

УТВЕРЖДЕНО
ВУ.РТНК.45004-01 34 01-ЛУ

Программный продукт
«Клиент безопасности мобильный
Bel VPN Client-M 4.5»

Руководство пользователя
ВУ.РТНК.45004-01 34 01

Листов 63

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

Содержание

1. Комплект поставки.....	7
2. Требования к программно-аппаратным средствам.....	8
3. Назначение и функции продукта.....	9
4. Установка и инициализация продукта	10
5. Запуск продукта	14
5.1. Запуск Bel VPN Client-M.....	14
5.2. Регистрация пользователя.....	15
6. Начальная настройка продукта	17
6.1. Переход на экран Настройки	17
6.2. Формирование запроса на сертификат	17
6.3. Импорт сертификатов.....	21
6.4. Создание политики безопасности	25
6.5. Создание защищенного соединения	27
7. Использование продукта.....	30
7.1. Интерактивный режим логина пользователя.....	30
7.2. Лицензионная информация	31
8. Описание элементов меню главного экрана	32
8.1. Главный экран Bel VPN Client-M	32
8.2. Настройки	33
8.3. Информация о соединении	33
8.4. Сменить пароль	34
8.5. Сменить пользователя	35
8.6. Автоблокировка.....	35
8.7. Протоколирование	36
8.8. Обновить лицензию	36
8.9. О приложении	38
8.10. Выход.....	38
9. Описание элементов экрана Настройки	39
9.1. Переход на экран Настройки	39
9.2. Раздел Конфигурация IKE/IPsec.....	39
9.3. Раздел Сертификаты.....	45
9.4. Раздел Задать общий ключ (preshared key).....	52
9.5. Раздел Протоколирование.....	52
9.6. Переключатель Темная тема.....	54

9.7. Переключатель Анимация.....	55
9.8. Переключатель Звуковые уведомления	55
9.9. Переключатель Биометрическая аутентификация	56
10. Деинсталляция продукта.....	57
11. Приложение. Настройка Bel VPN Client-M с использованием конфигурационного файла	58



Лицензионное Соглашение
о праве пользования программным продуктом
«Bel VPN Client-M 4.5»
производства ООО «С-Терра Бел»

© 2008 – 2020 ООО «С-Терра Бел». Все права защищены.

Настоящее Лицензионное Соглашение определяет условия использования законно приобретенного программного продукта «Клиент безопасности мобильный Bel VPN Client-M 4.5» (далее – Продукт) Конечным Пользователем (физическим или юридическим лицом, указанным в Лицензии на использование Продукта, являющейся неотъемлемой частью Продукта). Предметом настоящего Лицензионного Соглашения является возмездная передача Конечному Пользователю неисключительных прав использования Продукта на территории Республики Беларусь.

Под Продуктом понимается комплекс объектов (программного кода Продукта и документации на него в печатной и электронной формах), включенных в Комплект поставки Продукта.

Продукт может использоваться только в качестве персонального средства защиты (устанавливаться на персональное мобильное устройство пользователя — смартфон или планшет) и не предназначено для использования в других целях. Использование Продукта в прочих продуктах и/или в иных целях является нарушением настоящего Лицензионного Соглашения.

Продукт может включать компоненты (программные модули 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.

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

Продукт и его компоненты являются интеллектуальной собственностью Производителя (ООО «С-Терра Бел») и, при наличии третьих поставщиков, интеллектуальной собственностью третьих поставщиков и защищаются законодательством Республики Беларусь об авторском праве на объекты интеллектуальной собственности.

Установка Продукта после предъявления Конечному Пользователю Лицензионного Соглашения рассматривается как согласие Конечного Пользователя с условиями Лицензионного Соглашения и вступлением 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 Продукта.

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 Продукта. Конечный Пользователь имеет право на копирование, установку и использование всех компонент третьих поставщиков, поставленных в составе Продукта только в составе работ, связанных с использованием Продукта. Копирование, распространение, установка и использование отдельных компонент Продукта 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 Продукта и не имеет права устанавливать и использовать большее количество экземпляров Продукта.

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

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

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

Неисполнение требований настоящего Лицензионного Соглашения является нарушением Закона Республики Беларусь "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 при использовании Продукта Конечным Пользователем или любым третьим лицом будет обнаружена Критичная Проблема, Производитель Продукта обеспечивает¹:
 - а) информирование доступными способами Конечного Пользователя о существовании Критичной Проблемы и о способах ее устранения
 - б) бесплатное предоставление обновлений программного обеспечения Производителя Продукта, в которых устранены Критичные Проблемы².
2. Если Конечный Пользователь обнаружит в течение 90 (девяноста) дней со дня поставки Продукта дефекты в составе информационных носителей или некомплектность Продукта, то информационные носители будут заменены, а комплектность Продукта восстановлена. По истечении 90 дней претензии Конечного Пользователя по некомплектности Продукта и/или дефектам носителей информации рассматриваться не будут.

Настоящее Лицензионное Соглашение не содержит никаких гарантий по поставке, функциональности и соответствию Продукта любым техническим требованиям, стандартам и условиям. Эти вопросы относятся к области лицензирования деятельности поставщика, сертификации Продукта 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 использованием Продукта и возможных материальных, финансовых и прочих потерь Конечного Пользователя в результате использования Продукта.

Срок действия настоящего Лицензионного Соглашения распространяется на весь период использования Продукта Конечным Пользователем. В случае использования лицензии с ограниченным сроком действия - на срок, указанный в лицензии. Действие настоящего Лицензионного Соглашения может быть прекращено по решению Конечного Пользователя. В этом случае Конечный Пользователь должен уничтожить все информационные носители, содержащие программный код и прочие компоненты Продукта. Прекращение действия Лицензионного Соглашения по инициативе Конечного Пользователя является односторонней добровольной акцией Конечного Пользователя и не является предметом для взаиморасчетов и других хозяйственных операций.

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

1 Гарантийное обязательство по п.1а базируется на следующем определении: Критичная Проблема заключается в том, что Продукт, 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.

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

Java является торговой маркой корпорации Oracle.

Другие названия компаний и продуктов, упомянутые в настоящем Лицензионном Соглашении и в составе информационных источников Продукта 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, пом. 611

Телефон: (+375 17) 280 6000

Эл. почта: info@s-terra.by

<https://s-terra.by>

1. Комплект поставки

В комплект поставки программного продукта «Клиент безопасности мобильный Bel VPN Client-M 4.5» (далее – Bel VPN Client-M) входит:

№ пп	Элемент комплекта	Пояснения
1	Файл «S-Terra_Bel_Client-M_4.5.apk»	архивный исполняемый файл-приложение для ОС
2	Файл «BelVPN_Client-M_4-5_User_Guide.pdf»	документ «Программный продукт «Клиент безопасности мобильный Bel VPN Client-M 4.5». Руководство пользователя» в электронном виде
3	Сертификат соответствия техническому регламенту Республики Беларусь	заверенная копия документа на бумажном носителе
4	Лицензия на использование экземпляра Bel VPN Client-M	набор данных пользователя продукта, передаваемый на любом носителе или в электронном виде

2. Требования к программно-аппаратным средствам

Bel VPN Client-M может функционировать на устройствах, работающих под управлением операционной системы Android (далее – ОС Android)³.

Возможность использования Bel VPN Client-M протестирована⁴ на следующих версиях ОС Android:

- Android 5.0 – 5.1.1 (API 21, 22);
- Android 6.0 – 6.0.1 (API 23);
- Android 7.0 – 7.1.2 (API 24, 25);
- Android 8.0 – 8.1 (API 26, 27);
- Android 9.0 (API 28);
- Android 10.0 (API 29).

3 Под управлением ОС Android работают разнообразные устройства от множества производителей. Перед использованием Bel VPN Client-M рекомендуется провести тестирование предполагаемых к использованию устройств на совместимость с продуктом.

4 По состоянию на 1 июня 2020 г.

3. Назначение и функции продукта

Программный продукт Bel VPN Client-M предназначен для создания защищенного VPN соединения между устройством, на котором он установлен, и взаимодействующим с ним шлюзом безопасности Bel 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 ключей (предопределенных⁵ или электронной цифровой подписи) в рамках протокола IKE;
- выполняет генерацию данных аудита и вывод на syslog-сервер (локальный или удаленный).

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.

В Bel VPN Client-M реализованы требования следующих стандартов Республики Беларусь:

- | | |
|---|--|
| - шифрование | СТБ 34.101.31-2011 (пункт 6.4) |
| - имитозащита | СТБ 34.101.31-2011 (пункт 6.6) |
| - формирование общего ключа | СТБ 34.101.66-2014 (приложение А) |
| - запрос на получение сертификата открытого ключа | СТБ 34.101.17-2012
СТБ 34.101.78-2019 (пункт 8.2)
СТБ 34.101.45-2013 (пункт 6.2) |
| - распространение сертификата открытого ключа | СТБ 34.101.19-2012 (разделы 6, 8)
СТБ 34.101.78-2019 (пункт 8.3) |
| - проверка статуса сертификата открытого ключа (списки отозванных сертификатов) | СТБ 34.101.19-2012 (раздел 7)
СТБ 34.101.78-2019 (пункт 8.5) |
| - генерация псевдослучайных чисел | СТБ 34.101.47-2017 (пункт 6.2) |
| - требования безопасности к программным СКЗИ | СТБ 34.101.27-2011 (класс 1) |

5 Предопределенный ключ – произвольная последовательность символов.

4. Установка и инициализация продукта

4.1. Установка

1. Скопируйте на устройство файл с дистрибутивом Bel VPN Client-M (S-Terra_Bel_VPN_Client-M_4.5.apk).
2. На устройстве выберите *Настройки* → *Безопасность* и разрешите установку приложений из неизвестных источников.
3. Запустите установку приложения Bel VPN Client-M.
4. При первичном запуске проведите инициализацию Bel VPN Client-M.

4.2. Инициализация

1. Для того чтобы одобрить Лицензионное соглашение (Рисунок 1) нажмите кнопку *Принять*. При нажатии кнопки *Отклонить* инициализация приложения прерывается.



Рисунок 1

2. Нажмите кнопку *Разрешить* (Рисунок 2) и предоставьте приложению доступ к данным на внутреннем накопителе. На SD-карте будет создан каталог /S-Terra⁶, где хранятся файлы с лицензией на продукт, открытыми сертификатами, логами и т.п.

⁶ Каталог /S-Terra, создается в Android External Storage Directory. Путь к Android External Storage Directory строго не регламентируется в ОС Android, но на практике обычно находится в /sdcard либо /storage/emulated/0.

