Программное обеспечение
«VPN/FW «ЗАСТАВА-Офис», версия 8»

Руководство администратора

2024

ОГЛАВЛЕНИЕ

1 ВВЕДЕНИЕ 6

1.1 Назначение 6
1.2 Требования к уровню подготовки персонала 6
1.3 Типографские соглашения 6

2 ОБЩИЕ СВЕДЕНИЯ 8

2.1 Варианты использования 8
2.2 Минимальные аппаратные требования 8
2.3 Требования к персональным идентификаторам 9

3 УСТАНОВКА ПО 10

3.1 Входной контроль комплектующих изделий 10
3.2 Порядок установки ПО «VPN/FW «ЗАСТАВА-Офис», версия 8 КС1 10
3.3 Порядок установки ПО «VPN/FW «ЗАСТАВА-Офис», версия 8 КС3 12
3.4 Проверка корректности и завершение установки 14

4 ПОДГОТОВКА К РАБОТЕ И БЫСТРЫЙ СТАРТ 15

4.1 Вход в ПО 15
4.2 Проверка контрольной суммы 15
4.3 Смена пароля Администратора 16
4.4 Настройка сетевых параметров 16
4.4.1 Настройка адресации 17
4.4.2 Настройка маршрутизации 17
4.4.3 Настройка DNS 17
4.4.4 Применение настроек 17
4.4.5 Настройка в режиме пользовательского псевдографического интерфейса 18
4.4.6 Назначение псевдонимов для сетевых интерфейсов 22
4.5 Расширенные настройки сети 23
4.5.1 Настройка автоматической синхронизации системного времени (NTP) 23
4.5.2 Настройка удаленной регистрации событий (SYSLOG) 25
4.5.3 Настройка мониторинга (SNMP) 25
4.5.4 Настройка PROXY HTTP 26
4.5.5 Настройка DHCP-сервера 26
4.6 Включение двухфакторной аутентификации 27
4.7 Конфигурирование программного обеспечения «ЗАСТАВА-Управление» 28

5 ОПИСАНИЕ СРЕДСТВ КОНФИГУРИРОВАНИЯ И МОНИТОРИНГА 30

6 ОПИСАНИЕ ДОСТУПНЫХ ОПЕРАЦИЙ ИНТЕРПРЕТАТОРА KLISH 32

6.1 Назначение интерпретатора KLISH 32
6.2 Негрупповые команды 32
6.3 Команда смены пароля 33
6.4 Команды просмотра настроек 33
6.5 Команды выполнения настроек 35
6.6 Команды для диагностики состояния сетевого соединения 39
6.7 Резервирование и восстановление данных 41

7 ОПИСАНИЕ ДОСТУПНЫХ ОПЕРАЦИЙ ИНТЕРПРЕТАТОРА BASH 42

7.1 Обзор средств мониторинга 42

7.1.1 Файл регистрации системных событий ... *42*
7.1.1.1 Упорядочение и сортировка событий ... 42
7.1.1.2 Очистка файла регистрации системных событий ... 43
7.1.2 Утилита vpnmonitor ... *43*
7.1.2.1 Справочная система по работе с утилитой ... 43
7.1.2.2 Просмотр статистики ... 44
7.1.2.3 Вывод информации об активированной политике ... 48
7.1.2.4 Просмотр информации о созданных IKE/IPSec SA ... 49
7.1.2.5 Фильтрация фильтров и созданных SA по параметрам ... 50
7.1.2.6 Команды применимые к отфильтрованным SA ... 55
7.1.2.7 Просмотр списка фильтров ... 56
7.1.2.8 Просмотр статистики ike-cfg ... 59
7.1.2.9 Просмотр статистики RRI ... 60
7.1.3 Утилита tcping ... *60*
7.1.4 Утилита arping ... *61*
7.2 Обзор средств конфигурирования ... 61
7.2.1 Утилита vpnconfig ... *61*
7.2.1.1 Справочная система по работе с утилитой ... 61
7.2.1.2 Просмотр информации о ПО ... 62
7.2.1.3 Работа с сертификатами и ключами ... 62
7.2.1.3.1 Свойства сертификата и его проверка ... 62
7.2.1.3.2 Регистрация сертификата ... 63
7.2.1.3.3 Удаление сертификата ... 65
7.2.1.3.4 Создание запроса PKCS10 на выпуск сертификата ... 65
7.2.1.3.5 Настройки функции двухфакторной аутентификации ... 69
7.2.1.3.6 Предварительно распределенные ключи ... 70
7.2.1.3.7 Списки отозванных сертификатов ... 70
7.2.1.3.8 Импортирование СОС вручную ... 71
7.2.1.4 Работа с настройками ЛПБ ... 71
7.2.1.4.1 Настройка параметров политик ПО ... 71
7.2.1.4.2 Использование в качестве прогрузчика ... 73
7.2.1.4.3 Активация ЛПБ ... 73
7.2.1.4.4 Просмотр текущей ЛПБ ... 73
7.2.1.5 Файл регистрации событий ... 74
7.2.1.6 Параметры журнала Syslog ... 76
7.2.1.7 Протокол IKE ... 77
7.2.1.7.1 Параметры протокола IKE ... 77
7.2.1.7.2 Маршрутизация IKE-CFG ... 83
7.2.1.7.3 RRI ... 83
7.2.1.7.4 Описание режимов обработки CRL ... 84
7.2.1.7.5 Политика выбора метода работы через NAT ... 85
7.2.1.8 Токены ... 86
7.2.1.8.1 Просмотр модулей токенов ... 86
7.2.1.8.2 Добавление модулей токенов ... 86
7.2.1.8.3 Удаление модуля токена ... 86
7.2.1.8.4 Аутентификация на токене ... 87
7.2.1.8.5 Смена PIN-кода токена ... 87
7.2.1.9 Настройка псевдонимов сетевых интерфейсов ... 87
7.2.2 Утилита icv_checker ... *88*
7.2.3 Использование команд программной составляющей и конфигурирование модулей ... *89*
7.2.3.1 Работа с системными журналами программной составляющей ПО ... 89
7.2.3.2 Конфигурирование модуля vpnpcap ... 89

7.3 Доступные сетевые службы ... 91
8 ОПИСАНИЕ КОНФИГУРИРОВАНИЯ В КЛАСТЕРНОМ ИСПОЛНЕНИИ ... 93
8.1 Настройка кластера с помощью мастера ... 94
8.1.1 Меню мастера настройки кластера ... 94
8.1.1.1 Пункт 1 (настройка keepalive) ... 95
8.1.1.2 Пункт 2 (настройка ПО в части кластеризации) ... 96
8.1.1.3 Пункт 3 (применение настроек) ... 97
8.1.1.4 Пункт 4 (передача настроек на другой узел) ... 98
8.1.1.5 Пункт 5 (просмотр текущих настроек) ... 99
8.1.1.6 Пункт 69 (очистка всех настроек) ... 99
8.1.1.7 Пункт 6 (выход) ... 99
8.2 Настройка кластера вручную ... 100
8.2.1 Ручное редактирование файлов конфигурации ... 100
8.2.2 Настройка синхронизации состояний IKEv2 ... 104
8.3 Настройка маршрутизации при работе с кластером ... 105
9 ОПИСАНИЕ КОНФИГУРИРОВАНИЯ L2TP СОЕДИНЕНИЯ ... 106
9.1 Создание нового соединения ... 106
9.2 Просмотр созданных соединений ... 108
9.3 Удаление соединения ... 108
9.4 Запуск соединений в соответствии с настройками ... 109
10 РАБОТА С ДИНАМИЧЕСКОЙ МАРШРУТИЗАЦИЕЙ ... 111
10.1 Работа с BGP ... 111
10.1.1 Конфигурация стенда ... 111
10.1.2 Состав ПО участников стенда ... 111
10.1.3 Настройка конфигурации ... 112
10.1.3.1 Настройки узла ISP_1 ... 112
10.1.3.2 Настройки узла ISP_2 ... 112
10.1.3.3 Настройки узла ZASTAVA-1 ... 113
10.1.3.4 Настройки узла ZASTAVA-2 ... 114
10.1.4 Проверка правильности настройки стенда ... 115
10.1.5 Настройка правил шифрования ... 116
10.1.6 Проверка работоспособности решения ... 117
10.2 Работа с OSPF ... 118
10.2.1 Конфигурация стенда ... 118
10.2.2 Состав ПО участников стенда ... 119
10.2.3 Настройка конфигурации ... 119
10.2.3.1 Настройки узла ISP_1 ... 119
10.2.3.2 Настройки узла ISP_2 ... 120
10.2.3.3 Настройки узла ZASTAVA-1 ... 121
10.2.3.4 Настройки узла ZASTAVA-2 ... 122
10.2.4 Проверка правильности настройки стенда ... 122
10.2.5 Настройка правил шифрования ... 123
10.2.6 Проверка работоспособности решения ... 124
11 ОБНОВЛЕНИЕ ... 127
11.1 Регламент обновления ... 127
11.1.1 Процедуры получения обновления ... 127
11.1.2 Процедуры контроля целостности обновления ... 127
11.1.3 Типовые процедуры тестирования обновления ... 127

11.1.4 Процедуры установки и применения обновления 128
11.2 Получение обновления с ПО «ЗАСТАВА-Управление» 128
12 НЕШТАТНЫЕ СИТУАЦИИ 130
12.1 Некорректная работа ПО после обновления 130
12.2 Возврат к эталону 130
12.3 Нарушение целостности образа 130
12.4 Компрометация ключей аутентификации 131
13 ВОЗМОЖНЫЕ НЕИСПРАВНОСТИ И СПОСОБЫ ИХ УСТРАНЕНИЯ 132
ПЕРЕЧЕНЬ ПРИНЯТЫХ ТЕРМИНОВ И СОКРАЩЕНИЙ 136
ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ 138

1 ВВЕДЕНИЕ

Настоящий документ предназначен для администратора Программного обеспечения «VPN/FW «ЗАСТАВА-Офис», версия 8» (далее – ПО) и содержит описание ПО, описание интерфейса ПО, процедур, выполняемых администратором в процессе подготовки ПО к работе, доступных операций, действий при возникновении нештатных ситуаций.

1.1 Назначение

ПО предназначено для защиты корпоративных вычислительных ресурсов на сетевом уровне модели взаимодействия OSI/ISO (стек протоколов TCP/IP) с использованием технологий VPN на основе интернет-протоколов семейства IKEv2/IPSec.

ПО обеспечивает защиту информации конфиденциального характера, не содержащей сведений, составляющих государственную тайну: сведений для служебного пользования, персональных данных, сведений, составляющих коммерческую, банковскую тайну, и других видов конфиденциальной информации.

1.2 Требования к уровню подготовки персонала

Уровень подготовки обслуживающего персонала должен удовлетворять следующим требованиям:

– техническое образование в области информационных технологий;

– знание команд и командного языка Linux;

– знание положений настоящего руководства и эксплуатационной документации, входящей в комплект поставки;

– выполнение настройки и эксплуатации ПО в соответствии с эксплуатационной документацией.

Администратор ПО должен знать основы администрирования локальных сетей.

1.3 Типографские соглашения

Полужирный шрифт	Полужирный шрифт используется для выделения названий меню, вкладок, кнопок, полей, объектов политики, строк контекстного меню, а также для визуального выделения.
Курсив	*Курсив* используется, чтобы выделить названия файлов. Курсив также может использоваться для смыслового акцента.

«Кавычки»	Текст, заключенный в кавычки, используется для названий элементов интерфейса.
`Непропорциональный`	Непропорциональный шрифт используется для ссылок на системные папки и каталоги, команд в интерфейсе командной строки.
<Угловые скобки>	Угловые скобки используются в названиях клавиш на клавиатуре компьютера, а также в описаниях параметров.

2 ОБЩИЕ СВЕДЕНИЯ

2.1 Варианты использования

2.2.1. В зависимости от требований по уровню защиты СКЗИ (КС1 или КС3) ПО «VPN/FW «ЗАСТАВА-Офис», версия 8» может применяться в качестве:

- Программного обеспечения «VPN/FW «ЗАСТАВА-Офис», версия 8 КС1;
- Программного обеспечения «VPN/FW «ЗАСТАВА-Офис», версия 8 КС3.

2.2.2. В случае применения «VPN/FW «ЗАСТАВА-Офис», версия 8» в системах, где необходимо обеспечить уровень защиты СКЗИ класса КС3 («Программное обеспечение «VPN/FW «ЗАСТАВА-Офис», версия 8 КС3»), СВТ, на котором устанавливается ПО, должно быть укомплектовано аппаратно-программным модулем доверенной загрузки (АПМДЗ), прошедшим оценку соответствия ФСБ России.

2.2 Минимальные аппаратные требования

СВТ, на котором устанавливается ПО, должно удовлетворять следующим требованиям:

- процессор архитектуры Intel 64 не менее 4 ядер с тактовой частотой не менее 2 ГГц;
- ОЗУ - не менее 4 Гбайт;
- внутренний накопитель - не менее 32 Гбайт;
- не менее двух, а для кластерного исполнения - не менее трёх сетевых интерфейсов GbE/SFP/SFP+;
- BIOS с поддержкой Compatibility Support Module (CSM);
- один свободный порт PCI-E / Mini PCI-E / PCI;
- не менее двух USB портов.

СВТ, на котором устанавливается ПО в исполнении «Программное обеспечение «VPN/FW «ЗАСТАВА-Офис», версия 8 КС3», должно быть укомплектовано аппаратно-программным модулем доверенной загрузки (АПМДЗ), прошедшим оценку сообветствия ФСБ России.

Допускается эксплуатация ПО в виде виртуальных машин при использовании средств виртуализации, для которых обеспечена защита от несанкционированного доступа к серверам виртуальных машин и средствам управления инфраструктуры.

2.3 Требования к персональным идентификаторам

В ПО в качестве персонального идентификатора используются функциональные ключевые носители в виде USB-токена: ESMART Token ГОСТ (форм-фактор USB) и Рутокен ЭЦП 3.0 (форм-фактор USB).

Персональный идентификатор пользователя должен содержать цифровой сертификат, содержащий следующие поля:

— Extended Key Usage (EKU), включающее в себя OID=Smart Card Logon;

— User Principal Name (UPN), равное [admin|user]@localhost].

Роль пользователя определяется на основании поля UPN в предъявленном на персональном идентификаторе цифровом сертификате. Значение admin@localhost соответствует Администратору ПК, user@localhost – Оператору ПО.

Перед использованием Рутокен ЭЦП 2.0/3.0 (форм-фактор USB) необходимо сменить заводской PIN-код персонального идентификатора средствами производителя персонального идентификатора.

3 УСТАНОВКА ПО

3.1 Входной контроль комплектующих изделий

Входной контроль включает в себя последовательность следующих действий:

1) проверку комплектации согласно комплекту поставки и поставочной спецификации;
2) подготовку установочного USB-носителя;
3) проверку целостности дистрибутива ПО.

	Проверка целостности подразумевает подсчёт КС трёх файлов на установочном USB-flash носителе, расположенных по относительным путям: – `SPECOS\bzImage;` – `SPECOS\LIVE_IMAGE\rootfs.squashfs;` – `SPECOS\INITRD_IMAGE\rootfs.cpio.gz.`
	Проверка контрольных сумм может быть осуществлена на отдельном АРМ с ОС Windows, который оснащён антивирусным ПО с обновлёнными базами вирусов. Для вычисления КС можно использовать: – утилиту подсчета КС (icv_writer) из состава поставки, расположенную в корне поставочного CD/DVD-диска. Формат команды: `icv_writer.exe -F=<путь к файлу>` – при наличии на АРМ с ПО КриптоПро CSP утилиту cpverify. Формат команды: `cpverify.exe -mk <путь к файлу\имя файла> -alg GR3411_2012_256.`
	Вычисленные значения должны совпадать со значениями, указанными в таблице 3 раздела 5 Формуляра. КС файла `rootfs.squashfs` должна соответствовать КС файла `LIVE`. КС файла `rootfs.cpio.gz` должна соответствовать КС файлу `initrd`. КС файла `rootfs.squashfs` должна соответствовать КС файла `bzImage`.
	USB-носитель должен быть предварительно отформатирован.

3.2 Подготовка установочного USB-носителя

USB-носитель должен отвечать следующим характеристикам:

— объем не менее 8 ГБ;

— поддержка стандартов USB 2.0 и/или 3.0.

Для того что бы подготовить USB-носитель, необходимо:

— отформатировать USB-носитель, создав файловую систему FAT32;

— скопировать содержимое архива ZASTAVA-Office_<версия> в корень USB-носителя;

— открыть терминал cmd (Win+R «Выполнить», cmd);

— выполнить смену рабочего каталога командой *cd* указав букву USB-носителя, как он определился в системе (например, *cd E:*);

— перейти в рабочий каталог, введя букву из предыдущего шага;

— выполнить команду, расположенную по пути *utils\win32\makeboot.bat;*

— нажать клавишу Enter и затем еще раз клавишу Enter;

— дождаться сообщения об окончании выполнения команды, затем закрыть окно cmd;

— безопасно извлечь USB-носитель.

3.3 Порядок установки ПО «VPN/FW «ЗАСТАВА-Офис», версия 8 КС1

Разворачивание ПО включает в себя следующие действия:

1) В соответствии с эксплуатационной документацией на аппаратную платформу подключить монитор и клавиатуру к системному блоку.
2) В соответствии с эксплуатационной документацией на аппаратную платформу подключить аппаратную платформу к сети электропитания. Включить аппаратную платформу.
3) Войти в BIOS. Произвести настройку для загрузки ОС с внешнего USB-накопителя.
4) Установить подготовленный установочный USB-накопитель в USB-разъём аппаратной платформы. Сохранить настройки BIOS и перезагрузить платформу. Начнётся загрузка образа ПО с установочного USB-накопителя.
5) В процедуре установки выбрать пункт **ZASTAVA-Office firmware install**.
6) В процессе автоматической установки на монитор будет выводится информация о процессе размещения образа на внутреннем накопителе аппаратной платформы. При появлении надписи **Install complete** аппаратная платформа автоматически перезагрузится.
7) Извлечь USB-накопитель. В BIOS перенастроить порядок загрузки, если это необходимо.

По умолчанию в ZASTAVA-Office создаются две учётные записи:
- `admin` (пароль по умолчанию `admin`);
- `user` (пароль по умолчанию `user`).

По окончанию процедуры установки ПО пароли для учётных записей должны быть изменены Администратором ПО.

3.4 Порядок установки ПО «VPN/FW «ЗАСТАВА-Офис», версия 8 КС3

Разворачивание ПО включает в себя следующие действия:

1) В соответствии с эксплуатационной документацией на аппаратную платформу открыть корпус системного блока аппаратной платформы для установки АПМДЗ.
2) В соответствии с эксплуатационной документацией на АПМДЗ установить АПМДЗ в разъём аппаратной платформы (в зависимости от форм-фактора PCI-E / Mini PCIE / PCI). Закрыть корпус аппаратной платформы.
3) Подключить монитор и клавиатуру к системному блоку согласно эксплуатационной документации.
4) В соответствии с эксплуатационной документацией на аппаратную платформу подключить аппаратную платформу к сети электропитания. Включить аппаратную платформу.
5) Войти в BIOS. Произвести настройку на загрузку ОС с внешнего USB-накопителя.
6) Установить подготовленный установочный USB-накопитель в USB-разъём аппаратной платформы. Сохранить настройки BIOS и перезагрузить платформу. Начнётся загрузка образа ПАК с установочного USB-накопителя.
7) В процедуре установки выбрать пункт **ZASTAVA-Office firmware install**.
8) В процессе автоматической установки на монитор будет выводится информация о процессе размещения образа на внутреннем накопителе аппаратной платформы. При появлении надписи **Install complete** аппаратная платформа автоматически перезагрузится.
9) Извлечь USB накопитель. В BIOS перенастроить порядок загрузки, если это необходимо. Включить режим CSM и установить режим загрузки **Legacy** для возможности перехвата загрузки АПМДЗ.

Установка режима загрузки **Legacy** у каждой реализации BIOS может отличаться. Для включения режима следует ознакомится с документацией на аппаратную платформу.

10) Произвести инициализацию АПМДЗ в соответствии с общим порядком, изложенным в эксплуатационной документации на АПМДЗ.

11) Опциональный шаг для необслуживаемого режима эксплуатации. В АПМДЗ требуется создание пользователя **autoload** и настройка автоматического входа в АПМДЗ.
12) Пройти аутентификацию на АПМДЗ, загрузиться в ZASTAVA-Office, используя пункт меню «ZASTAVA-Office», и пройти аутентификацию на пароле по умолчанию.

По умолчанию в ZASTAVA-Office создаются две учётные записи:
- `admin` (пароль по умолчанию `admin`);
- `user` (пароль по умолчанию `user`).

По окончанию процедуры установки ПО пароли для учётных записей должны быть изменены Администратором ПО.

3.5 Проверка корректности и завершение установки

Для завершения установки выполнить следующие действия:

1) в меню загрузчика выбрать пункт «`Checksum test`». Дождаться подсчёта КС, вычисленные значения должны совпадать со значениями, указанными в таблице 3 раздела 5 Формуляра.
2) выключить аппаратную платформу. Установка и инициализация ПО завершена.

4 ПОДГОТОВКА К РАБОТЕ И БЫСТРЫЙ СТАРТ

4.1 Вход в ПО

В ПО реализованы два режима функции идентификации и аутентификации:

— однофакторная идентификация и аутентификация (включена по умолчанию);

— двухфакторная идентификация и аутентификация.

При включенном режиме однофакторной идентификации и аутентификации идентификация и аутентификация Администратора ПО (имя пользователя - admin) и Оператора ПО (имя пользователя - user) осуществляется на основании введенного логина и пароля.

При включенном режиме двухфакторной идентификации и аутентификации идентификация и аутентификация Администратора ПО и Оператора ПО осуществляется на основании цифрового сертификата, хранящегося на персональном идентификаторе предъявленного PIN-кода. Требования к персональным идентификаторам приведены в подразделе 2.3.

	Имена пользователей зафиксированы в образе ПО. Перед началом использования ПО требуется сменить пароли предустановленных пользователей.
	После ввода PIN-кода не допускается оставлять ключевой носитель без контроля, в том числе при уходе с рабочего места.
	Включение режима двухфакторной аутентификации является обязательным!

Для включения режима двухфакторной идентификации и аутентификации необходимо выполнить команду:

```
enable
set 2nd_factor_authorization ESMART/RuToken
```

4.2 Проверка контрольной суммы

При первом включении необходимо проверить КС образа ПО.

Процедура проверки КС:

1) после включения ПО дождаться появления меню загрузчика;
2) выбрать пункт меню «Checksum test» и нажать клавишу <Enter>;

3) на экране появится сообщение о проверке КС образа ПО. Дождаться окончания проверки;

4) по окончании проверки на экране появится сообщение с вычисленной КС, которое будет также содержать сообщение о соответствии/несоответствии вычисленной КС с эталонной. Сверить вычисленную КС с указанной в Формуляре;

5) выключить СВТ, нажав кнопку питания;

6) включить СВТ, дождаться загрузки;

7) по окончании проверки выведется сообщение о вычисленных КС, а также о их соответствии/несоответствии эталонным значениям. Сверить вычисленные КС с указанными в формуляре.

4.3 Смена пароля Администратора

Для смены пароля для текущей учётной записи ввести команду:

```
> password
```

Далее выполнить шаги в соответствии с отображаемыми подсказками. В случае успешно выполненной замены пароля на новый будет отображено соответствующее сообщение:

passwd: пароль успешно обновлён

В случае, если введённые новые пароли не совпадают, будет отображено сообщение:

Извините, но пароли не совпадают.

passwd: Службе паролей не удалось выполнить предварительную проверку.

passwd: Пароль не изменён

В случае введения нового пароля, равного текущему, будет отображено сообщение:

passwd: Пароль не изменён

4.4 Настройка сетевых параметров

Настройка сетевых параметров включает настройку IP-адреса, DNS, NTP и, при необходимости, настройку таблицы маршрутизации.

Настройка сетевых параметров выполняется в командной оболочке KLISH. Для перехода в режим администрирования KLISH требуется войти с использованием данных учётной записи admin и выполнить команду:

```
> enable
```

4.4.1 Настройка адресации

Для настройки статического адреса необходимо выполнить следующие команды:

network connection add type ethernet con-name <название соединения> ifname <название физического интерфейса>

network connection modify <название соединения> ipv4.addresses <ip адрес/маска>

network connection modify <название соединения> ipv4.method manual

network connection modify <название соединения> autoconnect yes

Для настройки получения адреса по DHCP необходимо выбрать **ipv4.method –auto** без задания параметра **ipv4.addresses <ip адрес/маска>.**

4.4.2 Настройка маршрутизации

Для задания параметров маршрутизации необходимо выполнить команду:

network connection modify <название соединения> +ipv4.routes <ip-адрес/маска> <ip-адрес шлюза>

Для задания адреса шлюза по умолчанию необходимо выполнить команду:

network connection modify <название соединения> ipv4.gateway <ip-адрес>.

4.4.3 Настройка DNS

Для добавления DNS-сервера необходимо выполнить команду:

network connection modify <название соединения> +ipv4.dns <IP адрес>

Для удаления DNS-сервера необходимо выполнить команду:

network connection modify <название соединения> -ipv4.dns <IP адрес>

4.4.4 Применение настроек

Для применения заданных настроек необходимо выполнить команду:

network connection up <название соединения>

4.4.5 Настройка в режиме пользовательского псевдографического интерфейса

Для базовой настройки сетевых параметров необходимо использовать псевдографическую утилиту nmtui. Для запуска утилиты nmtui в оболочке KLISH необходимо выполнить команду:

```
network nmtui
```

При запуске утилиты будут предложены варианты действий, см. рис.1.

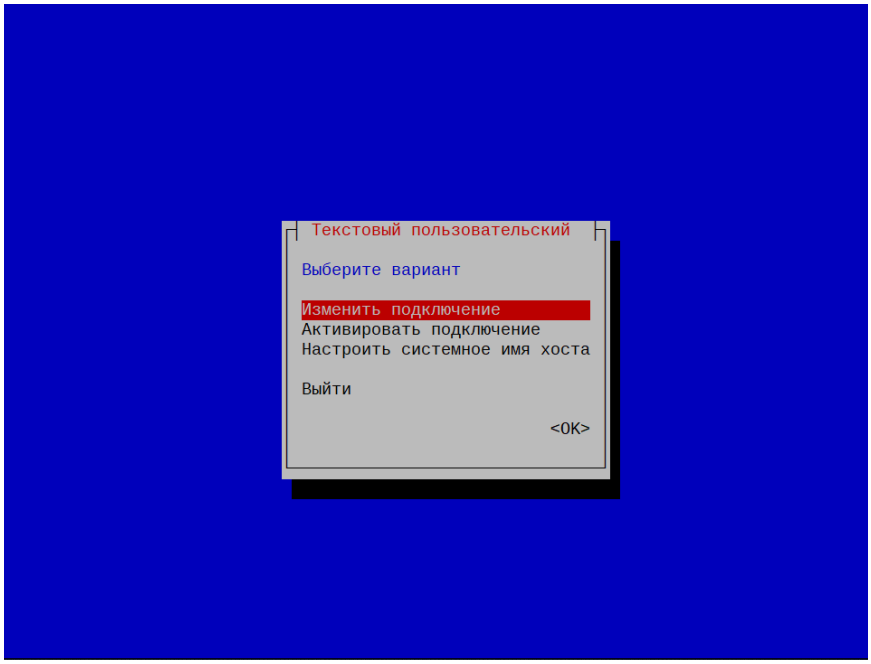

Рисунок 1 - Главное окно утилиты nmtui

При выборе «Изменить подключение» у администратора ПО есть возможности:

1) добавить, изменить, удалить подключения (см. рис. 2);
2) задать имя, IP-адрес:маску, шлюз по умолчанию, сервер разрешения имён (рис. 3, рис. 4);
3) добавить и удалить статические маршруты (см. рис. 5, рис. 6);
4) отобразить свойства подключения (см. рис. 7)

