

**Программный комплекс  
«VPN/FW «ЗАСТАВА-Офис», версия 8 KC1»**

**Руководство администратора**

2023

## СОДЕРЖАНИЕ

<b>1</b>	<b>ВВЕДЕНИЕ .....</b>	<b>5</b>
1.1	НАЗНАЧЕНИЕ .....	5
1.2	ТРЕБОВАНИЯ К УРОВНЮ ПОДГОТОВКИ ПЕРСОНАЛА .....	5
1.3	ТИПОГРАФСКИЕ СОГЛАШЕНИЯ .....	5
<b>2</b>	<b>ОБЩИЕ СВЕДЕНИЯ .....</b>	<b>6</b>
2.1	Минимальные аппаратные требования .....	6
2.2	Требования к персональным идентификаторам .....	6
<b>3</b>	<b>УСТАНОВКА ПК.....</b>	<b>8</b>
3.1	Входной контроль комплектующих изделий .....	8
3.2	Порядок установки ПК .....	8
3.4	Проверка корректности и завершение установки .....	10
<b>4</b>	<b>ПОДГОТОВКА К РАБОТЕ И БЫСТРЫЙ СТАРТ .....</b>	<b>11</b>
4.1	Вход в ПК .....	11
4.2	Проверка контрольной суммы .....	11
4.3	Смена пароля Администратора .....	12
4.4	Настройка сетевых параметров .....	12
4.4.1	Настройка адресации .....	12
4.4.2	Настройка маршрутизации .....	13
4.4.3	Настройка DNS .....	13
4.4.4	Применение настроек .....	13
4.4.5	Настройка в режиме пользовательского псевдографического интерфейса .....	13
4.4.6	Назначение псевдонимов для сетевых интерфейсов .....	18
4.5	Расширенные настройки сети .....	18
4.5.1	Настройка автоматического синхронизации системного времени (NTP) .....	18
4.5.2	Настройка удаленной регистрации событий (SYSLOG) .....	20
4.5.3	Настройка мониторинга (SNMP) .....	20
4.5.4	Настройка PROXY HTTP .....	21
4.5.5	Настройка DHCP сервера .....	22
4.6	Включение двухфакторной аутентификации .....	23
4.7	Конфигурирование ПК «ЗАСТАВА-УПРАВЛЕНИЕ» .....	24
<b>5</b>	<b>ОПИСАНИЕ СРЕДСТВ КОНФИГУРИРОВАНИЯ И МОНИТОРИНГА.....</b>	<b>25</b>
<b>6</b>	<b>ОПИСАНИЕ ДОСТУПНЫХ ОПЕРАЦИЙ ИНТЕРПРЕТАТОРА KLIST .....</b>	<b>26</b>
6.1	Назначение интерпретатора KLIST .....	26
6.2	Негрупповые команды .....	26
6.3	Команда смены пароля .....	27
6.4	Команды просмотра настроек .....	27
6.5	Команды выполнения настроек .....	29
6.6	Команды для диагностики состояния сетевого соединения .....	33
6.7	Резервирование и восстановление данных .....	34
<b>7</b>	<b>ОПИСАНИЕ ДОСТУПНЫХ ОПЕРАЦИЙ ИНТЕРПРЕТАТОРА BASH.....</b>	<b>36</b>
7.1	Обзор средств мониторинга .....	36
7.1.1	Файл регистрации системных событий .....	36
7.1.2	Утилита <i>urptmonitor</i> .....	37
7.1.3	Утилита <i>tcping</i> .....	53
7.1.4	Утилита <i>arping</i> .....	54

7.2	ОБЗОР СРЕДСТВ КОНФИГУРИРОВАНИЯ .....	54
7.2.1	<i>Утилита vrpncconfig</i> .....	54
7.2.2	<i>Утилита icv_checker</i> .....	79
7.2.3	<i>Использование команд программной составляющей и конфигурирование модулей.</i> .....	81
7.3	ДОСТУПНЫЕ СЕТЕВЫЕ СЛУЖБЫ .....	82
<b>8</b>	<b>ОПИСАНИЕ КОНФИГУРИРОВАНИЯ В КЛАСТЕРНОМ ИСПОЛНЕНИИ .....</b>	<b>84</b>
8.1	НАСТРОЙКА КЛАСТЕРА С ПОМОЩЬЮ МАСТЕРА .....	85
8.1.1	<i>Меню мастера настройки кластера:</i> .....	85
8.1.2	<i>Пункт 1 – Настроить ПО keepalive:</i> .....	86
8.1.3	<i>Пункт 2 – Настроить ПО ЗАСТАВА:</i> .....	87
8.1.4	<i>Пункт 3 – Применить настройки ПО:</i> .....	87
8.1.5	<i>Пункт 4 – Передать настройки ПО на другой узел по сети:</i> .....	89
8.1.6	<i>Пункт 5 – Посмотреть текущие настройки</i> .....	89
8.1.7	<i>Пункт 69 – Очистить все настройки:</i> .....	89
8.1.8	<i>Пункт 6 – Выход:</i> .....	90
8.2	НАСТРОЙКА ПО KEEPALIVED .....	90
8.3	НАСТРОЙКА КЛАСТЕРА ВРУЧНУЮ .....	90
8.3.1	<i>Настройки ПО keepalived</i> .....	90
8.3.2	<i>Настройка синхронизации состояний IKEv2</i> .....	94
8.4	НАСТРОЙКА МАРШРУТИЗАЦИИ ПРИ РАБОТЕ С КЛАСТЕРОМ .....	95
<b>9</b>	<b>ОПИСАНИЕ КОНФИГУРИРОВАНИЯ L2TP СОЕДИНЕНИЯ.....</b>	<b>96</b>
9.1	СОЗДАНИЕ НОВОГО СОЕДИНЕНИЯ .....	96
9.2	ПРОСМОТР СОЗДАННЫХ СОЕДИНЕНИЙ.....	97
9.3	УДАЛЕНИЕ СОЕДИНЕНИЯ.....	98
9.4	ЗАПУСК СОЕДИНЕНИЙ В СООТВЕТСТВИИ С НАСТРОЙКАМИ .....	99
<b>10</b>	<b>РАБОТА С ДИНАМИЧЕСКОЙ МАРШРУТИЗАЦИЕЙ .....</b>	<b>100</b>
10.1	РАБОТА С BGP.....	100
10.1.1	<i>Конфигурация стенда</i> .....	100
10.1.2	<i>Состав ПО участников стенда</i> .....	100
10.1.3	<i>Настройка конфигурации</i> .....	100
10.1.4	<i>Проверка правильности настройки стенда</i> .....	103
10.1.5	<i>Настройка правил шифрования</i> .....	104
10.1.6	<i>Проверка работоспособности решения</i> .....	105
10.2	РАБОТА С OSPF.....	107
10.2.1	<i>Конфигурация стенда</i> .....	107
10.2.2	<i>Состав ПО участников стенда</i> .....	107
10.2.3	<i>Настройка конфигурации</i> .....	108
10.2.4	<i>Проверка правильности настройки стенда</i> .....	111
10.2.5	<i>Настройка правил шифрования</i> .....	112
10.2.6	<i>Проверка работоспособности решения</i> .....	113
<b>11</b>	<b>ОБНОВЛЕНИЕ .....</b>	<b>115</b>
11.1	РЕГЛАМЕНТ ОБНОВЛЕНИЯ .....	115
11.1.1	<i>Процедуры получения обновления</i> .....	115
11.1.2	<i>Процедуры контроля целостности обновления</i> .....	115
11.1.3	<i>Типовые процедуры тестирования обновления</i> .....	115
11.1.4	<i>Процедуры установки и применения обновления</i> .....	116
11.2	ПОЛУЧЕНИЕ ОБНОВЛЕНИЯ С ПК«ЗАСТАВА-УПРАВЛЕНИЕ».....	116
<b>12</b>	<b>НЕШТАТНЫЕ СИТУАЦИИ.....</b>	<b>118</b>

12.1	НЕКОРРЕКТНАЯ РАБОТА ПК ПОСЛЕ ОБНОВЛЕНИЯ .....	118
12.2	ВОЗВРАТ К ЭТАЛОНУ .....	118
12.3	НАРУШЕНИЕ ЦЕЛОСТНОСТИ ОБРАЗА .....	118
12.4	КОМПРОМЕТАЦИЯ КЛЮЧЕЙ АУТЕНТИФИКАЦИИ.....	119
<b>13</b>	<b>ВОЗМОЖНЫЕ НЕИСПРАВНОСТИ И СПОСОБЫ ИХ УСТРАНЕНИЯ .....</b>	<b>120</b>
	<b>ПЕРЕЧЕНЬ ПРИНЯТЫХ ТЕРМИНОВ И СОКРАЩЕНИЙ .....</b>	<b>123</b>
	<b>ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ .....</b>	<b>125</b>

## 1 ВВЕДЕНИЕ

Настоящий документ предназначен для администратора Программного комплекса «VPN/FW «ЗАСТАВА-Офис», версия 8 КС1» (далее – ПК) и содержит описание ПК, описание интерфейса программного обеспечения (ПО), процедур, выполняемых администратором в процессе подготовки ПК к работе, доступных операций, действий при возникновении нештатных ситуаций.

### 1.1 Назначение

ПК предназначен 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.

ПК 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 ПК в соответствии с эксплуатационной документацией.

Администратор ПК должен знать основы администрирования локальных сетей.

### 1.3 Типографские соглашения

<b>Полужирный шрифт</b>	Полужирный шрифт используется для выделения названий меню, вкладок, кнопок, полей, объектов политики, строк контекстного меню, а также для визуального выделения.
<i>Курсив</i>	Курсив используется, чтобы выделить названия файлов. Курсив также может использоваться для 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 Минимальные аппаратные требования**

СВТ, на котором устанавливается ПК 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 2 (для кластерного исполнения не менее 3) сетевых интерфейсов GbE/SFP/SFP+;
- BIOS с поддержкой CSM Compatibility Support Module;
- Один свободный порт PCI-E / Mini PCI-E / PCI;
- Не менее 2 USB портов.

Рекомендуемые платформы для установки ПК:

- Сервер Аквариус T40 S208DF;
- Сервер Аквариус T30 S001DC.

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

### **2.2 Требования к персональным идентификаторам**

В ПК в качестве персонального идентификатора используются функциональные ключевые носители (ФКН) 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:

- сертификат должен содержать поле Extended Key Usage (EKU) включающее в себя OID=Smart Card Logon;
- сертификат должен содержать поле 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 – Администратору ПК, user@localhost – Оператору ПК.



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

### 3 УСТАНОВКА ПК

#### 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 по инструкции `readme_install.txt`, размещённой на диске;
- 3) Проверку целостности дистрибутива ПК.



Проверка целостности подразумевает подсчёт контрольных сумм (КС) трёх файлов на установочном USB-flash носителе, расположенных по относительным путём:

- `SPECOS\bzImage`;
- `SPECOS\ZASOS_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 следующие варианты:

- Утилитой подсчета КС (`icv_checker`) из состава поставки, расположенной в корне поставочного CD/DVD-диска. Формат команды `icv_checker.exe -F=<путь к файлу\имя файла>`
- При наличии на АРМ с ПО КриптоПро CSP утилитой `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 файлу `bzImage`.



USB-носитель должен быть предварительно отформатирован.

#### 3.2 Порядок установки ПК

Разворачивание ПК 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 на загрузку 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 ПК с установочного USB-накопителя.
- 5) В процедуре установки выбрать пункт `ZASTAVA OS grub 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 OS создаются две учётные записи:

- `admin` пароль по умолчанию `russia`
- `user` пароль по умолчанию `russia`



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

### **3.4 Проверка корректности и завершение установки**

- 1) В меню загрузчика выбрать пункт «Checksum test». Дождаться подсчёта КС и вычисленные значения должны совпадать со значениями, указанными в таблице 3 раздела 5 формуляра.
- 2) Выключить аппаратную платформу. Установка и инициализация ПК завершена.

## 4 ПОДГОТОВКА К РАБОТЕ И БЫСТРЫЙ СТАРТ

### 4.1 Вход в ПК

В ПК 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 ПК (имя пользователя - admin) и Оператора ПК (имя пользователя - user) осуществляется на основании введенного логина и пароля.

При включенном режиме двухфакторной идентификации и аутентификации Идентификация и аутентификация Администратора ПК и Оператора ПК осуществляется на основании цифрового сертификата, хранящегося на персональном идентификаторе, предъявленного PIN-кода. Требования к персональным идентификаторам приведены в подразделе **Ошибка! Источник ссылки не найден..**

	Имена пользователей зафиксированы в образе программной составляющей ПК. Перед началом использования ПК 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 программной составляющей.

Процедура проверки КС:

- 1) после включения ПК дождаться появления меню загрузчика (см. **Ошибка! Источник ссылки не найден.;**);

- 2) выбрать пункт меню «Checksum test» и нажать клавишу <Enter>;

- 3) на экране появится сообщение о проверке КС образа программной составляющей.