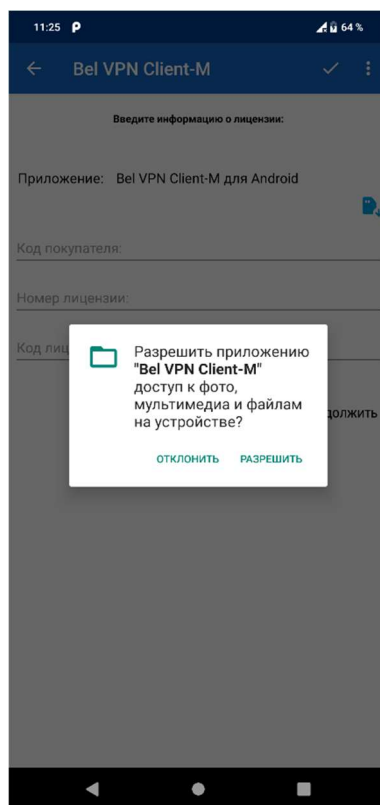


Рисунок 2

3. Заполните графы с информацией о лицензии (Рисунок 3). Нажмите кнопку *Продолжить*.

Лицензионную информацию также можно ввести путем импорта из файла. Описание действий приведено в подразделе 7.2.

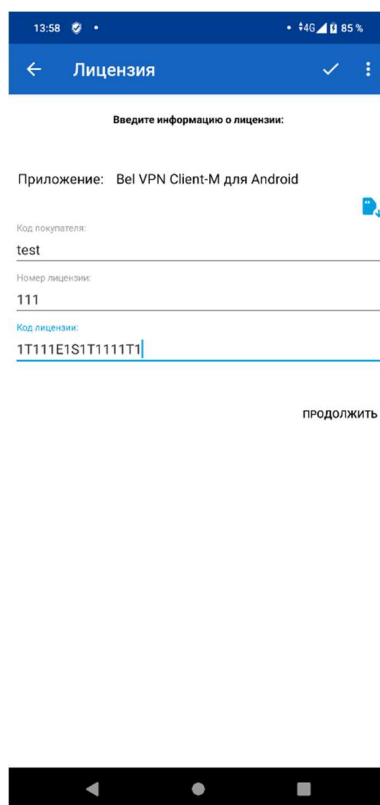


Рисунок 3

4. Далее инициализируется генератор случайных чисел. Для сбора входных данных генератора случайных чисел выберите источник - акселерометр или сенсорный экран (Рисунок 4).

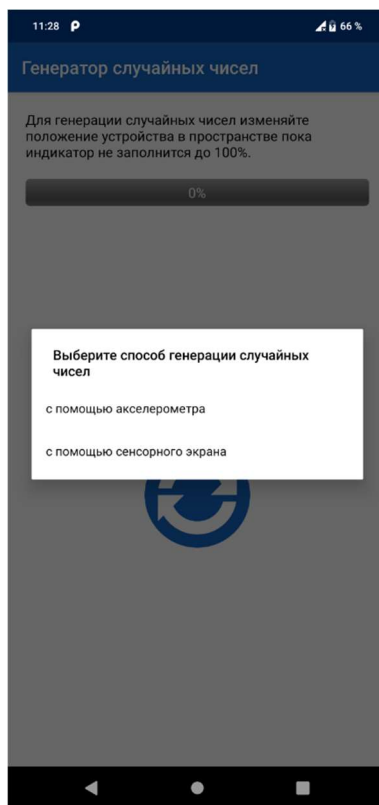


Рисунок 4

5. При использовании акселерометра изменяйте положение устройства в пространстве, пока выполняется инициализация (Рисунок 5).



Рисунок 5

При использовании сенсорного экрана нажимайте в разных частях экрана пока идет сбор входных данных для генератора случайных чисел (Рисунок 6).

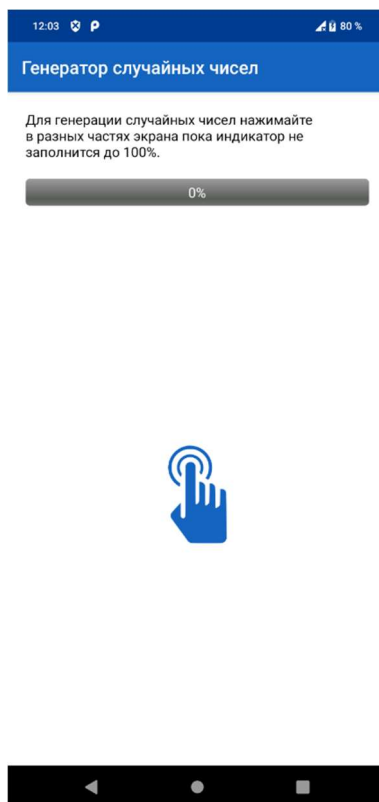


Рисунок 6

6. По завершению процесса инициализации открывается главный экран Bel VPN Client-M.
7. Далее выполните запуск Bel VPN Client-M и необходимые настройки, используя элементы интерфейса пользователя.

5. Запуск продукта

5.1. Запуск Bel VPN Client-M

При запуске Bel VPN Client-M появляется главный экран (Рисунок 7).



Рисунок 7

Изначально доступны только отдельные пункты меню (Рисунок 8) главного экрана. Остальные настройки будут доступны после запуска служб IKE/IPsec.



Рисунок 8

Подробно все элементы меню главного экрана описаны в [Разделе 8](#).
Для начала работы запустите службы IKE/IPsec нажав кнопку *СТАРТ*.

5.2. Регистрация пользователя

После успешного старта служб IKE/IPsec выдается окно логина пользователя (Рисунок 9).

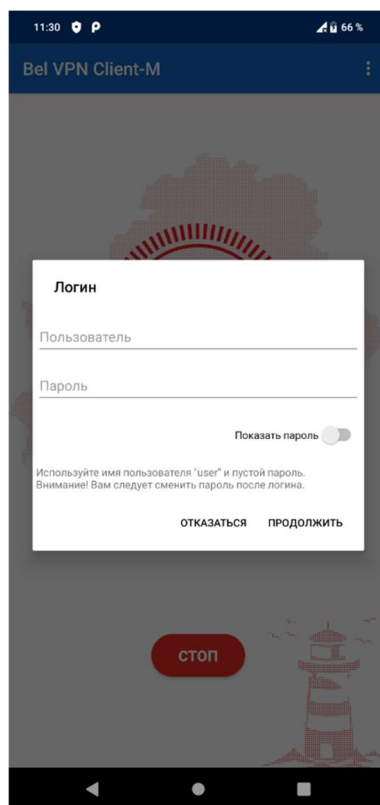


Рисунок 9

Введите имя пользователя, пароль и нажмите кнопку *Продолжить*. Изначально: Пользователь – user, пароль пустой. Эта подсказка появляется в окне логина, пока не изменится имя пользователя и/или его пароль.

Если нажать кнопку *Отказаться*, то регистрация пользователя не выполнится, Bel VPN Client-M не запустится, а службы IKE/IPsec будут остановлены. Для последующих попыток логина надо снова нажать кнопку *СТАРТ*.

При успешном логине пользователя будет выведено информационное сообщение, что логин произведен.

6. Начальная настройка продукта

6.1. Переход на экран Настройки

После запуска служб IKE/IPsec (запускаются нажатием кнопки *СТАРТ*) на панели действий появляется иконка в виде шестеренки для перехода на экран настройки основных параметров. Также перейдите на данный экран возможно выбрав на главном экране пункт меню *Настройки*.

С помощью экрана Настройки задается (редактируется) локальная политика безопасности продукта (далее - конфигурация IKE/IPsec), производится управление сертификатами или общим ключом, включается протоколирование событий, осуществляется конфигурирование пользовательского интерфейса. Кроме того, на экране настройки отображается текущее состояние всех основных элементов настройки (Рисунок 10).

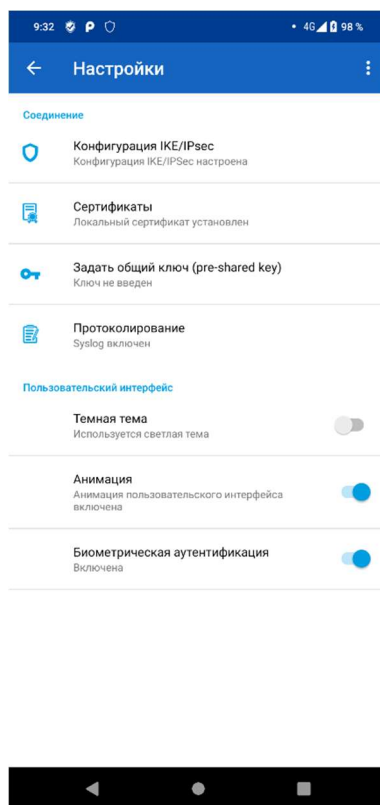


Рисунок 10

Для первоначальной настройки Bel VPN Client-M необходимо сформировать запрос на сертификат, импортировать запрошенный сертификат, сертификат открытого ключа удостоверяющего центра (далее - УЦ) и создать конфигурацию IKE/IPsec.

6.2. Формирование запроса на сертификат

1. На экране *Настройки* выберите раздел [Сертификаты](#), затем *Запрос на сертификат* (Рисунок 11).

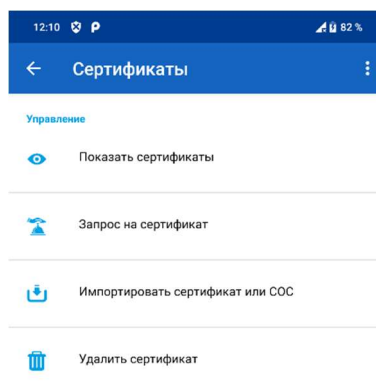


Рисунок 11

2. В появившемся окне заполните поле *Subject DN* для *сертификата* и нажмите кнопку *Продолжить* (Рисунок 12). Например: C=BY, O=MyCompany, CN=MyName.

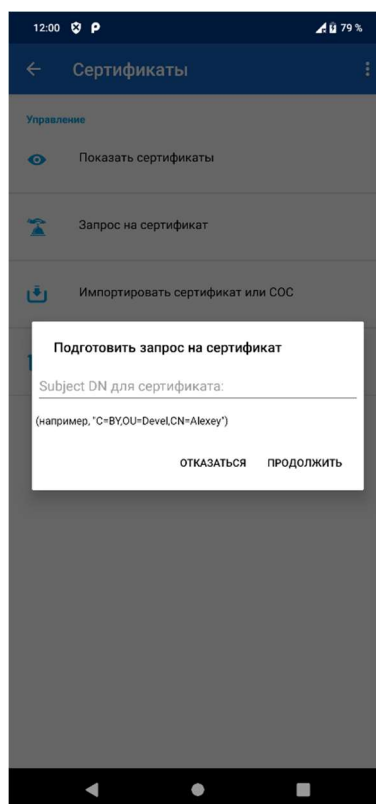


Рисунок 12

3. Далее инициализируется генератор случайных чисел. В случае отсутствия в мобильном устройстве акселерометра для сбора входных данных генератора случайных чисел выберите сенсорный экран (Рисунок 4).

