Закрытое акционерное общество «НТЦ КОНТАКТ»

УТВЕРЖДАЮ

Директор

ЗАО «НТЦ КОНТАКТ»

_____А.А.Тепляков

25 октября 2021 г.

КОМПЛЕКС ПРОГРАММНО-АППАРАТНЫЙ КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ «БАС»

Руководство по эксплуатации

СЮИК.465634.001 РЭ

Содержание

Настоящее руководство по эксплуатации распространяется на комплекс программно-аппаратный криптографической защиты информации «БАС» СЮИК.465634.001 (далее – ПАК «БАС»), предназначенный для защиты информации, циркулирующей в каналах передачи данных.

ПАК «БАС» применяется в системах обработки информации ограниченного распространения и обеспечивает защиту как клиентской, так и серверной части системы.

Данный документ является эксплуатационным документом (ЭД), содержащим сведения по эксплуатации, техническому обслуживанию и ремонту.

Руководство по эксплуатации описывает следующее:

– назначение и технические характеристики;

– принцип работы;

– порядок хранения и транспортирования;

– порядок монтажа и ввода в эксплуатацию.

1 Описание и работа

1.1 Назначение изделия

1.1.1 ПАК «БАС» предназначен для защиты каналов обмена информацией между абонентами, взаимодействующими по цифровому протоколу IP через сети передачи данных.

1.1.2 ПАК «БАС» обеспечивают криптографическую защиту передаваемых данных посредством полной инкапсуляции IP-пакетов путем их шифрования с использованием криптографических алгоритмов на основе протоколов IPsec.

1.1.3 Область применения ПАК «БАС» – системы обработки информации ограниченного распространения.

1.2 Технические характеристики

1.2.1 ПАК «БАС» производится в следующих конфигурациях:

а) устройства защиты клиента;

б) сервера защиты.

1.2.2 ПАК «БАС» конструктивно представляет собой вычислитель, работающий под управлением ОС Linux, и встроенное программное обеспечение. При этом устройство защиты клиента и сервер защиты имеют одинаковое программное обеспечение, что обеспечивает выполнение одинаковых функциональных возможностей, но различное аппаратное исполнение, вследствие чего устройство защиты клиента и сервер защиты имеют различную вычислительную мощность.

1.2.3 ПАК «БАС» реализует следующие функциональные возможности:

1 Защиту информации путем ее шифрования с использованием криптографических алгоритмов на основе протоколов IPsec.

2 Шифрование передаваемых данных в соответствие с СТБ 34.101.31-2020.

3 Контроль целостности пакетов данных (вычисление имитовставки) в соответствие с СТБ 34.101.31-2020, СТБ 34.101.47-2017.

4 Согласование ключей шифрования производится по СТБ 34.101.66-2014.

5 Генерацию ключей и синхропосылок при помощи СТБ 34.101.47-2017 с использованием генератора случайных числовых последовательностей (ГСЧП) на основе физического источника шума.

6 Выработку открытых ключей при помощи СТБ 34.101.45-2013.

7 Формирование запроса на получение сертификата открытого ключа в соответствии с СТБ 34.101.17-2012.

8 Обработку сертификатов открытых ключей и списки отозванных сертификатов в соответствии с СТБ 34.101.19-2012 (Проверена работоспособность с сертификатами УЦ ГосСУОК, БУТБ, Министерства финансов, АСБ «Беларусбанк»).

9 Защиту секретных (личных) ключей от несанкционированного раскрытия, модификации и подмены, открытых – от модификации и подмены.

10 Проверку работоспособности устройства при включении и по запросу администратора.

11 При тестировании ПАК «БАС» осуществляет:

– тесты криптографических алгоритмов;

– контроль целостности программного обеспечения;

– контроль работоспособности ГСЧП и качества вырабатываемых случайных числовых последовательностей.

12 Возможность работы через NAT при помощи протокола NAT Traversal (NAT-T).

13 Ведение журнала аудита и предоставление доступа к нему по протоколу SYSLOG, в который заносится следующая информация:

– дата и время;

– вызываемая функция;

– результат (успешно/неуспешно).

14 Защиту от несанкционированного доступа (НСД) при вскрытии корпуса, причем защита обеспечивается даже при отсутствии внешнего питания.

ПАК «БАС» при помощи «Комплекса программно-аппаратного защиты информации от несанкционированного доступа «Барьер – USB» СЮИК.467458.004 (далее – ПАК «Барьер - USB»), входящего в его состав ведет непрерывный контроль вскрытия корпуса. При обнаружении вскрытия корпуса уничтожается личный ключ, хранящийся в защищенном хранилище ПАК «Барьер - USB», и фиксируется время вскрытия корпуса во внутреннем журнале ПАК «Барьер-USB» (журнал критических событий). Устройство при этом переходит в режим блокировки, из которого может быть выведено только администратором. Доступ к журналу разрешен только администратору после предъявления пароля для доступа к защищенному хранилищу.

Механизм контроля вскрытия корпуса и аудита критических событий является не отключаемым и выполняется даже при отсутствии внешнего питания устройства.

15 Автоматическую смену ключей шифрования при достижении заданного объема переданных данных либо «времени жизни» ключа.

16 Наличие световой индикации работоспособности.

17 Время готовности к работе после включения питания не превышает 60 с.

18 ПАК «БАС» не ограничивает функциональные возможности защищаемых серверных и абонентских (клиентских) устройств.

19 ПАК «БАС» рассчитан на непрерывную круглосуточную необслуживаемую работу.

1.2.4 Устройство защиты клиента реализует следующие функциональные возможности:

1 Защиту информации, передаваемой со скоростью не менее 7 Мбит/с.

2 Управление через отдельный от портов обмена защищаемыми данными USB-порт.

3 Подключение к 10/100 Мбит/с Ethernet IEEE 802.3 порту IP-сети.

4 Подключение к 10/100 Мбит/с Ethernet IEEE 802.3 порту абонентского (клиентского) устройства (ПЭВМ, IP-телефона и др.).

5 Электропитание устройства защиты клиента осуществляется от одного из следующих источников:

– сеть постоянного тока стандарта PoE напряжением 48 В (плюс/минус 10%);

– USB 3.0-порт защищаемого оборудования;

– сеть электропитания 220 В, с использованием micro-USB AC-DC адаптера.

6 Потребляемая мощность не превышает 5 Вт.

1.2.5 Сервер защиты реализует следующие функциональные возможности:

1 Защиту информации, передаваемой со скоростью определенной в договоре на поставку, но не менее 70 Мбит/с (При отсутствии в договоре на поставку особых указаний – Скорость шифрования на сервере защиты не менее 1 Гбит/с).

2 Подключение к 10/100/1000 Мбит/с Ethernet IEEE 802.3 порту IP-сети.

3 Подключение к 10/100/1000 Мбит/с Ethernet IEEE 802.3 порту серверного устройства (ПЭВМ, SIP-сервера, сервера приложение и др.).

4 Мощность, потребляемая сервером защиты, зависит от комплектации необходимой для обеспечения скорости шифрования, определенной договором на поставку (Мощность сервера защиты, обеспечивающего скорость шифрования не менее 70 Мбит/с не превышает 50 Вт. Мощность сервера защиты, обеспечивающего скорость шифрования не менее 1000 Мбит/с не превышает 400 Вт.

1.2.6 ПАК «БАС» реализует следующие дополнительные функциональные возможности:

1 Удаленное управление по протоколу SSH, причем ПАК «БАС» может быть предварительно настроен таким образом, что управляющие SSH пакеты будут защищены при помощи протоколов IPsec.

2 Передача сведений о своем состоянии по протоколу SNMP для сбора статистики о работе ПАК «БАС».

3 Защиту данных второго уровня сетевой модели (L2), путем «захвата» пакетов второго уровня, инкапсулирования их заголовками UDP и передачи по защищенному «псевдопроводу» при помощи протокола L2TPv3 pseudowire.

4 Объединение нескольких ПАК «БАС» в кластер для обеспечения отказоустойчивости с использованием протоколов CARP или VRRP.

5 Поддержка протоколов динамической маршрутизации (RIP, OSPF, BGP) при помощи пакета Quagga.

6 Пакетная фильтрация данных при помощи встроенного межсетевого экрана.

1.3 Состав изделия

1.3.1 Комплект поставки ПАК «БАС» определяется договором. Возможный комплект поставки приведен в таблице 1.

Таблица 1 – Комплект поставки ПАК «БАС»

Обозначение изделия	**Наименование изделия**	**Коли-чество (шт.)**	**Заводской номер**	**Приме-чание**
СЮИК.465634.002	Комплекс программно-аппаратный криптографической защиты информации «БАС». Устройство защиты клиента.			Приме-чание 1, приме-чание 2
СЮИК.465634.003	Комплекс программно-аппаратный криптографической защиты информации «БАС». Сервер защиты.			Приме-чание 2
СЮИК.465634.001 ВЭ	Комплект эксплуатационной документации согласно ведомости			
Примечания 1 По согласованию с заказчиком в комплект поставки устройства защиты клиента может быть включен источник питания стандарта PoE (инжектор – PoE). 2 Количество поставляемых устройств определяется договором на поставку.				

1.4 Устройство и работа

1.4.1 Устройство

1.4.1.1 ПАК «БАС» конструктивно представляет собой вычислитель, работающий под управлением ОС Linux, и встроенное программное обеспечение. При этом устройство защиты клиента и сервер защиты имеют одинаковое программное обеспечение, что обеспечивает выполнение одинаковых функциональных возможностей, но различное аппаратное исполнение, вследствие чего устройство защиты клиента и сервер защиты имеют различную вычислительную мощность.

1.4.1.2 Устройство защиты клиента выполнено в виде уложенного в корпус исполнительного блока, который содержит аппаратную часть устройства, включая ПАК «Барьер - USB».

1.4.1.3 Сервер защиты представляет собой ПЭВМ, предназначенную для установки в 19-дюймовую стойку (если другое не оговорено договором на поставку), оснащенную ПАК «Барьер – USB».

Выбор варианта исполнения сервера защиты определяется в зависимости от требований заказчика к производительности ПАК «БАС» и выбору места его последующей установки.

