УТВЕРЖДЕН
МКЕЮ.00628.ИЗ-ЛУ

«Программный комплекс защиты корпоративных вычислительных ресурсов на сетевом уровне с использованием технологий VPN и распределенного межсетевого экранирования на основе интернет-протоколов семейства IPsec/IKE «VPN/FW «ЗАСТАВА-Офис», версия 6 КС3»

(«VPN/FW-агент «ЗАСТАВА-Офис», версия 6 КС3»)
(исполнение ZO6-L64-FV-03»)

Руководство системного программиста

МКЕЮ.00628-01 32 01

Листов 69

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

2021

СОДЕРЖАНИЕ

1. ВВЕДЕНИЕ

Данный документ предназначен для администратора программного комплекса защиты корпоративных вычислительных ресурсов на сетевом уровне с использованием технологий VPN и распределенного межсетевого экранирования на основе интернет-протоколов семейства IPsec/IKE «VPN/FW «ЗАСТАВА», версия 6 исполнение КС3» в комплектации ZO6-L64-FV-03» (далее – ПК) и содержит описание интерфейса программного обеспечения (ПО), процедуры, выполняемые администратором в процессе подготовки ПК к работе, текущие операции, действия 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 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:

- высшее или среднее техническое образование;
- знание положений настоящего руководства и эксплуатационной документации, входящей в комплект поставки.

Администратор ПК должен знать основы администрирования локальных сетей.

1.3. Типографские соглашения

Курсив	*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. Полная функциональная спецификация

2.1.1. Список функциональных возможностей ПК

ПК реализует следующие функции безопасности:

- Аудит безопасности;
- Идентификация и аутентификация;
- Защита данных пользователей;
- Управление безопасностью;
- Защита функций безопасности объекта (ФБО);
- Использование ресурсов.

2.1.1.1. Аудит безопасности

В процессе функционирования ПК в локальных журналах аудита ПК по умолчанию фиксируется следующий список событий:

- запуск и завершение выполнения функций;
- действия, предпринимаемые ПК в ответ на нарушения безопасности;
- действия, предпринимаемые ПК при соблюдении политики безопасности;
- факт очистки и архивации журнала bin_log;
- внесение изменений в список информации, подлежащей аудиту;
- все решения по запросам на информационные потоки;
- все попытки подключения к субъектам защищаемого сегмента сети из неконтролируемого сегмента сети, включая любые атрибуты безопасности;
- все попытки подключения субъектов, находящихся в защищаемом сегменте сети, к ресурсам, расположенным в неконтролируемом сегменте сети;
- все модификации списка типов контролируемого сетевого трафика;
- изменение настроек программной составляющей ПК;
- изменение настроек получения политики безопасности;
- сообщения синхронизации при использовании кластеризации;
- удачный вход Администратора ПК;
- неудачный вход Администратора ПК;
- запуск и остановка службы ПК;
- результат проверки контрольных сумм ПК.

Администратор ПК имеет возможность выбора одного из четырех уровней журналирования:

– заблокирован;
– события;
– подробный;
– отладочный.


Не рекомендуется устанавливать уровень лога – «заблокирован».

Администратор ПК, прошедший аутентификацию, имеет возможность просматривать события локальных журналов аудита средствами программной составляющей.

Администратору ПК при обращении к журналам аудита разрешены следующие действия: просмотр, удаление и очистка локального журнала аудита. Администратор ПК имеет возможность производить поиск, сортировку, упорядочение событий, фиксируемых в локальном журнале аудита средствами программной составляющей.

2.1.1.2. Идентификация и аутентификация

Доступ к ПО «ЗАСТАВА-Офис», локальным журналам аудита ПК предоставляется Администратору ПК после аутентификации и авторизации по логину и паролю.

2.1.1.3. Защита данных пользователей

ПК осуществляет фильтрацию сетевого трафика в соответствии с его локальной политикой фильтрации.

ПК использует при фильтрации следующие атрибуты: IP-адреса, протоколы и порты отправителя и получателя, идентификатор интерфейса. ПК обеспечивает фильтрацию, в том числе, фрагментированных пакетов.

ПК при фильтрации трафика использует идентификатор сетевого интерфейса ПК на уровне сетевого адреса.

ПК имеет интерфейс управления, позволяющий принимать управляющие команды от МКЕЮ.00631-01 «Программный комплекс «VPN/FW ЗАСТАВА-Управление», версия 6 КС3» («VPN/FW ЗАСТАВА-Управление», версия 6 КС3») (исполнение ZM-WS64-VO-03) (ЦУП), позволяющий задавать отдельные элементы политики безопасности ПК, доставлять их и активировать.

При фильтрации пакетов, приходящих из сети Интернет или неконтролируемой зоны, ПК способен игнорировать атрибуты безопасности: IP-адрес, порт протокола сетевого уровня, путем задания в фильтре условия «для всех (звездочка)».

ПК обеспечивает конфиденциальность данных информационных потоков, используя криптографические методы технологии IKE/IPSec.

ПК обеспечивает конфиденциальность данных сетевого траффика путем использования режима туннелирования протоколов IKE/IPSec. Режим туннелирования обеспечивает сокрытие пользователей (IP-адресов), типов информации в защищаемой информационной системе.

ПК обеспечивает фильтрацию сетевого трафика с использованием состояний (statefull). ПК осуществляет проверку пакетов с учетом состояния и контролирует входящие и исходящие пакеты с течением времени, а также состояние соединения, и сохраняет данные в динамических фильтрах.

ПК обеспечивает для каждого соединения ведение таблицы состояний, основанной на информации состояния соединения. ПК имеет в своем составе следующие автоматы состояний: ICMP, UDP, TCP, FTP.

2.1.1.4. Управление безопасностью

Администратор ПК, прошедший аутентификацию, имеет возможность производить следующие действия:

- производить настройки ПК;
- просматривать, удалять и очищать локальный журнал аудита;
- останавливать, запускать и перезапускать службу ПО «ЗАСТАВА-Офис»;
- вносить изменения в список информации, подлежащей аудиту;
- просматривать и активировать локальную политику безопасности (ЛПБ);
- производить сетевые настройки ОС на котором функционирует ПК;
- производить другие настройки ОС на котором функционирует ПК;
- просматривать, сбрасывать значения таблицы состояний соединений;
- восстанавливать работоспособность ПК.

В ПК реализован механизм удаленного управления.

Администратор ПК имеет возможность задавать и доставлять на ПК правила фильтрации по доверенному каналу связи с ЦУП, основанные на атрибутах безопасности.

2.1.1.5. Защитные меры, реализованные в ПК

В случае сбоя при прогрузке ЛПБ ПК продолжает обработку всех пакетов в соответствии с ранее прогруженной политикой безопасности. При этом в мониторе ЦУП соответствующий объект топологии отображается со статусом «Состояние неизвестно». В это время ПК продолжает обращения за ЛПБ на сервер прогрузки. Новая политика будет прогружена, как только будет устранена причина сбоя доставки политики безопасности.

В случае сбоя во время работы службы (vpndmn) ПК перестает посылать на компонент ЦУП сигналы, свидетельствующие о нормальном функционировании. При этом ЦУП сигнализирует об аварийном состоянии ПК администратору ПК. При этом ПК переходит в

аварийный режим, который предполагает применение политики аварийного режима, определенной в настройках службы vpndmn.

В случае сбоя при запуске службы (vpndmn) ПК переходит в аварийный режим, который предполагает применение политики аварийного режима, определенной в настройках драйвера vpnpcap.

Для безопасного функционирования предполагается задавать в политиках аварийного режима правила для запрета прохождения сетевого трафика через ПК.

Для восстановления работы ПК Администратор ПК имеет возможность вручную перезапустить службу ПО «ЗАСТАВА-Офис», настроить ПК на автоматический запуск службы ПО «ЗАСТАВА-Офис» или вернуть ПК к заводским параметрам.

Для обеспечения надежности меток времени ПК использует системное время программной составляющей ПК. Программная составляющая ПК имеет возможность синхронизировать системные часы со службы времени по протоколу NTP, в том числе по настроенному с помощью ПК доверенному каналу связи.

При каждом включении ПК, выполняется проверка целостности модуля-загрузки и программной составляющей ПК. При несовпадении контрольных сумм с эталонными значениями ПК выключается по питанию. События об удачном и неудачном прохождении проверки контрольных сумм с эталонными значениями записываются в локальный журнал аудита.

При каждом запуске службы vpndmn производится проверка контрольной суммы всех файлов ПО «ЗАСТАВА-Офис». Результаты проверки фиксируются в файле журнала bin_log.txt.

Реализована ручная возможность запустить проверку контроля целостности программной составляющей ПК или ПО «ЗАСТАВА-Офис». Доступ к данной функции ограничен и предоставляется только Администратору ПК.

2.1.1.6. Использование ресурсов

Резервирование функциональных возможностей ПК обеспечивается кластеризацией. При сбое службы ПО «ЗАСТАВА-Офис», внеплановом прерывании работы службы ПО «ЗАСТАВА-Офис», выходе из строя или выключении серверной платформы основного узла ПК, резервный узел становится основным и продолжает выполнять все предписанные и настроенные функции ПК.

ПК осуществляет приоритизацию информационных потоков на основе информации о субъекте межсетевого взаимодействия и типе передаваемых данных путем установки битов поля ToS, основываясь на IP-адресах портах и протоколах отправителя и получателя.

ПК обеспечивает обработку данных, основываясь на приоритизации информационных потоков.

2.1.2. Описание назначения и метод использования интерфейсов взаимодействия с функциями безопасности (описание интерфейсов управления)

Интерфейсы взаимодействия с функциями безопасности обеспечивают загрузку политики безопасности. Политика безопасности бывает двух типов: «Политика драйвера по умолчанию» (Default Driver Policy, DDP) и «Системная политика». «Системная политика» вступает в силу с момента загрузки программной составляющей. «Политика драйвера по умолчанию» применяется в случае сбоя.

Настройка «Политики драйвера по умолчанию» описана в п. 0.

Системная политика может быть загружена из файла с сервера прогрузки политики или соответствовать «Политике драйвера по умолчанию». Настройка «Системной политики» описана в п. 0.

До загрузки программной составляющей применяется политика по умолчанию, которая сконфигурирована способом, описанным в п. 4.2.6.

2.1.3. Описание всех параметров интерфейсов взаимодействия

Для задания «Политики драйвера по умолчанию» необходимо указание следующих параметров:

- Применяемое действие. Допустимые значения: Пропускать все (PASS), Сбрасывать все кроме DHCP (DROP), Сбрасывать все(DROPALL);
- Уровень журналирования. Допустимые значения: Disabled, Events, Details, Debug.

Для задания «Системной политики», загружаемой из файла, необходимо указать путь к файлу с описанием ЛПБ.

Для задания «Системной политики», получаемой с сервера прогрузки политики, необходимо указать следующие параметры:

- Адрес или имя сервера прогрузки и порт;
- идентификатор для установки защищенного соединения (идентификатор персонального сертификата или предварительно распределенного ключа);
- уровень журналирования. Допустимые значения: Disabled, Events, Details, Debug;
- режим работы протокола IKEv1. Допустимые значения: Основной режим и агрессивный режим.

2.1.4. Описание всех действий с каждым интерфейсом взаимодействия

К ЛПБ можно применить следующие действия:

– Просмотр текущей политики;

– Активация политики;

– Изменение параметров политики.

Действия, применимые к ЛПБ, описаны в п. 4.2.2.5.