4. Изменяйте положение устройства в пространстве, пока выполняется инициализация (Рисунок 5).
5. Выберите способ доставки сертификата администратору УЦ (Рисунок 13).

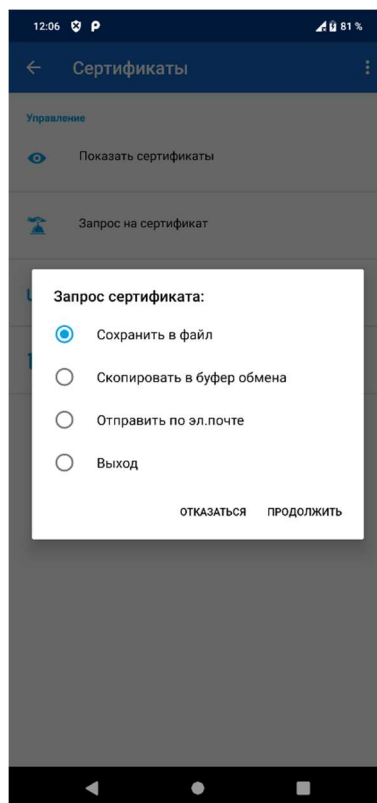


Рисунок 13

В случае, если запрос на сертификат сохраняется в файл, то он будет размещен в папке /S-Terra⁷.

Если выбрать пункт *Отправить по эл. почте*, то появится диалоговое окно где нужно будет указать подходящую для отправки запроса почтовую программу/Viber/Skype и т.п. (Рисунок 14).

⁷ Каталог /S-Terra, создается в Android External Storage Directory. Путь к Android External Storage Directory строго не регламентируется в ОС Android, но на практике обычно находится в /sdcard либо /storage/emulated/0.

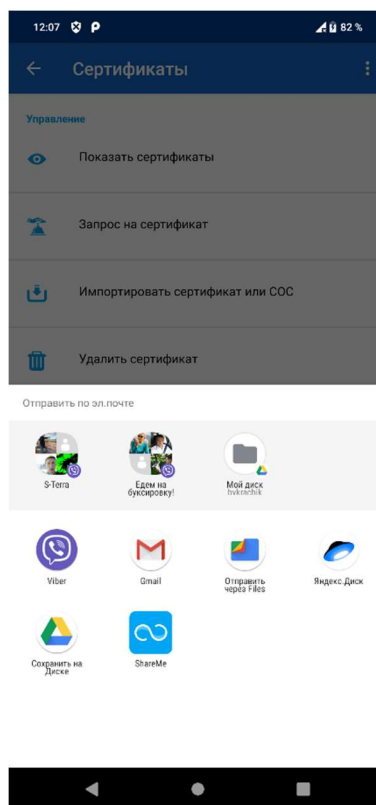


Рисунок 14

В сформированном сообщении необходимо будет выбрать из списка получателя или ввести его адрес вручную и подтвердить отправку (Рисунок 15).

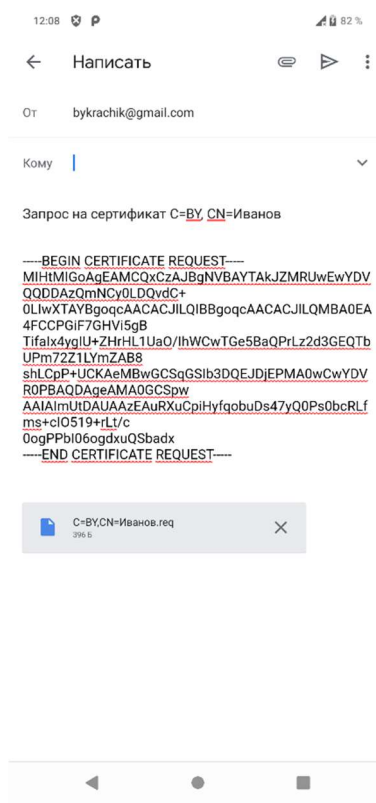


Рисунок 15

6.3. Импорт сертификатов

Импорт сертификатов из файлов

1. Скопировать полученные сертификаты⁸ в папку /S-Terra⁹.
2. С основного экрана перейдите в *Настройки* и выберите раздел *Сертификаты*. Затем - *Импортировать сертификат или СОС*.
3. В появившемся меню выберите пункт *Сертификат открытого ключа УЦ* (Рисунок 16).

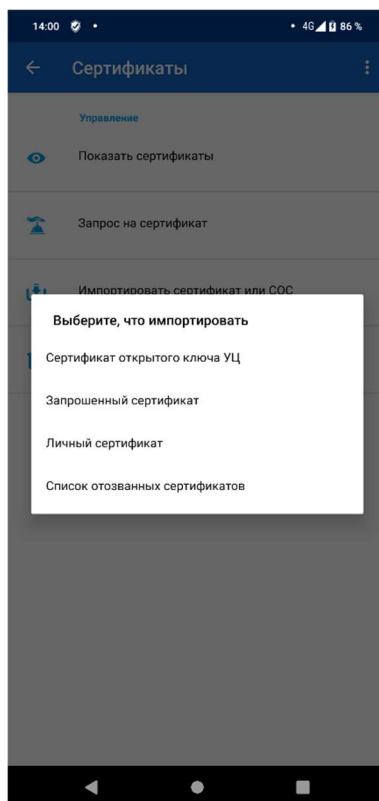


Рисунок 16

4. В появившемся меню выберите пункт *Добавить из файла* (Рисунок 17).

⁸ Сертификат открытого ключа УЦ и запрошенный сертификат (локальный сертификат)

⁹ Каталог /S-Terra, создается в Android External Storage Directory. Путь к Android External Storage Directory строго не регламентируется в ОС Android, но на практике обычно находится в /sdcard либо /storage/emulated/0.

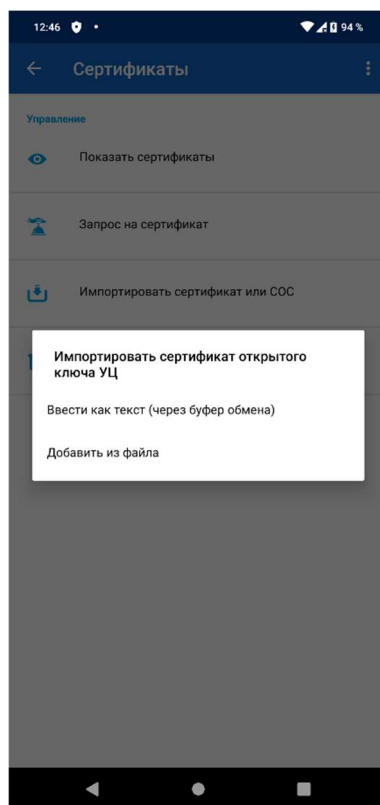


Рисунок 17

5. В появившемся меню выберите сертификат открытого ключа УЦ, который ранее был скопирован в папку /S-Terra¹⁰ и нажмите кнопку *Продолжить* (Рисунок 18).

¹⁰ Каталог /S-Terra, создается в Android External Storage Directory. Путь к Android External Storage Directory строго не регламентируется в ОС Android, но на практике обычно находится в /sdcard либо /storage/emulated/0.

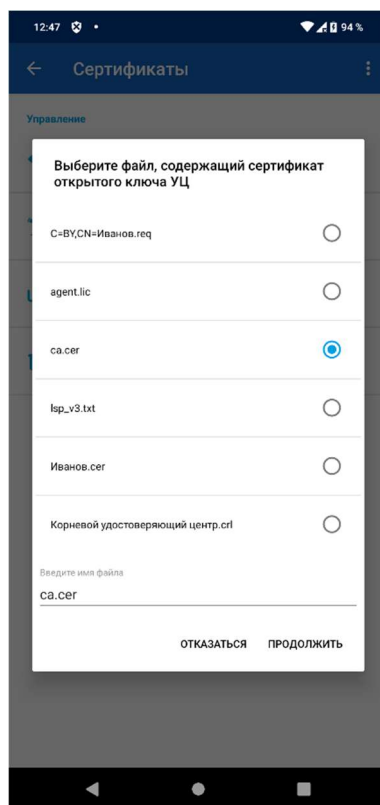


Рисунок 18

6. В следующем диалоговом окне подтвердить выбранный сертификат нажатием кнопки *Продолжить* (Рисунок 19).

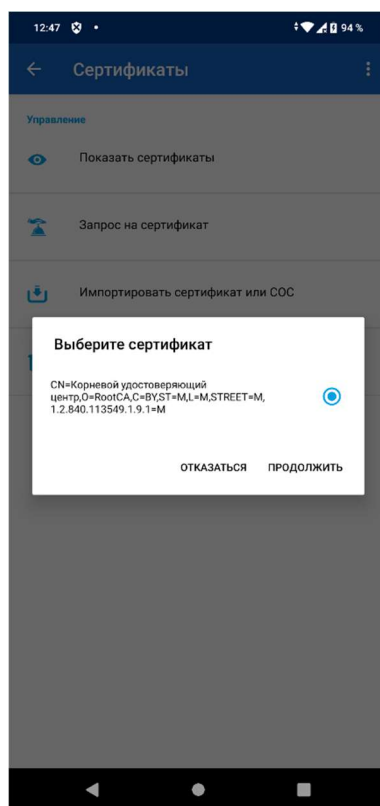


Рисунок 19

7. После успешного завершения операции импорта в нижней части экрана будет выведено информационное уведомление (Рисунок 20).

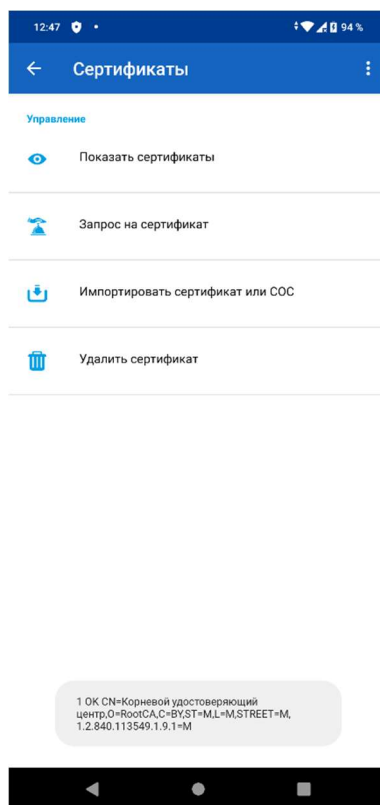


Рисунок 20

8. На экране *Сертификаты* снова выберите пункт *Импортировать сертификат или СОС*. В появившемся меню выберите пункт *Запрошенный сертификат* (Рисунок 16).
9. Проведите процедуру импорта запрошенного сертификата (локального сертификата) аналогично импорту сертификата открытого ключа УЦ (п.4-7).
10. При наличии списка отозванных сертификатов (далее – СОС) его импорт производится аналогично импорту сертификатов (п.3-7). При этом в меню выбора типа сертификатов необходимо указать пункт *Список отозванных сертификатов* (Рисунок 16).

