УТВЕРЖДЕНО

BY.РТНК.00001-03.01 13 01-ЛУ

Программно-аппаратный комплекс «Шлюз безопасности Bel VPN Gate 3.0.1»

ОПИСАНИЕ ПРОГРАММЫ

BY.РТНК.00001-03.01 13 01

Листов 14

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

2012

1. Общее описание

Программно-аппаратный комплекс «Шлюз безопасности Bel VPN Gate 3.0.1» предназначен для защиты межсетевого трафика и удаленного доступа с применением средств криптографической защиты информации (далее – СКЗИ) в ведомственных (корпоративных) распределенных вычислительных IP-сетях, а также пакетной фильтрации трафика (межсетевой экран).

Программно-аппаратный комплекс «Шлюз безопасности Bel VPN Gate 3.0.1» включает:
– программный комплекс «Шлюз безопасности Bel VPN Gate 3.0.1», содержащий программное средство ЭЦП и шифрования «AvCrypt ver 5.1» (РБ.ЮСКИ.09000-02, производитель ЗАО «Авест»), а также программные модули «Криптоплагин», «Утилита для работы с контейнером» для вызова криптографических процедур из «AvCrypt ver 5.1»;
– ОС Red Hat Linux 9;
– аппаратную платформу (сервер, терминал, ПЭВМ) с архитектурой Intel x86;
– внешнее устройство хранения информации (USB-носитель), совместимое с «AvCrypt ver 5.1» (РБ.ЮСКИ.09000-02) – по усмотрению пользователя;
– комплект программной документации.

Программный комплекс «Шлюз безопасности Bel VPN Gate 3.0.1» представляет собой модификацию Программного комплекса «Шлюз безопасности Bel VPN Gate 3.0» в соответствии с требованиями ОКР «Разработать аппаратно-программное устройство IP шифрования для обработки информации ограниченного распространения» (утверждены ОАЦ 13.05.2011г., шифр «Река»).

Программно-аппаратный комплекс «Шлюз безопасности Bel VPN Gate 3.0.1» обеспечивает:
– автоматическое шифрование/расшифрование информации по ГОСТ28147-89 в режиме гаммирования с обратной связью;
– скорость шифрования (по ГОСТ 28147-89 в режиме UDP, пакеты 1400 байт) зависит от используемой аппаратной платформы;
– количество туннелей шифрования (и одновременной работы в сети с доверенными Продуктами – совместимыми шлюзами и клиентами) – от 2 туннелей до неограниченного количества;
– контроль целостности пакетов данных – имитозащита по ГОСТ28147-89 или по стандарту СТБ 1176.1-99 в режиме HMAC (для совместимости с Bel VPN Gate 3.0);
– выработку (проверку) ЭЦП от хэш-значения, выработанного по СТБ 34.101.31-2011;
– протокол формирования ключей по алгоритму Диффи-Хэллмана;
– возможность хранения ключей/сертификатов на внешнем устройстве хранения информации (USB-носитель), совместимом с «AvCrypt ver 5.1»;
– возможность генерации сеансовых ключей для работы в сети с использованием ДСЧ внешнего устройства хранения информации (USB-носитель), совместимого с «AvCrypt ver 5.1»;
– проверку целостности программного обеспечения криптомодулей с использованием алгоритма СТБ 1176.1-99;
– пакетную фильтрацию IP-пакетов (функции межсетевого экрана);
– гибкую настройку с использованием Cisco-ориентированной системы команд управления;
– систему мониторинга и аудита работы, ведение автономного журнала аудита;
– защиту от НСД – обнаружение вскрытия корпуса, защищенного пломбировочной индикаторной наклейкой;
– круглосуточную необслуживаемую работу;
– питание осуществляется от сети переменного тока напряжением 230 В, частотой 50 Гц.

Шлюз безопасности «Bel VPN Gate 3.0.1» использует для шифрования/расшифрования защищаемой информации криптографические библиотеки программного средства электронной цифровой подписи и шифрования «AvCrypt ver. 5.1» (РБ.ЮСКИ.09000-02), которое реализует:

– белорусские алгоритмы криптографического преобразования в соответствии с Государственным стандартом Республики Беларусь ГОСТ 28147-89;

– функции хеширования в соответствии с Государственным стандартом Республики Беларусь СТБ 1176.1-99;

– функции хеширования в соответствии с Государственным стандартом Республики Беларусь СТБ 34.101.31-2011;

– процедуру выработки и проверки электронной цифровой подписи в соответствии с Государственным стандартом Республики Беларусь СТБ 1176.2-99;

– процедуру выработки псевдослучайных данных в соответствии с РД РБ 07040.1202-2003 «Банковские технологии. Процедуры выработки псевдослучайных данных с использованием секретного параметра».

В «Шлюзе безопасности Bel VPN Gate 3.0.1» реализованы следующие международные стандарты архитектуры IKE/IPsec:

- Security Architecture for the Internet Protocol (SA) – 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

Bel VPN Gate функционирует в программной среде – ОС Red Hat Linux 9.

