УТВЕРЖДЕН

BY.СЮИК.00436-01 34 02-ЛУ

КОМПЛЕКС ПРОГРАММНЫЙ ВИРТУАЛЬНЫЙ КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ «БАС-V»

Руководство оператора

Использование в качестве сервера

BY.СЮИК.00436-01 34 02

Листов 28

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

2021

№ изм.	Подп.	Дата

Литера O_1

АННОТАЦИЯ

В настоящем документе описывается последовательность действий по запуску «Комплекса программного виртуального криптографической защиты информации «БАС-V» (КП «БАС-V») и порядок взаимодействия оператора с данным программным обеспечением.

Для понимания изложенного в документе материала необходимы навыки администрирования операционных систем семейства Linux, а также знание основ криптографии и нормативных правовых актов в области технического нормирования и стандартизации – СТБ 34.101.17-2012, СТБ 34.101.19-2012, СТБ 34.101.31-2020, СТБ 34.101.45-2013, СТБ 34.101.47-2017, СТБ 34.101.60-2014, СТБ 34.101.66-2014 и СТБ 34.101.78-2019.

Данный документ предназначен для операторов (администраторов), обеспечивающих надежную и безопасную работу сетей передачи данных.

СОДЕРЖАНИЕ

1. НАЗНАЧЕНИЕ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

1.1. КП «БАС-V» предназначен для защиты каналов обмена информацией между абонентами, взаимодействующими по цифровому протоколу IP через сети передачи данных.

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

1.3. Область применения КП «БАС-V» – системы обработки информации ограниченного распространения.

1.4. КП «БАС-V» производится в следующих конфигурациях:

а) виртуальная машина с минимальными требованиями к аппаратной платформе для защиты рабочего места оператора (клиент);

б) виртуальная машина, предназначенная для работы в многопроцессорных системах, для защиты больших объемов данных (сервер).

1.5. КП «БАС-V» реализует следующие функциональные возможности:

а) защиту информации путем ее шифрования с использованием криптографических алгоритмов на основе протоколов IPsec;

б) шифрование передаваемых данных в соответствие с СТБ 34.101.31-2020;

в) контроль целостности пакетов данных (вычисление имитовставки) в соответствие с СТБ 34.101.31-2020, СТБ 34.101.47-2017;

г) согласование ключей шифрования производится по СТБ 34.101.66-2014;

д) генерацию ключей и синхропосылок при помощи СТБ 34.101.47-2017 с использованием генератора случайных числовых последовательностей (ГСЧП) на основе физического датчика;

е) выработку открытых ключей при помощи СТБ 34.101.45-2013;

ж) формирование запроса на получение сертификата открытого ключа в соответствии с СТБ 34.101.17-2012;

и) обработку сертификатов открытых ключей и списки отозванных сертификатов в соответствии с СТБ 34.101.19-2012;

к) защиту секретных (личных) ключей от несанкционированного раскрытия, модификации и подмены, открытых – от модификации и подмены;

л) проверку работоспособности при включении и по запросу администратора;

м) тестирование следующих параметров;

– тесты криптографических алгоритмов;

– контроль целостности программного обеспечения;

н) возможность работы через NAT при помощи протокола NAT Traversal (NAT-T);

о) ведение журнала аудита и предоставление доступа к нему по протоколу SYSLOG, в который заносится следующая информация:

– дата и время;

– вызываемая функция;

– результат (успешно/неуспешно);

п) автоматическую смену ключей шифрования при достижении заданного объема переданных данных либо «времени жизни» ключа;

р) не ограничивает функциональные возможности защищаемых серверных и абонентских (клиентских) устройств.

1.6. КП «БАС-V» реализует следующие дополнительные функциональные возможности:

а) удаленное управление по протоколу SSH, причем КП «БАС-V» может быть предварительно настроен таким образом, что управляющие SSH пакеты будут защищены при помощи протоколов IPsec.