Импорт сертификатов, полученных по электронной почте

1. Перед импортом сертификатов, полученных по электронной почте/Viber/Skype и т.п., необходимо запустить службы IKE/IPsec. Для этого нажмите на главном экране Bel VPN Client-M кнопку *СТАРТ*.
2. Перейдите в почтовую программу, в полученном сообщении нажмите на файл с прикрепленным сертификатом открытого ключа УЦ.
3. В появившемся диалоговом окне выберите¹¹ *Открыть с помощью приложения "Bel VPN Client-M (импорт сертификатов)"* и нажмите кнопку *Только сейчас* (Рисунок 21).

¹¹ В отдельных случаях файлы с определенными расширениями могут по умолчанию открываться другими приложениями. Для того чтобы отменить это действие и перевести его в интерактивный режим выберите в ОС Андроид *Настройки -> Приложения -> соответствующее приложение* (Например, *Документы*) -> *Открывать по умолчанию -> Удалить настройки по умолчанию*.

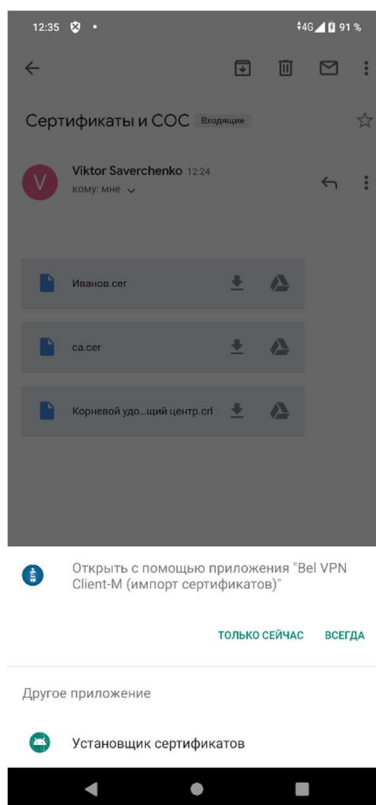


Рисунок 21

4. Сертификат передается в Bel VPN Client-M и импортируется в базу данных аналогично процедуре [импорта сертификатов из файлов](#) (п.3-7).

Аналогичным способом импортируются запрошенный сертификат и СОС.

6.4. Создание политики безопасности

Упрощенная конфигурация

1. С основного экрана Bel VPN Client-M перейдите [на экран Настройки](#) и выберите [раздел Конфигурация IKE/IPsec](#) (Рисунок 22).

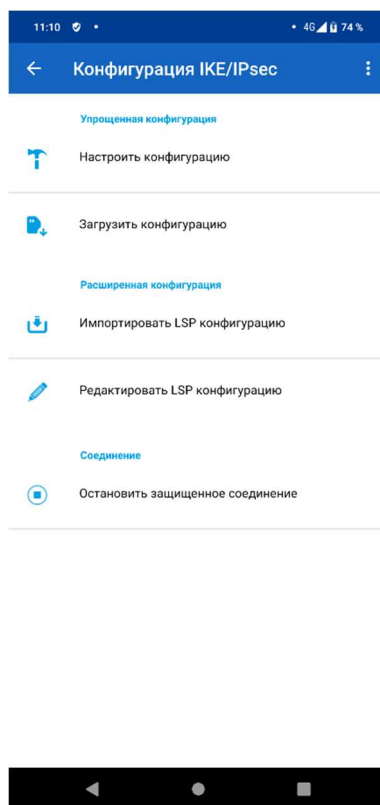


Рисунок 22

2. Выберите пункт *Настроить конфигурацию*.
3. В поле *Защищенный шлюз* введите IP адрес шлюза, защищающего подсеть, с которой строится защищенное соединение. В поле *Защищаемые подсети* укажите адреса подсетей, к которым необходим удаленный доступ. Адреса вводятся через запятую, с указанием маски подсети. Например: 192.168.101.10/24, 192.168.102.0/24 (Рисунок 23).

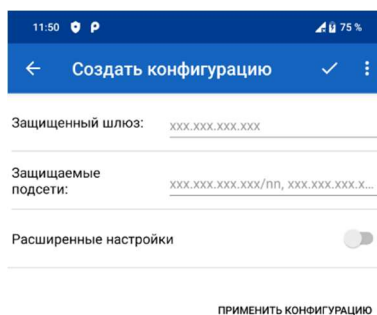


Рисунок 23

4. Нажмите кнопку *Применить конфигурацию*.
5. После успешного завершения операции создания конфигурации на экране будет выведено соответствующее информационное уведомление.

Другие варианты создания конфигурации описаны в [разделе Конфигурация IKE/IPsec](#).

Импорт конфигурации, полученной по электронной почте

1. Перед импортом конфигурации, полученной по электронной почте/Viber/Skype и т.п., необходимо запустить службы IKE/IPsec. Для этого нажмите на главном экране Bel VPN Client-M кнопку *СТАРТ*.
2. Перейдите в почтовую программу, в полученном сообщении нажмите на прикрепленный конфигурационный файл.
3. В появившемся диалоговом окне выберите¹² *Открыть с помощью приложения Bel VPN Client-M (импорт конфигурации)* и нажмите кнопку *Только сейчас* (Рисунок 24).

¹² В отдельных случаях файлы с определенными расширениями могут по умолчанию открываться другими приложениями. Для того чтобы отменить это действие и перевести его в интерактивный режим выберите в ОС Андроид *Настройки -> Приложения -> соответствующее приложение* (Например, *Документы*) -> *Открывать по умолчанию -> Удалить настройки по умолчанию*.

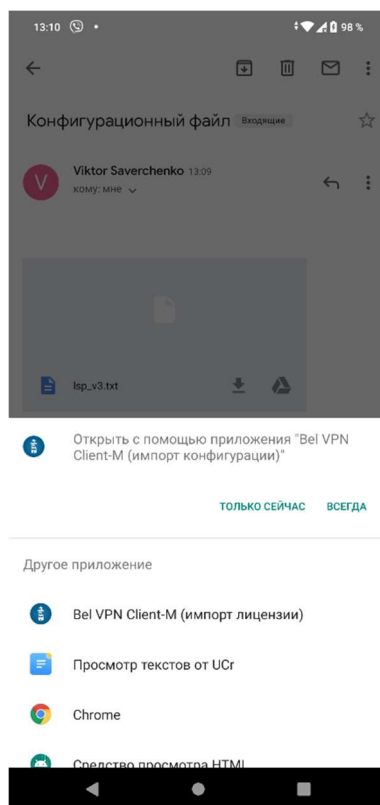


Рисунок 24

4. Далее конфигурация передается в Bel VPN Client-M, выводится на экран и импортируется в базу данных после нажатия на кнопку *Применить*.

6.5. Создание защищенного соединения

При создании защищенного соединения будет выдан запрос на подтверждение установления VPN-соединения (Рисунок 25).

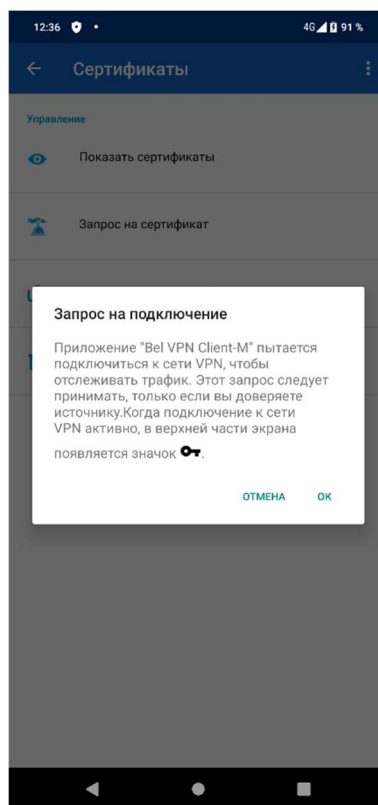


Рисунок 25

Разрешите установление VPN-соединения. В противном случае защищенное соединение не будет установлено. 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.

Пользовательский интерфейс ОС Android предполагает возможность ручного разрыва 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 остановить службы IKE/IPsec (нажмите на главном экране кнопку *СТОП*).

В новых версиях ОС Android (9.0 и выше) появилась возможность блокирования любых соединений без VPN. Для этого выберите в ОС Android *Настройки* -> *Сети и Интернет* (или *Беспроводные сети*) -> *Дополнительно* (или *Еще*) -> *VPN* -> *Bel VPN Client-M* -> нажмите на значок шестеренки -> *Постоянный VPN* + *Блокировать соединения без VPN* (Рисунок 26).

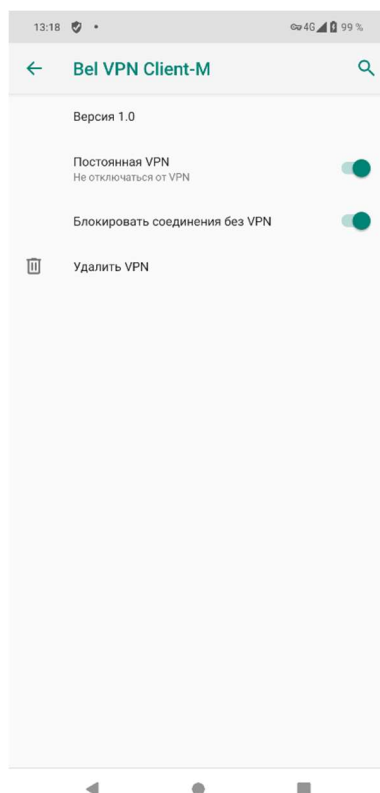


Рисунок 26

7. Использование продукта

7.1. Интерактивный режим логина пользователя

После успешного старта служб IKE/IPsec выдается окно логина (Рисунок 27).

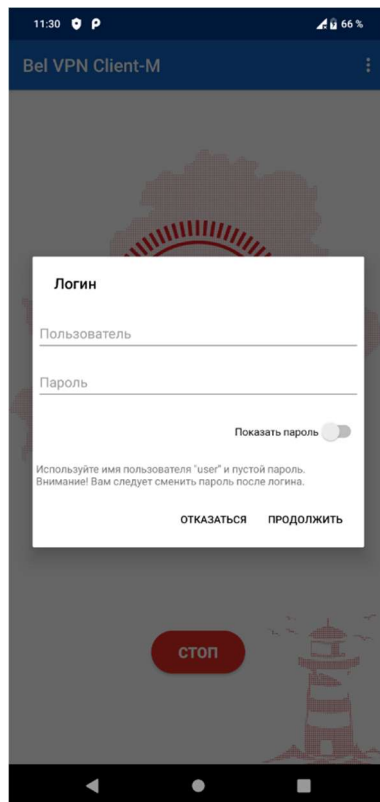


Рисунок 27

Введите имя пользователя, пароль и нажмите кнопку *Продолжить*. Изначально: Пользователь – user, пароль пустой. Эта подсказка появляется в окне логина, пока не изменится пользователь и/или пароль.