1.4.2 Принцип работы

1.4.2.1 Принцип работы ПАК «БАС» основан на организации шифрованного канала связи между защищаемыми устройствами.

1.4.2.2 В процессе работы ПАК «БАС» выполняет следующие процессы:

– выпуск и экспорт запроса на получение сертификата открытого ключа в соответствии с СТБ 34.101.17-2012;

– импорт сертификатов открытых ключей и списков отозванных сертификатов в соответствии с СТБ 34.101.19-2012;

– аутентификация и формирование общего ключа, используемого в качестве материала ключа шифрования, в соответствии с СТБ 34.101.66-2014;

– шифрование и контроль целостности данных в соответствии с СТБ 34.101.31-2020.

– пересылка шифрованных сообщений;

– согласование окончания сеанса связи и уничтожение сеансовых объектов;

– контроль вскрытия корпуса.

1.4.2.3 Подключение ПАК «БАС» производится в разрыв защищаемой линии передачи данных до оконечного оборудования.

1.4.2.4 ПАК «БАС» имеет два Ethernet-порта (если иное не оговорено в договоре на поставку): порт «Абонент» и порт «Сеть». К порту «Абонент» подключается оконечное устройство (IP-телефон, ПЭВМ, SIP-сервер), к порту «Сеть» подключается сеть передачи защищаемых данных.

1.4.2.5 ПАК «БАС» обеспечивает шифрование передаваемой информации путем создания защищенных IPsec-туннелей между ними.

1.4.2.6 Электропитание устройства защиты клиента осуществляется от одного из следующих источников:

– сеть постоянного тока стандарта PoE напряжением 48 В (плюс/минус 10%);

– USB 3.0-порт защищаемого оборудования;

– сеть электропитания 220 В, с использованием micro-USB AC-DC адаптера.

1.4.2.7 Электропитание сервера защиты осуществляется от сети электропитания 220 В.

1.4.2.8 ПАК «БАС» сохраняет работоспособность и при отсутствии внешнего питания, выполняя контроль вскрытия корпуса, при помощи входящего в его состав ПАК «Барьер - USB».

1.4.2.9 При обнаружении вскрытия корпуса происходит уничтожение личного ключа, а если вскрытие корпуса произошло при включенном внешнем питании, производится прерывание сеанса связи и перезагрузка устройства.

1.4.2.10 При включении и по запросу администратора ПАК «БАС» выполняет самотестирование.

1.4.2.11 ПАК «БАС» имеет световую индикацию неисправностей. При обнаружении неисправности ПАК «БАС» формирует серии вспышек светодиода «Ошибка». При этом количество вспышек в серии указывает на причину неисправности:

– одна вспышка – нарушение целостности личного ключа (был вскрыт корпус, уничтожен личный ключ);

– две вспышки – ошибка аппаратной составляющей (неработоспособность генератора случайных чисел или плохое качество случайной числовой последовательности, нарушение целостности прошивки ПАК «Барьер - USB»;

– четыре вспышки – ошибка выполнения криптографических алгоритмов или нарушение целостности программного обеспечения.

1.4.2.12 Количество вспышек в серии, равное сумме некоторых из перечисленных вариантов, указывает на наличие нескольких ошибочных ситуаций.

1.4.3 Роли пользователей

1.4.3.1 ПАК «БАС» предполагает наличие двух ролей пользователей с доступными для каждой из ролей функциями и с наличием определенных прав:

– роль администратора;

– роль пользователя.

1.4.3.2 Роль администратора предназначена для ввода ПАК «БАС» в эксплуатацию, настройки устройства, восстановления работоспособности в случае

возникновения ошибок, а также для вывода ПАК «БАС» из эксплуатации. Основными функциями, выполняемыми администратором, являются:

– первичная настройка устройства для работы в сети передачи данных;

– генерация личных ключей и ввод в устройство сертификатов открытых ключей;

– управление личной ключевой информацией пользователей (запись, удаление, администрирование);

– регистрация устройств защиты клиента на сервере защиты;

– периодический контроль работоспособности устройства и изменение настроек устройства, в случае необходимости;

– администрирование журнала;

– восстановление работоспособности устройства в случае возникновения ошибок.

1.4.3.3 Роль пользователя выполняют устройства, находящиеся в защищаемой сети. ПАК «БАС» предназначен для криптографической защиты информации, передаваемой его пользователями.

1.5 Средства измерения, инструмент и принадлежности

1.5.1 Для подключения ПАК «БАС» к сети передачи защищаемых данных и абонентским устройствам используются сетевые кабели с разъемами, соответствующими стандарту 8P8C.

1.5.2 Для подключения сервера защиты ПАК «БАС» к сети электропитания 220 В используется шнур – соединитель, соответствующий ГОСТ 28244-96.

1.5.3 Настройка и управление устройством защиты клиенты осуществляется через ПЭВМ, подключенную к нему через micro-USB кабель.

1.5.4 Для осуществления настройки и технического обслуживания устройства защиты клиента ПАК «БАС» необходим персональный компьютер, соответствующий следующим требованиям:

– наличие свободного USB порта;

– наличие установленной ОС;

– наличие установленного драйвер для CP210x USB – UART моста (доступен на сайте производителя: https://www.silabs.com/products/development-tools/software/usb-to-uart-bridge-vcp-drivers);

– наличие терминального ПО (putty, Microsoft HyperTerminal);

– наличие свободно распространяемой утилиты tftp32.exe.

1.6 Маркировка и пломбирование

1.6.1 Маркировка ПАК «БАС» содержит следующую информацию:

– номинальное напряжение в вольтах;

– номинальную частоту в герцах;

– номинальный ток в миллиамперах или амперах;

– наименование изготовителя, торговый или фирменный знак;

– обозначение модели или типа, присваиваемого изготовителем.

1.6.2 На транспортной таре нанесена транспортная маркировка в соответствии с ГОСТ 14192-96 с указанием манипуляционных знаков «Верх», «Хрупкое. Осторожно», «Беречь от влаги».

1.7 Упаковка

1.7.1 ПАК «БАС» и эксплуатационная документация, входящие в комплект поставки, упакованы в пакеты из полиэтиленовой пленки толщиной не менее 0,1 мм по ГОСТ 10354-82 с последующей заваркой шва.

1.7.2 Временная противокоррозионная защита ПАК «БАС» проведена по варианту В3-10 – защита с помощью статического осушения воздуха по ГОСТ 9.014-78. Силикагель технический по ГОСТ 3956-76 в пакете из

хлопчатобумажной ткани по ГОСТ 29298-92 помещен вместе с изделием в полиэтиленовый пакет до его запайки.

1.7.3 В подборную транспортную тару вложен упаковочный лист. Упаковочный лист составлен по форме предприятия-изготовителя, содержащей следующие сведения:

а) наименование и обозначение изделия;

б) количество упакованных изделий;

в) дату упаковки;

г) подпись или штамп ответственного за упаковку;

д) штамп ОТК.

2 Использование по назначению

ВНИМАНИЕ: ПРИ РАБОТЕ С УСТРОЙСТВОМ СЛЕДУЕТ СОБЛЮДАТЬ МЕРЫ ЭЛЕКТРОБЕЗОПАСНОСТИ.

2.1 Эксплуатационные ограничения

2.1.1 Климатическое исполнение ПАК «БАС» УХЛ 4 по ГОСТ 15150-69.

2.1.2 Условия эксплуатации ПАК «БАС»:

а) температура окружающей среды от плюс 5 до плюс 40 ºС;

б) относительная влажность окружающего воздуха не более 95 % при температуре окружающего воздуха плюс 25 ºС;

в) атмосферное давление от 84 до 107 кПа (от 630 до 800 мм рт. ст.).

2.2 Подготовка изделия к использованию

2.2.1 Перед началом работы необходимо внимательно ознакомиться с технической документацией на ПАК «БАС».

2.2.2 ПАК «БАС» обеспечивает при эксплуатации безопасность обслуживающего персонала, электрическую и пожарную безопасность в соответствии с требованиями ГОСТ IEC 60950-1-2014, предъявляемыми к оборудованию класса I.

2.2.3 Подключать и отключать любые внешние устройства допускается только в выключенном состоянии.

2.2.4 Перед началом эксплуатации ПАК «БАС» необходимо убедиться в отсутствии механических повреждений.

2.2.5 Ввод в эксплуатацию ПАК «БАС» должен осуществляться в соответствии с технической документацией на поставляемое изделие.

2.2.6 Для ввода в эксплуатацию ПАК «БАС» необходимо:

– подключить его к абонентскому (клиентскому) устройству и сети передачи защищаемых данных;

– обеспечить электропитание;

– произвести настройку соединений.

2.2.7 Для подключения устройства защиты клиента необходимо выполнить следующие действия:

– извлечь устройство защиты клиента из упаковки;

– подключить к порту «Сеть» устройства защиты клиента сеть передачи защищаемых данных при помощи сетевого кабеля, соответствующего стандарту 8P8C (Ethernet-кабеля);

– обеспечить электропитание устройства защиты клиента от одного из следующих источников:

а) сеть постоянного тока стандарта PoE напряжением 48 В (плюс/минус 10%);

б) USB 3.0-порт защищаемого оборудования;

в) сеть электропитания 220 В, с использованием micro-USB AC-DC адаптера;

– подключить к порту «Абонент» устройства защиты клиента абонентское устройство (ПЭВМ, IP-телефон и т.п.) при помощи Ethernet-кабеля;

– произвести запись о подключении устройства в паспорте.

2.2.8 Схема подключения устройства защиты клиента с электропитанием от сети передачи защищаемых данных представлена на рисунке 1.

2.2.9 Схема подключения устройства защиты клиента с электропитанием от дополнительного источника питания стандарта IEEE 802.3af представлена на рисунке 2.

2.2.10 Схема подключения устройства защиты клиента с электропитанием от USB 3.0-порт защищаемого оборудования представлена на рисунке 3.

2.2.11 Схема подключения устройства защиты клиента с электропитанием от сети 220 В, с использованием micro-USB AC-DC адаптера представлена на рисунке 4.