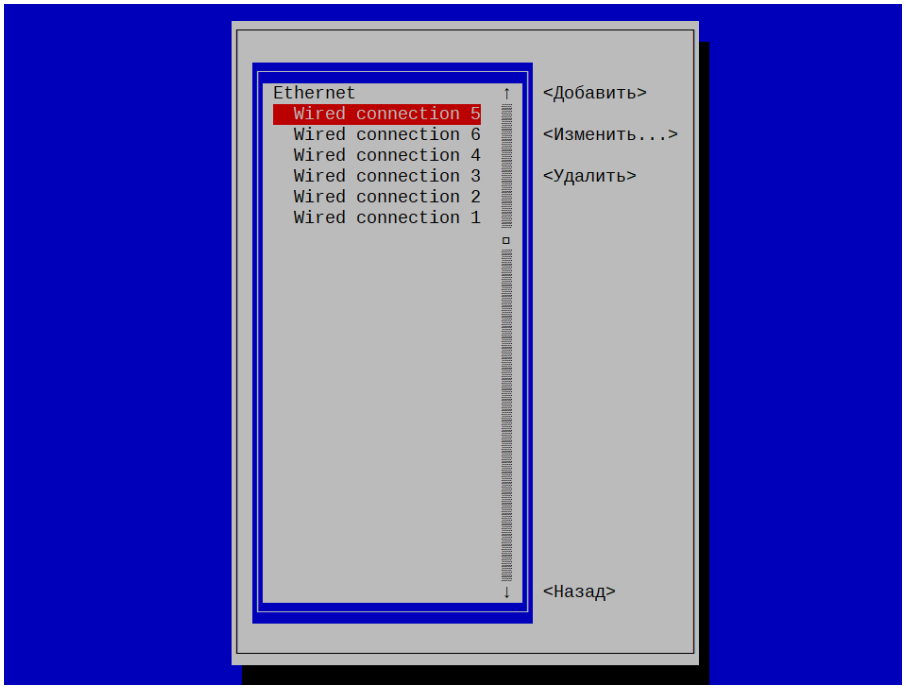

Рисунок 2 - Перечень соединений

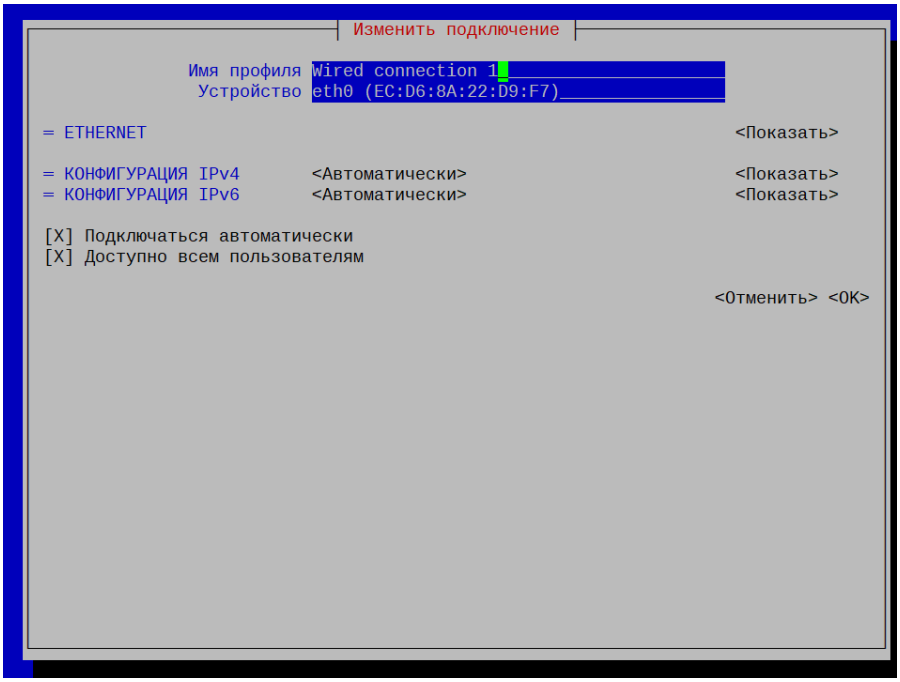

Рисунок 3 – Редактирование имени подключения

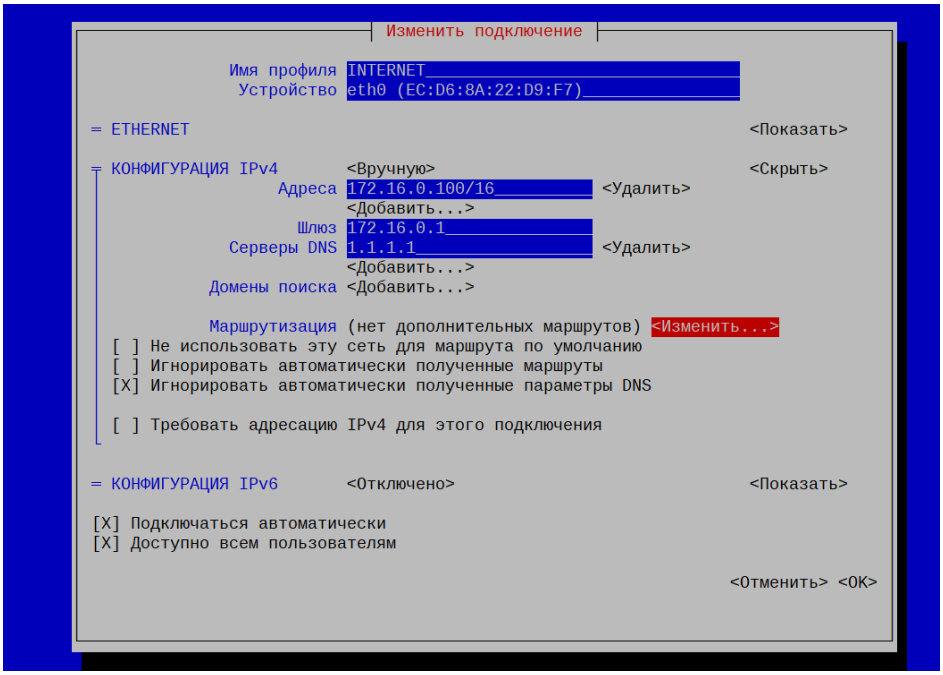

Рисунок 4 – Задание IP-адреса

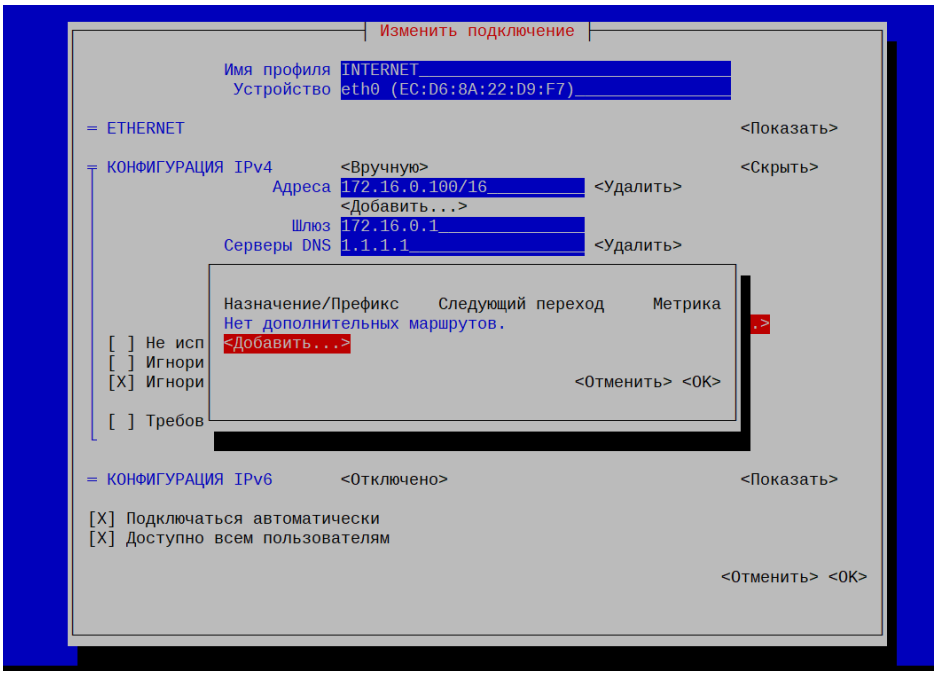

Рисунок 5 – Добавление статического маршрута

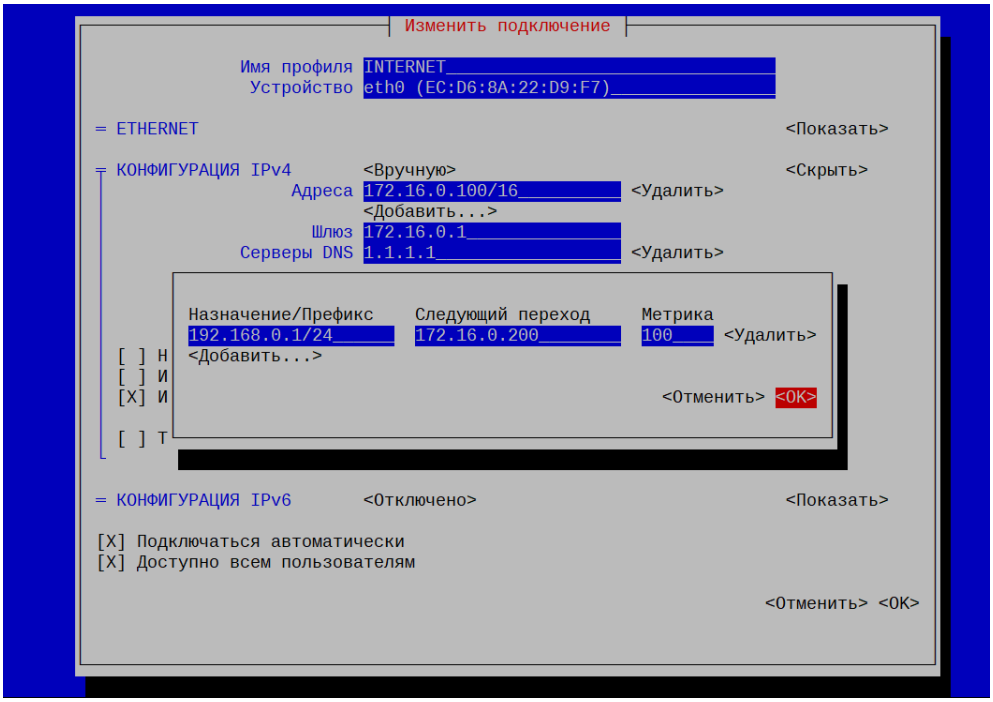

Рисунок 6 - Отображение статического маршрута

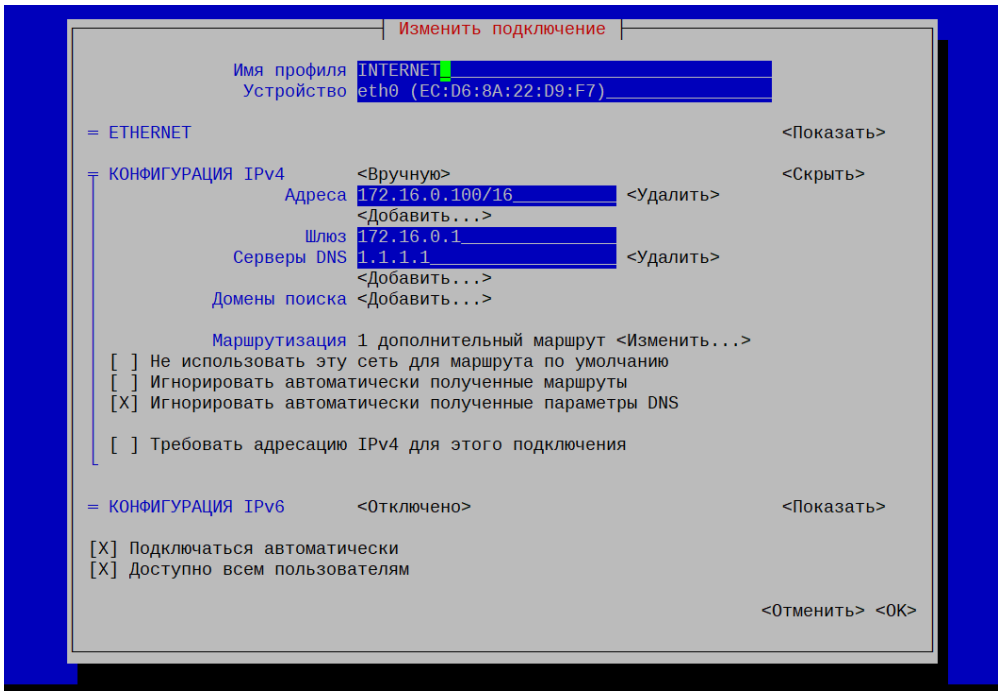

Рисунок 7 – Итоговые настройки соединения

Для применения изменений необходимо выбрать активируемое соединение и последовательно произвести действия: «Отключить» → «Включить» (см. рис. 8).

При отключении подключения через удалённый терминал по протоколу SSH произойдёт разрыв соединения. Включение подключения будет возможно локально.

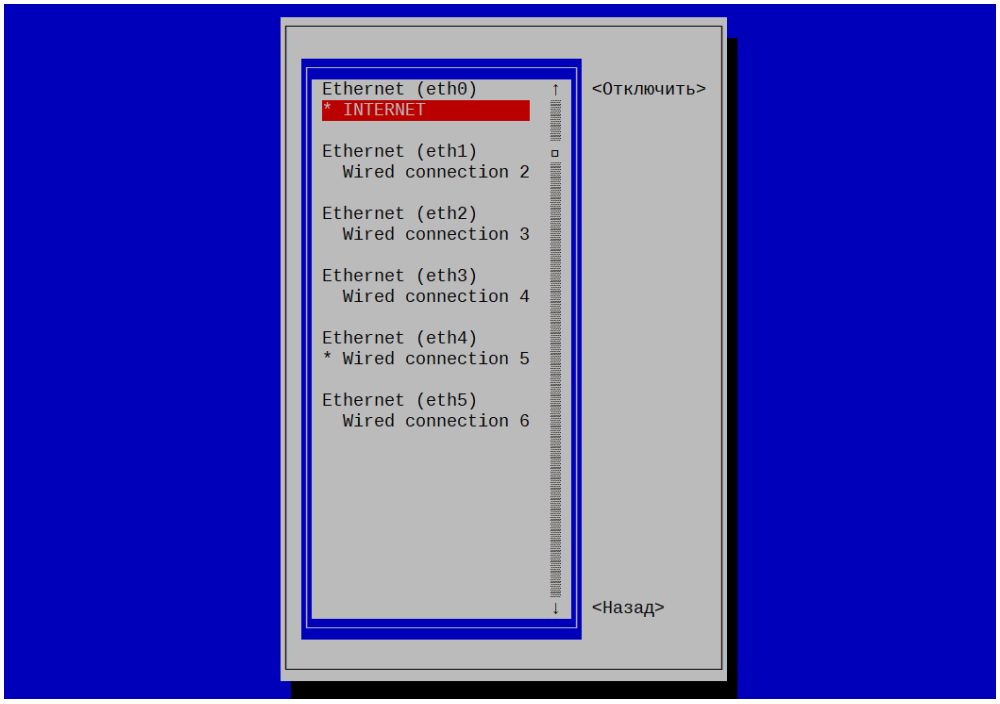

Рисунок 8 – Применение настроек подключения

Утилита позволяет переименовать ПО. Настройки применяются после перезагрузки СВТ (см. рис. Рисунок 9).

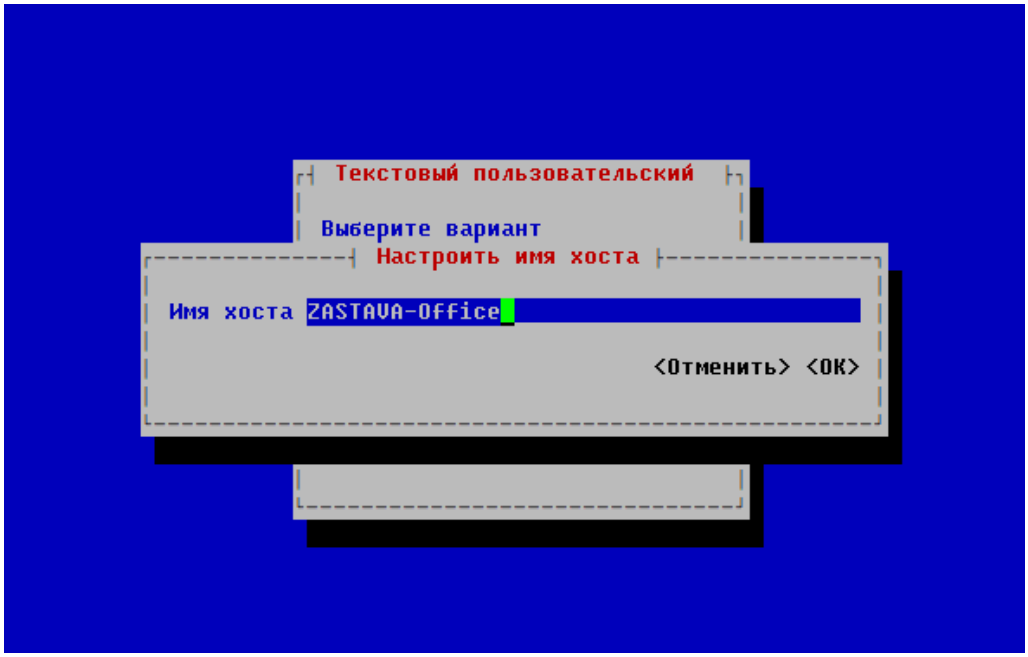

Рисунок 9 – Задание имени хоста

4.4.6 Назначение псевдонимов для сетевых интерфейсов

Псевдонимы необходимы для перехвата трафика для последующей обработки в соответствии с заданной политикой. Псевдоним может отличаться от физического названия интерфейса: например, физическое устройство eth3, а псевдоним - dmz.

По умолчанию псевдонимы на интерфейсах не заданы.

Для того, чтобы назначить псевдонимы (alias) для сетевых интерфейсов, необходимо выполнить следующую команду в оболочке KLISH в режиме enable:

vpnconfig set interface <id> alias <string>

Для того, чтобы узнать список идентификаторов интерфейса, можно воспользоваться командой:

vpnconfig list interface

	Псевдонимы сетевых интерфейсов должны строго совпадать с логическим именем интерфейса при описании объекта в глобальной политике в ЦУП.
	Назначение псевдонимов сетевым интерфейсам является обязательным. В противном случае обработка трафика заданной политикой будет невозможна.
	Рекомендуется задавать псевдонимы (alias) равными именам, присвоенным сетевым соединениям.

4.5 Расширенные настройки сети

4.5.1 Настройка автоматической синхронизации системного времени (NTP)

По умолчанию в ПО NTP-сервер запущен и имеет базовые настройки в файле /etc/ntp.conf.

```
server ntp1.vniiftri.ru iburst prefer
server ntp2.vniiftri.ru iburst
server ntp3.vniiftri.ru iburst
server ntp4.vniiftri.ru iburst
# server 127.127.1.0 позволит в случае отказа сети Интернет брать время из своих системных часов
server 127.127.1.0
#restrict default – задает значение по умолчанию для всех рестриктов.
restrict default nomodify nopeer noquery limited kod
restrict 127.0.0.1
restrict [::1]
```

Для синхронизации времени с NTP-серверами ВНИИФТРИ[1)] ntp1.vniiftri.ru, ntp2.vniiftri.ru, ntp3.vniiftri.ru. ntp4.vniiftri.ru требуется включить разрешение имён, см. пункт 4.4.3.

Статус синхронизации времени можно посмотреть командой:

ntpq -p

```
     remote           refid      st t when poll reach   delay   offset  jitter
==============================================================================
 LOCAL(0)        .LOCL.           5 l   15   64    1    0.000   +0.000   0.000
*ntp1.vniiftri.r .MRS.            1 u    1   64    7    6.098   -2.110  18.527
+ntp2.vniiftri.r .MRS.            1 u   66   64    3    5.936   -0.881  20.801
+ntp3.vniiftri.r .MRS.            1 u   64   64    3    6.121   -0.946  20.691
+ntp4.vniiftri.r .MRS.            1 u    1   64    7    5.762   -1.991  18.415
```

Для коррекции настроек NTP-сервера необходимо выполнить следующие действия:

1) войти в оболочку BASH и открыть файл /etc/ntp.conf на редактирование текстовым редактором (например, vi, vim, nano, редактором файл-менеджера mc):

sudo [vim|vi|nano] /etc/ntp.conf

2) указать серверы:

```
server [имя сервера 1 | IP сервера 1] iburst prefer
server [опционально имя сервера 2 | IP сервера 2]  iburst
server [опционально имя сервера | IP сервера 3]  iburst
```

3) при использовании DNS-имен вместо IP-адресов необходимо включить разрешение имён, см. пункт 4.4.3.

4) после изменения настроек следует перезапустить ntpd:

/etc/init.d/S49ntp restart

Внимание! Для функционирования NTP-сервера в качестве источника времени после перезапуска требуется значительное время (около 6 минут). Статус можно посмотреть командой:

ntpq -p

```
remote           refid      st t when poll reach   delay   offset  jitter
==============================================================================
*LOCAL(0)        .LOCL.           5 l   19   64   37    0.000   +0.000   0.000
```

Символ * напротив сервера означает возможность работы в качестве источника времени.

[1)] Подробно об актуальных адресах NTP-серверов можно узнать, открыв веб-сайт ВНИИФТРИ (http://www.vniiftri.ru/ru/uslugi-serverov).

4.5.2 Настройка удаленной регистрации событий (SYSLOG)

ПО позволяет настроить регистрацию событий с помощью системного журнала Syslog. При этом syslog-сервер может находиться как на локальном, так и на удалённом компьютере.

Для настройки удалённой регистрации событий необходимо выполнить команду в оболочке KLISH:

```
set zastava_syslog facility <facility> ip <A.B.C.D syslog-server-addr> [порт поумолчанию 514]
```

где: `<facility>` – одно из значений `local0...local7`, заданное в настройках включения удаленной регистрации событий описаны в 7.2.1.5.

4.5.3 Настройка мониторинга (SNMP)

Для мониторинга ПО и отправки сигналов нарушения по протоколу SNMP нужно зарегистрировать библиотеку расширения сервиса snmpd (MIB-модуль). MIB-модуль можно взять из файловой системы ПО по пути: */opt/ZASTAVAoffice/etc/tws.mib*.

Сигналы нарушения (snmp-traps) будут отправляться только по указанным в локальной политике безопасности событиям.

Для настройки мониторинга ПО и отсылки сигналов нарушения (snmp-traps) в оболочке BASH необходимо выполнить следующие действия:

1) с помощью текстового редактора скорректировать файл */etc/snmp/snmpd.conf* в соответствии с приведённым ниже текстом:

```
dlmod snmpagent /opt/ZASTAVAoffice/lib/libsnmpagent.so
view all included .1.3.6.1.4.1.20145
view all included .1.3.6.1.2
rocommunity public default -V all
sysContact support@elvis.ru
sysDescr ZASTAVA-Office [номер версии]
agentAddress udp:<A.B.C.D адрес для мониторинга>:[порт SNMP по умолчанию 161]
```

2) в оболочке BASH для принятия изменений перезапустить демон:

```
/etc/init.d/S59snmpd restart
```

Также для корректировки настройки мониторинга ПО можно использовать команды оболочки KLISH в режиме enable.

3) далее для указания конкретного адреса мониторинга выполнить команду:

```
snmp set listening_address <A.B.C.D адрес ПАК для снятия SNMP статистики>
```

4) для задания локации сервера администратором выполнить команду:

```
snmp set system sysLocation
```

5) для задания имени сервера администратором выполнить команду:

```
snmp set system sysName
```

Для перезапуска, остановки и запуска сервиса использовать следующие команды:

```
snmp service restart
snmp service stop
snmp service start
```

4.5.4 Настройка PROXY HTTP

Для того, чтобы ПО функционировало в режиме proxy-сервера для обработки HTTP-трафика, необходимо:

1) открыть файл локальных настроек ПО *(/var/vpnagent/localsettings.ini*);
2) заполнить секцию PROXY:

```
/PROXY=
        HTTP_LISTEN_PORT=<PORT>
        HTTP_LISTEN_ADDR=<IP>
    end=
```

3) перезапустить службу командой: `/etc/init.d/S47vpngate restart`;
4) на proxy-клиенте в настройках интернет-обозревателя указать режим подключения с использованием proxy.

Правила обработки http-трафика задаются ЛПБ ПО в ЦУП.

4.5.5 Настройка DHCP-сервера

Для настройки службы DHCP-сервера, необходимо:

1) открыть файл /etc/init.d/S80dhcp-server;
2) если требуется ограничить интерфейсы, которые будут прослушивать DHCP-сервер, то необходимо отредактировать параметр INTERFACES="", указав там конкретные названия прослушиваемых интерфейсов, например: INTERFACES="eth2 eth3";
3) закрыть файл /etc/init.d/S80dhcp-server с сохранением изменений;

4) открыть файл /etc/dhcp/dhcpd.conf. В файле задать параметры работы сервера. Ниже приведен пример содержимого файла dhcpd.conf, для следующих параметров DHCP-сервера:
   - сервер является авторитарным;
   - имеет сетевой интерфейс в сети 172.16.0.0/24;
   - диапазон выдаваемых IP-адресов 172.16.0.10-172.16.0.250;
   - широковещательный IP-адрес выдаваемой сети 172.16.0.255;
   - шлюз по–умолчанию в выдаваемой сети 172.16.0.1;
   - сервер DNS 172.20.0.1;
   - префикс домена dhcp.example.ru;
   - время аренды IP-адресов 600 секунд;
   - максимальное время аренды IP-адресов 7200 секунд.

Содержимое файла dhcpd.conf:

```
authoritative;
subnet 172.16.0.0 netmask 255.255.255.0 {
range 172.16.0.0 172.16.0.0;
option subnet-mask 255.255.255.0;
option broadcast-address 172.16.0.255;
option routers 172.16.0.1;
option domain-name-servers 172.20.0.0;
option domain-name "dhcp.example.ru";
default-lease-time 600;
max-lease-time 7200;
}
```

5) сохранить файл конфигурации после внесения в него изменений;
6) запустить DHCP-сервер с помощью команды: `/etc/init.d/S80dhcp-server start`

4.6 Включение двухфакторной аутентификации

Для включения режима двухфакторной аутентификации необходимо выполнить команду: **`set 2nd_factor_authorization {ESMART|RuToken}`** в режиме enable. При наличии импортированного доверенного сертификата будет отображено сообщение:

```
Список имеющихся в системе доверенных сертификатов УЦ:

  Type: trusted
  Subject: CN=CA-ELVIS-PLUS
  Issuer: CN=CA-ELVIS-PLUS
  Device Name: Trusted Certificates token
  Expiration Date: 23.06.2027 20:18:30
  Algorithm: GOST R 34.10-2012 256
```

```
  Possible Id Types: DN
Внимательно изучите доверенные сертификаты, есть ли в списке нужный
Включить двухфакторную аутентификацию? (y/n)
```

Для включения режима двухфакторной аутенитфикации необходимо нажать клавишу «y». После этого отобразится следующее сообщение:

```
Перед включением необходимо проверить возможность входа в ОС.
Предоставьте токен и нажмите клавишу Enter
```

Необходимо предъявить персональный идентификатор, соответствующий требованиям. Требования к персональным идентификаторам приведены в подразделе 2.3. Для отмены включения режима двухфакторной аутенитфикации необходимо нажать клавишу «n».

При включении режима двухфакторной аутенитфикации возможно возникновение следующих сообщений об ошибках:

— в случае отсутствия импортированного доверенного сертификата появится сообщение:

```
Нет доверенных сертификатов. Включение двухфакторной авторизации
невозможно.
Пожалуйста, сначала выполните импорт доверенного сертификата.
```

— в случае несоответствия предъявленного персонального идентификатора требованиям будет отображено сообщение:

```
Читается токен...
pamtester: User not known to the underlying authentication module
Двухфакторная аутентификация с сертификатом на токене не может быть
включена.
Причина:На токене отсутствует сертификат для входа.
```

Отключение режима двухфакторной аутентификации не предусмотрено.

4.7 Конфигурирование программного обеспечения «ЗАСТАВА-Управление»

Для того, чтобы ПО получало политику безопасности от программного обеспечения «ЗАСТАВА-Управление» (далее - ЦУП), необходимо в ЦУП:

1) создать объект топологии – шлюз безопасности, которым будет являться ПО. Добавить все объекты топологии, которые будут функционировать в сети;

2) в свойствах объекта ПО:

– задать имя объекта;

– задать топологию объекта, в качестве логического имени интерфейса использовать псевдонимы (alias) интерфейсов, заданных в ПО;

Псевдонимы сетевых интерфейсов должны строго совпадать с логическим именем интерфейса при описании объекта в глобальной политике в ЦУП.

– импортировать персональный сертификат (или задать описание), указанный в ПО, для создания соединения;

– задать прогрузчик;

3) выполнить трансляцию и активацию политики.

Также необходимо в самом ПО задать получение политики с ЦУП, как описано в п. 7.2.1.4.3.

Подробная информация о списке доступных настроек ЦУП приведена в руководстве администратора для ПО «VPN/FW «ЗАСТАВА-Управление», версия 6 КС3».

5 ОПИСАНИЕ СРЕДСТВ КОНФИГУРИРОВАНИЯ И МОНИТОРИНГА

Интерфейс конфигурирования и мониторинга ПО представлен двумя видами командной оболочки: KLISH и BASH. Информация о работе с BASH представлена в разделе 7. Информация о работе с KLISH представлена в разделе 6.

После локальной аутентификации или удаленном управлении по SSH под учётной записью admin для управления ПО Администратор ПО автоматически работает в оболочке KLISH. Для перехода в оболочку BASH используется последовательность команд:

```
> enable
# bash
```

При необходимости повышения привилегий (например, для изменения конфигурационных файлов) необходимо выполнять команды с утилитой sudo:

```
$ sudo <команда требующая повышенных привилегий>
```

Также возможно повышение полномочий на время сеанса работы в оболочке `BASH` через команду:

```
$ sudo su -
#
```

Выход из режима суперпользователя BASH производится комбинацией клавиш Ctrl-D, либо командой:

```
# exit
```

Выход из BASH производится комбинацией клавиш Ctrl-D, либо командой:

```
$ exit
```

Запрещается использовать протокол SSH по открытым каналам связи (сети Интернет) без использования технологии VPN для удаленного подключения к ПО.

При начале конфигурирования какой-либо настройки в одном интерпретаторе, продолжить конфигурирование необходимо в этом же интерпретаторе. Например, если сначала конфигурирование сетевых настроек (названия интерфейсов, IP-адресация) было произведено в KLISH, то продолжить конфигурацию (например, если добавилась необходимость конфигурирования маршрутизации) необходимо тоже в KLISH.

После локальной аутентификации или удаленном управлении по SSH под учётной

записью user для мониторинга ПО Администратор ПО автоматически работает в оболочке KLISH с ограниченным набором команд без возможности выхода в режим конфигурирования и загрузки оболочки BASH.

6 ОПИСАНИЕ ДОСТУПНЫХ ОПЕРАЦИЙ ИНТЕРПРЕТАТОРА KLISH

6.1 Назначение интерпретатора KLISH

Командный интерпретатор KLISH (далее – KLISH) предназначен для создания удобного окружения пользователя с ограниченным набором команд и автодополнением.

KLISH позволяет сформировать различные списки команд, доступных для исполнения каждому из пользователей. Администратору ПО доступны команды, необходимые для просмотра настроек и журналов, а также для выполнения настроек.

У некоторых команд есть дополнительные, но необязательные параметры, служащие для уточнения или более детального просмотра настроек. Такие параметры будут обозначены в конце символом «(н)».

Например, команда `network connection show` может быть выполнена как сама, без дополнительных параметров, так и как `network connection show id <имя_соединения>`. В первом случае, выводом команды будет список всех существующих сетевых соединений в системе, а во втором все параметры какого-то конкретного сетевого соединения.

6.2 Негрупповые команды

Не все команды KLISH можно объединить в логические группы. В таблице 1 представлен список таких команд.

Таблица 1 – Негрупповые команды

Команда	Описание действия
exit	Выход из оболочки enable
enable	Вход в оболочку enable
bash	Вход в оболочку BASH
password	Смена пароля
check integrity	Проверка целостности файлов агента безопасности ПО
snmp	Настройка протокола SNMP
l2_tp_configure	Настройка l2tp
reboot	Перезагрузка
halt	Выключение питания
?	Запрос справки об использовании команды

6.3 Команда смены пароля

Интерактивная команда по смене пароля, производящая смену пароля для текущей учётной записи:

```
> password
```

Далее запустится диалог:

```
Смена пароля для [user | admin].
Текущий пароль:
Новый пароль:
Повторите ввод нового пароля:
```

При успешной смене пароля выводится сообщение

```
passwd: пароль успешно обновлён
```

При несовпадении паролей при задании нового пароля будет отображено сообщение:

```
Извините, но пароли не совпадают.
passwd: Службе паролей не удалось выполнить предварительную проверку.
passwd: Пароль не изменён
```

При задании нового пароля, равного текущему, появится сообщение:

```
passwd: Пароль не изменён
```

6.4 Команды просмотра настроек

Группа команд просмотра настроек, начинаются с префиксов **`show`**, **`vpnconfig`**, **`vpnmonitor`** и **`network`**.

Список доступных команд с префиксом *show* представлен в таблице 2.

Таблица 2 – Команды с префиксом *show*

Ключ 1	Ключ 2	Описание действия
`log`	**`audit`**	Открыть в режиме чтения журнал аудита действий администратора
	`bin_log`	Просмотр журнала событий vpnagent
`interfaces`	**`-`**	Вывести информацию о сетевых интерфейсах

Список доступных команд с префиксом `vpnconfig list` представлен в таблице 3.

Таблица 3 – Команды с префиксом *vpnconfig list*

Ключ 1	Описание действия
`cert`	Вывести информацию о сертификатах

Ключ 1	Описание действия
ha	Вывести информацию о настройках кластера
jk	Вывести информацию о методах прогрузки политики безопасности
interface	Вывести информацию об интерфейсах и их alias
ike	Вывести информацию о настройках IKE
lsp	Вывести информацию о текущем источнике получения политик безопасности
log	Вывести информацию о параметрах логирования
provider	Вывести информацию о криптопровайдерах
token	Вывести информацию о токенах
admin	Вывести информацию об учетной записи с правами Администратора ПО

Список доступных команд с префиксом `vpnmonitor` представлен в таблице 4.

Таблица 4 – Команды с префиксом *vpnmonitor*

Ключ 1	Ключ 2	Описание действия
p	**-**	Вывести информацию о текущей политике безопасности
pp	**-**	Вывести подробную информацию о текущей политике безопасности
s	**-**	Вывести статистику
	ipsec (н)	Вывести статистику протокола IPsec
	ike (н)	Вывести статистику протокола IKE
	ike1 (н)	Вывести только статистику протокола IKE v1
	ike2 (н)	Вывести только статистику протокола IKE v2
	ha (н)	Вывести статистику протокола ha
	fcache (н)	Вывести информацию по кэшу фильтров
	all(н)	Вывести статистику всех фильтров
i	**-**	Вывести краткую информацию о количестве IKE/IPsec сессий
	show	Вывести краткую информацию о сессиях конкретного протокола
	ike-id	Вывести подробную информацию об IKE сессии с конкретным id
	ipsec-id	Вывести информацию об IPsec сессии с конкретным id
f	**-**	Вывести информацию о фильтрах
	id	Вывести подробную информацию о конкретном фильтре с id

Ключ 1	Ключ 2	Описание действия
ike-cfg	**-**	Вывести информацию об IKE-cfg
rri	**-**	Вывести информацию таблицы reverse routing enjection
proxy	**-**	Вывести информацию о работе proxy

С префиксом *network* существует единственная команда, `network connection show`, которая выводит список всех существующих сетевых соединений. Имеет необязательный ключ `id`, после которого необходимо ввести имя соединения, чтобы просмотреть детально его параметры.

6.5 Команды выполнения настроек

Команды выполнения настроек начинаются с префиксов `set`, `vpnconfig`, `vpnmonitor` и `network`.

Список доступных команд с префиксом *set* представлен в таблице 5.

Таблица 5 – Команды с префиксом *set*

Ключ 1	Ключ 2	Ключ 3	Ключ 4	Описание действия
cron	**job**	**reboot**	**<time>**	Изменить время ежедневной перезагрузки на time
		-	**-**	Открыть журнал заданий cron
ntp	**<ip>**			Добавить NTP-сервер
cluster	**settings**	**-**	**-**	Открыть файл keeplaived.conf
	mode	**on**	**-**	Включить кластерезацию
		off	**-**	Выключить кластерезацию
date	**<date>**	**-**	**-**	Установить системную дату\время, равными date
timezone	**<zone>**	**<city>**	**-**	Установить часовой пояс, равный zone city
zastava_syslog	**<facilty>**	**<ip>**	**<порт>**	Добавить syslog сервер с IP-адресом и портом, которому будут посылаться события с источника facility
BGP	**on**	**-**	**-**	Включает сервис поддержки протоколов динамической маршрутизации
	off	**-**	**-**	
dhcp				Включает службу DHCP-server
dhcp_relay	**<interface>**			Включает механизм переадресации запросов на получение сетевых настроек на указанный интерфейс
Multi_wan_configuration	**on**			Запускает интерактивную утилиту настройки простой реализации multi wan для двух операторов связи
diffserv				Параметр, отвечающий за включение функции

Ключ 1	Ключ 2	Ключ 3	Ключ 4	Описание действия
				приоритизации трафика на основании поля ToS заголовка IP-пакета. diffserv=1 – приоритизация трафика включена. По умолчанию установлено значение «0»
OSFP	**on**	**-**	**-**	Включает сервис поддержки протоколов динамической маршрутизации
	off	**-**	**-**	

Список доступных команд с префиксом `vpnconfig` представлен в таблице 6.