2.1.5. Описание всех возможных ошибок при вызове каждого интерфейса взаимодействия

При возникновении ошибочных ситуаций в файл регистрации событий заносится сообщение об ошибке. При загрузке ЛПБ возможно возникновение следующих ошибочных ситуаций:

– Ошибка при чтении файла политики. Пример сообщения:

```
2017.07.06 11:51:24               ERROR LP    Local Policy parse error at
line: 373:24 \
      expected '(' begin of section: filter filt_user_manage
2017.07.06 11:51:24               ERROR LP    Fail to activate security
policy \
     Type: System \
     File: /home/admin/TestPolicy.txt
```

– Сервер прогрузки политики недоступен. Пример сообщения об ошибке:

```
2017.07.06 11:59:22    5017755A925276B6        ERROR IKE   Failed to create
IKEv1 SA: \
     Reason:     Exchange timeout \
     Peer Address:     10.111.10.137:500 \
     IKE SPIs:   5017755A925276B6:0000000000000000 \
     Attempts in progress:   None
```

– Ошибка аутентификации на сервере прогрузки:

```
2017.07.06 12:01:14    4EC6E7BD8DAA992E.00000001,I         WARN  IKE   Peer
reported authentication failed
2017.07.06 12:01:14    4EC6E7BD8DAA992E        ERROR IKE   Failed to create
IKEv2 SA: \
     Reason:     Peer reported error \
     Peer Address:     10.111.10.130:500 \
     IKE SPIs:   4EC6E7BD8DAA992E:56B8628A8D8FD050 \
     Attempts in progress:   None
```

– Персональный сертификат отсутствует или истек:

```
2018.04.27 12:08:48               ERROR CM    Local certificate is not
selected. \
     Search params:  \
       LSP rule: 'pmp_auth_ike_sign', cert subject:
C=RU,CN=GateWin131_CPROCA2016 \
     Found certificates: 2/4  \
       1: cert_local[1]:     Not valid after: 26.04.2018 13:57:03:
     C=RU,CN=GateWin131_CPROCA2016 / GOST R 34.10-2001 \
       2: cert_local[1]:     Not valid after: 26.04.2018 16:55:36:
     C=RU,CN=GateWin131_CPROCA2016 / GOST R 34.10-2001
2018.04.27 12:08:48               WARN  LP    Local certificate not found
or not valid, activation of system security policy from Policy Management
Server was paused. \
     Certificate: C=RU,CN=GateWin131_CPROCA2016
```

– Отсутствует доверенный сертификат партнера:

```
2017.07.06 12:14:23    C6F308940C07032E.00000001,I         ERROR CM
     Trusted certificates are not selected to form list of Cert Request: \
     LSP rule: 'pmp_auth_ike_sign_gost2001' - 'cert_trust' is empty \
     Reason: Trusted Certificates DB is empty
2017.07.06 12:14:23    C6F308940C07032E.00000001,I         ERROR CM    Peer
certificate is not selected. \
     Search params:  \
       id_remote:       (DN) C=RU,CN=win_130_gost3 \
       LSP rule:  'pmp_auth_ike_sign_gost2001' - 'cert_remote' is empty,
      CRL processing: disabled \
     Found certificates: 1  \
       1:  Certificates chain is not complete \
         [income] C=RU,CN=win_130_gost3 / GOST R 34.10-2001       (issuer:
C=RU,O=AO ELVIS PLUS,OU=ORPO,CN=CPROCA2016)
2017.07.06 12:14:23    C6F308940C07032E.00000001,I         ERROR IKE   Peer
(DN) C=RU,CN=win_130_gost3 (IP address: 10.111.10.130) is not authorized to
communicate with this host
2017.07.06 12:14:23    C6F308940C07032E        ERROR IKE   Failed to create
IKEv2 SA: \
     Reason:     Authentication failed \
     Peer Address:     10.111.10.130:500 \
     IKE SPIs:   C6F308940C07032E:04679801071C8D05 \
     Attempts in progress:   None
```

– IP-адрес объекта не соответствует указанному в политики безопасности:

```
2017.07.06 12:16:03    B41B1B33AB9B37F5.00000001,I         WARN  IKE   Peer
reported authentication failed
2017.07.06 12:16:03    B41B1B33AB9B37F5        ERROR IKE   Failed to create
IKEv2 SA: \
     Reason:     Peer reported error \
     Peer Address:     10.111.10.130:500 \
     IKE SPIs:   B41B1B33AB9B37F5:36799AD292FA26C8 \
     Attempts in progress:   None
```

2.1.6. Демонстрация прослеживания функциональных требований безопасности к интерфейсам взаимодействия

Описанные выше интерфейсы взаимодействия обеспечивают доставку ЛПБ, реализующую ФБО, описанные в п.п. 2.1.1.2, 2.1.1.3, 2.1.1.5.

2.1.7. Описание доступных пользователям функций, возможных прав и обязанностей, которыми следует управлять в защищенной среде функционирования

Описание доступных пользователям функций, возможных прав и обязанностей описаны в п. 2.1.1.1.

2.1.8. Описание для каждой пользовательской роли принципов безопасной работы с предоставленными в ОО интерфейсами взаимодействия

К интерфейсу прогрузки ЛПБ имеет доступ только Администратор ПК.

Администратору ПК рекомендуется обеспечивать следующие меры безопасности:

– Запрет передачу ЛПБ по открытому каналу;
– Запрет на использование протокола SSH по открытым каналам связи (сеть Интернет) без использования технологии VPN для удаленного подключения к ПК;
– Запрет на установку уровня журналирования равный Disable;

– Выполнять операцию logout по завершении своих действий в системе.

Из соображений безопасности рекомендуется устанавливать «Политика драйвера по умолчанию» в значение «Сбрасывать все» (`dropall`). Следует учесть, что в этом случае сеть не будет доступна, 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).

2.1.9. Описание для каждой пользовательской роли доступных функций и интерфейсов с указанием безопасных значений

Меры для обеспечения безопасной работы с интерфейсом прогрузки политики описаны в п. 2.1.8.

2.1.10. Описание для каждой пользовательской роли типов событий, имеющих значение для безопасности

Типовые действия Администратора ПК включают в себя:

– Вход в систему с корректными аутентификационными данными;
– Выход из системы;
– Попытка входа с некорректными данными;
– Изменение параметров безопасности и управление настройками;
– Запуск программ и порождение процессов, относящихся к ПО «ЗАСТАВА-Офис»;
– Очистка журнала ПО «ЗАСТАВА-Офис»;
– Активация ЛПБ;
– Выполнение процедуры Контроля целостности;
– Возвращение к заводским настройкам.

2.1.11. Описание мер безопасности для среды функционирования

Для того чтобы ПК выполнял все заявленные функции по защите информации от несанкционированного доступа из внешней сети необходимы следующие организационно-распорядительные и технические меры применимые к среде функционирования характерные для всех определенных ролей:

– обеспечение сохранности оборудования и физической целостности СВТ на котором функционирует ПК;
– обеспечение исключение каналов связи защищаемой информационной системы с иными информационными системами в обход ПК;
– разработка нормативных документов, определяющих порядок допуска персонала к ресурсам ПК и назначения их полномочий;

– обеспечение физической защиты административного персонального идентификатора;

– сохранение в секрете идентификаторов (имен) и паролей Администратора ПК.

2.2. Минимальные системные требования

СВТ, на котором установлен компонент ZO6-L64-FV-03 должно удовлетворять следующим требованиям:

– процессор Intel Xeon (4 ядра) с тактовой частотой не менее 2 ГГц;

– ОЗУ - не менее 16 Гбайт;

– внутренний твердотельный накопитель - 32 Гбайт SSD (1 шт.);

3. УСТАНОВКА И ПОДГОТОВКА К ИСПОЛЬЗОВАНИЮ ПО «ЗАСТАВА-ОФИС»

3.1. Входной контроль комплектующих изделий

Входной контроль комплектующих изделий включает в себя последовательность следующих действий:

1) проверку целостности упаковки комплектующих изделий;
2) проверку внешнего вида, отсутствие сколов, царапин, грязи, развальцованных винтов, отсутствие винтов и т.п.;
3) проверку комплектации (согласно комплекту поставки и поставочной спецификации);
4) проверку работоспособности аппаратной платформы.

3.2. Порядок проверки работоспособности аппаратной платформы и установки ПО «ЗАСТАВА-Офис»

Проверка работоспособности аппаратной платформы включает в себя следующие действия:

1) Произвести установку АПМДЗ «ПАК защиты от НСД «Соболь» RU.40308570.501410.001 (версии кода расширения BIOS 1.0.99, 1.0.180).
2) Подключить монитор и клавиатуру к системному блоку (согласно эксплуатационной документации).
3) Подключить аппаратную платформу к линии 220В.
4) Включить электропитание нажатием кнопки питания на корпусе аппаратной платформе в соответствии с эксплуатационной документацией.
5) В соответствии с эксплуатационной документацией на аппаратную платформу загрузиться в BIOS.
6) В BIOS произвести проверку жесткого диска на соответствие поставочной спецификации.
7) В BIOS произвести настройку на загрузку ОС с внешнего USB-накопителя.
8) Установить подготовленный USB-накопитель в аппаратную платформу. Сохранить настройки BIOS и перезагрузить платформу.
9) В процедуре установки выбрать пункт «KoK-OS install (Default settings, VGA 800x600)» для вывода на монитор.
10) После автоматической установки аппаратная платформа автоматически перезагрузится.
11) Извлечь USB накопитель и перенастроить порядок загрузки, если это необходимо.

12) Произвести инициализацию АПМДЗ в соответствии с общим порядком, изложенным в эксплуатационной документацией на АПМДЗ «ПАК защиты от НСД «Соболь» RU.40308570.501410.001 (версии кода расширения BIOS 1.0.99, 1.0.180).
13) Включить электропитание нажатием кнопки питания на передней панели. Пройти аутентификацию на АПМДЗ, загрузиться в ОС используя пункт меню «KoK-OS loading»и пройти аутентификацию на пароле по умолчанию.
14) С помощью утилиты cat /proc/cpuinfo убедиться в соответствии модели процессора поставочной спецификации.
15) Проверить, что все сетевые карты аппаратной платформы обнаружены, воспользовавшись командами lspci –k | grep –C 3 'net' и ip link show. Убедиться в соответствии модели сетевых карт поставочной спецификации.

После проверки работоспособности необходимо задать шаблон контроля целостности АПМДЗ «ПАК защиты от НСД «Соболь».

3.3. Задание шаблона контроля целостности в АПМДЗ

Для задания шаблона контроля целостности в АПМДЗ «ПАК защиты от НСД «Соболь» RU.40308570.501410.001 (версии кода расширения BIOS 1.0.99, 1.0.180), необходимо:

1) Дождаться загрузки Zastava OS и аутентифицироваться, используя значения по-умолчанию.
2) Выполнить очистку дефолтных файлов и монтирование раздела с помощью команд:

   rm –rf /boot/sobol/

   mkdir /boot/sobol/

   mount /dev/sda3 /boot/sobol/

   Раздел для монтирования всегда sda3.
3) Выполнить очистку файлов и секторов

   scheck --reset-sectors

   scheck --reset-files
4) Добавить файлы, которые необходимо поставить на контроль:

   scheck --add-file=/image/syslinux/alt0/full.cz

   scheck --add-file=/image/syslinux/alt0/vmlinuz
5) Проверить, что файлы на контроле целостности с помощью команды:

   scheck --ls-files
6) Проверить пути с помощью команды:

   scheck --ls-path

Вывод команд указанных в п. 5 и п.6 приведен на рисунке (см. Рисунок 1).

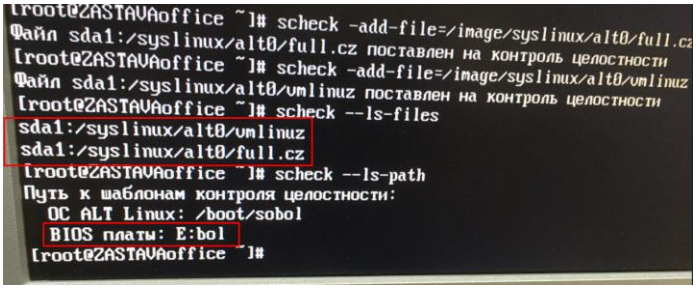

Рисунок 1 – Проверка файлов на контроле целостности и пути файлов контроля целостности

7) Перезагрузить аппаратную платформу. Авторизоваться в АПМДЗ «ПАК защиты от НСД «Соболь» с персональным идентификатором администратора.
8) В меню выбрать пункт «Контроль целостности».
9) Выбрать пункт меню «Каталог с шаблонами КЦ». Указать (подтведить) путь до каталога (по умолчанию диск E: но может быть другой) с шаблонами. Внешний вид меню приведен на рисунке (см. Рисунок 2).

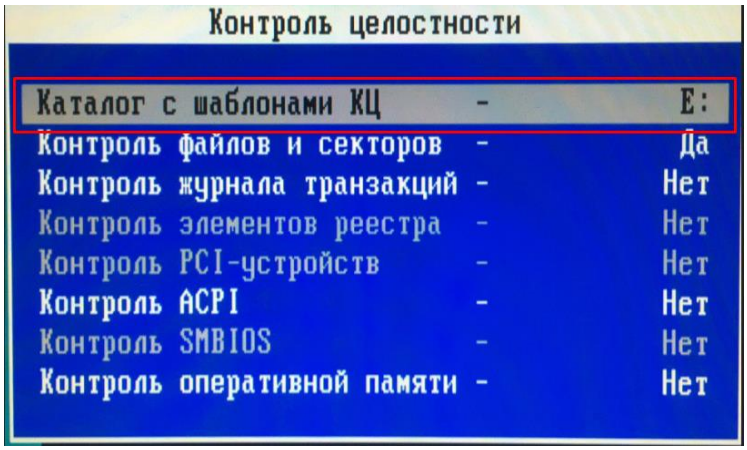

Рисунок 2 – Каталог с шаблонами КЦ

10) После указания Каталога с шаблонами КЦ будет разблокирован пункт меню «Расчёт контрольной суммы». Произвести расчёт контрольных сумм.