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 ПК, нажав кнопку питания;

- 6) включить ПК, нажав кнопку питания , дождаться появления меню выбора вариантов загрузки «ZASTAVA OS»;
- 7) выбрать пункт меню «ZASTAVA OS» и нажать клавишу <Enter>;
- 8) 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**

Интерактивная команда password производит смену пароля для текущей учётной записи.

**> password**

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:**

**Извините, но пароли не совпадают.**

**passwd: Службе паролей не удалось выполнить предварительную проверку.**

**passwd: Пароль не изменён**

При задании нового пароля равного текущему.

**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 под учётной записью admin и выполнить команду:

**> enable**

##### **4.4.1 Настройка адресации**

Для настройки статического адреса необходимо выполнить:

```

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:

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

Для задания адреса шлюза поумолчанию необходимо выполнить:

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

#### 4.4.3 Настройка DNS

Для добавления DNS-сервера необходимо выполнить:

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

Для удаления DNS-сервера необходимо выполнить:

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

#### 4.4.4 Применение настроек

Для того чтобы заданные настройки успешно применились необходимо выполнить:

```
network connection up <название соединения>
```

#### 4.4.5 Настройка в режиме пользовательского псевдографического интерфейса

Для проведения базовых настроек сетевых параметров можно использовать псевдографическую утилиту nmtui. Для запуска утилиты в оболочке KLIBH необходимо выполнить:

```
network nmtui
```

При запуске утилиты будут предложены варианты действий см. Рисунок 1.

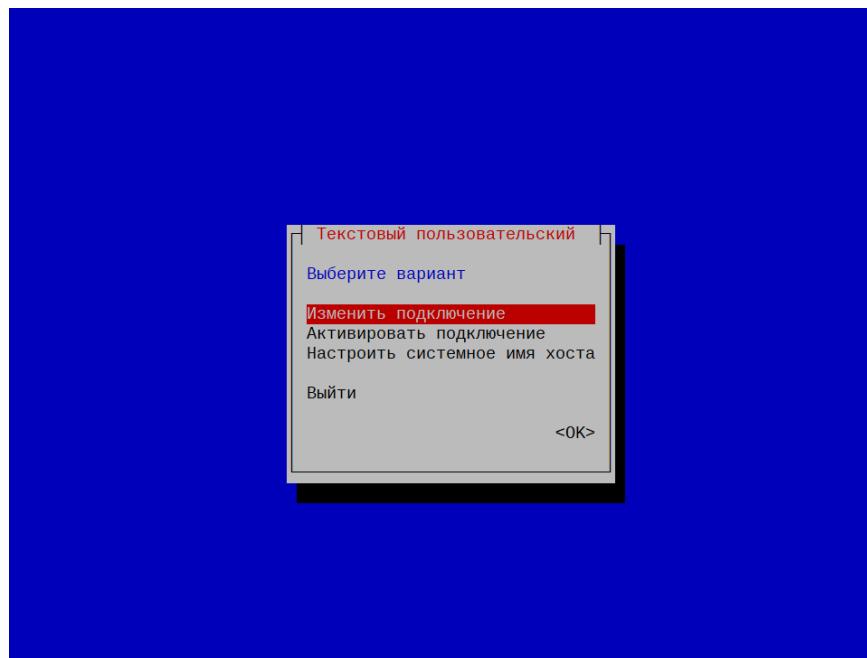


Рисунок 1 - Главное окно утилиты nmtui

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

- 1) Добавить / Изменить / Удалить подключения (см. Рисунок 2)
- 2) Задать Имя / IP адрес:маску / Шлюз по умолчанию / Сервер разрешения имён (см. Рисунок 3, Рисунок 4);
- 3) Добавить / удалить статические маршруты (см. Рисунок 5, Рисунок 6);
- 4) Отобразить свойства подключения (см. Рисунок 7)

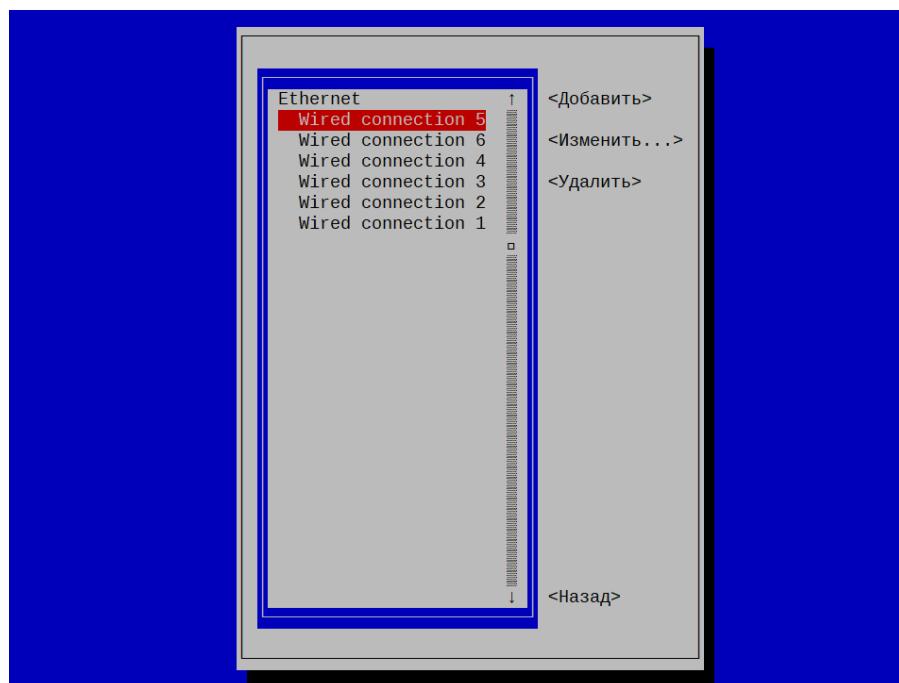


Рисунок 2 - Перечень соединений

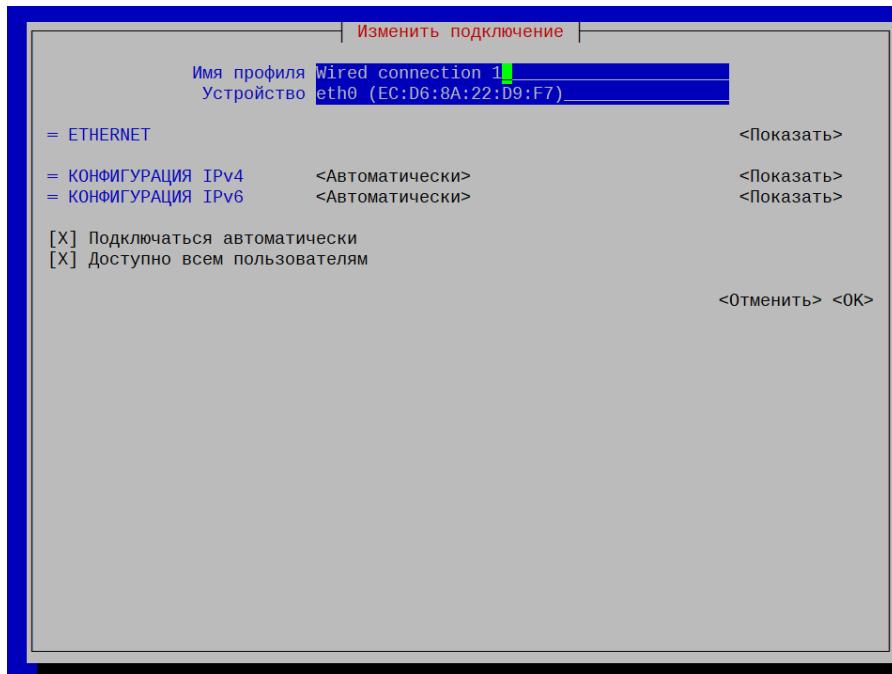


Рисунок 3 – Редактирование имени подключения

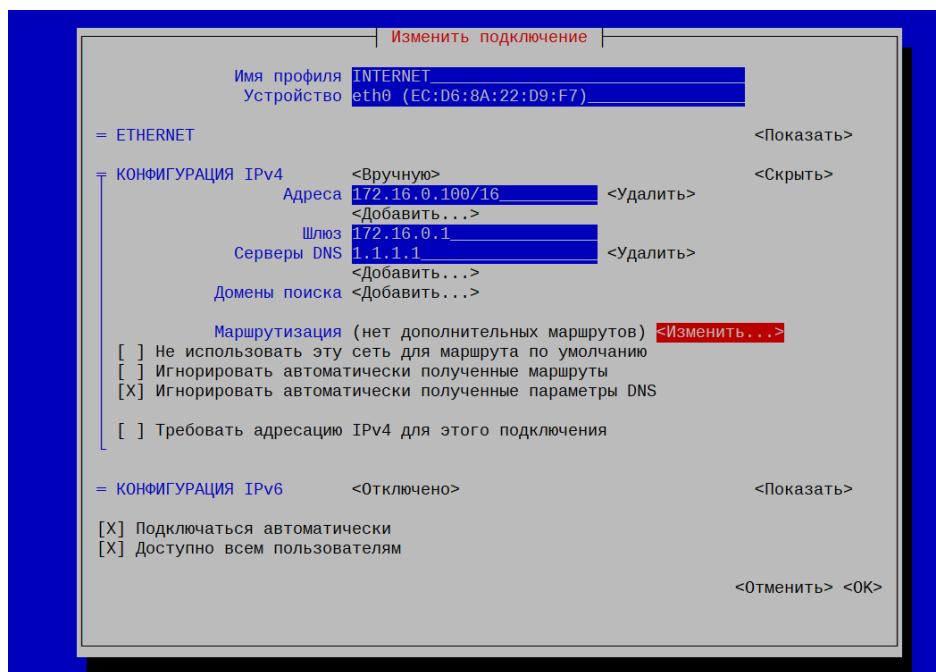


Рисунок 4 – Задание IP адреса

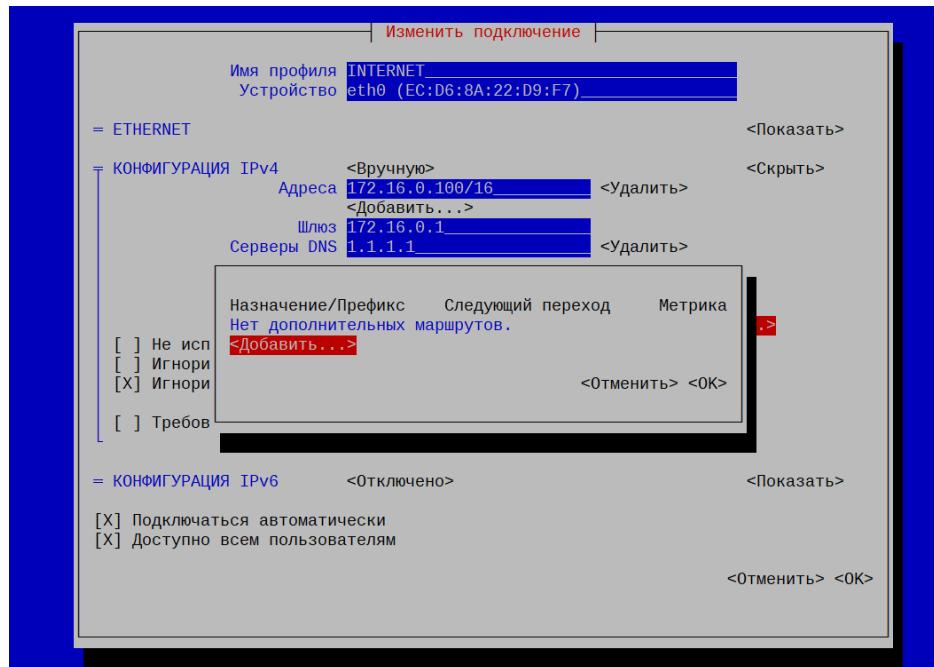


Рисунок 5 – Добавление статического маршрута

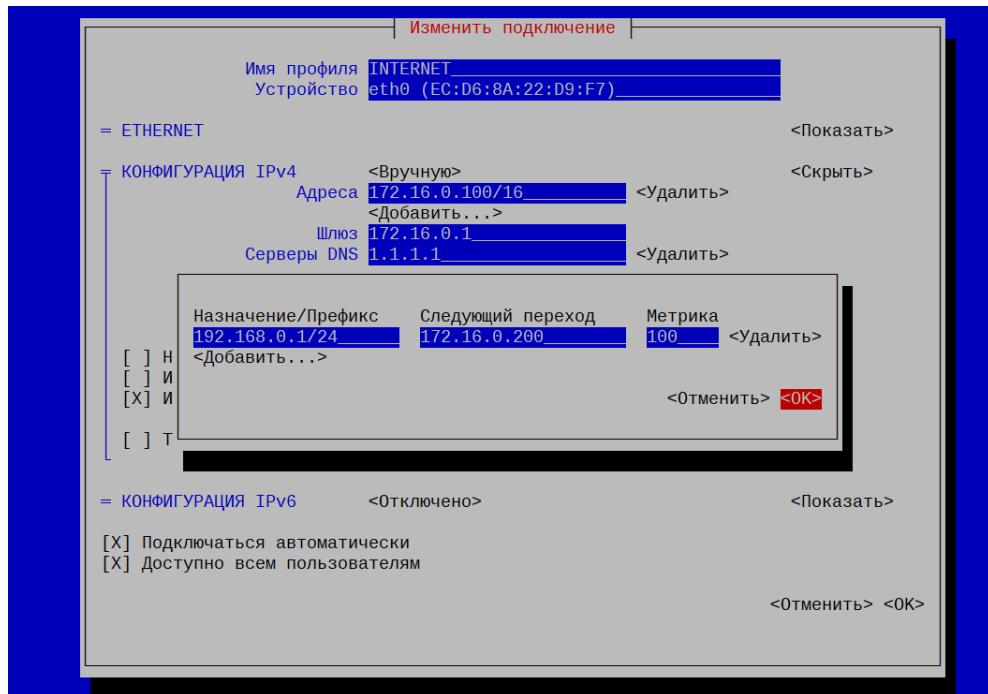


Рисунок 6 - Отображение статического маршрута

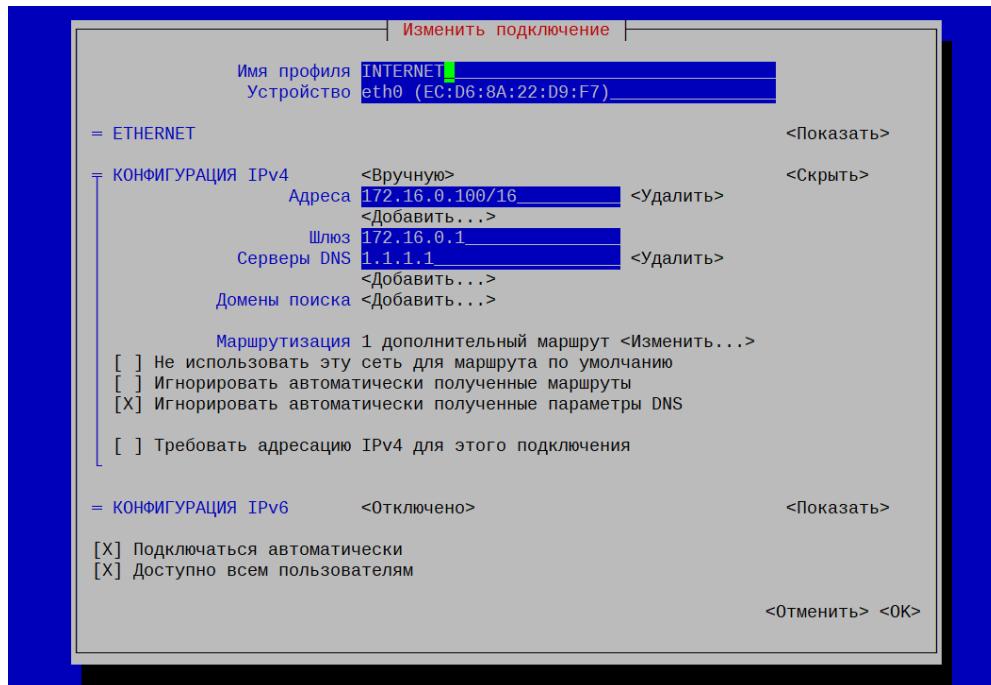


Рисунок 7 – Итоговые настройки соединения

Для применения изменений необходимо выбрать активируемое соединение и последовательно произвести действия Отключить → Включить. |(см. Рисунок 8).

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

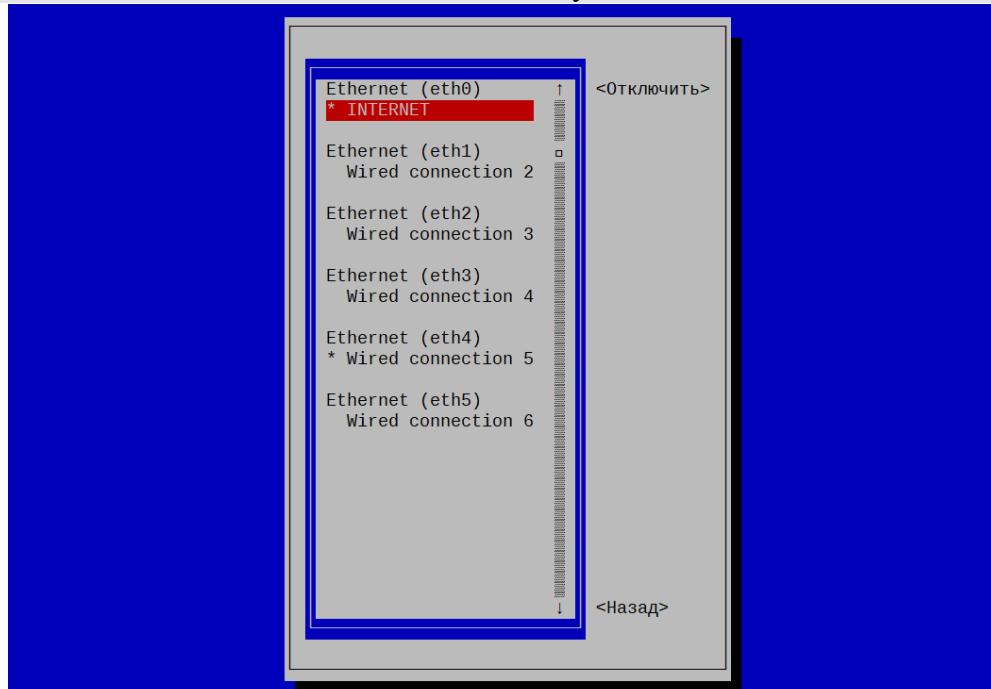


Рисунок 8 – Применение настроек подключения

Утилита позволяет переименовать ПК. Настройки применяются после перезагрузки ПК. |(см. Рисунок 9).

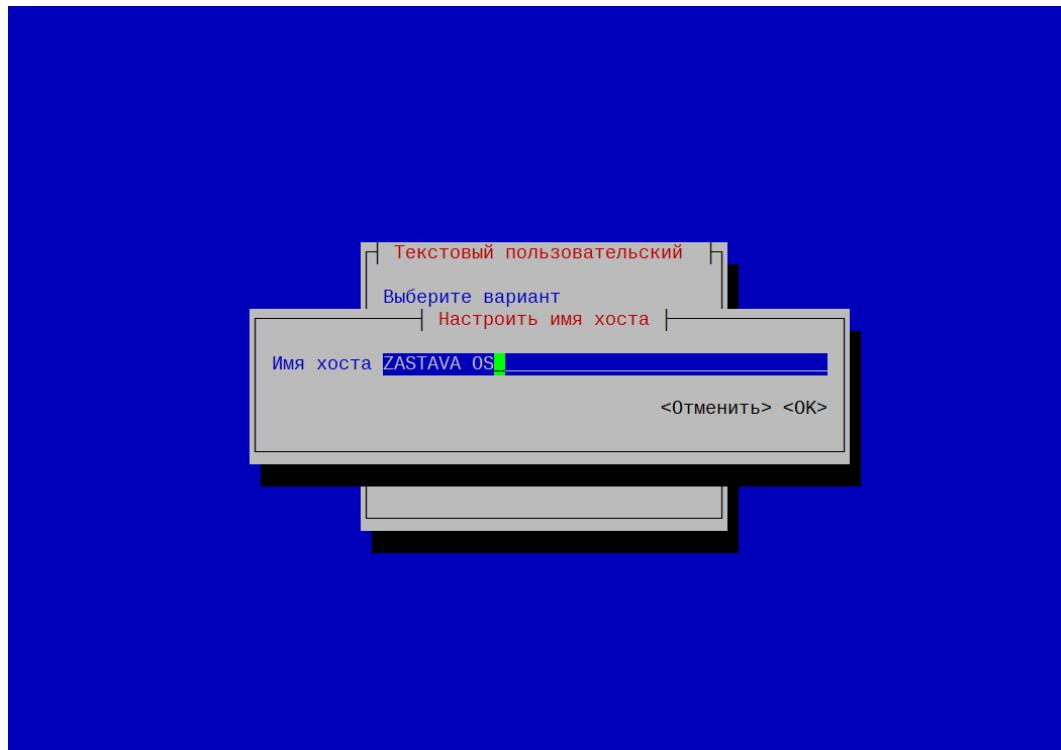


Рисунок 9 – Задание имени хоста

#### 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 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.
	Рекомендация задавать alias равными именами присвоенных сетевым соединениям.

### 4.5 Расширенные настройки сети

#### 4.5.1 Настройка автоматического синхронизации системного времени (NTP)

По умолчанию в ПК сервер NTP 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 серверов NTP-серверов ВНИИФТРИ\*: 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

<b>ntpq -p</b>									
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:

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

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

- 2) Задать сервера:

```
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
```

---

\* Подробно об актуальных адресах NTP-серверов можно узнать, открыв веб-сайт ВНИИФТРИ (<http://www.vniiftri.ru/ru/uslugi-serverov>)

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

Для настройки ПК в качестве источника времени от собственных системных часов ПК следует оставить только сервер.

```
server 127.127.1.0
```

4) После изменения настроек следует перезапустить ntpd:

```
/etc/init.d/S49ntp restart
```



Внимание для функционирования сервера NTP в качестве источника времени после перезапуска требуется значительное время ~6 минут. Статус можно посмотреть командой

```
ntpq -p
```

remote	refid	st	t	when	poll	reach	delay	offset	jitter
*LOCAL(0)	.LOCL.	5	1	19	64	37	0.000	+0.000	0.000

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

#### 4.5.2 Настройка удаленной регистрации событий (SYSLOG)

ПК 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 п. 0.

#### 4.5.3 Настройка мониторинга (SNMP)

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



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

Для настройки мониторинга ПК и отсылки трапов надо в оболочке BASH:

Скорректировать (текстовым редактором vi,vim,nano, редактором файл менеджера mc) файл *etc/snmp/snmpd.conf* следующего содержания:

```
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
sysName APK ZASTAVA-150
sysDescr ZASTAVA OS [версия OS генерируется автоматически]
agentAddress udp:<A.B.C.D адрес для мониторинга>:[порт SNMP по
умолчанию 161]

```

В оболочке BASH для принятия изменений перезапустить демон:

**/etc/init.d/S59snmpd restart**

Также для корректировки настройки мониторинга ПК можно использовать команды оболочки Klish в режиме enable.

Для указания конкретного адреса мониторинга.

**snmp set listening\_address <A.B.C.D адрес ПАК для снятия SNMP
статистики>**

Для задания локации сервера администратором.

**snmp set system sysLocation**

Для задания имени сервера администратором.

**snmp set system sysName**

Группа команд по работе с сервисом (перезапуск, останов, запуск)

**snmp service restart**  
**snmp service stop**  
**snmp service start**

#### 4.5.4 Настройка PROXY HTTP

Для того чтобы ПК функционировал в режиме proxy-сервер для обработки HTTP-трафика необходимо:

- 1) Открыть файл локальных настроек ПК (*/var/vpnagent/localsettings.ini*).
- 2) Заполнить секцию PROXY

```

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

```

- 3) Перезапустить службу **/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 ПК в ЦУП.

#### 4.5.5 Настройка DHCP сервера

Для того чтобы ПК функционировал в режиме dhcp-сервера необходимо:

- 1) Создать директорию /etc/default/
- 2) В директории /etc/default/ создать файл isc-dhcp-server
- 3) В этом файле прописать название интерфейса через который будет работать dhcpcd сервер. Например: (INTERFACES="eth2")
- 4) Открыть файл /etc/dhcp/dhcpd.conf. В файле задать параметры работы сервера

```
# If this DHCP server is the official DHCP server for the
local
# network, the authoritative directive should be uncommented.
authoritative; #обычно эта секция размещена после сетевых
настроек. Для корректного запуска ее необходимо разместить
выше

# option definitions common to all supported networks...
option subnet-mask 255.255.255.0;
option broadcast-address 10.222.1.255;
option routers 10.222.1.2;
option domain-name-servers 10.111.1.30;
option domain-name "offce.elvis.ru";

subnet 10.222.1.0 netmask 255.255.255.0 {
range 10.222.1.20 10.222.1.254;
interface eth2; # Важная строка, без неё сервер после
перезагрузки не запускается
}
```

```
default-lease-time 600;
max-lease-time 7200;
```

- 5) Сохранить файл конфигурации после внесения туда изменений
- 6) Запустить dhcpcd сервер с помощью команды **/etc/init.d/S80dhcp-server start**
- 7) Убедиться, что сервер запущен.
- 8) Перезагрузиться, убедиться, что сервер перезапускается после перезагрузки