Управление Bel VPN Gate осуществляется:

- централизованно посредством графического интерфейса центра управления CiscoWorks VPN/Security Management Solution v.2.2 – CiscoWorks Router Management Center (Router MC)
- с помощью интерфейса командной строки

Шлюз безопасности «Bel VPN Gate 3.0.1» реализует политику защищенного соединения следующими способами:

- для исходящего трафика, направляемого другому доверенному Продукту[1] защищенной виртуальной частной вычислительной сети (далее ВЧВС), шлюз устанавливает или использует существующее защищенное соединение;
- для исходящего трафика, не направляемого доверенному Продукту защищенной ВЧВС, шлюз не задействует механизмы безопасности, и, таким образом, защищенное соединение не устанавливается;
- для входящего трафика, поступающего от доверенного Продукта защищенной ВЧВС, шлюз устанавливает или использует существующее защищенное соединение;
- для входящего трафика, не связанного с доверенным Продуктом защищенной ВЧВС, шлюз не задействует механизмы безопасности, и, таким образом, защищенное соединение не устанавливается.

Продукты защищенных ВЧВС обмениваются идентификационной информацией и выполняют процедуры аутентификации. Защищенное соединение может быть установлено только после выполнения процедур взаимной аутентификации Продуктов ВЧВС.

Рассматриваются следующие варианты построения защищенной ВЧВС:

- объединение вычислительных сетей (далее ВС), т.е. создание защищенных соединений между различными локальными вычислительными сетями (далее ЛВС);
- объединение сегментов ВС, т.е. создание защищенных соединений между различными сегментами одной ЛВС;
- объединение ЛВС с удаленными пользователями, т.е. создание защищенных соединений между ЛВС и отдельными рабочими местами пользователей сети (в том числе и мобильных).

Bel VPN Gate может функционировать в роли резервного шлюза ВЧВС по отношению к основному шлюзу ВЧВС и находиться, таким образом, в режиме «горячей» замены. В случае выхода из строя основного шлюза ВЧВС Bel VPN Gate продолжает осуществлять все функции вышедшего из строя шлюза ВЧВС максимально прозрачно (первоначально с небольшой задержкой, связанной в некоторых случаях с необходимостью переустановки защищенных соединений) для всех участников информационного взаимодействия, использующих при взаимодействии основной шлюз ВЧВС. При устранении неисправности

[1] здесь и далее используется терминология СТБ 34.1.101.1-3-2004 «Информационные технологии и безопасность. Критерии оценки безопасности информационных технологий. Часть 1-3»

на основном шлюзе ВЧВС и возобновлении его функционирования, Bel VPN Gate осуществляет передачу управления основному шлюзу ВЧВС и продолжает функционировать в роли резервного шлюза ВЧВС.

Bel VPN Gate может взаимодействовать (обмениваться данными) с другими Продуктами ВЧВС через защищенное соединение (канал) с обеспечением защиты информационного потока и, одновременно, через незащищенное соединение (канал) без обеспечения защиты информационного потока. Таким образом, при помощи Bel VPN Gate существует возможность создания как защищенных ВЧВС-соединений, так и не защищенных ВЧВС-соединений (фильтрация потоков данных).

Bel VPN Gate 3.0.1 предоставляет следующие функциональные возможности:

- обеспечивает идентификацию и взаимную аутентификацию средств построения ВЧВС в рамках протокола IKE (The Internet Key Exchange, спецификация RFC 2409);
- поддерживает метод аутентификации на предопределенном ключе (Pre-Shared Key);
- поддерживает метод аутентификации электронной цифровой подписью (Signatures);
- поддерживает: белорусские алгоритмы криптографического преобразования в соответствии с Государственным стандартом Республики Беларусь ГОСТ 28147-89; функции хеширования в соответствии с Государственным стандартом Республики Беларусь СТБ 1176.1-99; функции хеширования в соответствии с Государственным стандартом Республики Беларусь СТБ 34.101.31-2011; процедуру выработки и проверки электронной цифровой подписи в соответствии с Государственным стандартом Республики Беларусь СТБ 1176.2-99, процедуру выработки псевдослучайных данных в соответствии с РД РБ 07040.1202-2003 «Банковские технологии. Процедуры выработки псевдослучайных данных с использованием секретного параметра»;
- поддерживает формат цифровых сертификатов публичных ключей X.509 версии. 3.0;
- в рамках протокола IKE поддерживает различные режимы обмена цифровыми сертификатами;
- поддерживает обработку списка отозванных сертификатов (Certificate Revocation List, CRL версии 2), Продукт не допускает создания защищенного соединения на базе просроченных и отозванных сертификатов;
- поддерживает два режима первой фазы протокола IKE – Main Mode и Aggressive Mode, Продукт поддерживает информационные обмены протокола IKE – Quick mode, Transaction Exchanges, Informational Exchanges;
- поддерживает необходимые типы Delete Payload в сообщениях Informational Exchange протокола IKE, а также необходимую внутреннюю логику процедур с целью восстановления прерванных защищенных соединений между шлюзами ВЧВС;
- обеспечивает целостность, аутентификацию и конфиденциальность данных на уровне передаваемых IP-пакетов в рамках протоколов AH (IP Authentication Header, спецификация RFC 2402) и ESP (IP Encapsulating Security Payload, спецификация RFC 2406);
- обеспечивает использование протокола AH в туннельном или транспортном режимах, а также в комбинации с протоколом ESP;
- обеспечивает использование протокола ESP в туннельном или транспортном режимах, а также в комбинации с протоколом AH;
- обеспечивает надежность защищенных соединений в рамках протокола Dead Peer Detection (DPD);
- обеспечивает пакетную фильтрацию IP-трафика с использованием информации в полях заголовков сетевого и транспортного уровней
- обеспечивает возможность регулирования степени загрузки процессора обработкой трафика, и возможность выборочного «сбрасывания» пакетов в зависимости от заполненности очереди на обработку и значения поля ToS пакета.