Таблица 6 – Команды с префиксом *vpnconfig*

Ключ 1	Ключ 2	Ключ 3	Ключ 4	Описание действия
activate	**lsp**	**system**		Выполнить активацию системной политики
add	**cert**	**<string>**		Добавить сертификат
	request	**<Id of token>**		Запрос на выпуск сертификата, пример команды представлен ниже. В результате будет сгенерирован запрос на выпуск сертификата, который необходимо передать в центр сертификации
	key	**<name>**	**[<options>]**	Добавить PSK-ключ
	provide	**<name>**		Добавить криптопровайдера
clear	**log**			Выполнить очистку лога
export	**cert**	**<id>**	**<path>**	Выполнить экспорт сертификата id в файл path
login	**admin**	**<name>**	**<pass>**	Выполнить вход под администратором
	token	**<id>**	**<pin>**	Выполнить login к токену с id
logout	**<id>**	**-**	**-**	Выполнить logout токена с id
password	**<id>**	**<pin1>**	**<pin2>**	Сменить текущий pin1 на новый pin2 токена id
remove	**cert**	**<id>**		Удалить сертификат с id
	provider	**<name>**		Удалить провайдер и именем name
reset	**<param>**	**<id> (н)**		Восстановить значение всех параметров param или конкретного параметра id. Можно восстановить значения параметров ha, jk, ike, log, update
set	**<param>**	**<id>**	**<value>**	Установить значение value для параметра id из группы param
update	**status**			Проверить статус обновлений
	check			Проверить доступность обновлений
	install			Установить обновления

Ключ 1	Ключ 2	Ключ 3	Ключ 4	Описание действия
ver				Показать информацию о версии
view	**cert**	**<id>**		Показать подробную информацию о сертификате id
	lsp	**current**		Показать информацию о текущей политике безопасности

Команда `vpnconfig set <param><id><value>` позволяет выполнить установку основных параметров для групп HA, JK INTERFACE,IKE, LOG, LSP, UPDATE, ADMIN, REQUEST. Использование команды в KLISH аналогично ее использованию в BASH.

Запрещено использовать уровень регистрации событий «Заблокирован (Disabled»).

Список доступных команд установки настроек с префиксом `vpnmonitor` представлен в таблице 7.

Таблица 7 – Команды с префиксом *vpnmonitor*

Ключ 1	Ключ 2	Описание действия
single	-	Перевести vpnagent в режим одиночного функционирования
active	-	Перевести vpnagent в режим кластера и сделать ноду активной
passive	-	Перевести vpnagent в режим кластера и сделать ноду пассивной

Список доступных команд с префиксом *network* представлен в таблице 8.

Таблица 8 – Команды с префиксом *network*

Ключ 1	Описание действия
device	Показать существующие сетевые устройства
nmtui	Псеводографическая утилита настройки, повторяет функционал командной строки
connection	Утилита настройки сети (см. таблицу 9)

Таблица 9 – Команды с префиксом *network connection*

Ключ 1	Ключ 2	Ключ 3	Описание действия
show	**<id> (н)**		Показать настройки соединения id
			Показать существующие соединения
up	**<id>**		Сделать активным соединение id
down	**<id>**		Сделать неактивным соединение id
add	**-**	**-**	Добавить новое соединение (см. таблицу10)
modify	**<id>**	**-**	Изменить существующее соединение (см. таблицу 11)
clone	**<id1>**	**<id2>**	Скопировать соединение id1 в соединение с именем id2
edit	**-**	**-**	Отредактировать соединения
delete	**<id>**		Удалить соединение id

Ключ 1	Ключ 2	Ключ 3	Описание действия
monitor	**-**		Отследить, в режиме реального времени, изменения в настройках соединения
reload	**<id>**		Перезагрузить соединение id
load	**<path>**		Загрузить соединение из файла path

Таблица 10 – Команды с префиксом *network connection add*

Ключ 1	Ключ 2	Ключ 3	Ключ 4	Ключ 5	Описание действия
type	**ethernet**	**<con-name>**	**<ifname>**	**<Master> (н)**	Добавить соединение типа Ethernet с именем con-name применимое к интерфейсу ifname. Если указана опция master то соединение будет участником соединения с именем master
	vlan	**<con-name>**	**<dev>**	**<id>**	Добавить соединение типа vlan с именем con-name, которое будет использовать интерфейс dev и иметь VID id
	bridge	**<con-name>**	**-**	**-**	Добавить соединение типа bridge с именем con-name
	bond	**<con-name>**	**-**	**-**	Добавить соединение типа bond с именем con-name
	tun	**<con-name>**	**-**	**-**	Добавить соединение типа tun с именем con-name

Таблица 11 – Команды с префиксом *network connection modify*

Ключ 1	Ключ 2	Ключ 3	Описание действия
ipv4.addresses	**<ip>**	**-**	Установить ipv4-адрес для соединения равный IP-адресу
ipv4.method	**manual**	**-**	Изменить метод получения настроек соединения на ручной (т.н. static)
	auto	**-**	Изменить метод получения настроек соединения на автоматический, по протоколу DHCP
autoconnect	**yes**	**-**	Автоматически применять соединение в момент появления линка
	no	**-**	Не применять автоматически соединение в момент появления линка
ipv4.dns	**<ip>**	**-**	Установить DNS сервер ip для соединения. Замещает все существующие DNS сервера
ipv4.gateway	**<ip>**	**-**	Установить шлюз поумолчанию для соединения равный IP-адресу
ipv4.dhcp-timeout	**<value>**	**-**	Установить DHCP-timeout для соединения равный value
vlan.id	**<id>**	**-**	Изменить VID для соединения и сделать равным id
vlan.parent	**<id>**	**-**	Изменить parent для соединения и сделать равным id

Ключ 1	Ключ 2	Ключ 3	Описание действия
+ipv4.routes	**<net>**	**<hope>**	Добавить дополнительный маршрут к соединению на сеть net через шлюз hope
+ipv4.dns	**<ip>**	**-**	Добавить дополнительный DNS-сервер с IP-адресом для соединения
-ipv4.routes	**<net>**	**-**	Удалить дополнительный маршрут у соединения на сеть net
-ipv4.dns	**<ip>**	**-**	Удалить DNS сервер с IP-адресом

Список доступных команд с префиксом *snmp* представлен в таблице 12.

Таблица 12 – Команды с префиксом *snmp*

Ключ 1	Ключ 2	Ключ 3	Ключ 4	Описание действия
set	**listening_address**	**<ip>**	**_**	Задать адрес для мониторинга
set	**system**	**sysLocation**	**<строка>**	Задать локацию для монитороинга
set	**system**	**sysName**	**<строка>**	Задать имя сервера для монитороинга
service	**restart**	**_**	**-**	Рестарт службы SNMP
service	**stop**	**_**	**-**	Останов службы SNMP
service	**start**	**_**	**-**	Старт службы SNMP

6.6 Команды для диагностики состояния сетевого соединения

Список доступных команд для диагностики состояния сетевого соединения представлен в таблице 13.

Таблица 13 – Диагностика состояния сетевого соединения

ping {<IP-address|IPv6-address>|ip|ipv6|arp}		**Доступ к команде:АЕ**
1	**Ping <IP-address|IPv6-address > {без дополнительного параметра|source| repeat}**	
1.1	**без дополнительного параметра**	Выполнить команду ping на <IP-address>
1.2	**Source <IP-address>**	Выполнить команду ping на <IP-address> от IP-адреса шлюза, указанного в параметре source (например с заднего интерфейса шлюза)
1.3	**repeat**	Выполнить команду ping на <IP-address> указанное в параметре **repeat** число раз
2	**ip|ipv6 <IP-address> {без дополнительного параметра|source|size|repeat|interval|resolve}**	
2.1	**без дополнительного параметра**	Выполнить команду ping на <IP-address>
2.2	**source <IP-address>**	Выполнить команду ping на <IP-address> от IP-адреса шлюза, указанного в параметре source (например с заднего интерфейса шлюза)
2.3	**size <>**	Выполнить команду ping на <IP-

		address> пакетами, указанного размера
2.4	**repeat <целое число>**	Выполнить команду ping на <IP-address> указанное в параметре число раз
2.5	**interval <целое число>**	Выполнить команду ping на <IP-address> с интервалом между пакетами, указанным в параметре
2.6	**resolve {source|interval|repeat|flood| broadcast| duplicate-detect|size}**	
3	**arp <Hostname or IP-address>**	
3.1	**<Hostname or IP-address>**	Отправляет ARP-запрос на <Hostname> или <IP-address>
traceroute {ip|ipv6} <IP-address|IPv6-address>		**Доступ к команде:АЕ**
4	**ip <IP-address> {без дополнительного параметра| resolve|source|interface}**	
4.1	**без дополнительного параметра**	Трассировка маршрута до определенного IP-адреса
4.2	**source <ip-address>**	Трассировка маршрута до определенного IP-адреса от IP-адреса шлюза, указанного в параметре source
4.3	**interface <interface-name>**	Трассировка маршрута до определенного IP-адреса от интерфейса шлюза, указанного в параметре interface
4.4	**resolve {source|interface}**	
4.4.1	**source <ip-address>**	Трассировка маршрута до определенного IP-адреса от IP-адреса шлюза, указанного в параметре source (с определением dns-имен)
4.4.2	**interface <interface-name>**	Трассировка маршрута до определенного IP-адреса от интерфейса шлюза, указанного в параметре interface (с определением dns-имен)
5	**ipv6 <IPv6-address> {без дополнительного параметра| resolve|source|interface}**	
5.1	**без дополнительного параметра**	Трассировка маршрута до определенного IP-адреса
5.2	**source <ipv6-address>**	Трассировка маршрута до определенного IP-адреса от IP-адреса шлюза, указанного в параметре source
5.3	**interface <interface-name>**	Трассировка маршрута до определенного IP-адреса от интерфейса шлюза, указанного в параметре interface
5.4	**resolve {source|interface}**	
5.4.1	**source <ipv6-address>**	Трассировка маршрута до определенного IP-адреса от IP-адреса шлюза, указанного в параметре source (с определением DNS-имен)
5.4.2	**interface <interface-name>**	Трассировка маршрута до

		определенного IP-адреса от интерфейса шлюза, указанного в параметре interface (с определением DNS-имен)

6.7 Резервирование и восстановление данных

Описание команды для резервирования и восстановления данных приведено в таблице 14.

Резервированию подлежат сетевые настойки, локальные настройки агента безопасности ПО, локальное хранилище сертификатов агента безопасности.

	Внимание! При возврате к заводским установкам, архивы, созданные в файловой системе, не сохраняются. Для хранения настроек они должны быть перемещены из файловой системы ПО в систему резервирования.
	Внимание! Требования правил пользования ПО по обращению с ключевой информацией распространяются на локальный архив, содержащий ключевой контейнер.

Таблица 14 – Резервирование и восстановление данных

backup_and_restore <Enter>		**Доступ к команде:АЕ**
1	1)	Отображает список доступных токенов и архивов. Требует ввода PIN-кода
2	2)	Создает архив настроек для восстановления. Требует ввода PIN-кода, указания номера токена, на котором будет создана резервная копия данных (если токен единственный, то необходимо указать 1)
3	3)	Создает архив настроек для восстановления локально. Архив будет расположен по пути: /mnt/backup/BACKUP-LOCAL.tar
4	4)	Создает архив настроек для восстановления. Требует ввода PIN-кода, указания номера токена (если токен единственный, то необходимо указать 1), с которого будет выполнено восстановление данных
5	5)	Выполняет восстановление настроек из локального архива
6	6)	Выход из подпрограммы резервирования и восстановления данных

7 ОПИСАНИЕ ДОСТУПНЫХ ОПЕРАЦИЙ ИНТЕРПРЕТАТОРА BASH

7.1 Обзор средств мониторинга

Для осуществления мониторинга работы ПО используются следующие средства:

— журналы регистрации событий (bin_log.txt, vpndmn_init.log);

— системный журнал syslog;

— утилита vpnmonitor.

7.1.1 Файл регистрации системных событий

Записи о регистрируемых системных событиях хранятся в директории `/var/vpnagent/log/` (например, `bin_log.txt` и `vpndmn_init.log`, или `clish_audit.log`, который хранится в директории `/var/log`).

В ЛПБ для каждой группы системных событий ([POLICY] (политика безопасности), [CERTS] (сертификаты) и т.д.) может содержаться настройка уровня детализации. Если уровень детализации для соответствующей группы событий отсутствует в ЛПБ, то в этом случае будут использованы локальные настройки уровня журналирования.

7.1.1.1 Упорядочение и сортировка событий

Для сортировки событий используется утилита `sort`. Утилита может использоваться как для сортировки текста из файла, так и для сортировки вывода команд.

Общий синтаксис использования утилиты:

sort <опции> <файл>;
– <команда> | sort <опции>.

Основные опции утилиты:

– -b - не учитывать пробелы;
– -d - использовать для сортировки только буквы и цифры;
– -i - сортировать только по ASCII-символам;
– -n - сортировать строки по числовому значению;
– -r - сортировать в обратном порядке;
– -c – проверить, был ли отсортирован файл;
– -o - вывести результат в файл;
– -u - игнорировать повторяющиеся строки;
– -m - объединенить ранее отсортированные файлов;

– -k - указать поле, по которому нужно сортировать строки, если не задано, сортировка выполняется по всей строке;

– -f - использовать в качестве разделителя полей ваш символ вместо пробела.

Примеры использования `sort`:

1) команда отсортирует журнал по дате и времени в обратном порядке:

```
sort –k1,2 -r /var/vpnagent/log/bin_log.txt
```

2) команда отсортирует вывод журнала по дате и времени в обратном порядке:

```
cat /var/vpnagent/log/bin_log.txt sort –k1,2 -r
```

Однако вышеуказанный вывод журнала может быть неудобен для восприятия. Для того, чтобы события при сортировке имели читаемый формат, используется утилита `sed` с опцией `"s:\\\\\n:\\\\\t:g"`.

Таким образом, сортировка вывода журнала выглядит так (сортировка по дате и времени в обратном порядке):

```
cat /var/vpnagent/log/bin_log.txt | sed "s:\\\\\n:\\\\\t:g" | sort –k1,2 –r
```

Для поиска в выводе журнала определенного события используется утилита `grep`:

```
cat /var/vpnagent/log/bin_log.txt | grep <текст>
```

Пример использования (вывод всех событий типа NOTICE):

```
cat /var/vpnagent/log/bin_log.txt | grep NOTICE
```

7.1.1.2 Очистка файла регистрации системных событий

Очистка содержимого файла регистрации системных событий происходит автоматически по достижении им максимально допустимого размера. Подробно о настройке параметров регистрации системных событий и управлении файлами регистрации см. п. 7.2.1.5. Событие очистки файла будет зарегистрировано и размещено в начале файла журнала.

Для принудительной очистки журнала можно воспользоваться командой `vpnconfig –clear log`. Данная команда требует ввода пароля Администратора ПК.

7.1.2 Утилита vpnmonitor

Утилита `vpnmonitor` предоставляет возможность обзора активных в настоящее время защищенных соединений, установленных с данным компьютером. Кроме того, `vpnmonitor` позволяет просмотреть статистику по пакетам.

7.1.2.1 Справочная система по работе с утилитой

Для получения справки по работе утилиты командной строки `vpnmonitor`

необходимо ввести команду `vpnmonitor -h`.

7.1.2.2 Просмотр статистики

Для вывода статистики надо выполнить команду:

```
vpnmonitor -s [ipsec|ike|ike2|ha|fcache|all].
```

Описание параметров команды `vpnmonitor -s` представлено в таблице 15.

Таблица 15 – Параметры команды vpnmonitor –s

Параметр	Описание
`ipsec`	Просмотр текущей скорости пакетов по протоколу IPsec
`ike`	Просмотр текущей скорости пакетов по протоколам IKE
`ha`	Просмотр текущей скорости пакетов по протоколу ha
`fcache`	Просмотр статистики fcache
`em`	Просмотр полной статистики event manager
`all`	Просмотр полной статистики

Список параметров выводимой статистики представлен в таблице 16.

Таблица 16 – Печень параметров статистики

Параметр	Описание
IPsec	
`Packets (bytes) received`	Получено пакетов (байт)
`Packets (bytes) sent`	Послано пакетов (байт)
`Decapsulated packets`	Декапсулировано (расшифровано) пакетов
`Encapsulated packets`	Инкапсулировано (зашифровано) пакетов
`Packets received unsecure`	Количество полученных незашифрованных пакетов
`Packets sent unsecure`	Количество отправленных незашифрованных пакетов
`Incoming errors`	Ошибки во входящих пакетах
`Outgoing errors`	Ошибки в исходящих пакетах
`Incoming auth errors`	Количество ошибок аутентификации во входящих пакетах
`Incoming anti-replay errors`	Количество ошибок при подавлении атак воспроизведения во входящих пакетах
`Dropped packets (in/out)`	Отброшено пакетов (входящих/исходящих)
`Input frags consumed`	Количество использованных входных фрагментов
`Output frags consumed`	Количество использованных выходных фрагментов
`Output frags created`	Количество созданных выходных фрагментов

Параметр	Описание
Decrease MTU requests	Количество пакетов-запросов на понижение MTU
Incoming packets not found in hash table	Количество промахов для входящих пакетов при поиске фильтра в хэш-таблице
Outgoing packets not found in hash table	Количество промахов для исходящих пакетов при поиске фильтра в хэш-таблице
IKEv2	
IKE SAs created (failed) initiated/responded	Количество созданных (не созданных) инициированных/ отвеченных IKE SA в формате x(x)/x(x)
Resumed IKE SA initiated/responded	Количество возобновленных IKE SA инициированных/ отвеченных
IKE SA redirections received/sent	Количество перенаправлений IKE SA получено/послано
COOKIE requested/sent	Количество запрошенных/отправленных токенов COOKIE
Denied IKE SA requests	Количество отвергнутых запросов на создание IKE SA
IKE SA rekeys initiated/responded/collisions	Количество обновлений ключей IKE SA инициированных/отвеченных/коллизий в формате x/x/x
IPsec SA bundless created	Количество созданных IPsec SA
IPsec SA rekeys initiated/responded/collisions	Количество обновлений ключей IPsec SA инициированных/полученных/коллизий в формате x/x/x
Attempts to rekey non-existend IPsec SA by this host/by peer	Количество попыток обновления ключей несуществующей IPsec SA данным хостом/партнером
Temporary rekey failures on this host/on peer	Количество временных отказов в обновлении ключей данным хостом/партнером
INIT exchanges completed (with errors or failed) initiated/responded	Количество обменов INIT_IKE_SA успешных (с ошибками или неуспешных) инициировано/отвечено в формате x(x)/x(x)
RESUME exchanges completed (with errors or failed) initiated/responded	Количество обменов RESUME_IKE_SA успешных (с ошибками или неуспешных) инициировано/отвечено в формате x(x)/x(x)
AUTH exchanges completed (with errors or failed) initiated/responded	Количество успешных (с ошибками или неуспешных) обменов IKE_AUTH инициировано/отправлено в формате x(x)/x(x)
CHILD exchanges completed (with errors or failed) initiated/responded	Количество успешных (с ошибками или неуспешных) обменов CREATE_CHILD_SA инициировано/отправлено в формате x(x)/x(x)

Параметр	Описание
INFO exchanges completed (with errors or failed) initiated/responded	Количество успешных (с ошибками или неуспешных) обменов INFORMATIONAL инициировано/отправлено в формате x(x)/x(x)
HA	
Single start at	Время старта одиночного режима
Single start count	Количество переходов в одиночный режим
Active start count	Количество переходов в активный режим
Passive start count	Количество переходов в пассивный режим
Total recv/sent messages (bytes)	Объем полученных/отправленных сообщений в байтах
Total errors in recv/sent messages	Количество ошибок при получении/отправке сообщений
Unknown messages(bytes) recv	Количество неизвестных сообщений (байт) при получении сообщений
Create IKE SA: recv/sent messages (bytes)	Объем полученных/отправленных сообщений в байтах при создании IKE SA
Create IKE SA: errors in recv/sent messages	Количество ошибок в полученных/отправленных сообщениях при создании IKE SA
Delete IKE SA: recv/sent messages (bytes)	Объем полученных/отправленных сообщений в байтах при удалении IKE SA
Delete IKE SA: errors in recv/sent messages	Количество ошибок в полученных/отправленных сообщениях при удалении IKE SA
Update IKE SA: recv/sent messages (bytes)	Объем полученных/отправленных сообщений в байтах при обновлении параметров IKE SA
Update IKE SA: errors in recv/sent messages	Количество ошибок в полученных/отправленных сообщениях при обновлении параметров IKE SA
Request IKE SA list: recv/sent messages (bytes)	Объем полученных/отправленных сообщений в байтах при запросе списка IKE SA
Request IKE SA list: errors in recv/sent messages	Количество ошибок в полученных/отправленных сообщениях при запросе списка IKE SA
Get IKE SA list: recv/sent messages (bytes)	Объем полученных/отправленных сообщений в байтах при запросе IKE SA
Get IKE SA list: errors in recv/sent messages	Количество ошибок в полученных/отправленных сообщениях при запросе IKE SA
IKE-CFG sync: recv/sent messages (bytes)	Объем полученных/отправленных сообщений в байтах при обновлении записей IKE-CFG
IKE-CFG sync: errors in recv/sent messages	Количество ошибок в полученных/отправленных сообщениях при обновлении записей IKE-CFG
IKE-CFG del: recv/sent messages (bytes)	Объем полученных/отправленных сообщений в

Параметр	Описание
	байтах при удалении записей IKE-CFG
IKE-CFG del: errors in recv/sent messages	Количество ошибок в полученных/отправленных сообщениях при удалении записей IKE-CFG
IKE-CFG clear: recv/sent messages (bytes)	Объем полученных/отправленных сообщений в байтах при обновлении сбросе записей IKE-CFG
IKE-CFG clear: errors in recv/sent messages	Количество ошибок в полученных/отправленных сообщениях при сбросе записей IKE-CFG
FiltDB Cache	
Hash table size (bytes max/alloc)	Размер хэш-таблицы (байт максимум/выделено) в формате x*x*x(x/x)
Validity tag	Текущее значение метки, служащей для определения возможности использования записей в хэш-таблице
Live entries	Количество активных записей
Dead entries	Количество удаленных записей
Allocated entries	Количество записей выделенных из памяти
Dead reused	Количество повторно использованных удалённых записей
Line reused	Количество использованных записей в линиях
Collisions	Количество попыток добавления одинаковых записей
Full lines	Количество заполненных линий
Empty lines	Количество пустых линий
Other lines	Количество остальных линий
Average length of non-empty lines	Средняя длина непустых линий
Event Manager	
Task queue size	Количество асинхронных задач в очереди на обработку(например бандл-реквестов)
UDP queue size	Количество пришедших IKE - udp пакетов в очереди на обработку
Timer queue size	Количество задач от внутреннего таймера (раз в секунду) в очереди на обработку
Wait timers count	Количество задач ожидающих наступления заданного времени для их исполнения (при наступлении этого времени задачи помещаются в очередь Timer queue size.
Task queue size	Количество асинхронных задач в очереди на обработку(например бандл-реквестов)

Пример вывода результата команды `vpnmonitor -s`:

```
param                          |value
-------------------------------|------------------------------
```

```
IPsec                          |
Packets (bytes) received       |398 774 (69 396 140)
Packets (bytes) sent           |79 362 (15 988 088)
Decapsulated packets           |0
Encapsulated packets           |0
Packets received unsecure      |398 774
Packets sent unsecure          |79 362
Incoming errors                |0
Outgoing errors                |0
Incoming auth errors           |0
Incoming anti-replay errors    |0
Dropped packets (in/out)       |0 (0 / 0)
Input frags consumed           |0
Output frags consumed          |0
Output frags created           |0
Decrease MTU requests          |0
Incoming packets not found i~|45 171
n hash table                   |
Outgoing packets not found i~|842
n hash table                   |

IKEv1:  init: 0, resp: 0
IKEv2:  init: 0, resp: 1
IPsec:  bundles: 0, ESP: 0, AH: 0, IPcomp: 0
FiltDB: alt: 3, main: 6, dynamic: 0

HA mode: single

vpndmn started at: 2024.03.10 03:00:54
       worked: 23 hours 37 minutes 35 seconds
```

7.1.2.3 Вывод информации об активированной политике

Для просмотра информации об активированной политике необходимо выполнить команду: `vpnmonitor -p`.

Пример вывода результата данной команды:

```
Current Policy:
        Type: System policy
        Source: Server: 10.10.10.10
        Title: ZASTAVA-Office
        Activated: Sun Mar 10 03:00:58 2024
```

Для просмотра подробной информации о параметрах прогруженной политики используется команда: `vpnmonitor -pp`.

Пример вывода подробной информации о политике:

```
        LSP request:
                type: System PMP
                file path:
```

```
                pmp servers: 10.10.10.10
                cert subject: CN=ZASTAVA-Office
                log level: VERBOSE

        LSP active:
                type: System PMP
                file path:
                pmp servers: 10.10.10.10
                pmp cert subject: CN=ZASTAVA-Office
                pmp cert issuer: CN=ELVIS-CA
                pmp cert serial:
  3E00000004874B58CB2F30860E000000000004
                pmp cert key alg: GOST R 34.10-2012 256
                pmp log level: VERBOSE
                title: ZASTAVA-Office
                hash: CFBD939CA6C8732C512A9BADD5765EA0
                time: Sun Mar 10 03:00:58 2024
                in progress: false
                from DB: false
                cert present: true
                connected to TPN: true
                last error:
                diagnostic: System policy 'ZASTAVA-Office'
  activated at Sun Mar 10 03:00:58 2024
```

7.1.2.4 Просмотр информации о созданных IKE/IPSec SA

Для просмотра активных защищённых соединений, установленных с данным компьютером, а также создающихся защищённых соединений необходимо выполнить команду `vpnmonitor -i`. Команда выводит информацию по каждому из созданных соединений в следующем формате: [Идентификатор сессии Адрес партнера Идентификатор партнера Метод аутентификации и количество установленных IKE и IPSec соединений].

Пример:

```
      C4E4102DD1900627.D2B64E50EBA937B9       10.10.10.10
(DN)CN=ZASTAVA-Office   GOST3410.2012(256)-Sig / GOST3410.2012(256)-
Sig
      1       ESP(Tunnel) Responder   10.11.10.168 ->
192.168.21.0..192.168.21.255   rule_ipsec
      35644A41932BB5E394.3ED09011BE4EE9D0       10.10.10.130   (DN)
C=RU,CN=130_gost3      GOST3410.2012(256)-Sig / GOST3410.2012(256)-
Sig
      AE746FD322B297DB.820EE0D33788D2BA       10.10.10.132   (DN)
C=RU,CN=Client132_EPCSP    GOST3410.2012(256)-Sig /
GOST3410.2012(256)-Sig
      IKE states count 3
      IPsec states count 1
```

7.1.2.5 Фильтрация фильтров и созданных SA по параметрам

Для фильтрации защищенных соединений необходимо выполнить команду:

```
vpnmonitor –i <options>,
```
где: options:
```
-show (all | ike | ipsec | ipsectree);
-view (line | list | table | details | count);
-ike-sa;
-ipsec-sa;
-clearikesa.
-cmd (delete | rekey);
-delete;
-ike-id <id>;
-ipsec-id <id>.
```

Перед фильтрами можно задать параметры отображения:

```
-show all | ike | ipsec | ipsectree.
```

Описание значений параметра `show`:

`show all` – показывать все установленные соединения;

`show ike` – показывать только IKE SA;

`show ipsec` – показывать только IPsec SA;

`show ipsectree` – показывать IKE и IPSec SA. IKE SA, которые не имеют дочерних IPSec SA не показываются;

– `-view line | table | list| details` (по умолчанию используется `–view line -show all`). Опция предназначена для форматирования вывода списка SA.

Описание значений параметра `view`:

`view line` – показывать информацию в виде строк;

`view table` – показывать основную информацию в виде таблицы;

`view list` – показывать подробную информацию по каждому соединению в формате параметр-значение;

`view details` – показывать подробную информацию по каждому соединению в табличном виде;

`view count` – показывать только количество соединений.

Также предусмотрена возможность фильтрации по параметрам соединения в зависимости от протокола:

— для фильтрации по IKE: vpnmonitor –i [-ike-sa <filtering rules>];

— для фильтрации по IPsec: vpnmonitor –i [-ipsec-sa <filtering rules>].

При использовании правил фильтрации по IKE и IPsec фильтру ключ `-ike-sa` можно не указывать, т.е. все, что написано до ключа `-ipsec-sa`, будет считаться IKE-фильтром.

Для задания правил фильтраций необходимо воспользоваться командой:

`vpnmonitor –i [[-ike-sa] <filtering rules (правило_фильтрации)>].`

Правила фильтрации можно объединять с помощью логических операций: `and | or`

`<rule1> <and|or> <rule2>`, где: `rule1…N` правило фильтрации SA выбранного типа.

Для составления правила фильтрации (параметр <rule1…N>) необходимо указать поле, по которому будет производиться фильтрация, и операцию для нахождения того или иного SA. Формат правила может быть введен следующим образом:

`<field> <operation> <etalon> (<имя_поля> <операция> <эталон>),`

где: `field` – поле, по которому будет произведена фильтрация (см. таблицу 17 и таблицу 18),

`operation` – операция для произведения сравнения по выбранному полю с эталоном (см. таблицу 18),

`etalon` – эталонное значение выбранного поля, по которому будет произведено сравнение в соответствии с выбранной операцией.

Параметры фильтрации протокола IKE SA приведены в таблице19.

Таблица 17 – Параметры фильтрации протокола IKE SA

Параметр	Характеристика
`type`	Тип создания SA
`mode`	Режим создания SA
`role`	Роль локальной машины при создании SA
`state`	Состояние IKE SA
`eapid_local`	Локальный EAP ID
`ikeid_local`	Локальный IKE ID
`eapid_remote`	EAP ID партнера
`ikeid_remote`	IKE ID партнера
`id_remote`	ID партнера
`rule_name`	Имя правила
`algcipher`	Алгоритм шифрования
`alghash`	Алгоритм хэширования
`dhgroup`	DH группа
`algintegrity`	Алгоритм контроля целостности

Параметр	Характеристика
algprf	Псевдослучайная функция
local_ip	IP-адрес локального компьютера, использованный при создании защищенного соединения
local_port	UDP-порт на локальном компьютере, использованный при создании защищенного соединения
peer_ip	IP-адрес партнера, с которым создано защищенное соединение
peer_port	UDP-порт партнера, с которым создано защищенное соединение
redirect_ip	IP компьютера, с которого произошло перенаправление на данный
peer_auth_method	Метод аутентификации партнера
auth_method	Метод аутентификации локальный
cookie	IKEv1 SA cookie
spi	IKEv2 SPI
log_level	Уровень регистрации событий
features	Список поддерживаемых опций

Параметры фильтрации протокола IPsec SA приведены в таблице 18.