```
[root@ZASTAVA OS: ~]# ps -ef | grep dhcp
root 936 1 0 08:35 ? 00:00:00 /usr/sbin/dhcpcd -q
root 1112 1104 0 08:38 ttys0 00:00:00 grep dhcp
```

#### 4.6 Включение двухфакторной аутентификации

Для включения режима двухфакторной аутентификации необходимо выполнить команду **set 2nd\_factor\_authorization {ESMART|RuToken}** в режиме enable.

После ввода команды **set 2nd\_factor\_authorization** отображается сообщение (при наличии импортированного доверенного сертификата):

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? (у/н)

Для включения режима двухфакторной аутентификации необходимо нажать клавишу «у». 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 2.2. Для отмены включения режима двухфакторной аутентификации необходимо нажать клавишу «п».

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

- в случае отсутствия импортированного доверенного сертификата;

Нет доверенных сертификатов. Включение двухфакторной авторизации невозможно.

Пожалуйста, сначала выполните импорт доверенного сертификата.

— в случае несоответствия предъявлennого персонального идентификатора требованиям:

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 ПК«ЗАСТАВА-Управление»**

Для того чтобы ПК получал политику безопасности с ПК «ЗАСТАВА-Управление» необходимо в ПК «ЗАСТАВА-Управление» (далее – центр управления политиками, ЦУП):

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

2) в свойствах объекта ПК:

- задать имя объекта;
- задать топологию объекта, в качестве логического имени интерфейса использовать псевдонимы (alias) интерфейсов, заданных на ПК;



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 ПК, для создания соединения;
- задать загрузчик;

3) выполнить трансляцию и активацию политики.

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

Подробная информация о списке доступных настроек ПК «ЗАСТАВА-Управление» находится в документе «Программный комплекс «ЗАСТАВА-Управление «VPN/FW «ЗАСТАВА», версия 6» Руководство администратора».

## 5 ОПИСАНИЕ СРЕДСТВ КОНФИГУРИРОВАНИЯ И МОНИТОРИНГА

Интерфейс конфигурирования и мониторинга программной части ПК представлен двумя видами командной оболочки: KLISH и BASH. Информация о работе с BASH представлена в разделе 0. Информация о работе с KLISH представлена в разделе 6.

После локальной аутентификации или удаленном управлении по SSH под учётной записью – admin для управления ПК Администратор ПК 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 ПК.
	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 ПК Администратор ПК 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 (т.н. Kommand Line Interface SHell для реализации Cisco-подобного интерфейса командной строки на Unix-системах).

KLISH позволяет сформировать различные списки команд, доступных для исполнения каждому из пользователей. Администратору ПК 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 представлен список таких команд (см. Таблица 1).

Таблица 1 – Негрупповые команды

Команда	Описание действия
<code>exit</code>	Выполнить выход из оболочки enable
<code>enable</code>	Выполнить вход в оболочку enable
<code>bash</code>	Выполнить вход в оболочку bash
<code>password</code>	Смена пароля
<code>check integrity</code>	Проверка целостности файлов агента безопасности ПК.
<code>snmp</code>	Настройка протокола snmp
<code>l2_tp_configure</code>	Настройка l2tp
<code>reboot</code>	Перезагрузка
<code>halt</code>	Выключение питания
<code>?</code>	Запросить справку об использовании команды

### 6.3 Команда смены пароля

Интерактивная команда по смене пароля. Производит смену пароля для текущей учётной записи.

```
> password
```

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:

Извините, но пароли не совпадают.

passwd: Службе паролей не удалось выполнить предварительную проверку.

passwd: Пароль не изменён

При задании нового пароля равного текущему.

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 (см. Таблица 2).

Таблица 2 – Команды с префиксом *show*

Ключ 1	Ключ 2	Описание действия
<b>log</b>	<b>audit</b>	Открыть, на просмотр, журнал аудита действий администратора
	<b>bin_log</b>	Просмотр журнала событий vpnaagent
<b>interfaces</b>	-	Вывести информацию о сетевых интерфейсах

Список доступных команд с префиксом *vpnconfig list* представлен в таблице (см. Таблица 3).

Таблица 3 – Команды с префиксом *vpnconfig list*

Ключ 1	Описание действия
<b>cert</b>	Вывести информацию о сертификатах
<b>ha</b>	Вывести информацию о настройках кластера

<b>Ключ 1</b>	<b>Описание действия</b>
<b>jk</b>	Вывести информацию о методах загрузки политики безопасности
<b>interface</b>	Вывести информацию об интерфейсах и их alias
<b>ike</b>	Вывести информацию о настройках IKE
<b>lsp</b>	Вывести информацию о текущем источнике получения политик безопасности
<b>log</b>	Вывести информацию о параметрах логирования
<b>provider</b>	Вывести информацию о криптовайдерах
<b>token</b>	Вывести информацию о токенах
<b>admin</b>	Вывести информацию об администраторской учетной записи ПО «ЗАСТАВА-Офис»

Список доступных команд с префиксом *vpnmonitor* представлен в таблице (см. Таблица 4).

Таблица 4 – Команды с префиксом *vpnmonitor*

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

Ключ 1	Ключ 2	Описание действия
<b>rri</b>	-	Вывести информацию таблицы reverse routing enjection
<b>proxy</b>	-	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

Группа команд выполнения настроек, начинаются с префиксов *set*, *vpnconfig*, *vpnmonitor* и *network*.

Список доступных команд с префиксом *set* представлен в таблице (см. Таблица 5).

Таблица 5 – Команды с префиксом *set*

Ключ 1	Ключ 2	Ключ 3	Ключ 4	Описание действия
<b>cron</b>	<b>job</b>	<b>reboot</b>	<b>&lt;time&gt;</b>	Изменить время ежедневной перезагрузки на time
		-	-	Открыть журнал заданий cron
<b>ntp</b>	<b>&lt;ip&gt;</b>			Добавить NTP сервер
<b>cluster</b>	<b>settings</b>	-	-	Открыть файл keeplaived.conf
	<b>mode</b>	<b>on</b>	-	Включить кластеризацию
		<b>off</b>	-	Выключить кластеризацию
<b>date</b>	<b>&lt;date&gt;</b>	-	-	Установить системную дату\время равной date
<b>timezone</b>	<b>&lt;zone&gt;</b>	<b>&lt;city&gt;</b>	-	Установить часовой пояс равный zone city
<b>zastava_syslog</b>	<b>&lt;facility&gt;</b>	<b>&lt;ip&gt;</b>	<b>&lt;порт&gt;</b>	Добавить syslog сервер с IP-адресом и портом, которому будут посыпаться события с источника facility
<b>BGP</b>	<b>on</b>	-	-	включает сервис поддержки протоколов динамической маршрутизации
	<b>off</b>	-	-	
<b>dhcp</b>				включает службу DHCP-server
<b>dhcp_rel</b>	<b>&lt;interface&gt;</b>			включает механизм переадресации запросов на получение сетевых настроек на указанный интерфейс
<b>Multi_wan_config_uration</b>	<b>on</b>			запускает интерактивную утилиту настройки простой реализации multi wan для двух операторов связи
<b>difffserv</b>				параметр, отвечающий за включение функции приоритизации трафика на основании поля ToS заголовка IP-пакета. difffserv=1 – приоритизация трафика включена. По умолчанию установлено значение «0».

Ключ 1	Ключ 2	Ключ 3	Ключ 4	Описание действия
<b>OSFP</b>	<b>on</b>	-	-	включает сервис поддержки протоколов динамической маршрутизации
	<b>off</b>	-	-	

Список доступных команд с префиксом `vpnconfig` представлен в таблице (см. Таблица 6).

Таблица 6 – Команды с префиксом `vpnconfig`

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

Ключ 1	Ключ 2	Ключ 3	Ключ 4	Описание действия
	<b>lsp</b>	<b>current</b>		Показать информацию о текущей политике безопасности

Команда `vpnconfig set <param><id><value>` позволяет выполнить установку основных параметров для групп НА, 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 (см. Таблица 7).

Таблица 7 – Команды с префиксом `vpnmonitor`

Ключ 1	Ключ 2	Описание действия
<b>single</b>	–	Перевести vрапгент в режим одиночного функционирования
<b>active</b>	–	Перевести vрапгент в режим кластера и сделать ноду активной
<b>passive</b>	–	Перевести vрапгент в режим кластера и сделать ноду пассивной

Список доступных команд с префиксом `network` представлен в таблице (см. Таблица 8).

Таблица 8 – Команды с префиксом `network`

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

Таблица 9 – Команды с префиксом `network connection`

Ключ 1	Ключ 2	Ключ 2	Описание действия
<b>show</b>	<b>&lt;id&gt; (н)</b>		Показать настройки соединения id
			Показать существующие соединения
<b>up</b>	<b>&lt;id&gt;</b>		Сделать активным соединение id
<b>down</b>	<b>&lt;id&gt;</b>		Сделать неактивным соединение id
<b>add</b>	–	–	Добавить новое соединение (см. Таблица 10)
<b>modify</b>	<b>&lt;id&gt;</b>	–	Изменить существующее соединение (см. Таблица 11)
<b>clone</b>	<b>&lt;id1&gt;</b>	<b>&lt;id2&gt;</b>	Скопировать соединение id1 в соединение с именем id2
<b>edit</b>	–	–	Отредактировать соединения
<b>delete</b>	<b>&lt;id&gt;</b>		Удалить соединение id
<b>monitor</b>	–		Отследить, в режиме реального времени, изменения в настройках соединения
<b>reload</b>	<b>&lt;id&gt;</b>		Перезагрузить соединение id
<b>load</b>	<b>&lt;path&gt;</b>		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
<b>type</b>	<b>ethernet</b>	<con-name>	<ifname>	<Master> (и)	Добавить соединение типа Ethernet с именем con-name применимое к интерфейсу ifname. Если указана опция master то соединение будет участником соединения с именем master
	<b>vlan</b>	<con-name>	<dev>	<id>	Добавить соединение типа vlan с именем con-name, которое будет использовать интерфейс dev и иметь VID id
	<b>bridge</b>	<con-name>	-	-	Добавить соединение типа bridge с именем con-name
	<b>bond</b>	<con-name>	-	-	Добавить соединение типа bond с именем con-name
	<b>tun</b>	<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
<b>ipv4.addresses</b>	<ip>	-	Установить ipv4-адрес для соединения равный IP-адресу
<b>ipv4.method</b>	<b>manual</b>	-	Изменить метод получения настроек соединения на ручной (т.н. static)
	<b>auto</b>	-	Изменить метод получения настроек соединения на автоматический, по протоколу DHCP
<b>autoconnect</b>	<b>yes</b>	-	Автоматически применять соединение в момент появления линка
	<b>no</b>	-	Не применять автоматически соединение в момент появления линка
<b>ipv4.dns</b>	<ip>	-	Установить DNS сервер ip для соединения. Замещает все существующие DNS сервера
<b>ipv4.gateway</b>	<ip>	-	Установить шлюз поумолчанию для соединения равный IP-адресу
<b>ipv4.dhcp-timeout</b>	<value>	-	Установить DHCP-timeout для соединения равный value
<b>vlan.id</b>	<id>	-	Изменить VID для соединения и сделать равным id
<b>vlan.parent</b>	<id>	-	Изменить parent для соединения и сделать равным id
<b>+ipv4.routes</b>	<net>	<hope>	Добавить дополнительный маршрут к соединению на сеть net через шлюз hope
<b>+ipv4.dns</b>	<ip>	-	Добавить дополнительный DNS сервер с IP-адресом для соединения
<b>-ipv4.routes</b>	<net>	-	Удалить дополнительный маршрут у соединения на сеть net
<b>-ipv4.dns</b>	<ip>	-	Удалить DNS сервер с IP-адресом

Таблица 12 – Команды с префиксом *snmp*

<b>Ключ 1</b>	<b>Ключ 2</b>	<b>Ключ 3</b>	<b>Ключ 4</b>	<b>Описание действия</b>
<b>set</b>	<b>listening_address</b>	<b>&lt;ip&gt;</b>	-	Задать адрес для мониторинга
<b>set</b>	<b>system</b>	<b>sysLocation</b>	<b>&lt;строка&gt;</b>	Задать локацию для мониторинга
<b>set</b>	<b>system</b>	<b>sysName</b>	<b>&lt;строка&gt;</b>	Задать имя сервера для мониторинга
<b>service</b>	<b>restart</b>	-	-	Рестарт службы SNMP
<b>service</b>	<b>stop</b>	-	-	Останов службы SNMP
<b>service</b>	<b>start</b>	-	-	Старт службы SNMP

## 6.6 Команды для диагностики состояния сетевого соединения

Список доступных команд для диагностики состояния сетевого соединения представлен в таблице (см. Таблица 13).

Таблица 13 – Диагностика состояния сетевого соединения

<b>ping {&lt;IP-address IPv6-address&gt; ip ipv6 arp}</b>		<b>Доступ к команде: АЕ</b>
1	<b>Ping &lt;IP-address IPv6-address&gt; {без дополнительного параметра source  repeat}</b>	Выполнить команду ping на <IP-address>
1.1	<b>без дополнительного параметра</b>	
1.2	<b>Source &lt;IP-address&gt;</b>	Выполнить команду ping на <IP-address> от IP-адреса шлюза, указанного в параметре source (например с заднего интерфейса шлюза)
1.3	<b>repeat</b>	Выполнить команду ping на <IP-address> указанное в параметре <b>repeat</b> число раз.
2	<b>ip ipv6 &lt;IP-address&gt; {без дополнительного параметра source size repeat interval resolve}</b>	
2.1	<b>без дополнительного параметра</b>	Выполнить команду ping на <IP-address>
2.2	<b>source &lt;IP-address&gt;</b>	Выполнить команду ping на <IP-address> от IP-адреса шлюза, указанного в параметре source (например с заднего интерфейса шлюза)
2.3	<b>size &lt;&gt;</b>	Выполнить команду ping на <IP-address> пакетами, указанного размера
2.4	<b>repeat &lt;целое число&gt;</b>	Выполнить команду ping на <IP-address> указанное в параметре число раз.
2.5	<b>interval &lt;целое число&gt;</b>	Выполнить команду ping на <IP-address> с интервалом между пакетами, указанным в параметре.
2.6	<b>resolve {source interval repeat flood broadcast  duplicate-detect size}</b>	

3	<b>arp &lt;Hostname or IP-address&gt;</b>	
3.1	<b>&lt;Hostname or IP-address&gt;</b>	Отправляет ARP-запрос на <Hostname> или <IP-address>
<b>traceroute {ip ipv6} &lt;IP-address IPv6-address&gt;</b>		<b>Доступ к команде: AE</b>
4	<b>ip &lt;IP-address&gt; {без дополнительного параметра   resolve source interface}</b>	
4.1	<b>без дополнительного параметра</b>	Трассировка маршрута до определенного IP-адреса
4.2	<b>source &lt;ip-address&gt;</b>	Трассировка маршрута до определенного IP-адреса от IP-адреса шлюза, указанного в параметре source.
4.3	<b>interface &lt;interface-name&gt;</b>	Трассировка маршрута до определенного IP-адреса от интерфейса шлюза, указанного в параметре interface.
4.4	<b>resolve {source interface}</b>	
4.4.1	<b>source &lt;ip-address&gt;</b>	Трассировка маршрута до определенного IP-адреса от IP-адреса шлюза, указанного в параметре source (с определением dns-имен).
4.4.2	<b>interface &lt;interface-name&gt;</b>	Трассировка маршрута до определенного IP-адреса от интерфейса шлюза, указанного в параметре interface (с определением dns-имен).
5	<b>ipv6 &lt;IPv6-address&gt; {без дополнительного параметра   resolve source interface}</b>	
5.1	<b>без дополнительного параметра</b>	Трассировка маршрута до определенного IP-адреса
5.2	<b>source &lt;ipv6-address&gt;</b>	Трассировка маршрута до определенного IP-адреса от IP-адреса шлюза, указанного в параметре source.
5.3	<b>interface &lt;interface-name&gt;</b>	Трассировка маршрута до определенного IP-адреса от интерфейса шлюза, указанного в параметре interface.
5.4	<b>resolve {source interface}</b>	
5.4.1	<b>source &lt;ipv6-address&gt;</b>	Трассировка маршрута до определенного IP-адреса от IP-адреса шлюза, указанного в параметре source (с определением dns-имен).
5.4.2	<b>interface &lt;interface-name&gt;</b>	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 (см. Таблица 14).

Резервированию подлежат сетевые настройки, локальные настройки агента безопасности ПК, 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 ПК в систему резервирования.
	Внимание! Требования правил пользования на ПК по обращению с ключевой информацией распространяются на локальный архив содержащий ключевой контейнер.

Таблица 14 – Резервирование и восстановление данных

<b>backup_and_restore &lt;Enter&gt;</b>			<b>Доступ к команде :AE</b>
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. Требует ввода PIN-кода, указания номера токена (если токен единственный, то необходимо указать 1), с которого будет выполнено восстановление данных.	
4	4	Выход из подпрограммы резервирования и восстановления данных	

## 7 ОПИСАНИЕ ДОСТУПНЫХ ОПЕРАЦИЙ ИНТЕРПРЕТАТОРА BASH

### 7.1 Обзор средств мониторинга

Для осуществления мониторинга работы ПО «ЗАСТАВА-Офис» используются следующие средства:

- журналы регистрации событий (bin\_log.txt, vpndmn\_init.log);
- системный журнал syslog;
- утилита vrpmonitor.

#### 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 символах;
- -n - сортировка строк по числовому значению;
- -r - сортировать в обратном порядке;
- -c – проверить, был ли отсортирован файл;
- -o - вывести результат в файл;
- -u - игнорировать повторяющиеся строки;
- -m - объединение ранее отсортированных 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 такой 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:

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

Описание параметров команды `vpmonitor -s` представлено в таблице (см. Таблица 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 (см. Таблица 16).

Таблица 16 – Печень параметров статистики

Параметр	Описание
<b>IPsec</b>	
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
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
<b>IKEv2</b>	
IKE SAs created (failed) initiated/responded	Количество созданных (не созданных) инициированных/ отвеченных IKE SA в формате

<b>Параметр</b>	<b>Описание</b>
	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 bundleless 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-existent 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) иницировано/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) иницировано/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 иницировано/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 иницировано/отправлено в формате x(x)/x(x)
INFO exchanges completed (with errors or failed) initiated/responded	Количество успешных (с ошибками или неуспешных) обменов INFORMATIONAL иницировано/отправлено в формате x(x)/x(x)
<b>НА</b>	
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

<b>Параметр</b>	<b>Описание</b>
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 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
<b>FiltDB Cache</b>	
Hash table size (bytes)	Размер хэш-таблицы (байт максимум/выделено) в

Параметр	Описание
max/alloc)	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
<b>Event Manager</b>	
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: 2016.04.26 11:23:58
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: 10.111.10.130
Title: GateWin131
Activated: Fri Jun 16 14:36:32 2017