б) передача сведений о своем состоянии по протоколу SMNP для сбора статистики о работе КП «БАС-V».

в) защита 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;

г) объединение нескольких КП «БАС-V» в кластер для обеспечения отказоустойчивости с использованием протоколов CARP или VRRP;

д) поддержка протоколов динамической маршрутизации (RIP, OSPF, BGP) при помощи пакета Quagga;

е) пакетная фильтрация данных при помощи встроенного межсетевого экрана.

2. УСЛОВИЯ ВЫПОЛНЕНИЯ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

КП «БАС-V» поставляется с заранее предустановленной операционной системой семейства Linux.

Для работы КП «БАС-V» необходимы следующие свободные ресурсы, для разворачивания виртуальной машины:

- процессор, совместимый с Intel Pentium, с тактовой частотой не менее 900 МГц;
- оперативное запоминающее устройство (ОЗУ) с объемом памяти не менее 256 Мбайт;
- накопитель на жестких магнитных дисках (НЖМД) с объемом свободного адресного пространства 2 Гбайт,
- средство подключения к сети передачи данных (сетевая карта или модем).

Для функционирования КП «БАС-V» в качестве сервера необходимо наличие среды виртуализации.

3. ВЫПОЛНЕНИЕ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

3.1. Принцип работы

3.1.1. Принцип работы КП «БАС-V» основан на организации шифрованного канала связи. КП «БАС-V» может устанавливать канал связи с другими КП «БАС-V» либо с ПАК «БАС».

3.1.2. В процессе работы КП «БАС-V» 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.

3.1.3.5 КП «БАС-V» обеспечивает шифрование передаваемой информации путем создания защищенных IPsec-туннелей между ними.

3.1.4. При включении и по запросу администратора КП «БАС-V» выполняет самотестирование.

3.2. Роли пользователей

3.2.1. КП «БАС-V» предполагает наличие двух ролей пользователей с доступными для каждой из ролей функциями и с наличием определенных прав:

– роль администратора;

– роль пользователя.

3.2.2. Роль администратора предназначена для ввода КП «БАС-V» в эксплуатацию, настройки устройства, восстановления работоспособности в случае возникновения ошибок, а также для вывода КП «БАС-V» из эксплуатации. Основными функциями, выполняемыми администратором, являются:

– первичная настройка для работы в сети передачи данных;

– генерация личных ключей и ввод в КП «БАС-V» сертификатов открытых ключей;

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

– регистрация средств создания защищенного канала, находящихся на другой стороне;

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

– администрирование журнала;

– восстановление работоспособности устройства в случае возникновения ошибок.

3.2.3. Роль пользователя при использовании КП «БАС-V» в качестве сервера выполняют устройства, находящиеся в защищаемой сети.

3.2.4. КП «БАС-V» предназначен для криптографической защиты информации, передаваемой его пользователями.

3.3. Этапы использования КП «БАС-V»

3.3.1. Использование КП «БАС-V» включает в себя следующие основные этапы:

– ввод КП «БАС-V» в эксплуатацию – настройка администратором;

– эксплуатация КП «БАС-V» – использование для защиты информации, передаваемой по каналам связи;

– вывод КП «БАС-V» из эксплуатации.

3.3.2 Ввод КП «БАС-V» в эксплуатацию осуществляется администратором. На этапе ввода в эксплуатацию выполняется настройка, которая заключается в редактировании необходимых конфигурационных файлов, а также генерации личных ключей и загрузке сертификатов открытых ключей в КП «БАС-V».

3.3.3 Эксплуатацию КП «БАС-V» осуществляет пользователь. При этом администратор может проводить контроль работоспособности системы, при необходимости осуществляет смену используемых криптографических алгоритмов и ключей.

3.3.4 Вывод КП «БАС-V» из эксплуатации осуществляется администратором. На этапе вывода из эксплуатации происходит полное уничтожение всей ключевой информации, хранящейся в памяти КП «БАС-V».

