БАНК ИТ

Комплексное решение по защите коммуникаций для банков на основе Bel VPN продуктов версии 4.1

Сапрыкин А.М., директор ООО «С-Терра Бел»
представитель НП «Инфофорум» в Республике Беларусь

XII Международный форум по банковским информационным технологиям

18-20 ноября 2015 года
Президент-Отель, г. Минск

БЕЛОРУССКАЯ КРИПТОГРФИЯ В СЕТЕВЫХ РЕШЕНИЯХ ЛЮБОЙ СЛОЖНОСТИ

s·terra
BEL

Реализация белорусской криптографии в версии 4.1

Приказ Оперативно-аналитического центра при Президенте Республики Беларусь «О некоторых вопросах технической и криптографической защиты информации» 30 августа 2013 г. № 62 (в редакции от 15 января 2015г. №3)

- Перечень технических нормативных правовых актов и документов, в которых определены требования к криптографическим механизмам:
  - Ш1, И1 – ГОСТ 28147-89 «Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования»
  - П1 – СТБ 1176.2-99 «Информационная технология. Защита информации. Процедуры выработки и проверки электронной цифровой подписи»
  - Ш2, И2 – СТБ 34.101.31-2011 «Информационные технологии. Защита информации. Криптографические алгоритмы шифрования и контроля целостности»
  - П2 – СТБ 34.101.45-2013 «Информационные технологии и безопасность. Алгоритмы электронной цифровой подписи и транспорта ключа на основе эллиптических кривых»
  - К82 – СТБ 34.101.66-2014 «Информационные технологии и безопасность. Протоколы аутентификации и выработки общего ключа на основе эллиптических кривых»
  - С2, С3 – СТБ 34.101.19-2012 «Информационные технологии и безопасность. Форматы сертификатов и списков отозванных сертификатов инфраструктуры открытых ключей»
  - Г1 – СТБ 34.101.27-2011 «Информационные технологии и безопасность. Требования безопасности к программным средствам криптографической защиты информации» и/или

    – СТБ П 34.101.43-2009 «Информационные технологии. Методы и средства безопасности. Профиль защиты технических и программно-аппаратных средств криптографической защиты информации»

Bel VPN продукты версии 4.1

- в Bel VPN 4.1:
  - полномасштабное соответствие требованиям приказа ОАЦ «О некоторых вопросах технической и криптографической защиты информации» от 30 августа 2013 г. №62 (с изменениями и дополнениями согласно приказу от 15 января 2015г. №3), в частности:
    - по умолчанию шифрование и контроль целостности осуществляется по СТБ 34.101.31 (БЕЛТ) в качестве основного стандарта
    - использование сертификатов ЭЦП на эллиптических кривых согласно СТБ 34.101.45
    - генерация псевдослучайных чисел по СТБ 34.101.47
    - протокол формирования общего ключа осуществляется по рекомендованной ОАЦ Методике на основе эллиптических кривых согласно СТБ 34.101.66 (приложение А)
    - межсетевой экран по ОК: СТБ 34.101.1-2014, СТБ 34.101.2-2014, СТБ 34.101.3-2014 (3Б)
    - продукт Bel VPN Gate соответствует в общей сложности 14-ти белорусским стандартам и ТНПА

Bel VPN продукты версии 4.1

- усовершенствованный VPN-инструментарий:
  - расширение перечня поддерживаемых операционных систем:
    - Debian 6 (32/64bit)
    - Windows XP/Vista/7/8 (32/64bit)
    - Windows Server 2003, 2008, 2008 R2, 2012
    - Android 4.xx, 5.xx
  - усовершенствованный МСЭ
  - модуль централизованной системы удаленного управления – Bel VIN KP 4.1
  - модуль для защищенного взаимодействия на канальном уровне – Bel VPN L2
  - расширенные сценарии обработки сетевого трафика, в т.ч.:
    - приоритезация, маркировка трафика
    - туннелирование трафика
  - IKECFG-сервер
  - интеграция с Radius-сервером
  - расширен перечень аппаратных платформ: HP /Cisco /Huawei /Samsung /DEPO /Kraftway /Bevalex / TradeixBel
  - поддержка виртуальных систем VmWare ESXi, Citrix Xen, Microsoft Hyper-V
  - увеличена производительность – до 10 Гб/с (в кластерном решении)
  - криптобиблиотека AvC и USB-носители ключей/сертификатов AvBign/AvPass производства ЗАО «Авест»

Bel VPN продукты версии 4.1

- Продукты Bel VPN 4.1 включают следующий набор средств защиты сетевого уровня:

  - Bel VPN Gate 4.1 – масштабируемый набор программно-аппаратных шлюзов безопасности для защиты межсетевого обмена данных в распределенных корпоративных (ведомственных) сетях
  - Bel VPN Gate-V 4.1 – программный виртуальный шлюз безопасности, функционирующий в виртуальной среде (VMware ESXi, Citrix XenServer, Microsoft Hyper-V). Предназначен как для защиты периметра облачной инфраструктуры, так и взаимодействия между отдельными виртуальными машинами
  - Bel VPN Client 4.1 – программно-аппаратное устройство для защиты индивидуального (удаленного) пользователя
  - Bel VPN Client-M 4.1 – программный продукт для защиты мобильных устройств
  - Bel VPN KP 4.1 – программный модуль для централизованного управления Bel VPN продуктами (входит в состав шлюза как функциональная опция)
  - Bel VPN L2 – программный модуль для защиты на канальном уровне (входит в состав шлюза как функциональная опция)

Шлюз безопасности Bel VPN Gate 4.1

- Bel VPN Gate 4.1 – системообразующий программно-аппаратный комплекс шлюз безопасности на базе серверных платформ HP, Cisco, Huawei, Kraftway, Tonk, Depo, а также белорусских производителей - Bevalex, TradeixBel, Belsoft, функционирующий под управлением ОС *Debian*
- Предлагается перечень масштабируемых шлюзов, различающихся по производительности – от 50 Мб/с до 5 Гб/с и количеству туннелей шифрования – от 5 туннелей до неограниченного количества
- Обеспечивает:
  - ✓ защиту транзитного и собственного трафика;
  - ✓ пакетную и statefull фильтрацию трафика, туннелирование (маскировку топологии)
  - ✓ протоколы IPsec ESP/AH, IKE, PKI
  - ✓ маркировку и приоритезация трафика (QoS)
  - ✓ событийное протоколирование Syslog, мониторинг SNMP
  - ✓ горячее резервирование по VRRP, балансировку по RRI и т.д.

Виртуальный шлюз безопасности Bel VPN Gate-V 4.1

Bel VPN Gate-V 4.1 – программный комплекс «Виртуальный шлюз безопасности Bel VPN Gate-V» обеспечивает полную функциональность Bel VPN Gate и функционирует в виртуальной среде (VMware ESXi, Citrix XenServer, Microsoft Hyper-V).

Предназначен как для защиты периметра облачной инфраструктуры, так и взаимодействия между отдельными виртуальными машинами. Производительность зависит от аппаратной платформы

- Преимущества:
  - ✓ интеграция непосредственно в виртуальную инфраструктуру
  - ✓ простая и быстрая установка и настройка
  - ✓ высокая производительность шифрования трафика
  - ✓ реализация сценариев обеспечения высокой доступности и отказоустойчивости
  - ✓ оперативная адаптация к меняющимся задачам и требованиям сетевых приложений и инфраструктуры
  - ✓ легкое сохранение или восстановление резервной копии
  - ✓ эффективное использование вычислительных ресурсов
  - ✓ экономия электроэнергии и места в стойке

Клиент безопасности Bel VPN Client 4.1

- Bel VPN Client 4.1 - программно-аппаратное устройство Клиент безопасности Bel VPN Client предназначено для безопасного удаленного доступа к защищенным ресурсам. Функционирует на следующих ОС:
  - Windows XP
  - Windows Vista
  - Windows 7 (x32/x64)
  - Windows 8 (x32,x64)
  - Windows Server 2003, 2008, 2008 R2, 2012

- Обеспечивает защиту и пакетную фильтрацию трафика между удаленным компьютером и другими Bel VPN продуктами
- Может быть сконфигурирован для массового развертывания с помощью технологии *«установки одним нажатием кнопки»*
- Конфигурирование политики безопасности клиента осуществляется централизовано с помощью графического интерфейса
- Реализован сценарий хранения всех необходимых данных пользователя для VPN соединения непосредственно на ключевом носителе
- Обеспечивает фактически функционал шлюза, в т.ч. МСЭ, событийное протоколирование Syslog, маркировку трафика, мониторинг SNMP, интеграцию с Radius сервером, получение IKECFG, split tunneling, statefull фильтрацию и др.