```

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: 10.111.10.130
    cert subject: C=RU,CN=GateWin131_CPROCA2016
    log level: EVENTS

LSP active:
    type: System PMP
    file path:
    pmp servers: 10.111.10.130
    pmp cert subject: C=RU,CN=GateWin131_CPROCA2016
    pmp cert issuer: C=RU,O=AO ELVIS PLUS,OU=ORPO,CN=CPROCA2016
    pmp cert serial: 5600000080930538360CC5729B000000000080
    pmp cert key alg: GOST R 34.10-2001
    pmp log level: EVENTS
    title: GateWin131
    hash: BD5EB22D4EE4EE31C801457F7E9C5D06
    time: Mon Jun 19 10:19:47 2017
    in progress: false
    from DB: false
    cert present: true
    connected to TPN: true
    last error:
    diagnostic: System policy 'GateWin131' activated at Mon Jun 19
10:19:47
2017

```

#### 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      10.111.10.168      (DN) C=RU,O=Элвис
Плюс,OU=Отдел разработки ПО,CN=WIN 7_32,E=mozhaeva@elvas.ru GOST3410.2001-Sig /
GOST3410.2001-Sig
    1      ESP(Tunnel) Responder 10.111.10.168 ->
192.168.21.0..192.168.21.255 rule_ipsec
    35644A41932BB5E394.3ED09011BE4EE9D0      10.111.10.130      (DN)
C=RU,CN=win_130_gost3      GOST3410.2001-Sig / GOST3410.2001-Sig
    AE746FD322B297DB.820EE0D33788D2BA      10.111.10.132      (DN)
C=RU,CN=Client132_EPCSP      GOST3410.2001-Sig / GOST3410.2001-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. Таблица 17 и Таблица 18),

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

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

Параметры фильтрации протокола IKE SA приведены в таблице (см. Таблица 19).

Таблица 17 – Параметры фильтрации протокола IKE SA

Параметр	Характеристика
<code>type</code>	Тип создания SA
<code>mode</code>	Режим создания SA
<code>role</code>	Роль локальной машины при создании SA
<code>state</code>	Состояние IKE SA
<code>eapid_local</code>	Локальный EAP ID
<code>ikeid_local</code>	Локальный IKE ID
<code>eapid_remote</code>	EAP ID партнера

Параметр	Характеристика
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
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 (см. Таблица 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

Тип	Характеристика
	(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)
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 декапсулации (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 декапсулации (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)
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	
icontains	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

Команда	Характеристика
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 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.exe -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 10.111.6.97
```

```
vpnmonitor -i -ike-sa peer_ip equal 10.111.6.97 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-программистом.

#### 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 (см. Таблица 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. Таблица 20),

**operation** – операция для произведения сравнения по выбранному полю с эталоном (см. Таблица 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 «Фаерволльные 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
Операции для фильтрации по содержанию строк	
icontains	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

Команда	Характеристика
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 vpnmmonitor -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:

```
vpnmmonitor -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 vpnmmonitor -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 (см. Таблица 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 vpnmmonitor -ike-cfg:

```
192.168.21.30 (DN) C=RU,O=Элвис Плюс,OU=Отдел разработки ПО,CN=WIN XP  
[3FF4381E8440F4F8] 10.111.10.226 Allocated 2015.03.13 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 «ЗАСТАВА-Офис» 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 «ЗАСТАВА-Офис» с включенным RRI автоматически вносится запись омаршруте к удаленной сети партнера или клиенту. При нарушении защищенного соединения добавленный маршрут из таблицы маршрутизации ПО «ЗАСТАВА-Офис» 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>**

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

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

## 7.2 Обзор средств конфигурирования

Для конфигурирования ПО «ЗАСТАВА-Офис» используются следующие средства:

- утилита vpnconfig;
- утилита plg\_ctl;
- утилита icv\_checker (используется для проверки КС);
- команды программной составляющей ПК.

### 7.2.1 Утилита vpnconfig

Утилита конфигурирования **vpnconfig** предназначена для изменения и просмотра локальных установок ПО «ЗАСТАВА-Офис». При штатной работе ПО «ЗАСТАВА-Офис» 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 «ЗАСТАВА-Офис»

Для получения информации о ПО «ЗАСТАВА-Офис» необходимо воспользоваться командой:

```
vpnconfig -ver
```

Пример вывода команды:

```
Product name: ZASTAVA Office
Vendor name: AO ELVIS-PLUS
Product build: 6.3.16253
Product release: 6.3
Build date: 2016/03/30 17:35
Product/platform information: GATE LINUX x64
```

#### 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 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 (см. Таблица 24).

Таблица 24 – Свойства сертификата

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

Свойство	Описание
Действителен с	Начальная дата действия сертификата
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 списков отзыва сертификатов (COC), 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 COC; – <Issuer Value>- имя организации, выпустившей COC.
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 ПК 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:

3) выполнить команду: **vpnconfig add cert <path> password [password]**,

где: [**<password>**] – пароль доступа к PKCS#12 контейнеру;

4) 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 в ПО «ЗАСТАВА-Офис». 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 (см. Таблица 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

Ключ	Описание действия
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> <e-mail> <upn>	Опциональные поля AltSubjectName
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 токенов (`InternalCrypto`, `ESMARTToken GOST`, `Rutoken ECP`), в системе 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-150-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-150-key512" eku=ipsec
```

Пример команды генерации ключа и запроса на издание сертификата для входа в ПК 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. Подробности требований к сертификатам для входа в ПК в подразделе 2.2.

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+0YAg0JDQn9CaMR4wHAYJKoZIhvNAQkBf91c2VyQGRvbWFpbis5uZXQw
ZjAfBggqhQMHAQEBAТАTBgcqhQMCAiMBBggqhQMHAQECAgNDAARAtUeSOEcaj1+U
LNFUma0mJk340WOSOBjDeabeDFkkPu92Pp7EtCuetvZgmEX5FCNscv6AoO7ewZH
XRY2cPA05qCB1DCBkQYJKoZIhvNAQkOMYGDMIGAMA4GA1UdDwEB/wQEAWIFoDAV
BgNVHSUEDjAMBgorBgEEAYI3FAICMCoGA1UdEQQjMCGgHwYKKwYBBAGCNxQCA6AR
DA9hZG1pbkBsb2NhbGhv3QwKwyDVR0QBCQwIoAPMjAyMzA4MzAxMzQxMDVagQ8y
MDI0MTEzMDEzNDEwNVowCgYIKoUDBwEBAwIDQQARQLAc52wTDwayStDSkDLdFEnO
R3sif3EcuCKU3TzhQ5frNQiyp2JYCiQDX5ZT7byC6KBE/ANa7kToQc32GrnE
-----END CERTIFICATE REQUEST-----
```



Пример дан с заполнением всех возможных полей в 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 ПК 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 ПК 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
ПК, 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

#	Имя параметра	Псевдоним параметра	Имя
0	Logon on	LOGON_ON	Используется для включение двухфакторной аутентификации на ОС семейства WINDOWS, на ПК 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 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 <code>vpnconfig -list token verbose</code> (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 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 или проверки сертификатов после перезапуска службы агента безопасности или рестарата ПК 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 Импортование СОС вручную

Можно в любое время вручную импортировать СОС. Процесс импорта – тот же самый, что и при регистрации сертификата. Чтобы зарегистрировать СОС в «ЗАСТАВА-Офис» 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 «ЗАСТАВА-Офис»

###### 7.2.1.4.1.1 Системная ЛПБ

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



Для ПК запрещается устанавливать параметр «Системная политика» в значение загрузки политики из файла.

Для настройки системной политики необходимо:

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

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

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

где:

**<server>** – адрес сервера загрузки;

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

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

**<log\_level>** – уровень журналирования событий;

**<timeout>** – временной промежуток между обращениями к серверу.

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



Вместе с настройками параметров политики возможна одновременная активации. Для этого надо дать команду с префиксом -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 ПК – до момента загрузки рабочей ЛПБ, в случае если произошла ошибка при загрузке 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 не возможно, 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 прорузчика

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

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

где: **<server ip>** – IP-адрес ЦУП, с которого прорузчик 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. Таблица 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 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

#	Имя псевдонима	Псевдоним	Расшифровка
			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 «ЗАСТАВА-Офис»

#### 7.2.1.6 Параметры журнала Syslog

ПО «ЗАСТАВА-Офис» 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 <ikey>
```