2. Описание в терминах подсистем

ПК «Шлюз безопасности Bel VPN Gate 3.0.1» представляет собой набор взаимодействующих между собой функциональных подсистем, которые работают как на уровне приложения (Application Level), так и на уровне ядра (Kernel Level) операционной системы Red Hat Linux 9. Структурно-функциональная схема Bel VPN Gate приведена на рисунке 1.1.

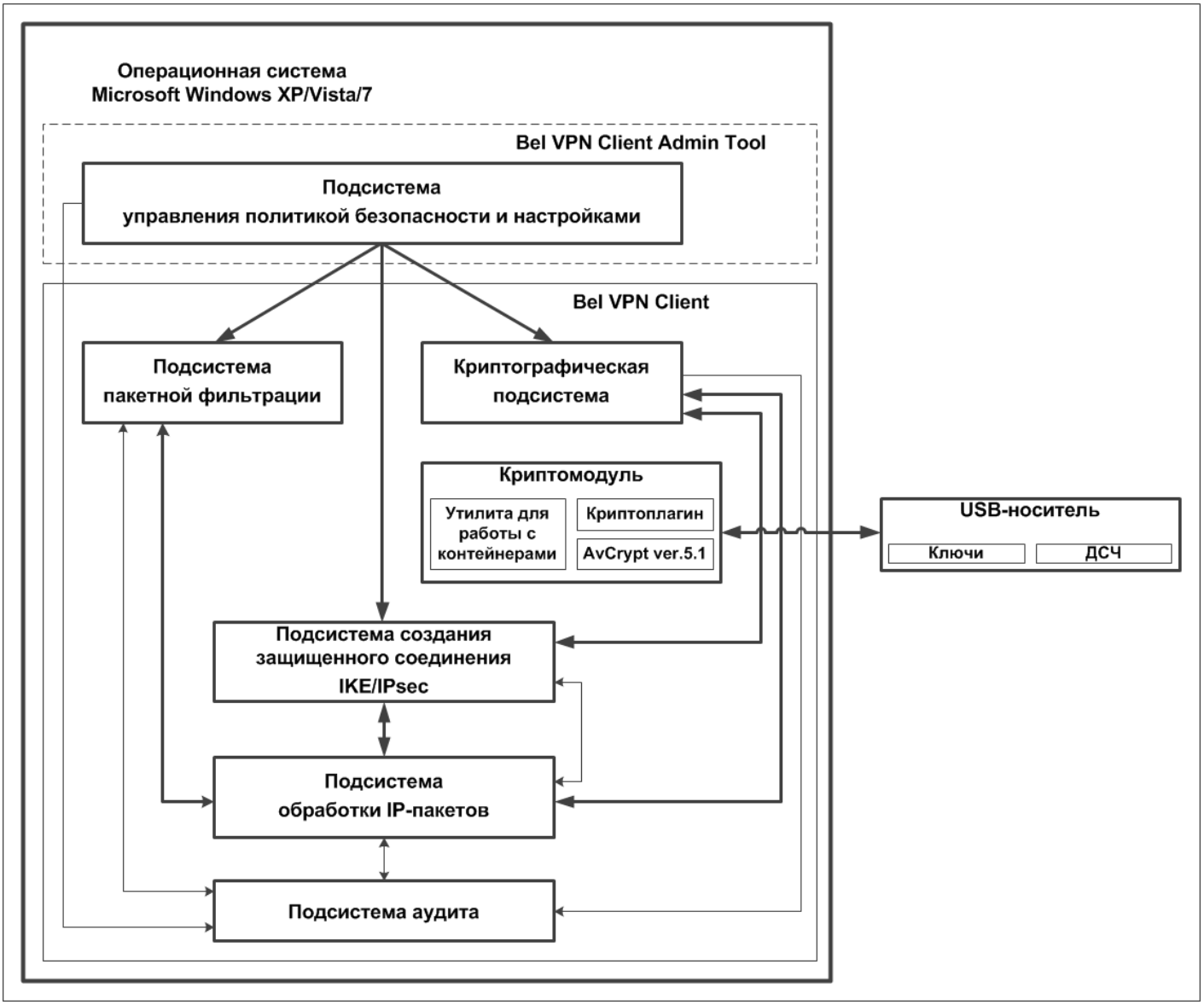

Рис.1.1. Структурно-функциональная схема «Bel VPN Gate 3.0.1»

В состав Bel VPN Gate входят:

- **Подсистема обработки IP-пакетов** (VPN драйвер) – обеспечивает перехват пакетов из IP стека между уровнем драйвера сетевой карты и уровнем IP. Перехваченные пакеты после грубого первичного анализа поступают на обработку. В подсистеме происходит фильтрация пакетов, по результатам фильтрации пакет либо пропускается без изменений, либо «сбрасывается»/уничтожается, либо передается на «IPsec-обработку». «IPsec-обработка» выполняется «за один проход», то есть, после этой обработки пакет либо уничтожается, либо возвращается в стек, повторно пакет не анализируется. Модульный состав подсистемы и описание функциональных возможностей безопасности приведены в разделе 0;
- **Подсистема создания защищенного соединения IKE/IPsec** – обеспечивает подготовку данных для обработки трафика подсистемой обработки IP-пакетов. Подсистема получает локальную политику безопасности, сформированную Администратором в подсистеме управления политикой и настройками, обрабатывает полученную информацию и передает (копирует) ее в драйвер. Модульный состав подсистемы и описание функциональных возможностей безопасности приведены в разделе 0;
- **Подсистема пакетной фильтрации** – обеспечивает подготовку данных для проведения пакетной фильтрации подсистемой обработки IP-пакетов. Подсистема получает набор правил фильтрации

(Access List), сформированный Администратором в подсистеме управления политикой и настройками, обрабатывает полученную информацию и передает (копирует) ее в драйвер. Модульный состав подсистемы и описание функциональных возможностей безопасности приведены в разделе 0;

- **Подсистема управления политикой безопасности и настройками** – обеспечивает Администратору интерфейс для управления шлюзом безопасности. Описание функциональных возможностей подсистемы приведены в разделе 0. Подсистема поддерживает четыре режима управления:
    - централизованно посредством графического интерфейса центра управления CiscoWorks VPN/Security Management Solution
    - централизованно удаленно посредством графического интерфейса Cisco Security Manager версии 3.2
    - с помощью интерфейса командной строки CSP VPN Command Line Interface, CLI (используется подмножество команд Cisco IOS) и использования специализированных команд;
    - путем загрузки управляющей информации из внешнего файла и использования специализированных команд;
- **Подсистема аудита** – совместно с операционной системой обеспечивает сбор, хранение событий аудита и управление аудитом. Модульный состав подсистемы и описание функциональных возможностей безопасности приведены в разделе 0;
- **Криптографическая подсистема** – предоставляет доступ к функциям криптографического модуля уровня ядра операционной системы драйверам и прикладным программам, предоставляют криптографические функции на уровне ядра ОС, используя для этого интерфейс соответствующий RFC 2628. Модульный состав подсистемы и описание функциональных возможностей безопасности приведены в разделе 0;
- **Криптомодуль на основе AvCrypt ver. 5.1** – обеспечивает формирование и управление криптографическими ключами, а также реализацию следующих криптографических алгоритмов:
    - белорусские алгоритмы криптографического преобразования в соответствии с Государственным стандартом Республики Беларусь ГОСТ 28147-89;
    - функции хеширования в соответствии с Государственным стандартом Республики Беларусь СТБ 1176.1-99;
    - функции хеширования в соответствии с Государственным стандартом Республики Беларусь СТБ 34.101.31-2011;
    - процедуру выработки и проверки электронной цифровой подписи в соответствии с Государственным стандартом Республики Беларусь СТБ 1176.2-99;
    - процедуру выработки псевдослучайных данных в соответствии с РД РБ 07040.1202-2003 «Банковские технологии. Процедуры выработки псевдослучайных данных с использованием секретного параметра».

- **Операционная система Red Hat Linux 9** обеспечивает:
    - совместно с подсистемой аудита «Bel VPN Gate 3.0.1» сбор, хранение событий аудита и управление аудитом;
    - идентификацию и аутентификацию Администратора «Bel VPN Gate 3.0.1» до осуществления доступа непосредственно к шлюзу безопасности с целью администрирования. Аутентификация Администратора основана на пароле, который вводится с клавиатуры, не отображаясь на экране монитора в явном виде, идентификация основана на идентификаторе, который вводится с клавиатуры;
    - средства защиты комплекса средств безопасности Продукта связанные с тестированием среды функционирования «Bel VPN Gate 3.0.1», а также его восстановлением после сбоев и прерываний обслуживания, тестированием на предмет контроля целостности и корректности функционирования.

2.1 Подсистема обработки IP-пакетов (VPN драйвер)

Подсистема обработки IP-пакетов обеспечивает перехват пакетов из IP стека между уровнем драйвера сетевой карты и уровнем IP и их обработку в соответствии с политикой безопасности и локальными настройками «Bel VPN Gate 3.0.1».

В состав подсистемы обработки IP-пакетов входят следующие исполняемые модули и библиотеки:

- **Библиотека вспомогательных функций** предоставляет платформо-независимый интерфейс к некоторым функциям ядра операционной системы: примитивам синхронизации, таймерам, динамическому распределению памяти, выводу отладочных сообщений, работе с текстовыми строками и др.;
- **Перехватчик пакетов** – обеспечивает перехват, преобразование пакетов в платформо-независимый формат и обратно, передачу пакетов на обработку IPsec, отправку пакетов в сеть, предоставление уникальных имен сетевых интерфейсов;
- **Универсальный интерфейс для обмена данными с приложениями** - предоставляет платформо-независимый интерфейс для пересылки сообщений из приложений в драйвер;
- **Диспетчер пакетов** - реализует логику обработки входящих и выходящих пакетов. Определяет последовательность вызовов функций инкапсуляции/декапсуляции пакетов в IPsec протоколы, порядок производимых проверок, пакетной фильтрации. По результатам фильтрации пакет либо пропускается без изменений, либо «сбрасывается»/уничтожается, либо передается на «IPsec-обработку». Пакеты, которые должны пройти «IPsec-обработку» помещаются в очередь, при этом может быть включена функция дополнительного анализа, которая может уничтожать эти пакеты в зависимости от степени заполнения очереди и поля ToS заголовка пакета (если эта функция не включена, то пакеты уничтожаются при заполнении очереди без анализа их содержимого);
- **Библиотека функций IPsec** содержит общие для ESP и AH протоколов функции по обработке пакета (защита от replay-атак, формирование заголовков, интерфейс с криптографической подсистемой и т.д.)
- **Модуль протокола ESP** выполняет инкапсуляцию/декапсуляцию пакетов в протокол ESP;
- **Модуль протокола AH** выполняет инкапсуляцию/декапсуляцию пакетов в протокол AH;
- **Библиотека вспомогательных функций для обработки пакетов** – проверка контрольных сумм, проверка целостности пакетов, извлечение полей заголовков;
- **Модуль пакетной фильтрации** – хранение и поиск правил для обработки пакетов, поддержка хеш-таблицы для ускорения поиска;
- **База данных IPsec SA** – хранение и поиск IPsec SA;
- **Библиотека упаковки структур** реализует протокол обмена данными с приложениями - преобразует внутренние структуры драйвера в “плоское” представление и обратно (сериализация/десериализация данных);
- **Модуль управления** – загрузка правил обработки пакетов, IPsec SA из приложения. Отсылка запросов на IPsec SA в приложение;
- **Модуль протоколирования** – обеспечение интерфейса для протоколирования событий и управления уровнями протоколирования, пересылка сообщений на пользовательский уровень;
- **Модуль фрагментации IP-пакетов** обеспечивает стандартный механизм для фрагментации и сбора IP пакетов из фрагментов;
- **Модуль идентификации сетевых интерфейсов** определяет соответствие физических сетевых интерфейсов логическим идентификаторам, используемым при конфигурировании. Этот модуль реплицирует соответствующую информацию, хранимую в базе данных настроек Продукта;
- **Модуль информации о сетевых интерфейсах** – получение параметров сетевых интерфейсов (например, IP-адрес, маска).

2.2 Подсистема создания защищенного соединения IKE/IPsec

Подсистема создания защищенного соединения IKE/IPsec – обеспечивает подготовку данных для обработки трафика подсистемой обработки IP-пакетов. Подсистема получает локальную политику безопасности, сформированную Администратором в подсистеме управления политикой и настройками, обрабатывает полученную информацию и передает (копирует) ее в драйвер.

- Подсистема обеспечивает формирование и согласование с другим средством построения ВЧВС сеансовых ключей, которые затем используются подсистемой обработки IP-пакетов. Параметры этих ключей, криптографические алгоритмы, использующиеся для обработки трафика, параметры протокола согласования ключей задаются в политике безопасности «Bel VPN Gate 3.0.1» .
- Подсистема реализует протокол IKE и обеспечивает согласование IKE контекстов (IKE Security Associations, SA) в рамках протокола IKE.
- Подсистема реализует расширения протокола IKE, которые используются для дополнительной аутентификации партнеров и для взаимного дополнительного конфигурирования средств построения ВЧВС.
- Подсистема обеспечивает хранение, разбор, проверку подписи, срока применимости, области использования, построение цепочек сертификатов X.509 v.3. Если для построения цепочек сертификатов необходим их поиск и доставка из хранилища (Directory), то подсистема обеспечивает эту функциональность, используя протокол LDAP. Если сертификаты могут быть досрочно отозваны, то сервис обеспечивает поиск и доставку CRL v.2, блокируя использование отозванных сертификатов для аутентификации партнеров при создании соединений. Параметры работы с сертификатами задаются в политике безопасности «Bel VPN Gate 3.0.1» .
- Подсистема реализует протоколы IPsec AH и IPsec ESP и обеспечивает согласование IPsec контекстов (IPsec Security Associations, SA) в рамках протокола IKE.
- Подсистема обеспечивает взаимодействие с подсистемами управления политикой безопасности и настройками, обработки IP-пакетов, криптографической подсистемой и подсистемой аудита.

В состав подсистемы создания защищенного соединения IKE/IPsec входят следующие исполняемые модули и библиотеки:

- **Модуль начальной загрузки и инициализации** выполняет регистрацию подсистемы в операционной системе, в определенном порядке вызывает функции инициализации остальных модулей (для которых инициализация необходима), при этом стартуют внутренние очереди событий, служебные нити, загружаются необходимые динамические библиотеки. Фактически, модуль начальной загрузки и инициализации представляет собой main и непосредственно вызываемые из main статические библиотеки;
- **Модуль-менеджер** используется в качестве регистратора вспомогательных подмодулей. Желающий получить некоторый сервис модуль обращается к модулю-менеджеру с запросом, а модуль-менеджер обеспечивает поиск и загрузку необходимых динамических библиотек. Также модуль менеджер содержит базовые примитивы контроля использования объектов (smart pointers, reference counters), что позволяет реализовать горячую загрузку и замену модулей. Модуль-менеджер представляет собой динамическую библиотеку, которая статически связывается с подсистемой;
- **Модуль интерфейса с другими приложениями** поддерживает очереди сообщений, которые используются для межпроцессных обменов с другими приложениями. Все управляющие воздействия от программ пользовательских интерфейсов «Bel VPN Gate 3.0.1» поступают в подсистему через этот модуль. Модуль обеспечивает сериализацию-десериализацию данных и выполнен в виде набора статических библиотек;
- **Модуль интерфейса с драйверами** поддерживает очереди сообщений, которые используются для межпроцессных обменов с подсистемой обработки IP-пакетов и криптографической подсистемой. Модуль обеспечивает сериализацию-десериализацию данных и выполнен в виде статической библиотеки;
- **Модуль обработки системных событий** и асинхронных вызовов поддерживает очередь внутренних сообщений, которые используются модулями для асинхронных вызовов функций. Кроме того, в эту же очередь помещаются события прихода сигналов от внутренних таймеров, прихода сетевых пакетов. При инициализации модуля создаются несколько рабочих нитей, одна из них контролирует состояние очереди событий и, как только в очереди появляется событие, начинает его обработку, при этом контроль очереди событий передается следующей нити. Таким образом, нити тоже образуют очередь. Нить, выполнившая обработку события, добавляется в очередь нитей. Если очередь событий пуста, то все нити ждут, если очередь нитей пуста, то необработанные события накапливаются в очереди событий. Такой механизм позволяет реализовать многонитевую обработку, но не использует порождение/удаление нитей в процессе работы. Все, внешние по

отношению к подсистеме события, проходят через очередь событий, кроме того, через эту же очередь проходят все внутренние асинхронные вызовы. Модуль выполнен в виде набора статических библиотек;

- **Модуль трансляции политики безопасности** выполняет преобразование данных из текстового представления политики безопасности во внутренние структуры подсистемы. При трансляции выполняется проверка синтаксиса политики и согласованности составляющих ее правил. После проверки политика безопасности передается на исполнение. Если политика безопасности загружалась из файла и ее проверка прошла успешно, то политика безопасности сохраняется во внутреннем хранилище «Bel VPN Gate 3.0.1» . Модуль выполнен в виде набора статических библиотек;
- **Модуль хранения политик** безопасности обеспечивает чтение-запись политики безопасности во внутреннее хранилище «Bel VPN Gate 3.0.1» . Модуль выполнен в виде набора статических библиотек;
- **Модуль исполнения политики** безопасности осуществляет управление работой подсистемы создания защищенного соединения в соответствии с загруженной политикой безопасности. При загрузке политики производится передача информации о правилах фильтрации и обработки пакетов в подсистему обработки IP-пакетов, модули протоколирования, статистики, протокольные и сертификатные модули получают свои настройки. Затем модуль исполнения политики ожидает запросов от подсистемы обработки IP-пакетов на создание соединений. При получении такого запроса модуль передает этот запрос в модуль реализации протокола IKE и обеспечивает модуль IKE необходимой информацией (предложения партнеру, выбор из предложений партнера подходящего для «Bel VPN Gate 3.0.1» , проверка аутентификационной информации партнера). При успешном создании соединения параметры этого соединения транслируются из модуля реализации протокола IKE в подсистему обработки IP-пакетов, если же соединение установить не удалось, то подсистему обработки IP-пакетов сообщается об отказе в создании соединения. Модуль выполнен в виде набора статических библиотек;
- **Модуль хранения локальных настроек** обеспечивает чтение-запись во внутреннее хранилище «Bel VPN Gate 3.0.1» параметров, которые настраиваются вне политики безопасности (список интерфейсов, на которых он работает, настройки поведения при отсутствии загруженной политики безопасности). Модуль выполнен в виде набора статических библиотек;
- **Модуль реализации протокола IKE** и его расширений: IKE-cfg, XAUTH, ESP through NAT является самым большим по объему модулем подсистемы. Протокол IKE используется для согласования параметров IPsec соединений между партнерами, взаимной аутентификации партнеров по IPsec, дополнительной настройки (IKE-cfg), обмена сертификатами партнеров и промежуточными сертификатами для построения цепочек. Модуль IKE выполняет построение IPsec соединений либо по запросу модуля исполнения локальной политики, либо при получении пакета от партнера. Модуль IKE реализует протокольную часть взаимодействия. Параметры предложений партнеру, выбор параметров для ответов, ограничения на аутентификационные данные партнеров модуль IKE запрашивает у модуля исполнения локальной политики. Модуль выполнен в виде набора статических библиотек;
- **База активных IPsec SA** соединений содержит актуальную информацию обо всех установленных в настоящий момент IPsec соединениях. Модуль выполнен в виде статической библиотеки;
- **Модуль обработки X.509 сертификатов** выполняет кодирование/декодирование данных в соответствии со стандартами X.509 (RFC 3280), построение цепочек сертификатов, проверку срока годности сертификата, проверки по спискам отозванных сертификатов, вызов криптографических операций подписи и проверки подписи с использованием соответствующих ключей. Данный модуль является основным сертификатным модулем, который управляет работой остальных модулей сертификатного блока, предоставляя интерфейс для работы с их функциональностью. Режим обработки списков отозванных сертификатов устанавливается из модуля исполнения политики безопасности;
- **Модуль хранения X.509 сертификатов** обеспечивает чтение-запись сертификатов во внутреннее хранилище, поиск сертификатов, хранение приватных ключей или информации о способе выполнения криптоопераций с приватным ключом для локальных сертификатов;
- **PKSC модули** предоставляют возможности упаковки/распаковки/генерации данных в соответствии со стандартами PKCS#5, PKCS#7, PKCS#8, PKCS#10, PKCS#12, необходимых для функционирования «Bel VPN Gate 3.0.1» ;

- **Модуль base64** упаковывает/распаковывает данные в соответствии с этой кодировкой;
- **Модуль протокола LDAP** реализует протокол LDAP версии 3 и используется модулем обработки сертификатов для доставки промежуточных CA-сертификатов для построения цепочек и для доставки CRL. Параметры этого модуля настраиваются модулем исполнения политики безопасности;
- **Модуль работы с сетевыми интерфейсами** обеспечивает контроль активности сетевых интерфейсов, получение из подсистемы обработки IP-пакетов информации об их свойствах. Модуль отслеживает изменения сетевой конфигурации аппаратной платформы. Модуль выполнен в виде набора статических библиотек.

2.3 Подсистема пакетной фильтрации

Подсистема пакетной фильтрации обеспечивает подготовку данных для проведения пакетной фильтрации подсистемой обработки IP-пакетов. Подсистема получает набор правил фильтрации (Access List), сформированный Администратором в подсистеме управления политикой и настройками, обрабатывает полученную информацию и передает (копирует) ее в подсистему обработки IP-пакетов (драйвер). Подсистема совместно с подсистемой обработки IP-пакетов обеспечивает пакетную фильтрацию входящей во внутреннюю ВС и исходящей из внутренней ВС информации с использованием информации в полях заголовков IP-пакетов сетевого и транспортного уровней.