Мобильный клиент безопасности Bel VPN Client-M 4.1

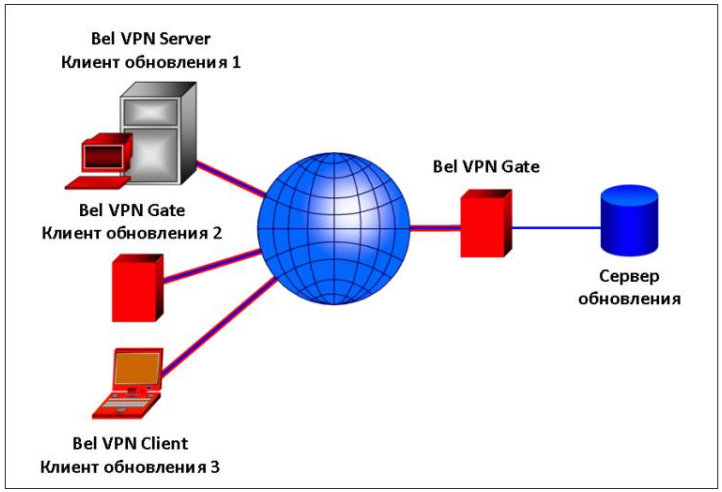
- Bel VPN Client-M – программный продукт мобильный клиент безопасности Bel VPN Client-M предназначен для обеспечения безопасного удаленного доступа к информационным ресурсам, защищаемым Bel VPN продуктами, защиты трафика мобильных устройств на платформах Android.xx

- Пользователи смартфонов, коммуникаторов и планшетов теперь защищены.

- Обеспечивает функционал обычного Клиента безопасности, но работает без внешнего носителя ключей/сертификатов. Использует физический датчик генерации случайных чисел (встряхивание).
- Политика безопасности продукта настраивается с помощью графического интерфейса. Существует возможность непосредственного редактирования локальной политики безопасности (LSP)
- Для установки Bel VPN Client-M не требуется взлома устройства (получения прав root)
- Совместим с MDM-системами (SafePhone, XenMobile и др.)

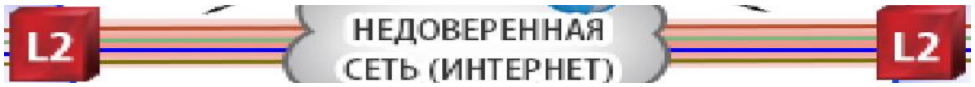
Панель управления Bel VPN KP 4.1

- Программный модуль Bel VPN KP 4.1 (в составе шлюза) состоит из Сервера управления и Клиента управления (ставится на управляемое VPN-устройство):
  - предназначена для централизованного управления продуктами линейки Bel VPN 4.1: Gate, Client, Gate-V, Client-M;
  - позволяет изменять на VPN-устройствах локальную политику безопасности, сертификаты, списки сертификатов, preshared key, настройки логирования, формировать ключевую пару непосредственно на VPN-устройстве;
  - позволяет контролировать активность управляемых VPN-устройств, срок действия сертификатов, осуществлять статистический сбор и анализ управляемых VPN-устройств;
  - поддерживает дополнительные функции по сбору сообщений из журнала регистрации событий, сбору настроек, обновлению настроек клиентов и др.