2) для изменения настроек протокола надо выполнить команду:

```
vpnconfig -set <ikey> <id-parameter> <value>
```

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

```
vpnconfig -reset <ikey> <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 (см. Таблица 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_HALFOOPEN	Максимальное количество IKE соединений в процессе создания SA, в которых нет подтверждения IP-адреса партнера (0-256, по 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 посыпался с несуществующего IP-адреса, то COOKIE инициатором получено не будет и, соответственно, не будет возвращено. Если же адрес был реальным, то инициатор повторно посыпает запрос,

#	Имя	Псевдоним	Назначение
			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 посыпает 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 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 паззов 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 паззов (0-31, по умолчанию 16)
10	Servers selecting	SERVERS_POLICY	Политика выбора серверов (по

#	Имя	Псевдоним	Назначение
	policy		умолчанию – Try servers sequentially)
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 of SA exceeds	REDIRECT_AUTH	Перенаправлять аутентифицированных инициаторов если превышено 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 отсыпать 1 – не более 1/сек 10 – не более 10/сек (по

#	Имя	Псевдоним	Назначение
			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 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-

#	Имя	Псевдоним	Назначение
			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_REPLY_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; 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:

#	Имя	Псевдоним	Назначение
			<p>ip rule add from all lookup &lt;table id&gt;, где: &lt;table id&gt; – номер таблицы, который задан в локальных настройках (RRI table id), в противном случае те маршруты, которые прописываются в таблицу с номером &lt;table id&gt;, система не видит.</p> <p>Пример команды: ip rule add from all lookup 111</p> <p>Для удаления правила нужно вызвать команду: ip rule del table &lt;table id&gt;</p>
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	<p>Параметр, регулирующий режимы обработки CRL (по умолчанию 0). Возможные значения:</p> <ul style="list-style-type: none"> <li>— - Disabled (Выключена) (используется по умолчанию);</li> <li>— - Enabled, revoke also if CRL not available (Включена, отывать, если CRL недоступен);</li> <li>— - Enabled, don't revoke if CRL not available (Включена, не отывать, если CRL недоступен) .</li> </ul>
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 «ЗАСТАВА Офис».

#### 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 на ПК 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 (см. Таблица 29).

Таблица 29 – Режимы работы обработки СОС

Числовое значение	Режим работы обработки СОС
-------------------	----------------------------

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

Таймаут при загрузке СОС 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. Таблица 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 отсутствует 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 отсутствует по трассе прохождения пакетов.

#### 7.2.1.8 Токены

Агенты безопасности позволяет использовать токены как среду транспортировки важной информации (сертификатов, закрытых ключей). ПО «ЗАСТАВА-Офис» 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

ПК имеет фиксированный набор провайдеров. Добавление модулей не требуется.

##### 7.2.1.8.3 Удаление модуля токена

ПК 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 «ЗАСТАВА-Офис»

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).

#### 7.2.1.1 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 ПК.

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 ПК 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\_control\_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 ПК

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

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/messages
```

### 7.2.3.2 Конфигурирование модуля vpncsrp

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

```
vpnconfig -set pcap <id> <value>
```

Параметры модуля vpncsrp приведены в таблице (см. Таблица 28).

Таблица 31 – Параметры протокола IKE

#	Имя	Псевдоним	Назначение
0	pkt_queue	PKT_QUEUE	размер очереди пакетов, поступающих на обработку/фильтрацию
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_inv	FCACHE_ALWAYS_	сбрасывать(инвалидировать) весь кеш

#	Имя	Псевдоним	Назначение
	alidate	INVALIDATE	фильтров при создании/удалении динамических фильтров, 1 – вкл, 0 – выкл*. Если выключено, то при создании/удалении динамических фильтров будут удаляться 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 vpncap есть параметр pcap\_defcfg, определяющий политику драйвера, действующую во время загрузки программной составляющей с момента загрузки драйвера vpncap 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 vpncap
/sbin/modprobe vpncap 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 (см. Таблица 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, modem)
	S45network-manager		Запускает демон NetworkManager
	S46vpngate_pcap		Запуск сетевого перехватчика пакетов для ПО «ЗАСТАВА-Офис»
	S47vpngate		Запуск ПО «ЗАСТАВА-Офис»
	S49ntp		Запуск демона точного времени
	S50sshd		Запуск демона SecurityShell
	S59snmpd		Запуск демона Simple Network Management Protocol
	S70keepalived		Запуск демона высокой сетевой доступности keepalived
	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 ПК, 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 «ЗАСТАВА-Офис» 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 «ЗАСТАВА-Офис» в составе кластера необходимо произвести следующие настройки:

Для работы ПО «ЗАСТАВА-Офис» 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 (см.подраздел 8.3.1);
- выполнить настройки ПО «ЗАСТАВА-Офис» для включения режима синхронизации IKEv2 состояний (см. подраздел 8.3.2).
- описать в ГПБ (см. документацию на ЦУП) объект типа шлюз в кластерном исполнении.

Рассмотрим на примере создания типовой конфигурации кластера:

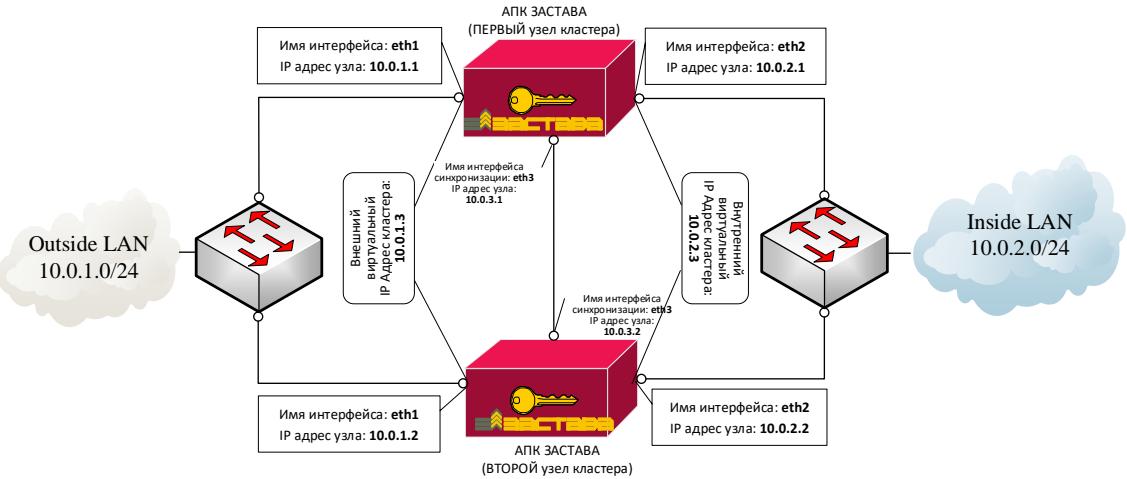


Рисунок 10 – Пример топологии кластера

## 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:

```
# set cluster settings
```

Запустится мастера.

### 8.1.1 Меню мастера настройки кластера:

Это мастер автоматизирует настройки ПК 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, дополнительно пункт 4.



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

### 8.1.2 Пункт 1 – Настроить ПО keepalive:

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**

8.1.3 Пункт 2 – Настроить ПО ЗАСТАВА:

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

8.1.4 Пункт 3 – Применить настройки ПО:

Выберите:

**3**

Запустится диалог:

Если в ПК ранее была проведена настройка кластера будет задан вопрос

Вы хотите перезаписать текущую конфигурацию? (y/n)

**Y**

В случае утвердительного ответа, либо конфигурация на данный момент отсутствует, 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
```

#### 8.1.5 Пункт 4 – Передать настройки ПО на другой узел по сети:

Мастером предусмотрена возможность по автоматизации передачи настроек на второго (BACKUP) узла 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 ПО keepalived и ПО ЗАСТАВА для второго (BACKUP) узла кластера.

Нажмите клавишу Enter для продолжения

#### 8.1.6 Пункт 5 – Посмотреть текущие настройки

Выберите :

**5**

В консоли отобразятся сведения о настройках ПО 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

#### 8.1.7 Пункт 69 – Очистить все настройки:

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

8.1.8 Пункт 6 – Выход:

Выберите:

**6**

Произойдёт возврат в оболочку Klish.

## 8.2 Настройка ПО keepalived

### 8.3 Настройка кластера вручную

8.3.1 Настройки ПО keepalived

Для настройки ПО keepalived в оболочке BASH:

Скорректировать (текстовым редактором vi, vim, nano, редактором файла 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
    # различия 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_inside
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
# различия 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 над
    # 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 ПО keepalive:

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

### 8.3.2 Настройка синхронизации состояний IKEv2

Для настройки ПО ЗАСТАВА-Офис (далее – агент безопасности ПК) в режима 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 16-ричном формате с помощью команды `vpnconfig -set ike QCD_secret <value>` где `value` (от `8` до `20` шестнадцатеричных цифр).

#### **8.4 Настройка маршрутизации при работе с кластером**

При использовании в сетевой инфраструктуре кластера ПК необходимо, чтобы в сетевых настройках устройств, которые имеет маршруты через кластер, в качестве шлюза по умолчанию были заданы виртуальные IP-адреса кластера ПК (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 ПК 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. Рисунок 11).

```
доброНожаловать в интерфейс настройки L2 шифрования
1. Необходимо задать интерфейс перехватчик
2. Необходимо задать интерфейс на котором происходит шифрование
На данном криптошлюзе имеются 8 ядер процессора

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
█
```

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 (суммарное кол-во ядер используемое для всех настроенных на ПК соединений не должно превышать минимальное кол-во доступных ядер среди всех взаимодействующих ПК);
- 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 рисунке (см. Рисунок 12).

```

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
2
Пожалуйста, называйте соединение так, что бы было отличие хотя бы в одном из ПЕРВЫХ СЕМИ
символов (например 12tp_1_con, 12tp_2_con)
В противном случае соединение просто не сможет быть применено т.к. названия будут совпада-
ть.
Это связано с ограничением на длину названия соединения в Linux. Хороший пример названий
Moscow, Spb, hospital, cod, office и т.д.
Введите название соединения >>
con1
Введите имя интерфейса перехватчика >>
eth5
Введите имя интерфейса шифрования >>
eth0
Введите IP-адрес интерфейса шифрования >>
10.111.6.113
Введите IP-адрес интерфейса шифрования партнера >>
10.111.6.101
Будет ли соединение участником какого-либо объединения (название). Нажите Enter если не т-
ребуется >>
Введите количество ядер для данного соединения >>
2
L2tpv3 соединение успешно создано

Передать соединение партнеру? (у/н)
у
Профильт соединения будет отправлено партнеру на его внешний адрес: 10.111.6.101
Введите имя пользователя на удаленном АПК:
admin
admin@10.111.6.101:
(Admin@10.111.6.101) Password:
con1.conf
100% 157 9.6KB/s 00:00
Не забудьте перенести соединение из папки /home/пользователь/Соединение.conf в папку /etc/
/12_conf/ на удаленном АПК перед стартом

```

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 OS: /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 созданных соединения необходимо:

- 1) выбрать пункт меню «1». Будет отображен список всех настроенных соединений (см. Рисунок 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. Рисунок 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. Рисунок 15).

```

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
3
Сейчас настроено 1 соединений, вот их список:
11
введите название соединения для удаления или введите ESC для выхода в предыдущее меню
11
удалить соединение 11.conf ? (y/n)
у
Профиль удален
для завершения нажмите любую клавишу

```

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. Рисунок 16).