4. ИНТЕРФЕЙС КОМАНДНОЙ СТРОКИ ПО «ЗАСТАВА-ОФИС»

4.1. Мониторинг работы ПО «ЗАСТАВА-Офис»

4.1.1. 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 vpnmonitor.

4.1.1.1. Файл регистрации системных событий

Записи о регистрируемых системных событиях хранятся в директории `/var/vpnagent/log/` (например: `bin_log.txt` и `vpndmn_init.log`).

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.

4.1.1.2. 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. 4.2.2.6. 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.

4.1.2. 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.

4.1.2.1. Справочная система по работе с утилитой

Для получения справки по работе утилиты командной строки `vpnmonitor` необходимо ввести команду `vpnmonitor -h`.

4.1.2.2. Просмотр статистики

Для вывода статистики надо выполнить команду:

```
vpnmonitor -s [ipsec|ike|ike1|ike2|ha|fcache|all].
```

Описание параметров команды `vpnmonitor –s` представлено в таблице (см. Таблица 1).

Таблица 1 – Параметры команды vpnmonitor –s

Параметр	Описание
ipsec	Просмотр статистики по протоколу IPsec
ike	Просмотр статистики протоколам IKE (IKE v1 и IKE v2)
ike1	Просмотр статистики отдельно по протоколу IKE v1
ike2	Просмотр статистики отдельно по протоколу IKE v2
ha	Просмотр статистики по протоколу ha
fcache	Просмотр статистики fcache
all	Просмотр полной статистики

Список параметров выводимой статистики представлен в таблице (см. Таблица 2).

Таблица 2 – Печень параметров статистики

Параметр	Описание
IPsec	
Packets (bytes) recieved	Получено пакетов (байт)
Packets (bytes) sent	Послано пакетов (байт)
Decapsulated packets	Декапсулировано (расшифровано) пакетов
Encapsulated packets	Инкапсулировано (зашифровано) пакетов
Packets recieved unsecure	Количество полученных ПО 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
IKEv1	
IKE SAs created (failed) initiated/responded	Количество созданных (не созданных) инициированных/ отвеченных IKE SA в формате x(x)/x(x)
Denied IKE SAs requests	Количество отвергнутых запросов на создание IKE SA
IPsec SA bundless created	Количество созданных IPsec SA
MM exchanges completed (failed) initiated/responded	Количество успешных (неуспешных) обменов Main Mode инициировано/отвечено в формате x(x)/x(x)
AM exchanges completed (failed) initiated/responded	Количество успешных (неуспешных) обменов Aggressive Mode инициировано/отвечено в формате x(x)/x(x)
QM exchanges completed (failed) initiated/responded	Количество успешных (неуспешных) обменов Quick Mode инициировано/отвечено в формате x(x)/x(x)

Параметр	Описание
IX exchanges completed (failed) initiated/responded	Количество успешных (неуспешных) обменов Informational Exchange инициировано/отвечено в формате x(x)/x(x)
TX exchanges completed (failed) initiated/responded	Количество успешных (неуспешных) обменов Transaction Exchange инициировано/отвечено принятых запросов на создание IX в формате x(x)/x(x)
IKEv2	
IKE SAs created (failed) initiated/responded	Количество созданных (не созданных) инициированных/ отвеченных IKE SA в формате x(x)/x(x)
Resumed IKE SA initiated/responded	Количество возобновленных IKE SA инициированных/ отвеченных
IKE SA redirections received/sent	Количество перенаправлений IKE SA получено/послано
COOKIE requested/sent	Количество запрошенных/отправленных токенов COOKIE
Denied IKE SA requests	Количество отвергнутых запросов на создание IKE SA
IKE SA rekeys initiated/responded/collisions	Количество обновлений ключей IKE SA инициированных/отвеченных/коллизий в формате x/x/x
IPsec SA bundless created	Количество созданных IPsec SA
IPsec SA rekeys initiated/responded/collisions	Количество обновлений ключей IPsec SA инициированных/полученных/коллизий в формате x/x/x
Attempts to rekey non-existend IPsec SA by this host/by peer	Количество попыток обновления ключей несуществующей IPsec SA данным хостом/партнером
Temporary rekey failures on this host/on peer	Количество временных отказов в обновлении ключей данным хостом/партнером
INIT exchanges completed (with errors or failed) initiated/responded	Количество обменов INIT_IKE_SA успешных (с ошибками или неуспешных) инициировано/отвечено в формате x(x)/x(x)
RESUME exchanges completed (with errors or failed) initiated/responded	Количество обменов RESUME_IKE_SA успешных (с ошибками или неуспешных) инициировано/отвечено в формате x(x)/x(x)
AUTH exchanges completed (with errors or failed) initiated/responded	Количество успешных (с ошибками или неуспешных) обменов IKE_AUTH инициировано/отправлено в формате x(x)/x(x)
CHILD exchanges completed (with errors or failed) initiated/responded	Количество успешных (с ошибками или неуспешных) обменов CREATE_CHILD_SA инициировано/отправлено в формате x(x)/x(x)
INFO exchanges completed (with errors or failed) initiated/responded	Количество успешных (с ошибками или неуспешных) обменов INFORMATIONAL инициировано/отправлено в формате x(x)/x(x)
HA	
Single start at	Время старта одиночного режима
Single start count	Количество переходов в одиночный режим
Active start count	Количество переходов в активный режим
Passive start count	Количество переходов в пассивный режим
Total recv/sent messages (bytes)	Объем полученных/ отправленных сообщений в байтах
Total errors in recv/sent messages	Количество ошибок при получении/отправке сообщений
Unknown messages(bytes) recv	Количество неизвестных сообщений (байт) при получении сообщений
Create IKE SA: recv/sent messages (bytes)	Объем полученных/ отправленных сообщений в байтах при создании IKE SA

Параметр	Описание
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
FiltDB Cache	
Hash table size (bytes max/alloc)	Размер хэш-таблицы (байт максимум/выделено) в формате x*x*x(x/x)
Validity tag	Текущее значение метки, служащей для определения возможности использования записей в хэш-таблице
Live entries	Количество активных записей
Dead entries	Количество удаленных записей
Allocated entries	Количество записей выделенных из памяти
Dead reused	Количество повторно использованных удалённых записей
Line reused	Количество использованных записей в линиях
Collisions	Количество попыток добавления одинаковых записей
Full lines	Количество заполненных линий
Empty lines	Количество пустых линий
Other lines	Количество остальных линий
Avarage length of non-empty lines	Средняя длина непустых линий

Пример вывода результата команды `vpnmonitor -s`:

```
param                          |value
```

```
-----------------------------|-------------------------------
IPsec                        |
Packets (bytes) recieved     |398 774 (69 396 140)
Packets (bytes) sent         |79 362 (15 988 088)
Decapsulated packets         |0
Encapsulated packets         |0
Packets recieved 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
```

4.1.2.3. 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
```

4.1.2.4. 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
```

4.1.2.5. 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;`

`-cmd (delete | rekey);`

`-delete.`

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 3 и Таблица 4),

`operation` – операция для произведения сравнения по выбранному полю с эталоном (см. Таблица 4),

`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 3).

Таблица 3 – Параметры фильтрации протокола IKE SA

Параметр	Характеристика
type	Тип создания SA
mode	Режим создания SA
role	Роль локальной машины при создании SA
state	Состояние IKE SA
eapid_local	Локальный EAP ID
ikeid_local	Локальный IKE ID
eapid_remote	EAP ID партнера
ikeid_remote	IKE ID партнера
id_remote	ID партнера
rule_name	Имя правила
algcipher	Алгоритм шифрования
alghash	Алгоритм хэширования
dhgroup	DH группа
algintegrity	Алгоритм контроля целостности
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 4).

Таблица 4 – Параметры фильтрации протокола IPsec SA

Тип	Характеристика
idstr	Идентификационный номер

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

Таблица 5 – Описание типов операций фильтрации

Команда	Характеристика

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	
icontain	поле содержит подстроку (эталон), игнорируя регистр букв
not_icontain	поле не содержит подстроку (эталон), игнорируя регистр букв
contain	поле содержит подстроку (эталон), учитывая регистр букв
not_contain	поле не содержит подстроку (эталон), учитывая регистр букв
iequal	поле равняется эталону, игнорируя регистр букв
not_iequa	поле не равняется эталону, игнорируя регистр букв
equal	поле равняется эталону, учитывая регистр букв
not_equal	поле не равняется эталону, учитывая регистр букв
Операции для фильтрации по полю IP-адрес	
inrange	значение поля (IP-адрес) входит в диапазон заданный эталоном, в качестве эталона можно указать просто IP-адрес (10.1.1.1) или диапазон (10.1.1.1...10.1.1.255) или подсеть (10.1.1.0/24 или 10.1.1.0/255.255.255.0)
not_inrange	значение поля (IP-адрес) не входит в диапазон
equal	значение поля (IP-адрес) равно эталону (IP-адрес)
not_equal	значение поля (IP-адрес) не равно эталону (IP-адресу)
Операции для фильтрации по полю IP-порт	
equal	значение поля (порт) равно эталону
not_equal	значение поля не равно эталону
inrange	значение поля входит в диапазон заданный эталоном, в качестве эталона можно указать просто порт (8080) или диапазон (0...65535)
not_inrange	значение поля не входит в диапазон заданный эталоном
Операции для фильтрации по полю уровень лога	
equal	значение поля равно эталону (возможные значения: disabled, events, details, verbose)
not_equal	значение поля не равно эталону
gt	значение поля больше эталона (disabled < events < details < verbose)
lt	значение поля меньше эталона
gteq	значение поля больше или равно эталону
lteq	значение поля меньше или равно эталону
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 -view details dhgroup.not_contain(test1) or local_ip.equal(test2)-ipsec-sa log_level.gt(test3) and transform.not_iequal(test4)
```

4.1.2.6. 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, заисключением установленных с сервером-прогрузчиком.

4.1.2.7. 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 8).

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 на 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 6),

operation – операция для произведения сравнения по выбранному полю с эталоном (см. Таблица 7),

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

Таблица 6 – 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»

Параметр	Характеристика
bytes_out	Фильтрация поля «Исходящих байт»
drop_in	Фильтрация поля «Входящих байт отброшено»
drop_out	Фильтрация поля «Исходящих байт отброшено»
miss_in	Фильтрация поля «Входящих промахов в кэше»
miss_out	Фильтрация поля «Исходящих промахов в кэше»
fh_count	Фильтрация поля «Записей в кэше»
fwprocs	Параметр фильтрации по полю «Фаервольные процедуры»

Таблица 7 – 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	
icontain	поле содержит подстроку (эталон), игнорируя регистр букв
not_icontain	поле не содержит подстроку (эталон), игнорируя регистр букв
contain	поле содержит подстроку (эталон), учитывая регистр букв
not_contain	поле не содержит подстроку (эталон), учитывая регистр букв
iequal	поле равняется эталону, игнорируя регистр букв
not_iequa	поле не равняется эталону, игнорируя регистр букв
equal	поле равняется эталону, учитывая регистр букв
not_equal	поле не равняется эталону, учитывая регистр букв
Операции для фильтрации по полю уровень лога	
equal	значение поля равно эталону (возможные значения: disabled, events, details, verbose)
not_equal	значение поля не равно эталону
gt	значение поля больше эталона (disabled < events < details < verbose)
lt	значение поля меньше эталона
gteq	значение поля больше или равно эталону
lteq	значение поля меньше или равно эталону
Операции для фильтрации по полю IP-адрес	
contain	значение поля (IP-адрес) содержит эталон (IP-адрес)
not_ contain	значение поля (IP-адрес) не содержит эталон (IP-адрес)
Операции для фильтрации по полю IP-порт	
contain	значение поля (порт) содержит эталон
not_ contain	значение поля не содержит эталон
Unsigned int operation	
equal	значение поля равно эталону (возможные значения: disabled, events, details, verbose)
not_equal	значение поля не равно эталону
gt	значение поля больше эталона (disabled < events < details < verbose)
lt	значение поля меньше эталона
gteq	значение поля больше или равно эталону
lteq	значение поля меньше или равно эталону

Пример:

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

Таблица 8 – Отображаемые параметры информации о действующих фильтрах

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

Пример вывода команды `vpnmonitor –f`:

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

Существует возможность поиска фильтра по его ID:
`vpnmonitor -f [-view details|list] -id <значение id>`

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

4.1.2.8. Просмотр статистики ike-cfg

Команда vpnmonitor –ike-cfg позволяет просмотреть информацию об установленных соединениях с использованием протокола IKE-CFG. Результат вывода данной команды представляет собой строку с данными, представленными в таблице (см. Таблица 9).

Таблица 9 – Отображаемые параметры информации о действующих соединениях на основе IKE-CFG

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

Пример вывода команды `vpnmonitor –ike-cfg`:

```
vpnmonitor -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
```

4.1.2.9. 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 о маршруте 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`.

4.2. Конфигурирование ПО «ЗАСТАВА-Офис»

4.2.1. Обзор средств конфигурирования

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

- Утилита vpnconfig;
- Утилита plg_ctl;
- Команды операционной систем (ОС).

4.2.2. 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).


Пользоваться утилитой vpnconfig могут только пользователь root и пользователи, добавленные системными средствами в группу, указанную в файле `/var/vpnagent/localsettings.ini` в параметре ADMIN_GROUP.


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

4.2.2.1. 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 надо ввести команду `vpnconfig –h all`.

4.2.2.2. Просмотр информации о ПО «ЗАСТАВА-Офис»

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

```
vpnconfig -ver
```

Пример вывода команды `vpnmonitor –ver`:

```
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
```

4.2.2.3. Указание логина и пароля администратора

Команды изменения настроек ПО «ЗАСТАВА-Офис», изменения уровня журналирования, изменения настроек получения политики, очистки журнала требуют ввода пароля администратора. Для этого перед командой следует указать опцию –login admin <username> <password>. Пример:

```
vpnconfig -login admin zoadmin russia -activate lsp system pmp
0/0 DN 10.111.10.61 1
```

4.2.2.4. Работа с сертификатами и ключами

4.2.2.4.1. 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 10).

Таблица 10 – Свойства сертификата

Свойство	Описание
Version	Версия формата сертификата
Серийный номер	Серийный номер сертификата
Issuer	Кем выдан сертификат
Subject	Содержит отличительное имя субъекта, то есть владельца закрытого ключа, соответствующего открытому ключу данного сертификата.
Sign Algorithm	Алгоритм цифровой подписи сертификата
Key Algorithm	Тип открытого ключа (алгоритм цифровой подписи и длина)
Public Key	Значение открытого ключа
Действителен с	Начальная дата действия сертификата
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 отозванных сертификатов (СОС), указанные в данном сертификате. Для каждой точки распространения отображается следующая информация: DP[N] "<DP Value>", CRLI[N] "<Issuer Value>", где: – N – номер точки распространения; – <DP Value>- месторасположение точки, где можно получить СОС; – <Issuer Value>- имя организации, выпустившей СОС.
Authority Info Access	Способ доступа к информации УЦ.
Fingerprint (md5)	Хэш-сумма сертификата, вычисляемая по алгоритму md5
Fingerprint (sha1)	Хэш-сумма сертификата, вычисляемая по алгоритму sha1

Пример вывода *цепочки доверия* Сертификата:

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

4.2.2.4.2. Регистрация сертификата

Вы можете регистрировать два типа X.509 сертификатов в ПО «ЗАСТАВА-Офис»*:* сертификаты УЦ и сертификаты конечных пользователей (локальные и партнёров по связи).

Чтобы зарегистрировать новый сертификат УЦ в ПО «ЗАСТАВА-Офис» необходимо произвести следующие действия:

1) Выполнить команду `vpnconfig –list token`, найти в появившемся списке токен `Trusted Certificates token` и запомнить его ID.

2) Выполнить команду `vpnconfig –add cert <file> password <password> pin <pin> ca token <token_id>`, где: `<password>` – пароль доступа к закрытому ключу, `<pin>` – пароль доступа к токену, `<token_id>` - ID для `Trusted Certificates token`.

3) В случае ввода корректного PIN-кода и пароля появится следующее сообщение, сигнализирующее об успешной регистрации сертификата:

```
Certificate is imported.
```

4) Выполнить команду `vpnconfig –login token <token_id> <pin> save` где: `<pin>` – пароль доступа к токену, `<token_id>` - ID для `Trusted Certificates token`.

Чтобы зарегистрировать новый персональный сертификат в ПО «ЗАСТАВА-Офис» необходимо произвести следующие действия:

1) Выполнить команду `vpnconfig –add cert <path> [<password>]`, где: `[<password>]` – пароль доступа к контейнеру.

2) При импортировании Персонального сертификата необходимо ввести PIN-код токена в появившемся окне. После ввода PIN-кода нужно нажать кнопку «Готово».

3) Поставить флаг в поле «Save password for future requests», если требуется сохранить пароль токена для будущих соединений.

4) В случае ввода корректного PIN-кода появится следующее сообщение, сигнализирующее об успешной регистрации сертификата:

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

Чтобы зарегистрировать новый персональный сертификат в ПО «ЗАСТАВА-Офис» путем копирования контейнера необходимо сделать следующее:

1) Скопировать содержимое контейнера, содержащего закрытый ключ и сертификат, поместить его /var/opt/cprocsp/keys.

2) ПО «ЗАСТАВА-Офис» автоматически определит сертификат как «Персональный», по наличию ключа. Но, необходимо помнить, что для того чтобы была возможность использовать персональный сертификат необходимо, чтобы сеанс с токеном был открыт.

Если сертификат УЦ был получен через незащищённый канал (например, по электронной почте) и Вы хотите сохранить его как «Доверяемый», Вы должны проверить подлинность этого сертификата вручную. Непосредственно после регистрации его в «ЗАСТАВА-Офис» свяжитесь с администратором УЦ, чтобы сравнить сигнатуру (fingerprint) оригинального сертификата УЦ с сигнатурой полученного сертификата УЦ, которая отображается в полях «Fingerprint» в таблице сертификатов ПО «ЗАСТАВА-Офис». Если сигнатуры не совпадают, немедленно удалите сертификат из ПО «ЗАСТАВА-Офис».

4.2.2.4.3. Экспорт сертификата

Для того чтобы выполнить процедуру экспорта сертификата необходимо выполнить команду `vpnconfig -export cert <id> <file> [key] [der] [base64] [pkcs7] [pkcs12] [path] [password <password>]`.

4.2.2.4.4. Удаление сертификата

Для удаления сертификата из ПО «ЗАСТАВА-Офис» необходимо узнать id сертификата, который Вы хотите удалить. Для этого нужно воспользоваться командой `vpnconfig –list cert`. После этого необходимо выполнить команду `vpnconfig –remove cert <id>`.

Если для Доверенного токена был задан пароль пользователя, то при удалении сертификата требуется ввод пароля пользователя.

Если срок действия сертификата, находящегося в ПО «ЗАСТАВА-Офис», закончился, данный сертификат будет автоматически удалён из ПО «ЗАСТАВА-Офис» после проверки. Однако это не относится к локальным сертификатам (с закрытыми ключами). Поэтому надо удостовериться в том, что дата, время и настройки часового пояса правильно установлены на Вашем компьютере.

4.2.2.4.5. Предварительно распределенные ключи

Как и сертификаты, предварительно распределенные ключи позволяют проводить аутентификацию при установлении защищенного соединения с удаленным партнером. Эта процедура аутентификации будет успешной, если удалённый партнёр имеет предварительно распределенный ключ с тем же самым значением что и Ваш ключ (эти значения должны быть согласованы с партнёром заранее). Если ключи не совпадают, защищённое подключение не будет установлено.

Существенным недостатком предварительно распределенных ключей по сравнению с сертификатами является недостаточная масштабируемость, поскольку необходимо ручное согласование значений ключей для всех возможных пар партнёров.

4.2.2.4.6. Регистрация предварительно распределенного ключа

Чтобы зарегистрировать предварительно распределенный ключ в ПО «ЗАСТАВА-Офис» необходимо произвести следующие действия:

1) Выполнить команду `vpnconfig –add key <name> [<options>]`,

где: `<name>` – имя предварительно распределенного ключа, `[<options>]` – дополнительные параметры для создания предварительно распределенного ключа. При создании предварительно распределенного ключа возможны следующие опции:

- `token <token id>` – устройство для хранения предварительно распределенного ключа;
- `file <path>` – путь к файлу, содержащему значение ключа;
- `inline <key>` – параметр для ввода ключа в строку.

2) Если опции `file` и `inline` не использовались, то в консоли появится сообщение для ввода значение предварительно распределенного ключа: `Enter key:` и его подтверждения `Repeat key:`.

Имя ключа *не должно* содержать пробелов или любых других специальных знаков, за исключением символа подчёркивания (“_”).

3) Если опция `token` не использовалась, то ключ будет сохранен на установленном по умолчанию токене, пригодном для регистрации предварительно распределенного ключа. Если опция `token` использовалась, то появится запрос вида `Enter user password:`, после чего необходимо ввести пароль для этого токена.

4) Появится запрос вида `Save password for future requests? (Y/N) [N]:`, после чего необходимо ввести <y> для сохранения пароля, или ввести <n> для того, чтобы пароль запрашивался при каждом обращении к токену.

5) Если все введенные данные корректны - появятся следующие сообщения:

1. `Password OK.`
2. `Preshared key imported.`

4.2.2.4.7. Просмотр предварительно распределенных ключей

Для того чтобы просмотреть все предварительно распределенные ключи необходимо выполнить команду `vpnconfig -list cert preshared`. Пример вывода результата исполнения данной команды:

```
Certificate
    Id: 5/0
    Type: preshared
    Name: ExampleKey
    Device Name: SoftToken common
```

4.2.2.4.8. Удаление предварительно распределенного ключа

Для удаления предварительно распределенного ключа из ПО «ЗАСТАВА-Офис» необходимо выполнить команду `vpnconfig -remove cert <id>`. В случае успешного удаления предварительно распределенного ключа будет выведено сообщение: «`Preshared key was deleted`».

4.2.2.4.9. Списки Отозванных Сертификатов

COC – это список сертификатов, которые с данного момента времени не имеют силы и не должны использоваться для формирования Защищенных Соединений (SA) в течение сеанса безопасного соединения. Для того чтобы просмотреть зарегистрированный COC следует выполнить команду `vpnconfig -list cert crl`.

4.2.2.4.10. Импортирование COC вручную

Вы можете в любое время вручную импортировать COC. Процесс импорта – тот же самый, что и при регистрации сертификата. Чтобы зарегистрировать COC в ПО «ЗАСТАВА-Офис» необходимо выполнить команду `vpnconfig –add cert <file>`.

Как только COC будет успешно импортирован, все сертификаты, зарегистрированные в ПО «ЗАСТАВА-Офис», будут сверены с COC. Если сертификат, который зарегистрирован в ПО «ЗАСТАВА-Офис», соответствует полям «Серийный номер» и «Издатель» одного из сертификатов в COC, он будет отмечен как аннулированный. Защищённое соединение с любым партнером по связи, использующим этот сертификат, будет невозможно.

COC не может быть удален из ПО «ЗАСТАВА-Офис». Когда срок действия списка истек, он должен быть обновлен автоматически с LDAP-сервера (это произойдет при установлении очередного защищенного соединения). Если поддержка LDAP-серверов не настроена, надо обновить COC вручную, импортируя файл.

4.2.2.5. Работа с 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.

4.2.2.5.1. Настройка параметров политик ПО «ЗАСТАВА-Офис»

Системная ЛПБ

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

Для настройки системной политики необходимо:

1) При выборе метода прогрузки из файла необходимо выполнить команду `vpnconfig -set lsp system file <path>`, где: `path` – путь к файлу конфигурации;

2) При выборе метода прогрузки с сервера необходимо выполнить команду `vpnconfig -set lsp system pmp [<cert_id> <id_type> <server_ip>|<server_name> <log level> [<timeout>]]`, где:

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

– `<id_type>` – тип идентификатора для прогрузки политики, который должен быть согласован с ЦУП;

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

– `<log level>` – уровень журналирования событий;

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

3) При выборе метода прогрузки «отсутствует», необходимо выполнить команду `vpnconfig -set lsp system none`, тогда в случае ошибки при прогрузке системной политики, будет прогружаться политика драйвера по умолчанию.

Для настройки параметров политики и её активации необходимо воспользоваться командой `vpnconfig -activate lsp system [file <path>]` или `vpnconfig -activate lsp system [pmp <cert_id> <id_type> <server_ip> <log level> [<timeout>]]` или `vpnconfig -activate lsp system [pmp <key_id> <id_type> <id_value> <server_ip> <log level> [<timeout>]]` или `vpnconfig -set lsp system [none]`.

Политика драйвера по умолчанию

В ПО «ЗАСТАВА-Офис» имеется простая политика обработки трафика, которая используются при отсутствии (или недоступности) рабочей ЛПБ. Это «Политика драйвера по умолчанию».

«Политика драйвера по умолчанию» (Default Driver Policy, DDP) вступает в силу при запуске ОС – до момента загрузки рабочей ЛПБ, в случае если произошла ошибка при прогрузке политики или остановлен сервис vpndmn.

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


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

Из соображений безопасности рекомендуется устанавливать «Политика драйвера по умолчанию» в значение «Сбрасывать все» (`dropall`). Следует учесть, что в этом случае сеть не будет доступна, 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).

4.2.2.5.2. Изменение сертификата для соединения с сервером

Для изменения сертификата, с помощью которого будет устанавливаться соединение с сервером политики, нужно выполнить команду `vpnconfig -set lsp system cert <cert_id>`, где: `<cert_id>` – идентификатор сертификата. Для просмотра `<cert_id>` можно воспользоваться командой `vpnconfig -list cert personal`.

Для изменения предварительно распределенного ключа, с помощью которого будет устанавливаться соединение с сервером политики, нужно выполнить команду `vpnconfig -set lsp system key <key_id>`, где: `<key_id>` – идентификатор предварительно распределенного ключа. Для просмотра `<key_id>` можно воспользоваться командой `vpnconfig -list cert preshared`.

4.2.2.5.3. Изменение уровня регистрации событий

Для журналирования сообщений при передаче ЛПБ с сервера политики необходимо установить уровень регистрации событий, для этого нужно выполнить команду `vpnconfig -set lsp system loglevel <log level>`, где: `<log level>` – уровень регистрации событий при передаче ЛПБ с сервера политики. Допустимые значения: `Disabled, Events, Details, Debug`.

4.2.2.5.4. Изменения типа IKE идентификатора

Чтобы изменить значение тика IKE id, необходимо выполнить команду `vpnconfig -set lsp system|user idtype <id_type>`. Допустимые значения: DN, DNS, IP, EMAIL.

4.2.2.5.5. Серверы политик

Чтобы изменить адрес или имя сервера, с которого будет получена политика, необходимо выполнить команду `vpnconfig -set lsp system server <server_ip>|<server_name>`.

4.2.2.5.6. Активация ЛПБ

Для настройки параметров политики и её активации необходимо воспользоваться командой:

`vpnconfig -activate lsp system [file <path>]` – для прогрузки из файла;

`vpnconfig -activate lsp system [pmp <cert_id> <id_type> <server_ip> <log level> [<timeout>]]` – для прогрузки с сервера с использованием сертификата;

`vpnconfig -activate lsp system [pmp <key_id> <id_type> <id_value> <server_ip> <log level> [<timeout>]]` – для прогрузки с сервера с использованием предварительно распределенного ключа.

4.2.2.5.7. Просмотр текущей ЛПБ

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

4.2.2.6. Файл регистрации событий

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

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

Для задания уровня журналирования необходимо выполнить команду `vpnconfig -set log LOG_LEVEL <value>`, где: `<value> - Disabled, Events, Details, Debug` –для уровня приложения. И `vpnconfig -set log LOG_LEVEL_KERNEL <value>`, где: `<value> - Disabled, Events, Details, Debug`

Предусмотрено архивированное хранение файлов журнала.

Чтобы установить максимальный размер файла необходимо выполнить команду `vpnconfig -set log MAX_LOG_SIZE`. 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 BACKUP_DEPTH <value>`.

Для установки языка журналирования необходимо выполнить команду `vpnconfig -set log LANGUAGE <value>`. Возможные значения: 0 – Английский, 1 – Русский.

Некоторые параметры уровней регистрации хранятся также в ЛПБ, созданной для ПО «ЗАСТАВА-Офис»

4.2.2.7. 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 SYSLOG_ON <value>`, где: `<value>1/0/on/off/true/false/Enabled/ Disabled`.

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

Для настойки уровня протоколирования Syslog необходимо выполнить команду `vpnconfig -set log FACILITY <value>`,`<value>` – одно из значений от 0 до 7.

Для удаления символов конца строки из сообщений - `vpnconfig -set log SYSLOG_SINGLELINE ON`

4.2.2.8. Протокол IKE

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

1) Для просмотра настроек протокола надо выполнить команду `vpnconfig –list <ike>`.

2) Для изменения настроек протокола надо выполнить команду `vpnconfig –set <ike> <id-parameter> <value>`.

3) Для установки параметра в значение по умолчанию необходимо выполнить команду `vpnconfig –reset <ike> <id-parameter>`.

4.2.2.8.1. 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 11).

Таблица 11 – Параметры протокола IKE

Номер параметра	Параметр	Расшифровка
0	IKEv1	Управление режимом работы IKEv1. Возможные значения: – Disabled – Enabled (используется по умолчанию) – Responder only
1	IKEv2	Управление режимом работы IKEv2 Возможные значения: – Disabled – Enabled (используется по умолчанию) – Responder only
2	IKE port	Номер порта для IKE-соединения (1 - 65535, по умолчанию 500)
3	NAT-T port	Порт для работы алгоритма NAT-Traversal. Трафик IKE будет переключен на этот порт, когда при установлении соединения между партнерами обнаруживается присутствие NAT-устройств. Значение по умолчанию: (1 - 65535, по умолчанию 4500)
4	Time to complete exchange (sec)	Максимальное время для создания защищенного соединения (SA). (5-600, по умолчанию 60)
5	Shortened time to complete exchange	Укороченное время для завершения обмена (3-60, по умолчанию 5)
6	Max half-open states	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 посылался с несуществующего IP-адреса, то COOKIE инициатором получено не будет и, соответственно, не будет возвращено. Если же адрес был реальным, то инициатор повторно посылает запрос, включая в него COOKIE. Такие запросы считаются ответчиком подтвержденными и минуют проверку на превышение описываемого параметра
7	Initiate no more exchanges	Максимальное количество параллельных обменов (1 – 16, по умолчанию – 4), которые могут быть инициированы в рамках одной IKE SA. Если система посылает больше запросов, то они будут ожидать завершения какого-либо из активных обменов. Данный параметр актуален только для IKEv1.
8	Respond to no more	Максимальное количество параллельных обменов, которые

Номер параметра	Параметр	Расшифровка
	exchanges	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.
9	Servers selecting policy	Политика выбора серверов (по умолчанию – Try servers sequencially)
10	NAT traversal policy	Политика выбора метода работы через NAT (по умолчанию – Автовыбор)
11	Sending unprotected error notifications	Частота отправки незащищенных сообщений об ошибках (по умолчанию – Limit rate to 10 per second)
12	IKE v1 fragmentation	Включение/отключение режима фрагментации (IKEv1) (по умолчанию включен)
13	IKE v2 fragmentation	Управление режимом фрагментации (IKEv2) (по умолчанию – Auto)
14	IKEv2 SA lifetime jitter	Рандомизация времени жизни IKE SA (IKEv2) (по умолчанию включена)
15	IKEv2 IPsec SA lifetime jitter	Рандомизация времени жизни IKE IPsec SA (IKEv2) (по умолчанию включена)
16	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. Для выключения необходимо указать значение «не использовать». Отключение параметра не рекомендуется, но возможно в тестовых и отладочных целях или в случае проблем со сторонним ПО.
17	NAT Keep alive interval (sec)	Интервал в секундах для отправки UDP пакета для поддержания трансляции на NAT устройстве (1 - 60, по умолчанию 20)
18	IPsec SA provision traffic (KB)	Запас трафика IPsec, по достижении которого запускается процесс обновления ключей (0 - 16384, по умолчанию 2048)
19	IPsec SA removal delay (sec)	Задержка до удаления IPsec (по умолчанию – 5)
20	IPsec SA anti-replay window	IPSec размер окна для подавления атак воспроизведения (по умолчанию 64). Возможные значения: 32, 64, 128,264, 512, отключено.
21	Save SAs on LSP reload	Сохранение SA при перезагрузке ЛПБ (по умолчанию выключено)
22	Initiate Persistent IPsec SAs on LSP reload	При включенном режиме на каждое IPSec правило в политике создается ike и ipsec sa при перегрузке политики (по умолчанию – false)
23	IKE-CFG most long unused address	Параметр, контролирующий использование IKE-CFG
24	IKE-CFG auto route	При старте системы в LINUX необходимо вызывать команду: `ip rule add from all lookup <table id>` Где: `<table id>` – номер таблицы, который задан в локальных

Номер параметра	Параметр	Расшифровка

		настройках ПО (RRI table id), в противном случае те маршруты, которые прописываются в таблицу с номером <table id>, система не видит.
		Пример команды:
		`ip rule add from all lookup 111`
		Для удаления правила нужно вызвать команду:
		`ip rule del table <table id>`

25	CRL processing	Параметр, регулирующий режимы обработки CRL. Возможные значения: — Disabled (Выключена) (используется по умолчанию); — Enabled, revoke also if CRL not available (Включена, отзывать, если CRL недоступен); — Enabled, don't revoke if CRL not available (Включена, не отзывать, если CRL недоступен).

Некоторые дополнительные параметры протокола IKE хранятся в ЛПБ, создаваемой для ПО «ЗАСТАВА Офис».

4.2.2.8.2. Описание режимов обработки CRL

В локальных настройках в группе параметров IKE находится параметр CRL_PROCESSING, который служит для управления режимами обработки CRL.

Для просмотра значения этого параметра с помощью утилиты командной строки нужно выполнить команду: `vpnconfig -l ike`.

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 CRL будет производиться в режимах, приведенных в таблице (см. Таблица 12).

Таблица 12 – Режимы работы обработки CRL

Числовое значение	Режим работы обработки CRL
0	Disabled. Обработка CRL выключена. Поиск и проверка CRL не производятся.
1	Enabled, revoke also if CRL not available. Обработка CRL включена, при этом, если CRL не доступен, сертификат будет считаться отозванным. Обработка осуществляется следующим образом: Если в сертификате нет поля CDP (CRL Distribution Points), то поиск и проверка CRL для него не производится. Если поле CDP есть, делается попытка загрузить CRL, если по данному CDP CRL не был загружен ранее, или наступило время обновления ранее загруженного CRL. Если CRL не удалось загрузить или в процессе загрузки произошла ошибка, в локальной базе (токены, способные хранить CRL) ищется CRL, соответствующий эмитенту (issuer) сертификата. Если CRL получить не удалось, или у полученного CRL наступило время обновления (CRL истек) считается, что сертификат отозван. Если получен действительный CRL, в нем ищется серийный номер сертификата,

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

4.2.2.8.3. Политика выбора метода работы через NAT

Управление политикой выбора метода работы через NAT осуществляется из локальных настроек ПО «ЗАСТАВА-Офис». В зависимости от выбранного числового значения параметра с id = 15 политика может быть следующей (см. Таблица 13):. Под Агентом понимается ПО «ЗАСТАВА-Офис».

Таблица 13 – Варианты политики выбора метода работы через NAT

Числовое значение	Политика
0 (Запретить)	*Агент* не предлагает (будучи инициатором) и не воспринимает (будучи респондентом) ни один из методов UDP-инкапсуляции. То есть, инкапсуляции не будет даже при наличии NAT между *Агентами*.
1 (Стандарт)	Этот режим устанавливается по умолчанию после установки *Агента*. Будучи инициатором, предлагаются все варианты UDP-инкапсуляции, кроме метода Huttunen, будучи респондентом приоритетным считается метод Стандарт.
2 (Все методы)	Использовать все методы. Будучи инициатором, предлагаются все варианты UDP-инкапсуляции, будучи респондентом приоритетным считается метод Стандарт.
3 (Huttunen)	Этот метод делает вариант Huttunen более приоритетным. Будучи инициатором, *Агент* предлагает только его. Будучи респондером метод Huttunen считается более приоритетным (но не единственно возможным).
4 (Автовыбор)	Режим характеризуется тем, что, будучи инициатором, в Main Mode *Агент* пытается сам выбрать подходящий метод UDP-инкапсуляции.
129 (Стандарт (Принудительно))	Стандартный режим с принудительной инкапсуляцией. Полностью аналогичен режиму Стандарт, за тем исключением, что инкапсуляция используется всегда, независимо от наличия или отсутствия NAT-а между

Числовое значение	Политика
	партнерами.
130 (Все методы (Принудительно))	Режим Все методы с принудительной инкапсуляцией. Полностью аналогичен режиму Все методы, за тем исключением, что инкапсуляция используется всегда, независимо от наличия или отсутствия NAT-а между партнерами.
131 (Huttunen (Принудительно))	Режим Huttunen с принудительной инкапсуляцией. Полностью аналогичен режиму Huttunen, за тем исключением, что инкапсуляция используется всегда, независимо от наличия или отсутствия NAT-а между партнерами
132 (Автовыбор (Принудительно))	Автоопределение с принудительной инкапсуляцией. Режим полностью аналогичен режиму Автовыбор, за тем исключением, что инкапсуляция используется всегда, независимо от наличия или отсутствия NAT-а между партнерами.

4.2.2.9. Токены

ПО «ЗАСТАВА-Офис» 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.

4.2.2.9.1. 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:

```
3.  Provider
4.    Name: Builtin Trusted Module
5.    Path: softpkcs11-trusted.dll
6.    Cryptoki Version: 2.20
7.    Library Version: 2.32
8.    Manufacturer: ELVIS-PLUS
9.    Description: Trusted Certificates
10.   Tokens: 1
11.     Token: Trusted Certificates token
```

4.2.2.9.2. Добавление Модулей токенов

Для регистрации модуля PKCS#11 в ПО «ЗАСТАВА-Офис» необходимо выполнить команду `vpnconfig -add provider <module_name> <module_file>`,
где: `<module_name>` - имя для регистрируемого модуля, `<module_file>` - указание на путь к файлу с библиотекой модуля токена PKCS#11.

4.2.2.9.3. Удаление Модуля токена

Чтобы удалить модуль PKCS#11 из ПО «ЗАСТАВА-Офис» необходимо определить его Имя (Name), для этого надо воспользоваться командой `vpnconfig –list provider`. Затем необходимо выполнить команду `vpnconfig -remove provider <name>`.

4.2.2.9.4. 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>`.

4.2.2.9.5. 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, если интерфейс PKCS#11 токена позволяет это действие.
	PIN-код может быть изменен только на активном токене (соединение с токеном должно быть открыто).
	Функция смены PIN-кода токена будет недоступна, если нет токенов, зарегистрированных в ПО «ЗАСТАВА-Офис».

4.2.2.10. Локальные интерфейсы

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.

4.2.3. Утилита plg_ctl

Утилита plg_ctl – модуль управления криптобиблиотеками (криптоплагинами) – встроенный программный модуль, предназначенный для подключения криптобиблиотек, используемых в ПО «ЗАСТАВА-Офис». Криптобиблиотека включает в себя различные криптографические функции (генератор случайных чисел, функции хеширования, вычисления цифровой подписи и шифрования), которые используются при аутентификации пользователей и создании защищенных соединений. Криптобиблиотека может быть разработана независимым

производителем и подключаться к ПО «ЗАСТАВА-Офис» как отдельный модуль (плагин). По умолчанию в состав ПО «ЗАСТАВА-Офис» входит набор штатных криптобиблиотек.

При помощи модуля криптоплагинов можно регистрировать и активировать криптобиблиотеки, а также управлять отдельными криптоалгоритмами, входящими в состав библиотек. Криптоалгоритмы используются для следующих целей:

- выполнение криптографических процедур на уровне ядра программной составляющей для защиты сетевого трафика;
- выполнение криптографических процедур на прикладном уровне.

Все действия по конфигурированию выполняются через утилиту управления `plg_ctl`, которая используется для управления как криптобиблиотеками, так и содержащимися в них криптоалгоритмами.

4.2.3.1. Синтаксис

Криптобиблиотеки однозначно идентифицируются по именам, основанным на алгоритме или алгоритмах, которые они содержат. Если имя криптобиблиотеки содержит пробелы или символы, которые имеют специальное значение в интерфейсе командной строки, то имя криптобиблиотеки должно стоять в кавычках.

Следующий общий синтаксис используется при запуске утилиты `plg_ctl`:

```
plg_ctl [действие <аргумент>] [опция],
```

где: [`действие`] – это операция, которую утилита должна выполнить.

4.2.3.1.1. Действия

Утилита `plg_ctl` поддерживает следующие действия, представленные в таблице (см. Таблица 14).

Таблица 14 – Действия, поддерживаемые утилитой `plg_ctl`

Ключ	Название	Описание
`-e`	Enable	Активировать криптобиблиотеку или криптоалгоритм
`-d`	Disable	Деактивировать криптобиблиотеку или криптоалгоритм
`-l`	List	Показать список криптобиблиотек (данное действие производится при вызове plg_ctl без параметров)
`-r`	Remove	Удалить информацию о криптобиблиотеке из текущей конфигурации
`-i`	Install	Добавить информацию о криптобиблиотеке в текущую конфигурацию
`-p`	Print	Напечатать детальное описание криптобиблиотеки или криптоалгоритма

4.2.3.1.2. Опции

Утилита plg_ctl поддерживает следующие опции, представленные в таблице (см. Таблица 15).

Таблица 15 – Опции, поддерживаемые утилитой plg_ctl

Ключ	Название	Описание
-k	Kernel (уровень ядра)	Выполнить операции только с криптобиблиотеками уровня ядра программной составляющей. Данный флаг совместим с действиями: -e, -d, -r и -p.
-u	User (прикладной уровень)	Выполнить операции только с криптобиблиотеками уровня пользователя. Данный флаг совместим с действиями: -e, -d, -r и -p.
-a	Algorithm	Имя криптоалгоритма, для которого выполняется действие. Данный флаг совместим с действиями: -e, -d и -p.
-b	Binary file	Имя двоичного файла криптобиблиотеки (динамическая библиотека или драйвер) Данный флаг совместим с действиями: -i.
-x	Backup	Путь к файлу, в который нужно сохранить настройки криптоалгоритмов из удаляемой криптобиблиотеки. При добавлении криптобиблиотеки путь к файлу, из которого нужно зачитать сохраненные настройки. Данный флаг совместим с действиями: -i и -r.

Некоторые опции могут быть объединены в одной команде для указания имени криптоалгоритма и/или уровня ядра или приложения.

Например, -a <имя_криптоалгоритма> -u

4.2.3.2. Добавление криптобиблиотеки

Для добавления криптобиблиотеки необходимо указать следующее:

plg_ctl -i <путь к файлу конфигурации криптобиблиотеки> [-b <путь к файлу криптобиблиотеки>] [-loglevel ERROR|NOTE|WARNING|DEBUG|DISABLE]

Если при добавлении криптобиблиотеки не была указана опция -b, то путь к файлу криптобиблиотеки будет браться из файла конфигурации.

Пример: plg_ctl -i c:\temp\test_plg.cfg -b c:\work\bin\test_plg.dll

4.2.3.3. Удаление криптобиблиотеки

Для удаления криптобиблиотеки необходимо указать следующее:

plg_ctl -r <имя криптобиблиотеки> [-u|-k] [-x <путь к файлу для сохранения настроек>] [-loglevel ERROR|NOTE|WARNING|DEBUG|DISABLE].

Если указана опция –u или –k, то удаление произойдет, если найдена криптобиблиотека соответственно уровня пользователя или уровня ядра.

4.2.3.4. Вывод информации о криптобиблиотеке или криптоалгоритмах

Для вывода информации о криптобиблиотеки или криптоалгоритмах необходимо указать следующее:

`plg_ctl –p` <имя криптобиблиотеки> [-a <имя криптоалгоритма>] [-u | -k].

Если не указана опция –a, то будет выведена информация о криптобиблиотеке для указанного имени. С опцией –a будет выведена информация об указанном алгоритме.

При указании имен можно использовать специальный символ - *, означающий любое количество любых символов.

Пример: Вывод информации о всех зарегистрированных криптоалгоритмах уровня приложения: `plg_ctl –p * -a * -u`

4.2.3.5. Примеры команд в интерфейсе командной строки

Примеры команд в интерфейсе командной строки приведены в таблице (см. Таблица 16).

Таблица 16 – Примеры команд в интерфейсе командной строки

Команда	**Выполняемое действие**
`plg_ctl –p * –u`	Показать информацию о всех криптобиблиотеках прикладного уровня
`plg_ctl –p crypto_plg1_user –a *`	Показать список криптоалгоритмов в существующем прикладном уровне криптобиблиотеки, названной `crypto_plg1_user`
`plg_ctl –d crypto_plg1_kernel`	Деактивировать криптобиблиотеку с именем `crypto_plg1_kernel`
`plg_ctl –e crypto_plg1_user –a *`	Активировать все алгоритмы из криптобиблиотеки с именем `crypto_plg1_kernel`
`plg_ctl –r crypto_plg1_kernel`	Удалить существующую криптобиблиотеку `crypto_plg1_kernel`
`plg_ctl –i <path_cfg> –b <path_lib>`	Добавить криптобиблиотеку. Примеры значений для `<path_cfg>` и `<path_lib>` приведены выше.
`plg_ctl –h`	Показать справочную информацию по утилите.

4.2.4. Утилиты icv_writer и icv_checker

Утилита `icv_writer` предназначена для вычисления контрольной суммы.

Для получения справки по работе утилиты необходимо выполнить команду: `icv_writer –h`

Следующий синтаксис используется для запуска утилит icv_writer:

```
icv_writer.exe -L<FileList file name> [> outfile]
```

или

```
icv_writer.exe -
F[DestPath/]FileName.ext[=SourcePath/FileName.ext] [> outfile]
```

Утилита возвращает следующие коды:

0 – OK;

1 – неправильный параметр запуска;

-1 - иные ошибки.

Пример использования команды для вычисления контрольной суммы от файла filelist.hash:

```
icv_writer.exe -Ffilelist.hash > filelist_hash.hash
```

Проверить контрольные суммы можно, запустив утилиту `icv_checker`.

Для получения справки по работе утилиты необходимо выполнить команду: `icv_checker.exe –h`

Используется следующий синтаксис:

```
icv_checker.exe <filelist.hash>
```

Формат файла с контрольными суммами 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 контрольная сумма в файле;

-2 – иные ошибки.

Для проверки целостности ПО необходимо выполнить команду `icv_checker filelist.hash`, где: filelist.hash - файл с текущим значением контрольных сумм.

Для проверки целостности файла filelist.hash необходимо выполнить команду `icv_checker filelist_hash.hash`, где: filelist_hash.hash - файл с текущим значением контрольной суммы для файла filelist.hash.

Пример выполнения утилиты `icv_checker`:

```
icv_checker.exe filelist_hash.hash
Files processed      1
   Changed     Files 0
   NotFound    Files 0
   NotAccessed Files 0
```

4.2.5. Конфигурирование модуля токенов

Существует возможность конфигурировать поведение Softtoken common с помощью конфигурационного файла pkcs11.cfg. Файл pkcs11.cfg расположен в директории /etc/vpnagent .

Данный файл не устанавливается совместно с инсталлятором, при необходимости его нужно создать.

При загрузке токена подхватываются настройки из конфигурационного файла:

– перезапуск службы vpndmn;

– выгрузить/загрузить токен из графического интерфейса *Агента.*

На данный момент поддерживается всего одна настройка для Builtin CryptoPro Module. Эта настройка позволяет либо кешировать сессии СКЗИ ЖТЯИ.00088-01 «КриптоПро CSP» Версия 4.0 (исполнение 2-Base) либо открывать сессии по запросу.

Пример конфигурационного файла:

[CryptoPro]

delayed=0|1, где: 0 - немедленное создание сессий, кеширование включено, либо 1 - сессии открываются по запросу, кеширование выключено.

4.2.6. Конфигурирование модуля vpnpcap

Существует возможность конфигурировать поведение модуля vpnpcap с помощью задания параметров:

– filth_max_count - размер хэш-таблицы фильтров (по умолчанию 8192). Хэш-Таблица обеспечивает быстрый поиск фильтра при точном соответствии записи в ней параметрам пакета;

– 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.

– pcap_defcfg - политика драйвера действующая во время загрузки программной составляющей с момента загрузки драйвера vpnpcap в оперативную память и до момента запуска службы vpndmn

  – 2 - PASS(default);

  – 1 – DROP.

– 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.

Для задания этих параметров необходимо выполнить следующе команды:

– /etc/init.d/S99vpngate stop
– /sbin/rmmod vpnpcap
– /sbin/modprobe vpnpcap pcap_defcfg=1 filth_max_count=5000 hreads_mask=c0000000,00000000 diffserv=1
– /etc/init.d/S99vpngate start.

4.2.7. Конфигурирование модуля cp_plg_cpro

Для конфигурирования модуля `cp_plg_cpro-40` используется параметр max_handles. Параметр Max_handles - максимальное количество хэндлов СКЗИ ЖТЯИ.00088-01 «КриптоПро CSP» Версия 4.0 (исполнение 2-Base), параметр влияет на максимальное количество IPsec SA, которое может быть установлено. По умолчанию данный параметр равен 262140.

Для изменения этого параметра необходимо выполнить следующие команды:

– /etc/init.d/S99vpngate stop
– /sbin/rmmod cp_plg_cpro40;
– /sbin/modprobe cp_plg_cpro-40 max_handles=120000;
– /etc/init.d/S99vpngate start

4.2.8. Конфигурирование ПО «ЗАСТАВА-Офис» в кластерном исполнении

ПО «ЗАСТАВА-Офис» в кластерном варианте, будучи основным узлом, 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:

– синхронизировать время на всех узлах;
– выполнить настройки ПО «keepalived» и описать виртуальные интерфейсы кластера в файле keepalived.conf;
– настроить прогрузку политики (из файла или по PMPv2);
– включить и настроить режим кластера в ПО «ЗАСТАВА-Офис» (см п. 4.2.8.2);

– Установить одинаковое значение QCD secret в настройках каждого узла.

4.2.8.1. Настройка ПО keepalived

Для настройки keepalived необходимо выполнить следующие действия:

– описать виртуальные интерфейсы кластера в файле `/etc/keepalived/keepalived.conf`.

Пример описания с пояснения:

```
vrrp_sync_group G1 {
  group {
    VI_0
    VI_1
  }
  notify_backup "/usr/local/bin/vrrp.back arg1 arg2"
  notify_master "/usr/local/bin/vrrp.mast arg1 arg2"
  notify_fault "/usr/local/bin/vrrp.fault arg1 arg2"
}
vrrp_script chk_vpndmn {
  script "killall -0 vpndmn"
  interval 2
  fall 2
  rise 2
}

vrrp_instance VI_0 {
  interface eth0 #Публичный интерфейс
  state MASTER #Состояние, в котором запускается узел кластера.
Master для основного, backup для резервного
  virtual_router_id 121 #Именное обозначение узла
  priority 100 # приоритет узла перед другими, у BACKUP он всегда
должен быть ниже чем у MASTER
  authentication #Данные для аутентификации. Пароль может быть
любым, но одинаковым для всех узлов
{
    auth_type PASS
    auth_pass 1111
  }
  virtual_ipaddress #Виртуальный адрес кластера
{
    10.111.10.135/24
  }
track_script {
     chk_vpndmn
   }
}
```

– В пПКу `/usr/local/bin/` добавить файлы, на которые ссылается `keepalived.conf`. Это скрипты, которые будут выполняться в момент переключения кластера.

Пример скриптов:

```
vrrp.back
#! /bin/bash
logger –t vrrp.mast deactivating mode
```

```
/opt/ZASTAVAoffice/bin/vpnmonitor -passive

vrrp.mast
#! /bin/bash
logger –t vrrp.mast activating mode
/opt/ZASTAVAoffice/bin/vpnmonitor -active

vrrp.fault
#! /bin/bash
logger –t vrrp.mast deactivating mode
/opt/ZASTAVAoffice/bin/vpnmonitor -passive
```

– Установить разрешение на выполнение скриптов:

```
Chmod +x /usr/local/bin/vrrp*
```

– Перезапустить keepalived

4.2.8.2. Настройка ПО «ЗАСТАВА-Офис»

Для настройки режима кластера *для каждого узла кластера* необходимо включить режим кластера и настроить синхронизацию узлов кластера. Для этого надо:

1) Для включения режима кластера необходимо *для каждого узла кластера* выполнить следующие настройки:

– Включить режим «Multicast» командой `vpnconfig –set ha HA_MODE Multicast`;

– Установить одинаковое для всех узлов значение «Ключ кластера» с помощью команды `vpnconfig –set ha KEY <key value>;`

– Задать одинаковое для всех узлов значение QCD secret в 16-ричном формате с помощью команды `vpnconfig –set ike QCD_secret <value>`;

2) Для настройки синхронизации, необходимо для каждого узла кластера указать адрес интерфейса, который будет использоваться для синхронизации кластерных узлов. `Vpnconfig –set ha MULTICAST_ADDRS <ip adr>;`

3) Указать групповой адрес режима Multicast из диапазона 224.0.0.0 до 239.255.255.255 с помощью команды `vpnconfig –set ha MULTICAST_GROUP <ip adr>`;

4) Указать порт режима Multicast (любое десятичное целое число) с помощью команды `vpnconfig –set ha MULTICAST_PORT <value>`;

5) Задать уровень регистрации событий для фильтра Multicast с помощью команды `vpnconfig – set ha MULTICAST_FILTER_LOGLEVEL <value>`.

4.2.9. Конфигурирование удаленной регистрации событий (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.

4.2.9.1. Настройка ПО «ЗАСТАВА-Офис»

Настройки ПО «ЗАСТАВА-Офис» для включения удаленной регистрации событий описаны в п. 4.2.2.7.

4.2.9.2. Настройка Syslog

Для настройки удалённой регистрации событий необходимо отредактировать файл `/etc/syslog.conf`, добавив строку вида:

`<facility>.<level> @<syslog-server-addr>`,

где: `<facility>` – одно из значений local0...local7, заданное в настройках ПО «ЗАСТАВА-Офис»;

`<syslog-server-addr>` – адрес удалённого syslog-сервера;

`<level>` – уровень протоколирования (info, error, и т.д.). Для подробной информации по уровню протоколирования обратитесь к документации по Syslog.

Пример записи в syslog.conf для отсылки на удалённый syslog-сервер сообщений об ошибках: `local0.err @192.168.0.3`

4.2.10. Конфигурирование snmp

При необходимости получать от *Агентов* статистику и сигналы нарушения по протоколу SNMP (net-snmp) нужно зарегистрировать библиотеку расширения сервиса snmpd (MIB-модуль). Для этого надо:

В файл snmpd.conf добавить строку:

```
dlmod snmpagent /opt/ZASTAVAoffice/lib/libsnmpagent.so
```

Дать команду snmpd для подгрузки модуля расширения:

```
/etc/init.d/snmpd restart
```

Для настройки мониторинга в файле snmpd.conf изменить параметр:

`"rocommunity public default -V systemonly"` на `"rocommunity public default -V all "`

Сигналы нарушения (snmp-traps) будут отправляться только по указанным в ЛПБ событиям.

5. ПОДГОТОВКА К РАБОТЕ

Подготовка ПК к работе включает следующие операции:

– Проверку контрольной суммы образа ОС;
– Настройку сетевых параметров (при необходимости);
– Установку персонального и доверенного сертификатов;
– Настройку получения политики безопасности;

5.1. Шаги, для настройки поставленного ПК

5.1.1. Задание контроля целостности в АПМДЗ

1) Дождаться загрузки Zastava OS и аутентифицироваться, используя значения по-умолчанию (логин - admin, пароль - neeVohPho7Ei);
2) Выполнить очистку дефолтных файлов и монтирование раздела с помощью команд:
   rm –rf /boot/sobol/
   mkdir /boot/sobol/
   mount /dev/sda3 /boot/sobol/
   Раздел для монтирования всегда sda3, т.к. он является бэкапом.
3) Выполнить очистку файлов и секторов
   scheck --reset-sectors
   scheck --reset-files
4) Добавить файлы, которые необходимо поставить на контроль целостности в АПМДЗ: загрузчик и ядро
   scheck --add-file=/image/syslinux/alt0/full.cz
   scheck --add-file=/image/syslinux/alt0/vmlinuz
5) Проверить, что файлы на контроле целостности с помощью команды:
   scheck --ls-files
6) Проверить пути с помощью команды:
   scheck --ls-path
   Вывод команд указанных в п. 5 и п.6 приведен на риснуке (См. Рисунок 3).

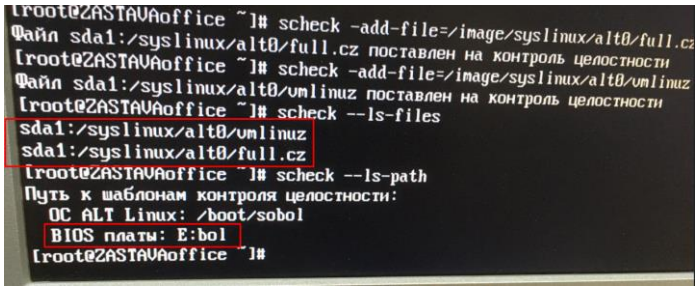

Рисунок 3 – Проверка файлов на контроле целостности и пути файлов контроля целостности

7) Перезагрузить АПК. Войти в Соболя с персональным идентификатором администратора.
8) В меню выбрать пункт «Контроль целостности»
9) Выбрать пункт меню «Каталог с шаблонами КЦ». Указать (подтведить) путь до каталога (по умолчанию диск E: но может быть и другой) с шаблонами. Внешний вид меню приведен на рисунке (см. Рисунок 4).

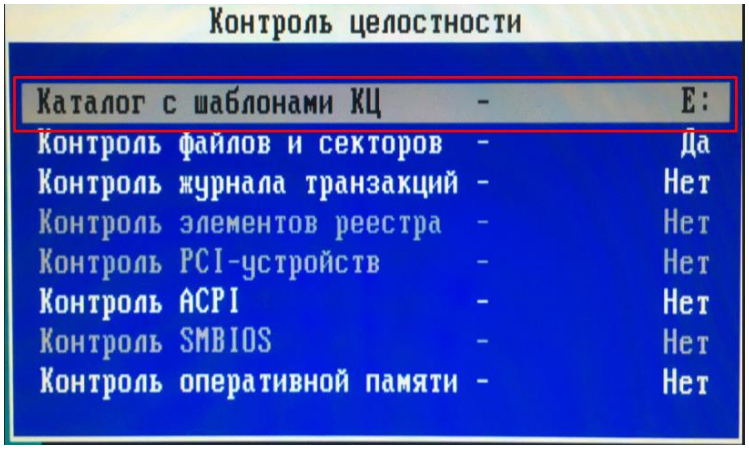

Рисунок 4 – Каталог с шаблонами КЦ

10) После указания Каталога с шаблонами КЦ будет разблокирован пункт меню АПМДЗ «Рассчёт контрольные суммы». Произвести расчёт контрольных сумм.

5.1.2. Проверка контрольной суммы

После установки ПК необходимо проверить контрольную сумму образа программной составляющей. Процедура проверки приведена в подразделе 6.1.

5.1.3. Настройка базовых сетевых параметров

Для настройки сетевых параметров необходимо выполнить следующие шаги:

1) В каталоге `/etc/net/ifaces` создать (или отредактировать содержимое) подкаталоги для каждого из настраиваемых сетевых интерфейсов. Имя каталога должно соответствовать имени интерфейса. В этих подкаталогах будут храниться

файлы с настройками конфигурации сетевых интерфейсов. Имена сетевых интерфейсов можно определить, используя команду `ip link`;

2) В каждом из подкаталогов создать (или отредактировать содержимое) файл `ipv4address`, в котором указать необходимый ip-адрес интерфейса с указанием маски;
3) В каждом из подкаталогов создать (или отредактировать содержимое) файл `options` и внести в него следующие строки

```
TYPE=eth
DISABLED=no
BOOTPROTO=static
```

В конце файла `options` необходимо наличие пустой строки.

4) В каждом из подкаталогов создать (или отредактировать содержимое) файл `ipv4route` в него строки необходимые для задания правил маршрутизации строки, например:

```
default via 10.111.15.1 metric 10
10.111.6.0/24 via 10.111.15.146 metric 15
```

Если необходимо обеспечить конфигурирование интерфейса по протоколу DHCP, то в файл `/etc/net/ifaces/eth0/options` следует записать строку `BOOTPROTO=dhcp`. Указание ip-адреса в файле `ipv4address` не требуется.

После выполнения настроек необходимо выполнить команду `service network restart` и убедиться в правильности применения заданных конфигурационных параметров.

Для создания и редактирования файлов рекомендуется использовать текстовый редактор vi.

5.1.4. Конфигурирование ПО «ЗАСТАВА-Офис»

При подготовке к работе необходимо в ПО «ЗАСТАВА-Офис» установить персональный и доверенный сертификаты и настроить параметры получения политики безопасности. Подробное описание процедуры установки сертификатов находится в п. 4.2.2.4.2. Подробное описание процедуры настройки политики безопасности находится в п. 4.2.2.5.1.

Кроме того, ПО «ЗАСТАВА-Офис» может быть сконфигурирован в соответствии с потребностями пользователя с помощью утилит конфигурирования, как описано в подразделе 4.2.

6. ОПИСАНИЕ ОПЕРАЦИЙ

Основные операции, выполняемые в ПК:

- просмотр локальных журналов событий (см. подраздел 6.5);
- проверка контрольной суммы программной составляющей (см. подраздел 6.1);
- смена пароля (см. подраздел 6.2);
- настройка задания автоматической перезагрузки СКЗИ (см. подраздел 6.4);
- обновление (см. подраздел 6.6);
- автоматический контроль целостности (см. подраздел 6.7).

6.1. Проверка контрольной суммы

Проверка контрольной суммы образа программной составляющей производится администратором ПК в следующих случаях:

- После процедуры установки ПК на СВТ;
- один раз в месяц;
- каждый раз после обновления ПО ПК.

Результаты проверки заносятся в формуляр ПК.

Процедура проверки контрольной суммы:

1) Включить СВТ с установленным ПК.
2) Выбрать пункт меню «ELVIS VPN GATE - Verify checksums» и нажать клавишу <Enter>.
3) На экране появится сообщение о проверке контрольной суммы образа программной составляющей. Дождаться окончания проверки.
4) По окончании проверки на экране появится сообщение с вычисленной контрольной суммой. Сверить вычисленную контрольную сумму, с указанной в формуляре.
5) Выключить СВТ с установленным ПК, нажав кнопку питания.

6.2. Смена пароля

Для смены пароля в ОС установлена утилита passwd.

После входа в ОС можно изменить пароль пользователя, для этого необходимо:

- если пользователь **root**, и необходимо поменять **его же пароль**, то выполнить команду *passwd*, затем, следуя инструкциям на экране ввести новый пароль и подтвердить правильность ввода, введя его повторно;
- если пользователь **root**, и необходимо поменять **пароль пользователя**, то выполнить команду *passwd <имя пользователя>*, затем, следуя инструкциям на экране ввести новый пароль и подтвердить правильность ввода, введя его повторно;

– если пользователь **не root**, то необходимо выполнить команду *passwd*, затем, следуя инструкциям на экране ввести текущий пароль, затем новый пароль и подтвердить правильность ввода нового пароля, введя его повторно.

6.3. 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.

Для просмотра доступных токенов в системе необходимо ввести команду:

vpnconfig -list token (см. Рисунок 5).

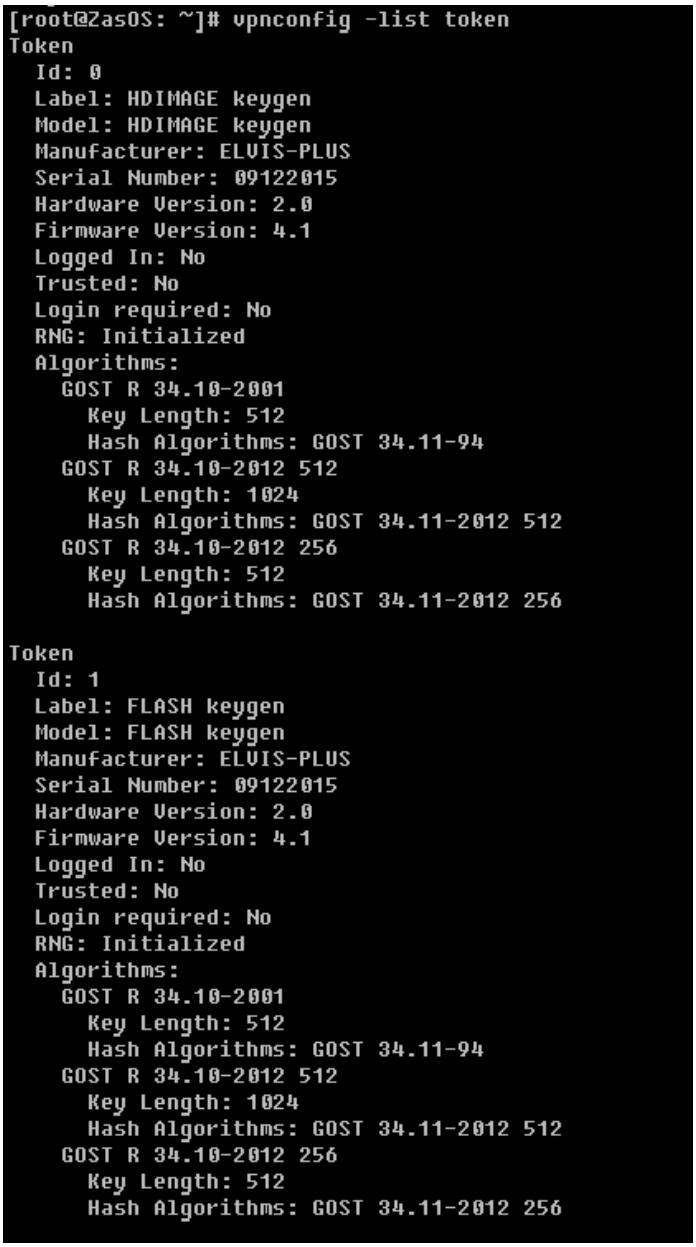

Рисунок 5 - Пример вывода команды *vpnconfig -list token*

Внизу, после описания каждого токена, после слова Algorithms: приведены все доступные для данного токена алгоритмы.

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).

Пример команды:

vpnconfig -add request 0 "GOST R 34.10-2012 256" 512 "GOST 34.11-2012 256" "C=RU,OU=PO,CN=APK-150" eku=ipsec

В результате выполнения команды будет создан ключевой контейнер и на экране появится запрос на выпуск сертификата, который необходимо передать в УЦ (см.Рисунок 6).

Рисунок 6 – Пример запроса на выпуск сертификата

После получения сертификата необходимо его добавить в ПО «ЗАСТАВА-Офис», для этого необходимо ввести команду:

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

6.4. Настройка задания автоматической перезагрузки СКЗИ

Для настройки заданий в ОС имеется утилита cron.

Шаблон заданий доступен для просмотра в файле /etc/crontab.template (см. Рисунок 7).

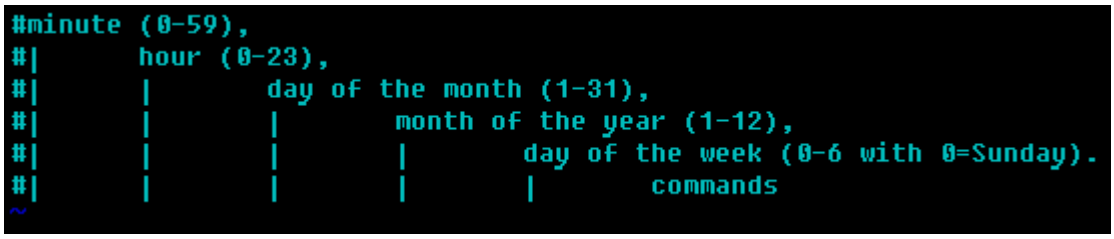

Рисунок 7 – Шаблон задания для *cron*

Для создания задания на перезагрузку СКЗИ необходимо:

– Войти в систему под учетной записью root;

– Ввести команду cronetab –e;

– Отредактировать строку следующего вида:

*1 3 * * * /usr/sbin/reboot*

Данная строка означает, что команда на перезагрузку будет выполняться в 3:01 каждый день. Исходя из вышеприведённого шаблона, изменить время на то, в которое необходимо осуществлять перезагрузку. Перезагрузка должна осуществляться каждый день.

6.5. Просмотр локальных журналов событий

Записи о регистрируемых системных событиях хранятся в директории `/var/vpnagent/log/` (например: `bin_log.txt` и `vpndmn_init.log`).

Для просмотра файлов журналов можно воспользоваться стандартными командами `cat, more, tail, less`, указав им путь к файлу в качестве параметра.

Для фильтрации записей в файлах журналов рекомендуется использовать команду `grep`.

6.6. Обновление

После установки обновления необходимо проверить контрольную сумму, как описано в п. 6.6.1.2. Результат проверки занести в формуляр.

6.6.1. Регламент обновления

6.6.1.1. 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 контрольные суммы этого дистрибутива в соответствии с ГОСТ Р 34.11-2012.

Доставка нового сертифицированного обновления ПК, должна производиться только по доверенному каналу.

6.6.1.2. Процедуры контроля целостности обновления

Для образа обновления необходимо произвести процедуру контроля целостности, используя утилиты icv_checker и icv_write, и, сравнив полученные контрольные суммы с указанными в формуляре.

6.6.1.3. Типовые процедуры тестирования обновления

Для тестирования обновлений необходимо выполнить загрузку ПК, убедиться в том, что контроль целостности успешно пройден и построить защищенное соединение.

6.6.1.4. 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*.

6.6.1.5. Процедуры контроля установки и применения обновления.

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

---

* «Специальными требованиями и рекомендациями по технической защите конфиденциальной информации (СТР-К)», утвержденного приказом Гостехкомиссии России от 30.08.2002 № 282;
«Требованиями о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах», утвержденными Приказом ФСТЭК России от 11.02.2013 г. № 17;
«Составом и содержанием организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных», утвержденными Приказом ФСТЭК России от 18.02.2013 г. № 21.

6.7. Автоматический контроль целостности

В ПК реализован автоматический запуск контроля целостности ПО «ЗАСТАВА-Офис», входящего в состав ПК.

По-умолчанию контроль целостности запускается один раз в 3 часа.

В случае положительного результата прохождения контроля целостности в системный журнал messages, расположенный в директории /var/log/, записывается событие «Динамический контроль СКЗИ пройден УСПЕШНО».

В случае отрицательного прохождения контроля целостности в системный журнал messages, записывается событие о нарушении целостности «Динамический контроль СКЗИ ПРОВАЛЕН».

Результаты проверки по каждому из проверяемых файлов записываются в файл /var/log/skzi_exist_cheksum.

В случае нарушения целостности аппаратная платформа ПК автоматически выключится.

6.7.1. Настройка параметров запуск автоматического контроля целостности

Для изменения параметров запуска автоматического контроля целостности необходимо:

1) Авторизоваться с правами учетной записи root, выполнив команду sudo su-
2) Выполнить команду crontab –e

Откроется файл настроек демона cron, в котором инструкции заданы в виде:

<Время выполнения задания> <Выполняемая команда>,

где параметр **<Время выполнения задания>** задается с помощью пяти параметров — минута, час, день, месяц, день недели. Для каждого параметра определен диапазон допустимых числовых значений: минута — от 0 до 59, час — от 0 до 23, день — от 1 до 31, месяц — от 1 до 12, день недели — от 0 до 7 (0 и 7 означают воскресенье).

По-умолчанию запуск regular_check_control_sum.sh выполняется каждую 1-ую минуту каждого 3-его часа.

Автоматический контроль целостности запускается скриптом regular_check_control_sum.sh

Изменить параметры запуска, сохранить файл. Изменения вступят в силу сразу же, перегрузка ПК не требуется.

7. НЕШТАТНЫЕ СИТУАЦИИ

7.1. Некорректная работа ПК после обновления

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

Возврат к эталону выполняется следующим образом:

1) Включить СВТ, дождаться появления меню выбора вариантов загрузки.
2) Выбрать пункт меню «ELVIS VPN GATE - FACTORY RESET» и нажать клавишу <Enter>.
3) На экране появится сообщение о проверке контрольной суммы заводского образа ОС. Дождаться окончания проверки.
4) По окончании проверки в случае совпадения контрольных сумм 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.).

При несовпадении контрольных сумм на экран будет выведено соответствующее сообщение. В этом случае необходимо обратиться к производителю.

7.2. Нарушение целостности образа

В случае нарушения целостности образа необходимо:

- назначить ответственного за расследование инцидента. Всю ключевую информацию считать скомпрометированной;
- 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 (см. подраздел 7.1) и выпустить новую ключевую информацию для VPN (см. подраздел 6.3);
- в случае если действия, которые привели к инциденту, являются угрозой безопасности, то необходимо отправить ПК Производителю на восстановление.

7.3. Автоматическое отключение АПК

Автоматическое отключение АПК происходит в случае неуспешного прохождения автоматического контроля целостности (см. подраздел 6.7). В случае автоматического отключения необходимо включить АПК заново. Если после включение обнаружится нарушение целостности образа АПК необходимо выполнить действия, описанные в подразделе 7.2.

Перечень принятых терминов и сокращений

Некоторые (в основном, англоязычные) сокращения и термины употребляются только во внутренних идентификаторах программ и приведены здесь для справки.

BIOS	–	Basic input/output system – Базовая система ввода-вывода
CA	–	Certification Authority – см. УЦ
CRL	–	Certificate Revocation List – см. СОС
CSP	–	Cryptographic Service Provider – Криптопровайдер
DH	–	Diffie-Hellman – протокол Диффи-Хеллмана
DHCP	–	Dynamic Host Configuration Protocol — протокол динамической настройки узла
DN	–	Distinguished Name – Уникальное имя
DNS	–	Domain Name System – система доменных имен для именования хостов в глобальных сетях
EAP		Extensible Authentication Protocol - расширяемый Протокол Аутентификации
ESP	–	Encapsulated Security Payload – протокол из группы IPsecGMT – время по Гринвичу
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
ПК		Аппаратно-программный комплекс
ГОСТ	–	Государственный стандарт
ЛПБ	–	Локальная политика безопасности
МЭ	–	Межсетевой экран
ОО		Объект оценки
ОС	–	Операционная система
ПО	–	Программное обеспечение
СКЗИ	–	Средство криптографической защиты информации
СОС	–	Список отозванных сертификатов
УЦ	–	Удостоверяющий центр
ФБО		Функции безопасности объекта
ФСТЭК России	–	Федеральная служба по техническому и экспортному контролю
ЦУП	–	Центр управления политиками безопасности

Лист регистрации изменений

Изменение	Номера листов				Всего листов в документе	Номер документа	Вх. № сопроводительного документа и дата	Подпись	Дата
	измененных	замененных	новых	изъятых					
1	2	3	4	5	6	7	8	9	10