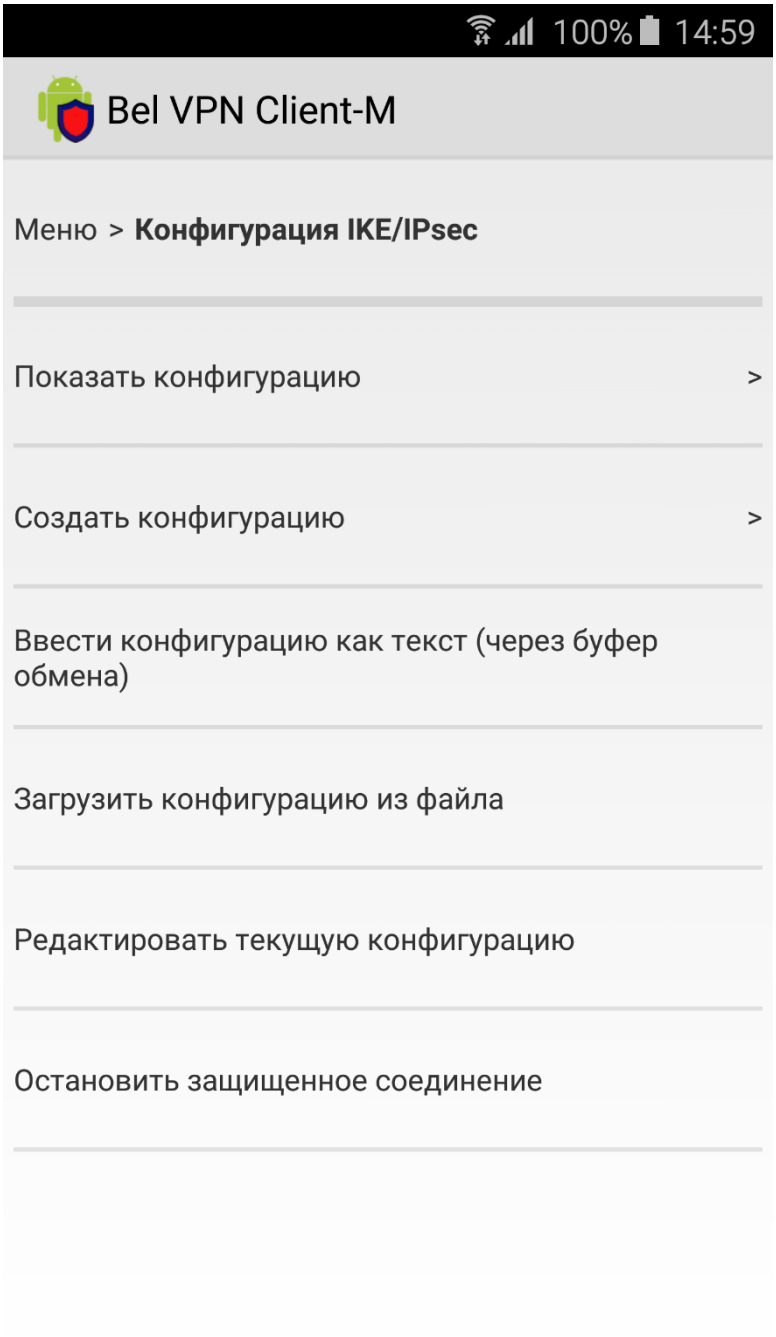

Рисунок 17

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 «Bel VPN Client-M» 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.