Таблица 18 – Параметры фильтрации протокола IPsec SA

Тип	Характеристика
idstr	Идентификационный номер
ike_saref_str	Ссылка на IKE SA
ike_id_remote	IKE SA ID партнера
mode	Режим создания SA
role	Роль при создании SA
peer_id	ID партнёра
local_id	ID локальный
peer_ip	IP-адрес партнера
peer_port	UDP-порт партнера
local_ip	IP-адрес локальный
local_port	UDP-порт на локальном компьютере
Ike_cfg_server	IKE CFG адрес, выданный клиенту
dhgroup	DH группа
filter	Фильтр
rule	Правило
ah_proto	(AH) Правило
ah_spi_in	Значение SPI для входящей SA (AH)
ah_spi_out	Значение SPI для исходящей SA (AH)
ah_rekey_spi	Значение SPI для входящей SA, ключи которой были обновлены (AH)
ah_log_level	(AH) Уровень регистрации событий
ah_pmtu	(AH) значение MTU, которое установлено на промежуточном шлюзе
ah_status	(AH) Состояние
ah_auth	(AH) Алгоритм имитозащиты
ah_pkts_decap	AH) Декапсулировано пакетов
ah_bytes_decap	(AH) Декапсулировано байт
ah_pkts_decap_ce	(AH) Ошибки дешифрации (пакетов)

Тип	Характеристика
ah_pkts_decap_ae	(AH) Ошибки аутентификации (пакетов)
ah_pkts_decap_re	(AH) Ошибки атак воспроизведения (пакетов)
ah_pkts_decap_tl	(AH) Ошибки ограничения трафика (пакетов)
ah_pkts_decap_oe	(AH) Прочие ошибки декапсуляции (пакетов)
ah_pkts_encap	(AH) Инкапсулировано пакетов
ah_bytes_encap	(AH) Инкапсулировано байт
ah_pkts_encap_ce	(AH) Ошибки шифрации (пакетов)
esp_proto	(ESP) Правило
esp_spi_in	Значение SPI для входящей SA (ESP)
esp_spi_out	Значение SPI для исходящей SA (ESP)
esp_rekey_spi	Значение SPI для входящей SA, ключи которой были обновлены (ESP)
esp_log_level	(ESP) Уровень регистрации событий
esp_pmtu	(ESP) значение MTU, которое установлено на промежуточном шлюзе
esp_status	(ESP) Состояние
esp_transform	(ESP) Алгоритм шифрования
esp_auth	(ESP) Алгоритм имитозащиты
esp_orig_peer_ip	(ESP) Исходный адрес партнера
esp_orig_local_ip	(ESP) Исходный адрес данного компьютера
esp_pkts_decap	(ESP) Декапсулировано пакетов
esp_bytes_decap	(ESP) Декапсулировано байт
esp_pkts_decap_ce	(ESP) Ошибки дешифрации (пакетов)
esp_pkts_decap_ae	(ESP) Ошибки аутентификации (пакетов)
esp_pkts_decap_re	(ESP) Ошибки атак воспроизведения (пакетов)
esp_pkts_decap_tl	(ESP) Ошибки ограничения трафика (пакетов)
esp_pkts_decap_oe	(ESP) Прочие ошибки декапсуляции (пакетов)
esp_pkts_encap	(ESP) Инкапсулировано пакетов
esp_bytes_encap	(ESP) Инкапсулировано байт
esp_pkts_encap_ce	(ESP) ошибки шифрации (пакетов)
ipcomp_proto	(IPcomp) Правило
ipcomp_spi_in	Значение CPI для входящей SA (IPcomp)
ipcomp_spi_out	Значение CPI для исходящей SA (IPcomp)
ipcomp_rekey_spi	Значение CPI для входящей SA, ключи которой были обновлены (IPcomp)
ipcomp_log_level	(IPcomp) Уровень регистрации событий
ipcomp_pmtu	(IPcomp) значение MTU, которое установлено на промежуточном шлюзе
ipcomp_status	(IPcomp) Состояние
ipcomp_compression	(IPcomp) Алгоритм сжатия

Таблица 19 – Описание типов операций фильтрации

Команда	Характеристика
Операции для фильтрации по типу обмена	
equal	значение поля равно эталону (значение может быть: mm (Main Mode), am (Aggressive Mode), qm (Quick Mode), ix (Informational), tx (Transaction), для IKEv2: resume, init, auth, child, info)

Команда	Характеристика
not_equal	значение поля не равно эталону
Операции для фильтрации по роли в процессе обмена	
equal	значение поля равно эталону (значение может быть: initiator, responder)
not_equal	значение поля не равно эталону
Операции для фильтрации по содержанию строк	
icontain	поле содержит подстроку (эталон), игнорируя регистр букв
not_icontain	поле не содержит подстроку (эталон), игнорируя регистр букв
contain	поле содержит подстроку (эталон), учитывая регистр букв
not_contain	поле не содержит подстроку (эталон), учитывая регистр букв
iequal	поле равняется эталону, игнорируя регистр букв
not_iequa	поле не равняется эталону, игнорируя регистр букв
equal	поле равняется эталону, учитывая регистр букв
not_equal	поле не равняется эталону, учитывая регистр букв
Операции для фильтрации по полю «IP-адрес»	
inrange	значение поля (IP-адрес) входит в диапазон заданный эталоном, в качестве эталона можно указать просто IP-адрес (10.1.1.1) или диапазон (10.1.1.1...10.1.1.255) или подсеть (10.1.1.0/24 или 10.1.1.0/255.255.255.0)
not_inrange	значение поля (IP-адрес) не входит в диапазон
equal	значение поля (IP-адрес) равно эталону (IP-адрес)
not_equal	значение поля (IP-адрес) не равно эталону (IP-адресу)
Операции для фильтрации по полю IP-порт	
equal	значение поля (порт) равно эталону
not_equal	значение поля не равно эталону
inrange	значение поля входит в диапазон заданный эталоном, в качестве эталона можно указать просто порт (8080) или диапазон (0...65535)
not_inrange	значение поля не входит в диапазон заданный эталоном
Операции для фильтрации по полю уровень лога	
equal	значение поля равно эталону (возможные значения: disabled, events, details, verbose)
not_equal	значение поля не равно эталону
gt	значение поля больше эталона (disabled < events < details < verbose)
lt	значение поля меньше эталона
gteq	значение поля больше или равно эталону
lteq	значение поля меньше или равно эталону

Команда	Характеристика
Операции для фильтрации по IPsec-соединению по полю mode	
`equal`	значение поля равно эталону (возможные значения: tunnel, transport)
`not_equal`	значение поля не равно эталону

В некоторых командных оболочках запрещено использование некоторых символов (например, в BASH '(', ')', '*', кавычки и т.д.), поэтому перед этими символами нужно ставить знак '\', или использовать другие служебные символы данной командной оболочки, или пользоваться другой командной оболочкой.

Для просмотра всех возможных полей и типов операций для фильтрации протоколов IKE и IPsec необходимо воспользоваться командой **`vpnmonitor -i –help`**.

Существует возможность фильтрации списка установленных соединений по ID:

vpnmonitor -i [-view details|list] -ike-id <значение id>

vpnmonitor -i [-view details|list] -ipsec-id <значение id>

ID для IKE SA - это cookie инициатора (как в логе session id). ID для IPsec SA - это целое число, которое было ему присвоено, и которое увеличивается при каждом создании нового SA.

Пример:

`vpnmonitor -i -ike-sa peer_ip equal 10.10.10.97`

`vpnmonitor -i -ike-sa peer_ip equal 10.10.10.97 and role equal initiator`

7.1.2.6 Команды применимые к отфильтрованным SA

Для выполнения команд над отфильтрованными SA предусмотрена опция `–cmd` **`<delete|rekey>:`**

- `delete` – удаляет SA;
- `rekey` – дает команду на смену ключа соединения.

Для удаления всех SA используется команда:

vpnmonitor -i –clearikesa delpmp

`vpnmonitor -i –clearikesa` удаляет все SA, кроме тех, что установлены с сервером-прогрузчиком.

7.1.2.7 Просмотр списка фильтров

Команда **vpnmonitor –f** позволяет просмотреть как статические, так и динамические фильтры, прогруженные в драйвер (список фильтров определяется ЛПБ). Результат вывода данной команды представляет собой табличную структуру со следующими полями, представленными в таблице 22.

Для просмотра определенного фильтра можно воспользоваться опциями фильтрации:

vpnmonitor –f [-view <table|line|list|details|count>] [-filter <…>] [-delay <num>] [-orderby <field> [up] [-tail <num>] [-cmd <delete>],

где: – **view <table|line|list|details|count>** – определяет формат вывода информации:

- `table` – в виде таблицы;
- `line` – в виде строк;
- `list` – в формате параметр – значение, для каждого фильтра;
- `details` – в таблице формата параметр – значение, для каждого фильтра;
- `count` – показывать количество фильтров;
- `-filter` – фильтрация в соответствии с заданным правилом;
- `-orderby <field>` - сортировка по заданному полю;
- `-delay <num>` - вывод команды с задержкой в заданное количество секунд;
- `-tail <num>` - вывод последних <num> строк;
- `-cmd <delete>` - удалить отфильтрованные значения (только для динамических фильтров).

Для задания правил фильтраций следует воспользоваться командой:

vpnmonitor –filter <filtering rules (правило_фильтрации)>].

Правила фильтрации можно объединять с помощью логических операций: `and | or`

`<rule1> <and|or> <rule2> … <ruleN>`, где: `rule1 … N` – правила фильтрации.

Для составления правила фильтрации (параметр <rule1…N>) следует указать поле, по которому будет производиться фильтрация, и операцию для нахождения того или иного фильтра. Формат правила может быть введен следующим образом:

`<field> <operation> <etalon> (<имя_поля> <операция> <эталон>),`

где: `field` – поле, по которому будет произведена фильтрация (см. таблицу 20),

operation – операция для произведения сравнения по выбранному полю с эталоном (см. таблицу 21),

etalon – эталонное значение выбранного поля, по которому будет произведено сравнение в соответствии с выбранной операцией.

Таблица 20 – Параметры фильтрации протокола

Параметр	Характеристика
type	Параметр фильтрации по полю «Тип»
name	Параметр фильтрации по полю «Название»
action	Параметр фильтрации по полю «Действие»
log_level	Параметр фильтрации по полю «Уровень лога»
flags_ttl_str	Параметр фильтрации по времени жизни
comment	Параметр фильтрации по полю «Комментарий»
if-names	Параметр фильтрации по полю «Интерфейс»
srcsel_as_str	Параметр фильтрации по полю «Локальный селектор»
srcsel_ip	Фильтрация поля «Локальный селектор» по IP-адресу
srcsel_port	Фильтрация поля «Локальный селектор» по порту
dstsel_as_str	Параметр фильтрации по полю «Удаленный селектор»
dstsel_ip	Фильтрация поля «Удаленный селектор» по IP-адресу
dstsel_port	Фильтрация поля «Удаленный селектор» по порту
pkt_in	Фильтрация поля «Входящие пакеты»
pkt_out	Фильтрация поля «Исходящие пакеты»
bytes_in	Фильтрация поля «Входящих байт»
bytes_out	Фильтрация поля «Исходящих байт»
drop_in	Фильтрация поля «Входящих байт отброшено»
drop_out	Фильтрация поля «Исходящих байт отброшено»
miss_in	Фильтрация поля «Входящих промахов в кэше»
miss_out	Фильтрация поля «Исходящих промахов в кэше»
fh_count	Фильтрация поля «Записей в кэше»
fwprocs	Параметр фильтрации по полю «Фаервольные процедуры»

Таблица 21 – Описание типов операций фильтрации

Команда	Характеристика
Операции для фильтрации по типу обмена	
equal	значение поля равно эталону
not_equal	значение поля не равно эталону

Команда	Характеристика
Операции для фильтрации по содержанию строк	
icontain	поле содержит подстроку (эталон), игнорируя регистр букв
not_icontain	поле не содержит подстроку (эталон), игнорируя регистр букв
contain	поле содержит подстроку (эталон), учитывая регистр букв
not_contain	поле не содержит подстроку (эталон), учитывая регистр букв
iequal	поле равняется эталону, игнорируя регистр букв
not_iequa	поле не равняется эталону, игнорируя регистр букв
equal	поле равняется эталону, учитывая регистр букв
not_equal	поле не равняется эталону, учитывая регистр букв
Операции для фильтрации по полю уровень лога	
equal	значение поля равно эталону (возможные значения: disabled, events, details, verbose)
not_equal	значение поля не равно эталону
gt	значение поля больше эталона (disabled < events < details < verbose)
lt	значение поля меньше эталона
gteq	значение поля больше или равно эталону
lteq	значение поля меньше или равно эталону
Операции для фильтрации по полю IP-адрес	
contain	значение поля (IP-адрес) содержит эталон (IP-адрес)
not_ contain	значение поля (IP-адрес) не содержит эталон (IP-адрес)
Операции для фильтрации по полю IP-порт	
contain	значение поля (порт) содержит эталон
not_ contain	значение поля не содержит эталон
Unsigned int operation	
equal	значение поля равно эталону (возможные значения: disabled, events, details, verbose)
not_equal	значение поля не равно эталону
gt	значение поля больше эталона (disabled < events < details < verbose)
lt	значение поля меньше эталона
gteq	значение поля больше или равно эталону
lteq	значение поля меньше или равно эталону

Пример:

```
vpnmonitor -f -view list -filter srcsel_ip not_contain test1 or name not_contain test2 and fh_count lt test3
```

Таблица 22 – Отображаемые параметры информации о действующих фильтрах

Имя поля	Описание поля
id	Идентификатор фильтра
Name	Название фильтра
Action	Действие фильтра
Log level	Уровень журналирования

Пример вывода команды `vpnmonitor –f`:

```
id      Name                        Action      Log level
1       autopass ike                PASS        Disabled
2       autopass broadcast in       PASS        Disabled
3       autopass broadcast out      PASS        Disabled
4       filt4 (ONE_BREQ)            APPLY       Disabled
```

Существует возможность поиска фильтра по его ID:

vpnmonitor -f [-view details|list] -id <значение id>

<id> – идентификационный номер фильтра, позволяет просмотреть подробную информацию о выбранном фильтре.

7.1.2.8 Просмотр статистики ike-cfg

Команда vpnmonitor –ike-cfg позволяет просмотреть информацию об установленных соединениях с использованием протокола IKE-CFG. Результат вывода данной команды представляет собой строку с данными, представленными в таблице 23.

Таблица 23 – Отображаемые параметры информации о действующих соединениях на основе IKE-CFG

Параметр	Характеристика
`ip`	Выделенный адрес
`ike_idref`	Идентификационный номер соединения
`ike_id_remote`	IKE ID первой фазы партнера
`peer_ip`	IP-адрес партнера
`status`	Текущий статус выделенного адреса
`request_time_str`	Дата и время запроса адреса
`free_time_str`	Дата и время освобождения адреса
`rule_name`	Правило IKE CFG

Пример вывода команды `vpnmonitor –ike-cfg`:

```
     192.168.21.30    (DN)    CN=ZASTAVA-Client    [3FF4381E8440F4F8]
10.10.10.226    Allocated    2024.02.11    16:57:52    rule_isakmp34:
192.168.21.30..192.168.21.40 IKE-CFG addrs count 1
```

7.1.2.9 Просмотр статистики RRI

В ПО существует возможность просмотреть таблицу с маршрутами. RRI (Reverse Route Injection) – это протокол для управления топологией VPN и системой маршрутизации, позволяющий маршрутам к удаленным защищенным подсетям и клиентам, автоматически принимать участие в процессе маршрутизации. После создания защищенного соединения IPsec SA в таблицу маршрутизации ПО с включенным RRI автоматически вносится запись о маршруте к удаленной сети партнера или клиенту. При нарушении защищенного соединения добавленный маршрут из таблицы маршрутизации ПО удаляется.

Команда **vpnmonitor –rri [-view <line|list|table|details|count>] [-show <vpn|sys|all>] [-filter<…>]** позволяет просмотреть системный журнал маршрутизации и маршрут к удаленной сети партнера или клиенту.

Описание значений параметра `view`:

– `view line` – показывать информацию по маршруту в виде строк;

– `view table` – показывать информацию по маршруту в виде таблицы;

– `view list` – показывать всю информацию по маршруту в формате параметр-значение;

– `view details` – показывать всю информацию по маршруту в таблице формата «параметр: значение».

Описание значений параметра `show`:

– `show vpn` – показывать только маршрут для IPsec;

– `show sys` – показывать только системную таблицу маршрутизации;

– `show all` - показывать все маршруты.

Описание значений параметра `filter`:

– для настройки фильтрации использовать команду:

`vpnmonitor –rri –filter –h`.

7.1.3 Утилита tcping

Утилита предназначена для проверки сетевой доступности по протоколу TCP.

tcping [ключ] <host> <port>

без ключа	Выполнить команду tcping на <IP-address> и порт назначения <port>
ключ -q	Тихий режим, нет вывода, за исключением вывода ошибок
ключ -t	Задать таймаут в секундах

ключ -u	Задать таймаут в микросекундах

7.1.4 Утилита arping

Утилита предназначена для проверки доступности объектов на канальном уровне.

arping [ключ/опция] < dns name or ip address>

без опций	Выполнить команду arping на <dns name or ip address >
опция -c <количество>	Задать количество пакетов
опция -w <таймаут>	Задать таймаут в секундах
опция -i <interval>	Задать таймаут в секундах
опция -I <device>	Выбор интерфейса
опция -s <source ip address>	Задать источник ip address в пакетах
ключ -f	Выход при первом ответе
ключ -q	Тихий режим
ключ -b	Не использовать unicast
ключ -D	Режим обнаружения дубликатов адресов
ключ -U	Режим инициативных ARP-пакетов используется для обновления ARP-кэша соседа
ключ -A	Режим ответов ARP
ключ -V	Отображение версии

7.2 Обзор средств конфигурирования

Для конфигурирования ПО в части функционала межсетевого экранирования и виртуальных частных сетей (FW, VPN) используются следующие средства:

- утилита vpnconfig;
- утилита plg_ctl;
- утилита icv_checker (используется для проверки КС);
- команды программной составляющей ПО.

7.2.1 Утилита vpnconfig

Утилита конфигурирования **vpnconfig** предназначена для изменения и просмотра локальных установок ПО. При штатной работе ПО изменение локальных установок обычно не требуется, и управление производится централизованно путем внесения изменений в ЛПБ.

Некоторые изменения вступают в силу только после того, как будет перезагружена ЛПБ.

7.2.1.1 Справочная система по работе с утилитой

Для получения справки по работе утилиты командной строки необходимо ввести

команду **vpnconfig –h**.

Справка о конкретной команде: **vpnconfig -help <команда>**.

Справка о конкретной команде и типе объектов: **vpnconfig -help <команда> <тип объекта>**.

Также существует возможность получить подробную справку с примерами и описанием команд, для этого ввести команду: **vpnconfig –h all**.

7.2.1.2 Просмотр информации о ПО

Для получения информации о ПО необходимо воспользоваться командой:

vpnconfig -ver

7.2.1.3 Работа с сертификатами и ключами

7.2.1.3.1 Свойства сертификата и его проверка

Для просмотра всех свойств сертификата необходимо узнать id сертификата, для этого надо выполнить команду: **vpnconfig –list cert**. Затем выполнить команду: **vpnconfig –view cert <id>**.

Будет выведена полная информация о свойствах сертификата, а также выведена его *цепочка доверия*, т.е. список данных из удостоверяющего центра (УЦ), подтверждающих подлинность сертификата. Обычно нет необходимости проверять сертификат вручную, поскольку после получения сертификата от партнёра по связи через протокол IKE, сертификат всегда проверяется автоматически. Однако, ручная проверка сертификата полезна, когда возникают проблемы при создании защищенного соединения с данным партнёром связи.

Описание всех свойств сертификата представлено в таблице 24.

Таблица 24 – Свойства сертификата

Свойство	Описание
Version	Версия формата сертификата
Серийный номер	Серийный номер сертификата
Issuer	Кем выдан сертификат
Subject	Содержит отличительное имя субъекта, то есть владельца закрытого ключа, соответствующего открытому ключу данного сертификата.
Sign Algorithm	Алгоритм цифровой подписи сертификата
Key Algorithm	Тип открытого ключа (алгоритм цифровой подписи и длина)
Public Key	Значение открытого ключа
Действителен с	Начальная дата действия сертификата

Свойство	Описание
Действителен до	Конечная дата действия сертификата
Authority Key Identifier	Идентификатор ключа издателя, помогает определить правильный ключ для верификации подписи на сертификате
Subject Key Identifier	Идентификатор ключа субъекта, используется для того, чтобы различать ключи подписи в сертификатах одного и того же владельца
Key Usage	Назначение ключа
Ext. Key Usage	Расширенное назначение ключа
CRL Distribution Points	Точки распространения СОС, указанные в данном сертификате. Для каждой точки распространения отображается следующая информация: DP[N] "<DP Value>", CRLI[N] "<Issuer Value>", где: – N – номер точки распространения; – <DP Value>- месторасположение точки, где можно получить СОС; – <Issuer Value>- имя организации, выпустившей СОС
Authority Info Access	Способ доступа к информации УЦ
Fingerprint (md5)	Хэш-сумма сертификата, вычисляемая по алгоритму md5
Fingerprint (sha1)	Хэш-сумма сертификата, вычисляемая по алгоритму sha1

Пример вывода *цепочки доверия* сертификата:

```
.-+- E=info@cryptopro.ru,C=RU,O=CRYPTO-PRO,CN=Test Center
CRYPTO-PRO
  .--- C=RU,L=Moscow,O=ELVIS-PLUS,OU=TC,CN=CLIENT-LINUX
```

7.2.1.3.2 Регистрация сертификата

Можно регистрировать несколько типа X.509 сертификатов*:*

- доверенные сертификаты самоподписанные;
- доверенные сертификаты промежуточные;
- сертификаты с ключом (personal)
- сертификаты партнёров по связи (other).

Для работы с сертификатами требуется обеспечить доступ к контейнеру ключевой информации. Для этого необходимо:

1) выполнить команду **`vpnconfig list token`**, найти в появившемся списке токен `ELVIS-PLUS CSP token` и запомнить его ID по умолчанию 0;
2) выполнить команду vpnconfig login token <token_id> <pin> save,

   где:

   `<pin>` – пин код пользователя к токену (по умолчанию 12345678),

   `<token_id>` - ID для `ELVIS-PLUS CSP token`

ключ `save` нужен для автологина в токен после перезапуска;

3) следует убедится, что вход в токен `ELVIS-PLUS CSP token` осуществлён, пин-код сохранён и датчик случайных чисел проинициализирован (см. подчёркнутые свойства).

```
 #vpnconfig –list token
Token
  Id: 0
  Label: ELVIS-PLUS CSP token
  Model: InternalCrypto
  Manufacturer: ELVIS-PLUS
  Serial Number: 18042017
  Logged In: YES, PIN-code saved
  Trusted: Yes
  Login required: Yes
  RNG: Initialized
  Algorithms:
    GOST R 34.10-2001
      Key Length: 512
      Hash Algorithms: GOST 34.11-94
    GOST R 34.10-2012 512
      Key Length: 1024
      Hash Algorithms: GOST 34.11-2012 512
    GOST R 34.10-2012 256
      Key Length: 512
      Hash Algorithms: GOST 34.11-2012 256
```

Чтобы зарегистрировать новый сертификат УЦ или промежуточный сертификат УЦ в ПО необходимо произвести следующие действия:

1) выполнить команду **`vpnconfig add cert <file>`**
2) при импортировании сертификата необходимо ввести SO PIN-код (пин код администратора) токена (по умолчанию 12345678). После ввода PIN-кода нужно нажать клавишу <Enter>; в случае ввода корректного PIN-кода и пароля появится следующее сообщение, сигнализирующее об успешной регистрации сертификата:

```
Certificate is imported
```

Чтобы импортировать новый персональный сертификат необходимо произвести следующие действия:

1) выполнить команду: **vpnconfig add cert <path> password [<password>]**, где: **[<password>]** – пароль доступа к PKCS#12 контейнеру;
2) в случае ввода корректного PIN-кода появится следующее сообщение, сигнализирующее об успешной регистрации сертификата:

```
Password OK.
Certificate is imported.
```

7.2.1.3.3 Удаление сертификата

Для удаления сертификата из необходимо узнать id сертификата, который необходимо удалить. Для этого нужно воспользоваться командой **vpnconfig list cert**. После этого необходимо выполнить команду:

vpnconfig remove cert <id>.

При удалении сертификата требуется ввод пользовательского пин-кода. Для удаления доверенных сертификатов потребуется ввод пин-кода администратора токена.

7.2.1.3.4 Создание запроса PKCS10 на выпуск сертификата

Для создания запроса на выпуск сертификата используются встроенные возможности ПО. Для создания запроса необходимо указать носитель, на котором будет создан ключевой контейнер.

Общий вид команды выглядит следующим образом:

vpnconfig -add request <token_id> <key_algorithm> <key_length> <hash_algorithm> <subject> [ip=<ip-address>] [dns=<dns>] [email=<e-mail>] [upn=<upn>] [eku=ipsec|sclogin] [noexport].

Параметры, заключенные в прямоугольные скобки, кроме eku=ipsec, которой необходимо указывать всегда, не являются обязательными. Описание параметров представлено в таблице 25.

Таблица 25 – Описание параметров команды vpnconfig -add request

Ключ	Описание действия
token_id	Указать используемый токен
key_algorithm	Указать используемый алгоритм
key_length	Указать длину ключа
hash_algorithm	Указать используемый хэш алгоритм
subject	Указать информацию о владельце сертификата: C= Country Code, ST=State, L=Locality, O=Organization, OU=Organizational Unit, T=Title, CN=Common Name
<ip-address> <dns>	Опциональные поля AltSubjectName

Ключ	Описание действия
<e-mail> <upn>	
eku	Указать область использования сертификата «IKE/IPsec» или «Smart Card Login»
noexport	Указать возможность экспорта сертификата
cms	Сгенерировать запрос на подпись в формате cms
signer	Указать субъект сертификата. Если параметр не указан, то будет использоваться значение из локальных настроек

Для просмотра доступных в системе токенов (InternalCrypto, ESMARTToken GOST, Rutoken ECP) и поддерживаемых алгоритмов (см. подчёркнутые свойства) необходимо ввести команду: **vpnconfig list token**.

```
Token
  Id: 0
  Label: ELVIS-PLUS CSP token
  Model: InternalCrypto
  Manufacturer: ELVIS-PLUS
  Serial Number: 18042017
  Logged In: Yes, PIN-code saved
  Trusted: Yes
  Login required: Yes
  RNG: Initialized
  Algorithms:
    GOST R 34.10-2001
      Key Length: 512
      Hash Algorithms: GOST 34.11-94
    GOST R 34.10-2012 512
      Key Length: 1024
      Hash Algorithms: GOST 34.11-2012 512
    GOST R 34.10-2012 256
      Key Length: 512
      Hash Algorithms: GOST 34.11-2012 256

Token
  Id: 1
  Label: Internal
  Model: ESMARTToken GOST
  Manufacturer: ISBC
  Serial Number: 34600EE204084204
  Logged In: No
  Trusted: Yes
  Login required: Yes
  RNG: Initialized
  Algorithms:
    RSA
```

```
            Key Length: 1024
            Hash Algorithms: SHA1, MD5, SHA256, SHA224, SHA384,
SHA512
          GOST R 34.10-2001
            Key Length: 512
            Hash Algorithms: GOST 34.11-94
          ECDSA
            Key Length: 192, 224, 256, 384, 521
            Hash Algorithms: SHA1, SHA256, SHA224, SHA384, SHA512
          GOST R 34.10-2012 256
            Key Length: 512
            Hash Algorithms: GOST 34.11-2012 256
      Token
        Id: 2
        Label: Рутокен ЭЦП 3.0
        Model: Rutoken ECP
        Manufacturer: Aktiv Co.
        Serial Number: 424f84a2
        Logged In: No
        Trusted: Yes
        Login required: Yes
        RNG: Initialized
        Algorithms:
          RSA
            Key Length: 1024, 2048, 4096
            Hash Algorithms: MD5, SHA1, SHA224, SHA256, SHA384,
SHA512
          GOST R 34.10-2001
            Key Length: 512
            Hash Algorithms: GOST 34.11-94
          GOST R 34.10-2012 512
            Key Length: 1024
            Hash Algorithms: GOST 34.11-2012 512
          ECDSA
            Key Length: 192, 224, 256, 384, 521
            Hash Algorithms: SHA1, SHA224, SHA256, SHA384, SHA512
          GOST R 34.10-2012 256
            Key Length: 512
            Hash Algorithms: GOST 34.11-2012 256
```

Примеры команды генерации ключей и запросов на издание сертификата с разной длиной ключа для защищённых соединений:

```
vpnconfig add request 0 "GOST R 34.10-2012 256" 512 "GOST
34.11-2012 256" "C=RU,OU=PO,CN=APK-key256" eku=ipsec
vpnconfig add request 0 "GOST R 34.10-2012 512" 1024 "GOST
34.11-2012 512" "C=RU,OU=PO,CN=APK-key512" eku=ipsec
```

Пример команды генерации ключа и запроса на издание сертификата для входа в ПО на

отчуждаемом носителе «Рутокен ЭЦП 3.0»:

```
vpnconfig add request 2 "GOST R 34.10-2012 256" 512 "GOST
34.11-2012 256" "C=RU,ST=77 Москва,L=Город или населённый
пункт,O=ООО \\\"Имя
организации\\\",OU=Подразделение,GN=Иванов,SN=Иван
Иванович,CN=Администратор ПК,E=user@domain.net" eku=sclogin
upn=admin@localhost
```

Пример дан с заполнением всех возможных полей subject. Количество полей subject может быть сокращено. Для использования в полях кавычек требуется применять знаки экранирования \\\ (три подряд обратные косые черты).

При использовании eku=sclogin поле upn не должно быть пустым. Требования к сертификатам для входа в ПО приведены в подразделе 2.3.

После генерации ключевого контейнера на экране будет отображен BASE64-запрос на выпуск сертификата. Если необходимо сохранить запрос в файл, то необходимо воспользоваться перенаправлением вывода после команды на генерацию (> имя_файла рекомендуемая директория сохранения /home/admin).

```
-----BEGIN CERTIFICATE REQUEST-----
MIICmTCCAkYCAQAwggFAMQswCQYDVQQGEwJSVTEYMBYGA1UECAwPNzcg0JzQvtGB
0LrQstCwMTowOAYDVQQHDDHQk9C+0YDQvtC0INC40LvQuCDQvdCw0YHQtdC70ZHQ
vdC90YvQuSDQv9GD0L3QutGCMS8wLQYDVQQKDCbQntCe0J4gItCY0LzRjyDQvtGA
0LPQsNC90LjQt9Cw0YbQuNC4IjEjMCEGA1UECwwa0J/QvtC00YDQsNC30LTQtdC7
0LXQvdC40LUxFTATBgNVBCoMDNCY0LLQsNC90L7QsjEiMCAGA1UEBAwZ0JjQstCw
0L0g0JjQstCw0L3QvtCy0LjRhzEqMCgGA1UEAwwh0JDQtNC80LjQvdC40YHRgtGA
0LDRgtC+0YAg0JDQn9CaMR4wHAYJKoZIhvcNAQkBFg91c2VyQGRvbWFpbi5uZXQw
ZjAfBggqhQMHAQEBATATBgcqhQMCAiMBBggqhQMHAQECAgNDAARAtUeSOECaj1+U
LNFUma0mJk340WOSOBjDeabeDFkkPu92Pp7EtdCuetvZgmEX5FCNscv6AoO7ewZH
XRY2cPA05qCBlDCBkQYJKoZIhvcNAQkOMYGDMIGAMA4GA1UdDwEB/wQEAwIFoDAV
BgNVHSUEDjAMBgorBgEEAYI3FAICMCoGA1UdEQQjMCGgHwYKKwYBBAGCNxQCA6AR
DA9hZG1pbkBsb2NhbGhvc3QwKwYDVR0QBCQwIoAPMjAyMzA4MzAxMzQxMDVagQ8y
MDI0MTEzMDEzNDEwNVowCgYIKoUDBwEBAwIDQQARQLAc52wTDwayStDSkDLdFEnO
R3sif3EcuCKU3TzhQ5frNQiyP2JYCiQDX5ZT7byC6KBE/ANa7kToQc32GrnE
-----END CERTIFICATE REQUEST-----
```

Пример дан с заполнением всех возможных полей subject. Количество полей subject может быть сокращено Для использования в полях кавычек требуется применять знаки экранирования \\\ (три подряд обратные косые черты).

После создания запроса в базе сертификатов агента безопасности ПО появится запись

```
Certificate
  Id: 0/1
  Type: personal
  Subject: Key Pair without Certificate
  Issuer:
  Device Name: Рутокен ЭЦП 3.0
  Expiration Date: Error time
  Algorithm: GOST R 34.10-2012 256
  Possible Id Types: DN
```

Способ извлечения запроса - использование Secure Copy Protocol (SCP).

После выпуска ключевым или удостоверяющим центром сертификата необходимо импортировать его в ПО для прикрепления сертификата к контейнеру ключевой пары, для этого ввести команду:

vpnconfig add cert <путь_к_сертификату> pin <pin_токена> token <token id>

```
Import certificate 'C=RU,ST=77 Москва,L=Город или населённый пункт,O=ООО\"Имя организации",OU=Подразделение, CN=Администратор ПО , E=user@domain.net'
  to token 'Рутокен ЭЦП 3.0'...
Certificate is imported.
```

7.2.1.3.5 Настройки функции двухфакторной аутентификации

Для тонкой настройки режимов двухфакторной аутентификации применяется команда

vpnconfig set logon <id-parameter>

Таблица 26 – Параметры модуля двухфакторной аутентификации

#	Имя параметра	Псевдоним параметра	Имя
0	Logon on	LOGON_ON	Используется для включения двухфакторной аутентификации на ОС семейства Windows, в ПО не используется, должно быть всегда установлено в false
1	Trusted token	TRUSTED_TOKEN	Используется для определения места хранения доверенного сертификата для проверки цепочки предъявляемого при двухфакторной аутентификации сертификата. Если значение не указано, то используется любой токен.
2	CRL processing	CRL_PROCESSING	Задает режим обработки CRL

#	Имя параметра	Псевдоним параметра	Имя
			0 - Disabled 1 - Enabled, revoke also if CRL not available 2 - Enabled, don't revoke if CRL not available При включения обработки CRL необходимо также включить и настроить службу разрешения DNS имен для обеспечения успешного скачивания CRL.
3	CRL timeout	CRL_TIMEOUT	Таймаут на обращении по URL за CRL для проверки сертификата
4	Store downloaded CRL on token	CRL_STORE_ON_TOKEN	Задает Label токена, на котором сохраняется скачанный CRL. При сохранении CRL на токен предыдущие версии CRL (по полю NextUpdate с тем же issuer) удаляются
5	Command to execute when token removed	TOKEN_REMOVE_CMD	Команда, которая выполняется при извлечении персонального идентификатора
6	Wait token timeout	WAIT_TOKEN_TIMEOUT	Время ожидания ответа токена
7	pkcs11_module	PKCS11_MODULE	Задает имя провайдера или путь к библиотеке. Пустое значение параметра интерпретируется как любой.
8	pkcs11_slotid	PKCS11_SLOTID	Задает идентификатор слота, используемого для двухфакторной аутентификации. Для определения SLOTID необходимо воспользоваться командой vpnconfig -list token verbose (Slot Id). Допустимо использовать префикс «NOT» для инвертирования условия выбора SLOTID. Пустое значение параметра интерпретируется как любой.