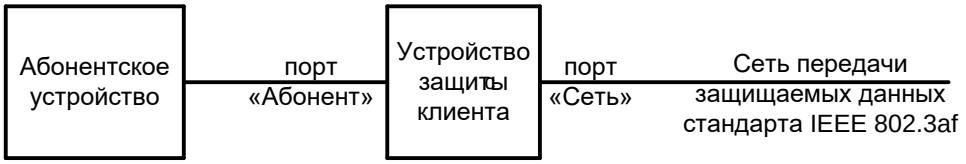

Рисунок 1 – Схема подключения устройства защиты клиента с электропитанием от сети передачи защищаемых данных

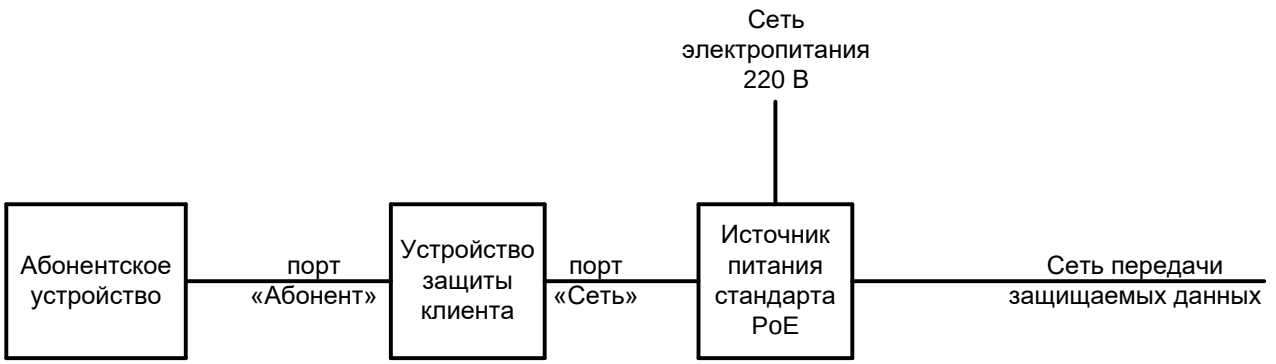

Рисунок 2 – Схема подключения устройства защиты клиента с электропитанием от дополнительного источника питания стандарта IEEE 802.3af

ВНИМАНИЕ: СЕТЬ ПЕРЕДАЧИ ЗАЩИЩАЕМЫХ ДАННЫХ СТАНДАРТА IEEE 802.3AF ДОЛЖНА ПОДКЛЮЧАТЬСЯ К ПОРТУ «СЕТЬ», ПОДКЛЮЧЕНИЕ СЕТИ ПЕРЕДАЧИ ДАННЫХ СТАНДАРТА IEEE 802.3AF К ПОРТУ «АБОНЕНТ» НЕДОПУСТИМО.

2.2.12 При электропитании устройства защиты клиента от сети IEEE 802.3af (стандарт PoE) оно может передавать электропитание стандарта IEEE 802.3af, полученное с порта «Сеть», на порт «Абонент» для питания абонентского устройства. Для этого необходимо установить параметр **power_translate=yes** в файле **/etc/power_translate.conf**.

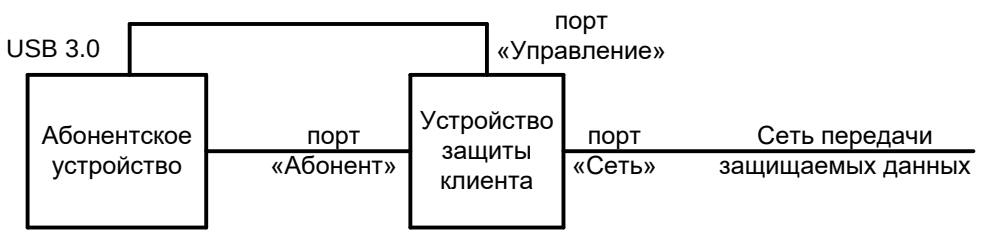

Рисунок 2 – Схема подключения устройства защиты клиента с электропитанием от USB 3.0-порт защищаемого оборудования

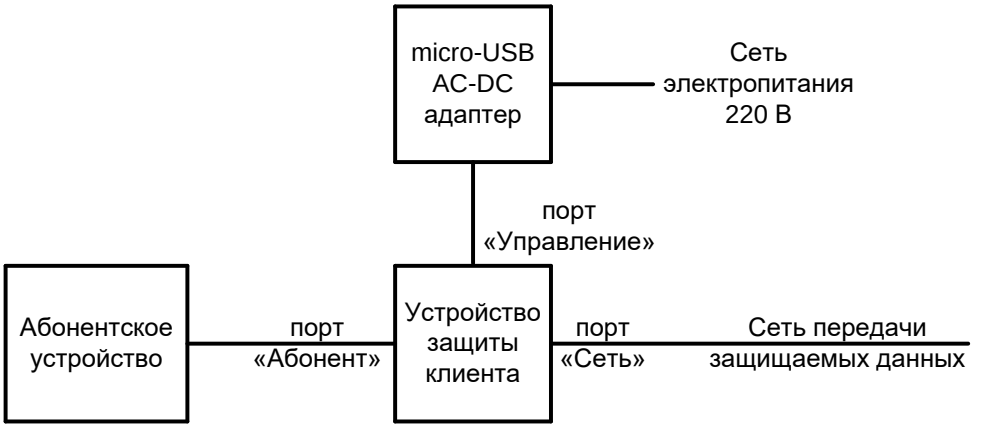

Рисунок 4 – Схема подключения устройства защиты клиента с электропитанием от сети 220 В, с использованием micro-USB AC-DC адаптера

2.2.13 Для подключения сервера защиты необходимо выполнить следующие действия:

– извлечь сервер защиты из упаковки;

– подключить к порту «Сеть» сервера защиты сеть передачи защищаемых данных при помощи Ethernet-кабеля;

– подключить к порту «Абонент» сервера защиты серверное устройство (ПЭВМ, SIP-сервер, защищаемая подсеть) при помощи Ethernet-кабеля;

– подключить сервер защиты к сети электропитания 220 В при помощи кабеля питания, соответствующего ГОСТ 28244-96;

– для управления сервером защиты подключить к нему монитор, клавиатуру и мышь;

– произвести запись о подключении устройства в паспорте.

2.2.14 Схема подключения сервера защиты представлена на рисунке 3:

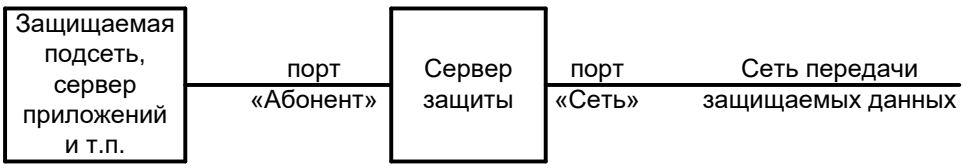

Рисунок 3 – Схема подключения сервера защиты

2.3 Использование изделия

2.3.1 Этапы использования ПАК «БАС»

2.3.1.1 Использование ПАК «БАС» включает в себя следующие основные этапы:

– ввод ПАК «БАС» в эксплуатацию – настройка устройства администратором;

– эксплуатация ПАК «БАС» – использование устройства для защиты информации, передаваемой по каналам связи;

– вывод ПАК «БАС» из эксплуатации.

2.3.1.2 Ввод ПАК «БАС» в эксплуатацию осуществляется администратором. На этапе ввода в эксплуатацию выполняется настройка сервера защиты (устройства защиты клиента), которая заключается в редактировании необходимых конфигурационных файлов, а также генерации личных ключей и загрузке сертификатов открытых ключей в память устройства.

2.3.1.3 Эксплуатацию ПАК «БАС» осуществляют пользователи. При этом администратор проводит контроль работоспособности системы, при необходимости осуществляет смену используемых криптографических алгоритмов.

2.3.1.4 Вывод ПАК «БАС» из эксплуатации осуществляется администратором. На этапе вывода из эксплуатации происходит полное уничтожение всей ключевой информации, хранящейся в памяти ПАК «БАС», а также отключение устройства от сети передачи защищаемых данных.

2.3.2 Ввод ПАК «БАС» в эксплуатацию – настройка

2.3.2.1 Последовательность настройки

2.3.2.1.1 Ввод в эксплуатацию ПАК «БАС» состоит из следующих этапов:

– смена пароля администратора;

– настройка сетевых интерфейсов;

– настройка даты и времени;

– управление ключевой информацией (генерация ключевой пары, экспорт открытого ключа из устройства в виде запроса на получение СОК и импорт открытого ключа в устройство в виде СОК);

– настройка программного обеспечения.

ВНИМАНИЕ: ПОСЛЕ ВЫПОЛНЕНИЯ ВСЕХ ВЫШЕПЕРЕЧИСЛЕННЫХ НАСТРОЕК НЕОБХОДИМО ПЕРЕЗАГРУЗИТЬ ПАК «БАС».

2.3.2.1.2 Для осуществления настройки сервера защиты необходимо предварительно выполнить следующие операции:

– подключить к серверу защиты монитор и клавиатуру;

– включить питание сервера защиты, нажав кнопку на корпусе устройства;

– убедиться в появлении на экране приглашения на ввод логина и пароля;

– осуществить вход в операционную систему сервера защиты, введя логин администратора **server** и транспортный пароль **11111111**;

– получить доступ к командной строке операционной системы сервера защиты.

2.3.2.1.3 Для осуществления настройки устройства защиты клиента необходимо предварительно выполнить следующие операции:

– подключить к порту «Управление» устройства защиты клиента ПЭВМ, соответствующей требованиям, указанным в п. 1.5.4, при помощи micro-USB-кабеля, входящего в комплект поставки.

– на ПЭВМ запустить терминальную программу, установив следующие параметры COM порта:

Скорость: 115200 бит/с;

Биты данных: 8

Четность: Нет

Стоповые биты: 1

Управление потоком: Нет

– убедиться в появлении в лога загрузки операционной системы;

– осуществить вход в операционную систему сервера защиты, введя логин администратора **client** и транспортный пароль **11111111**.