```

[root@ZASTAVA OS: /home/admin]# /sbin/L2_create.sh start con1
Соединение con1 успешно создано
[root@ZASTAVA OS: /home/admin]# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 brd 127.255.255.255 scope host lo
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1608 qdisc mq state UP group default qlen 1000
    link/ether ec:d6:8a:22:d4:1b brd ff:ff:ff:ff:ff:ff
    inet 10.111.6.113/24 brd 10.111.6.255 scope global dynamic noprefixroute eth0
        valid_lft 949178sec preferred_lft 949178sec
3: eth1: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc mq state DOWN group default qlen 1000
    link/ether ec:d6:8a:22:d4:1c brd ff:ff:ff:ff:ff:ff
4: eth2: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc mq state DOWN group default qlen 1000
    link/ether ec:d6:8a:22:d4:1d brd ff:ff:ff:ff:ff:ff
5: eth3: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc mq state DOWN group default qlen 1000
    link/ether ec:d6:8a:22:d4:1e brd ff:ff:ff:ff:ff:ff
6: eth4: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc mq state DOWN group default qlen 1000
    link/ether ec:d6:8a:22:d4:1f brd ff:ff:ff:ff:ff:ff
7: eth5: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1608 qdisc mq master br_con1 state UP group default qlen 1000
    link/ether ec:d6:8a:22:d4:20 brd ff:ff:ff:ff:ff:ff
8: ip_vti0@NONE: <NOARP> mtu 1480 qdisc noop state DOWN group default qlen 1000
    link/ipip 0.0.0.0 brd 0.0.0.0
9: bond0: <BROADCAST,MULTICAST,MASTER> mtu 1500 qdisc noop state DOWN group default qlen 1000
    link/ether 6a:d3:f1:57:d2:e1 brd ff:ff:ff:ff:ff:ff
14: bo_l2_con1: <BROADCAST,MULTICAST,MASTER,UP,LOWER_UP> mtu 1608 qdisc noqueue master br_con1 state UP group default qlen 1000
    link/ether a6:f2:e5:02:56:e4 brd ff:ff:ff:ff:ff:ff
15: L2_TP_2: <BROADCAST,MULTICAST,SLAVE,UP,LOWER_UP> mtu 1608 qdisc pfifo_fast master bo_l2_con1 state UNKNOWN group default qlen 1000
    link/ether a6:f2:e5:02:56:e4 brd ff:ff:ff:ff:ff:ff
16: L2_TP_3: <BROADCAST,MULTICAST,SLAVE,UP,LOWER_UP> mtu 1608 qdisc pfifo_fast master bo_l2_con1 state UNKNOWN group default qlen 1000
    link/ether a6:f2:e5:02:56:e4 brd ff:ff:ff:ff:ff:ff
17: br_con1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1608 qdisc noqueue state UP group default qlen 1000
    link/ether a6:f2:e5:02:56:e4 brd ff:ff:ff:ff:ff:ff

```

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 ПК 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 ПК.

#### 10.1.1 Конфигурация стенда

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

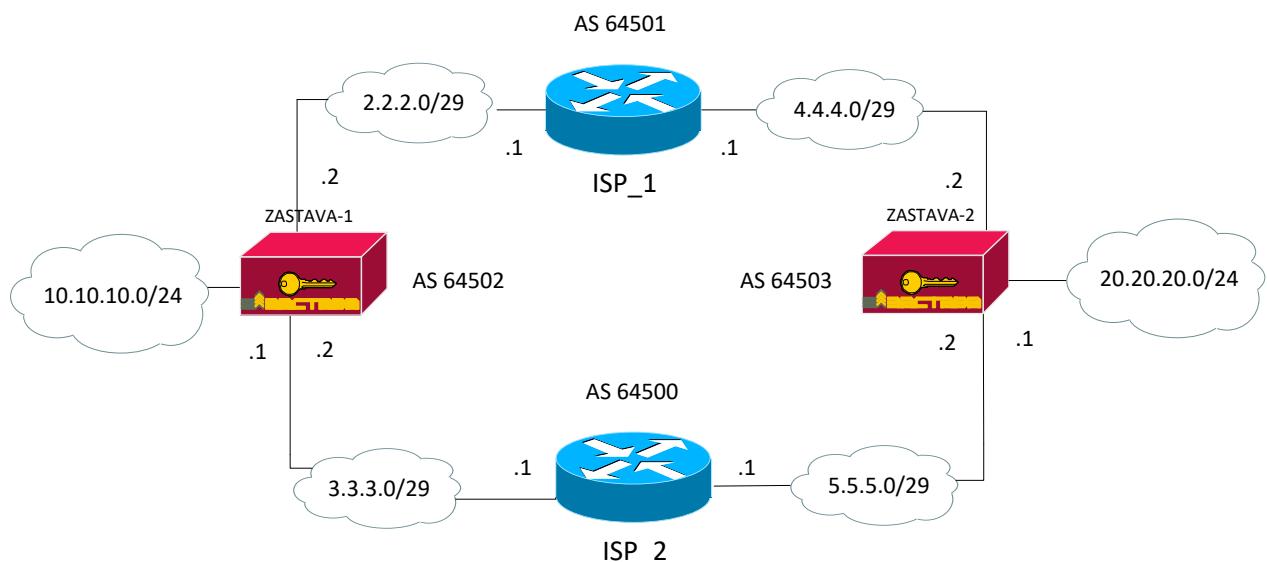


Рисунок 17 – Схема стенда для проверки работы с BGP

#### 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: OC ALT Linux, пакет quagga, пакет NetworkManager;
- 2) ISP\_2: OC 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:

1) ISP\_1:

–Выполнить настройку интерфейсов командой

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

–Поставить службы zebra и bgpd в автозагрузку командами:

```
systemctl enable zebra
```

```
systemctl enable bgpd
```

–Запустить службы zebra и bgpd командами:

```
systemctl start zebra
```

```
systemctl start bgpd
```

–Выполнить вход в интерпретатор Cisco-Like Sheel командой **vtysh**

–Перейти в режим конфигурации командой **configure terminal**

–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
```

–Выполнить выход командой **exit** и затем ещё раз **exit**

–Сохранить конфигурацию командой **write**

–Выполнить выход из интерпретатора Cisco-Like Sheel командой **exit**

2) ISP\_2:

–Выполнить настройку интерфейсов командой

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

–Поставить службы zebra и bgpd в автозагрузку командами:

```
systemctl enable zebra
```

```
systemctl enable bgpd
```

–Запустить службы zebra и bgpd командами:

```
systemctl start zebra
systemctl start bgpd
```

–Выполнить вход в интерпретатор Cisco-Like Sheel командой **vtysh**

–Перейти в режим конфигурации командой **configure terminal**

–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
```

–Выполнить выход командой **exit** и затем ещё раз **exit**

–Сохранить конфигурацию командой **write**

–Выполнить выход из интерпретатора Cisco-Like Sheel командой **exit**

### 3) ZASTAVA-1:

–Перейти в режим enable командой *enable*

–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>
```

–Запустить службу bgpd командой **set BGP on AS 64502**

–Выполнить вход в интерпретатор Cisco-Like Sheel командой

```
set BGP settings
```

–Перейти в режим конфигурации командой **configure terminal**

–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
```

- Выполнить выход командой **exit** и затем ещё раз **exit**
- Сохранить конфигурацию командой **write**
- Выполнить выход из интерпретатора Cisco-Like Sheel командой **exit**

4) ZASTAVA-2:

- Перейти в режим enable командой **enable**
- Выполнить настройку интерфейсов командами

```
network connection add type ethernet con-name <имя_соединения>
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>
```

- Запустить службу bgpd командой **set BGP on AS 64503**

- Выполнить вход в интерпретатор Cisco-Like Sheel командой:

**set BGP settings**

- Перейти в режим конфигурации командой **configure terminal**

- 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
```

- Выполнить выход командой **exit** и затем ещё раз **exit**
- Сохранить конфигурацию командой **write**
- 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 на ПК 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. Рисунок 18).

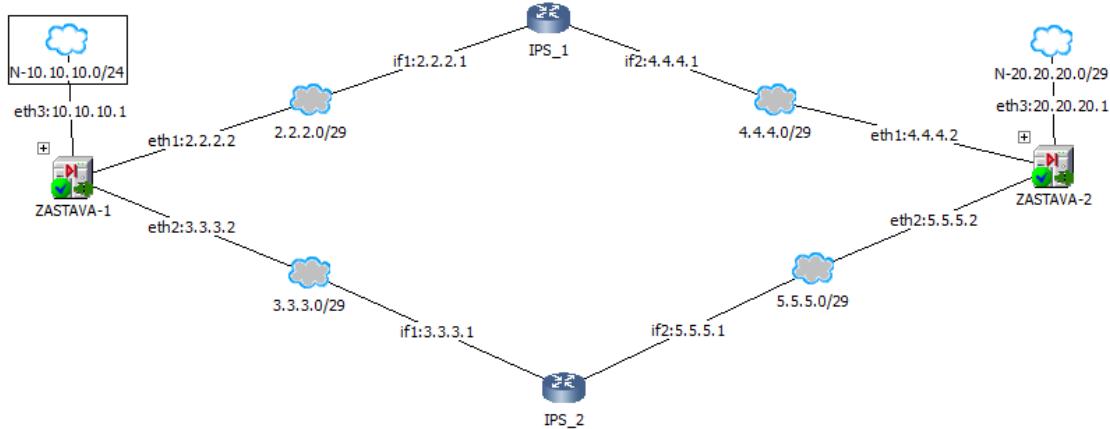


Рисунок 18 – Топология в графической консоли «ЗАСТАВА-Управление»

После создания необходимых объектов и правила, 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 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-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 траффик
- 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 ПК и двух маршрутизаторах, 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 ПК.

### 10.2.1 Конфигурация стенда

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

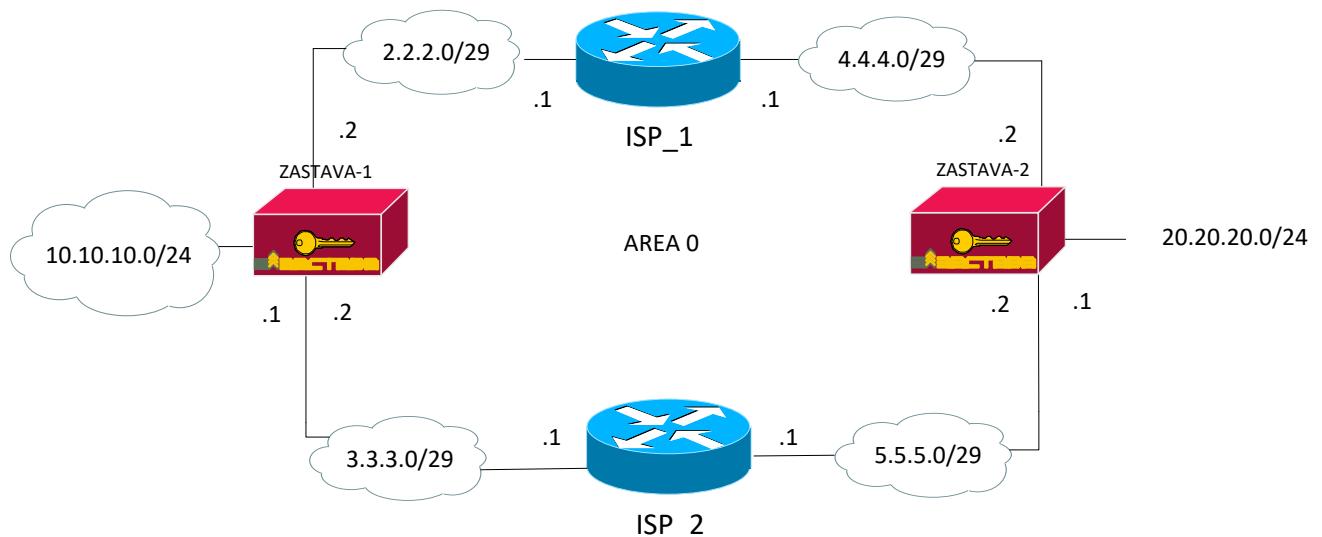


Рисунок 19 - Схема стенда для проверки работы с BGP

### 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: OC ALT Linux, пакет quagga, пакет NetworkManager;
- 2) ISP\_2: OC 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:

#### 1) ISP\_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
```

–Поставить службы zebra и bgpd в автозагрузку командами:

```
systemctl enable zebra
systemctl enable ospfd
```

–Запустить службы zebra и bgpd командами:

```
systemctl start zebra
systemctl enable ospfd
```

–Выполнить вход в интерпретатор Cisco-Like Sheel командой **vtysh**

–Перейти в режим конфигурации командой **configure terminal**

–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
```

–Выполнить выход командой **exit** и затем ещё раз **exit**

–Сохранить конфигурацию командой **write**

–Выполнить выход из интерпретатора Cisco-Like Sheel командой **exit**

#### 2) ISP\_2:

–Выполнить настройку интерфейсов командой

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

–Поставить службы zebra и bgpd в автозагрузку командами:

```
systemctl enable zebra
```

```
systemctl enable ospf
```

–Запустить службы zebra и bgpd командами:

```
systemctl start zebra
```

```
systemctl start ospf
```

–Выполнить вход в интерпретатор Cisco-Like Sheel командой **vtysh**

–Перейти в режим конфигурации командой **configure terminal**

–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
```

–Выполнить выход командой **exit** и затем ещё раз **exit**

–Сохранить конфигурацию командой **write**

–Выполнить выход из интерпретатора Cisco-Like Sheel командой **exit**

### 3) ZASTAVA-1:

–Перейти в режим enable командой **enable**

–Выполнить настройку интерфейсов командами

```
network connection add type ethernet con-name
<имя_соединения> iface <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>
```

–Запустить службу bgpd командой **set OSPF on**

–Выполнить вход в интерпретатор Cisco-Like Sheel командой  
**set OSPF settings**

–Перейти в режим конфигурации командой **configure terminal**

–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_интерфеса_с_адресом_10.10.10.1>
```

–Выполнить выход командой **exit** и затем ещё раз **exit**

–Сохранить конфигурацию командой **write**

–Выполнить выход из интерпретатора Cisco-Like Sheel командой **exit**

#### 4) ZASTAVA-2:

–Перейти в режим enable командой **enable**

–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>
```

–Запустить службу bgpd командой **set OSPF on**

–Выполнить вход в интерпретатор Cisco-Like Sheel командой:

```
set OSPF settings
```

–Перейти в режим конфигурации командой **configure terminal**

–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_интерфеса_с_адресом_20.20.20.1>
–Выполнить выход командой exit и затем ещё раз exit
–Сохранить конфигурацию командой write
–Выполнить выход из интерпретатора Cisco-Like Shell командой exit
```

#### 10.2.4 Проверка правильности настройки стенда

Стенд считается настроенным правильно, когда выполнены следующие условия:

- 1) В таблице маршрутов на ПК 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. Рисунок 20).