7.2.1.3.6 Предварительно распределенные ключи

Предварительно распределённые ключи не могут быть использованы для защиты информации и не рассматриваются в руководстве.

7.2.1.3.7 Списки отозванных сертификатов

Для того, чтобы просмотреть доступные СОС, следует выполнить команду: **vpnconfig list cert crl**. СОС может быть получен динамически в рамках создания

соединения IKE или проверки сертификатов по протоколу HTTP (при наличии в сертификате ссылки на размещение СОС в сети и доступности http-сервера).

```
CRL
  Id: 4/0
  Issuer:        E=kc@elvis.ru,C=RU,ST=Москва,L=Зеленоград,O=АО
ЭЛВИС-ПЛЮС,CN=КЦ ЭЛВИС-ПЛЮС (ГОСТ 2012)
  Device Name: http://crl.zastava.ru/elvis.crl
  Last Update: 25.08.2023 13:40:11
  Next Update: 02.09.2023 02:00:11
  Algorithm: STREEBOG256/GOST R 34.10-2012 256
```

СОС, полученный в рамках создания соединения IKE, либо проверки сертификатов после перезапуска службы агента безопасности или рестарата ПО, не сохраняется в базе данных сертификатов.

СОС, полученный в рамках проверки сертификата при двухфакторной аутентификации, сохраняется в локальной БД агента безопасности.

7.2.1.3.8 Импортирование СОС вручную

Можно в любое время вручную импортировать СОС. Процесс импорта тот же самый, что и при регистрации сертификата. Чтобы зарегистрировать СОС в ПО, необходимо выполнить команду, аналогичную импорту сертификата **vpnconfig add cert <file>**.

7.2.1.4 Работа с настройками ЛПБ

Для просмотра доступных политик необходимо выполнить команду:

vpnconfig list lsp

Вывод результата выполнения данной команды будет содержать список ЛПБ и их параметры, а также состояние ЛПБ.

7.2.1.4.1 Настройка параметров политик ПО

7.2.1.4.1.1 Системная ЛПБ

Системная политика может быть получена из файла, с сервера или соответствовать «Политике драйвера по умолчанию».

Для ПО запрещается устанавливать параметр «Системная политика» в значение прогрузки политики из файла.

Для настройки системной политики необходимо:

1) при выборе метода прогрузки из файла необходимо выполнить команду: **vpnconfig set lsp system file <path>,**

где: **path** – путь к файлу политики безопасности;

2) при выборе метода прогрузки с сервера по PMP необходимо выполнить команду: **vpnconfig set lsp system pmp <cert_id> <id_type> <server_ip>|<server_name> <log level> [<timeout>]],**

где:

cert_id – идентификатор сертификата; для просмотра id сертификата можно воспользоваться командой **vpnconfig list cert personal**;

<id_type> – тип идентификатора для прогрузки политики, который должен быть согласован с ЦУП. Идентификатор IKE бывает нескольких видов: DN, DNS, E-mail, IP. DN – использование данных о субъекте импортированного сертификата. Для использования альтернативного имени субъекта (которое указывается в сертификате) необходимо выбирать оставшиеся три типа идентификатора IKE – DNS, E-mail, IP;

<server_ip>|<server_name> – адрес сервера прогрузки|имя компьютера и порт. Если порт не указан, то берется значение по умолчанию (500). Если серверов несколько, IP-адреса указываются через запятую. Номер порта указывается через двоеточие;

<log level> – уровень журналирования событий;

<timeout> – временной промежуток между обращениями к серверу;

3) при выборе метода прогрузки с сервера по HTTP необходимо выполнить команду: **vpnconfig set lsp system http <server> <login> [password] [log level] [timeout],**

где:

<server> – адрес сервера прогрузки;

<login> – логин для прогрузки политики, который должен быть согласован с ЦУП;

<password> – пароль для прогрузки политики, который должен быть согласован с ЦУП;

<log level> – уровень журналирования событий;

<timeout> – временной промежуток между обращениями к серверу;

4) при отсутствии необходимости прогрузки следует выполнить команду: **vpnconfig set lsp system none**, тогда в случае ошибки при прогрузке системной политики, будет прогружаться «Политика драйвера по умолчанию».

Вместе с настройками параметров политики возможна одновременная активации. Для этого применяется префикс -active. **vpnconfig activate lsp . . .**

7.2.1.4.1.2 Политика драйвера по умолчанию

В агенте безопасности имеется простая политика обработки трафика, которая используется при отсутствии (или недоступности) рабочей ЛПБ - «Политика драйвера по умолчанию» (Default Driver Policy, DDP).

DDP вступает в силу при запуске агента безопасности ПО, до момента загрузки рабочей ЛПБ в случае, если произошла ошибка при прогрузке политики или остановлен сервис vpndmn.

Для изменения параметров «Политика драйвера по умолчанию» необходимо выполнить команду: **vpnconfig set lsp ddp pass|drop|dropall.**

Для настройки параметров политики и ее активации можно воспользоваться одной командой: **vpnconfig activate ddp [pass|drop|dropall]**.

Из соображений безопасности необходимо устанавливать «Политика драйвера по умолчанию» в значение «Сбрасывать все» (`dropall`). Следует учесть, что в этом случае получение политики будет невозможно, если компьютеру не присвоен статический IP-адрес. Если компьютер получает IP-адрес по DHCP, то следует выбрать опцию «Сбрасывать все, кроме DHCP» (`drop`). В этом случае сеть будет недоступна до момента активации рабочей ЛПБ (исключение составляет только трафик DHCP, необходимый для назначения компьютеру IP-адреса).

7.2.1.4.2 Использование в качестве прогрузчика

Для того чтобы использовать ПО в качестве промежуточного прогрузчика политики безопасности для других объектов (например, другого ПО или клиентов), необходимо выполнить команду:

vpnconfig set jk HTTP_URI http://<server ip>:3118/distributor/,

где: **<server ip>** – IP-адрес ЦУП, с которого прогрузчик получает политику безопасности.

7.2.1.4.3 Активация ЛПБ

Для активации системной политики необходимо воспользоваться командой:

vpnconfig activate lsp system

7.2.1.4.4 Просмотр текущей ЛПБ

С помощью утилиты **vpnconfig** можно произвести просмотр текущей ЛПБ, для этого необходимо выполнить команду **vpnconfig -view lsp current**.

7.2.1.5 Файл регистрации событий

Записи о регистрируемых системных событиях хранятся в файле `bin_log.txt` в директории `/var/vpnagent/log/`.

Для чтения информации из файла `bin_log.txt` может использоваться утилита `vpnconfig` в следующем формате:

`vpnconfig -view log [nocase] [<filter>],`

где `[nocase]` – фильтрация без учета регистра,

`<filter>` может быть:

- `session <IKE session>` - фильтр по сессии IKE;
- `exchange <IKE exchange>` - фильтр по обмену IKE;
- `level <level>` - фильтр по уровню (INFO, WARN, ERROR, NOTICE);
- `source <source>` - фильтр по источнику;
- `text <text>` - фильтр по полному тексту в любой колонке;
- `sub <text>` - фильтр по подстроке в любой колонке;
- `last <count>` - показать count последних строк.

Конфигурирование регистрации событий происходит с помощью команды **`vpnconfig -set log`**, параметры команды представлены числами от 0 до 13 (см. таблицу 27).

Таблица 27 – Параметры команды **`vpnconfig –set log`**

#	Имя псевдонима	Псевдоним	Расшифровка
0	`Log Level`	`LOG_LEVEL`	Уровень регистрации событий
1	`Log Level kernel`	`LOG_LEVEL_KERNEL`	Уровень регистрации событий для уровня драйвера
2	`File Log`	`FILELOG_ON`	Включение или отключение параметра записи системных событий в файл
3	`Max Log Size`	`MAX_LOG_SIZE`	Установка максимального размера файла записи системных событий
4	`Backup Depth`	`BACKUP_DEPTH`	Установка количества создаваемых резервных копий файла записи системных событий
5	`SysLog`	`SYSLOG_ON`	Включение или отключение параметра записи системных событий на syslog-сервер
6	`Encoding from`	`ENCODING_FROM`	Выбор алгоритма кодировки для открытия журнала событий
7	`Encoding to`	`ENCODING_TO`	Выбор алгоритма кодирования

#	Имя псевдонима	Псевдоним	Расшифровка
			сообщений записи системных событий
8	Facility	FACILITY	Настойка уровня протоколирования Syslog
9	Language	LANGUAGE	Установка языка журналирования
10	Broadcast messages to terminals from vpndmn	WALL_ON	Широковещательные сообщения терминалам от службы *ЗАСТАВА-Офис*
11	Debug mode for application level	VERBOSE_MODE_ON	Установить отладочный уровень регистрации событий для уровня приложения
12	Debug mode for kernel level	VERBOSE_MODE_ON_KERNEL	Установить отладочный уровень регистрации событий для уровня драйвера
13	Remove new line symbols from messages	SYSLOG_SINGLELINE	Удалять символы новой линии из сообщений
14	Expand LSP filters	EXPAND_LSP_FILTERS	Удалять символы новой линии из сообщений

Для включения или отключения функции записи системных событий в файл необходимо выполнить команду: **vpnconfig -set log 2 <value>, где: <value> - 1/0/on/off/true/false/Enabled/ Disabled**.

Уровень регистрации событий может быть установлен командой **vpnconfig -set log 0 (Log Level) <0 (Disabled), 1 (Events), 2 (Details), 4 (Verbose)>**. Доступны следующие значения для уровня регистрации событий (в порядке от наименьшего количества информации к наибольшему):

— заблокирован (disabled) – события не будут регистрироваться;

— события (event) – будет регистрироваться минимальное количество информации об операциях, а также все сообщения об ошибках;

— подробный (details) – будет регистрироваться полная информация об операциях (для поиска неисправностей);

— отладочный (verbose) – все события будут зарегистрированы; уровень используется, в основном, для отладки.

Запрещено использовать уровень регистрации событий «Заблокирован (Disabled»).

Предусмотрено архивированное хранение файлов журнала.

Чтобы установить максимальный размер файла, необходимо выполнить команду:

vpnconfig set log MAX_LOG_SIZE <value>

Когда размер файла превысит заданное значение, текущий файл будет переименован в файл с именем bin_log_0000000000.bak (с увеличением номера для последующих файлов резервного хранения), после чего будет начат новый файл.

Для задания количества создаваемых резервных копий необходимо выполнить команду:

vpnconfig set log 4 <value>

Для установки языка журналирования необходимо выполнить команду:

vpnconfig set log 9 <value>

Возможные значения <**value**>: 0 – английский, 1 – русский.

Некоторые параметры уровней регистрации хранятся также в ЛПБ, созданной для ПО.

7.2.1.6 Параметры журнала Syslog

ПО позволяет настроить регистрацию событий с помощью системного журнала Syslog. При этом syslog-сервер может находиться как на локальном, так и на удалённом компьютере.

Для включения или отключения параметра записи системных событий на syslog-сервер необходимо выполнить команду:

vpnconfig set log 5 <value>,

где: `<value>` может быть `1/0/on/off/true/false/Enabled/ Disabled`.

Для выбора алгоритма кодировки сообщений необходимо выполнить команду **vpnconfig set log 7 <value>**, где: `<value>` - алгоритм кодировки сообщений, возможные значения: KOI8-R, DOS-866, Win-1251, UTF-8.

Для настройки уровня протоколирования Syslog необходимо выполнить команду:

vpnconfig set log 8 <value>,

где: `<value>` - одно из значений от 0 до 7.

Для удаления символов конца строки из сообщений Syslog необходимо выполнить команду:

vpnconfig set log 13 ON

Для задания адреса syslog-сервера необходимо отредактировать файл

/etc/rsyslog.conf, добавив строку local0.err @<адрес сервера>.

7.2.1.7 Протокол IKE

С помощью утилиты vpnconfig можно выполнить настройку для протокола IKE. Все параметры для этих протоколов изменяются и просматриваются одинаково:

1) для просмотра настроек протокола надо выполнить команду:

   vpnconfig –list <ike>

2) для изменения настроек протокола надо выполнить команду:

   vpnconfig –set <ike> <id-parameter> <value>

3) для установки параметра в значение по умолчанию необходимо выполнить команду:

   vpnconfig –reset <ike> <id-parameter>

7.2.1.7.1 Параметры протокола IKE

Протокол IKE является протоколом управления ключами. IKE подтверждает подлинность IPsec-партнёров и организует вторичные IPsec-соединения. Параметры IKE приведены в таблице 28.

Таблица 28 – Параметры протокола IKE

#	Имя	Псевдоним	Назначение
0	Allow IPsec over TCP	IKETCP_ENABLED	Разрешает использовать TCP инкапсуляцию для IKE и ESP (по умолчанию включено)
1	Use mixed transport mode	MIXED_TRANSPORT_MODE	Управление смешанным транспортным режимом (когда IKE работает по TCP, а ESP – по IP (или UDP). OFF – не использовать (по умолчанию) ALWAYS – всегда использовать AUTO – использовать только при больших сообщениях IKE
2	Time to complete exchange (sec)	EXCHANGE_TIMEOUT	Максимальное время для создания защищенного соединения (SA). (5-600, по умолчанию 60). Это таймаут на обращение по URL за CRL сертификатом.
3	Shortened time to complete exchange	SHORT_EXCHANGE_TIMEOUT	Укороченное время для завершения обмена (3-60, по умолчанию 5)
4	Max half-open states	MAX_HALFOPEN	Максимальное количество IKE соединений в процессе создания SA, в которых нет подтверждения IP-адреса партнера (0-256, по

#	Имя	Псевдоним	Назначение
			умолчанию 64). Если количество запросов от неподтвержденных IP-адресов превышает этот параметр, то дальнейшие действия зависят от версии протокола IKE. Для IKEv1 любой новый запрос игнорируется. Для IKEv2 любой новый запрос также игнорируется, но при этом запускается процедура подтверждения IP-адреса. Эта процедура заключается в отправке инициатору специального значения – COOKIE, которое тот должен вернуть. SA при этом не создается. Если запрос посылался с несуществующего IP-адреса, то COOKIE инициатором получено не будет и, соответственно, не будет возвращено. Если же адрес был реальным, то инициатор повторно посылает запрос, включая в него COOKIE. Такие запросы считаются ответчиком подтвержденными и минуют проверку на превышение описываемого параметра
5	Initiate no more exchanges	WNDSIZE_INITIATOR	Максимальное количество параллельных обменов (1–16, по умолчанию – 4), которые могут быть инициированы в рамках одной IKE SA. Если система посылает больше запросов, то они будут ожидать завершения какого-либо из активных обменов. Данный параметр актуален только для IKEv1.
6	Respond to no more exchanges	WNDSIZE_RESPONDER	Максимальное количество параллельных обменов, которые данный хост готов принимать в качестве ответчика в рамках одной IKE SA (1–16, по умолчанию – 4). Для IKEv2 этот же параметр (но заданный у партнера) будет определять максимальное количество параллельных обменов, которые могут быть инициированы

#	Имя	Псевдоним	Назначение
			данным хостом в рамках одной IKE SA
7	Honor puzzles	SOLVE_PUZZLES	Разрешает инициатору реагировать на паззлы (решать их) (по умолчанию включено)
8	Puzzles policy	PUZZLES_POLICY	Управляет отсылкой паззлов на ответчике: NEVER – не посылать (по умолчанию) ALWAYS (INIT only) – всегда отсылать, но только в IKE_SA_INIT ALWAYS (INIT and AUTH) – всегда отсылать в IKE_SA_INIT и в IKE_AUTH Under attack – отсылать, если идет атака на ответчик [не реализовано]
9	Puzzles difficulty (bits)	PUZZLES_DIFFICULTY	Сложность паззлов (0-31, по умолчанию 16)
10	Servers selecting policy	SERVERS_POLICY	Политика выбора серверов (по умолчанию – Try servers sequencially)
11	Try to re-use existing SA's IP for new SAs	TRY_USE_EXISTING_IP	При создании новых IKE SA сначала пробовать адреса уже существующих IKE SA с данным ответчиком.
12	NAT traversal policy	NATT_POLICY	Политика выбора метода работы через NAT (по умолчанию 1 – Автовыбор) допустимые значения 0 – Disabled 1 – Autodetect 65 – Start from NAT-T port 129 – Forced UDP Encapsulation 193 – Start from NAT-T port & force UDP encapsulation
13	Redirect client if number of SA exceeds	REDIRECT_INIT	Перенаправлять инициатора если превышено число IKE SA на шлюзе (0-2^31, по умолчанию 0)
14	Redirect authenticated client if number	REDIRECT_AUTH	Перенаправлять аутентифицированных инициаторов если превышено

#	Имя	Псевдоним	Назначение
	of SA exceeds		число IKE SA на шлюзе (0-2^31, по умолчанию 0)
15	Redirect to (with 25% probability)|	REDIRECT_TO_1	IP адрес другого шлюза, куда перенаправлять инициатора
16	Redirect to (with 25% probability)	REDIRECT_TO_2	IP адрес другого шлюза, куда перенаправлять инициатора
17	Redirect to (with 25% probability)	REDIRECT_TO_3	IP адрес другого шлюза, куда перенаправлять инициатора
18	Redirect to (with 25% probability)	REDIRECT_TO_4	IP адрес другого шлюза, куда перенаправлять инициатора
19	Don't redirect redirected client in Initial exchange	RDRFROM_PASS_TO_AUTH	Не перенаправлять инициатора, которого уже ранее был перенаправлен (по умолчанию включено)
20	Sending unprotected error notifications	ERRNTF_POLICY	Управляет отсылкой незащищенных уведомлений об ошибках: NEVER – не отсылать 1 – не более 1/сек 10 – не более 10/сек (по умолчанию для клиента) 100 – не более 100/сек (по умолчанию для сервера) 1000 – не более 1000/сек (по умолчанию для клиента) ALWAYS – без ограничения
21	IKE v2 fragmentation	IKE2_FRAGMENTATION	Управление режимом фрагментации (IKEv2) (по умолчанию – Auto) 0 – Disabled 1 – Auto 2 – Always
22	IKEv2 SA lifetime jitter	IKE2_LIFETIME_JITTER	Рандомизация времени жизни IKE SA (IKEv2) (по умолчанию включена)
23	IKEv2 Resumption	RESUMPTION_ENABLED	Рандомизация времени жизни IKE SA (IKEv2) (по умолчанию включена)
24	MOBIKE	MOBIKE_ENABLED	Управляет поддержкой режима возобновления IKE SA (Resumption) (по умолчанию включен)
25	QCD Secret	QCD_SECRET	Ключ для выработки токена для

#	Имя	Псевдоним	Назначение
			метода Quick Crash Detection (по умолчанию отключен). На всех узлах кластера значение ключа должно быть одинаковое, сгенерированное на одном узле значение необходимо применить для всех узлов кластера
26	DPD Idle Time (sec)	DPD_IDLE_TIME	Интервал обнаружения что партнёр перестал отвечать (0-600, по–умолчанию 30)
27	Active DPD Idle Time (sec)	ADPD_IDLE_TIME	Интервал обнаружения что партнёр перестал отвечать со стороны сервера (0-7200, по умолчанию 300)
28	NAT Keep alive interval (sec)	NATKA_INTERVAL	Интервал в секундах для отправки UDP пакета для поддержания трансляции на NAT устройстве (1-60, по умолчанию 20)
29	IPsec SA provision traffic (KB)	IPSEC_PROV_TRAFFIC	Запас трафика IPsec, по достижении которого запускается процесс обновления ключей (0-16384, по умолчанию 2048)
30	IPsec SA removal delay (sec)	IPSEC_DELAYED_DELETE_IN_SA	Задержка до удаления IPsec (по умолчанию – 5)
31	IPsec SA anti-replay window	IPSEC_ANTI_REPLAY_WINDOW	IPSec размер окна для подавления атак воспроизведения (по умолчанию 64). Возможные значения: 32, 64, 128, 264, 512, отключено
32	TFC Padding	IPSEC_TFC_PADDING	Параметр, контролирующий использование Traffic Flow Confidentiality - методов, разработанных для скрытия/маскировки шаблона трафика для предотвращения атак с анализом статистического трафика. Параметр включен при значении On, выключен при значении Off. Параметр работает только при условии, что он включен на обоих партнерах
33	LDAP cache	IPSEC_LDAP_CACHE	Политика кэширования списка пользователей полученных с LDAP сервера: OFF – отключен;

#	Имя	Псевдоним	Назначение
			SOFT – мягкий режим; HARD – жесткая
34	IPsec SA try to use multicore crypto	IPSEC_MULTICORE	Использование режима multicore: OFF – не использовать ON – использовать (по умолчанию) On use multicore bundle – использовать multibundle
35	Save SAs on LSP reload	SAVE_SA_ON_RELOAD_LSP	Сохранение SA при перезагрузке ЛПБ (по умолчанию выключено)
36	Initiate Persistent IPsec SAs on LSP reload	PERSISTENT_SA	При включенном режиме на каждое IPSec правило в политике создается ike и ipsec sa при перегрузке политики (по умолчанию – false)
37	IKE-CFG most long unused address	IKECFG_MOST_UNUSED	Параметр, контролирующий использование IKE-CFG
38	IKE-CFG auto route	IKECFG_AUTO_ROUTE	При старте системы в LINUX необходимо вызывать команду: ip rule add from all lookup <table id>, где: <table id> – номер таблицы, который задан в локальных настройках (RRI table id), в противном случае те маршруты, которые прописываются в таблицу с номером <table id>, система не видит. Пример команды: ip rule add from all lookup 111 Для удаления правила нужно вызвать команду: ip rule del table <table id>
39	Reverse Route Injection	RRI	Параметр, контролирующий использование Reverse Route Injection
40	Route Injection Table Id	RRI_TABLE_ID	Название таблицы для сохранения информации о маршрутизации (по умолчанию 111)
41	CRL processing	CRL_PROCESSING	Параметр, регулирующий режимы обработки CRL (по умолчанию 0). Возможные значения:

#	Имя	Псевдоним	Назначение
			— - Disabled (Выключена) (используется по умолчанию); — - Enabled, revoke also if CRL not available (Включена, отзывать, если CRL недоступен); — - Enabled, don't revoke if CRL not available (Включена, не отзывать, если CRL недоступен).
42	CRL timeout	CRL_TIMEOUT	Время ожидания получения CRL (0-600, по умолчанию 0) Если параметр равен 0 – то время ожидания CRL определяется параметром IKE #2 Time to complete exchange

Некоторые дополнительные параметры протокола IKE хранятся в ЛПБ, создаваемой для ПО.

7.2.1.7.2 Маршрутизация IKE-CFG

Протокол IKE CFG используется для того, чтобы передать внутренний IP-адрес и другие данные сетевой конфигурации на удаленный клиент виртуальной частной сети (ВЧС), как часть предварительного согласования по протоколу IKE. Это помогает избежать маршрутизации ответных пакетов удаленному клиенту ВЧС с локального сервера; также это используется для того, чтобы выделять трафик, поступающий от аутентифицированных удаленных пользователей, и затем применять к нему фильтрацию, используя локальный пул IP-адресов вместо общих Интернет-адресов. Если данный шлюз безопасности требует конфигурирования удаленных Хостов Безопасности/пользователей через IKE-CFG, присваивая им IP-адреса в пространстве IP-адресов, расположенном за шлюзом безопасности, можно отразить это в конфигурации ЦУП, создавая Правила IKE-CFG.

Для включения автоматической маршрутизации IKE-CFG в ПО необходимо выполнить команду: **`vpnconfig set ike IKECFG_AUTO_ROUTE true`**

7.2.1.7.3 RRI

Для включения RRI необходимо выполнить команду **vpnconfig –set ike RRI true.**

В поле «Reverse Route Injection Table Id» задается название таблицы для сохранения информации о маршрутизации (по умолчанию 111, название можно посмотреть при помощи команды: **vpnconfig –list ike**). Для изменения названия таблицы необходимо выполнить команду: **vpnconfig –set ike RRI_TABLE_ID <название>**.

7.2.1.7.4 Описание режимов обработки CRL

В локальных настройках в группе параметров IKE находится параметр CRL_PROCESSING, который служит для управления режимами обработки CRL (далее СОС – список отозванных сертификатов).

Для просмотра значения этого параметра с помощью утилиты командной строки нужно выполнить команду: **vpnconfig –l ike |grep 'CRL processing'**.

Для изменения значения этого параметра с помощью утилиты командной строки нужно выполнить команду: **vpnconfig –s ike CRL_PROCESSING <id-parameter>**. В зависимости от выбранного значения id-parameter, обработка СОС будет производиться в режимах, приведенных в таблице 29.

Таблица 29 – Режимы работы обработки СОС

Числовое значение	**Режим работы обработки СОС**
0	Disabled. Обработка СОС выключена. Поиск и проверка СОС не производятся

Числовое значение	Режим работы обработки COC
1	`Enabled, revoke also if CRL not available.` Обработка COC включена, при этом, если COC не доступен, сертификат будет считаться отозванным. Обработка осуществляется следующим образом: — если в сертификате нет поля CDP (CRL Distribution Points), то поиск и проверка COC для него не производится; — если поле CDP есть, делается попытка загрузить COC, если по данному CDP COC не был загружен ранее, или наступило время обновления ранее загруженного COC; — если COC не удалось загрузить или в процессе загрузки произошла ошибка, в локальной базе (токены, способные хранить COC) ищется COC, соответствующий эмитенту (issuer) сертификата; — если COC получить не удалось, или у полученного COC наступило время обновления (COC истек) считается, что сертификат отозван; — если получен действительный COC, в нем ищется серийный номер сертификата, если номер найден, то считается, что сертификат отозван. Для каждого загружаемого COC проверяется подпись с помощью эмитента сертификата, для которого загружается COC. Если проверка подписи не прошла, COC не используется
2	`Enabled, don't revoke if CRL not available.` Обработка COC включена, при этом, если COC не доступен, считается, что сертификат не отозван. Обработка осуществляется следующим образом: — если в сертификате нет поля CDP (CRL Distribution Points), то поиск и проверка COC для него не производится; — если поле CDP есть, делается попытка загрузить COC, если по данному CDP COC не был загружен ранее, или наступило время обновления ранее загруженного COC; — если COC не удалось загрузить или в процессе загрузки произошла ошибка, в локальной базе (токены, способные хранить COC) ищется COC, соответствующий эмитенту (issuer) сертификата; — если COC получить не удалось, считается, что сертификат не отозван; — если получен COC, в нем ищется серийный номер сертификата, если номер найден, то считается, что сертификат отозван. Для каждого загружаемого COC проверяется подпись с помощью эмитента сертификата, для которого загружается COC. Если проверка подписи не прошла, COC не используется

Таймаут при загрузке COC определяется значением параметра Time to complete exchange (sec).

7.2.1.7.5 Политика выбора метода работы через NAT

В зависимости от выбранного числового значения параметра с id = 15 политика может быть следующей, см. таблицу 30.

vpnconfig set ike NATT_POLICY <значение>

Таблица 30 – Варианты политики выбора метода работы через NAT

Числовое значение	Политика
0 – Disabled	Обнаружение NAT запрещено
1 – Autodetect	Обнаружение NAT включено. Метод будет выбран автоматически
65 – Start from NAT-T port	Обнаружение NAT включено. Начинать обнаружение с порта 4500
129 – Forced UDP Encapsulation	UDP инкапсуляция включена принудительно, даже если NAT преобразования отсутствую по трассе прохождения пакетов
193 – Start from NAT-T port & force UDP encapsulation	Начинать обнаружение с порта 4500 и UDP инкапсуляция включена принудительно, даже если NAT преобразования отсутствую по трассе прохождения пакетов

7.2.1.8 Токены

Агенты безопасности позволяет использовать токены как среду транспортировки важной информации (сертификатов, закрытых ключей). ПО поддерживает работу с PKCS#11-совместимыми токенами, для работы необходимо наличие соответствующих динамически подключаемых библиотек.

7.2.1.8.1 Просмотр модулей токенов

Для просмотра всех зарегистрированных модулей токенов необходимо выполнить команду **vpnconfig –list provider**. Вывод результата выполнения данной команды будет содержать информацию обо всех зарегистрированных модулях токенов. Пример вывода:

```
Provider
    Name: Builtin Trusted Module
    Path: softpkcs11-trusted.dll
    Cryptoki Version: 2.20
    Library Version: 2.32
    Manufacturer: ELVIS-PLUS
    Description: Trusted Certificates
    Tokens: 1
    Token: Trusted Certificates token
```

7.2.1.8.2 Добавление модулей токенов

ПО имеет фиксированный набор провайдеров. Добавление модулей не требуется.

7.2.1.8.3 Удаление модуля токена

ПО имеет фиксированный набор провайдеров. Удаление модулей приведёт к неработоспособности.

7.2.1.8.4 Аутентификация на токене

Для того, чтобы токен был доступен, необходимо выполнить команду:

vpnconfig –login token <token_id> <pin> [save],

где:

<token_id> – идентификатор токена или его имя в системе,

<pin> – PIN-код токена,

[save] – необязательный параметр, если его не установить, то ПО будет запрашивать PIN-код при каждом обращении к токену.

Для того, чтобы закончить сеанс работы с токеном, необходимо выполнить команду:

vpnconfig logout token <token_id>.

7.2.1.8.5 Смена PIN-кода токена

Для смены PIN-кода токена следует выполнить команду: **vpnconfig -password token <token_id> <pin> [save]**,

где: **<token_id>** – идентификатор токена или его имя в системе,

<pin> – новый PIN-код токена,

[save] – необязательный параметр, который отвечает за сохранение PIN-кода для дальнейших обращений к токену.

PIN-код может быть изменен только на активном токене (с токеном, который присутствует в системе).

7.2.1.9 Настройка псевдонимов сетевых интерфейсов

С помощью утилиты **vpnconfig** можно выполнить настройку активных интерфейсов. Для просмотра всех зарегистрированных интерфейсов необходимо выполнить команду:

vpnconfig list interface

Для ввода/редактирования идентификатора интерфейса следует выполнить команду и задать псевдоним интерфейса:

vpnconfig set interface <id> alias <alias>,

где: **<id>** – идентификатор интерфейса,

<alias> – новый псевдоним интерфейса.

7.2.2 Утилита icv_checker

Проверить КС можно, запустив утилиту **icv_checker**.

Для получения справки по работе утилиты необходимо выполнить команду:

/opt/ZASTAVAoffice/bin/icv_checker –h

Используется следующий синтаксис:

/opt/ZASTAVAoffice/bin/icv_checker <filelist.hash>

Формат файла с КС должен быть следующий:

filename1(full path)=<hash value (64 chars)>

...

filenameN(full path)=<hash value (64 chars)>

утилита возвращает следующие коды:

0 – OK;

1 – Неправильный параметр запуска;

-1 – некорректная КС в файле;

-2 – иные ошибки.

Для проверки целостности ПО агента безопасности необходимо выполнить команду: **icv_checker filelist.hash**, где: filelist.hash - файл с шаблоном контроля целостности агента безопасности ПО.

Пример выполнения утилиты `icv_checker`:

icv_checker /opt/ZASTAVAoffice/bin/filelist.hash

```
/opt/ZASTAVAoffice/bin/icv_checker
/opt/ZASTAVAoffice/bin/filelist_hash.hash
 Files processed      1
    Changed     Files 0
    NotFound    Files 0
    NotAccessed Files 0
```

В ПО реализован запуск утилиты в автоматическом режиме каждые три часа */3. Для изменения периодичности запуска утилиты необходимо воспользоваться командой в оболочки KLISH в режиме enable:

set cron job

и изменить периодичность запуска скрипта /usr/sbin/regular_check_contorl_sum.sh (см. подчёркнутое).

Формат файла соответствует формату конфигурационного файла стандартной утилиты crontab.

```
* * * * /usr/sbin/sshd_test.sh
1 */3 * * * /usr/sbin/regular_check_control_sum.sh
2 */3 * * * /usr/sbin/check_firmware.sh
1 23 * * * /usr/sbin/logrotate.sh
0 3 * * 7 /usr/sbin/reboot
```

7.2.3 Использование команд программной составляющей и конфигурирование модулей

7.2.3.1 Работа с системными журналами программной составляющей ПО

В ПО запускается ротация системных журналов для защиты от переполнения разделов внутреннего накопителя ПО.

Ротация запускается скриптом *logrotate.sh* по умолчанию один раз в сутки по заданию службой cron.

```
* * * * /usr/sbin/sshd_test.sh
1 */3 * * * /usr/sbin/regular_check_control_sum.sh
2 */3 * * * /usr/sbin/check_firmware.sh
1 23 * * * /usr/sbin/logrotate.sh
0 3 * * 7 /usr/sbin/reboot
```

Для коррекции политики ротации требуется изменение файла */etc/logrotate.conf* .

