УТВЕРЖДЕНО

BY.РТНК.00004-04.1 34 01-3-ЛУ

Программный комплекс «Шлюз безопасности виртуальный Bel VPN Gate-V 4.1»

Руководство администратора

Введение

BY.РТНК.00004-04.1 34 01-3

Листов 11

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

2016

Содержание

Введение.....3

Комплект поставки ПАК Bel VPN Gate.....4

Назначение и функции ПАК Bel VPN Gate.....5

Архитектура ПАК Bel VPN Gate.....7

Требования по организационным и административным мерам обеспечения безопасности эксплуатации ПАК Bel VPN Gate.....9

Общие требования 9

Требования по размещению ПАК 9

Административные меры безопасности 9

Требования по защите ПАК от несанкционированного доступа (НСД) 10

Требования по установке ПО на ПАК 11

Введение

Программно-аппаратный комплекс «Шлюз безопасности Bel VPN Gate 4.1» (далее – ПАК, ПАК Шлюз) предназначен для работы на вычислительных системах (аппаратных платформах), построенных на базе одного, двух или более процессоров в архитектуре Intel x86/x86-64, и функционирует под управлением операционной системы Debian GNU/Linux 6.

Перечень протестированных аппаратных платформ:

- Lanner NCA-1010;
- DEPO Sky 171/1130/1230;
- ТОНК 1400 S-Terra / 1800 S-Terra;
- Сервер HAFF TradeicsBel (на базе процессоров Intel® Atom™ Processor / Intel® Xeon® Processor E3 Family / Intel® Xeon® Processor E5 Family);
- Сервер «Бевалекс» ТУ BY 100944292.002-2005 (на базе процессоров Intel® Atom™ Processor / Intel® Xeon® Processor E3 Family / Intel® Xeon® Processor E5 Family);
- Сервер «Белсофт» ТУ BY 101231219.003-2005 (на базе процессоров Intel® Atom™ Processor / Intel® Xeon® Processor E3 Family / Intel® Xeon® Processor E5 Family);
- Huawei RH1288 V3;
- KraftWay EL19 / ES29 / ES221
- HP Proliant DL20 Gen9;
- Cisco UCS C220 M4.

ПАК Шлюз поставляется в предустановленном виде.

Перед работой с программно-аппаратным комплексом «Шлюз безопасности Bel VPN Gate 4.1», необходимо выполнить инициализацию в соответствии с документом «Программно-аппаратный комплекс «Шлюз безопасности Bel VPN Gate 4.1». Руководство администратора. Инициализация», а также ознакомиться с документацией, список которой приводится в документе «Программно-аппаратный комплекс «Шлюз безопасности Bel VPN Gate 4.1». Структура документации».

Комплект поставки ПК Bel VPN Gate-V

В комплект поставки ПК Bel VPN Gate-V входят:

- образ виртуальной машины, который содержит:
  - предустановленную операционную систему Debian GNU/Linux 6, в которую входит OpenSSH;
  - предустановленный программный комплекс «Шлюз безопасности виртуальный Bel VPN Gate-V 4.1» со встроенной криптобиблиотекой AvC ver.1.0(РБ.ЮСКИ.13000-01), разработанной ЗАО «Авест».
- внешнее устройство хранения информации: AvPass (ИЯТА.467532.002) или AvBign (ИЯТА.467532.003);
- 2 компакт-диска, на которых находятся:
  - образ виртуальной машины программного комплекса «Шлюз безопасности Bel VPN Gate-V 4.1»;
  - руководство администратора программного комплекса «Шлюз безопасности виртуальный Bel VPN Gate-V 4.1»;
  - дистрибутив программного комплекса «Bel VPN KP 4.1»;
  - руководство администратора программного комплекса «Bel VPN KP 4.1».

В печатном виде поставляются:

- копия сертификата соответствия техническому регламенту Республики Беларусь ТР 2013/027/BY.
- лицензия на использование программного комплекса «Шлюз безопасности виртуальный Bel VPN Gate-V 4.1».
- лицензия на использование программного продукта «Bel VPN KP 4.1» - в случае централизованного удаленного управления более, чем двумя Bel VPN продуктами.

Документация на программный комплекс «Шлюз безопасности виртуальный Bel VPN Gate-V 4.1» также доступна для загрузки на сайте компании: http://www.s-terra.by

Назначение и функции ПК Bel VPN Gate

ПК Bel VPN Gate-V является средством шифрования/дешифрования сетевого трафика с контролем целостности по СТБ 34.101.31 и ГОСТ 28147.

Количество туннелей шифрования – до 10 (Gate 100), до 50 (Gate 1000), до 1000 (Gate 3000) и без ограничений (Gate 7000).

ПК Bel VPN Gate-V обеспечивает:

- создание виртуальных частных сетей (VPN) по технологии IPsec VPN;
- защиту транзитного трафика между различными узлами сети и защиту трафика самого шлюза безопасности на уровне аутентификации/шифрования сетевых пакетов по протоколам IPsec AH и/или IPsec ESP в рамках международных стандартов:
  - Security Architecture for the Internet Protocol – RFC2401
  - IP Authentication Header (AH) – RFC2402
  - 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;
- пакетную stateless фильтрацию трафика;
- контекстную (stateful) фильтрацию для протоколов TCP и FTP;
- работу по расписанию для правил пакетной фильтрации;
- классификацию и маркирование трафика;
- возможность применения различных наборов правил обработки трафика на различных виртуальных сетевых интерфейсах ПК;
- возможность получения сертификатов открытых ключей по протоколу LDAP;
- поддержку сертификатов открытых ключей ГосСУОК;
- событийное протоколирование (по протоколу syslog), с возможностью объединять события в группы и задавать для каждой группы свой независимый уровень протоколирования;
- сбор статистики для мониторинга (по протоколу SNMP v1 и v2c);
- маскировку топологии защищаемого сегмента сети (туннелирование трафика);
- возможность задания дополнительной аутентификации партнера на основе запросов на RADIUS сервер;
- возможность загрузки локальной политики безопасности из внешнего файла;
- защиту сети, подсети и самого шлюза от несанкционированного доступа;
- контроль целостности программной и информационной части программного обеспечения ПАК;
- построение отказоустойчивых схем, в том числе кластерных решений, горячее резервирование и балансировку.

Управление ПК Шлюз осуществляется:

- централизованно-удаленно, посредством программного продукта «Bel VPN KP 4.1»;
- локально и удаленно по протоколу SSH с помощью интерфейса командной строки;
- локально, при помощи конфигурационного текстового файла, описывающего политику безопасности.

ПК Bel VPN Gate-V использует криптографическую библиотеку программного средства электронной цифровой подписи и шифрования «AvC ver.1.0» (РБ.ЮСКИ.13000-01), а также внешнее устройство хранения информации: AvPass (ИЯТА.467532.002) или AvBign (ИЯТА.467532.003) производства ЗАО «Авест».

ПК Bel VPN Gate-V работает под управлением операционной системы Debian GNU/Linux 6, Сервер управления из программного продукта «Bel VPN KP 4.1» - под управлением ОС Windows Server 2003 SP2 Edition (32-bit), Windows Server 2008 SP1 Edition (32-bit,64-bit), Windows Server 2008R2 SP1 Edition (64-bit), Windows Server 2012 Edition (64-bit).

ПК Bel VPN Gate-V сертифицирован в национальной системе подтверждения соответствия Республики Беларусь по требованиям Технического регламента Республики Беларусь «Информационные технологии.

Средства защиты информации. Информационная безопасность» – ТР 2013/027/BY (взаимосвязанные ТНПА:

- хэширование – СТБ 1176.1-99, СТБ 34.101.31-2011 (подраздел 6.9 раздела 6);
- электронная цифровая подпись – СТБ 1176.2-99 (разделы 5, 6), СТБ 34.101.45-2013 (пункты 6.2, 7.1, приложения Б (таблица Б1), Д);
- шифрование и контроль целостности – ГОСТ 28147-89 (разделы 2, 4, 5), СТБ П 34.101.50-2012 (приложения Б-Г), СТБ 34.101.31-2011 (подраздел 6.4 раздела 6);
- генерация случайных данных – СТБ 34.101.47-2012 (пункт 6.2);
- управление ключами – СТБ 34.101.66-2014 (приложение А), управление криптографическими ключами, рекомендованное ОАЦ (Программно-аппаратный комплекс «Шлюз безопасности Bel VPN Gate 4.1». Методика создания и распределения ключевых данных. BY.РТНК.00001-04.1 91 01);
- формат сертификатов и списков отозванных сертификатов – СТБ 34.101.19-2012 (разделы 6-8);
- требования безопасности – СТБ 34.101.27-2011 (класс 1)

).

Архитектура ПК Bel VPN Gate-V

ПК Bel VPN Gate-V состоит из следующих функциональных компонентов:

- Шлюз – виртуальная машина под управлением ОС Debian GNU\Linux 6 и программным обеспечением «Шлюз безопасности виртуальный Bel VPN Gate-V 4.1»;
- Сервер управления – программное обеспечение «Bel VPN KP 4.1», установленное на персональном компьютере под управлением ОС семейства Microsoft Windows.

Модель размещения ПК Шлюз в локальной сети организации приведена на рисунке 1.

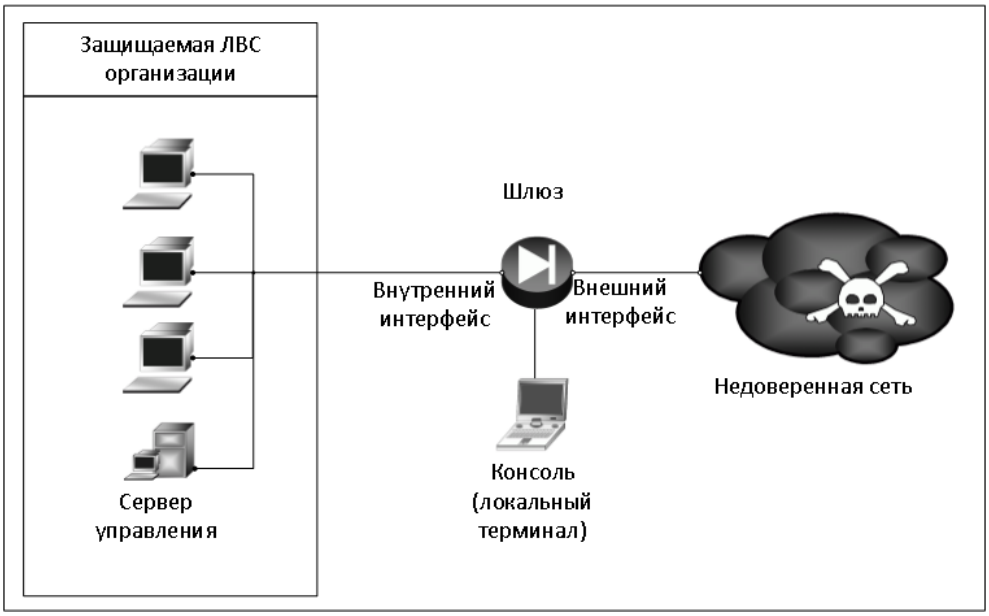

Рисунок 1 – Модель размещения ПК Шлюз в локальной сети организации

Программное обеспечение ПК Шлюз состоит из следующих основных компонентов:

- **VPN daemon** (демон) –часть программного обеспечения ПК Шлюз, обеспечивающая криптозащиту сетевых пакетов посредством реализации протоколов IKE и IPsec.

  Взаимодействует с драйвером (VPN driver), загружая в него конфигурационную информацию и обрабатывая его запросы на создание защищенных соединений (SA). Кроме этого, в демоне выполняется вся работа с сертификатами, событийное протоколирование, сбор статистики и реализована поддержка протоколов SNMP, LDAP, SYSLOG.

  Управляется локальной политикой безопасности – Local Security Policy (LSP).

  LSP (или “native configuration”) имеет текстовое представление и может быть загружена в демон с использованием консоли (cs_console) или при помощи специализированной утилиты (lsp_mgr).

  При загрузке новой LSP все существующие SA уничтожаются.

- **VPN driver** (драйвер) – часть программного обеспечения ПК Шлюз, реализующая перехват, фильтрацию и обработку сетевых пакетов.

  Для каждого перехваченного пакета драйвер применяет список фильтров и, при совпадении параметров пакета (адреса, порты, протокол) с параметрами фильтра, пакет либо передается на обработку демону (VPN daemon), либо пропускается его без обработки, либо уничтожается.

  При загрузке LSP, параметры фильтров и описание действия, которое необходимо выполнить с пакетом, загружаются демоном в драйвер.

- **Cisco-like console** (CLI консоль) – часть программного обеспечения ПК Шлюз, предоставляющая пользователю интерфейс в стиле командной строки Cisco IOS.

  Набор используемых команд консоли является подмножеством команд IOS с некоторыми ограничениями функциональности и дополнительными возможностями.

Как и у IOS, у консоли есть привилегированный и конфигурационный режимы (configure terminal). Однако, в отличие от IOS, изменения настроек вступают в действие не сразу, а только после выхода из конфигурационного режима. В момент выхода из конфигурационного режима, cisco-like конфигурация автоматически конвертируется в native-конфигурацию (LSP) и загружается в демон. Консоль включает в себя:

- интерфейс командной строки для ввода команд конфигурации;
- интерпретатор команд, родственных Cisco;
- обработчик конфигурации. Формирует и обрабатывает конфигурацию из команд консоли и передает ее конвертору.

- **Command Line Utilities** (утилиты командной строки) –служат для общего управления ПК Шлюз.

  Позволяют загружать и просматривать LSP, регистрировать в Базе Продукта предопределенные ключи (pre-shared keys) и сертификаты открытых ключей, получать различную информацию о текущем состоянии Продукта и др.

  Могут быть вызваны из CLI консоли с использованием специальной команды run. .

  Клиент управления (UPClient) – клиентская часть программного продукта «Bel VPN KP 4.1», устанавливается на управляемое устройство (ПК Шлюз, ПАК Шлюз или ПАУ Клиент). Предназначен для применения конфигураций, загружаемых с Сервера управления на целевом (управляемом) устройстве, а также для пересылки журналов аудита и статистической информации с управляемого устройства на Сервер управления.

- **База Продукта** – область файловой системы ПК Шлюз в которой размещаются локальная политика безопасности, сертификаты открытых ключей, предопределенные ключи (pre-shared keys), список интерфейсов, локальные настройки различных модулей, и др.

Схема взаимодействия компонентов программного обеспечения ПК Шлюз приведена на рисунке 2

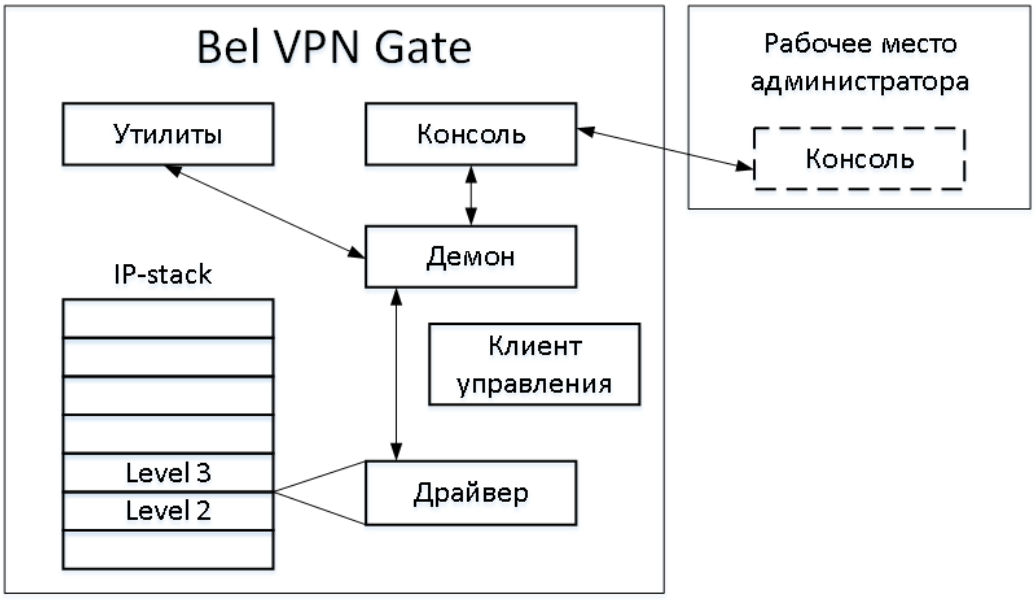

Рисунок 2 Схема взаимодействия модулей

Требования по организационным и административным мерам обеспечения безопасности эксплуатации ПК Bel VPN Gate-V

Общие требования

Для безопасности эксплуатации ПК Bel VPN Gate должны выполняться организационно-технические и административные требования. К ним относятся требования: по физическому размещению ПК, установке программного обеспечения на ПК, средствам защиты от несанкционированного доступа (НСД) к ОС и управлению комплексом, обеспечению бесперебойного режима работы ПАК.

Требования по размещению ПК

При размещении ПК на предприятии, помещения должны удовлетворять следующим требованиям физической безопасности:

- обеспечение круглосуточной охраны корпусов предприятия;
- обеспечение контроля внешнего периметра и внутренних помещений (видеонаблюдение);
- обеспечение пропускного режима;
- двери должны быть прочными и оборудованы надежными механическими замками;
- помещения должны быть оборудованы системой пожарной сигнализации;
- должен вестись Журнал выдачи ключей от входных дверей в офисы, в котором регистрируется время сдачи и выдачи ключей, фамилия сотрудника, взявшего или сдавшего ключ дежурному вахтеру по зданию;
- принять меры по исключению несанкционированного доступа в помещения, в которых размещен ПАК Шлюз, посторонних лиц, не являющихся персоналом, допущенным к работе в этих помещениях. В случае необходимости присутствия посторонних лиц в указанных помещениях, должен быть обеспечен контроль над их действиями и обеспечена невозможность негативных действий с их стороны на ПК
- внутренняя планировка, расположение и укомплектованность рабочих мест в помещениях должны обеспечивать исполнителям работ сохранность доверенных им ПАК, конфиденциальной информации, в том числе ключевой информации.

Административные меры безопасности

Безопасная эксплуатация ПК и обращение с СКЗИ должны регламентироваться следующими документами, которые следует разработать:

- соглашение о неразглашении сведений, составляющих коммерческую тайну организации, которое сотрудники подписывают при приеме на работу;
- перечень сведений, составляющих коммерческую тайну организации, утвержденный Генеральным директором;
- инструкция по обращению с сертифицированными Оперативно-аналитическим центром при Президенте Республики Беларусь шифровальными средствами (средствами криптографической защиты информации) на предприятии.
- журнал учета СКЗИ, тестовых ключей на предприятии.
- журнал регистрации администраторов безопасности.
- журнал учета обращения эталонных CD дисков на предприятии.

Обязательно наличие опечатываемого сейфа, оборудованного двумя внутренними замками, для хранения СКЗИ, тестовых ключей, эталонных CD дисков с продуктом, другой конфиденциальной информации. Для сейфа должно быть два ключа – основной ключ хранится у сотрудника, отвечающего за СКЗИ, а дубликат – в опечатанном его личной печатью пенале в сейфе руководителя.

Запрещается:

- обрабатывать на ПАК информацию, содержащую государственную тайну;
- осуществлять несанкционированное вскрытие ПАК.

Требования по защите ПК от несанкционированного доступа (НСД)

При организации работ на ПАК, должны быть выполнены следующие требования по защите ПАК от НСД:

- Администратором ПАК назначается администратор безопасности.
- Право доступа к ПАК имеет только администратор безопасности.
- Администратор безопасности должен ознакомиться со всей документацией, прилагаемой к ПАК.
- Аутентификация администратора безопасности основана на пароле, который должен вводиться им с клавиатуры собственноручно при осуществлении доступа в ОС, не отображаясь на экране монитора в явном виде, идентификация основана на идентификаторе, который вводится с клавиатуры. При первом доступе администратор безопасности должен заменить пароль на отличный от установленного при инсталляции ПАК.
- Право доступа к режиму управления ПАК (пользовательскому интерфейсу) имеет только администратор с уровнем привилегий 15. Об уровнях привилегий и их назначении см. Руководство администратора.
- Имя администратора с уровнем привилегий 15 должно быть уникальным и не превышать 8 символов.
- Имя администратора с уровнем привилегий 15 должно начинаться с буквы латинского алфавита (строчной или прописной). Далее могут идти буквы латинского алфавита (строчные или прописные), цифры, _ (подчеркивание) и - (дефис).
- Настройку ПАК (назначение IP-адресов интерфейсам, создание политики безопасности, регистрацию сертификатов, другие дополнительные настройки) осуществляет только администратор безопасности в соответствии с Руководством администратора.
- Необходимо организовать систему протоколирования и аудита, и вести регулярный анализ результатов аудита с целью выявления нарушений несанкционированного доступа к ПАК.
- Администратор безопасности не имеет права сообщать никому пароль доступа к ПАК.
- Периодичность смены пароля определяется принятой политикой безопасности, но не должна превышать 1 год.

Запрещается:

- Оставлять без контроля ПАК после прохождения аутентификации, ввода ключевой информации либо иной конфиденциальной информации.
- Осуществлять несанкционированное администратором безопасности копирование ключевых носителей.
- Разглашать содержимое носителей ключевой информации или передавать сами носители лицам, к ним не допущенным, выводить ключевую информацию на монитор, принтер и т.п. иные средства отображения информации.
- Использовать ключевые носители в режимах, не предусмотренных функционированием ПАК.
- Записывать на ключевые носители постороннюю информацию.

Защита ПАК и ключевой информации от НСД, должна обеспечиваться не только в режиме функционирования, но и при проведении ремонтных и регламентных работ.

Требования по установке ПО на ПАК

ПАК Шлюз поставляется с специальным образом настроенной операционной системой и инсталлированным ПО.

Администратору безопасности **запрещается** несанкционированное изменение среды функционирования ПАК, а именно:

- модернизация ОС, включая установку штатных обновлений;
- добавление/отключение отдельных сервисов операционной системы (по отношению к состоянию операционной системы на момент поставки ПАК);
- установка дополнительных приложений;
- внесение изменений в ПО ПАК;
- модификация файлов, содержащих исполняемые коды, при их хранении на жестком диске;
- добавление/удаление аппаратных компонент (в том числе сетевых карт, жестких дисков и т.п.).

Нарушение этих ограничений рассматривается, как нарушение целостности ПАК Шлюз и приводит к срыву заявленной функциональности ПАК, и является основанием для отказа в сервисе технического сопровождения и поддержки ПАК.

Разрешается:

- при нарушении содержимого жесткого диска ПАК восстановить ПО, используя образ диска и другое дополнительное ПО, предоставляемое компанией С-Терра Бел. Перед этим необходимо ознакомиться с Инструкцией по восстановлению ПАК;
- после восстановления ПО жесткого диска или обновления ПО провести контроль целостности установленного ПО в соответствии с документацией.