2.3.2.1.4 Настройка ПАК «БАС» также может выполняться при помощи внешнего (удаленного) ПЭВМ по протоколу SSH.

2.3.2.2 Смена пароля администратора ПАК «БАС»

2.3.2.2.1 В случае, если настройка ПАК «БАС» осуществляется в первый раз, необходимо сменить пароль администратора.

ВНИМАНИЕ: ПРОЦЕДУРА СМЕНЫ ПАРОЛЯ АДМИНИСТРАТОРА ЯВЛЯЕТСЯ ОБЯЗАТЕЛЬНОЙ, И В СЛУЧАЕ НЕВЫПОЛНЕНИЯ ТРЕБОВАНИЙ ПО СМЕНЕ ПАРОЛЯ ПРОИЗВОДИТЕЛЬ НЕ ГАРАНТИРУЕТ ВЫПОЛНЕНИЕ УСТРОЙСТВОМ СВОИХ ФУНКЦИЙ.

2.3.2.2.2 Для смены пароля администратора необходимо:

– осуществить вход в операционную систему ПАК «БАС» введя логин и транспортный пароль;

– ввести команду **passwd** в командную строку ПАК «БАС»;

– ввести текущий пароль администратора (**11111111**);

– ввести новый пароль администратора, затем подтвердить правильность набора, повторно введя новый пароль;

– ввести команду **sudo reboot** для перезагрузки ПАК «БАС»;

– осуществить вход в операционную систему ПАК «БАС» введя логин и новый пароль администратора.

2.3.2.3 Настройка сетевых интерфейсов ПАК «БАС»

2.3.2.3.1 Настройка сетевых интерфейсов ПАК «БАС» производится путем заполнения файла **/etc/network/interfaces** при помощи текстового редактора **nano** или **vi**.

2.3.2.3.2 Ниже приведен пример файла **/etc/network/interfaces**.

```
# interfaces(5) file used by ifup(8) and ifdown(8)
auto lo
iface lo inet loopback

iface eth0 inet static
address 10.0.0.1
netmask 255.255.255.0
auto eth0

iface eth1 inet static
address 100.0.0.1
netmask 255.255.255.0
gateway 100.0.0.10
auto eth1
```

2.3.2.4 Настройка даты и времени ПАК «БАС»

2.3.2.4.1 Для настройки даты и времени администратору необходимо выполнить следующие действия:

– осуществить подключение ПАК «БАС» и вход в операционную систему;

– установить (при необходимости) часовой пояс, в котором находится ПАК «БАС» (по умолчанию установлен часовой пояс, соответствующий Минску (Республике Беларусь) (GMT+3)), подав команду:

sudo ln -sf /usr/share/zoneinfo/<файл с часовым поясом> /etc/localtime

– подать команду формата **date MMDDhhmmCCYY.ss** в командную строку ПАК «БАС»,

где:

MM – текущий месяц;

DD – день месяца;

hh – часы;

mm – минуты;

CCYY – 4 цифры года;

ss – секунды;

– подать команду **sudo hwclock -w** в командную строку ПАК «БАС»;

– подать команду **sudo reboot** в командную строку для перезагрузки ПАК «БАС».

2.3.2.4.2 Также ПАК «БАС» поддерживает синхронизацию времени при помощи протокола SNTP (англ. Simple Network Time Protocol) – протокол синхронизации времени по компьютерной сети.

Настройка работы NTP, выполняется в файле **/etc/ntp.conf**.

Для настройки NTP-клиента необходимо указать адрес эталонного NTP-сервера, от которого ПАК «БАС» будет получать точное время, в следующем формате:

server <IP-адрес или доменное имя эталонного NTP-сервера>

например:

server www.belgim.by

Для того чтобы использовать ПАК «БАС» в качестве эталонного NTP-сервера, например, для других ПАК «БАС», необходимо настроить ограничения на доступ и управление NTP-сервером:

restrick <IP-адрес> mask <маска подсети> nomodify notrap

например:

restrick 192.168.0.0 mask 255.255.255.0 nomodify notrap

IP-адрес – адрес локальной подсети, которую обслуживает NTP-сервер;

маска подсети – маска локальной подсети, которую обслуживает NTP-сервер.

Для того, что разрешить NTP-серверу обмен данные серверу с самим собой, необходимо добавить:

restrict 127.0.0.1

restrict ::1

2.3.2.4.3 Необходимо отметить, что ПАК «БАС» имеет аппаратные часы реального времени, которые реализованы в ПАК «Барьер - USB». Эти часы синхронизируются с системными в момент инсталляции (генерации личного ключа).

Администратор, при необходимости, может настроить контроль рассинхронизации времени системных и аппаратных часов. Для этого необходимо отредактировать следующие параметры файла **/etc/support/UsbBarController.conf**:

– **MaxTimeDiff**. Значением параметра должно быть целое положительное число, задающее максимальный интервал расхождения часов реального времени ПАК «Барьер - USB» с текущим системным временем в секундах;

– **SyncBlock**. Определяет необходимость блокировки ПАК «БАС» при превышении значения расхождения времени указанного в **MaxTimeDiff** и может принимать значения **yes** и **no** (по умолчанию выбран вариант **no**, при превышении значения расхождения времени указанного в **MaxTimeDiff** будет проведена синхронизация времени).

2.3.2.5 Управление ключевой информацией ПАК «БАС»

2.3.2.5.1 Для создания ключевой информации администратору необходимо:

– сгенерировать ключевую пару;

– экспортировать открытый ключ из ПАК «БАС»;

– выпустить сертификат открытого ключа;

– загрузить корневой сертификат и сертификат открытого ключа в ПАК «БАС».

2.3.2.5.2 Для генерации личного ключа администратору необходимо выполнить следующие действия:

– выполнить процедуру формирования запроса на получение сертификата открытого ключа, подав команду **sudo RequestBuilder** в командную строку, после чего программа предложить отредактировать файл с персональными данными;

– отредактировать файл с персональными данными, указав данные устройства (пример файла с персональными данными приведен в Приложении Б);

– задать и подтвердить пароль для доступа к защищенному хранилищу, после чего ПАК «БАС» генерирует личный ключ и сохраняет его в защищенном хранилище ПАК «Барьер - USB», на его основе вырабатывает открытый ключ, который, вместе с персональными данными, помещает в запрос на получение СОК и сохраняет его в файле имя и путь к которому выводится в командную строку;

– задать и подтвердить пароль к частичным секретам, при необходимости создания резервной копии личного ключа для восстановления устройства после сбоев, имя и путь к созданному блобу личного ключа и частичным секретам выводится в командную строку;

Примечание: при необходимости создания резервной копии личного ключа для восстановления устройства после сбоев, ПАК «БАС» защитит его при помощи сгенерированного ключа защиты, который разделит на секреты, а частичные секреты защитит на ключе, полученном из пароля;

2.3.2.5.3 Экспорт запроса на получение СОК из ПАК «БАС» может быть выполнен любым удобным способом, поддерживаемым ОС.

Для устройства защиты клиента, рекомендуется воспользоваться утилитой tftpd32.exe, запущенной на ПЭВМ, подключенной к порту «Абонент» устройства защиты клиента. Для этого необходимо:

– в выпадающем меню Server interfaces программы tftpd32 указать IP-адрес ПЭВМ;

– нажать кнопку Browse, выбрать директорию, предназначенную для обмена данными с ПАК «БАС», нажать ОК;

– подать в командную строку ПАК «БАС» команду

cd <путь к директории, содержащей запрос на получение СОК>

для перехода в указанную директорию;

– подать в командную строку ПАК «БАС» команду

tftp -p -l <Имя_файла> <IP-адрес>,

где:

<Имя_файла> – имя запроса на получение СОК;

<IP-адрес> – IP-адрес ПЭВМ;

для передачи файла, содержащего открытый ключ, на ПЭВМ;

– убедиться в успешной передаче файла, запроса в директорию, предназначенную для обмена данными с ПАК «БАС».

Для сервера защиты, рекомендуется воспользоваться съемным USB-носителем:

– подключить USB-носителем к ПАК «БАС»;

– определить имя, присвоенное съемному USB-носителю операционной системой ПАК «БАС» при помощи команды

sudo fdisk -l

– примонтировать файловой системы съемного USB-носителя (с именем **dev/sdb1)** при помощи команды

sudo mount /dev/sdb1 /mnt

– выполнить копирование файла запроса на выпуск сертификата на съемный USB-носитель при помощи команды

cp <Имя_файла> /mnt/

<Имя_файла> – имя запроса на получение СОК и путь к нему;

– убедиться в успешной передаче файла, запроса на съемный USB-носитель при помощи команды

ls /mnt/

– размонтировать файловую систему съемного USB-носителя при помощи команды

sudo umount /mnt

2.3.2.5.4 Передать запрос на выпуск СОК администратору Удостоверяющего или Регистрационного центра для выпуска СОК по запросу.

2.3.2.5.5 Сохранить СОК и корневой СОК в директории, предназначенной для обмена данными с ПАК «БАС» либо на съемном USB-носителе.

2.3.2.5.6 Для загрузки СОК в устройство защиты клиента ПАК «БАС» необходимо:

– подать в командную строку устройства защиты клиента необходимокоманду

cd /etc/ipsec.d/certs

для перехода в директорию, предназначенную для хранения сертификатов открытого ключа;

– подать в командную строку ПАК «БАС» команду

tftp -g -r <Имя_файла> <IP-адрес>,

где:

<Имя_файла> – полное имя файла сертификата открытого ключа;

<IP-адрес> – IP-адрес ПЭВМ;

для записи сертификата открытого ключа в ПАК «БАС»;

– убедиться в успешной передаче сертификата в файловую систему ПАК «БАС» при помощи команды **ls**.