Очистка системного журнала происходит с использованием команды:

```
cat /dev/null > /var/log/massages
```

7.2.3.2 Конфигурирование модуля vpnpcap

Существует возможность конфигурировать поведение модуля vpnpcap с помощью задания параметров с использованием команды:

vpnconfig –set pcap <id> <value>

Параметры модуля vpnpcap приведены в таблице (см. таблицу 31).

Таблица 31 – Параметры модуля vpnpcap

#	Имя	Псевдоним	Назначение
0	pkt_queue	PKT_QUEUE	Размер очереди пакетов, поступающих на обработку/фильтрацию

#	Имя	Псевдоним	Назначение
1	threads_mask	THREADS_MASK	Битовая маска, определяющая, на каких процессорах будет выполняться код драйвера. По умолчанию - все нули, что означает - на всех, установленных в системе. Если маска отлична от нуля, то установленные биты разрешают выполнение кода драйвера на соответствующих CPU, а сброшенные – запрещают
2	fcache_lines	FCACHE_LINES	Размер кеша фильтров. Кеш фильтров представляет из себя хэш-таблицу, размер задает количество линий в этой таблице. Служит для быстрого поиска фильтров для одинаковых пакетов
3	fcache_icmp	FCACHE_ICMP	Добавлять фильтры в кеш для пакетов с протоколом ICMP, 1 – вкл, 0 – выкл*
4	fcache_always_invalidate	FCACHE_ALWAYS_INVALIDATE	Сбрасывать(инвалидировать) весь кеш фильтров при создании/удалении динамических фильтров, 1 – вкл, 0 – выкл*. Если выключено, то при создании/удалении динамических фильтров будут удалятся из кеша только записи связанные с этими фильтрами
5	diffserv	DIFFSERV	Параметр, отвечающий за включение функции приоритизации трафика на основании поля ToS заголовка IP-пакета. diffserv=1 – приоритизация трафика включена. По умолчанию установлено значение «0»
6	pkt_order	PKT_ORDER	Восстанавливать порядок пакетов после обработки, 1 - вкл, 0 – выкл*
7	pkt_list	PKT_LIST	Добавлять пакеты в очередь на обработку не по одному, а пачками (по 32 штуки), 1 – вкл, 0 – выкл*
8	fwd_pkt_no_queue	FWD_PKT_NO_QUEUE	Обрабатывать проходящие(forward) пакеты без перекладывания в очередь, 1 - вкл*, 0 – выкл.

Также у модуля vpnpcap есть параметр pcap_defcfg, определяющий политику драйвера, действующую во время загрузки программной составляющей с момента загрузки драйвера vpnpcap в оперативную память и до момента запуска службы vpndmn, который может принимать значения:

2 - PASS(default);

1 – DROP (all,except DHCP);

0 – DROP (all);

Для задания параметра pcap_defcfg необходимо выполнить следующие команды:

```
/etc/init.d/S47vpngate stop
/sbin/rmmod vpnpcap
/sbin/modprobe vpnpcap pcap_defcfg=1
/etc/init.d/S47vpngate start
```

Также для изменения параметра приоритизации (`diffserv`) в режиме enable доступна команда:

```
enable
set diffserv 1
```

7.3 Доступные сетевые службы

Список доступных сетевых служб указан в таблице 32.

Таблица 32 – Список доступных сетевых служб

Расположение	Служба	Параметры запуска	Описание
/etc/init.d	S40network	start	Выполняет команду ifup для всех перенастроенных интерфейсов
	S44modem-manager		Запускает менеджер би-стабильных устройств (например, модем)
	S45network-manager		Запускает демон NetworkManager
	S46vpngate_pcap		Запуск сетевого перехватчика пакетов для ПО
	S47vpngate_		Запуск ПО
	S49ntp		Запуск демона точного времени
	S50sshd		Запуск демона SecurityShell
	S59snmpd		Запуск демона Simple Network Management Protocol
	S70keepalived		Запуск демона высокой сетевой доступности keeplived
	S80dhcp-relay		Запуск службы, обеспечивающей ретрансляцию DHCP-пакетов от клиента к серверу
	S80dhcp-server		Запуск службы, обеспечивающей функцию dhcp-сервера
	S46network-down		Выполняет команды networking nmcli networking on|off

Для получения id запущенной службы в ПО необходимо выполнить:

`pidof <имя процесса>`, например, `pidof vpndmn`

Для внепланового завершения процесса необходимо воспользоваться командой:

```
kill –SIGSEGV <id процесса>
```

8 ОПИСАНИЕ КОНФИГУРИРОВАНИЯ В КЛАСТЕРНОМ ИСПОЛНЕНИИ

ПО в кластерном варианте, будучи основным узлом кластера, постоянно синхронизирует состояние активных IKE SA с другими узлами кластера через интерфейс синхронизации.

В случае возникновения события переключения узлов кластера, узел, ставший основным, имеет полную информацию об активных IKE SA и может использовать эти IKE SA для взаимодействия с партнерами кластера, то есть, событие переключения не приводит к необходимости заново создавать IKE SA. Поскольку IPsec SA не синхронизируются, то после переключения узлов кластера, они отсутствуют на узле, ставшем основным, но наличие IKE SA позволяет быстро диагностировать эту ситуацию и создать их заново.

Для работы ПО в составе кластера необходимо произвести следующие настройки:

– оснастить каждую из нод ключевым материалом (для каждой ноды должен использоваться отдельный персональный сертификат с ключом);

– синхронизировать время на всех узлах;

– выполнить настройки ПО «keepalived» и описать виртуальные интерфейсы кластера в файле keepalived.conf;

– выполнить настройки ПО для включения режима синхронизации IKEv2 состояний (см. подраздел 8.2.2).

– описать в ГПБ (см. документацию на ЦУП) объект типа шлюз в кластерном исполнении.

Рассмотрим на примере рис. 10 создание типовой конфигурации кластера:

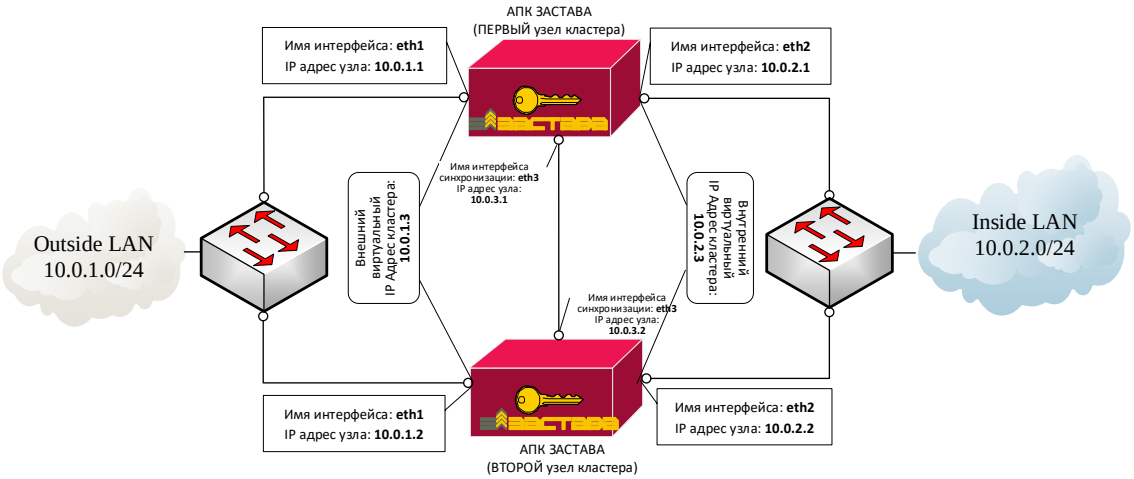

Рисунок 10 – Пример топологии кластера

8.1 Настройка кластера с помощью мастера

Для настройки шлюза в кластерном исполнении можно воспользоваться мастером настройки. Для запуска мастера из оболочки KLISH в режиме enable выполнить команду:

```
# set cluster settings
```

Запустится мастер.

8.1.1 Меню мастера настройки кластера

При запуске мастера будет отображено сообщение:

```
Это мастер автоматизирует настройки ПО в отказоустойчивом
исполнении.
Мастер создаст и применит конфигурации автоматически
(выполнить пункты 1-3).
После настройки этого узла кластера настройки могут быть
переданы на другой узел кластера (выполнить пункт 4).
Переданные настройки на другом узле могут быть применены
мастером без настроек (выполнить пункт 3).
Выберите:
 1.Настроить ПО keepalive
 2.Настроить ПО ЗАСТАВА
 3.Применить настройки ПО
 4.Передать настройки ПО на другой узел по сети
```

```
5.Посмотреть текущие настройки
6.Выход

69.Очистить все настройки
```

Последовательно на узле кластера, который выбран как основной (MASTER), выполняем пункты 1-3, проверка настроек - пункт 5, опционально пункт 4.

Конкретные значения, указанные в руководстве, приведены для примера и соответствуют топологии, см. рис. 10. В тексте диалогов вводимые пользователем сведения выделены жирным текстом.

8.1.1.1 Пункт 1 (настройка keepalive)

При выборе пункта 1 будет отображено сообщение:

```
Выберите:
1
Введите имя интерфейса: eth1
```

Следует ввести имя интерфейса (в примере это eth1).

В случае, если интерфейс будет отсутствовать в ОС, то появится сообщение:

```
Указанный интерфейс не найден в системе
Настройка интерфейсов не выполнена
Нажмите клавишу Enter для продолжения
```

После нажатия Enter будет осуществлён возврат в начальное меню мастера настройки.

Если на выбранном интерфейсе не настроен IP- адрес, мастер предложит задать его.

```
На выбранном интерфейсе отсутствует IP-адрес, хотите задать? (y/n)y
Введите IP-адрес для интерфейса eth1 (в формате A.B.C.D/mask):
10.0.1.1/24
Подключение успешно активировано (активный путь D-Bus: /org/freedesktop/NetworkManager/ActiveConnection/2)
```

Последовательно задать значения запрашиваемого мастером:

```
Введите кластерный IP-адрес/маска виртуального интерфейса кластера eth1 ( в формате A.B.C.D/mask):10.0.1.3/24
Введите номер виртуального роутера (virtual_router_id) (число от 1 до 255):101
Введите приоритет (priority) (число от 1 до 255), рекомендуемое 200):200
Введите пароль для шифрования сообщений синхронизации (не более 8 символов) (auth_pass):12345678
Использовать unicast рекомендуемое значение y)? (y/n)y
Введите IP-адрес другого узла кластера для приёма сообщений синхронизации (в формате A.B.C.D):10.0.1.2
Включить настройку - nopreempt (оставлять резервный узел в активном состоянии в случае если основной узел снова будет в онлайне (рекомендуемое значение y)? (y/n)y
 VI_1  VI_2
Настройка интерфейсов выполнена
Нажмите клавишу Enter для продолжения
```

В случае если формат ввода IP-адрес или IP-адрес/маска не соблюдён, то настройка интерфейсов не будет выполнена. После нажатия клавиши Enter будет осуществлён возврат в начальное меню мастера настройки. Процедуру следует повторить с корректными значениями.

После задания настроек внешнего интерфейса (в примере eth1) следует повторить настройки для внутреннего интерфейса (в примере eth2). Для этого снова требуется выбрать пункт 1.

```
Выберите:
1
```

8.1.1.2 Пункт 2 (настройка ПО в части кластеризации)

При выборе пункта 2 будет отображено сообщение:

```
Выберите:
2
```

Последовательно задать значения, запрашиваемые мастером:

```
Укажите IP-адрес интерфейса синхронизации состояний IKE
10.0.3.1
Укажите IP-адрес интерфейса синхронизации состояний IKE партнера
10.0.3.2
Укажите общий пароль
qwerty123
Parameter 'Cluster Key' was set to 'qwerty123'.
Parameter 'Multicast group' was set to '10.0.3.2'.
Parameter 'Multicast interface' was set to '10.0.3.1'.
Parameter 'Mode' was set to 'Multicast'.
Отказоустойчивый режим успешно включен
Нажмите клавишу Enter для продолжения
```

8.1.1.3 Пункт 3 (применение настроек)

При выборе пункта 3 будет отображено сообщение:

```
Выберите:
3
```

Если в ПО ранее была проведена настройка кластера, будет задан вопрос:

```
Вы хотите перезаписать текущую конфигурацию? (y/n)
y
```

В случае утвердительного ответа, либо отсутствия конфигурации на данный момент, настройки будут применены с сообщением в консоль.

```
Выполняется перезапуск службы
Restarting keepalived:
Stopping keepalived: OK
Starting keepalived: OK
Настройки применены успешно
Нажмите клавишу Enter для продолжения
```

Если на настраиваемом (BACKUP) узле кластера есть настройки, полученные от (MASTER) узла кластера, то пункт меню 3 мастера будет выглядеть следующим образом:

```
3.Применить настройки ПО (* Внимание! загружены настройки сделанные на другом узле)
Выберите:
```

3

Запустится диалог:

```
Вы хотите перезаписать текущую конфигурацию? (y/n)
```

y

```
Есть настройки, переданные с другого узла, применить их? (y/n)
```

y

```
Копирование успешно выполнено
Parameter 'Cluster Key' was set to 'qwerty123'.
Parameter 'Multicast group' was set to '10.0.3.1'.
Parameter 'Multicast interface' was set to '10.0.3.2'.
Parameter 'QCD Secret' was set to
'1567C05FA35CE5CC91099BB66B778316046CFF55'.
Parameter 'Mode' was set to 'Multicast'.
Проведены настройки ПО ЗАСТАВА для синхронизации состояний IKE
Выполняется перезапуск службы
Restarting keepalived:
Stopping keepalived: FAIL
Starting keepalived: OK
Настройки применены успешно
Нажмите клавишу Enter для продолжения
```

8.1.1.4 Пункт 4 (передача настроек на другой узел)

Мастером предусмотрена возможность автоматизации передачи настроек на второй (BACKUP) узел кластера по сети.

Передача настроек производится по сети. Для возможности передачи узлы кластера должны быть скоммутированы, заданы IP-адреса и должна быть обеспечена сетевая доступность по протоколам SSH/SCP.

```
Выберите:
```

4

Запустится диалог:

```
Введите IP-адрес узла в формате A.B.C.D: 10.0.3.2
Введите имя учетной записи узла:admin
Введите пароль:
```

В случае успешного прохождения аутентификации на второй BACKUP узел будут переданы конфигурации keepalived и ПО для второго (BACKUP) узла кластера.

```
Нажмите клавишу Enter для продолжения
```

8.1.1.5 Пункт 5 (просмотр текущих настроек)

При выборе пункта 5 меню будет отображено сообщение:

```
Выберите:
5
```

В консоли отобразятся сведения о настройках keepalived.

```
Настроено 2 виртуальных роутера(ов)
Интерфейс eth1 | Роутер ID 101 | Приоритет 200 | Виртуальный IP-адрес 10.0.1.3/24
Интерфейс eth2 | Роутер ID 199 | Приоритет 200 | Виртуальный IP-адрес 10.0.2.3/24
_____________________________________________________________
Нажмите клавишу Enter для продолжения
```

8.1.1.6 Пункт 69 (очистка всех настроек)

При выборе пункта 69 меню будет отображено сообщение:

```
Выберите:
69
```

Запустится диалог:

```
ВНИМАНИЕ!!! Все настройки будут удалены! (y/n)
y
```

При утвердительном ответе настройки кластера будут удалены. Режим кластера отключён.

```
Parameter 'Mode' was set to 'Disabled'.
Настройки успешно удалены
Нажмите клавишу Enter для продолжения
```

8.1.1.7 Пункт 6 (выход)

При выборе пункта 6 меню будет отображено сообщение:

```
Выберите:
6
```

Произойдёт возврат в оболочку KLISH.

8.2 Настройка кластера вручную

8.2.1 Ручное редактирование файлов конфигурации

Для настройки keepalived в оболочке BASH:

Скорректировать (текстовым редактором vi, vim, nano, редактором файл менеджера mc) файл `/etc/keepalived/keepalived.conf` следующего содержания.

Пример описания конфигурационного файла с рекомендуемыми параметрами **для первого узла**:

```
global_defs {
# Глобальные настройки для оптимизации логики переключения
узлов
# кластера.

        vrrp_higher_prio_send_advert true
        vrrp_garp_lower_prio_repeat 2
        vrrp_garp_lower_prio_delay 30
        vrrp_garp_master_refresh 60
        vrrp_garp_master_refresh_repeat 2
}
vrrp_sync_group [Имя группы например G1] {
group {
        [имя экземпляра для внешнего интерфейса например
VI_outside]
        [имя экземпляра для внутреннего интерфейса например
         VI_inside]
}
# Скрипт для выполнения перехода в активный режим
        notify_master "/usr/sbin/vrrp.mast"
# Скрипт для выполнения перехода в пассивный режим
        notify_backup "/usr/sbin/vrrp.back"
# Скрипт для выполнения перехода в пассивный режим
        notify_fault "/usr/sbin/vrrp.fault"
}

# Скрипт для отслеживания состояния службы ПО ЗАСТАВА
vrrp_script chk_vpndmn {
        script "killall -0 vpndmn"
        interval 1
        fall 1
        rise 2
}
# Описание экземпляра для внешнего интерфейса например
VI_outside
vrrp_instance VI_outside {
        # Имя внешнего интерфейса
```

```
                interface eth1
                #  Состояние,  в  котором  запускается  первый  узел
кластера
                state MASTER
                priority 200
                #  произвольный  уникальный  номер  от  1  до  255
используется для
                # различения нескольких экземпляров
                virtual_router_id 101
                #  Ключ определяющий поведение не переключать обратно
на
                # другой узел если другой узел вернулся в состояние
                # штатной работы
                nopreempt
                # таймаут анонса в секундах
                advert_int 2
                # определение IP источника unicast пакетов внешнего
                # интерфейса первого узла
                unicast_src_ip 10.0.1.1
                # определение IP назначения unicast пакетов внешнего
                # интерфейса второго узла
                unicast_peer {
                        10.0.1.2
                }
                # аутентификация на пароле
                authentication {
                        auth_type PASS
                # пароль не более 8 символов
                        auth_pass 12345678
                }
                # запуск скрипта для отслеживания состояния службы
                # ПО ЗАСТАВА
                track_script {
                        chk_vpndmn
                }
                #  Определение  виртуального  адреса  и  маски  сети
внешнего
                # интерфейса кластера
                virtual_ipaddress {
                        10.0.1.3/24
                }
        }
        #  Описание  экземпляра  для  внутреннего  интерфейса  например
VI_outside
        vrrp_instance VI_inside {
                # Имя внутреннего интерфейса
                interface eth2
                #  Состояние,  в  котором  запускается  первый  узел
кластера
                state MASTER
                # приоритет узла
                priority 200
```

```
                # таймаут анонса в секундах
                advert_int 2
                #  произвольный  уникальный  номер  от  1  до  255
используется для
                # различения нескольких экземпляров
                virtual_router_id 102
                #  Ключ  определяющий  поведение  не  переключать  обратно
на
                # другой узел если другой узел вернулся в состояние
                # штатной работы
                nopreempt
                # определение IP источника unicast пакетов внутреннего
                # интерфейса первого узла
                unicast_src_ip 10.0.2.1
                #   определение   IP   назначения   unicast   пакетов
внутреннего
                # интерфейса второго узла
                unicast_peer {
                        10.0.2.2
                }
                # аутентификация на пароле
                authentication {
                        auth_type PASS
                # пароль не более 8 символов
                auth_pass 12345678
                }
                # запуск скрипта для отслеживания состояния службы
                # ПО ЗАСТАВА
                track_script {
                        chk_vpndmn
                }
                #  Определение  виртуального  адреса  и  маски  сети
внутреннего
                # интерфейса кластера
                virtual_ipaddress {
                        10.0.2.3/24
                }
        }
```

Пример описания скрипта с рекомендуемыми параметрами **для второго узла** с указанием отличий (**выделено жирным шрифтом**):

```
        global_defs {
        #  Глобальные  настройки  для  оптимизации  логики  переключения  нод
кластера.
                vrrp_higher_prio_send_advert true
                vrrp_garp_lower_prio_repeat 2
                vrrp_garp_lower_prio_delay 30
                vrrp_garp_master_refresh 60
                vrrp_garp_master_refresh_repeat 2
        }

        vrrp_sync_group [Имя группы например G1] {
```

```
group {
        [имя экземпляра для внешнего интерфейса например VI_outside]
        [имя экземпляра для внутреннего интерфейса например
         VI_inside]
}
# Скрипт для выполнения перехода в активный режим
        notify_master "/usr/sbin/vrrp.mast"
# Скрипт для выполнения перехода в пассивный режим
        notify_backup "/usr/sbin/vrrp.back"
# Скрипт для выполнения перехода в пассивный режим
        notify_fault "/usr/sbin/vrrp.fault"
}

# Скрипт для отслеживания состояния службы ПО ЗАСТАВА
vrrp_script chk_vpndmn {
        script "killall -0 vpndmn"
        interval 1
        fall 1
        rise 2
}

# Описание экземпляра для внешнего интерфейса например VI_outside
vrrp_instance VI_outside {
        # Имя внешнего интерфейса
        interface eth1
        # Состояние, в котором запускается второй узел кластера
        state BACKUP
        priority 200
        # таймаут анонса в секундах
        advert_int 2
        # должен быть равен значению для master узла
        virtual_router_id 101
        # Ключ определяющий поведение не переключать обратно на
        # другой узел если другой узел вернулся в состояние
        # штатной работы
        nopreempt
        # определение IP источника unicast пакетов внешнего
        # интерфейса второго узла
        unicast_src_ip 10.0.1.2
        # определение IP назначения unicast пакетов внешнего
        # интерфейса первого узла
        unicast_peer {
                10.0.1.1
        }
        # аутентификация на пароле
        authentication {
                auth_type PASS
        # пароль не более 8 символов
                auth_pass 12345678
        }
        # запуск скрипта для отслеживания состояния службы
        # ПО ЗАСТАВА
        track_script {
                chk_vpndmn
        }
        # Определение виртуального адреса и маски сети внешнего
        # интерфейса кластера
```

```
        virtual_ipaddress {
                10.0.1.3/24
        }
}
# Описание экземпляра для внутреннего интерфейса например VI_outside
vrrp_instance VI_inside {
        # Имя внутреннего интерфейса
        interface eth2
        # Состояние, в котором запускается второй узел кластера
        state BACKUP
        priority 200
        # таймаут анонса в секундах
        advert_int 2
        # должен быть равен значению для master узла
        virtual_router_id 102
        # Ключ определяющий поведение не переключать обратно на
        # другой узел  если другой узел вернулся в состояние
        # штатной работы
        nopreempt
        # определение IP источника unicast пакетов внутреннего
        # интерфейса второго узла
        unicast_src_ip 10.0.2.2
        # определение IP назначения unicast пакетов внутреннего
        # интерфейса первого узла
        unicast_peer {
                10.0.2.1
        }
        # аутентификация на пароле
        authentication {
                auth_type PASS
        # пароль не более 8 символов
        auth_pass 12345678
        }
        # запуск скрипта для отслеживания состояния службы
        # ПО ЗАСТАВА
        track_script {
                chk_vpndmn
        }
        # Определение виртуального адреса и маски сети внутреннего
        # интерфейса кластера
        virtual_ipaddress {
                10.0.2.3/24
        }
}
```

После задания настроек на обоих узлах перестартовать службу keepalive:

```
/etc/init.d/S70keepalived restart
```

8.2.2 Настройка синхронизации состояний IKEv2

Для настройки ПО в режиме кластера (синхронизации состояний IKEv2 между узлами кластера) **для каждого узла кластера** необходимо:

1) включить режим «Multicast» командой `vpnconfig –set ha HA_MODE multicast;`

2) установить одинаковое для всех узлов значение «Ключ кластера» с помощью команды `vpnconfig –set ha KEY <key value>` например 1234567890;

3) Для каждого узла кластера указать адрес интерфейса, который будет использоваться для синхронизации кластерных узлов: `vpnconfig –set ha MULTICAST_ADDRS <ip adr>` (в примере это `10.0.3.1` для master узла и `10.0.3.2` для backup узла);

4) указать порт режима Multicast (любое десятичное целое число) с помощью команды: `vpnconfig –set ha MULTICAST_PORT <value>` (по умолчанию 35476);

5) задать уровень регистрации событий для фильтра Multicast с помощью команды: `vpnconfig – set ha MULTICAST_FILTER_LOGLEVEL <value>` (по умолчанию Events);

6) задать одинаковое для всех узлов значение QCD secret в шестнадцатеричном формате с помощью команды `vpnconfig –set ike QCD_secret <value>`, где `value` – значение от 8 до 20 шестнадцатеричных цифр.

8.3 Настройка маршрутизации при работе с кластером

При использовании в сетевой инфраструктуре кластера ПО необходимо, чтобы в сетевых настройках устройств, которые имеют маршруты через кластер, в качестве шлюза по умолчанию были заданы виртуальные IP-адреса кластера ПО (в примере, данном в этом разделе, это 10.0.1.3 и 10.0.2.3.).

9 ОПИСАНИЕ КОНФИГУРИРОВАНИЯ L2TP СОЕДИНЕНИЯ

Для настройки L2TP-соединения в образе ПО предусмотрен скрипт /sbin/L2_settings.sh. скрипт доступен в командной оболочке BASH.

В результате выполнения команды L2_settings.sh запускается мастер настройки l2-соединения (см. рис. 11).

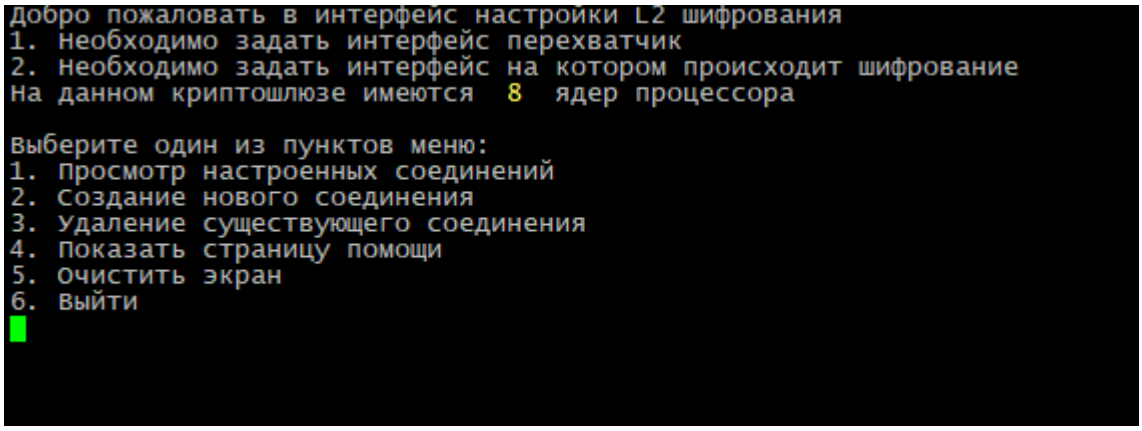

Рисунок 11 - Мастер настройки l2-соединения

Для вызова конкретного пункта меню необходимо нажать на клавиатуре клавишу с соответствующей цифрой и затем нажать клавишу <Enter>.

9.1 Создание нового соединения

Для создания нового соединения необходимо:

1) выбрать пункт меню «2»;
2) указать имя соединения (первые 7 символов в названии соединения должны быть уникальными);
3) указать имя интерфейса перехватчика;
4) указать имя интерфейса шифрования;
5) указать ip-адрес интерфейса шифрования;
6) указать ip-адрес интерфейса шифрования партнера;
7) если предполагается использование настраиваемого соединения в рамках объединения соединений, то необходимо указать имя объединения, в противном случае необходимо нажать клавишу «Enter»;
8) указать количество ядер для соединения;
9) после того, как настройки соединения будут сформированы, будет предложено передать соответствующий конфигурационный файл партнеру. Для передачи необходимо указать имя пользователя и пароль партнера.

Пример создания нового соединения приведен на рис. 12.

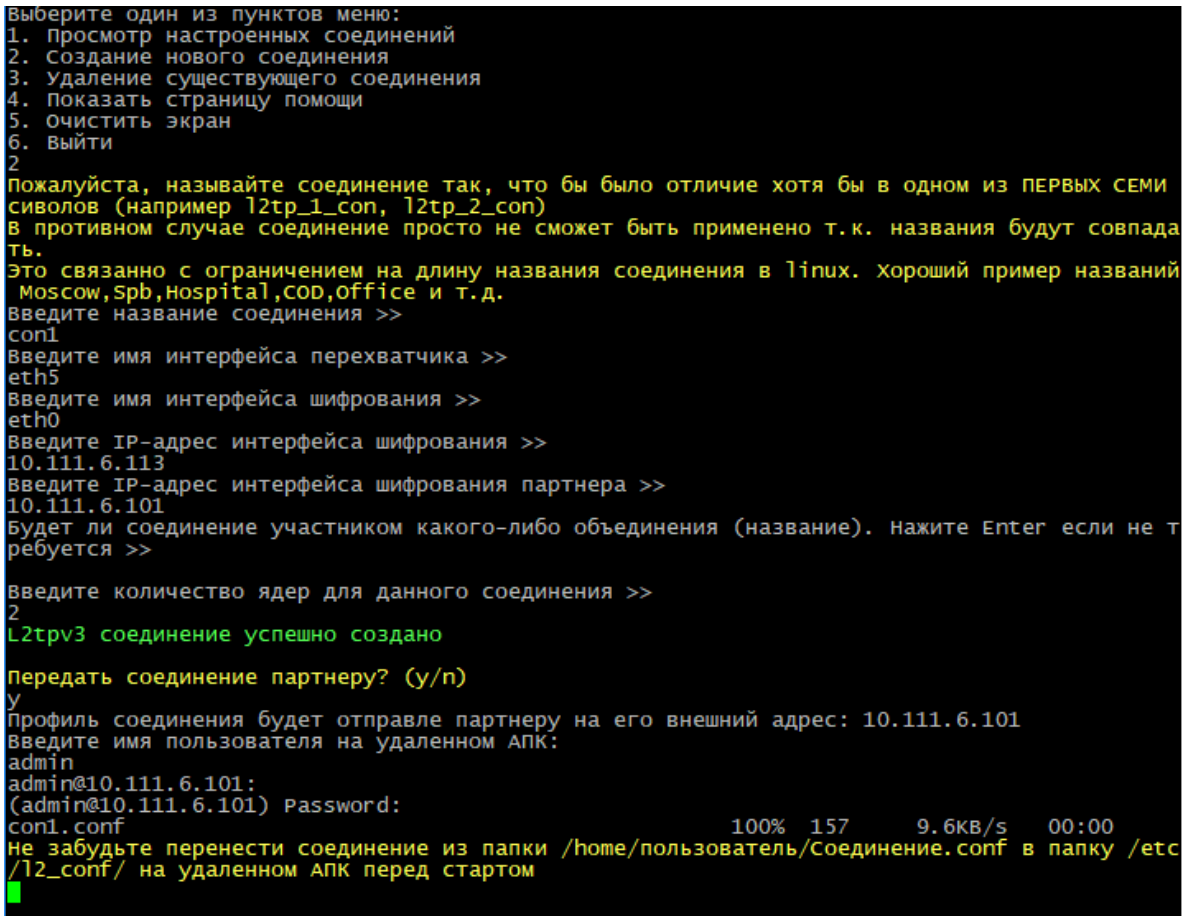

Рисунок 12 – Пример создания l2-соединения

После создания нового соединения в `/etc/l2_conf` создается конфигурационный файл с именем `<имя соединения>.conf`. Конфигурационный файл для партнера создается в `/etc/l2_conf_remote`, имя файла такое же.

```
[root@zastava: /home/admin]# cat /etc/l2_conf/con1.conf
L2_INTERFACE=eth5
TUNNEL_INTERFACE=eth0
IP_ADDRESS=10.111.6.113
IP_ADDRESS_REMOTE=10.111.6.101
MEMBER_OF=
CORES=2
SRC_PORT=20000
DST_PORT=20000
CON_NUM=1

cat /etc/l2_conf_remote/con1.conf
L2_INTERFACE=eth5
TUNNEL_INTERFACE=eth0
IP_ADDRESS=10.111.6.101
IP_ADDRESS_REMOTE=10.111.6.113
MEMBER_OF=
CORES=2
SRC_PORT=20000
DST_PORT=20000
CON_NUM=1
```

После передачи конфигурационного файла партнеру (`/home/admin`) его необходимо перенести в папку `/etc/l2_conf/`. Папку необходимо создать вручную.