3.4. Ввод КП «БАС-V» в эксплуатацию – настройка

3.4.1. Последовательность настройки

3.4.1.1. Ввод в эксплуатацию КП «БАС-V» состоит из следующих этапов:

– подготовка среды функционирования;

– установка КП «БАС-V»;

– 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 КП «БАС-V».

3.4.2. Подготовка среды функционирования

2.4.2.1. Для функционирования КП «БАС-V» в качестве сервера необходимо наличие среды виртуализации.

2.4.2.2. Подготовка среды виртуализации проводится в соответствии с документацией на используемую среду.

3.4.3. Установка КП «БАС-V»;

3.4.3.1. Для установки КП «БАС-V» необходимо выполнить импорт виртуальной машины из OVA файла в соответствии с документацией на используемую среду.

3.4.3.2. Для осуществления настройки КП «БАС-V» необходимо предварительно выполнить следующие операции:

– запустить КП «БАС-V» в среде виртуализации;

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

– осуществить вход в операционную систему КП «БАС-V», введя логин администратора **basv** и транспортный пароль **11111111**;

– получить доступ к командной строке КП «БАС-V».

3.4.4. Смена пароля администратора КП «БАС-V»

ВНИМАНИЕ: СМЕНА ТРАНСПОРТНОГО ПАРОЛЯ ЯВЛЯЕТСЯ ОБЯЗАТЕЛЬНОЙ

3.4.4.1. Для смены пароля необходимо воспользоваться командой **passwd**, после чего ввести транспортный пароль **11111111**, а затем задать и подтвердить новый. Пароль должен быть не менее 8 символов.

```
basv@basv:~$ passwd
Changing password for basv.
(current) UNIX password:
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
```

3.4.5. Настройка сетевых интерфейсов КП «БАС-V»

3.4.5.1. Настройка сетевых интерфейсов КП «БАС-V» производится путем заполнения файла **/etc/network/interfaces** при помощи текстового редактора **nano** или **vi**.

3.4.5.2. Файл **/etc/network/interfaces** необходимо заполнить в соответствии спримером:

```
# 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
```

Сохранить изменения в файле, нажав сочетание клавиш **Ctrl+O**, и выйдти из текстового редактора **nano**, нажав сочетание клавиш **Ctrl+X**.

3.4.5.3. Для вступления настроек в силу необходимо перезагрузить КП «БАС-V» при помощи команды **sudo reboot**.

3.4.5.4. Для проверки вступления сетевых настроек в силу необходимо:

– выполнить команду **sudo ifconfig** в командной строке КП «БАС-V»;

– убедиться в том, что сетевые настройки применены.

3.4.6. Настройка даты и времени КП «БАС-V»

3.4.6.1. Для настройки даты и времени администратору необходимо выполнить следующие действия:

– осуществить подключение КП «БАС-V» и вход в операционную систему;

– установить (при необходимости) часовой пояс, в котором находится КП «БАС-V» (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 **sudo date MMDDhhmmCCYY.ss** в командную строку КП «БАС-V»,

где:

MM – текущий месяц;

DD – день месяца;

hh – часы;

mm – минуты;

CCYY – 4 цифры года;

ss – секунды;

– подать команду **sudo reboot** в командную строку для перезагрузки КП «БАС-V».

3.4.6.2. Также КП «БАС-V» 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 КП «БАС-V» 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 КП «БАС-V» в качестве эталонного NTP-сервера, например, для других КП «БАС-V», 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 данных серверу с самим собой, необходимо добавить:

restrict 127.0.0.1

restrict ::1

3.4.7. Управление ключевой информацией КП «БАС-V»

3.4.7.1. Для создания ключевой информации администратору необходимо:

– сгенерировать ключевую пару;

– экспортировать открытый ключ из КП «БАС-V»;

– выпустить сертификат открытого ключа;

– загрузить корневой сертификат и сертификат открытого ключа в КП «БАС-V».