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

В случае ввода неправильного имени пользователя или пароля будет предложено повторить попытку. 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* Bel VPN Client-M не запустится, а службы IKE/IPsec будут остановлены.

Допускаются десять неудачных попыток логина подряд. Затем будет выдано сообщение, что пользователь заблокирован и нормальная работа с приложением в данной случае будет невозможна.

Решить проблему можно следующим образом:

1. В *Настройках* ОС Android войти в раздел *Приложения*.
2. Выберите приложение *Bel VPN Client-M*.
3. Войти в *Хранилище*.
4. Нажмите на кнопку *Стереть данные*. Подтвердите удаление данных.

5. Все действующие настройки приложения (данные лицензии, локальная политика безопасности, сертификаты, секретные ключи, начальное значение генератора случайных чисел и т.п.) будут удалены.
6. Далее следует запустите приложение и заново выполнить [инициализацию](#), [запуск](#) и [настройку](#) Bel VPN Client-M.

7.2. Лицензионная информация

Лицензионная информация может вводиться в приложение вручную и из файла.

Если имеется файл с лицензионной информацией импортируйте информацию о лицензии из этого файла с помощью кнопки *Импорт*, которая расположена в верхнем правом углу поля *Код покупателя* (Рисунок 28). Файл должен быть расположен в каталоге /S-Terra¹³.

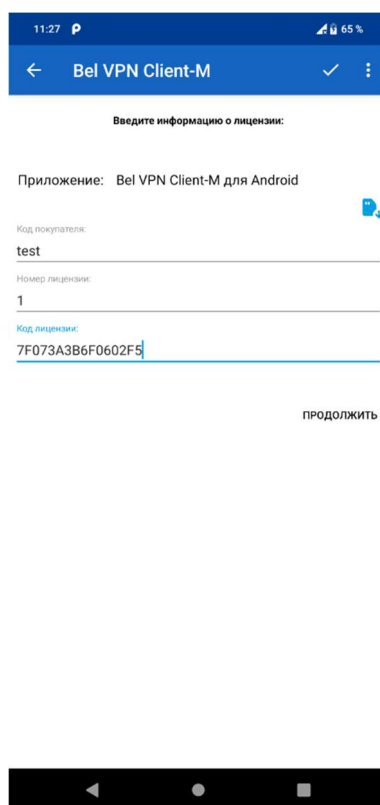


Рисунок 28

Файл с лицензионной информацией должен быть с расширением *.lic (например, client-m.lic) и содержать следующие поля:

```
[license]
CustomerCode=test
ProductCode=CLIENTM
LicenseNumber=111
LicenseCode=1234567890AACDDF
```

В данном файле недопустимы пробелы между названием поля, знаком “=” и значением поля.

¹³ Каталог /S-Terra, создается в Android External Storage Directory. Путь к Android External Storage Directory строго не регламентируется в ОС Android, но на практике обычно находится в /sdcard либо /storage/emulated/0.

8. Описание элементов меню главного экрана

8.1. Главный экран Bel VPN Client-M

При запуске Bel VPN Client-M появляется главный экран (Рисунок 29).



Рисунок 29

На главном экране содержатся следующие элементы:

- меню (в правом верхнем углу панели действий);
- анимированное изображение *Bel VPN* с текущим статусом приложения (по середине экрана);
- кнопка *СТАРТ/СТОП* (внизу экрана), которая используется для запуска или остановки служб IKE/IPsec.

Изначально доступны только отдельные пункты меню (Рисунок 30). Остальные настройки будут доступны после запуска служб IKE/IPsec. Для начала работы Bel VPN Client-M запустите службы IKE/IPsec нажав кнопку СТАРТ.



Рисунок 30

На главном экране могут отображаться следующие статусы приложения:

- Bel VPN соединен (службы IKE/IPsec запущены, защищенное соединение установлено);
- Bel VPN выключен (службы IKE/IPsec не запущены);
- Bel VPN ошибка (службы IKE/IPsec запущены с ошибкой);
- Bel VPN не активен (службы IKE/IPsec в процессе запуска/инициализации);
- Bel VPN не настроен (службы IKE/IPsec запущены, но для установки защищенного соединения необходимо произвести [настройку продукта](#));
- Bel VPN не соединен (службы IKE/IPsec запущены, но защищенное соединение не установлено);
- Bel VPN остановлен (защищенное соединение остановлено по требованиям пользователя, службы IKE/IPsec работают в режиме конфигурирования и диагностики).

8.2. Настройки

Переход к экрану настроек. Элементы меню Настройки описаны в [разделе 9](#).

8.3. Информация о соединении

Переход к экрану с информацией о соединении возможен после запуска служб IKE/IPsec. Для получения информации о защищенном соединении нажмите в центре экрана на круг с надписью Bel VPN или выберите в меню главного экрана пункт *Информация о соединении* (Рисунок 31).

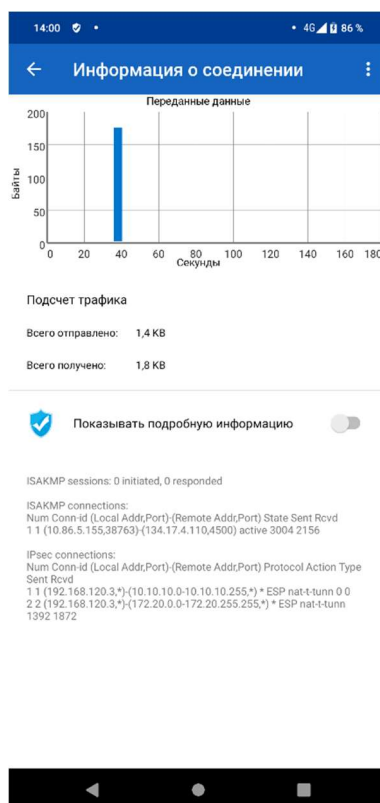


Рисунок 31

8.4. Сменить пароль

Для смены пароля выберите на главном экране соответствующий пункт меню. Появится окно (Рисунок 32). Введите старый пароль, потом новый пароль и повторить его. Нажмите кнопку *Продолжить*.

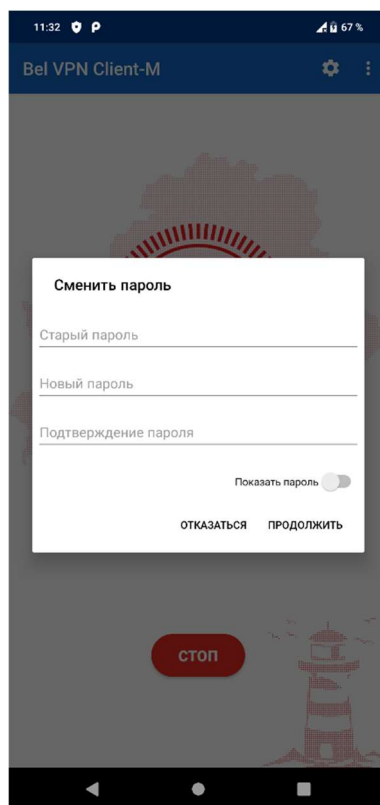


Рисунок 32

По умолчанию пароли не отображаются. Если установить флажок - *Показать пароль*, пароли будут показаны в открытом виде.

В случае успешной смены пароля появится уведомление:

Пароль успешно сменен.

8.5. Сменить пользователя

Для смены пользователя выберите на главном экране соответствующий пункт меню. В появившемся окне (Рисунок 33) введите пароль предыдущего пользователя, имя нового пользователя и два раза новый пароль. По умолчанию пароли не отображаются. Если установить флажок - *Показать пароль*, пароли будут показаны в открытом виде. Имя нового пользователя не должно быть пустым.

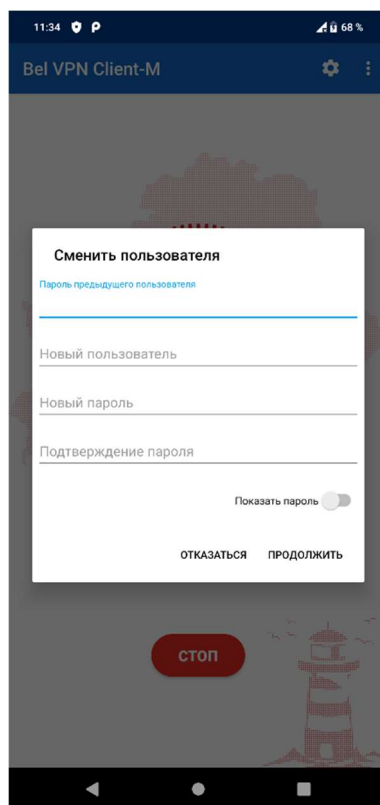


Рисунок 33

Нажмите на кнопку *Продолжить*, чтобы выполнить смену пользователя.

В случае успеха выдается уведомление:

Пользователь успешно сменен.

8.6. Автоблокировка

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

Настройки автоблокировки вызываются при выборе на главном экране пункта меню *Автоблокировка*.

Для включения автоблокировки нужно выставить флажок - *Включить* и Введите время ожидания в секундах (время между переходом устройства в спящий режим и активацией автоблокировки) (Рисунок 34).

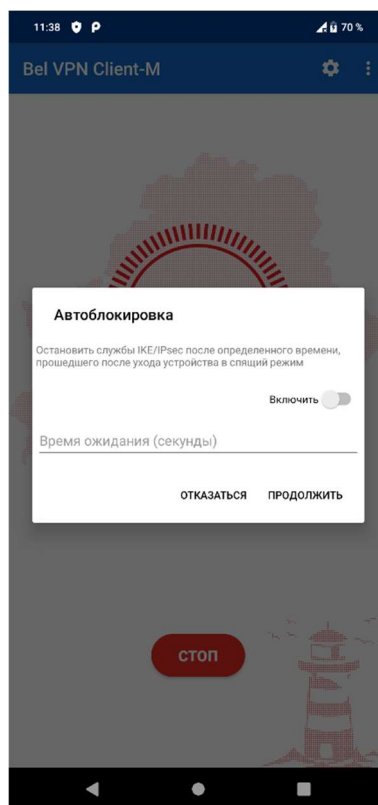


Рисунок 34

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

При активации автоблокировки:

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

Если после перехода в спящий режим, но до истечения времени ожидания, устройство перешло в активный режим, никаких действий активации автоблокировки не производится.

8.7. Протоколирование

Информация по данному пункту меню приведена в подразделе 9.5.

8.8. Обновить лицензию

В случае окончания срока действия лицензии с помощью данного пункта меню возможно ввести информацию о новой лицензии.

Заполните необходимые графы вручную или импортировать информацию о лицензии из файла с помощью кнопки *Импорт*, которая расположена в верхнем правом углу поля *Код покупателя* (Рисунок 35), нажмите кнопку *Продолжить*.

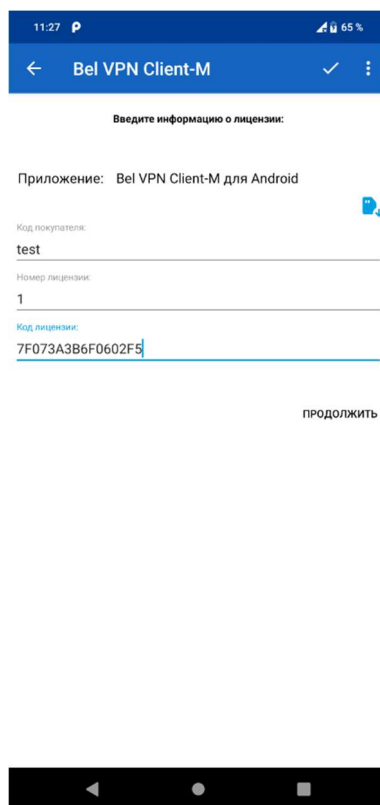


Рисунок 35

Также предусмотрена возможность обновления лицензии через электронную почту/Viber/Skype и т.п. Для обновления лицензии необходимо в сообщении нажать на прикрепленный файл с лицензией, выбрать - *Открыть с помощью приложения "Bel VPN Client-M (импорт лицензии)"*¹⁴ и нажать кнопку *Только сейчас* (Рисунок 36).

- 14 В отдельных случаях файлы с определенными расширениями могут по умолчанию открываться другими приложениями. Для того чтобы отменить это действие и перевести его в интерактивный режим выберите в ОС Android *Настройки -> Приложения -> соответствующее приложение (Например, Документы) -> Открывать по умолчанию -> Удалить настройки по умолчанию*.

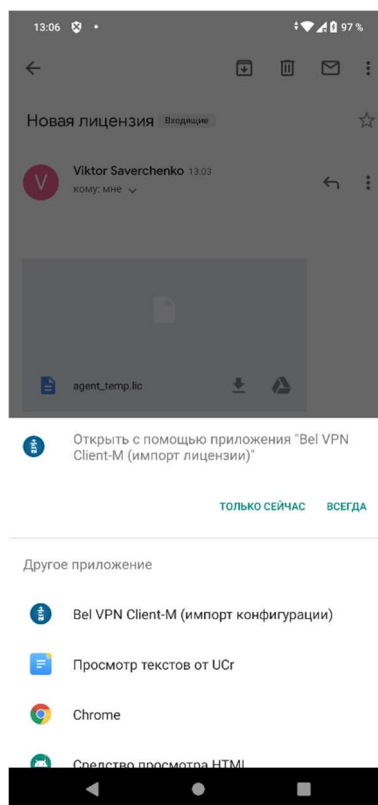


Рисунок 36

Далее лицензия передается в Bel VPN Client-M и импортируется в базу продукта аналогично ее первоначальному вводу.

8.9. О приложении

По данному пункту меню доступна информация о наименовании продукта, его версии и компании производителе.

8.10. Выход

С использованием данного пункта меню можно разорвать установленное защищенное соединение, завершить службы IKE/IPsec, выгрузить их и непосредственно само приложение из памяти устройства. Аналогичные действия можно произвести и с помощью стандартных методов ОС Android по выгрузке приложений из памяти.

9. Описание элементов экрана Настройки

9.1. Переход на экран Настройки

После запуска служб IKE/IPsec на панели действий появляется иконка в виде шестеренки для перехода на экран настройки основных параметров. Также перейдите на данный экран возможно выбрав на главном экране пункт меню *Настройки*.

С помощью экрана настройки задается (редактируется) локальная политика безопасности, производится управление сертификатами или общим ключом, ведется протоколирование событий, осуществляется конфигурирование пользовательского интерфейса. Кроме того, на экране настройки отображается текущее состояние всех основных элементов настройки (Рисунок 37).

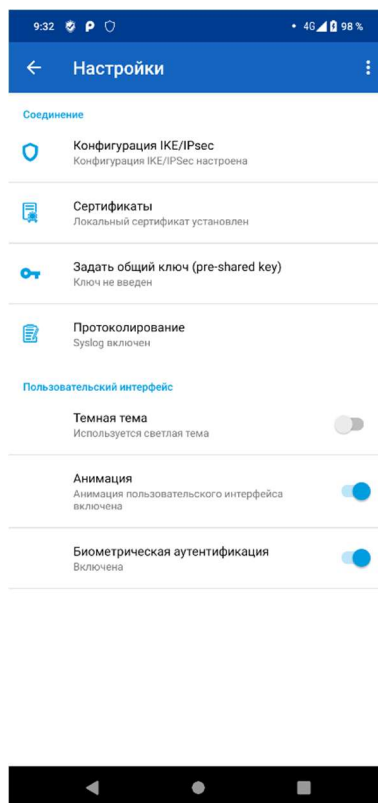


Рисунок 37

9.2. Раздел Конфигурация IKE/IPsec

В разделе *Конфигурация IKE/IPsec* можно создать, посмотреть или отредактировать текущую локальную политику безопасности (конфигурацию), либо произвести отключение сетевой защиты (Рисунок 38).

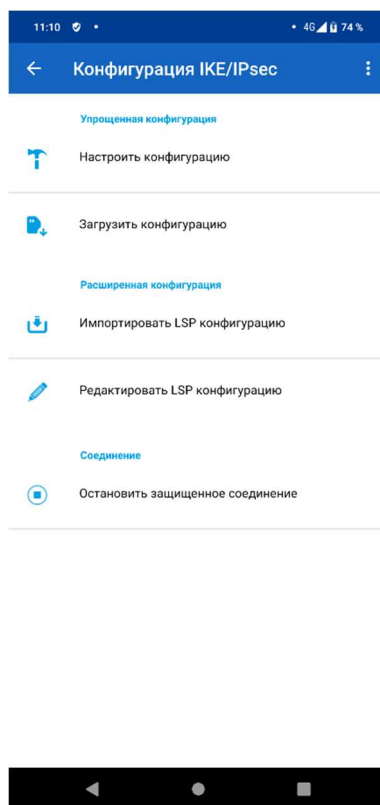


Рисунок 38

Создать локальную политику безопасности можно несколькими способами:

- используя графический интерфейс – пункт меню *Настроить конфигурацию*.
- подготовить конфигурацию в текстовом виде и:
 - ввести через буфер обмена – пункт меню *Импортировать LSP конфигурацию -> Ввести как текст (через буфер обмена)*;
 - загрузить из файла – пункт меню *Загрузить конфигурацию* (без предварительного просмотра), или *Импортировать LSP конфигурацию -> Установить из файла* (с предварительным просмотром);
 - импортировать из сообщения, полученного через электронную почту/Viber/Skype и т.п.

Некоторые особенности настройки Bel VPN Client-M с использованием конфигурационного файла описаны в [11](#).

Внести исправления в локальную политику безопасности можно, используя графический интерфейс – пункт меню *Настроить конфигурацию*, либо редактируя загруженную/сгенерированную LSP конфигурацию – *Редактировать LSP конфигурацию*.

Действия, которые будут выполняться при выборе элементов интерфейса данного раздела описаны далее.

Настроить конфигурацию

В данном разделе можно создать или отредактировать локальную политику безопасности, используя графический интерфейс (Рисунок 39). Можно очистить конфигурацию, воспользовавшись меню в правом верхнем углу.

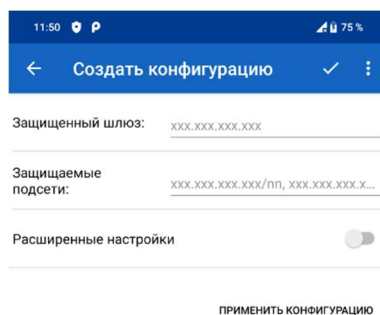


Рисунок 39

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:

192.168.101.10/24, 192.168.102.0/24

С помощью переключателя *Расширенные настройки* можно получить доступ к дополнительным параметрам (Рисунок 40).

Рисунок 40

Параметры IKE phase1

В этой области задаются параметры для первой фазы IKE.

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:

- *Сертификат bign* – аутентификация с использованием сертификата открытого ключа. Значение по умолчанию.
- *Общий ключ* – аутентификация с использованием общего ключа (preshared key).

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:

- *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 СОС. Возможные значения:

- *По возможности* – СОС используется при проверке сертификата только в том случае, если он является действующим. Этот режим отличается от режима *Необязательна* тем, что СОС может быть получен посредством протокола LDAP (если он настроен). Это значение используется по умолчанию.
- *Отключена* – при проверке сертификата СОС не обрабатывается.
- *Необязательна* – СОС 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 СОС.

Загрузить конфигурацию

При выборе этого пункта меню предлагается выбрать файл с конфигурацией. Файл с конфигурацией должен быть предварительно размещен в папке /S-Terra¹⁵. Порядок подготовки файла описан в [Приложении](#).

Импортировать LSP конфигурацию

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

Импортировать LSP конфигурацию, полученную по электронной почте

Перед импортом конфигурации, полученной по электронной почте/Viber/Skype и т.п., необходимо запустите службы IKE/IPsec. Для этого нажмите на главном экране Bel VPN Client-M кнопку *СТАРТ*, затем перейдите в почтовую программу и в полученном сообщении нажмите на конфигурационный файл. В появившемся диалоговом окне

¹⁵ Каталог /S-Terra, создается в Android External Storage Directory. Путь к Android External Storage Directory строго не регламентируется в ОС Android, но на практике обычно находится в /sdcard либо /storage/emulated/0.

выберите¹⁶ *Открыть с помощью приложения “Bel VPN Client-M (импорт конфигурации)”* и нажмите кнопку *Только сейчас* (Рисунок 41).

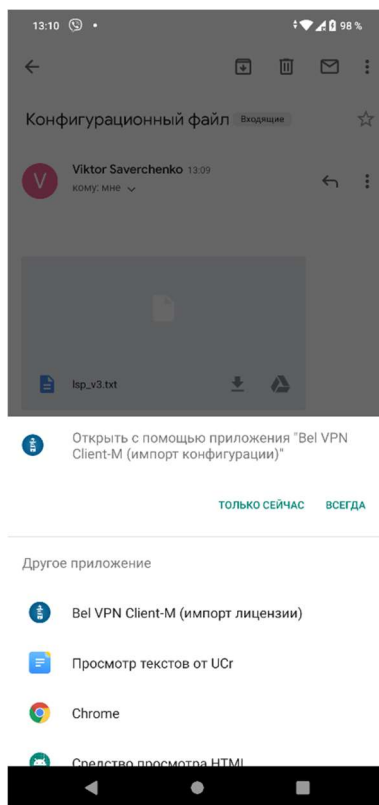


Рисунок 41

Далее конфигурация передается в Bel VPN Client-M и импортируется в базу данных аналогично другим методам.