9.2 Просмотр созданных соединений

Для просмотра созданного соединения необходимо:

1) выбрать пункт меню «1». Будет отображен список всех настроенных соединений (см. рис. 13);

```
Выберите один из пунктов меню:
1. Просмотр настроенных соединений
2. Создание нового соединения
3. Удаление существующего соединения
4. Показать страницу помощи
5. Очистить экран
6. Выйти
1
Сейчас настроено  2  соединений, вот их список:

con1
con2

Введите название соединения для просмотра или введите ESC для выхода в предыдущее меню
```

Рисунок 13 – Отображение списка соединений

2) ввести имя соединения для просмотра сведений о нем (см. рис. 14);

```
Выберите один из пунктов меню:
1. Просмотр настроенных соединений
2. Создание нового соединения
3. Удаление существующего соединения
4. Показать страницу помощи
5. Очистить экран
6. Выйти
1
Сейчас настроено  2  соединений, вот их список:

con1
con2

Введите название соединения для просмотра или введите ESC для выхода в предыдущее меню
con1
L2_INTERFACE=eth5
TUNNEL_INTERFACE=eth0
IP_ADDRESS=10.111.6.113
IP_ADDRESS_REMOTE=10.111.6.101
MEMBER_OF=
CORES=2
SRC_PORT=20000
DST_PORT=20000
CON_NUM=1
Передать соединение партнеру? (y/n)
```

Рисунок 14 – Отображение сведений о соединении

3) при просмотре сведений о соединении предоставляется возможность передать конфигурационный файл партнеру.

9.3 Удаление соединения

Для удаления соединения необходимо:

1) выбрать пункт меню «3»;

2) список настроенных соединений будет отображен на экране;
3) указать название соединения;
4) подтвердить удаление (см. рис. 15).

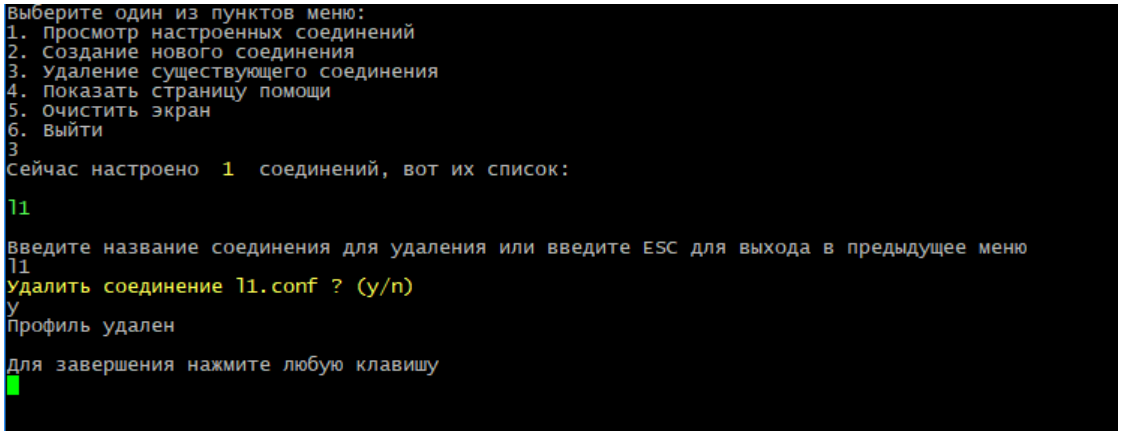

Рисунок 15 – Удаление соединения

9.4 Запуск соединений в соответствии с настройками

Для запуска соединения необходимо выполнить команду:

```
/sbin/L2_create.sh start <имя соединения>
```

В результате успешного выполнения команды выводится сообщение «Соединение <имя соединения> создано». Для просмотра созданного соединения можно воспользоваться командой `ip a` (см. рис. 16).

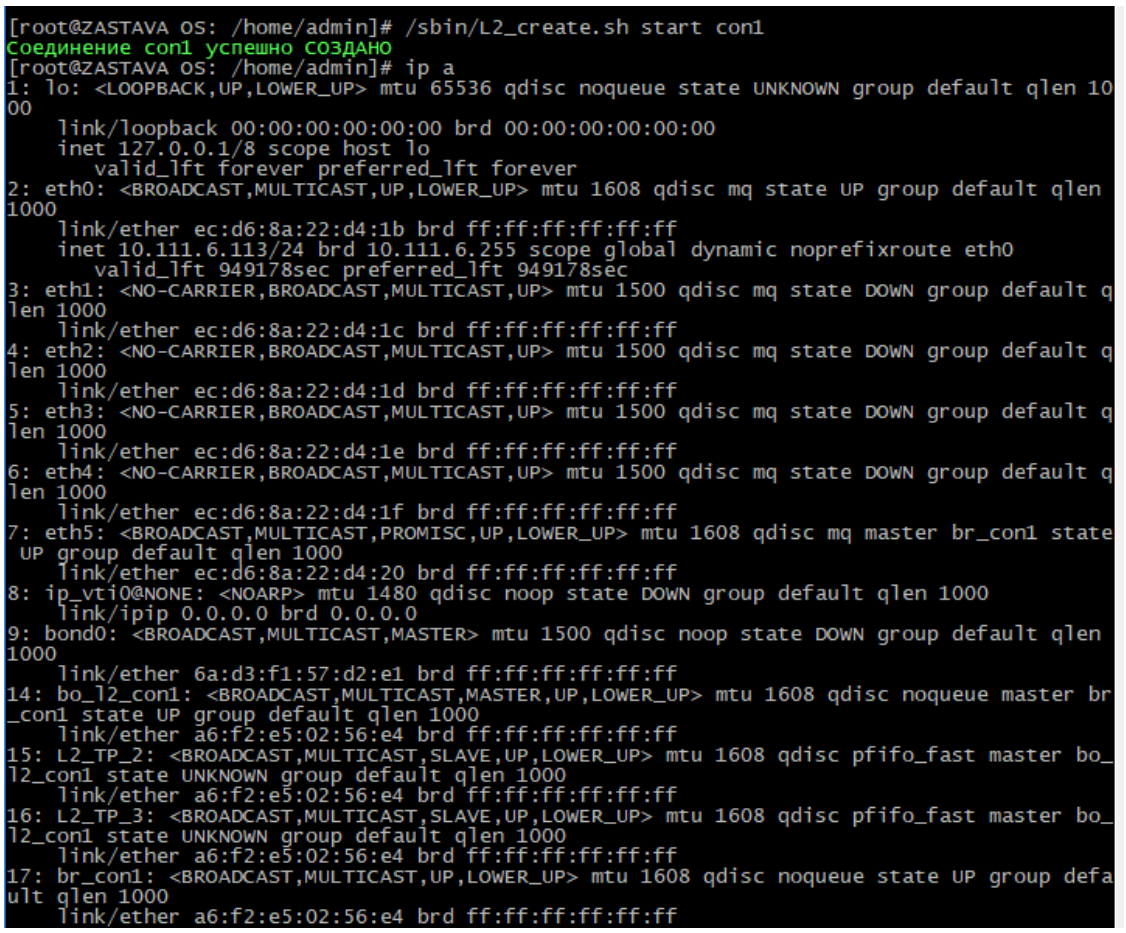

Рисунок 16 – Успешное создание соединения

10 РАБОТА С ДИНАМИЧЕСКОЙ МАРШРУТИЗАЦИЕЙ

10.1 Работа с BGP

В настоящем разделе представлен простой (в части конфигурации сети) сценарий настройки совместного функционирования ПО и двух провайдеров, для связи с которыми используется протокол динамической маршрутизации BGP (eBGP).

В случае недоступности основного канала, BGP обнаруживает данное событие, перестраивает таблицы маршрутизации, и IPsec туннель между площадками автоматически восстанавливается без дополнительных действий со стороны Администратора ПО.

10.1.1 Конфигурация стенда

Ниже приведена схема стенда, на котором будет осуществлена демонстрация работоспособности решения (см. рис. 17).

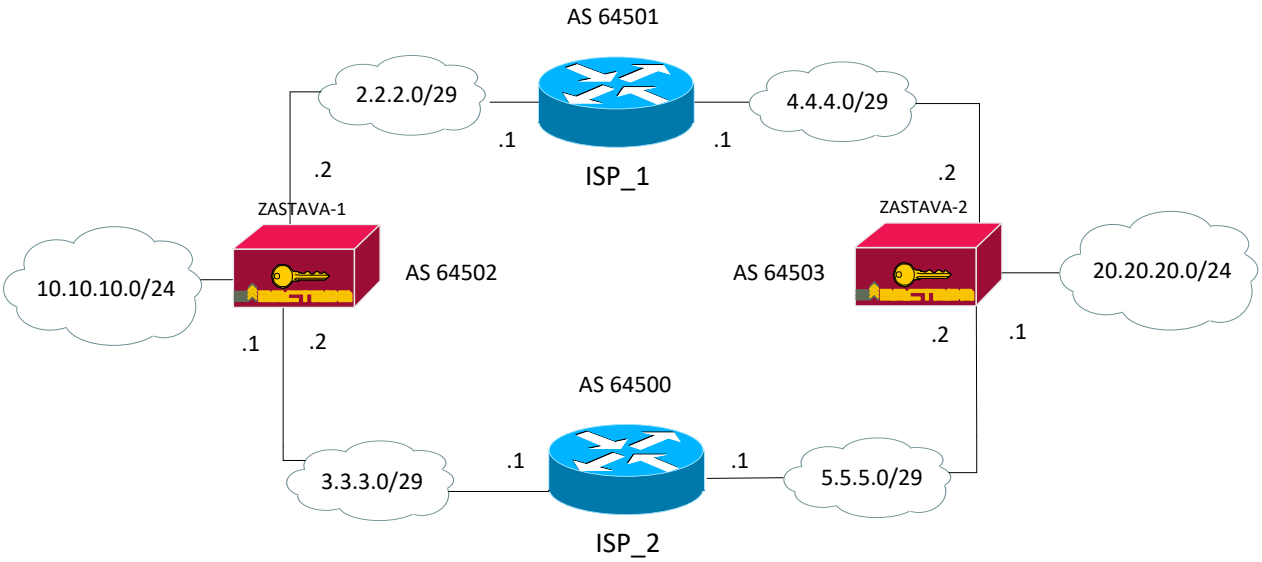

Рисунок 17 – Схема стенда для проверки работы с BGP

10.1.2 Состав ПО участников стенда

В качестве ISP_1 и ISP_2 используются Linux серверы (возможно исполнение в качестве виртуальных машин) и 2 ПК.

Состав ПО участников стенда:

1) ISP_1: ОС ALT Linux, пакет quagga, пакет NetworkManager;
2) ISP_2: ОС ALT Linux, пакет quagga, пакет NetworkManager;
3) ZASTAVA-1: ПК «VPN/FW ЗАСТАВА-150» исполнение ZO8-APK-150;

4) ZASTAVA-2: ПК «VPN/FW ЗАСТАВА-150» исполнение ZO8-APK-150.

10.1.3 Настройка конфигурации

Настройка ISP_1 и ISP_2 производится в командном интерпретаторе BASH.

Настройка ZASTAVA-1 и ZASTAVA-2 производится в командном интерпретаторе KLISH.

Ниже приведены команды для настройки узлов.

10.1.3.1 Настройки узла ISP_1

Для узла ISP_1 выполнить следующие настройки:

1) выполнить настройку интерфейсов командой:
   nmcli connection add type ethernet con-name <имя_соединения> ifname <название_интерфейса> ipv4.addresses <IP-адрес> ipv4.method static autoconnect yes
2) поставить службы zebra и bgpd в автозагрузку командами:
   systemctl enable zebra
   systemctl enable bgpd
3) запустить службы zebra и bgpd командами:
   systemctl start zebra
   systemctl start bgpd
4) выполнить вход в интерпретатор Cisco-Like Sheel командой **vtysh**
5) перейти в режим конфигурации командой **configure terminal**
6) выполнить последовательно команды:
   router bgp 64501
   bgp router-id 2.2.2.1
   network 2.2.2.0/29
   network 4.4.4.0/29
   neighbor 2.2.2.2 remote-as 64502
   neighbor 4.4.4.2 remote-as 64503
7) выполнить выход командой **exit** и затем ещё раз **exit**
8) сохранить конфигурацию командой **write**
9) выполнить выход из интерпретатора Cisco-Like Sheel командой **exit**

10.1.3.2 Настройки узла ISP_2

Для узла ISP_2 выполнить следующие настройки:

1) выполнить настройку интерфейсов командой

nmcli connection add type ethernet con-name <имя_соединения> ifname <название_интерфейса> ipv4.addresses <IP-адрес> ipv4.method static autoconnect yes

2) поставить службы zebra и bgpd в автозагрузку командами:

systemctl enable zebra

systemctl enable bgpd

3) запустить службы zebra и bgpd командами:

systemctl start zebra

systemctl start bgpd

4) выполнить вход в интерпретатор Cisco-Like Sheel командой **vtysh**

5) перейти в режим конфигурации командой **configure terminal**

6) выполнить последовательно команды:

router bgp 64500

bgp router-id 3.3.3.1

network 3.3.3.0/29

network 5.5.5.0/29

neighbor 3.3.3.2 remote-as 64502

neighbor 5.5.5.2 remote-as 64503

7) выполнить выход командой **exit** и затем ещё раз **exit**

8) сохранить конфигурацию командой **write**

9) выполнить выход из интерпретатора Cisco-Like Sheel командой **exit**

10.1.3.3 Настройки узла ZASTAVA-1

Для настройки узла ZASTAVA-1 выполнить следующие настройки:

1) перейти в режим enable командой *enable*

2) выполнить настройку интерфейсов командами

network connection add type ethernet con-name <имя_соединения> ifname <название_интерфейса>

network connection modify <имя_соединения> ipv4.addresses <IP-адрес>

network connection modify <имя_соединения> ipv4.method manual

network connection modify <имя_соединения> autoconnect yes

network connection up <имя_соединения>

3) запустить службу bgpd командой **set BGP on AS 64502**

4) выполнить вход в интерпретатор Cisco-Like Sheel командой

set BGP settings

5) перейти в режим конфигурации командой **configure terminal**

6) выполнить последовательно команды:

router bgp 64502

bgp router-id 10.10.10.1

network 2.2.2.0/29

network 3.3.3.0/29

network 10.10.10.0/24

neighbor 2.2.2.1 remote-as 64501

neighbor 3.3.3.1 remote-as 64500

7) выполнить выход командой **exit** и затем ещё раз **exit**

8) сохранить конфигурацию командой **write**

9) выполнить выход из интерпретатора Cisco-Like Sheel командой **exit**

10.1.3.4 Настройки узла ZASTAVA-2

Для настройки узла ZASTAVA-2 выполнить следующие шаги:

1) перейти в режим enable командой **enable**

2) выполнить настройку интерфейсов командами

network connection add type ethernet con-name <имя_соединения> ifname <название_интерфейса>

network connection modify <имя_соединения> ipv4.addresses <IP-адрес>

network connection modify <имя_соединения> ipv4.method manual

network connection modify <имя_соединения> autoconnect yes

network connection up <имя_соединения>

3) запустить службу bgpd командой **set BGP on AS 64503**

4) выполнить вход в интерпретатор Cisco-Like Sheel командой:

set BGP settings

5) перейти в режим конфигурации командой **configure terminal**

6) выполнить последовательно команды:

router bgp 64503

bgp router-id 20.20.20.1

network 4.4.4.0/29

network 5.5.5.0/29

```
network 20.20.20.0/24
neighbor 4.4.4.1 remote-as 64501
neighbor 5.5.5.1 remote-as 64500
```

7) выполнить выход командой **exit** и затем ещё раз **exit**
8) сохранить конфигурацию командой **write**
9) выполнить выход из интерпретатора Cisco-Like Sheel командой **exit**

10.1.4 Проверка правильности настройки стенда

Стенд считается настроенным правильно, когда выполнены следующие условия:

1) В таблице маршрутов в ПО присутствуют следующие записи:

```
[root@ZASTAVA-1: ~]# ip r
2.2.2.0/29 dev eth1 proto kernel scope link src 2.2.2.2 metric 101
3.3.3.0/29 dev eth2 proto kernel scope link src 3.3.3.2 metric 102
4.4.4.0/29 via 2.2.2.1 dev eth1 proto zebra metric 20
5.5.5.0/29 via 2.2.2.1 dev eth1 proto zebra metric 20
10.10.10.0/24 dev eth3 proto kernel scope link src 10.10.10.1 metric 103
20.20.20.0/24 via 2.2.2.1 dev eth1 proto zebra metric 20
```

```
[root@ZASTAVA-2: ~]# ip r
2.2.2.0/29 via 4.4.4.1 dev eth1 proto zebra metric 20
3.3.3.0/29 via 5.5.5.1 dev eth2 proto zebra metric 20
4.4.4.0/29 dev eth1 proto kernel scope link src 4.4.4.2 metric 101
5.5.5.0/29 dev eth2 proto kernel scope link src 5.5.5.2 metric 102
10.10.10.0/24 via 4.4.4.1 dev eth1 proto zebra metric 20
20.20.20.0/24 dev eth3 proto kernel scope link src 20.20.20.1 metric 103
```

2) Изменение таблицы маршрутизации после перезагрузки роутера:

```
[root@ZASTAVA-1: ~]# ip r
2.2.2.0/29 dev eth1 proto kernel scope link src 2.2.2.2 metric 101
3.3.3.0/29 dev eth2 proto kernel scope link src 3.3.3.2 metric 102
4.4.4.0/29 via 3.3.3.1 dev eth2 proto zebra metric 20
5.5.5.0/29 via 3.3.3.1 dev eth2 proto zebra metric 20
10.10.10.0/24 dev eth3 proto kernel scope link src 10.10.10.1 metric 103
20.20.20.0/24 via 3.3.3.1 dev eth2 proto zebra metric 20
```

```
[root@ZASTAVA-2: ~]# ip r
2.2.2.0/29 via 5.5.5.1 dev eth2 proto zebra metric 20
3.3.3.0/29 via 5.5.5.1 dev eth2 proto zebra metric 20
4.4.4.0/29 dev eth1 proto kernel scope link src 4.4.4.2 metric 101
5.5.5.0/29 dev eth2 proto kernel scope link src 5.5.5.2 metric 102
10.10.10.0/24 via 5.5.5.1 dev eth2 proto zebra metric 20
20.20.20.0/24 dev eth3 proto kernel scope link src 20.20.20.1 metric 103
```

3) Команда ping не прерывается после перезагрузки роутера:

```
[root@ZASTAVA-1: ~]# ping -I 10.10.10.1 20.20.20.1
PING 20.20.20.1 (20.20.20.1) from 10.10.10.1 : 56(84) bytes of data.
64 bytes from 20.20.20.1: icmp_seq=1 ttl=63 time=6.26 ms
64 bytes from 20.20.20.1: icmp_seq=2 ttl=63 time=7.77 ms
64 bytes from 20.20.20.1: icmp_seq=3 ttl=63 time=0.343 ms
64 bytes from 20.20.20.1: icmp_seq=4 ttl=63 time=3.73 ms
64 bytes from 20.20.20.1: icmp_seq=5 ttl=63 time=3.68 ms
64 bytes from 20.20.20.1: icmp_seq=6 ttl=63 time=3.76 ms
```

```
64 bytes from 20.20.20.1: icmp_seq=7 ttl=63 time=3.77 ms
64 bytes from 20.20.20.1: icmp_seq=8 ttl=63 time=3.77 ms
64 bytes from 20.20.20.1: icmp_seq=9 ttl=63 time=3.79 ms
```

10.1.5 Настройка правил шифрования

После проверки правильности настройки стенда, необходимо создать правила доступа между защищаемыми сетями за ZASTAVA-1 и ZASTAVA-2, как это делается для связи «сеть-сеть».

При доступе из сети 10.10.10.0/24 в сеть 20.20.20.0/24 и наоборот, трафик должен шифроваться.

Топология должна повторять приведенную схему, т.е. на ней должны быть созданы неуправляемые шлюзы, представляющие из себя маршрутизаторы ISP_1 и ISP_2 (см. рис. 18).

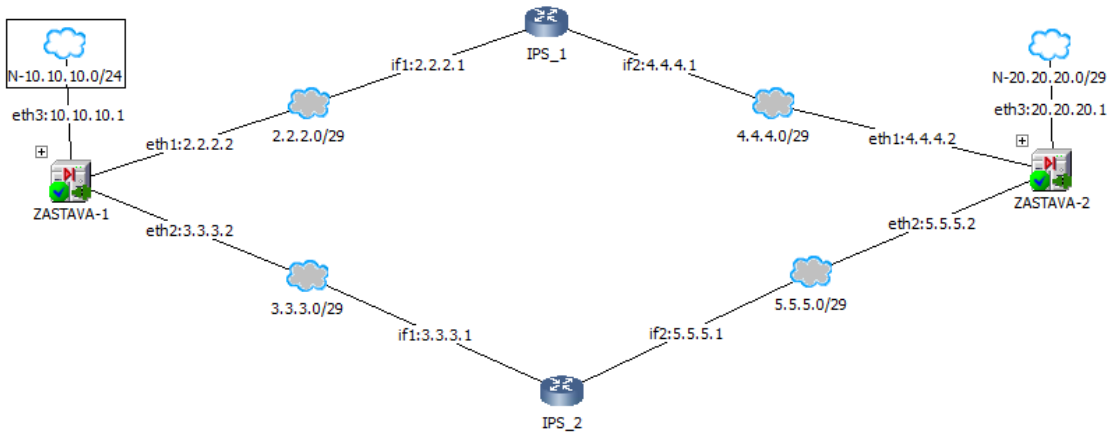

Рисунок 18 – Топология в графической консоли «ЗАСТАВА-Управление»

После создания необходимых объектов и правил необходимо выполнить трансляцию и активацию политик безопасности.

Для проверки возможности доступа между сетями необходимо запустить на ZASTAVA-1 команду **`ping -I 10.10.10.1 20.20.20.1`**.

Затем необходимо убедиться, что взаимодействие осуществляется с использованием шифрования. Для этого необходимо выполнить команду **`vpnmonitor -i`**. В выводе должна присутствовать IPsec-сессия с селекторами сетей *10.10.10.0/24* и *20.20.20.0/24*.

```
[root@ZASTAVA-2: ~]# vpnmonitor -i
A3DC7AF05619E10E.CE03278BBD2A876B       10.111.15.75    (DN) CN=TPN_75  GOST3410.2012(256)-Sig
/ GOST3410.2012(256)-Sig
D42F269AADEAD454.B812863B61D04DEB       3.3.3.2 (DN) OU=GATE,CN=ZASTAVA-1
GOST3410.2012(256)-Sig / GOST3410.2012(256)-Sig
        3       ESP(Tunnel) Responder   20.20.20.0..20.20.20.255 - 10.10.10.0..10.10.10.255
filt_enc_19->rule_ipsec8
IKE states count 2
Ipsec states count 1
```

10.1.6 Проверка работоспособности решения

Для того, чтобы убедиться, что в случае проблем на канале провайдера ISP_1, защищенное взаимодействие между сетями атоматически переключиться на ISP_2, необходимо:

1) Выполнить просмотр параметров туннеля командой **vpnmonitor -i -ipsec-id <id>.**

   Обратить внимание на текущий туннельный адрес партнера:

```
[root@ZASTAVA-2: ~]# vpnmonitor -i -ipsec-id 3
IPsec SA id: 3 (0x3)
IPsec bundle:   ESP(Tunnel) Responder
  ID:   3
  Rule: filt_enc_19->rule_ipsec8
  Selector:     20.20.20.0..20.20.20.7 -- 10.10.10.0..10.10.10.255
  Peer  IP:Port:        3.3.3.2 : 4500
  Local IP:Port:        5.5.5.2 : 4500
  DF bit:       COPY
  Key Exchange: from IKE SA
  IKE SA reference:     D42F269AADEAD454
  IKE SA Remote ID:     (DN) OU=GATE,CN=ZASTAVA-1
ESP:    (#14)
  SPI in/out:   6E0C404D / 471B5781
  Rule: proto_esp14
  Transform:    GOST28147.89DIVER-CTR (ELVIS+ CSP GOST 28147-89 cipher key diversification
CTR) (Multicore)
  Authentication:       GOST28147.89-IMIT (ELVIS+ CSP GOST 28147-89 IMIT)
  Anti Replay Service:  On, window size: 512
  Status:       Active
  Statistics:
    Packets(bytes) encapsulated / decapsulated: 88 (9 152) / 88 (9 152)
    Decrypt errors (packets):   0
    Auth errors (packets):      0
    Reply errors (packets):     0
    Traffic limit errors (packets):     0
    Other decap errors (packets):       0
    Encrypt/Other errors (packets):     0
  Other:
    Created:    2023.09.26 16:25:47
    Life time (sec.):   28713 (28800)
    Expire traffic (kB):        No limits
    Log level:  Events
```

2) Выполнить перезагрузку роутера, через который маршрутизируется трафик;

3) Выполнить команду **vpnmonitor –i** для просмотра текущих IKE/IPsec-сессий. Обратить внимание, что появилась дополнительная IPsec сессия:

```
[root@ZASTAVA-2: ~]# vpnmonitor -i
A3DC7AF05619E10E.CE03278BBD2A876B       10.111.15.75    (DN) CN=TPN_75  GOST3410.2012(256)-Sig
/ GOST3410.2012(256)-Sig
D42F269AADEAD454.B812863B61D04DEB       3.3.3.2 (DN) OU=GATE,CN=ZASTAVA-1
GOST3410.2012(256)-Sig / GOST3410.2012(256)-Sig
        3       ESP(Tunnel) Responder   20.20.20.0..20.20.20.7 -- 10.10.10.0..10.10.10.255
filt_enc_19->rule_ipsec8
9A6CCB9A803AF659.C4A90870C7C033C6       2.2.2.2 (DN) OU=GATE,CN=ZASTAVA-1
GOST3410.2012(256)-Sig / GOST3410.2012(256)-Sig
        4       ESP(Tunnel) Responder   20.20.20.0..20.20.20.7 -- 10.10.10.0..10.10.10.255
filt_enc_16->rule_ipsec7
IKE states count 3
IPsec states count 2
```

4) Выполнить просмотр параметров туннеля командой **vpnmonitor -i -ipsec-id <id>.**

Обратить внимание на изменившийся туннельный адрес партнера:

```
[root@ZASTAVA-2: ~]# vpnmonitor -i -ipsec-id 4
```

```
IPsec SA id: 4 (0x4)
IPsec bundle:   ESP(Tunnel) Responder
  ID:   4
  Rule: filt_enc_16->rule_ipsec7
  Selector:     20.20.20.0..20.20.20.7 -- 10.10.10.0..10.10.10.255
  Peer  IP:Port:        2.2.2.2 : 4500
  Local IP:Port:        4.4.4.2 : 4500
  DF bit:       COPY
  Key Exchange: from IKE SA
  IKE SA reference:     9A6CCB9A803AF659
  IKE SA Remote ID:     (DN) OU=GATE,CN=ZASTAVA-1
ESP:    (#18)
  SPI in/out:   77F5B473 / CF4DA8D5
  Rule: proto_esp14
  Transform:    GOST28147.89DIVER-CTR (ELVIS+ CSP GOST 28147-89 cipher key diversification
CTR) (Multicore)
  Authentication:       GOST28147.89-IMIT (ELVIS+ CSP GOST 28147-89 IMIT)
  Anti Replay Service:  On, window size: 512
  Status:       Active
  Statistics:
    Packets(bytes) encapsulated / decapsulated: 18 (1 872) / 18 (1 872)
    Decrypt errors (packets):   0
    Auth errors (packets):      0
    Reply errors (packets):     0
    Traffic limit errors (packets):     0
    Other decap errors (packets):       0
    Encrypt/Other errors (packets):     0
  Other:
    Created:    2023.09.26 16:27:38
    Life time (sec.):   28782 (28800)
    Expire traffic (kB):        No limits
    Log level:  Events
```

5) Ping не должен прерываться.

10.2 Работа с OSPF

В настоящем подразделе представлен простой (в части конфигурации сети) сценарий настройки совместного функционирования ПО и двух маршрутизаторов, для связи с которыми используется протокол динамической маршрутизации OSPF.

В случае недоступности активного канала передачи данных, OSPF обнаруживает данное событие, перестраивает таблицы маршрутизации, и IPsec туннель между площадками автоматически восстанавливается без дополнительных действий со стороны Администратора ПО.

10.2.1 Конфигурация стенда

Ниже приведена схема стенда, на котором будет осуществлена демонстрация работоспособности решения (см. рис. 19).

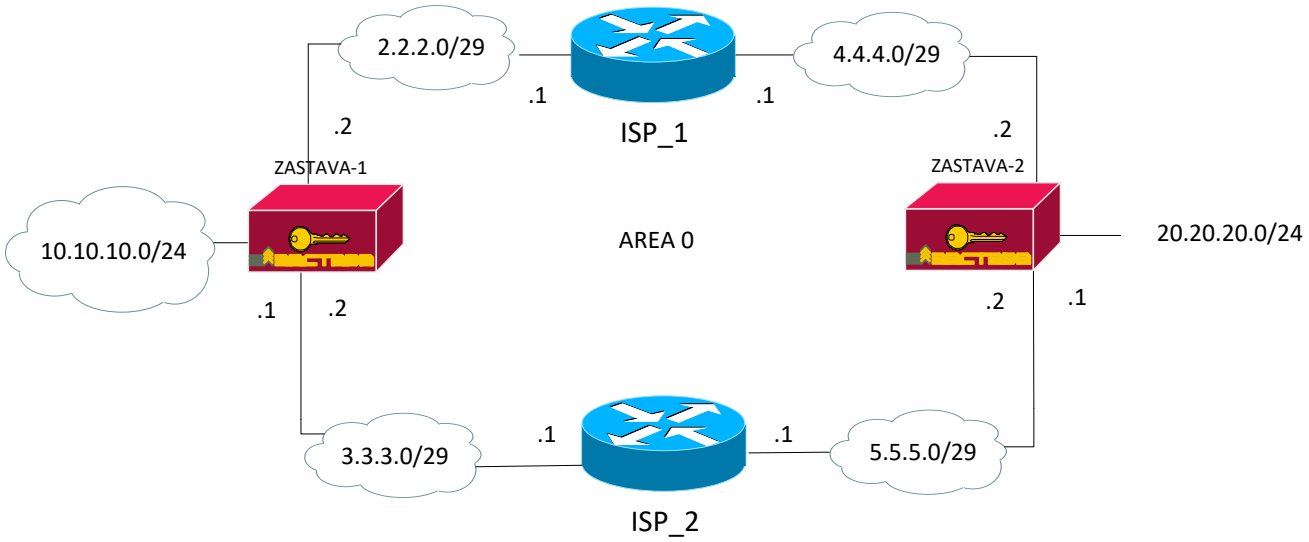

Рисунок 19 - Схема стенда для проверки работы с BGP

10.2.2 Состав ПО участников стенда

В качестве ISP_1 и ISP_2 используются Linux серверы (возможно исполнение в качестве виртуальных машин) и 2 ПК.

Состав ПО участников стенда:

1) ISP_1: ОС ALT Linux, пакет quagga, пакет NetworkManager;
2) ISP_2: ОС ALT Linux, пакет quagga, пакет NetworkManager;
3) ZASTAVA-1: ПК «VPN/FW ЗАСТАВА-150» исполнение ZO8-APK-150;
4) ZASTAVA-2: ПК «VPN/FW ЗАСТАВА-150» исполнение ZO8-APK-150.

10.2.3 Настройка конфигурации

Настройка ISP_1 и ISP_2 производится в командном интерпретаторе BASH.

Настройка ZASTAVA-1 и ZASTAVA-2 производится в командном интерпретаторе KLISH.

Ниже приведены команды для настройки узлов.