3.4.7.2. Для генерации запроса на выпуск сертификата открытого ключа необходимо воспользоваться утилитой **RequestBuilder**. Она выполнит самотестирование КП «БАС-V», сгенерирует личный ключ и ключ его защиты, разделит ключ защиты на секреты и сформирует запрос на выпуск сертификата открытого ключа.

3.4.7.3. По умолчанию ключ защиты личного ключа делится на 2 секрета. При необходимости изменить число секретов или места их сохранения необходимо отредактировать настроечный файл **/etc/support/RequestBuilder.conf**.

В настроечном файле указываются следующие параметры:

– тип комплекса:

BasType = software;

– путь к файлу с данными комплекса:

PersonalData =/etc/support/PersonalData.xml;

– путь к шаблону катрочки открытого ключа:

CardTemplate =/etc/support/Templates/PublicKeyCardTemplate.rtf;

– путь к директории, в которую необходимо сохранить сформированный запрос на выпуск сертификата открытого ключа, карточку открытого ключа, и контейнер личного ключа:

OutputDirectory: «/etc/support/IssueRequestsAndCards/»;

– количество частичных секретов, на которое должен быть разделен ключ защиты контейнера с личным ключом. Значение должно быть не меньше 2 и не больше 16;

ShareSecretsAmount =2;

– пороговое число частичных секретов, из которых должен быть восстановлен ключ защиты контейнера с личным ключом. Значение должно быть не меньше 2 и не больше значения параметра **ShareSecretsAmount**:

Threshold =2;

– путь к директории, в которую необходимо сохранить N-ый частичный секрет:

ShareSecretPath_N =/etc/support/IssueRequestsAndCards/.

```
basv@basv:~$ sudo RequestBuilder
```

3.4.7.4. После выполнения самотестирования необходимо инициализировать датчик случайных числовых последовательностей. После чего необходимо отредактировать XML-файл с данными о комплексе, указав в нем серийный номер, название и адрес организации, где эксплуатируется и др.

Сохранить изменения в файле, нажав сочетание клавиш **Ctrl+O**, и выйти из текстового редактора **nano**, нажав сочетание клавиш **Ctrl+X**.

3.4.7.5. Установить пароль для доступа к контейнеру личного ключа.

В результате выполнения утилиты **RequestBuilder**, в папке, указанной в параметре **OutputDirectory**: файла **RequestBuilder.conf**. (по умолчанию **/etc/support/IssueRequestsAndCards/)** будут сформированы;

– запрос на выпуск сертификата в соответствии с СТБ 34.101.17;

– карточка открытого ключа в соответствии с СТБ 34.101.49:

– защищенный контейнер личного ключа;

– частичные секреты по путям, указанным в параметрах **ShareSecretPath_N**.

3.4.7.6. Для выпуска сертификата открытого ключа необходимо экспортировать запрос на выпуск сертификата из КП «БАС-V» любым удобным способом и передать администратору Удостоверяющего центра.

Для экспорта СОК можно воспользоваться съемным USB-носителем:

– подключить USB-носителем к КП «БАС-V»;

– определить имя, присвоенное съемному USB-носителю операционной системой КП «БАС-V» 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

3.4.7.7. После получения сертификатов открытого ключа из Удостоверяющего центра необходимо импортировать их в КП «БАС-V». Сертификат устройства в папку **/usr/local/etc/ipsec.d/certs/**, корневой сертификат, а также промежуточные (при их наличии), в **/usr/local/etc/ipsec.d/cacerts/**, список отозванных сертификатов в папку **/usr/local/etc/ipsec.d/crls/**.

Для импорта СОК можно воспользоваться съемным USB-носителем и способом описанным выше.