1.1.5 Показать конфигурацию

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

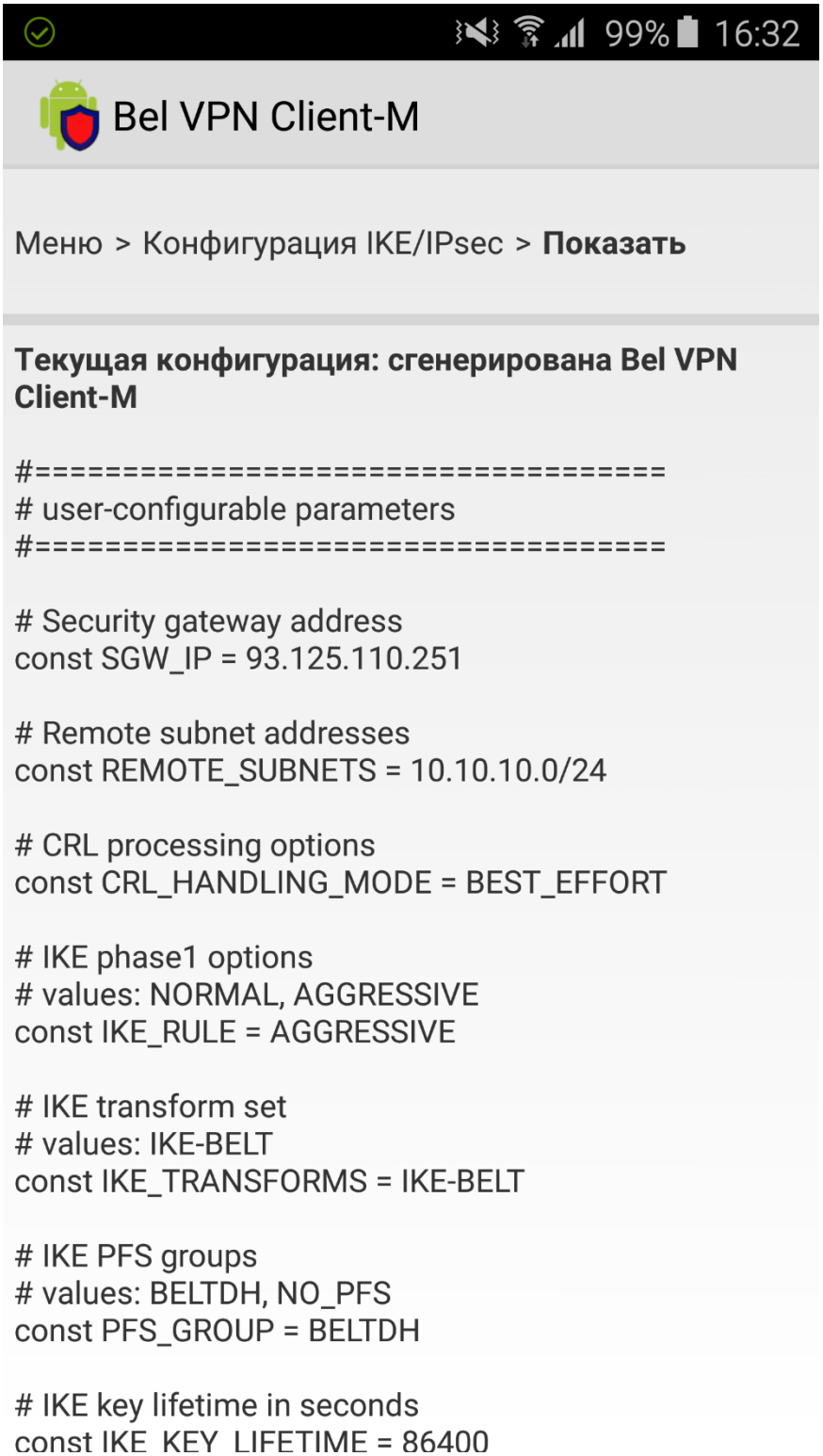

Рисунок 18

1.1.6 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 19).

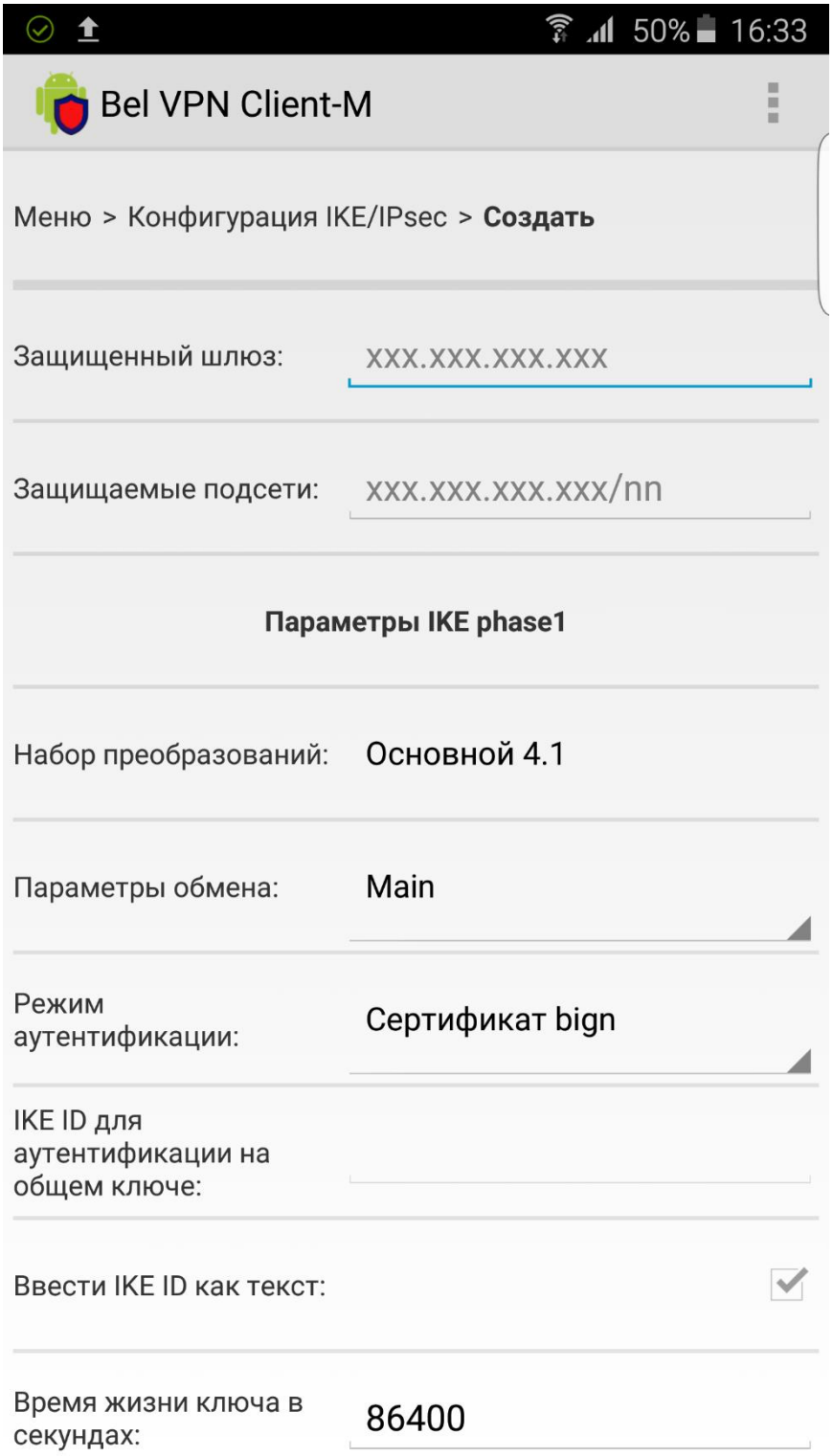

Рисунок 19

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.

- *Основной 4.1* – состоит из следующих преобразований:
  - алгоритм шифрования – СТБ 34.101.31-2011 (6.4)
  - алгоритм хэширования – СТБ 34.101.31-2011 (6.9)
  - алгоритм формирования общего ключа – СТБ 34.101.66-2013.

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).

- *Сертификат bign* – 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).

- *СТБ 34.101.66-2013* – при согласовании новой SA выполняется новый обмен ключами по алгоритму СТБ 34.101.66-2013. Это значение используется по умолчанию.
- *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:

- *СТБ 34.101.31-2011(6.4 + 6.6)* – алгоритм шифрования СТБ 34.101.31-2011 (в режиме гаммирования с обратной связью), алгоритм проверки целостности СТБ 34.101.31-2011 (в режиме выработки имитовставки). Значение по умолчанию.
- *СТБ 34.101.31-2011 (6.4)* – алгоритм шифрования СТБ 34.101.31-2011 (в режиме гаммирования с обратной связью).

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.

1.1.7 Ввести конфигурацию как текст

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

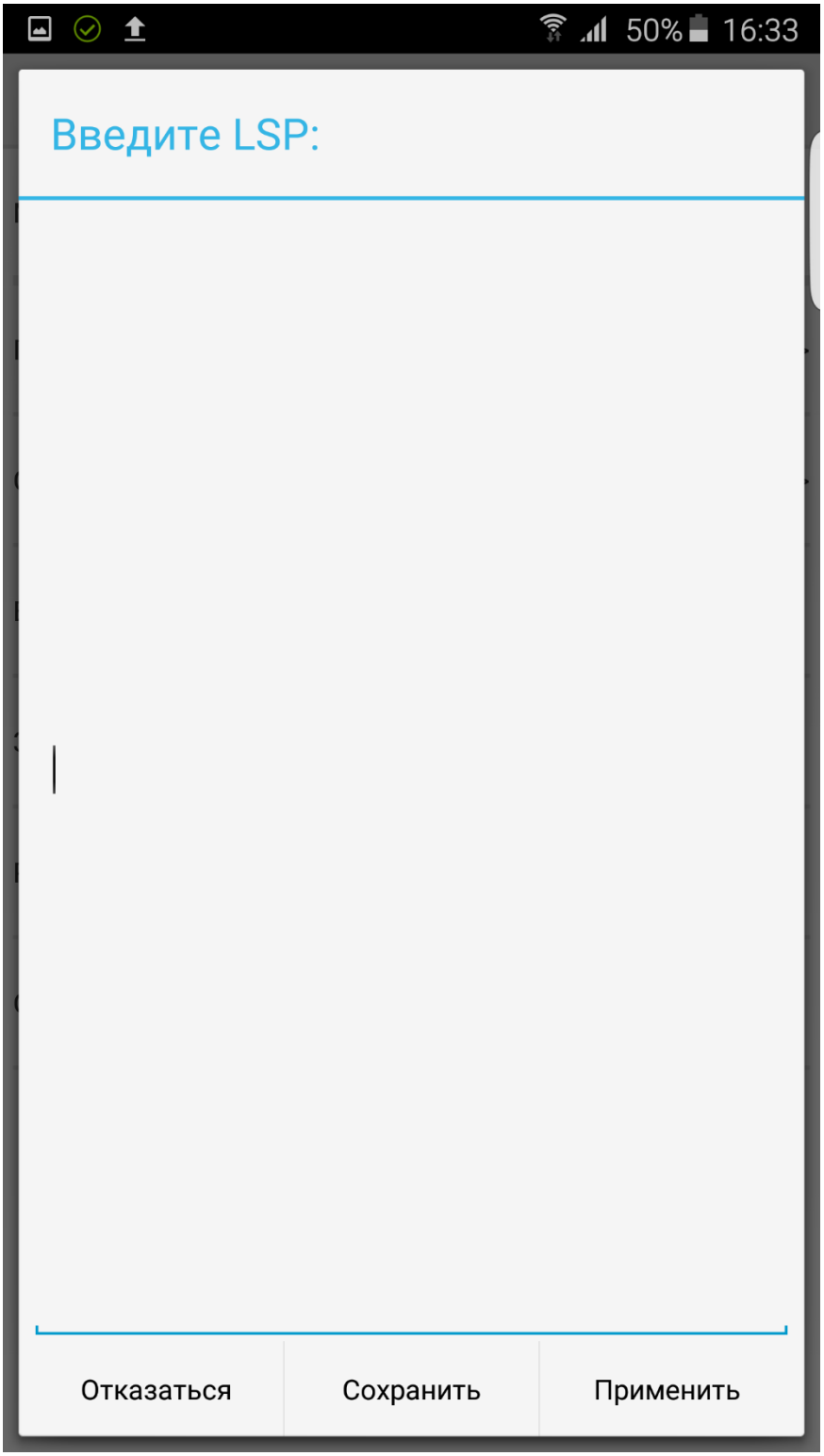

Рисунок 20

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

1.1.8 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.

1.1.9 Редактировать текущую конфигурацию

При выборе этого пункта меню выводится текстовое поле с локальной политикой безопасности (Рисунок 21).