10.2.3.1 Настройки узла ISP_1

Для настройки узла ISP_1 выполнить следующие шаги:

1) выполнить настройку интерфейсов командой

```
nmcli connection add type ethernet con-name <имя_соединения>
ifname <название_интерфейса> ipv4.addresses <IP-адрес>
ipv4.method static autoconnect yes
```

2) поставить службы zebra и bgpd в автозагрузку командами:

systemctl enable zebra

systemctl enable ospfd

3) запустить службы zebra и bgpd командами:

systemctl start zebra

systemctl enable ospfd

4) выполнить вход в интерпретатор Cisco-Like Sheel командой **vtysh**

5) перейти в режим конфигурации командой **configure terminal**

6) выполнить последовательно команды:

router ospf

router-id 2.2.2.1

network 2.2.2.0/29 area 0

network 4.4.4.0/29 area 0

exit

interface <название_интерфейса_с_адресом_2.2.2.1>

ospf cost 1

exit

interface < название_интерфейса_с_адресом_4.4.4.1>

ospf cost 1

7) выполнить выход командой **exit** и затем ещё раз **exit**

8) сохранить конфигурацию командой **write**

9) выполнить выход из интерпретатора Cisco-Like Sheel командой **exit**

10.2.3.2 Настройки узла ISP_2

Для настройки узла ISP_2 выполнить следующие шаги:

1) выполнить настройку интерфейсов командой

nmcli connection add type ethernet con-name <имя_соединения> ifname <название_интерфейса> ipv4.addresses <IP-адрес> ipv4.method static autoconnect yes

2) поставить службы zebra и bgpd в автозагрузку командами:

systemctl enable zebra

systemctl enable ospf

3) запустить службы zebra и bgpd командами:

systemctl start zebra

systemctl start ospf

4) выполнить вход в интерпретатор Cisco-Like Sheel командой **vtysh**

5) перейти в режим конфигурации командой **configure terminal**
6) выполнить последовательно команды:

```
router ospf
router-id 3.3.3.1
network 3.3.3.0/29 area 0
network 5.5.5.0/29 area 0
exit
interface < название_интерфейса_с_адресом_3.3.3.1>
ospf cost 2
exit
interface < название_интерфейса_с_адресом_5.5.5.1>
ospf cost 2
```

7) выполнить выход командой **exit** и затем ещё раз **exit**
8) сохранить конфигурацию командой **write**
9) выполнить выход из интерпретатора Cisco-Like Sheel командой **exit**

10.2.3.3 Настройки узла ZASTAVA-1

Для настройки узла ZASTAVA-1 выполнить следующие шаги:

1) перейти в режим enable командой *enable*
2) выполнить настройку интерфейсов командами

```
network connection add type ethernet con-name
<имя_соединения> ifname <название_интерфейса>
network connection modify <имя_соединения> ipv4.addresses
<IP-адрес>
network connection modify <имя_соединения> ipv4.method manual
network connection modify <имя_соединения> autoconnect yes
network connection up <имя_соединения>
```

3) запустить службу bgpd командой **set OSPF on**
4) выполнить вход в интерпретатор Cisco-Like Sheel командой

```
set OSPF settings
```

5) перейти в режим конфигурации командой **configure terminal**
6) выполнить последовательно команды:

```
router ospf
router-id 10.10.10.1
network 2.2.2.0/29 area 0
```

network 3.3.3.0/29 area 0

network 10.10.10.0/24 area 0

passive-interface <название_итерфеса_с_адресом_10.10.10.1>

7) выполнить выход командой **exit** и затем ещё раз **exit**
8) сохранить конфигурацию командой **write**
9) выполнить выход из интерпретатора Cisco-Like Sheel командой **exit**

10.2.3.4 Настройки узла ZASTAVA-2

Для настройки узла ZASTAVA-2 выполнить следующие шаги:

1) перейти в режим enable командой **enable**
2) выполнить настройку интерфейсов командами

network connection add type ethernet con-name <имя_соединения> ifname <название_интерфейса>

network connection modify <имя_соединения> ipv4.addresses <IP-адрес>

network connection modify <имя_соединения> ipv4.method manual

network connection modify <имя_соединения> autoconnect yes

network connection up <имя_соединения>

3) запустить службу bgpd командой **set OSPF on**
4) выполнить вход в интерпретатор командой:

set OSPF settings

5) перейти в режим конфигурации командой **configure terminal**
6) выполнить последовательно команды:

router ospf

router-id 20.20.20.1

network 4.4.4.0/29 area 0

network 5.5.5.0/29 area 0

network 20.20.20.0/24 area 0

passive-interface <название_итерфеса_с_адресом_20.20.20.1>

7) выполнить выход командой **exit** и затем ещё раз **exit**
8) сохранить конфигурацию командой **write**
9) выполнить выход из интерпретатора командой **exit**

10.2.4 Проверка правильности настройки стенда

Стенд считается настроенным правильно, когда выполнены следующие условия:

1) В таблице маршрутов в ПО присутствуют следующие записи:

```
[root@ZASTAVA-1: ~]# ip r
2.2.2.0/29 dev eth1 proto kernel scope link src 2.2.2.2 metric 101
3.3.3.0/29 dev eth2 proto kernel scope link src 3.3.3.2 metric 102
4.4.4.0/29 via 2.2.2.1 dev eth1 proto zebra metric 20
5.5.5.0/29 via 3.3.3.1 dev eth2 proto zebra metric 20
10.10.10.0/24 dev eth3 proto kernel scope link src 10.10.10.1 metric 103
20.20.20.0/24 via 2.2.2.1 dev eth1 proto zebra metric 20
```

```
[root@ZASTAVA-2: ~]# ip r
2.2.2.0/29 via 4.4.4.1 dev eth1 proto zebra metric 20
3.3.3.0/29 via 5.5.5.1 dev eth2 proto zebra metric 20
4.4.4.0/29 dev eth1 proto kernel scope link src 4.4.4.2 metric 101
5.5.5.0/29 dev eth2 proto kernel scope link src 5.5.5.2 metric 102
10.10.10.0/24 via 4.4.4.1 dev eth1 proto zebra metric 20
20.20.20.0/24 dev eth3 proto kernel scope link src 20.20.20.1 metric 103
```

2) Изменение таблицы маршрутизации после перезагрузки роутера:

```
[root@ZASTAVA-1: ~]# ip r
2.2.2.0/29 dev eth1 proto kernel scope link src 2.2.2.2 metric 101
3.3.3.0/29 dev eth2 proto kernel scope link src 3.3.3.2 metric 102
4.4.4.0/29 via 3.3.3.1 dev eth2 proto zebra metric 20
5.5.5.0/29 via 3.3.3.1 dev eth2 proto zebra metric 20
10.10.10.0/24 dev eth3 proto kernel scope link src 10.10.10.1 metric 103
20.20.20.0/24 via 3.3.3.1 dev eth2 proto zebra metric 20
```

```
[root@ZASTAVA-2: ~]# ip r
2.2.2.0/29 via 5.5.5.1 dev eth2 proto zebra metric 20
3.3.3.0/29 via 5.5.5.1 dev eth2 proto zebra metric 20
4.4.4.0/29 dev eth1 proto kernel scope link src 4.4.4.2 metric 101
5.5.5.0/29 dev eth2 proto kernel scope link src 5.5.5.2 metric 102
10.10.10.0/24 via 5.5.5.1 dev eth2 proto zebra metric 20
20.20.20.0/24 dev eth3 proto kernel scope link src 20.20.20.1 metric 103
```

3) Команда ping не прерывается после перезагрузки роутера:

```
[root@ZASTAVA-1: ~]# ping -I 10.10.10.1 20.20.20.1
PING 20.20.20.1 (20.20.20.1) from 10.10.10.1 : 56(84) bytes of data.
64 bytes from 20.20.20.1: icmp_seq=154 ttl=63 time=1.17 ms
64 bytes from 20.20.20.1: icmp_seq=155 ttl=63 time=0.508 ms
64 bytes from 20.20.20.1: icmp_seq=156 ttl=63 time=1.08 ms
64 bytes from 20.20.20.1: icmp_seq=157 ttl=63 time=1.09 ms
64 bytes from 20.20.20.1: icmp_seq=158 ttl=63 time=0.490 ms
64 bytes from 20.20.20.1: icmp_seq=159 ttl=63 time=1.10 ms
```

10.2.5 Настройка правил шифрования

После проверки правильности настройки стенда, необходимо создать правила доступа между защищаемыми сетями за ZASTAVA-1 и ZASTAVA-2, как это делается для связи «сеть-сеть».

При доступе из сети 10.10.10.0/24 в сеть 20.20.20.0/24 и наоборот, трафик должен шифроваться.

Топология должна повторять приведенную схему, т.е. на ней должны быть созданы неуправляемые шлюзы, представляющие из себя маршрутизаторы ISP_1 и ISP_2 (см. рис. 20).

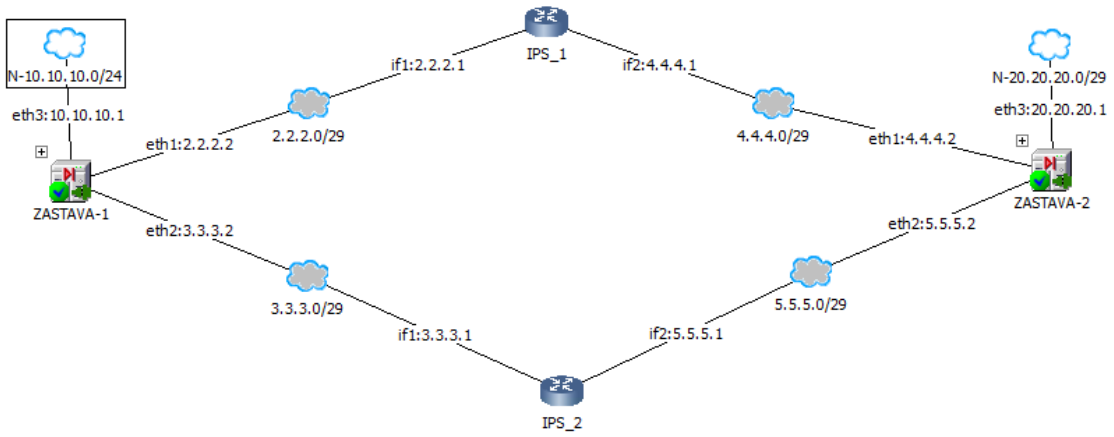

Рисунок 20 – Топология в графической консоли «ЗАСТАВА-Управление»

После создания необходимых объектов и правил, необходимо выполнить трансляцию и активацию политик безопасности.

Для проверки возможности доступа между сетями необходимо запустить на ZASTAVA-1 команду **`ping -I 10.10.10.1 20.20.20.1`**.

Затем необходимо убедиться, что взаимодействие осуществляется с использованием шифрования. Для этого необходимо выполнить команду **`vpnmonitor -i`**. В выводе должна присутствовать IPsec-сессия с селекторами сетей *10.10.10.0/24* и *20.20.20.0/24*.

```
[root@ZASTAVA-1: ~]# vpnmonitor -i
7D0AC3CE22F1BFF7.EA3D2D4A332FF8C8       4.4.4.2 (DN) OU=GATE,CN=ZASTAVA-2       GOST3410.2012(256)-
Sig / GOST3410.2012(256)-Sig
        1       ESP(Tunnel) Initiator   10.10.10.0..10.10.10.255 -- 20.20.20.0..20.20.20.255
filt_enc_13->rule_ipsec4
4E654DA71FC373FB.E6DD1ED7442D0428       10.111.15.75    (DN) CN=TPN_75  GOST3410.2012(256)-Sig /
GOST3410.2012(256)-Sig
IKE states count 2
IPsec states count 1
```

10.2.6 Проверка работоспособности решения

Для того, чтобы убедиться, что в случае проблем на канале провайдера ISP_1 защищенное взаимодействие между сетями автоматически переключиться на ISP_2, необходимо:

1) Выполнить просмотр параметров туннеля командой **vpnmonitor -i -ipsec-id <id>.**

Обратить внимание на текущий туннельный адрес партнера:

```
[root@ZASTAVA-1: ~]# vpnmonitor -i -ipsec-id 3
```

```
 IPsec SA id: 1 (0x1)
IPsec bundle:   ESP(Tunnel) Initiator
  ID:   1
  Rule: filt_enc_13->rule_ipsec4
  Selector:     10.10.10.0..10.10.10.255 -- 20.20.20.0..20.20.20.255
  Peer  IP:Port:        4.4.4.2 : 4500
  Local IP:Port:        2.2.2.2 : 4500
  DF bit:       COPY
  Key Exchange: from IKE SA
  IKE SA reference:     7D0AC3CE22F1BFF7
  IKE SA Remote ID:     (DN) OU=GATE,CN=ZASTAVA-2
ESP:    (#6)
  SPI in/out:   11933DEC / 12F277B9
  Rule: proto_esp14
  Transform:    GOST28147.89DIVER-CTR (ELVIS+ CSP GOST 28147-89 cipher key diversification CTR)
(Multicore)
  Authentication:       GOST28147.89-IMIT (ELVIS+ CSP GOST 28147-89 IMIT)
  Anti Replay Service:  On, window size: 512
  Status:       Active
  Statistics:
    Packets(bytes) encapsulated / decapsulated: 3 (312) / 3 (312)
    Decrypt errors (packets):   0
    Auth errors (packets):      0
    Reply errors (packets):     0
    Traffic limit errors (packets):     0
    Other decap errors (packets):       0
    Encrypt/Other errors (packets):     0
  Other:
    Created:    2023.10.05 12:27:22
    Life time (sec.):   28788 (28800)
    Expire traffic (kB):        No limits
    Log level:  Events
```

2) Выполнить перезагрузку роутера, через который маршрутизируется трафик.

3) Выполнить команду **vpnmonitor –i** для просмотра текущих IKE/IPsec сессий. Обратить внимание, что появилась дополнительная IPsec сессия:

```
[root@ZASTAVA-1: ~]# vpnmonitor -i
```

```
7AF651E258D572C1.C0C076F6B2782516       5.5.5.2 (DN) OU=GATE,CN=ZASTAVA-2
GOST3410.2012(256)-Sig / GOST3410.2012(256)-Sig
        2       ESP(Tunnel) Initiator   10.10.10.0..10.10.10.255 -- 20.20.20.0..20.20.20.255
filt_enc_16->rule_ipsec7
7D0AC3CE22F1BFF7.EA3D2D4A332FF8C8       4.4.4.2 (DN) OU=GATE,CN=ZASTAVA-2
GOST3410.2012(256)-Sig / GOST3410.2012(256)-Sig
        1       ESP(Tunnel) Initiator   10.10.10.0..10.10.10.255 -- 20.20.20.0..20.20.20.255
filt_enc_13->rule_ipsec4
4E654DA71FC373FB.E6DD1ED7442D0428       10.111.15.75    (DN) CN=TPN_75  GOST3410.2012(256)-Sig
/ GOST3410.2012(256)-Sig
IKE states count 3
IPsec states count 2
```

4) Выполнить просмотр параметров туннеля командой **vpnmonitor -i -ipsec-id <id>.**

Обратить внимание на изменившийся туннельный адрес партнера:

```
[root@ZASTAVA-1: ~]# vpnmonitor -i -ipsec-id 4
```

```
IPsec SA id: 2 (0x2)
IPsec bundle:   ESP(Tunnel) Initiator
```

```
  ID:   2
  Rule: filt_enc_16->rule_ipsec7
  Selector:     10.10.10.0..10.10.10.255 -- 20.20.20.0..20.20.20.255
  Peer  IP:Port:        5.5.5.2 : 4500
  Local IP:Port:        3.3.3.2 : 4500
  DF bit:       COPY
  Key Exchange: from IKE SA
  IKE SA reference:     7AF651E258D572C1
  IKE SA Remote ID:     (DN) OU=GATE,CN=ZASTAVA-2
ESP:    (#10)
  SPI in/out:   39BD0674 / 4FD7D67D
  Rule: proto_esp14
  Transform:    GOST28147.89DIVER-CTR (ELVIS+ CSP GOST 28147-89 cipher key diversification
CTR) (Multicore)
  Authentication:       GOST28147.89-IMIT (ELVIS+ CSP GOST 28147-89 IMIT)
  Anti Replay Service:  On, window size: 512
  Status:       Active
  Statistics:
    Packets(bytes) encapsulated / decapsulated: 5 (520) / 5 (520)
    Decrypt errors (packets):   0
    Auth errors (packets):      0
    Reply errors (packets):     0
    Traffic limit errors (packets):     0
    Other decap errors (packets):       0
    Encrypt/Other errors (packets):     0
  Other:
    Created:    2023.10.05 12:31:33
    Life time (sec.):   28749 (28800)
    Expire traffic (kB):        No limits
    Log level:  Event
```

5) Ping не должен прерываться.

11 ОБНОВЛЕНИЕ

После установки обновления необходимо проверить КС, как описано в п. 11.1.2. Результат проверки занести в Формуляр.

11.1 Регламент обновления

11.1.1 Процедуры получения обновления

Для обновления ПО потребитель должен самостоятельно получить на предприятии-поставщике (изготовителе) ПО согласно договору на поставку и/или техническую поддержку образ обновления на CD или USB-flash и прилагаемую к нему техническую документацию (новый Формуляр или предписание на внесение изменений), содержащую КС этого дистрибутива в соответствии с ГОСТ Р 34.11-2012.

Доставка нового сертифицированного обновления ПО должна производиться только по доверенному каналу.

11.1.2 Процедуры контроля целостности обновления

Для образа обновления необходимо произвести процедуру контроля целостности, используя утилиту icv_checker, и сравнить полученные КС с указанными в Формуляре.

11.1.3 Типовые процедуры тестирования обновления

После установки обновления необходимо проверить КС установленного ПО, для этого необходимо:

– включить СВТ с установленным ПО, дождаться появления меню выбора вариантов загрузки;

– выбрать пункт меню «Checksum test» и нажать клавишу <Enter>. На экране появится сообщение о проверке контрольной суммы образа программной составляющей. Дождаться окончания проверки;

– по окончании проверки на экране появится сообщение с вычисленной контрольной суммой, которое будет также содержать сообщение о соответствии/несоответствии вычисленной контрольной суммы с эталонной. Сверить вычисленную контрольную сумму с указанной на корпоративном http-сервере Разработчика;

– выключить СВТ с установленным ПО, нажав кнопку питания;

– включить СВТ с установленным ПО, дождаться появления меню выбора вариантов загрузки;

– выбрать пункт меню «ZASTAVA-Office» и нажать клавишу <Enter>. По окончании проверки выведется сообщение о вычисленных контрольных суммах, а также о их соответствии/несоответствии эталонным значениям.

11.1.4 Процедуры установки и применения обновления

Для установки нового сертифицированного обновления ПО в автоматизированном режиме может быть использован любой http-сервер, размещение и эксплуатация которого осуществляется в соответствии с требованиями руководящих документов ФСТЭК России по технической защите конфиденциальной информации.

Для контроля установки и верификации применения обновления необходимо выполнить подсчет КС нового образа и сравнить результаты с указанными в формуляре значениями.

11.2 Получение обновления с ПО «ЗАСТАВА-Управление»

Обновление осуществляется по протоколу HTTP.

Использование незащищенного канала обновления ЗАПРЕЩЕНО!

Для настройки сервера обновлений необходимо (сервер обновления настраивается в ПО «ЗАСТАВА-Управление»):

–установить в конфигурационном файле http.ini переменную root, указать путь к папке с файлами обновления. Например, C:\Program Files\ELVIS+\ZASTAVA Management\update;

–в каталоге, на который указывает переменная root, создать каталог с именем agentupdate;

–в каталоге agentupdate создать файл update.ini, который должен содержать набор секций, соответствующих типу обновляемого ПК, а также архитектуре процессора и названию ОС. В каталог agentupdate необходимо добавить дистрибутив, который будет служить образом обновления. Файл update.ini должен содержать следующее описание:

[GATE.LINUX.x64.zastava]

version= 6.8.23807

file=LIVE_UPG

silent=1

exec=mount -o remount,rw /.image && mv $DOWNLOAD_PATH/LIVE_UPG /.image/ && sed -i 's/LIVE\=\#GOST3411_256_2012\:[0-9a-z]*/LIVE\=\#GOST3411_256_2012\:ХЭШ_LIVE_UPG /g' /.image/syslinux/filelist.hash && mount -o remount,ro /image

hash=ХЭШ_LIVE_UPG

Параметры **version, DOWNLOAD_PATH, ХЭШ_ОБНОВЛЁННОГО_ОБРАЗА, ХЭШ_LIVE_UPG** могут быть изменены в соответствии с актуальными параметрами:
version – X.X.XXXXX – версия дистрибутива;
file – список имен файлов, разделенный запятыми, которые нужно загрузить;
exec – исполняемая команда;
silent – параметр, характеризующий оповещение пользователей (0 или 1, 0 - показывать сообщение пользователю);
LIVE_UPG – название файла установочного дистрибутива;
DOWNLOAD_PATH – каталог, в который были загружены файлы обновления;
ХЭШ_LIVE_UPG – КС загружаемых файлов, предназначена для проверки целостности при загрузке. КС должно быть столько же, сколько и файлов**.**

В каждой секции описывается версия доступного обновления, файлы для скачивания, исполняемая системная команда для осуществления обновления. Эти параметры редактируемы, можно изменять значения параметра, редактируя файл в любом текстовом редакторе.

Секции имеют следующий формат: [<тип *Агента*>.<ОС>.<процессор>.<вендор>], где:

- <тип *Агента*> - GATE;
- <ОС> - LINUX;
- <процессор> - x64;
- <вендор> - zastava.

Для обновления ПО согласно ЛПБ при использовании встроенного сервера обновления в ПО «ЗАСТАВА-Управление» необходимо добавить сетевой сервис TCP с портом 3118. После создания сетевого сервиса надо создать сервер обновления с методом подключения HTTP. Для этого надо выбрать созданный сервис и указать URL, например, http://10.111.10.231:3118/agentupdate. В настройках ПО открыть «*Управление*» → «*Обновления*» в поле «Тип обновления» выбрать параметр *«Обновлять согласно ЛПБ»*.

Для обновления с помощью команд с сервера обновлений необходимо в настройках ПО выбрать закладку «*Управление*» → «*Обновления*» в поле «Тип обновления» выбрать параметр «*Обновлять по командам с сервера обновления*» и в поле «Серверы обновления» добавить сервер обновления.

12 НЕШТАТНЫЕ СИТУАЦИИ

12.1 Некорректная работа ПО после обновления

В случае некорректной работы ПО после очередного обновления следует выполнить возврат к эталонной версии ПО. Эталонной версией является ПО, установленное при его поставке. Образ эталонной версии ПО хранится на жёстком диске и может быть развёрнут при необходимости.

12.2 Возврат к эталону

Возврат к эталону ПО выполняется следующим образом:

1) включить СВТ с установленным ПО, дождаться появления меню загрузчика;

2) выбрать пункт меню «Recovery system» и нажать клавишу <Enter>;

3) ввести имя пользователя admin, пароль 12345678;

4) на экране появится сообщение о проверке КС образа ОС, установленного при изготовлении ПО. Дождаться окончания проверки;

5) по окончании проверки в случае совпадения КС будет загружено эталонное ПО, далее СВТ с установленным ПО перезагрузится.

При возврате к эталонной версии ПО будут утеряны все выполненные ранее настройки (настройки политики безопасности, сетевые настройки и т.п.).

После запуска системы необходимо сразу же выставить параметр «Политика драйвера по умолчанию» в значение «DROP» для сохранения безопасного состояния.

При несовпадении КС на экран будет выведено соответствующее сообщение. В этом случае необходимо обратиться к разработчику ПО.

12.3 Нарушение целостности образа

В случае нарушения целостности образа необходимо:

1) назначить ответственного за расследование инцидента. Всю ключевую информацию считать скомпрометированной;

2) в случае, если действия, которые привели к инциденту, не являются угрозой безопасности (например, нарушение образа для обновления при передаче по каналам данных), необходимо выполнить откат в эталон и выпустить новую ключевую информацию для VPN;

3) в случае, если действия, которые привели к инциденту, являются угрозой безопасности, то необходимо отправить ПО разработчику ПО на восстановление.

12.4 Компрометация ключей аутентификации

В случае компрометации ключей аутентификации необходимо:

1) назначить ответственного за расследование инцидента;

2) в случае компрометации ключей для VPN необходимо выпустить новую ключевую информацию для VPN;

3) в случае компрометации ключей для входа в ОС необходимо отправить ПО разработчику ПО на восстановление.

В случае утери ключевого носителя:

1) сообщить разработчику ПО о факте утери;

2) заказать новый ключевой носитель;

3) сменить все пароли, заданные в ПО;

4) применить организационно-технические меры для обеспечения недоступности серверов для любых лиц;

5) если токен найдется, его нужно отформатировать и сделать новый запрос на выпуск сертификата и передать его доверенным способом для процедуры подписи.

13 ВОЗМОЖНЫЕ НЕИСПРАВНОСТИ И СПОСОБЫ ИХ УСТРАНЕНИЯ

Возможные неисправности и способы их устранения приведены в таблице 33.

Таблица 33 – Возможные неисправности и способы их устранения

Описание	Способы устранения
Не работает клавиатура	Последовательно выполнить приведённые ниже действия до устранения неисправности: 1. проверить подключение клавиатуры к USB-порту системного блока; 2. проверить кабель на наличие повреждений, заломов, разрезов; 3. проверить наличие световой индикации на клавиатуре в верхнем правом углу, нажав несколько раз на клавишу <Num Lock>; 4. при наличии повреждений кабеля или отсутствии световой индикации заменить клавиатуру
На экране входа в систему «Не удалось выполнить вход»	Последовательно выполнить приведённые ниже действия до устранения неисправности: 1. проверить правильность выбранной учётной записи (admin/user); 2.проверить правильность введенного пароля; 3.проверить наличие ключевого носителя в слоте USB; 4.убедиться в том, что ключевой носитель установлен в слот USB до конца; 5. если после выполнения действий не получено приглашение к вводу PIN-кода, - изъять ключевой носитель, выполнить перезагрузку СВТ с установленным ПО, установить ключевой носитель в слот USB после того, как на экране появится приглашение к вводу логина

Характерные ошибки при работе с ПО и рекомендации по их устранению приведены в таблице 34.

Таблица 34 – Характерные ошибки при работе с ПО и рекомендации по их устранению

Тип ошибки	Описание ошибки	Рекомендации по устранению
Неправильное использование утилиты командной строки ПО	Синтаксическая ошибка (Syntax error): 1) при вводе неверных/несуществующих параметров и ключей при использовании утилиты vpnconfig; 2) при вводе неверных/несуществующих параметров и ключей при использовании утилиты vpnmonitor; 3) при вводе неверных/несуществующих параметров и ключей при использовании утилиты icv_checker	1) Воспользоваться предлагаемым списком команд и ключей утилиты, который выводится при ошибке. Описание команд приведено в п. 7.2.1. 2) Воспользоваться предлагаемым списком команд и ключей утилиты, который выводится при ошибке. Описание команд приведено в п. 7.1.2. 3) Воспользоваться командой вызова справочной информации `icv_checker -h`. Описание команд утилиты приведено в п. 7.2.1.9

Тип ошибки	Описание ошибки	Рекомендации по устранению
Ошибка доступа	Возникает при вводе неправильного логина, или пароля, или PIN-кода персонального идентификатора Администратора ПО	1) Необходимо ввести правильный логин, пароль и PIN-код ключевого носителя (персонального идентификатора) Администратора ПО. 2) При отсутствии возможности указать верные данные, обратиться к разработчику ПО
Ошибки при настройке политики безопасности в ПО	Local Policy Parse error: возникает при указании политики безопасности из файла, который не содержит правильно объявленную политику безопасности	Необходимо указать в качестве политики безопасности файл, содержащий правильно объявленную политику безопасности
	IKE Connection timeout: возникает при указании в настройках получения политики безопасности неверный адрес сервера политик.	Необходимо узнать верный адрес сервера политик и указать его в настройках политики безопасности ПО. Если это не помогло, необходимо убедиться в сетевой доступности ЦУП
	IKE Peer reported error: возникает при указании в политике безопасности сертификата, не совпадающего с сертификатом, указанном в ЦУП	Необходимо указать в настройках политики безопасности ПО сертификат, указанный в ГПБ ЦУП
	IKE Error: возникает при отсутствии доверенного сертификата УЦ в ПО, либо указании неверного доверенного сертификата УЦ	Необходимо импортировать правильный доверенный сертификат УЦ в ПО, а также открыть сеанс с токеном для доверенного сертификата, выполнив авторизацию в этот токен: `vpnconfig –login token <id> <password> save`
	Не удалось загрузить политику: отсутствует персональный сертификат: возникает при отсутствии персонального сертификата для VPN в ПО. При этом в опциях политики безопасности отображается ошибка, что политика ссылается на несуществующий сертификат	Необходимо: 1) скопировать контейнер закрытого ключа, содержащий сертификат, указанный в ГПБ ЦУП как персональный, в /var/opt/cprocsp/keys. 2) выполнить авторизацию в токен с персональным сертификатом: `vpnconfig –login token <id> <password> save`
	Local certificate not found or not valid: возникает, если у сертификата, указанного в политике безопасности, истек срок валидности	Необходимо перевыпустить сертификат и контейнер закрытого ключа. Далее необходимо указать новый сертификат в ГПБ ЦУП и импортировать контейнер закрытого ключа в ПО. В политики безопасности ПО указать использование нового сертификата для подключения к серверу политик

Тип ошибки	Описание ошибки	Рекомендации по устранению

Переполнение диска СВТ с установленным ПО	Возникает при отсутствии свободного места на диске, характеризуется падением службы ПО (vpndmn)	Необходимо убедиться в отсутствии свободного места на диске, выполнив команду `df -h`. Если места на диске нет, то необходимо:
		1) в файле /etc/rsyslog.conf поставить # в начале строки:
		`#*.info;mail.none;authpriv.none;cron.none /var/log/messages`
		2) настроить ротацию журнала, как это описано в п. 7.2.3.1;
		3) очистить журнал: `cat /dev/null > /var/log/messages`
		4) после внесения изменений перезапустить сервис журналирования:
		`/etc/init.d/S01logging restart`.
		Если выше перечисленные рекомендации не помогли, и диск всё равно переполняется файлом журнала, необходимо добавить исключение в журналирование по ключевым словам в файле /etc/rsyslog.conf:
		`:msg, contains, "ip_vs" ~`
		`:msg, contains, "segfault" ~`
		затем снова перезапустить сервис журналирования

Отсутствие сетевого доступа к СВТ с установленным ПО	Возникает при неправильно заданных сетевых настройках ПО, либо падении службы ПО с заданной «Политикой драйвера по умолчанию» в значение «DROP» (и «DROP ALL»)	При отсутствии сетевого доступа к СВТ с установленным ПО (например, при использовании подключения по ssh) при условии, что ранее соединение работало, необходимо: 1) подключиться локально к СВТ с установленным ПО с административным токеном; 2) проверить работу службы vpndmn при помощи команды: `pidof vpndmn` если команда не вывела id процесса, значит, служба ПО не запущена. Необходимо перезагрузить СВТ с установленным ПО, и, если ситуация повторится, то необходимо убедиться в том, что отсутствует проблема переполнения диска; 3) если команда вывела id процесса, значит, СВТ с установленным ПО функционирует. Следует убедиться в том, что: – служба ssh запущена (см. подраздел 7.2.3), если СВТ с установленным ПО недоступно при подключении по ssh; – логические имена интерфейсов (alias) настроены верно (см. п. 7.2.1.7.5); – верно задан маршрут по умолчанию (см. таблицу 11)

ПЕРЕЧЕНЬ ПРИНЯТЫХ ТЕРМИНОВ И СОКРАЩЕНИЙ

AH – Authentication Header – протокол из группы IPsec

ASCII – American standard code for information interchange – стандарт кодирования символов

BASH – Bourne again shell – командная оболочка UNIX-подобных ОС

CRL – Certificate Revocation List – см. СОС

CSP – Cryptographic Service Provider – криптопровайдер

DH – Diffie-Hellman – протокол Диффи-Хеллмана

DHCP – Dynamic Host Configuration Protocol — протокол динамической настройки узла

DN – Distinguished Name – уникальное имя

DNS – Domain Name System – система доменных имен для именования хостов в глобальных сетях

EAP Extensible Authentication Protocol - расширяемый протокол аутентификации

ESP – Encapsulated Security Payload – протокол из группы IPsecGMT – время по Гринвичу

HTTP HyperText Transfer Protocol - протокол передачи гипертекста

IKE – Internet Key Exchange – протокол обмена ключевой информацией; используется совместно с протоколами IPsec для организации первичного защищенного канала ISAKMP SA

IP – Internet Protocol – протокол сетевого уровня, являющийся базовым протоколом IP-сетей

IPsec – IP security – группа протоколов для установления защищенных соединений в IP-сетях

KLISH – Kommand Line Interface SHell - командный интерпретатор

LDAP – Lightweight Directory Access Protocol - группа стандартных протоколов для доступа к каталогам («Directories»)

LSP – Local Security Policy – см. ЛПБ

MTU – Maximum Transmission Unit – максимальный размер полезного блока данных одного пакета, который может быть передан протоколом без фрагментации

NAT – Network Address Translation – трансляция сетевых адресов

NTP Network Time Protocol — протокол сетевого времени

PIN – Personal identification number – персональный идентификационный код

RRI – Reverse Route Injection - механизм, связывающий управление топологией VPN и систему маршрутизации

SA – Security Association – защищенное соединение (в контексте протоколов IPsec и IKE)

SNMP – Simple Network Management Protocol – протокол прикладного уровня для управления устройствами в IP-сетях на основе архитектур TCP/UDP

SSH	–	Secure Shell – протокол удаленного управления
TCP	–	Transmission Control Protocol - сетевой протокол транспортного уровня с гарантированной доставкой в IP-сетях
UDP	–	User Datagram Protocol - сетевой протокол транспортного уровня без гарантированной доставки в IP-сетях
USB	–	Universal serial bus – универсальная последовательная шина
VPN	–	Virtual Private Network – виртуальная частная сеть
АРМ	–	Автоматизированное рабочее место
ВЧС	–	Виртуальная частная сеть
ГОСТ	–	Государственный стандарт
ГПБ	–	Глобальная политика безопасности
КС	–	Контрольная сумма
ЛПБ	–	Локальная политика безопасности
ОС	–	Операционная система
ПО	–	Программное обеспечение
СВТ	–	Средство вычислительной техники
СОС	–	Список отозванных сертификатов
УЦ	–	Удостоверяющий центр
ФСТЭК России	–	Федеральная служба по техническому и экспортному контролю России
ЦУП	–	Центр управления политиками безопасности

ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ

Изменение	Номера листов				Всего листов в документе	Номер документа	Вх. № сопроводительного документа и дата	Подпись	Дата
	измененных	замененных	новых	изъятых					