В рамках фильтрации информации сетевого уровня подсистема обеспечивает:

- фильтрацию по IPv.4 адресам;
- фильтрацию по полю “протокол” IP-заголовка v.4.

В рамках фильтрации на основе информации транспортного уровня обеспечивает:

- фильтрацию по направлению установления TCP-соединений;
- фильтрацию по портам для протоколов TCP и UDP.

В состав подсистемы пакетной фильтрации входят следующие исполняемые модули и библиотеки:

- **Модуль трансляции правил фильтрации** выполняет преобразование данных из текстового представления правил пакетной фильтрации во внутренние структуры подсистемы. При трансляции выполняется проверка синтаксиса и согласованности правил. После проверки набор правил пакетной фильтрации передается в **Модуль пакетной фильтрации** подсистемы обработки IP-пакетов. Модуль выполнен в виде набора статических библиотек.

2.4 Подсистема управления политикой безопасности и настройками

Подсистема управления политикой безопасности и настройками обеспечивает Администратору интерфейс для управления «Bel VPN Gate 3.0.1» . Подсистема поддерживает четыре режима управления:

- централизованно посредством графического интерфейса центра управления CiscoWorks VPN/Security Management Solution
- централизованно удаленно посредством графического интерфейса Cisco Security Manager версии 3.2
- с помощью интерфейса командной строки CSP VPN Command Line Interface, CLI (используется подмножество команд Cisco IOS) и использования специализированных команд
- путем загрузки управляющей информации из внешнего файла и использования специализированных команд.

Кроме того, в состав подсистемы входят:

- **Модуль SSH service** – обеспечивает защищенный в рамках протокола SSH канал для удаленного управления «Bel VPN Gate 3.0.1» . В рамках протокола SSH обеспечивается как управление отдельными командами с использованием любого SSH Client, так и централизованное управление с использованием платформы управления CiscoWorks.

Интерфейс командной строки CSP VPN Command Line Interface позволяет создать совокупность правил, по которым обрабатываются пакеты входящего, исходящего или транзитного трафика. Пакеты могут проходить как простую обработку пакетным фильтром (обработку списков доступа на сетевых интерфейсах), так и

обработку с использованием криптографических алгоритмов – построение защищенных (VPN) туннелей между средствами построения ВЧВС.
Интерфейс командной строки включает в себя следующие специализированные утилиты и команды:

- утилита **cert_mgr** предназначена для работы с сертификатами и CRL. Позволяет регистрировать, просматривать и удалять сертификаты в базе Продукта. Создавать ключевые пары и формировать запросы на сертификат для последующей передачи их в PKI;
- утилита **key_mgr** предназначена для работы с предопределенными ключами (pre-shared keys). Позволяет регистрировать, просматривать и удалять ключи в базе «Bel VPN Gate 3.0.1»;
- утилита **lsp_mgr** предназначена для работы с локальными политиками безопасности. Позволяет загрузить, выгрузить и посмотреть загруженную в «Bel VPN Gate 3.0.1» политику;
- утилита **if_mgr** предназначена для настройки работы «Bel VPN Gate 3.0.1» с сетевыми интерфейсами. Позволяет просматривать список сетевых интерфейсов компьютера, на котором он установлен, включение и исключение из списка интерфейсов, трафик на которых обрабатывается «Bel VPN Gate 3.0.1»;
- утилита **dp_mgr** предназначена для работы с локальной политики по умолчанию, в период времени от установки IP стека до загрузки конфигурации (default driver policy);
- утилита **log_mgr** предназначена для просмотра и настройки параметров протоколирования событий;
- утилита **sa_show** предназначена для просмотра статистики по действующим в данный момент IPsec SA;
- утилита **drv_mgr** предназначена:
  - для просмотра и настройки параметров загрузки процессора;
  - для просмотра и настройки параметров VPN драйвера в части «сброса»/уничтожения «низкоприоритетных» (по параметру ToS) пакетов VPN-драйвером при достижении заданной максимальной загрузки процессора;
- утилита **klogview** предназначена для просмотра сообщений, генерируемых системой протоколирования VPN драйвера;
- команда **ip access-list** предназначена для создания правил пакетной фильтрации - формирования списков доступа и привязывания их к конкретным интерфейсам;
- команда **crypto isakmp policy** предназначена для создания IKE (ISAKMP) политики с различными приоритетами в рамках протокола IKE;
- команда **authentication** предназначена для задания метода аутентификации в рамках протокола IKE (аутентификация на предопределенных ключах, аутентификация на цифровых сертификатах);
- команда **encryption** предназначена для задания алгоритма шифрования в рамках протокола IKE;
- команда **hash** алгоритма расчета контрольных сумм в рамках протокола IKE;
- команда **group** группы Diffie-Hellman в рамках протокола IKE;
- команда **lifetime** предназначена для задания времени жизни IKE SA;
- команда **crypto ipsec transform set** предназначена для задания параметров IPSec наборов преобразований (или одного набора преобразований);
- команда **crypto map** предназначена для конфигурирования криптографических карт.