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

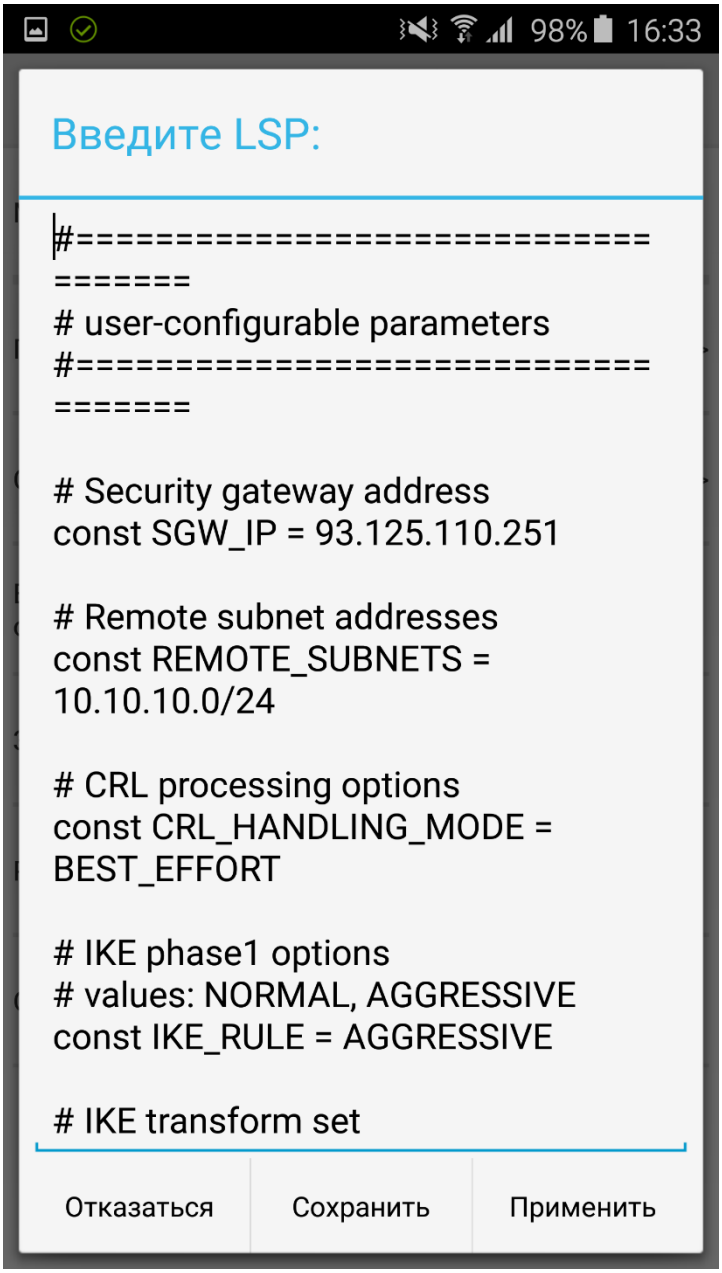

Рисунок 21

1.1.10 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 22).

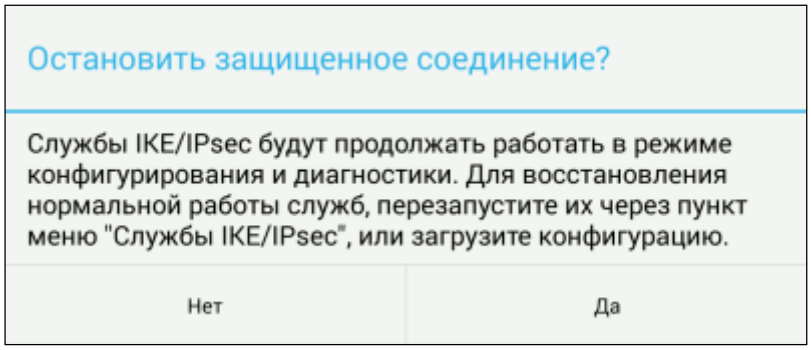

Рисунок 22

Для восстановления нормальной работы служб, перезапустите или загрузите конфигурацию.

6.4. 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 (Рисунок 23).

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.

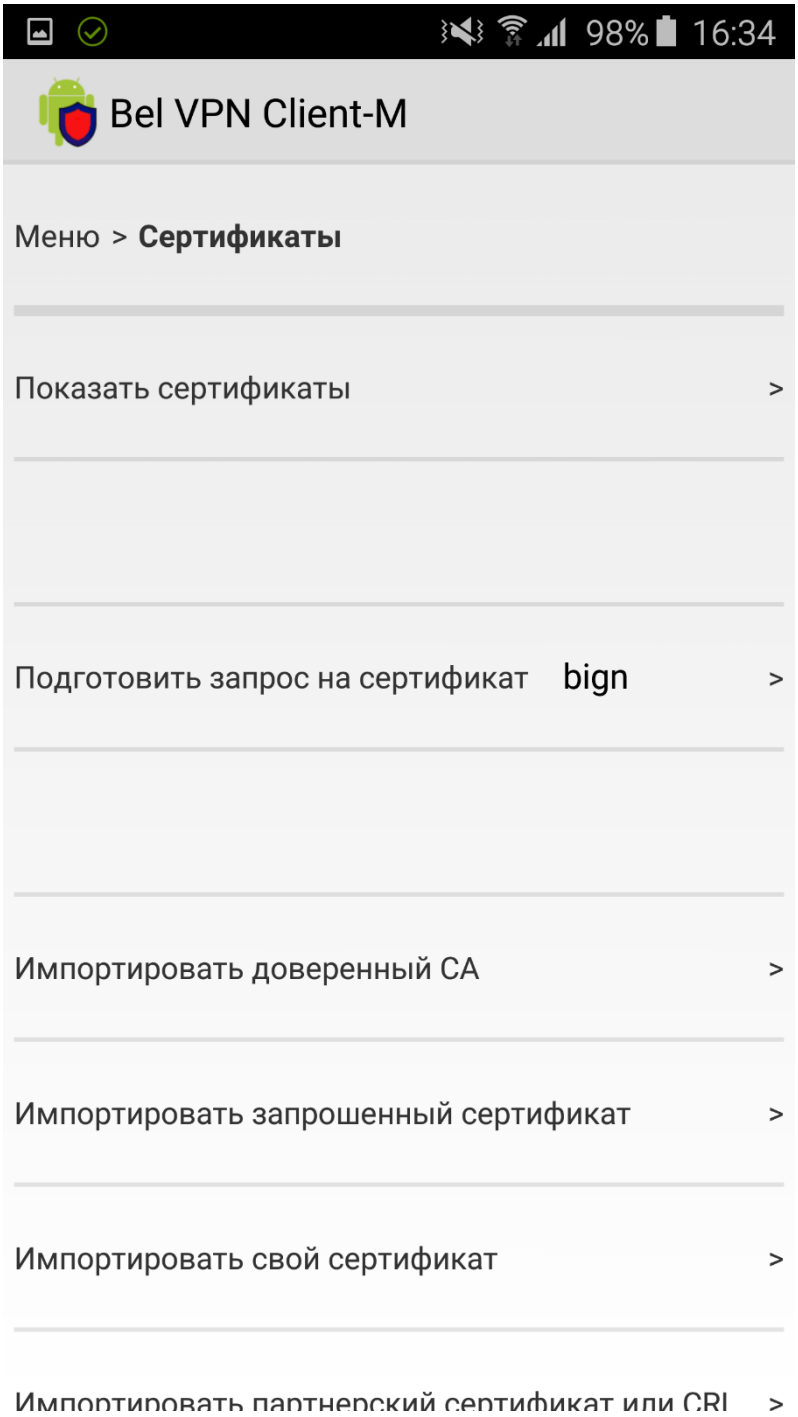

Рисунок 23

Показать сертификаты – выводится информация о сертификатах, находящихся в базе Продукта (Рисунок 24).

Рисунок 24

Подготовить запрос на сертификат

При выборе этого пункта появляется окно (Рисунок 25) в котором необходимо ввести значение поля Subject Name сертификата (применяется для подготовки запроса на сертификат).

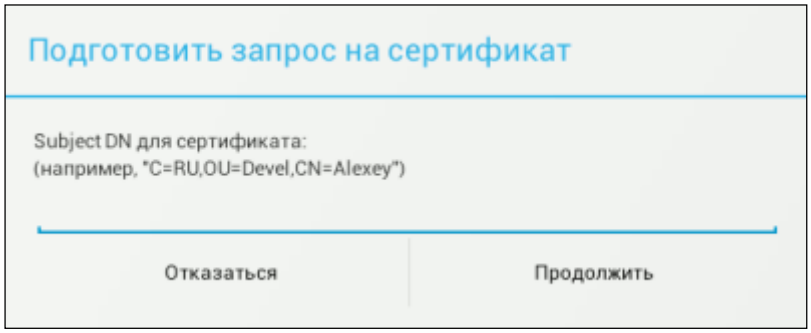

Рисунок 25

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 26).

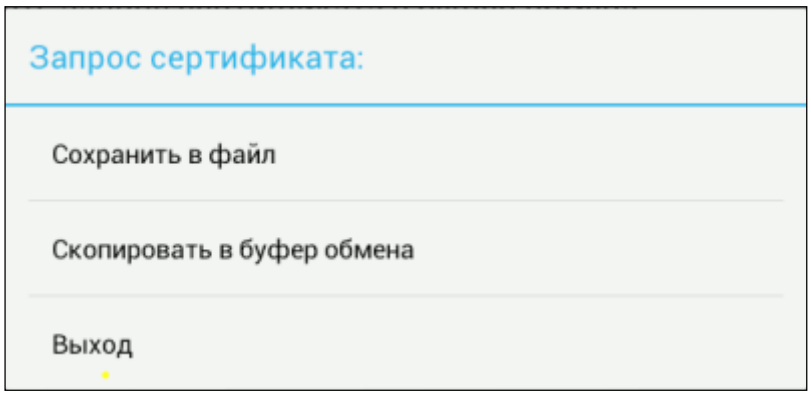

Рисунок 26

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

Для получения сертификата нужно отослать запрос в Удостоверяющий Центр.

Импортировать доверенный CA – при выборе этого пункта появляется окно (Рисунок 27), в котором надо выбрать способ получения CA сертификата для импорта в базу данных:

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

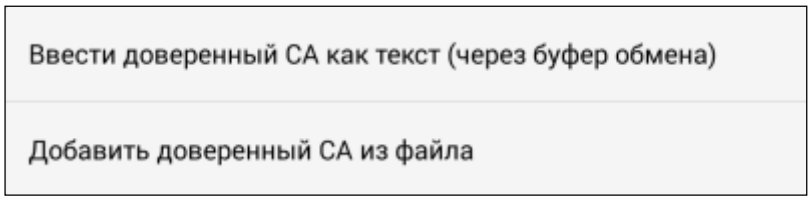

Рисунок 27

Импортировать запрошенный сертификат – выполняется импорт сертификата, полученного из Центра Сертификации. Появляется окно, аналогичное окну, описанному выше (Рисунок 27).
Буфер обмена может использоваться для сертификатов в формате Base64.

Далее появится окно (Рисунок 28), в котором надо выбрать свой сертификат.

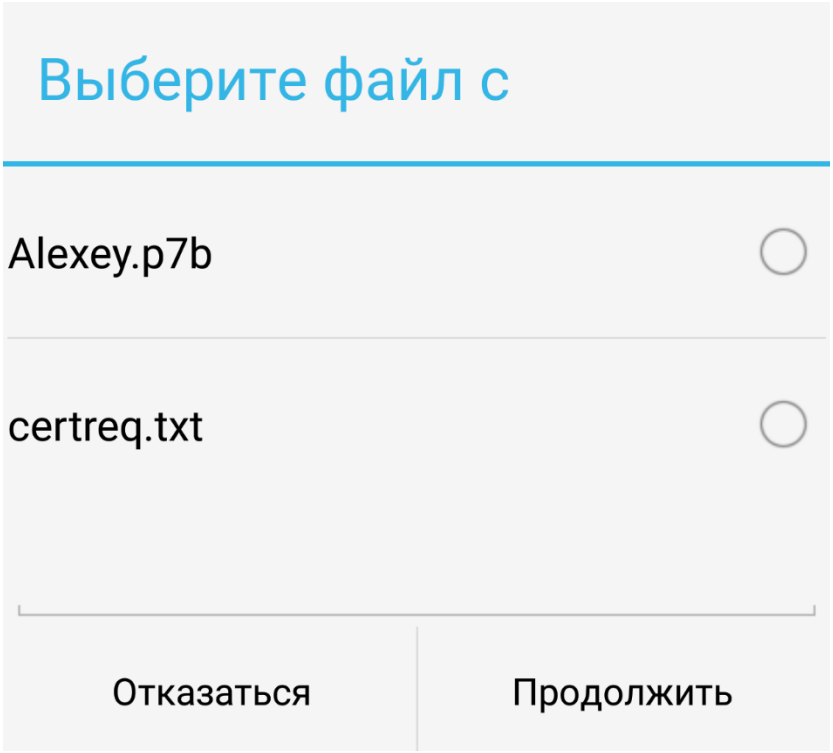

Рисунок 28

Выберите файл с сертификатом и нажмите Продолжить. В появившемся окне (Рисунок 29) отобразится Distinguished Name выбранного сертификата. Установите флажок и нажмите Продолжить, чтобы импортировать сертификат.

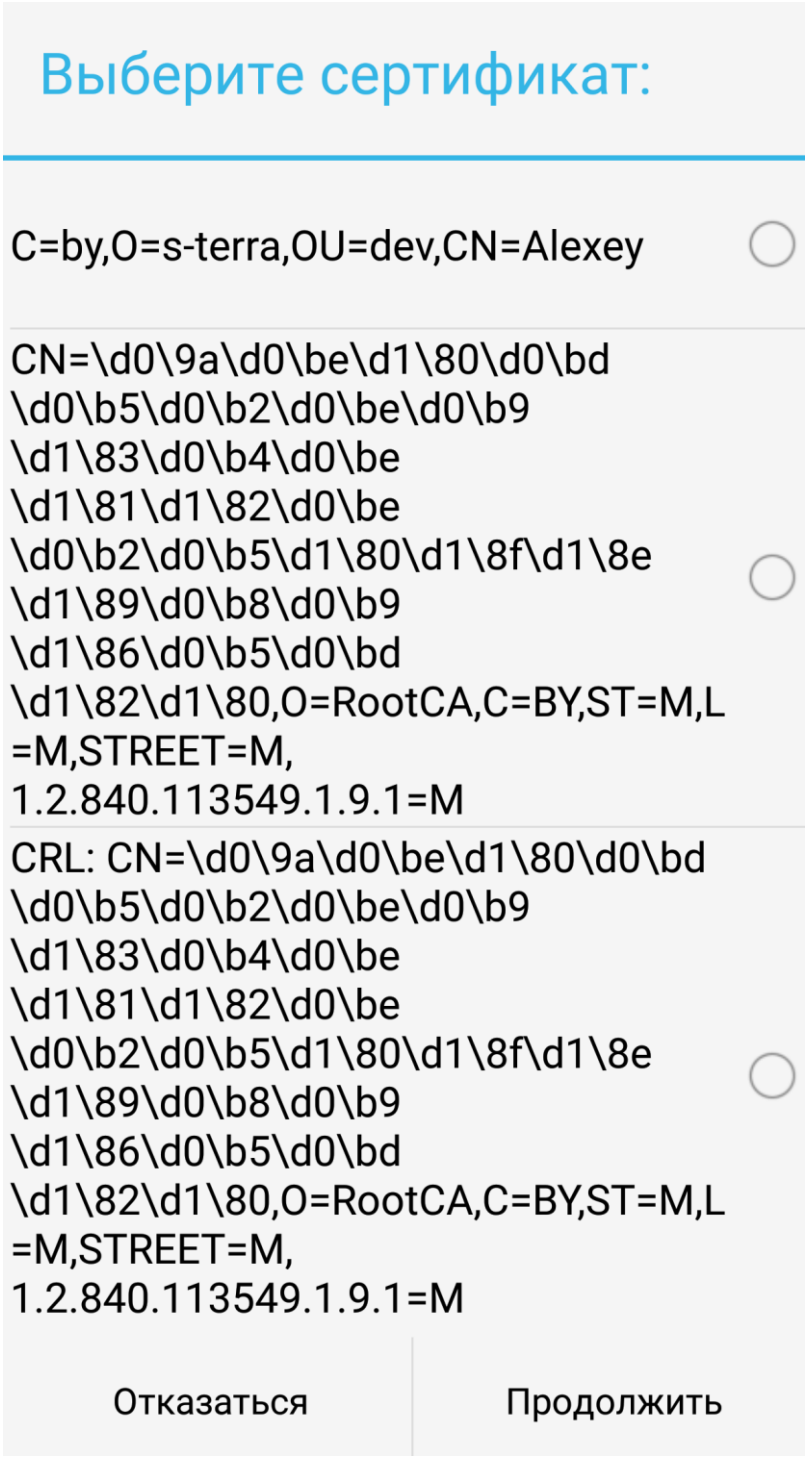

Рисунок 29

Импортировать партнерский сертификат или CRL – предлагается выбрать партнерский сертификат или CRL для регистрации в базе Продукта. Появляется окно, подобное окну на (Рисунок 27), в котором предлагается выбрать способ получения сертификата.

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

6.5. 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 30).

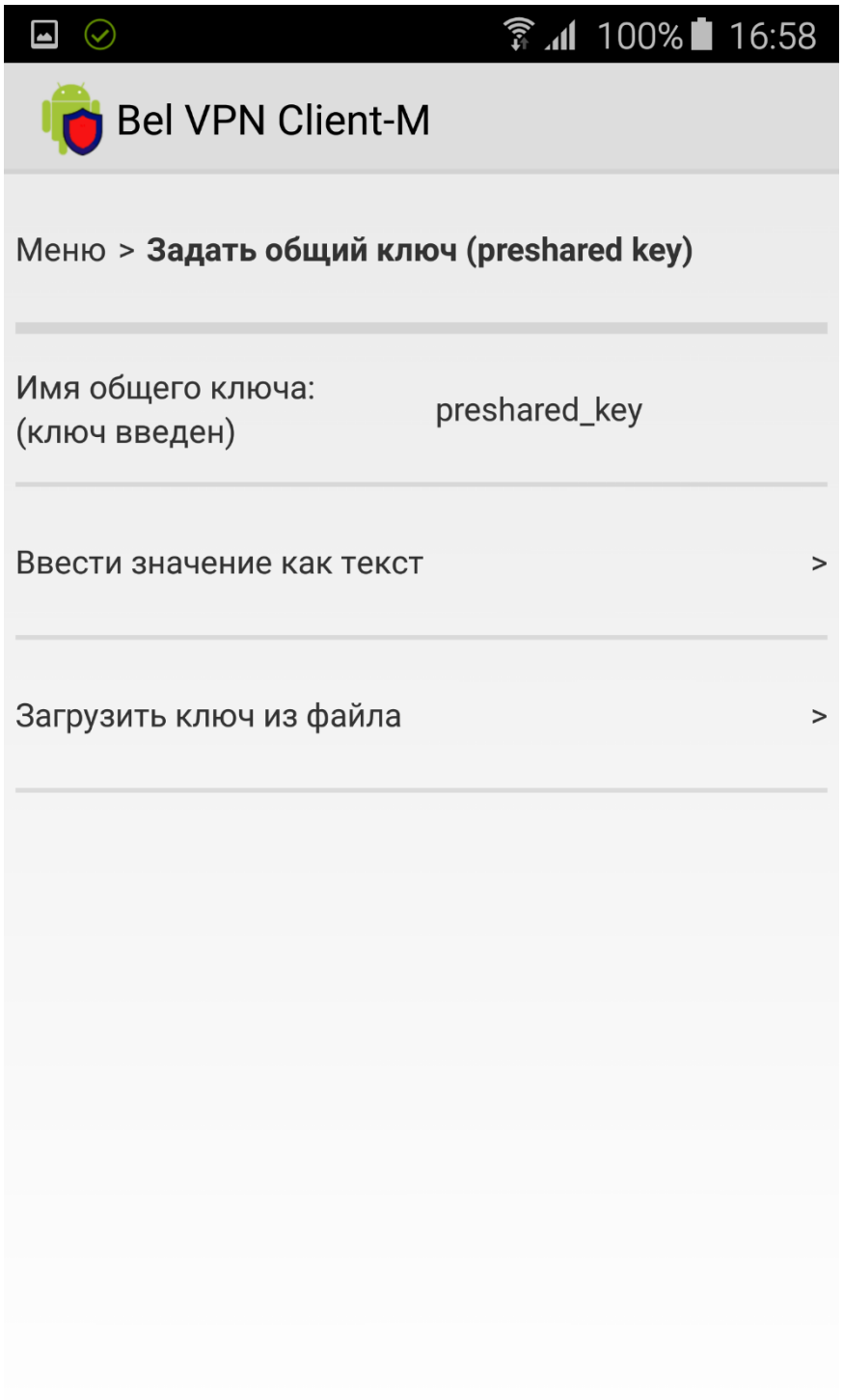

Рисунок 30

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.

6.6. Настройки протоколирования

В разделе **Настройки протоколирования** (Рисунок 31) можно задать протоколирование событий по протоколу Syslog и указать адрес сервера, куда будут отправляться эти сообщения.

Уровень важности (Severity) протоколируемых событий соответствует уровню debug.

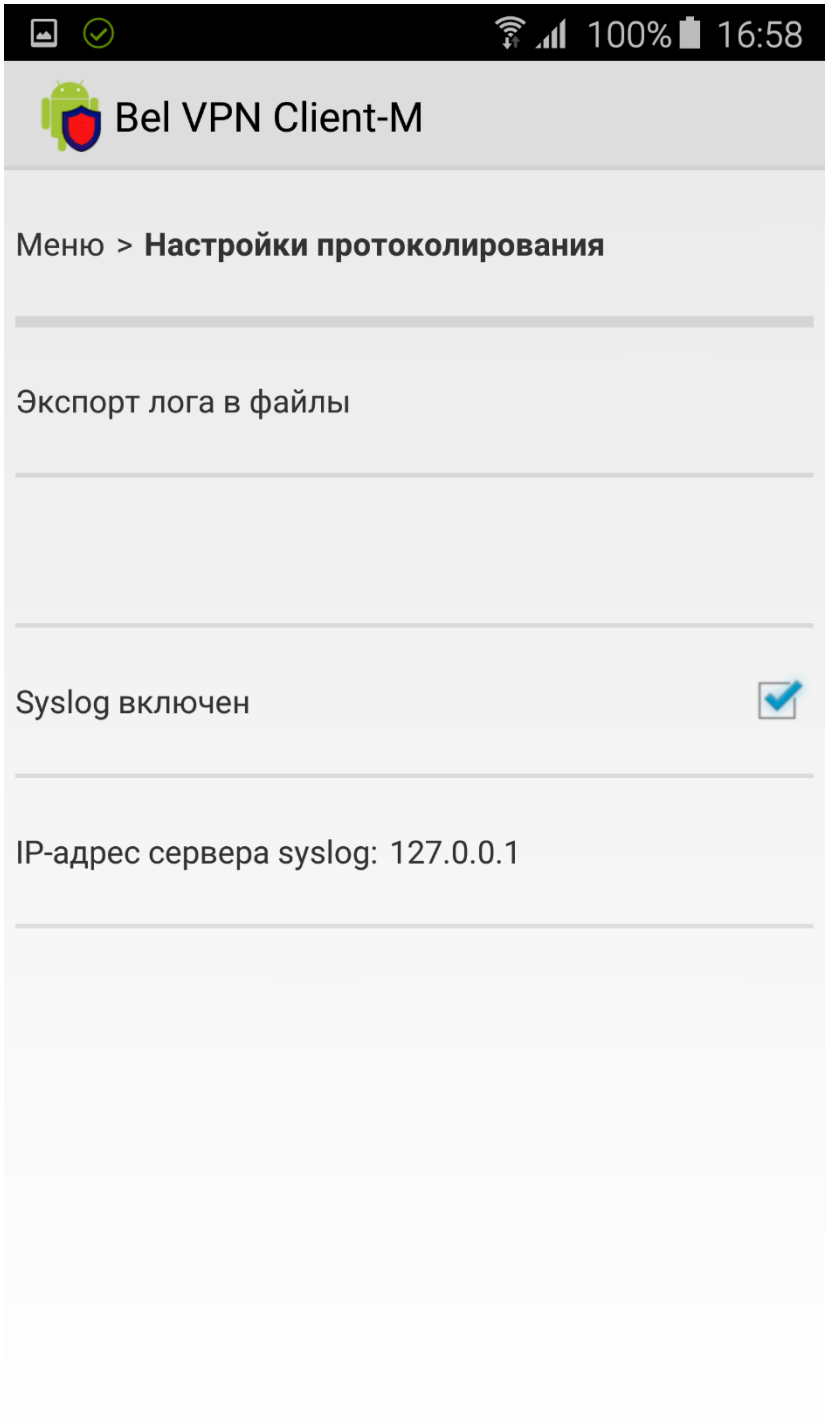

Рисунок 31

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 умолчания 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.

7. Деинсталляция «Программного комплекса Bel VPN Client-M»

Перед деинсталляцией «Bel VPN Client-M» необходимо остановить службу VPN. Для этого войдите в «Bel VPN Client-M» 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 «Bel VPN Client-M» производится стандартными средствами операционной системы. Войдите в *Настройки*, выберите *Диспетчер приложений –> Управление приложениями*. Выберите приложение Bel VPN Client-M и действие *Удалить*.

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

При создании защищенного соединения будет выдан запрос на подтверждение установления VPN-соединения (Рисунок 32).

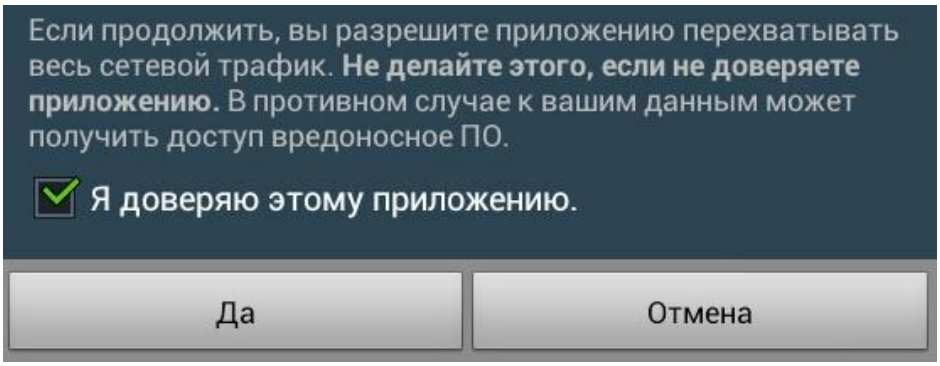

Рисунок 32

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.

9. Приложение

9.1. Настройка «Bel VPN Client-M» с использованием конфигурационного файла

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

Особенности настройки

1. Если в конфигурационном файле Bel VPN 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.
   Платформ Android, не поддерживает настройку iptables, фильтры InputFilter и OutputFilter не поддерживаются.
4. Структура RoutingTable для Bel VPN Client-M не поддерживается.
5. Структура AHProposal для Bel VPN Client-M не поддерживается.

9.2. Особенности настройки шлюза при работе с программным продуктом «Клиент безопасности мобильный Bel VPN Client-M 4.1

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

- Получение Bel VPN 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 Bel VPN Client-M не выставится.

    Фрагмент LSP на Bel VPN Gate:

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

  - Bel VPN Gate может передавать произвольное количество DNS-серверов, но сколько будет реально использоваться, зависит от типа устройства и версии прошивки. Если Bel VPN 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).

Описание конфигурационного файла для Bel VPN Gate смотрите на сайте ….

9.3. 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 Bel VPN Client-M using Android application manager	Пожалуйста, удалите Bel VPN 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 Bel VPN 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	
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	
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.	

9.4. Состояние служб IKE/IPsec

Таблица 2

Политика по умолчанию	Сообщение	Пояснение
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
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	
passall	не сконфигурирован сетевая защита отключена	LSP отсутствует в базе локальных настроек

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

- passall – пропускать все;
- error – неизвестно (аварийная ситуация);
- na – неприменима (в случае APK для прочих устройств – несовместимых);
- пустая ячейка – не зависит от политики по умолчанию.