3.4.8. Настройка программного обеспечения

3.4.8.1. Настройка программного обеспечения КП «БАС-V» заключается в редактировании конфигурационных файлов. Основным конфигурационным файлом КП «БАС-V» является файл **ipsec.conf**, который содержит информацию о настройках программного обеспечения КП «БАС-V». Файл **ipsec.conf** расположен по пути **/usr/local/etc/ipsec.conf**.

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

3.4.8.2. 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.

3.4.8.3. Для настройки программного обеспечения КП «БАС-V» необходимо:

– подать в командную строку команду

sudo nano /usr/local/etc/ipsec.conf

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 «внештего» интерфейса КП «БАС-V»;

– изменить IP-адрес, установленный по умолчанию, на IP-адрес «внешнего» интерфейса;

– 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 Б (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 Б (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 выделенных аппаратных ресурсов для эксплуатации КП «БАС-V». Пример расчета приведен в Приложении А документа

«Комплекс программный реализации протоколов IPsec strongSwanCont. Руководство оператора» ВУ.СЮИК.00371-02 34 01.

Пропустить и не изменять параметры lifebytes и marginbytes. Они всегда должны принимать следующие значения для обеспечения высокого уровня гарантии алгоритма шифрования:

lifebytes = 11000000000000

marginbytes = 10000000000

– 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.

КП «БАС-V» 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 включения аутентификации с помощью протокола Диффи-Хеллмана используется значение "**pubkey**".

– 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. ВУ.СЮИК.00371-02 34 01».

3.4.8.4. 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 КП «БАС-V». Администратору рекомендуется повысить уровень журналирования при поиске проблем в настройках IPsec.

3.4.9. Настройка удаленного администрирования

3.4.9.1. КП «БАС-V» 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 КП «БАС-V» без предварительной преднастройки. Для этого необходимо знать только IP-адрес, который ваш DHCP-сервер присвоил КП «БАС-V».

3.4.9.2. КП «БАС-V» 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.

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

3.4.10. Проверка работоспособности

3.4.10.1. После проведения всех настроек необходимо перезагрузить КП «БАС-V».

3.4.10.2. Убедиться в том, что КП «БАС-V» подгрузил сертификат открытого ключа и сопоставило его с личным ключом, можно при помощи команды **ipsec listcerts**.

```
basv@basv:~$ sudo ipsec listcerts
```

О том, что КП «БАС-V» верно подгрузил сертификат открытого ключа и сопоставил его с личным ключом, свидетельствует запись **pubkey: BIGN 512 bits, has private key**.

3.4.10.3. Для проверки работоспособности соединения необходимо от пользователя, находящегося в защищаемой подсети (leftsubnet), выполнить **ping** пользователя, находящегося в удаленной защищаемой подсети (rightsubnet).

```
C:\Documents and Settings\Администратор>ping 10.10.10.10

Обмен пакетами с 10.10.10.10 по 32 байт:

Ответ от 10.10.10.10: число байт=32 время<1мс TTL=64
Ответ от 10.10.10.10: число байт=32 время<1мс TTL=64
Ответ от 10.10.10.10: число байт=32 время<1мс TTL=64
Ответ от 10.10.10.10: число байт=32 время<1мс TTL=64

Статистика Ping для 10.10.10.10:
    Пакетов: отправлено = 4, получено = 4, потеряно = 0 (0% потерь),
Приблизительное время приема-передачи в мс:
    Минимальное = 0мсек, Максимальное = 0 мсек, Среднее = 0 мсек
```

3.4.10.4. Убедиться в том, что передача данных идет по защищенному туннелю, можно, подав команду **ipsec statusall** в командную строку КП «БАС-V».

```
basv@basv:~$ sudo ipsec statusall
```

После чего будет доступна статистика туннеля. В последних двух строках статистики предоставляются параметры туннеля (конечные адреса, используемые криптографические алгоритмы, количество переданной информации).

Убедиться в том, что в туннеле используются заданные криптографические алгоритмы и по туннелю передано 4 пакета в каждую сторону (пакеты ping).