2.3.2.5.7 Для загрузки корневого СОК и цепочки промежуточных сертификатов в ПАК «БАС» необходимо:

– подать в командную строку устройства защиты клиента команду

cd /etc/ipsec.d/cacerts

для перехода в директорию, предназначенную для хранения корневых сертификатов открытого ключа;

– подать в командную строку ПАК «БАС» команду

tftp -g -r <Имя_файла> <IP-адрес>,

где:

<Имя_файла> – полное имя файла корневого сертификата открытого ключа;

<IP-адрес> – IP-адрес ПЭВМ;

для записи корневого сертификата в ПАК «БАС»;

– для каждого промежуточного сертификата цепочки повторить предыдущую команду, указав в качестве **<Имени_файла>** имя промежуточного сертификата для его записи в ПАК «БАС»;

– убедиться в успешной передаче корневых сертификатов в файловую систему ПАК «БАС» при помощи команды **ls**.

2.3.2.5.8 Для загрузки списка отозванных сертификатов (при наличии) в ПАК «БАС» необходимо:

– подать в командную строку устройства защиты клиента команду

cd /etc/ipsec.d/crls

для перехода в директорию, предназначенную для хранения списков отозванных сертификатов;

– подать в командную строку ПАК «БАС» команду

tftp -g -r <Имя_файла> <IP-адрес>,

где:

<Имя_файла> – полное имя файла списка отозванных сертификатов;

<IP-адрес> – IP-адрес ПЭВМ;

для записи списка отозванных сертификатов в ПАК «БАС»;

– убедиться в успешной передаче списка отозванных сертификатов в файловую систему ПАК «БАС» при помощи команды **ls**.

2.3.2.5.9 Для загрузки СОК в сервер защиты ПАК «БАС» необходимо съемным USB-носителем и способом описанным выше, при этом скопировав файлы в следующие директории:

– сертификат: **/usr/local/etc/ipsec.d/certs**;

– корневые сертификаты: **/usr/local/etc/ipsec.d/cacerts**;

– список отозванных сертификатов: **/usr/local/etc/ipsec.d/crls**.

2.3.2.6 Настройка программного обеспечения

2.3.2.6.1 Настройка программного обеспечения ПАК «БАС» заключается в редактировании конфигурационных файлов. Основным конфигурационным файлом ПАК «БАС» является файл **ipsec.conf**, который содержит информацию о настройках программного обеспечения ПАК «БАС». Файл **ipsec.conf** расположен

по пути **/etc/ipsec.conf** устройства защиты клиента или **/usr/local/etc/ipsec.conf** сервера защиты.

Примечание: в начале некоторых строк файла **ipsec.conf** присутствует символ «#». Данный символ означает, что строка является неактивной, и записанные в ней параметры не воспринимаются операционной системой устройства. Для активации такой строки нужно удалить символ «#», сохранить изменения в файле и перезагрузить ПАК «БАС».

2.3.2.6.2 Файл **ipsec.conf** разделен на секции, в каждой из которых описаны определенные параметры IPsec-соединения:

– conn %default – содержит общие параметры для всех IPsec-соединений;

– conn <Имя_соединения> – содержит параметры конкретного IPsec-соединения.

2.3.2.6.3 Для настройки программного обеспечения ПАК «БАС» необходимо:

– подать в командную строку устройства защиты клиента команду

vi /etc/ipsec.conf

или

– подать в командную строку сервера защиты команду

nano /usr/local/etc/ipsec.conf в командную строку сервера защиты

для редактирования файла **ipsec.conf**;

– при помощи стрелок на клавиатуре перейти к секции conn %default файла **ipsec.conf**, содержащей общие настройки IPsec-соединения;

– перейти к строке формата

left=XXX.XXX.XXX.XXX,

где:

XXX.XXX.XXX.XXX – IP-адрес интерфейса eth1, соответствующего порту «Сеть» ПАК «БАС»;

– изменить IP-адрес, установленный по умолчанию, на IP-адрес интерфейса eth1 ПАК «БАС»;

– перейти к строке формата

leftsubnet=XXX.XXX.XXX.XXX/YY,

где:

XXX.XXX.XXX.XXX – IP-адрес подсети, в которой находятся защищаемые ресурсы (пользователи) (защищаемая подсеть);

YY – маска подсети в формате CIDR, в которой находятся защищаемые ресурсы (пользователи) (защищаемая подсеть);

– изменить адрес и маску подсети, установленную по умолчанию, на адрес и маску защищаемой подсети;

– перейти к строке формата

leftcert=<Имя_файла_СОК>,

– изменить имя файла СОК на нужное;

– перейти к строке формата

esp=<EALG>-<IALG>

– установить необходимый криптонабор, указав параметры EALG и IALG в соответствии с приложением В (при отличии от установленного по умолчанию);

– перейти к строке формата

ike=<EALG>-<IALG>-<PRF>-<DHGROUP>-<KEYREP>

– установить необходимый криптонабор, указав параметры EALG, IALG, PRF, DHGROUP и KEYREP в соответствии с приложением В (при отличии от установленного по умолчанию);

– перейти к строке формата

ikelifetime = X<h | m | s>

где:

X – целое положительное число (время, через которое происходит переаутентификация);

h – час;

m – минута;

s – секунда.

– установить необходимые параметры времени, через которое происходит повторная аутентификация (при отличии от установленных по умолчанию);

– перейти к строке формата

lifetime = X<h | m | s>

где:

X – целое положительное число (время, через которое происходит смена сеансового ключа);

h – час;

m – минута;

s – секунда.

– установить необходимые параметры времени, через которое происходит смена сеансового ключа (при отличии от установленных по умолчанию);

ВНИМАНИЕ: Изменение параметров ikelifetime и lifetime на значения, отличные от установленных по умолчанию, может привести к нарушению квоты ключа, что может повлечь за собой снижение надежности алгоритма шифрования. Установленные значения обеспечивают высокий уровень гарантии. Смена значений параметров ikelifetime и lifetime может быть выполнена после проведения расчетов времени жизни ключа с учетом пропускной способности используемого артикула ПАК «БАС». Пример расчета приведен в Приложении А документа «Комплекс программный реализации протоколов IPsec strongSwanCont. Руководство оператора» BY.СЮИК.00371-02 34 01.

– перейти к секции conn <Имя_соединения> файла **ipsec.con**f, содержащей настройки IPsec-соединения;

– перейти к строке формата

right=XXX.XXX.XXX.XXX,

где:

XXX.XXX.XXX.XXX – IP-адрес «внешнего» интерфейса, ПАК «БАС» или КП «БАС-V», с которым будет устанавливаться IPsec-соединение;

– изменить IP-адрес по умолчанию на IP-адрес «внешнего» интерфейса ПАК «БАС» или КП «БАС-V», с которым будет устанавливаться IPsec-соединение;

– перейти к строке формата

rightsubnet=XXX.XXX.XXX.XXX/YY,

где:

XXX.XXX.XXX.XXX – IP-адрес подсети, в которой находятся ресурсы, к которым необходимо осуществить VPN соединение (удаленная защищаемая подсеть);

YY – маска подсети в формате CIDR, в которой находятся ресурсы, к которым необходимо осуществить VPN соединение (удаленная защищаемая подсеть);

– изменить адрес и маску подсети, установленные по умолчанию, на адрес и маску удаленной защищаемой подсети, в которой находятся ресурсы, к которым необходимо осуществить VPN соединение;

– перейти к строкам формата

leftauth = <auth method>

rightauth = <auth method>

где:

auth method – Способ аутентификации, используемый локально (**left**) или требуемый от удаленной (**right**) стороны.

ПАК «БАС» поддерживает аутентификацию и выработку общего ключа в соответствии с протоколом **BSTS**, требования к которому установлены в п. 7.5 СТБ 34.101.66-2014, **BPACE**, требования к которому установлены в п. 7.6 СТБ 34.101.66-2014 и **pubkey**, требования к которому установлены в приложении А к СТБ 34.101.66-2014. Для включения аутентификации с помощью протокола BSTS используется значение "**eap-bsts**". Для включения аутентификации с помощью протокола BPACE используется значение "**eap-bpace**".

– для каждого IPsec-соединение, создается секция с описанием соединения **conn <Имя_соединения>**;

– выйти из текстового редактора, сохранив внесенные в файл **ipsec.conf** изменения.

Редактирование остальных строк файла **ipsec.conf** выполнять только при необходимости и в строгом соответствии с документацией. Подробное описание параметров и возможных значений файла **ipsec.conf** приведено в документе «Комплекс программный реализации протоколов IPsec strongSwanCont. Руководство оператора. BY.СЮИК.00371-02 34 01».

2.3.2.6.4 В файл **ipsec.conf** также выполняются настройки журналирования (протоколирования) работы IPsec-демона.

Демон IKE charon регистрируется в системном журнале, поэтому его сообщения будут появляться по пути **/var/log/syslog** для Сервера защиты или **/var/log/messages** для Устройства защиты клиента.

Настройка журналирования выполняется в секции **config setup** файла **ipsec.conf**. Уровни журналирования и источники формирования записей в журнале аудита устанавливаются в параметре **charondebug**.

Демон IKE поддерживает числовые уровни ведения журнала (от -1 до 4):

-1: абсолютно тихий (отключение аудита от источника);

0: очень простые журналы аудита (например, SA up / SA down);

1: общий поток управления с ошибками, по умолчанию, хорош для того, чтобы увидеть, что происходит;

2: более подробный поток управления, для отладки;

3: включение в журнал дампов в шестнадцатеричном формате (RAW);

4: включение в журнал чувствительного материала, приватных данных.

Каждое сообщение журнала также имеет источник, от которого оно получено для записи в журнал. В настройках могут быть указаны следующие источники:

app: приложения, кроме демонов;

asn: низкоуровневое кодирование / декодирование (ASN.1, X.509 и т. д.);

cfg: управление конфигурацией и плагинами;

chd: CHILD_SA/IPsec SA;

dmn: настройка / очистка / обработка сигналов основного демона;

enc: операции кодирование / декодирование, шифрования / расшифрования пакетов;

esp: сообщения библиотеки libipsec;

ike: IKE_SA/ISAKMP SA;

imc: контроль целостности;

imv: проверка целостности;

job: работа очереди / процессов и управление потоками;

knl: работа сетевого интерфейса ядра для IPsec;

lib: сообщения библиотеки libstrongwan;

mgr: управление IKE_SA, обработчик синхронизации для доступа IKE_SA;

net: сетевая связь в IKE;

pts: сервис доверенной платформы;

tls: сообщения библиотеки libtls;

tnc: доверенное сетевое соединение.

Такое количество источников журналирования при работе устройства избыточно. Установка большого количества источников и высокого уровня журналирования приводит к усложнению поиска информации в журнале, в связи с его объемом. В комплекте поставке установлены минимальные требования, достаточные для анализа работы ПАК «БАС». Администратору рекомендуется повысить уровень журналирования при поиске проблем в настройках IPsec.

2.3.2.7 Настройка межсетевого экрана

2.3.2.7.1 Межсетевой экран ПАК «БАС» предназначен для осуществления контроля и фильтрации проходящего через него сетевого трафика в соответствии с заданными правилами.

2.3.2.7.2 ПАК «БАС» обеспечивает межсетевую защиту данных при помощи встроенного в ядро ОС Linux компонента Netfilter.

Netfilter – межсетевой экран (брандмауэр), компонент ядра ОС Linux, обеспечивающий фильтрацию и модификацию трафика.

2.3.2.7.3 Управление межсетевым экраном Netfilter производится из пространства пользователя с помощью команд iptables и ip6tables.

Iptables – название пользовательской утилиты (запускаемой из командной строки), предназначенной для управления системой Netfilter. С её помощью администраторы создают и изменяют правила, управляющие фильтрацией и перенаправлением пакетов. Для работы с семейством протоколов IPv6 существует отдельная версия утилиты iptables – ip6tables.

2.3.2.7.4 Информация о встроенном в ПАК «БАС» межсетевом экране приведена в документе «Комплекс программно-аппаратный криптографической защиты информации «БАС». Встроенное программное обеспечение. Межсетевой экран. Руководство оператора» BY.СЮИК.00368-02 34 01.

2.3.2.8 Настройка удаленного администрирования

2.3.2.8.1 ПАК «БАС» имеет возможность удаленной настройки по протоколу SSH. При этом SSH-сервер включен в настройки по умолчанию. Также настройки по умолчанию поддерживают получение IP-адреса по протоколу DHCP. Поэтому есть возможность перейти к удаленной настройке ПАК «БАС» без предварительной преднастройки. Для этого необходимо знать только IP-адрес, который ваш DHCP-сервер присвоил ПАК «БАС».

2.3.2.8.2 ПАК «БАС» имеет возможность пересылки журнала своей работы удаленному SYSLOG-серверу. Для этого необходимо в конец файла **/etc/rsyslog.conf** добавить строку формата:

***.* @@<IP-адрес>:<порт>**

где:

<IP-адрес> – IP-адрес SYSLOG-сервера;

<порт> – порт на котором SYSLOG-сервер ожидает данные;

. – пересылка всех данных, попадающих в журнал аудита.

2.3.2.8.3 ПАК «БАС» предоставляет возможность удаленного мониторинга своей работы по средствам протокола SNMP при помощи пакета snmpd. В связи с этим в защищенной при помощи ПАК «БАС» сети может быть развернута свободно распространяемая система мониторинга (Zabbix, Cacti и др.)

2.3.2.9 Обеспечение бесперебойной работы ПАК «БАС»

2.3.2.9.1 При инициализации ПАК «БАС» администратор выпускает ключевую пару и загружает в ПАК «БАС» СОК. После чего производит настройки, и ПАК «БАС» обеспечивает защиту данных.

2.3.2.9.2 Однако, СОК имеет срок действия. После его окончания ПАК «БАС» хотя бы у одного устройства, ПАК «БАС» не смогут выполнить взаимную аутентификацию и установить IPsec соединение.

2.3.2.9.3 В связи с этим, ПАК «БАС» имеет возможность выпуска резервного (дополнительного) ключа.

2.3.2.9.4 Резервный ключ рекомендуется выпускать за несколько дней до истечения срока действия основного.

2.3.2.9.5 Выпуск резервного ключа выполняется при помощи утилиты **RequestBuilder**.

2.3.2.9.6 Действия по выпуску резервного кляча совпадают с действиями, описанными в п. 2.3.2.5.

2.3.2.9.7 После завершения процедуры **RequestBuilder** личный ключ будет сохранен в резервной область ПАК «Барьер - USB», а открытый помещен в запрос на выпуск сертификата, имя и путь к которому выводится в командную строку.

2.3.2.9.8 Запрос на выпуск СОК необходимо экспортировать из ПАК «БАС» и передать администратору Удостоверяющего или Регистрационного центра для выпуска СОК.

2.3.2.9.9 После того как СОК будет загружен в ПАК «БАС» необходимо отредактировать файл **ipsec.conf**, указав в параметре leftcert=<Имя_файла_СОК>, имя нового файла СОК.

2.3.2.9.10 Для переноса ключа из резервной области ПАК «Барьер - USB» в основную необходимо подать команду **sudo KeyReplacer** в командную строку.

2.3.2.9.11 Для установки IPsec соединения с использованием новой пары ключей необходимо подать команду **sudo ipsec restart** в командную строку.

2.3.2.9.12 Для проверки применения новой пары ключей необходимо подать команду **sudo ipsec listcerts** в командную строку и просмотреть срок действия СОК.

2.3.2.10 Типовые сценарии подключения, работы и настройки ПАК «БАС»

ПАК «БАС» является сетевым устройством, и его настройки могут существенно зависеть от топологии сети и включения в неё самого ПАК «БАС». В связи с этим, для облегчения работы администратора, был разработан ряд инструкций, описывающих типовые сценарии подключения, работы и настройки ПАК «БАС».

2.3.3 Эксплуатация ПАК «БАС»

2.3.3.1 В процессе эксплуатации возможны три основных состояния ПАК «БАС»:

– нормальная работа;

– ошибка;

– администрирование устройства.

2.3.3.2 Нормальная работа ПАК «БАС» не предполагает непосредственного взаимодействия администратора с устройством.

Поскольку ПАК «БАС» не накладывает ограничений на функциональные возможности защищаемых устройств (пользователей), то при нормальной работе ПАК «БАС» для них «прозрачен».

2.3.3.3 ПАК «БАС» имеет световую индикацию. На лицевую панель ПАК «БАС» вынесены 3 светодиода: «Работа», «Ошибка», «Питание». При правильной подаче на устройство напряжения питания загорается светодиод «Питание», и начинается загрузка ОС, после успешного завершения которой, ПАК «БАС» готов к работе, о чем сообщит загоревшийся светодиод «Работа» устройства защиты клиента. Светодиодом «Работа» сервера защиты является светодиод активности жесткого диска, поэтому о загрузке ОС сервера защиты и готовности к работе будет свидетельствовать активное мигание светодиода. Нормальная загрузка ОС ПАК «БАС» не должна превышать 60 сек.

2.3.3.4 В процессе работы ПАК «БАС» производит проверку своей работоспособности при включении и по запросу администратора.

2.3.3.5 При обнаружении неисправности ПАК «БАС» формирует серии вспышек светодиода «Ошибка». При этом количество вспышек в серии указывает на причину неисправности:

– одна вспышка – нарушение целостности личного ключа (был вскрыт корпус, уничтожен личный ключ);

– две вспышки – ошибка аппаратной составляющей (неработоспособность генератора случайных чисел или плохое качество случайной числовой последовательности, нарушение целостности прошивки ПАК «Барьер - USB»;

– четыре вспышки – ошибка выполнения криптографических алгоритмов или нарушение целостности программного обеспечения.

2.3.3.6 При возникновении ошибки на ПАК «БАС» связь между защищаемыми устройствами (пользователями) будет нарушена. При этом пользователям абонентских защищаемых устройств следует обратиться к администратору ПАК «БАС».

2.3.3.7 Для проверки работоспособности ПАК «БАС» администратору необходимо:

– подать команду **sudo basctl** в командную строку ПАК «БАС»;

– результат проверки выводится в командную строку.

2.3.3.8 Администрирование устройства производится администратором, который выполняет следующие основные функции:

– управление ключевой информацией (запись, удаление, администрирование);

– периодический контроль работоспособности устройства и изменение настроек устройства (при необходимости);

– администрирование журнала;

– создание и редактирование параметров IPsec-соединения;

– восстановление работоспособности устройства в случае возникновения ошибок.

2.3.3.9 Администратор осуществляет периодическую смену ключевой информации. Процедура генерации пары ключей описана в п. 2.3.2.5.

2.3.3.10 При необходимости администратор может сменить используемый криптонабор на ПАК «БАС». Процедура смены криптонабора описана в п. 2.3.2.6. После смены криптонабора необходимо перезапустить ПО ПАК «БАС», подав в командную строку устройства команду **sudo ipsec restart**.

2.3.3.11 В случае смены криптонабора на ПАК «БАС» администратор должен установить соответствующий криптонабор на каждом подключаемом к нему устройстве.

2.3.3.12 ПАК «БАС» ведет журнал аудита, в который заносится следующая информация:

– дата и время;

– вызываемая функция;

– идентификационные данные пользователя;

– результат (успешно/неуспешно).

2.3.3.13 Контроль системного журнала осуществляет администратор.

2.3.3.14 Для получения доступа к системному журналу ПАК «БАС» администратору необходимо подать в командную строку команду **cat /var/log/syslog** – для сервера защиты или **cat /var/log/messages** – для устройства защиты клиента.

2.3.3.15 ПАК «БАС» при помощи ПАК «Барьер - USB», входящего в его состав ведет непрерывный контроль вскрытия корпуса. При обнаружении вскрытия корпуса уничтожается личный ключ, хранящийся в защищенном хранилище ПАК «Барьер - USB», и фиксируется время вскрытия корпуса во внутреннем журнале ПАК «Барьер-USB» (журнал критических событий). Доступ к журналу разрешен только администратору после предъявления пароля для доступа к защищенному хранилищу.

2.3.3.16 Для получения доступа к журналу критических событий администратору необходимо подать в командную строку устройства команду **sudo LogViewer**.

2.3.3.17 В случае возникновения ошибки администратор должен принять меры по ее устранению. Наиболее вероятные ошибки описаны в разделе 4 настоящего РЭ.

2.3.4 Вывод ПАК «БАС»из эксплуатации

2.3.4.1 Вывод ПАК «БАС» из эксплуатации осуществляется администратором. На этапе вывода из эксплуатации происходит полное уничтожение всей ключевой информации, хранящейся в памяти ПАК «БАС», а также отключение устройства от сети передачи защищаемых данных и сети питания.

2.3.4.2 Для полного удаления ключевой информации из памяти ПАК «БАС» администратору необходимо:

– подать команду **sudo Uninstaller** в командную строку ПАК «БАС»;

– ввести пароль для доступа к личному ключу;

– убедиться, что ПАК «БАС» производит обнуление личного ключа с выводом результата в командную строку.

2.3.4.3 Вывод устройства защиты клиента из эксплуатации производится в следующем порядке:

– отключить сети передачи данных от портов «Абонент», «Сеть» устройства защиты клиента;

– если для электропитания устройства защиты клиента используется инжектор PoE, отключить его от сети электропитания 220 В и сети передачи защищаемых данных;

– произвести запись об отключении устройства в паспорте;

– поместить устройство защиты клиента в упаковку.

2.3.4.4 Вывод сервера защиты из эксплуатации производится в следующем порядке:

– подать в командную строку команду **sudo shutdown –h 0**;

– отключить сервер защиты от сети электропитания 220 В;

– отключить сервер защиты от сети передачи данных;

– отключить сервер защиты от защищаемой подсети;

– произвести запись об отключении устройства в паспорте;

– поместить сервер защиты в упаковку.

2.4 Действия в экстремальных условиях

2.4.1 На случай пожара, аварии или стихийного бедствия должны быть разработаны специальные инструкции, утвержденные руководством предприятия,

учреждения, в которых предусматривается порядок вызова администрации, должностных лиц, вскрытие помещений, очередность и порядок спасения.

2.4.2 В случае возгорания немедленно обесточить цепи питания и принять меры по ликвидации очага возгорания имеющимися средствами пожаротушения.

ВНИМАНИЕ: В СВЯЗИ С ТЕМ, ЧТО ПРИБОР ПОДКЛЮЧЕН К СЕТИ ЭЛЕКТРОПИТАНИЯ НАПРЯЖЕНИЕМ 220 В, ЗАПРЕЩАЕТСЯ ПРИМЕНЯТЬ ДЛЯ ТУШЕНИЯ КИСЛОТНЫЕ ОГНЕТУШИТЕЛИ.

3 Техническое обслуживание

3.1 Общие указания

3.1.1 Техническое обслуживание проводят с целью обеспечения нормальной работы ПАК «БАС» в течение всего срока эксплуатации.

3.1.2 Техническое обслуживание должно проводиться по графику, составленному и утвержденному потребителем на основании рекомендаций настоящего раздела.

3.2 Меры безопасности

3.2.1 К техническому обслуживанию допускаются работники, изучившие настоящее руководство по эксплуатации. При выполнении технического обслуживания необходимо соблюдать все меры по технике безопасности при работе с электроустановками.

3.3 Порядок технического обслуживания

3.3.1 Техническое обслуживание ПАК «БАС» заключается в выполнении своевременных профилактических осмотров. При эксплуатации ПАК «БАС» должны выполняться профилактические осмотры не реже одного раза в год, при этом:

– проверяется целостность корпусов ПАК «БАС», надежность крепления и подключения в местах использования;

– корпуса ПАК «БАС» очищаются от пыли и грязи.

3.3.2 В процессе обслуживания вскрытие корпуса ПАК «БАС» не допускается, поскольку вскрытие корпуса приводит к нарушению установленной политики безопасности и уничтожению ключевой информации.

4 Текущий ремонт

4.1 Общие положения

4.1.1 Текущий ремонт ПАК «БАС» осуществляется предприятием-изготовителем.

4.1.2 Краткий перечень возможных неисправностей приведен в таблице 2.

Таблица 2 – Краткий перечень возможных неисправностей ПАК «БАС»

Вид неисправности	Причина	Способ исправления
Не загорается светодиод «Питание» после включения устройства.	Неправильное включение ПАК «БАС».	Проверить правильность подключения ПАК «БАС». Произвести подключение согласно п. 2.2 данного РЭ.
Не загорается светодиод «Питание» после включения устройства.	Выход из строя ПАК «БАС».	Обратиться к производителю.
Не загорается светодиод «Работа».	Сбой загрузки ОС ПАК «БАС».	Перезапустить ПАК «БАС».
Не загорается светодиод «Работа».	Выход из строя ПО ПАК «БАС».	Обратиться к производителю.
Серия одиночных вспышек светодиода «Ошибка».	Был вскрыт корпус. Уничтожена ключевая информация.	Произвести восстановление личного ключа в соответствии с п. 4.2; Произвести возврат к заводским настройкам в соответствии с п. 2.3.4 и генерацию новых ключей.
Серия многократных вспышек светодиода «Ошибка».	Выход из строя отдельных узлов ПАК «БАС».	Обратиться к производителю.

4.2 Восстановление ПАК «БАС» после сбоя

4.2.1 ПАК «БАС» при помощи ПАК «Барьер - USB», входящего в его состав ведет непрерывный контроль вскрытия корпуса. При обнаружении вскрытия корпуса уничтожается личный ключ, хранящийся в защищенном хранилище ПАК «Барьер - USB», и фиксируется время вскрытия корпуса во внутреннем журнале ПАК «Барьер - USB» (журнал критических событий).

4.2.2 После уничтожения личного ключа администратор должен проанализировать журнал критических событий и определить причину уничтожения личного ключа. После чего выполнить действия по возврату устройства в работоспособное состояние. Это можно сделать двумя способами.

4.2.3 Вывести устройство из эксплуатация в соответствии с п. 2.3.4 и произвести новую генерацию ключевой пары, или произвести восстановление личного ключа из резервной копии (при ее наличии).

4.2.4 Для восстановления личного ключа из резервной копии необходимо:

– поместить блоб личного ключа в файловую систему ПАК «БАС»;

– подать в командную строку команду **sudo PrivateKeyRecovery**, предварительно отредактировав файл **/etc/support/PrivateKeyRecovery.conf**, (при отличии мест хранения контейнера ключа и частичных секретов от заданных по умолчанию).

– при запросе приложения, ввести пароль для доступа к защищенному хранилищу;

– при запросе приложения, ввести пароль для снятия защиты с блоба личного ключа;

– при запросе приложения, ввести новый пароль для доступа к защищенному хранилищу.

4.2.5. Настоечный файл представляет собой текстовый файл, разделённый на секции. Секции разделяются именем (секции), заключённым в прямоугольные скобки ([имя_секции]). Каждая секция может иметь одно или несколько полей

вида «Параметр = Значение». Имена параметров предопределены для каждой секции.

Секция, соответствующая модулю восстановления личного ключа, должна именоваться **PrivateKeyRecovery**. Данная секция включает следующие параметры:

– **PrivateKeyFileName**. Значением параметра должен быть путь к файлу контейнера основного личного ключа;

– **ShareSecretFileName_N**. N – порядковый номер основного частичного секрета. Значением параметра должен быть путь к файлу N-го частичного секрета;

– **PrivateKeyFileNameReserve**. Опциональный параметр. Значением параметра должен быть путь к файлу контейнера резервного личного ключа;

– **ShareSecretFileNameReserve_N**. Опциональный параметр. N – порядковый номер резервного частичного секрета. Значением параметра должен быть путь к файлу N-го частичного секрета.

5 Хранение

5.1 ПАК «БАС» не содержит в своем составе веществ и материалов, опасных для жизни и здоровья человека и окружающей среды, и не требует принятия специальных мер предосторожности при хранении.

5.2 Не допускается хранение ПАК «БАС» совместно с испаряющимися жидкостями, кислотами и другими веществами, которые могут вызвать коррозию.

5.3 Хранение должно осуществляться в упаковке в отапливаемых складских помещениях при температуре окружающего воздуха от плюс 5 до плюс 40 ºС и относительной влажности не более 80 % при температуре окружающего воздуха плюс 25 ºС.

5.4 Постановка ПАК «БАС» на хранение и снятие с хранения оформляется приказом (распоряжением) руководителя эксплуатирующей организации, в котором указывается перечень работ, правила их проведения, меры безопасности, условия хранения.

6 Транспортирование

6.1 ПАК «БАС» не содержит в своем составе веществ и материалов, опасных для жизни и здоровья человека и окружающей среды, и не требует принятия специальных мер предосторожности при транспортировании.

6.2 ПАК «БАС» в тарной упаковке должно транспортироваться в подборной таре железнодорожным, авиационным (в герметизированных отсеках), водным (кроме морского) и автомобильным видом транспорта на любое расстояние, в соответствии с правилами перевозок, действующими на каждом виде транспорта.

6.3 Размещение и крепление транспортной тары с транспортируемыми изделиями в транспортных средствах должно обеспечивать ее устойчивое положение и не допускать перемещения во время транспортирования.

6.4 ПАК «БАС» должно сохранять после транспортирования в упакованном виде конструкцию, внешний вид и работоспособность при воздействии на него в процессе транспортирования механических ударных нагрузок многократного действия с пиковым ускорением до 147 м/с^2 (15 g) при длительности действия ударного ускорения от 10 до 15 мс.

6.5 Условия транспортирования ПАК «БАС» должны соответствовать:

– температура окружающего воздуха при транспортировании – от минус 40 до плюс 50 °С;

– относительная влажность окружающего воздуха – не более 95 % при температуре окружающего воздуха плюс 25 °С;

– атмосферное давление от 84 до 107 кПа (от 630 до 800 мм рт. ст.).

6.6 В транспортных средствах, где перевозятся ПАК «БАС», не должно быть паров кислот, щелочей и других химически активных веществ, пары или газы которых могут вызвать коррозию.

6.7 Распаковку ПАК «БАС» после транспортирования при температуре ниже минус 10 °С проводить в отапливаемом помещении, предварительно выдержав его нераспакованным не менее 2 ч.

7 Утилизация

7.1 ПАК «БАС» не содержит в своем составе ядовитых и вредных веществ и материалов, опасных для жизни и здоровья человека, а также представляющих опасность для окружающей среды, и не требует специальных мер предосторожности при утилизации.