2.5 Подсистема аудита

Подсистема аудита совместно с операционной системой Red Hat Linux 9 обеспечивает сбор, хранение событий аудита и управление аудитом. Подсистема аудита использует протокол Syslog для отправки сообщений о протоколируемых событиях. Множество событий, подлежащих протоколированию, задается администратором «Bel VPN Gate 3.0.1» в подсистеме управления политикой безопасности и настройками.

В состав подсистемы аудита входят следующие исполняемые модули и библиотеки:

- **Модуль протокола Syslog** реализует соответствующий протокол и используется модулем обработки сообщений для передачи информации в удаленную систему мониторинга работы «Bel VPN Gate 3.0.1» или для регистрации этих событий в протоколе. Параметры этого модуля настраиваются модулем исполнения политики безопасности. Модуль выполнен в виде динамически загружаемой библиотеки, интерфейс к которой получается через модуль-менеджер;

- **Модуль протокола SNMP** реализует протокол версий 1 и 2c для передачи системно значимых событий (traps), данных о текущем состоянии «Bel VPN Gate 3.0.1» и наборов статистических данных о его работе (по запросам). Параметры этого модуля настраиваются модулем исполнения политики безопасности. Модуль выполнен в виде динамически загружаемой библиотеки, интерфейс к которой получается через модуль-менеджер;
- **Модуль обработки сообщений** собирает сообщения о событиях от других модулей, фильтрует эти события в соответствии с политикой безопасности и передает протокольным модулям для доставки информации об этих событиях потребителю. Модуль выполнен в виде динамически загружаемой библиотеки, интерфейс к которой получается через модуль—менеджер;
- **Модуль сбора и обработки статистики** предназначен для сбора статистики, которая накапливается в других модулях и передачи ее, используя протокольный модуль, для удаленного анализа. Модуль выполнен в виде динамически загружаемой библиотеки, интерфейс к которой получается через модуль-менеджер.

2.6 Криптографическая подсистема

Криптографическая подсистема – предоставляет доступ к функциям криптографических модулей.

В состав криптографической подсистемы входят следующие исполняемые модули и библиотеки:

- **Модуль Crypto Plug-in Manager driver** предоставляет доступ к функциям криптографических модулей уровня ядра ОС драйверам и прикладным программам в соответствии с информацией о криптографических модулях, предоставляемой менеджером криптоплагинов уровня приложений;
- **Модуль Crypto Plug-in Drivers** предоставляют криптографические функции на уровне ядра ОС, используя для этого интерфейс соответствующий RFC 2628;
- **Менеджер криптоплагинов** обеспечивает интерфейс к криптографическим функциям, реализованным в различных криптографических модулях, в том числе обеспечивает доставку в криптоплагины уровня ядра ОС сессионных ключей, полученных в результате работы протокола IKE.

2.7 Криптографический модуль (на основе AvCrypt ver. 5.1)

Криптографический модуль (на основе AvCrypt ver. 5.1) обеспечивает формирование и управление криптографическими ключами, а также реализацию следующих криптографических алгоритмов:

- белорусские алгоритмы криптографического преобразования в соответствии с Государственным стандартом Республики Беларусь ГОСТ 28147-89;
- функции хеширования в соответствии с Государственным стандартом Республики Беларусь СТБ 1176.1-99;
- функции хеширования в соответствии с Государственным стандартом Республики Беларусь СТБ 34.101.31-2011;
- процедуру выработки и проверки электронной цифровой подписи в соответствии с Государственным стандартом Республики Беларусь СТБ 1176.2-99;
- процедуру выработки псевдослучайных данных в соответствии с РД РБ 07040.1202-2003 «Банковские технологии. Процедуры выработки псевдослучайных данных с использованием секретного параметра».

Криптографический модуль использует для взаимодействия интерфейс, соответствующий RFC 2628. В его состав входят:

- криптографические библиотеки программного средства электронной цифровой подписи и шифрования AvCrypt ver. 5.1;
- криптоплагин, предоставляющий возможность обращения к функциям криптографических библиотек с использованием интерфейса, соответствующего RFC 2628;
- криптографическая утилита **cryptocont.exe**, предназначенная для работы с ключевыми контейнерами (создание ключевой пары, формирование запроса на сертификат и т.д.).

2.8 Операционная система Red Hat Linux 9

Операционная система Red Hat Linux 9 обеспечивает:

- совместно с подсистемой аудита сбор, хранение событий аудита и управление аудитом;
- при работе с журналом аудита:
    - просмотр событий в журнале с помощью команд more, cat, tail, vi;
    - поиск и сортировка событий с помощью команд sort, grep, перенаправление ввода/вывода в файл, настройки сервиса syslog для направления вывода событий с разными Severity в разные файлы;
    - доступ к журналу разрешен только администратору с правами root и защищен паролем администратора;
    - предотвращение аудирования событий при переполнении журнала осуществляется системным скриптом, который раз в сутки проверяет превышение файлом журнала размера 4 Гб и, в случае такового, настраивает вывод событий в новый файл (параметры скрипта частота проверки, длина файла и т.п. настраиваются);
- идентификацию и аутентификацию Администратора «Bel VPN Gate 3.0.1» до осуществления доступа непосредственно к шлюзу безопасности, с целью администрирования. Аутентификация Администратора основана на пароле, который вводится с клавиатуры не отображаясь на экране монитора в явном виде, идентификация основана на идентификаторе, который вводится с клавиатуры;
- средства защиты комплекса средств безопасности Продукта связанные с тестированием среды функционирования «Bel VPN Gate 3.0.1», его восстановлением после сбоев и прерываний обслуживания, тестированием на предмет контроля целостности и корректности функционирования.