3.5 Эксплуатация КП «БАС-V»

3.5.1. В процессе эксплуатации возможны три основных состояния КП «БАС-V»:

– нормальная работа;

– ошибка;

– администрирование.

3.5.2. Нормальная работа КП «БАС-V» не предполагает непосредственного взаимодействия с администратором.

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

3.5.4. В процессе работы КП «БАС-V» производит проверку своей работоспособности при включении и по запросу администратора.

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

3.5.6. Для проверки работоспособности КП «БАС-V» администратору необходимо:

– подать команду **sudo basctl** в командную строку КП «БАС-V»;

– результат проверки выводится в командную строку.

3.5.7. 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.

3.5.8. Администратор осуществляет периодическую смену ключевой информации. Процедура генерации пары ключей описана в п. 3.4.5.

3.5.9. При необходимости администратор может сменить используемый криптонабор на КП «БАС-V». Процедура смены криптонабора описана в п. 3.4.8. После смены криптонабора необходимо перезапустить КП «БАС-V», подав в командную строку устройства команду **sudo ipsec restart**.

3.5.10. В случае смены криптонабора на КП «БАС-V» администратор должен установить соответствующий криптонабор на удаленном ПАК «БАС» ил КП «БАС-V».

3.5.11. КП «БАС-V» ведет журнал аудита, в который заносится следующая информация:

– дата и время;

– вызываемая функция;

– идентификационные данные пользователя;

– результат (успешно/неуспешно).

3.5.12. Контроль системного журнала осуществляет администратор.

3.5.13 Для получения доступа к системному журналу КП «БАС-V» администратору необходимо подать в командную строку команду **cat /var/log/syslog**.

3.6. Вывод КП «БАС-V» из эксплуатации

3.6.1. Вывод КП «БАС-V» из эксплуатации осуществляется администратором. На этапе вывода из эксплуатации необходимо удалить все ключи и частичные секреты, хранящиеся в памяти КП «БАС-V».

4. СООБЩЕНИЯ ОПЕРАТОРУ

КП «БАС-V» выводит сообщения в системный журнал Linux. Сообщения четко описывают причину их появления и не нуждаются в разъяснении. Сообщения об ошибках формируются криптографической библиотекой. Список возможных ошибок приведен в документе «Библиотека криптографических преобразований CONTACTCRYPTO32LE. Руководство программиста» BY СЮИК.00365-04 33 01.

ПРИЛОЖЕНИЕ А

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 программный виртуальный
			криптографической защиты информации "БАС-V"
		</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="Идентификатор 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 Б

СПИСОК ОБОЗНАЧЕНИЙ ДОСТУПНЫХ КРИПТОГРАФИЧЕСКИХ АЛГОРИТМОВ

Таблица Б 1 – Список обозначений доступных алгоритмов шифрования 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 Б 1.

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

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

ПРИЛОЖЕНИЕ В

ПРИМЕР НАСТРОЕЧНОГО ФАЙЛА IPSEC.CONF КП «БАС-V»

```
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-V_Server.cer
        leftauth = eap-bsts
        keyingtries = %forever
        auto = start

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

ПРИЛОЖЕНИЕ Г

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 = 3m
        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 = 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
```

ПРИЛОЖЕНИЕ Д

ПЕРЕЧЕНЬ СОКРАЩЕНИЙ

В настоящем документе приняты следующие сокращения:

ОС – операционная система

ПЗУ – постоянное запоминающее устройство

ПО – программное обеспечение

ПЭВМ – персональная электронно-вычислительная машина

СОК – сертификат открытого ключа

ЭЦП – электронная цифровая подпись

Лист регистрации изменений

Изм.	Номера листов (страниц)				Всего листов (страниц) в докум.	№ документа	Входящий № сопроводительного докум. и дата	Подп.	Дата
	измененных	замененных	новых	аннулированных					