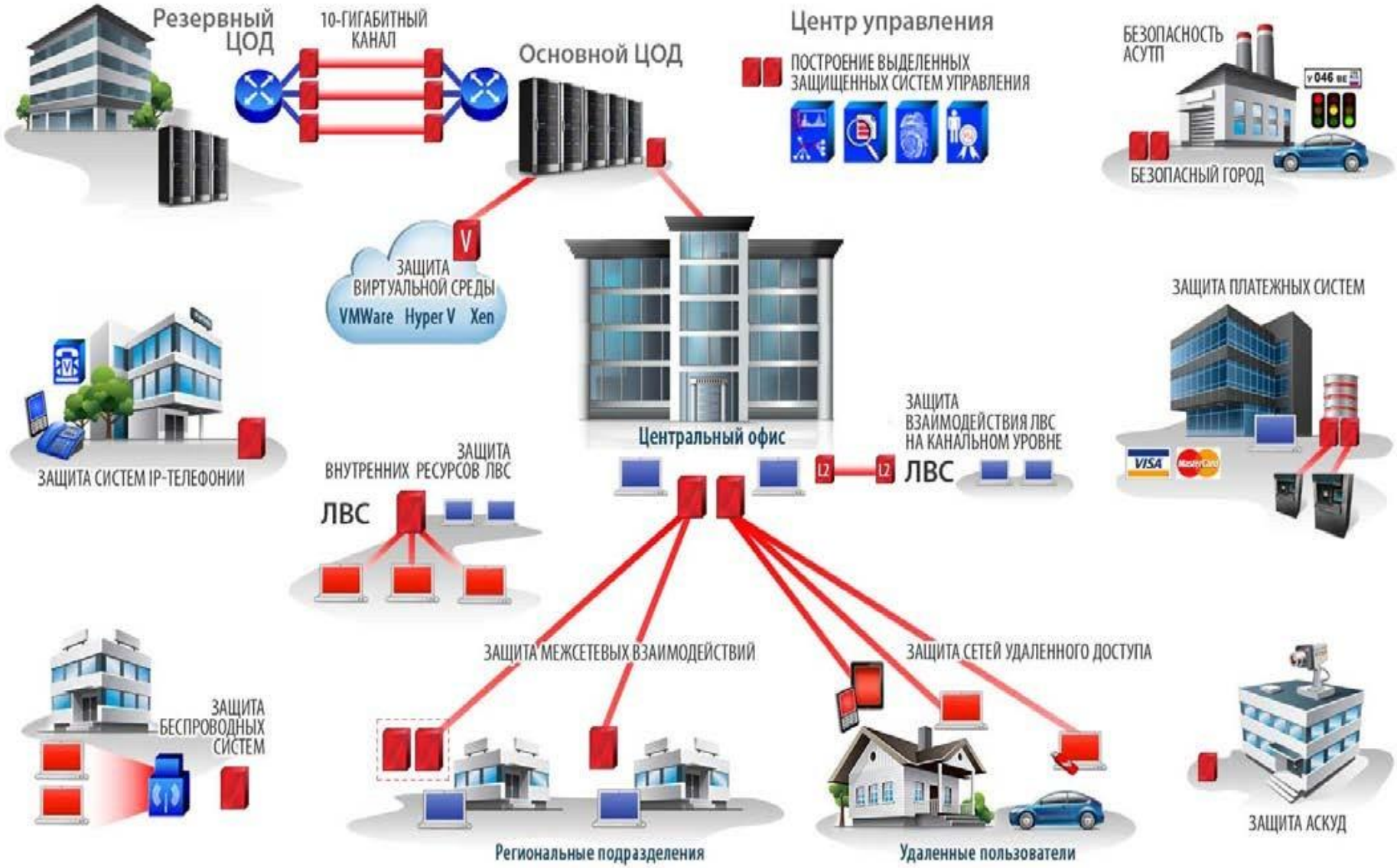


Модуль канального шифрования Bel VPN L2

- Программный модуль Bel VPN L2 (в составе шлюза) обеспечивает защищенное взаимодействие сегментов сети на канальном уровне.
- Обеспечивает:
  - ✓ объединение территориально-распределенных сетей в один широковещательный домен
  - ✓ передачу широковещательных (broadcast) и multicast пакетов, тестированного трафика (VLAN trunk), меток IPV4 и др.
  - ✓ обработку приоритетного трафика
  - ✓ минимальные настройки маршрутизации
- Применяется:
  - ✓ организация защищенного канала между ЦОД
  - ✓ реализация миграции сетевой инфраструктуры
  - ✓ защита IP-телефонии и видеоконференцсвязи
  - ✓ построение высокопроизводительного, отказоустойчивого решения с балансировкой нагрузки



От продуктов к решениям для банковской сферы

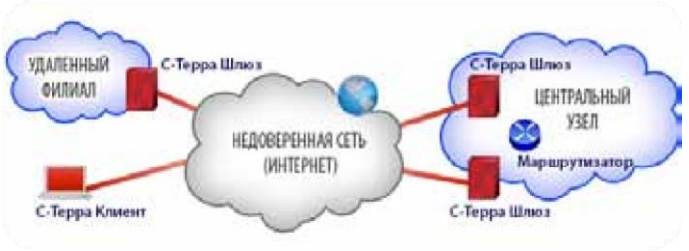


Защита корпоративной сети

Используются следующие Bel VPN продукты:

- Bel VPN Gate применяется для защиты передаваемых между сегментами сети данных и обеспечения МСЭ. При необходимости применяется Bel VPN Gate-V. В центральном офисе шлюзы могут быть организованы в отказоустойчивую схему

- Bel VPN Client и Bel VPN Client-M используются для удаленного защищенного доступа к ресурсам корпоративной сети
- Bel VPN L2 применяется при необходимости объединения нескольких сегментов сети на канальном уровне. Позволяет передавать multicast и broadcast пакеты, трафик с VLAN-тегами и другой трафик, который не проходит через IPsec в обычном режиме

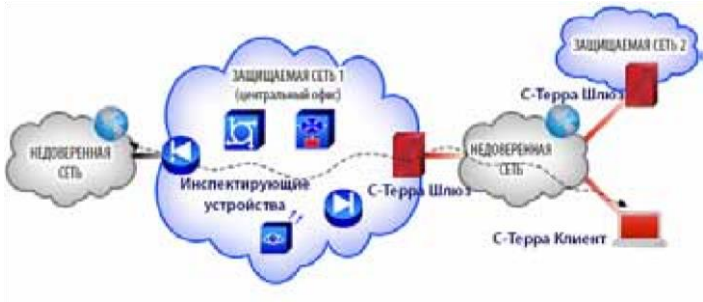


- Bel VPN KP упрощает управление и настройку применяемых в корпоративной сети Bel VPN продуктов. Администратор сети избавлен от рутинных операций, повышается управляемость, надежность сети в целом, обеспечивается регулярный мониторинг, при необходимости - оперативное вмешательство и др.

Защита удаленного и мобильного доступа

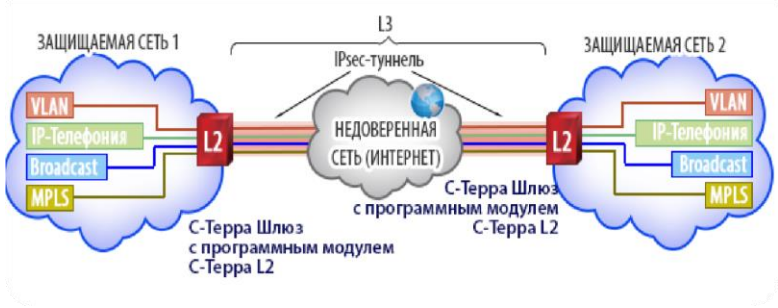
Используются следующие Bel VPN продукты:

- Bel VPN Client устанавливается на пользовательское устройство (под ОС Windows) и строит защищенный IPsec-туннель до шлюза безопасности Bel VPN Gate в центральном офисе
- Bel VPN Client-M работает аналогично Bel VPN Client, но предназначен для устройств с ОС Android
- В зависимости от выбранной политики безопасности может шифроваться как весь трафик, так и его часть (split tunneling). Обеспечивается межсетевое экранирование. Возможен сценарий, при котором инспекция всего трафика будет происходить в центральном офисе
- Bel VPN продукты поддерживают весь спектр современных сетевых протоколов, включая Radius и IKECFG и легко интегрируются в сетевую инфраструктуру ведомства
- При наличии большого количества удаленных пользователей целесообразно применение централизованной системы управления Bel VPN KP в т.ч. для обновления сертификатов на пользовательских устройствах



Защита ЦОД и высокопроизводительных каналов

- Для защиты ЦОД применяются шлюзы на наиболее производительных аппаратных платформах с балансирующим устройством
- В сетях с JumboFrames один Bel VPN Gate способен защищать поток данных до 5 Гбит/с
- При шифровании IMIX трафика – около 1 Гбит/с в обе стороны (1+1)
- Использование второго поколения Intel® Xeon® с двумя 10-ти гигабитными сетевыми картами дает до 10 Гбит/с (TCP, MTU 9000)
- Высокопроизводительная защита может быть обеспечена с помощью Bel VPN L2 и на канальном уровне
- И на сетевом, и на канальном уровне решения отказоустойчивы и масштабируются при возрастании трафика
- Механизм QoS позволяет обеспечить высокое качество сервиса для приоритетного трафика (например, IP-телефонии) даже в состоянии перегрузки



Защита виртуальной среды

- **Защита периметра виртуальной среды.** Для защиты периметра виртуальной среды (ВС) и безопасного доступа к ней может быть использован как ПАК Bel VPN Gate, так и виртуальный шлюз безопасности - ПК Bel VPN Gate-V.
- **Защита сетевых взаимодействий внутри виртуальной среды.** Виртуальный шлюз обеспечивает шифрование трафика и МСЭ между виртуальными машинами, находящимися как на одном, так и на разных физических серверах. При этом защита трафика может происходить как на сетевом, так и на канальном уровне.
- **Защита физических каналов связи между элементами виртуальной среды.** Bel VPN Gate-V может быть использован для защиты каналов связи между различными физическими серверами, составляющими ВС. Это целесообразно в территориально распределенной ВС, или в случае, если каналы связи и промежуточное оборудование не являются доверенными (например, при аренде серверов в ЦОДе различными банками).

Защита каналов передачи данных от банкоматов

- Вариант 1. Внутри корпуса банкомата устанавливается Bel VPN Gate 100B (на платформах Kraftway или Lanner) с минимальным числом туннелей шифрования
- Вариант 2. В ОС встроенной в банкомат ЭВМ устанавливается клиент безопасности для банкоматов - Bel VPN Client-B
- И шлюз, и клиент обеспечивают функции МСЭ
- В обоих случаях обеспечивается возможность удаленного обновления сертификатов
- Оба решения предусматривают для резервирования использование двух провайдеров, например Ethernet и 2G/3G/4G, с возможностью переключения

- **Преимущества**:
  - ✓решения полностью соответствуют белорусскому законодательству, в том числе требованиям к СКЗИ
  - ✓оба решения дешевле, чем ныне используемые с чужим шифрованием
  - ✓обеспечивается импортозамещение, поскольку иного оборудования, в том числе для МСЭ, не требуется

Техническая поддержка

Служба Технической поддержки:

- Порядок предоставления услуг
- Перечень предоставляемых услуг по технической поддержке
- Классификация Запросов по уровню важности

Портал технической поддержки:

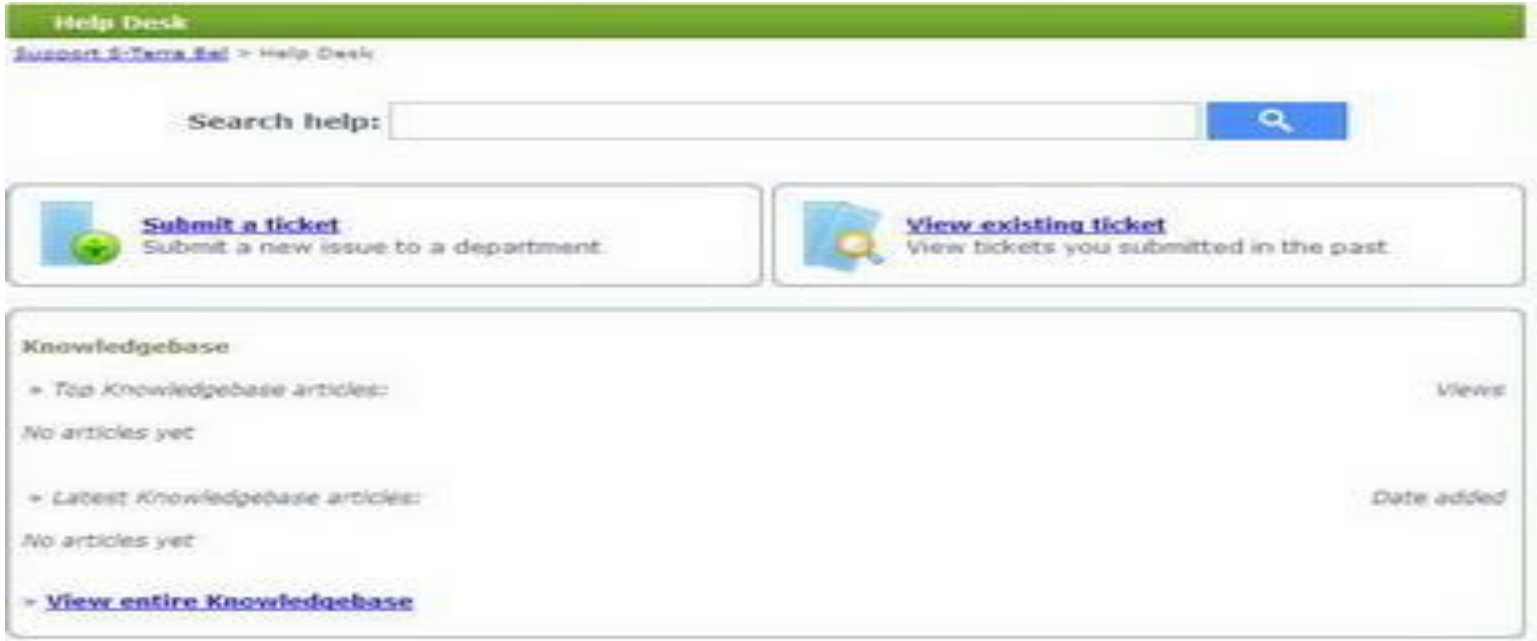
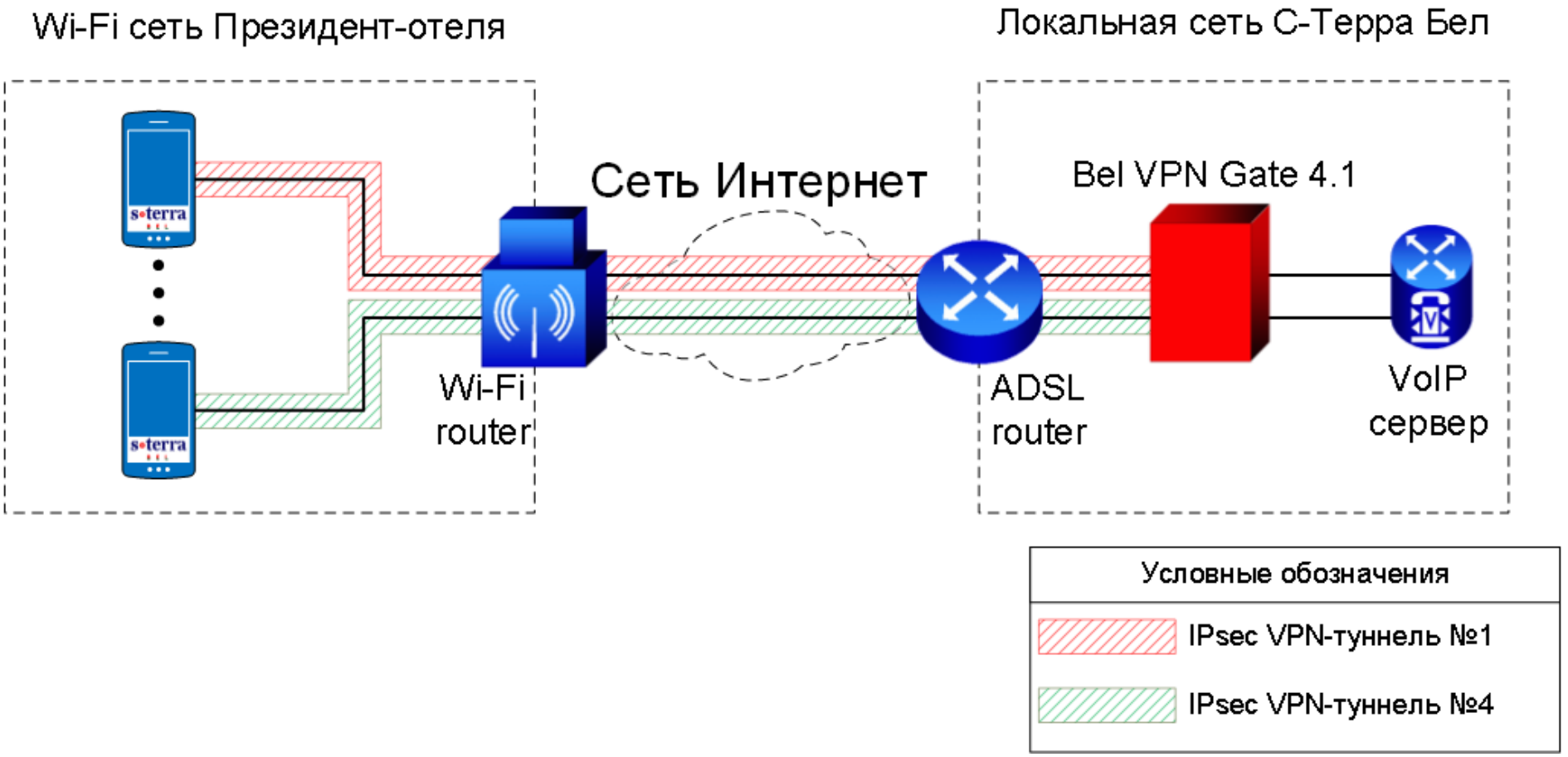
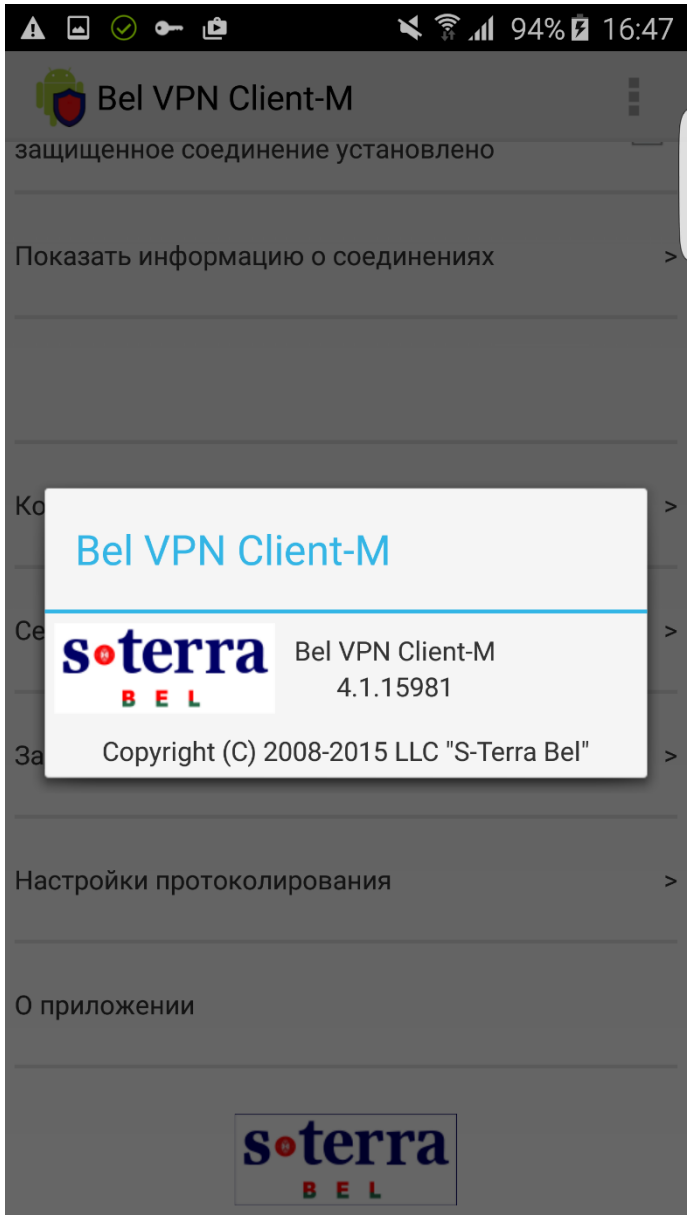
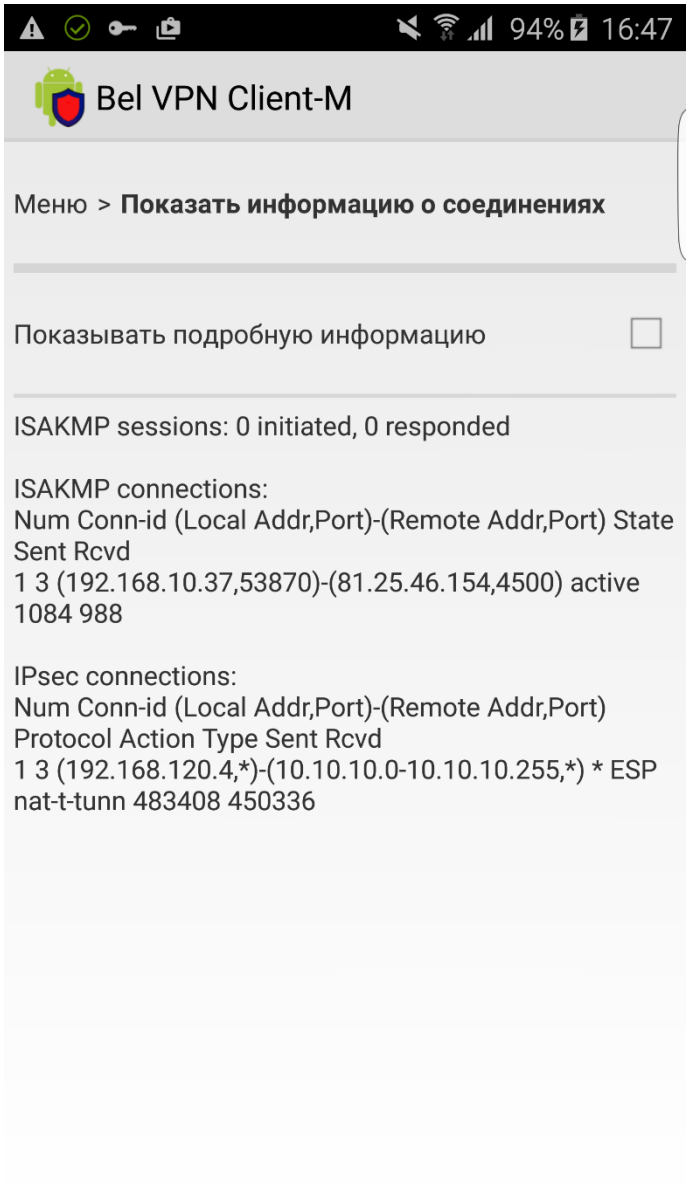


Схема практической демонстрации Bel VPN Client-M



Статистика защищенного соединения





КОНТАКТЫ

- **Адрес:**
  220012, г.Минск
  ул.Чернышевского, 10А
  пом.702
  (+375 17) 280 6000
  (+375 17) 280 7867
- **Факс:**
  (+375 17) 280 7867
- **Электронная почта:**
  info@s-terra.by

s•terra
BEL

Спасибо!

Обращайтесь к нам!