7.2 Утилизацию ПАК «БАС» проводят после окончания срока службы и заключения комиссии о нецелесообразности дальнейшей эксплуатации ПАК «БАС».

7.3 Мероприятия по подготовке и отправке на утилизацию разрабатываются согласно распоряжению руководителя предприятия в соответствии с порядком утилизации, установленным на предприятии.

7.4 Все мероприятия по подготовке и отправке ПАК «БАС» на утилизацию должны производиться при полном отключении защищаемых сетей.

7.5 При подготовке ПАК «БАС» к утилизации следует соблюдать меры безопасности, предусмотренные для монтажных и механических работ. Для подготовки к утилизации следует провести демонтаж ПАК «БАС» с целью извлечения узлов с электронными компонентами, которые содержат драгоценные металлы, и извлечения деталей, изготовленных из цветных металлов.

7.6 ПАК «БАС» не представляет опасности для жизни, здоровья и окружающей среды после окончания срока службы (эксплуатации).

8 Ресурсы, сроки службы и хранения, гарантии изготовителя (поставщика)

8.1 ПАК «БАС» при эксплуатации обеспечивает:

а) средний срок службы – не менее 10 лет с учетом проведения восстановительных работ;

б) средний срок сохраняемости (от момента изготовления до ввода в эксплуатацию) – не менее 18 месяцев, при соблюдении условий хранения.

8.2 Предприятие-изготовитель (поставщик) гарантирует соответствие ПАК «БАС» требованиям технической документации при соблюдении потребителем правил и условий эксплуатации, хранения, транспортирования и монтажа, установленных документацией.

8.3 Гарантийный срок хранения и эксплуатации ПАК «БАС» – 18 мес. со дня реализации предприятием-изготовителем, при соблюдении условий хранения и эксплуатации.

8.4 Гарантийное обслуживание ПАК «БАС» осуществляется изготовителем или другой организацией, имеющей с изготовителем соответствующее соглашение, за счет изготовителя.

8.5 Потребитель лишается права на гарантийное обслуживание при нарушении условий эксплуатации, хранения, транспортирования и монтажа ПАК «БАС».

8.6 Послегарантийное обслуживание ПАК «БАС» осуществляется за счет потребителя по договору между изготовителем или другой организацией, имеющей с изготовителем соответствующее соглашение, и потребителем.

Приложение А

(справочное)

Перечень принятых сокращений

В настоящем руководстве по эксплуатации приняты следующие сокращения:

ДСЧП	– датчик случайных числовых последовательностей
ОЗУ	– оперативное запоминающее устройство
ОС	– операционная система
ПАК	– программно-аппаратный комплекс
ПЗУ	– постоянное запоминающее устройство
ПО	– программное обеспечение
ПЭВМ	– персональная электронно-вычислительная машина
РЭ	– руководство по эксплуатации
ЭД	– эксплуатационный документ

Приложение Б

(справочное)

Пример файла с персональными данными

```
<?xml version="1.0" encoding="UTF-8" ?>
<PersonalData>
	<Subject>
		<CommonName OId="2.5.4.3" Description="Общее имя устройства">
			Комплекс программно-аппаратный
			криптографической защиты информации "БАС"
		</CommonName>
		<Name OId="2.5.4.41" Description="Полное название организации">
			Закрытое акционерное общество "НТЦ КОНТАКТ"
		</Name>
		<SerialNumber OId="2.5.4.5" Description="Серийный номер устройства">
			00001
		</SerialNumber>
		<CountryName OId="2.5.4.6" Description="Код страны организации">
			BY
		</CountryName>
		<LocalityName OId="2.5.4.7" Description="Населённый пункт организации">
			г. Минск
		</LocalityName>
		<StateOrProvinceName OId="2.5.4.8" Description="Область и район (опц.)" />
		<OrganizationName OId="2.5.4.10" Description="Сокращенное название">
			ЗАО "НТЦ КОНТАКТ"
		</OrganizationName>
		<OrganizationUnitName OId="2.5.4.11" Description="Подразделение (опц.)" />
		<OrganizationIdentifier OId="2.5.4.97" Description="Ид-тор организации
		следующего вида - 'TAX[2 символа кода страны]-[УНП организации]'">
			TAXBY-100037461
		</OrganizationIdentifier>
	</Subject>
	<ExtensionRequest OId="1.3.6.1.4.1.311.2.1.14" Description="Расширения сертиф.">
		<!--
		<SubjectAltName OId="2.5.29.17" Description="Альтернативное имя">
			<!-- <EMail> example@mail.by </EMail> -->
			<!-- <DNS> example.by </DNS> -->
			<!-- <URI> http://example.by </URI> -->
			<!-- <IP> 10.0.0.1 </IP> -->
		</SubjectAltName>
		-->
	</ExtensionRequest>
	<!--
	<CertificateValidityPeriod Description="Период действия сертификата, лет">
		2
	</CertificateValidityPeriod>
	-->
</PersonalData>
```

Приложение В

(справочное)

Список обозначений доступных криптографических алгоритмов

Таблица В 1 – Список обозначений доступных криптографических алгоритмов для записи в ipsec.conf

EALG	
belt_cbc	алгоритм шифрования СТБ 34.101.31-2020 в режиме сцепления блоков
belt_cfb	алгоритм шифрования СТБ 34.101.31-2020 в режиме гаммирования с обратной связью
belt_ctr	алгоритм шифрования СТБ 34.101.31-2020 в режиме счётчика
belt_cbc_legacy	алгоритм шифрования СТБ 34.101.31-2020 в режиме сцепления блоков (для совместимости с первой версией ПАК «БАС»)
belt_cfb _legacy	алгоритм шифрования СТБ 34.101.31-2020 в режиме гаммирования с обратной связью (для совместимости с первой версией ПАК «БАС»)
belt_ctr legacy	алгоритм шифрования СТБ 34.101.31-2020 в режиме счётчика (для совместимости с первой версией ПАК «БАС»)
IALG	
belt_mac	алгоритм выработки иммитовставки СТБ 34.101.31-2020
belt_hmac	алгоритм ключезависимого хэширования СТБ 34.101.47-2017
belt_mac_legacy	алгоритм выработки иммитовставки СТБ 34.101.31-2020 (для совместимости с первой версией ПАК «БАС»)
belt_hmac_legacy	алгоритм ключезависимого хэширования СТБ 34.101.47-2017 (для совместимости с первой версией ПАК «БАС»)
PRF	
prfbrng_ctr	алгоритм выработки псевдослучайных чисел СТБ 34.101.47-2017 в режиме счётчика
prfbrng_hmac	алгоритм выработки псевдослучайных чисел СТБ 34.101.47-2017 в режиме HMAC
DHGROUP	
ecp256bign	Алгоритм Диффи-Хеллмана с соответствии с СТБ 34.101.66-2014 Приложение А.
modp2048	(для совместимости с первой версией ПАК «БАС»)
KEYREP	
keyrep	алгоритм преобразования ключа СТБ 34.101.31-2020
Примечания: – жирным выделены алгоритмы, используемые по умолчанию; – курсивом выделены первые поддерживаемые значения.	

ВНИМАНИЕ: ОБОЗНАЧЕНИЕ АЛГОРИТМОВ ДЛЯ ЗАПИСИ В ФАЙЛ IPSEC.CONF ДОЛЖНО ТОЧНО СООТВЕТСТВОВАТЬ ТАБЛИЦЕ Д 1.

ПРИ ЗАПИСИ НЕОПОЗНАННОГО ОБОЗНАЧЕНИЯ АЛГОРИТМОВ В ФАЙЛ IPSEC.CONF ПАК «БАС» БУДЕТ ИСПОЛЬЗОВАТЬ ПЕРВЫЕ ПОДДЕРЖИВАЕМЫЕ ЗНАЧЕНИЯ.

ПРИ ОТСУТСТВИИ ЗАПИСИ АЛГОРИТМОВ В ФАЙЛ IPSEC.CONF ПАК «БАС» БУДЕТ ИСПОЛЬЗОВАТЬ ЗНАЧЕНИЯ ПО УМОЛЧАНИЮ.

Приложение Г

(справочное)

Пример настроечного файла ipsec.conf ПАК «БАС»

```
basv@basvr:~$ sudo nano /usr/local/etc/ipsec.conf

config setup
        charondebug = "ike 1, lib 1, cfg 1"

# Add connections here.
conn %default
        keyexchange = ikev2
        ikelifetime = 24h
        lifetime = 1h
        rekeymargin = 5m
        lifebytes = 11000000000000
        marginbytes = 10000000000
        dpdaction = restart
        closeaction = restart
        ike = belt_cfb-belt_mac-prfbrng_ctr-ecp256bign-keyrep
        esp = belt_cfb-belt_mac
        left = 200.0.0.100
        leftsubnet = 10.0.0.0/24
        leftid = %any
        leftcert = BAS_Client.cer
        leftauth = eap
        keyingtries = %forever
        auto = start

conn server-server
        right = 200.0.0.200
        rightsubnet = 10.10.10.0/24
        rightid = %any
        rightauth = eap
        rightsendcert = never
```

Приложение Д

(справочное)

Пример настроечного файла ipsec.conf удаленного сервера

```
basv@basvr:~$ sudo nano /usr/local/etc/ipsec.conf
config setup
        charondebug = "ike 1, lib 1, cfg 1"

# Add connections here.
conn %default
        keyexchange = ikev2
        ikelifetime = 24h
        lifetime = 1h
        rekeymargin = 5m
        lifebytes = 11000000000000
        marginbytes = 10000000000
        dpdaction = restart
        closeaction = restart
        ike = belt_cfb-belt_mac-prfbrng_ctr-ecp256bign-keyrep
        esp = belt_cfb-belt_mac
        left = 200.0.0.200
        leftsubnet = 10.10.10.0/24
        leftid = %any
        leftcert = BAS_Server.cer
        leftauth = eap-bsts
        auto = route

conn server-server
        right = 200.0.0.100
        rightsubnet = 10.0.0.0/24
        rightid = %any
        rightauth = eap-bsts
        rightsendcert = never
```