Редактировать LSP конфигурацию

При выборе этого пункта меню выводится текстовое поле с локальной политикой безопасности.

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

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 42).

¹⁶ В отдельных случаях файлы с определенными расширениями могут по умолчанию открываться другими приложениями. Для того чтобы отменить это действие и перевести его в интерактивный режим выберите в ОС Android *Настройки -> Приложения -> соответствующее приложение (Например, Документы) -> Открывать по умолчанию -> Удалить настройки по умолчанию*.

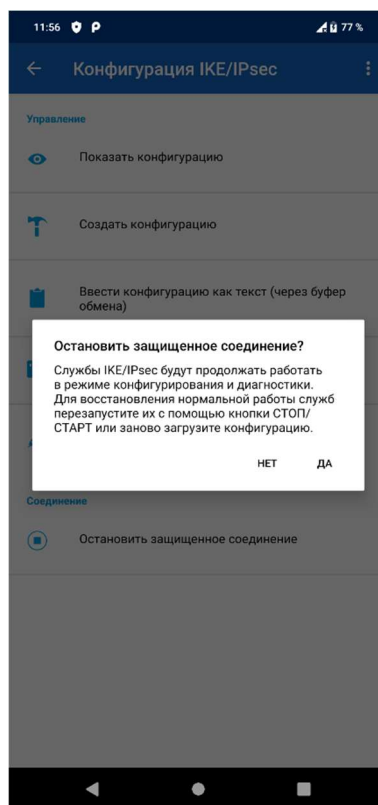


Рисунок 42

Для восстановления нормальной работы служб, перезапустите Bel VPN Client-M (нажмите вначале кнопку *СТОП*, затем *СТАРТ*).

9.3. Раздел Сертификаты

В разделе *Сертификаты* задаются локальный сертификат, сертификат открытого ключа удостоверяющего центра (далее - УЦ), СОС. Также в этом разделе можно создать запрос на получение локального сертификата, посмотреть сертификаты, находящиеся в базе продукта и при необходимости удалить их (Рисунок 43).

В случае, если импортируемый сертификат находится в файле, этот файл должен быть размещен в папке /S-Terra¹⁷.

¹⁷ Каталог /S-Terra, создается в Android External Storage Directory. Путь к Android External Storage Directory строго не регламентируется в ОС Android, но на практике обычно находится в /sdcard либо /storage/emulated/0.

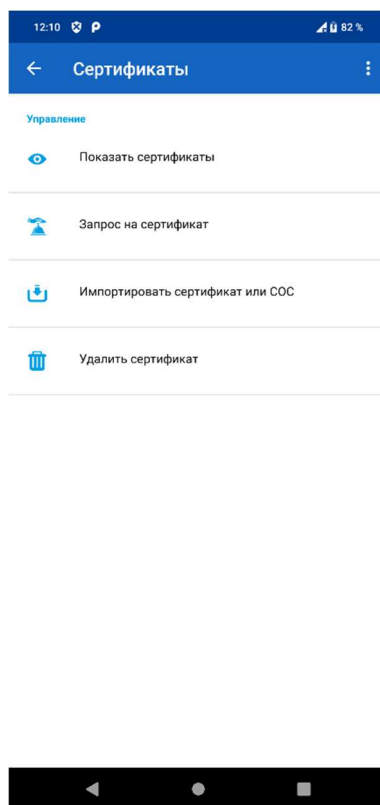


Рисунок 43

Действия, которые будут выполняться при выборе отдельных элементов интерфейса данного раздела:

Показать сертификаты

Выводится информация о сертификатах, находящихся в базе продукта (Рисунок 44).

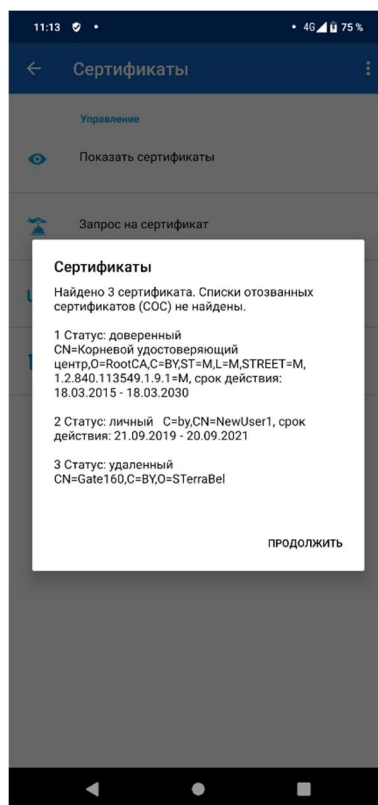


Рисунок 44

Запрос на сертификат

При выборе этого пункта появляется окно (Рисунок 45) в котором необходимо ввести значение поля *Subject DN* сертификата (используется для подготовки запроса на сертификат).

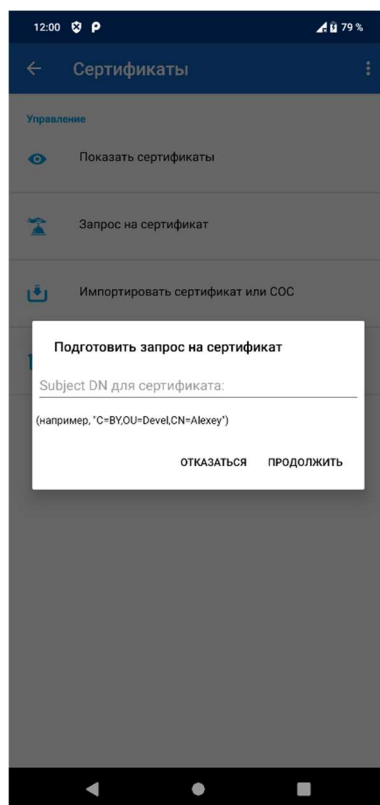


Рисунок 45

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 46).

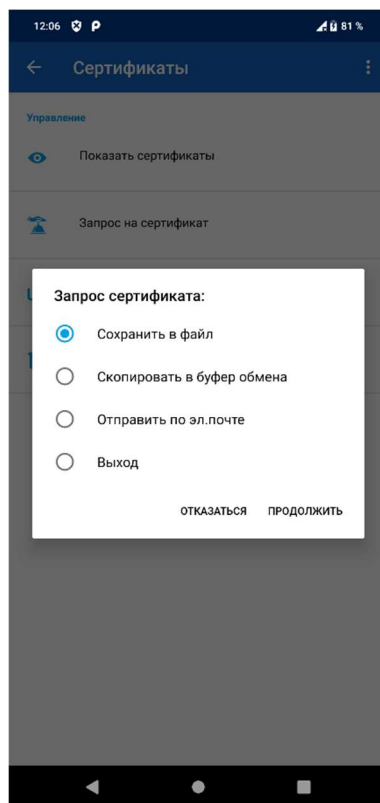


Рисунок 46

Для получения сертификата нужно отослать запрос в УЦ.

Эти же пункты (*Сохранить запрос сертификата в файл*, *Скопировать запрос сертификата в буфер обмена*, *Отправить по эл. почте*) добавятся в раздел *Запрос на сертификат* для того, чтобы можно было выполнить эти действия позже (Рисунок 47).

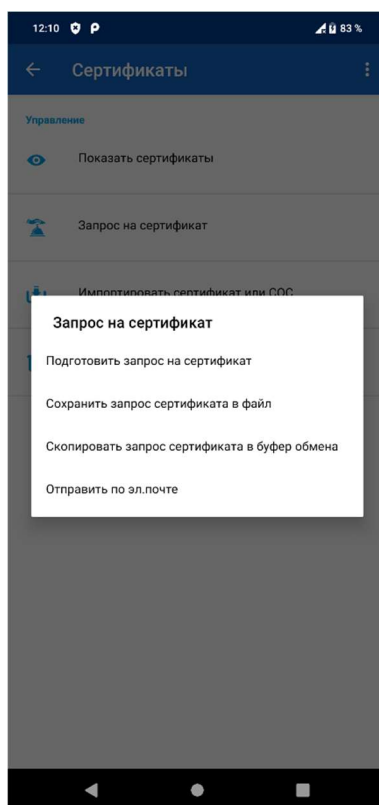


Рисунок 47

Импортировать сертификат или СОС

При выборе этого пункта появляется диалоговое окно (Рисунок 48), в котором надо выбрать тип сертификата, а затем способ его получения для импорта в базу продукта.

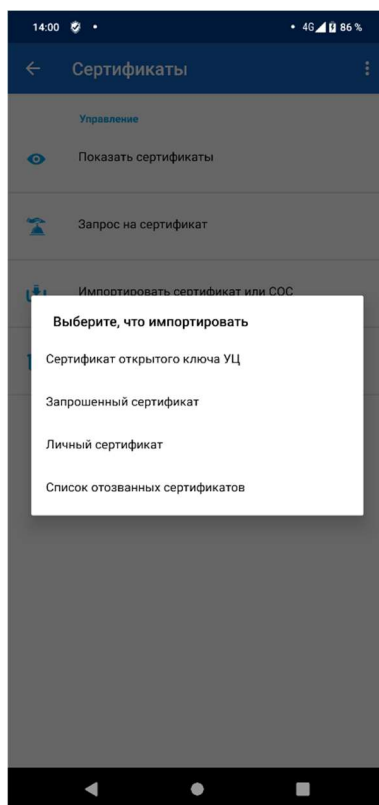


Рисунок 48

При импорте сертификата или СОС из файла, он должен быть предварительно размещен в папке /S-Terra¹⁸.

Импорт сертификата или СОС, полученных по электронной почте

Перед импортом сертификата или СОС, полученных по электронной почте/Viber/Skype и т.п. запустите службы IKE/IPsec (нажмите на главном экране Bel VPN Client-M кнопку *СТАРТ*), перейдите в почтовую программу, в полученном сообщении нажмите на файл с прикрепленным сертификатом, выберите¹⁹ *Открыть с помощью приложения "Bel VPN Client-M (импорт сертификатов)"* и нажмите кнопку *Только сейчас* (Рисунок 49).

¹⁸ Каталог /S-Terra, создается в Android External Storage Directory. Путь к Android External Storage Directory строго не регламентируется в ОС Android, но на практике обычно находится в /sdcard либо /storage/emulated/0.

¹⁹ В отдельных случаях файлы с определенными расширениями могут по умолчанию открываться другими приложениями. Для того чтобы отменить это действие и перевести его в интерактивный режим выберите в ОС Android *Настройки -> Приложения -> соответствующее приложение (Например, Документы) -> Открывать по умолчанию -> Удалить настройки по умолчанию*.

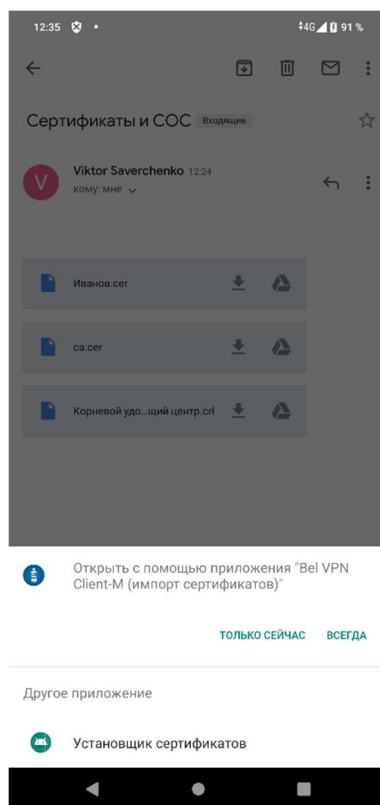


Рисунок 49

Далее сертификат или СОС передается в Bel VPN Client-M и импортируется в базу продукта аналогично другим методам.

Удалить сертификат

В появившемся диалоговом окне выводится список сертификатов, которые можно пометить для удаления (Рисунок 50).

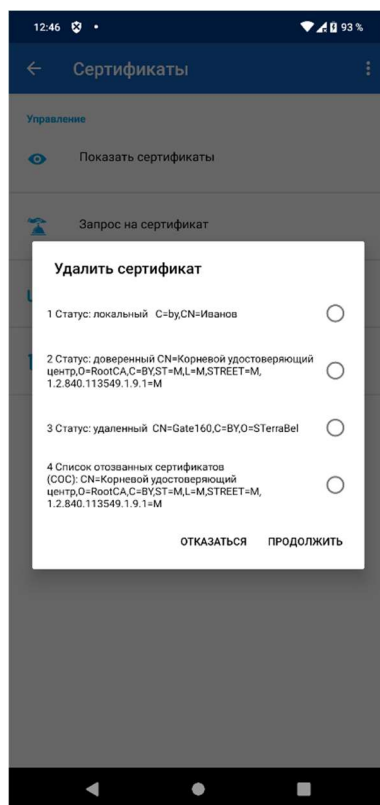


Рисунок 50

9.4. Раздел Задать общий ключ (preshared key)

Альтернативным способом аутентификации при помощи сертификатов является аутентификация с использованием общего ключа (preshared key).

В разделе *Задать общий ключ (preshared key)* задается общий ключ (Рисунок 51).

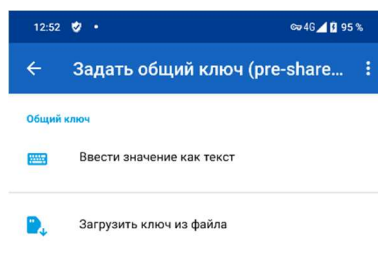


Рисунок 51

Введите 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-Terra²⁰.

9.5. Раздел Протоколирование

В разделе *Протоколирования* можно задать протоколирование событий по протоколу Syslog и указать адрес сервера, куда будут отправляться эти сообщения (Рисунок 52).

Уровень важности протоколируемых событий соответствует уровню отладки (debug).

²⁰ Каталог /S-Terra, создается в Android External Storage Directory. Путь к Android External Storage Directory строго не регламентируется в ОС Android, но на практике обычно находится в /sdcard либо /storage/emulated/0.

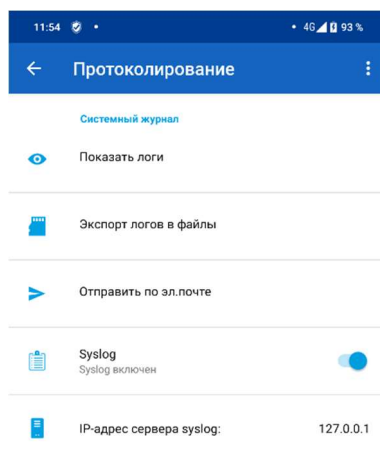


Рисунок 52

Показать логи – при выборе этого пункта можно выбрать и просмотреть основные журналы протоколирования.

Экспорт логов в файлы – при выборе этого пункта, все журналы протоколирования с расширением “.log” будут сохранены в папке /S-Terra²¹.

Отправить по эл. почте – с помощью этого пункта журналы протоколирования могут быть отправлены администратору по электронной почте/Viber/Skype и т.п. (Рисунок 53).

21 Каталог /S-Terra, создается в Android External Storage Directory. Путь к Android External Storage Directory строго не регламентируется в ОС Android, но на практике обычно находится в /sdcard либо /storage/emulated/0.

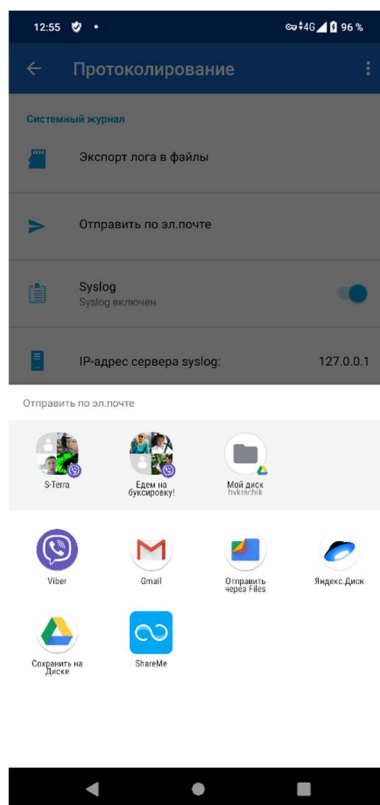


Рисунок 53

Syslog – переключатель включен – протоколирование ведется, если выключен, 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.

9.6. Переключатель Темная тема

Для переключения интерфейса на темную тему (режим Dark Mode) необходимо воспользоваться переключателем, расположенным справа от наименования данного параметра (Рисунок 54). Использование этого режима на устройствах с экраном AMOLED позволяет экономить заряд аккумулятора. В некоторых версиях ОС Android для полного переключения всех элементов интерфейса Bel VPN Client-M на темную тему необходимо перезагрузить приложение (выйти из него и снова войти).

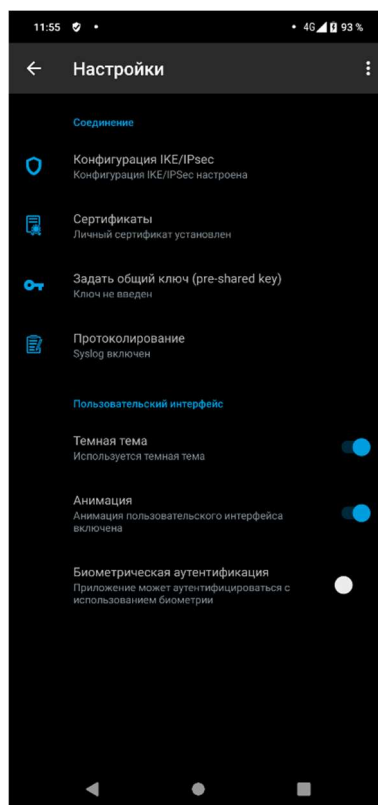


Рисунок 54

9.7. Переключатель Анимация

Анимация пользовательского интерфейса позволяет визуализировать процесс создания защищенного соединения. Для улучшения зрительного восприятия анимация используется в следующих элементах пользовательского интерфейса Bel VPN Client-M:

- Bel VPN Client-M;
- (Меню -> Информация о соединении);
- строка ОС Android с уведомлениями;
- экран генерации случайных чисел (доступен при (Меню->О приложении)).

По умолчанию анимация включена. Для отключения анимации необходимо воспользоваться переключателем, находящимся справа от наименования данного параметра.

9.8. Переключатель Звуковые уведомления

Данный параметр позволяет включить/отключить звуковые уведомления о создании/разрыве защищенного соединения. По умолчанию он включен. Для отключения звуковых уведомлений необходимо воспользоваться переключателем, находящимся справа от наименования данного параметра.

Этот параметр доступен для версий ОС Android 7.1 и ниже. В ОС Android 8.0 и выше, для управления звуковыми уведомлениями, перейдите в *Настройки ОС Android*, выберите раздел *Приложения и Уведомления*, разверните подраздел *Показать все приложения*, выберите там приложение *Bel VPN Client-M*, затем пункт *Уведомления* и откорректируйте его звуковые параметры (Рисунок 55).

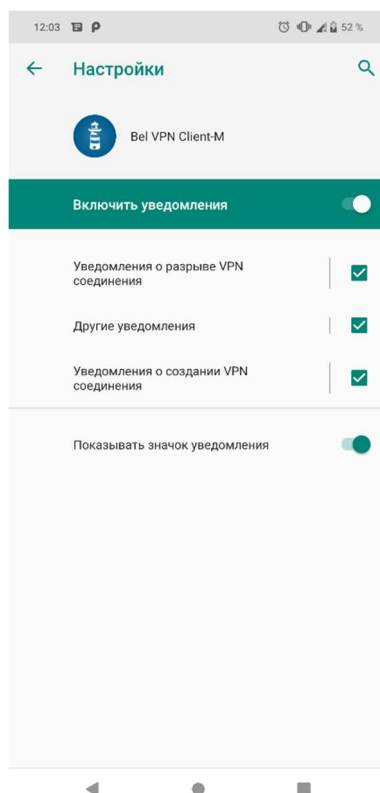


Рисунок 55

9.9. Переключатель Биометрическая аутентификация

Данный параметр позволяет включить биометрическую аутентификацию (Рисунок 56).



Рисунок 56

10. Деинсталляция продукта

Перед деинсталляцией приложения Bel VPN Client-M необходимо остановить службу IKE/IPsec. Для этого на главном экране нажмите кнопку *СТОП*.

Деинсталляция Bel VPN Client-M производится стандартными средствами ОС Android. Войдите в *Настройки* -> *Приложения* (в ОС 8.0 и выше *Приложения и уведомления*) -> Bel VPN Client-M и выберите действие *Удалить*.

11. Приложение. Настройка Bel VPN Client-M с использованием конфигурационного файла

Описание конфигурационного файла приведено в документе «Программные продукты Bel VPN. Руководство пользователя. Создание конфигурационного файла».

Особенности настройки конфигурационного файла

1. Если в конфигурационном файле Bel VPN Client-M включен механизм PathMTUDiscovery (IPsecAction.NoPathMTUDiscovery=FALSE), то значение IPsecAction.MTU должно быть больше 670.
7. Параметр PersistentConnection в структуре IPsecAction всегда должен быть TRUE.
8. Допускается только одна структура NetworkInterface со значением LogicalName по умолчанию.
Платформа Android, не поддерживает настройку iptables, фильтры InputFilter и OutputFilter не поддерживаются.
9. Структура RoutingTable для Bel VPN Client-M не поддерживается.
10. Структура AHProposal для Bel VPN Client-M не поддерживается.

[illegible]