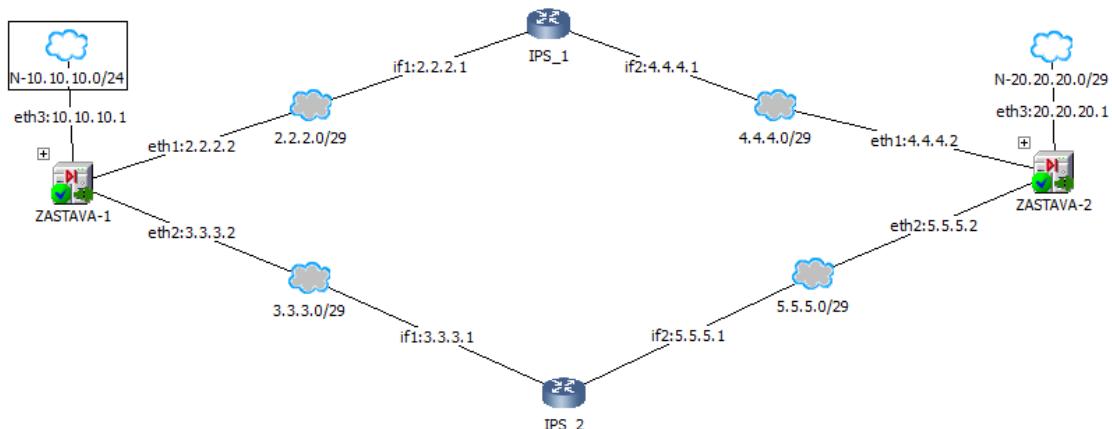


Рисунок 20 – Топология в графической консоли «ЗАСТАВА-Управление»

После создания необходимых объектов и правила, 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: ~]# vpngmonitor -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 ПК потребитель должен самостоятельно получить на предприятии-поставщике (изготовителе) ПК согласно договору на поставку и/или техническую поддержку образ обновления на CD или USB-flash обновляемого ПО 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 ПК , 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 установившейся программной составляющей ПК . Для этого необходимо:

- Включить ПК , нажав кнопку питания , 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 ПК , нажав кнопку питания;
- Включить ПК , нажав кнопку питания , дождаться появления меню выбора вариантов загрузки;
- Выбрать пункт меню «ZasOS» 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 ПК 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 ПК«ЗАСТАВА-Управление»

Обновление осуществляется по протоколу http.



**Использование незащищенного канала обновления ЗАПРЕЩЕНО!**

Для настройки сервера обновлений необходимо (сервер обновления настраивается в ПК «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=6.5.18999
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\:
XЭШ_LIVE_UPG /g' /.image/syslinux/filelist.hash && mount -o remount,ro /image
hash=XЭШ_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 – редактируемые; 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 ПК согласно ЛПБ при использовании встроенного сервера обновления в ПК «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 ПК открыть Управление → Обновления в поле **Тип обновления** выбрать параметр *Обновлять согласно ЛПБ*.

Для обновления с помощью команд с сервера обновлений необходимо в настройках ПК 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 ПК после обновления

В случае некорректной работы ПК после очередного обновления следует выполнить возврат к эталонной версии программной составляющей. Этalonной версией является программная составляющая, установленная при поставке ПК. Образ эталонной версии программной составляющей хранится на жестком диске ПК и может быть развернут при необходимости.

### 12.2 Возврат к эталону

Возврат к эталону выполняется следующим образом:

- 5) включить ПК, нажав кнопку  на аппаратной платформе, дождаться появления меню загрузчика (см. **Ошибка! Источник ссылки не найден.**);
- 6) выбрать пункт меню «Recovery system» и нажать клавишу <Enter>;
- 7) ввести имя пользователя admin, пароль 12345678;
- 8) на экране появится сообщение о проверке КС образа ОС, установленного при изготовлении ПК. Дождаться окончания проверки;
- 9) по окончании проверки в случае совпадения КС будет загружена эталонная программная составляющая, ПК перезагрузится.



При возврате к эталонной версии будут утеряны все выполненные ранее настройки (настройки политики безопасности, настройки ПО «ЗАСТАВА-офис», 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 ПК.

### 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 ПК разработчику ПК 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 ПК разработчику ПК на восстановление.

В случае утери ключевого носителя:

- 1) сообщить разработчику ПК (АО «ЭЛВИС-ПЛЮС») о факте утери;
- 2) заказать новый ключевой носитель;
- 3) сменить все пароли, заданные на ПК;
- 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 (см. Таблица 33).

Таблица 33 – Возможные неисправности и способы их устраниния

Описание	Способы устраниния
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 приглашения к вводу PIN-кода – изъять ключевой носитель, выполнить перезагрузку ПК, установить ключевой носитель в слот USB после того, как на экране появится приглашение к вводу логина.

Характерные ошибки при работе с ПК и рекомендации по их устраниению приведены в таблице (см. Таблица 34).

Таблица 34 – Характерные ошибки при работе с ПК и рекомендации по их устраниению

Тип ошибки	Описание ошибки	Рекомендации по устраниению
Неправильное использование утилиты командной строки ПК	<u>Синтаксическая ошибка (Syntax error):</u> 1) при вводе неверных/несуществующих параметров и ключей при использовании утилиты <code>vrpconfig</code> ; 2) при вводе неверных/несуществующих параметров и ключей при использовании утилиты <code>vrpmonitor</code> ; 3) при вводе неверных/несуществующих параметров и ключей при использовании утилиты <code>icv_checker</code> .	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 <code>icv_checker -h</code> . Описание команд утилиты приведено в п. 7.2.1.1.

<b>Тип ошибки</b>	<b>Описание ошибки</b>	<b>Рекомендации по устранению</b>
Ошибка доступа	Возникает при вводе неправильного логина, или пароля, или PIN-кода персонального идентификатора Администратора ПК.	1) Необходимо ввести правильный логин, пароль и PIN-код ключевого носителя (персонального идентификатора) Администратора ПК. 2) При отсутствии возможности указать верные данные, обратиться к разработчику ПК.
Ошибки при настройке политики безопасности и в ПО «ЗАСТАВА-Офис»	<u>Local Policy Parse error:</u> 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.
	<u>IKE Connection timeout:</u> 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 ПК. Если это не помогло, необходимо убедиться в сетевой доступности ЦУП.
	<u>IKE Peer reported error:</u> возникает при указании в политике безопасности сертификата, не совпадающего с сертификатом, указанном в ЦУП.	Необходимо указать в настройках политики безопасности ПК сертификат, указанный в ГПБ ЦУП.
	<u>IKE Error:</u> возникает при отсутствии доверенного сертификата УЦ в ПК, либо указании неверного доверенного сертификата УЦ.	Необходимо импортировать правильный доверенный сертификат УЦ в ПК, а также открыть сеанс с токеном для доверенного сертификата, выполнив авторизацию в этот токен: <code>vpnconfig -login token &lt;id&gt; &lt;password&gt; save.</code>
	<u>Не удалось загрузить политику: отсутствует персональный сертификат:</u> возникает при отсутствии персонального сертификата для VPN в ПК. 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 <code>/var/opt/cprocsp/keys</code> . 2) выполнить авторизацию в токен с персональным сертификатом: <code>vpnconfig -login token &lt;id&gt; &lt;password&gt; save.</code>
	<u>Local certificate not found or not valid:</u> возникает, если у	Необходимо перевыпустить сертификат и контейнер закрытого ключа. Далее необходимо указать новый сертификат в ГПБ ЦУП, и импортировать контейнер

Тип ошибки	Описание ошибки	Рекомендации по устранению
	сертификата, указанного в политике безопасности, истек срок валидности.	закрытого ключа в ПК. В политике безопасности ПК указать использование нового сертификата для подключения к серверу политик.
Переполнение диска ПК	Возникает при отсутствии свободного места на диске, характеризуется падением службы ПО «ЗАСТАВА-Офис» (vpndmn).	<p>Необходимо убедиться в отсутствии свободного места на диске, выполнив команду <code>df -h</code>. Если места на диске нет, то необходимо:</p> <ol style="list-style-type: none"> <li>1) в файле <code>/etc/rsyslog.conf</code> поставить # в начале строки:  <code>#*.info;mail.none;authpriv.none;cron.none /var/log/messages</code></li> <li>2) настроить ротацию журнала, как это описано в п. 7.2.3.1;</li> <li>3) очистить журнал: <code>cat /dev/null &gt; /var/log/messages</code></li> <li>4) после внесения изменений перезапустить сервис журналирования:  <code>/etc/init.d/S01logging restart</code></li> </ol> <p>Если выше перечисленные рекомендации не помогли, и диск всё равно переполняется файлом журнала, необходимо добавить исключение в журналирование по ключевым словам в файле <code>/etc/rsyslog.conf</code>:</p> <pre>:msg, contains, "ip_vs" ~ :msg, contains, "segfault" ~</pre> <p>затем снова перезапустить сервис журналирования.</p>
Недоступность ПК по сети	Возникает при неправильно заданных сетевых настройках в программной составляющей ПК, либо падении службы ПО «ЗАСТАВА-Офис» с заданной «Политикой драйвера по умолчанию» в значение «DROP» (и «DROP ALL»).	<p>При недоступности ПК по сети (например, при использовании подключения по ssh) при условии, что ранее соединение работало, необходимо:</p> <ol style="list-style-type: none"> <li>1) подключиться локально к ПК с административным токеном;</li> <li>2) проверить работу службы vpndmn при помощи команды:  <code>pidof vpndmn</code></li> </ol> <p>если команда не вывела id процесса, значит, служба ПО «ЗАСТАВА-Офис» не запущена. Необходимо перезагрузить ПК, и если ситуация повторится, то необходимо убедиться в том, что отсутствует проблема переполнения диска;</p> <ol style="list-style-type: none"> <li>3) если команда вывела id процесса, значит, ПО «ЗАСТАВА-Офис» функционирует. Следует убедиться в том, что: <ul style="list-style-type: none"> <li>– служба ssh запущена (см. подраздел 7.2.3), если ПК недоступен при подключении по ssh;</li> <li>– логические имена интерфейсов (alias) настроены верно (см. п. 0);</li> <li>– верно задан маршрут по умолчанию (см. Таблица 11).</li> </ul> </li> </ol>

## ПЕРЕЧЕНЬ ПРИНЯТЫХ ТЕРМИНОВ И СОКРАЩЕНИЙ

АДСЧ	– Аппаратный датчик случайных чисел
АПМДЗ	– Аппаратный модуль доверенной загрузки
ВЧС	– Виртуальная частная сеть
ГОСТ	– Государственный стандарт
ГПБ	– Глобальная политика безопасности
КС	– Контрольная сумма
ЛПБ	– Локальная политика безопасности
ПК	– Программный комплекс
ОС	– Операционная система
ПК	– Аппаратно-программный комплекс
ПО	– Программное обеспечение
СКЗИ	– Средство криптографической защиты информации
СОС	– Список отзываемых сертификатов
УЦ	– Удостоверяющий центр
ФСТЭК России	– Федеральная служба по техническому и экспортному контролю России
ЦУП	– Центр управления политиками безопасности
AH	– Authentication Header – протокол из группы IPsec
CA	– Certification Authority – см. УЦ
CRL	– Certificate Revocation List – см. СОС
CSP	– Cryptographic Service Provider – Криптовайдер
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
FTP	– File Transfer Protocol — протокол передачи файлов
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
- 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
- SA
  - Security Association – Защищенное соединение (в контексте протоколов IPsec и IKE)
- SMTP
  - Simple Mail Transfer Protocol — простой протокол передачи почты
- SSH
  - Secure Shell – протокол удаленного управления
- TCP
  - Сетевой протокол транспортного уровня (с гарантированной доставкой) в IP-сетях
- UDP
  - Сетевой протокол транспортного уровня (без гарантированной доставки) в IP-сетях
- USB
  - Universal serial bus – Универсальная последовательная шина
- VPN
  - Virtual Private Network – Виртуальная частная сеть

## **ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ**