УТВЕРЖДЕН
МКЕЮ.00630.ИЗ-ЛУ

«Аппаратно-программный комплекс
«VPN/FW «ЗАСТАВА-150», версия 6»

(«АПК «ЗАСТАВА-150», версия 6»)

Руководство администратора

МКЕЮ.00630.ИЗ

2021

Инв. № подл.	Подп. и дата	Взам. инв. №	Инв. № дубл.	Подп. и дата
7434				

СОДЕРЖАНИЕ

1 ВВЕДЕНИЕ

Данный документ предназначен для администратора системы МКЕЮ.00630 «Аппаратно-программный комплекс «VPN/FW «ЗАСТАВА-150», версия 6» (далее - «АПК «ЗАСТАВА-150», версия 6», далее – АПК) и содержит описание составных частей АПК, описание интерфейса программного обеспечения (ПО), процедуры, выполняемые администратором в процессе подготовки АПК к работе, текущие операции, действия при возникновении нештатных ситуаций.

1.1 Назначение

АПК 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.

АПК обеспечивает защиту информации конфиденциального характера, не содержащей сведений, составляющих государственную тайну.

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 АПК 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 Технические характеристики

Технические характеристики АПК приведены в таблице (см. Таблица 1).

Таблица 1 – Технические характеристики АПК

Наименование	Значение
Габаритные размеры (В×Ш×Г)	202 x 205 x 42 мм
Масса, не более	1,1 кг
Входное напряжение постоянного тока	От универсального (110-230 В) адаптера переменного тока 12 В 3 А
Потребляемая мощность, не более	24 Вт
Возможность установки локального ПО	Нет
Процессор	Intel Baytrail J1900 QuadCore
Частота процессора	2,0 ГГц
Объем оперативной памяти	4 Гбайт
Объем жесткого диска	32 Гбайт
Количество подключаемых мониторов	1

АПК может работать круглосуточно. При эксплуатации АПК в круглосуточном режиме требуются обязательное извлечение ключевого носителя и перезагрузка не реже, чем через каждые 24 часа.

2.2 Состав

В состав АПК входит:

- аппаратная платформа ТОНК 1800S производства ООО «Группа Компаний ТОНК» (процессор Intel Baytrail J1900 QuadCore);
- электронный идентификатор ESMART Token ГОСТ, аппаратно-реализующий российские стандарты электронной подписи, шифрования, хэширования;
- операционная система (ОС) собственной сборки на базе Linux, 64-битная версия;
- средство криптографической защиты информации (СКЗИ) ЖТЯИ.00088-01 «КриптоПро CSP», версия 4.0 (исполнение 2-Base);
- ПО «ЗАСТАВА-Офис», версия 6;
- программный компонент ESMART PKCS11.

2.2.1 Системный блок

Внешний вид передней панели системного блока АПК представлен на рисунке (см. Рисунок 1). Обозначения элементов на передней панели системного блока приведены в таблице (см. Таблица 2).

Рисунок 1 – Внешний вид передней панели системного блока

Таблица 2 – Назначение элементов передней панели системного блока

№ указателя	Назначение элемента
1	Кнопка питания
2	Разъем для подключения монитора, закрывается крышкой

Внешний вид задней панели системного блока представлен на рисунке (см. Рисунок 2). Обозначения элементов на задней панели системного блока приведены в таблице (см. Таблица 3).

Таблица 3 – Назначение элементов задней панели системного блока

№ указателя	Назначение элемента
1	Разъем электропитания
2	Порт USB (2 шт.)
3	COM порт
4-9	LAN (RJ-45)

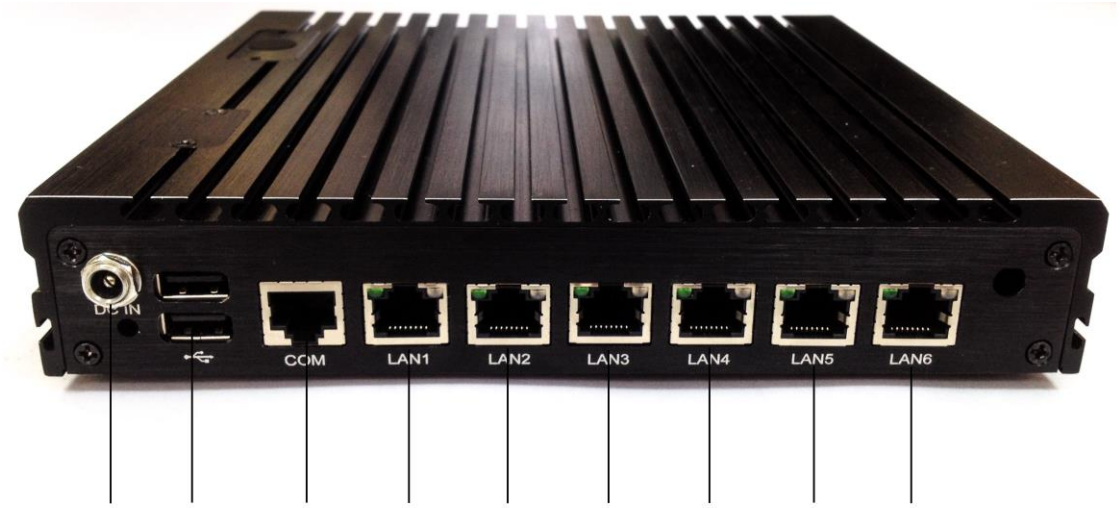

Рисунок 2 – Внешний вид задней панели системного блока

2.3 Полная функциональная спецификация

2.3.1 Список функциональных возможностей безопасности АПК

АПК реализует следующие функции безопасности:

- аудит безопасности;
- идентификация и аутентификация;
- защита данных пользователей;
- управление безопасностью;
- защита функций безопасности объекта (ФБО);
- использование ресурсов.

2.3.1.1 Описание пользовательских ролей (Пользователь, Администратор)

В АПК определены роли:

- Администратор АПК, имеющий непосредственный доступ (или удалённый доступ в шифрованном виде) к АПК и осуществляющий использование всех возможностей АПК и управляющий всем функционалом АПК;
- удаленный привилегированный пользователь (Администратор программного комплекса МКЕЮ.00631-01 «Программный комплекс «VPN/FW «ЗАСТАВА-Управление», версия 6 КС3» («VPN/FW «ЗАСТАВА-Управление», версия 6 КС3») (исполнение ZM-WS64-VO-03) (далее – ПК «ЗАСТАВА-Управление»)), осуществляющий формирование глобальной политики безопасности (ГПБ) в информационно-телекоммуникационной сети и локальную политику безопасности (ЛПБ) АПК, а также формирование и передачу управляющих команд в шифрованном виде по общедоступным каналам связи;

– удалённый пользователь, устанавливающий защищённое соединение согласно заданной ГПБ с целью получения доступа к ресурсам, которые защищает АПК.

2.3.1.2 Аудит безопасности

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

– запуск и завершение выполнения функций;
– действия, предпринимаемые АПК в ответ на нарушения безопасности;
– действия, предпринимаемые АПК 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 АПК;
– изменение настроек получения политики безопасности;
– все попытки использования функциональных возможностей распределения ресурсов АПК с учетом приоритетности обслуживания информационных потоков;
– сообщения синхронизации при использовании кластеризации;
– удачный вход Администратора АПК в программную составляющую;
– неудачный вход Администратора АПК в программную составляющую;
– запуск и остановка службы АПК;
– неудачный запуск и остановка службы АПК, реализующей ФБО;
– результат проверки контрольных сумм программной составляющей и ПО «ЗАСТАВА-Офис».

Администратор АПК имеет возможность выбора одного из четырех уровней журналирования:

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

Не рекомендуется устанавливать уровень лога – «заблокирован».

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

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

2.3.1.3 Идентификация и аутентификация

Доступ к ПО «ЗАСТАВА-Офис», данным программной составляющей АПК, локальным журналам аудита АПК предоставляется Администратору АПК после аутентификации и авторизации в программной составляющей АПК с использованием цифровых сертификатов, хранящихся на внешнем токене.

2.3.1.4 Защита данных пользователей

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

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

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

АПК имеет интерфейс управления, позволяющий принимать управляющие команды от взаимодействующих с АПК средств защиты информации других видов: интерфейс командной строки ПК «ЗАСТАВА-Управление», позволяющий задавать отдельные элементы политики безопасности АПК, доставлять их и активировать.

При нарушении функционирования или внеплановой остановке службы ПО «ЗАСТАВА Офис» происходит блокировка сетевого трафика, проходящего через АПК, при помощи активации политики Default Driver Policy, которая может блокировать любой сетевой трафик.

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

АПК осуществляет фильтрацию пакетов, исходящих за пределы АПК, переназначение IP-адресов и посредничество в передаче данных, исключающее прямое взаимодействие. При успешных результатах фильтрации информации сетевого трафика и других проверок при посредничестве в передаче АПК разрешает прохождение пакетов за пределы АПК.

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

АПК 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.

АПК обеспечивает фильтрацию сетевого трафика с использованием состояний (statefull). АПК 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.

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

2.3.1.5 Управление безопасностью

Администратор АПК, прошедший аутентификацию в программной составляющей АПК, имеет возможность производить следующие действия:

- производить настройки программной составляющей АПК;
- 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 ЛПБ;
- создавать и редактировать пользователей в программной составляющей АПК;
- производить сетевые настройки АПК;
- производить другие настройки программной составляющей АПК;
- просматривать, сбрасывать значения таблицы состояний соединений;
- восстанавливать работоспособность АПК.

В АПК реализован механизм удаленного управления.

Администратор АПК имеет возможность задавать и доставлять на АПК правила фильтрации по доверенному каналу связи с ПК «ЗАСТАВА-Управление», основанные на атрибутах безопасности.

2.3.1.6 Защита ФБО

В случае сбоя при прогрузке ЛПБ ПО «ЗАСТАВА Офис» продолжает обработку всех пакетов в соответствии с ранее прогруженной политикой безопасности. При этом в мониторе ПК «ЗАСТАВА-Управление» соответствующий объект топологии отображается со статусом «Состояние неизвестно». В это время АПК 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) ПО «ЗАСТАВА Офис» из состава АПК перестает посылать на ПК «ЗАСТАВА-Управление» сигналы, свидетельствующие о нормальном функционировании. При этом АПК переходит в аварийный режим, который предполагает применение политики аварийного режима, определенной в настройках службы vpndmn.

В случае сбоя при запуске службы (vpndmn) ПО «ЗАСТАВА Офис» АПК переходит в аварийный режим, который предполагает применение политики аварийного режима, определенной в настройках драйвера vpnpcap.

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

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

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

При каждом включении АПК выполняется проверка целостности модуля-загрузки и программной составляющей АПК. При несовпадении контрольных сумм с эталонными значениями АПК выключается по питанию. События об удачном и неудачном прохождении проверки контрольных сумм с эталонными значениями записываются в локальный журнал аудита. Совпадение контрольной суммы гарантирует правильность функционирования ФБО, дополнительных пакетов самотестирования не требуется.

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 АПК или ПО «ЗАСТАВА-Офис». Доступ к данной функции ограничен и предоставляется только Администратору АПК.

2.3.1.7 Использование ресурсов

Резервирование функциональных возможностей АПК обеспечивается кластеризацией. При сбое службы ПО «ЗАСТАВА-Офис», внеплановом прерывании работы службы ПО «ЗАСТАВА-Офис», выходе из строя или выключении серверной платформы основного узла

АПК, резервный узел становится основным и продолжает выполнять все предписанные и настроенные функции АПК.

2.3.2 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. 4.2.2.5.1.2.

Системная политика может быть загружена из файла с сервера прогрузки политики или соответствовать «Политике драйвера по умолчанию». Настройка «Системной политики» описана в п. 4.2.2.5.1.1.

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

2.3.3 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 IKE.

2.3.4 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.

2.3.5 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
```

2.3.6 Демонстрация прослеживания функциональных требований безопасности к интерфейсам взаимодействия

Описанные выше интерфейсы взаимодействия обеспечивают доставку ЛПБ, реализующую ФБО, описанные в пунктах 2.3.1.3, 2.3.1.4, 2.3.1.6.

2.3.7 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. 2.3.1.2.

2.3.8 Описание для каждой пользовательской роли принципов безопасной работы с предоставленными интерфейсами взаимодействия

К интерфейсу прогрузки ЛПБ имеет доступ только Администратор АПК.

Администратору АПК 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 АПК;

– запрет на установку уровня журналирования равный Disable;

– обеспечение физической защиты административного токена;

– сохранение в секрете PIN-кода административного токена;

– сохранение в секрете пароля на BIOS, запрет на использование пароля, установленного производителем;

– 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).

2.3.9 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. 2.3.8.

2.3.10 Описание для каждой пользовательской роли типов событий, имеющих значение для безопасности

Типовые действия Администратора АПК 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.

2.3.11 Идентификация всех режимов работы АПК (включая операции после сбоев и ошибок эксплуатации), их последствия и участие в обеспечении безопасного функционирования

Штатный режим работы АПК обеспечивает все функции в соответствии с заданной ЛПБ.

В аварийном режиме активируется «политика драйвера по умолчанию» или политика, заданная по умолчанию для модуля vpnpcap.

2.3.12 Описание для каждой пользовательской роли мер безопасности для среды функционирования

Для того чтобы АПК 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 АПК;
- обеспечение исключение каналов связи защищаемой информационной системы с иными информационными системами в обход АПК;
- разработка нормативных документов, определяющих порядок допуска персонала к ресурсам АПК и назначения их полномочий;
- обеспечение физической защиты административного персонального идентификатора;
- сохранение в секрете идентификаторов (имен) и паролей Администратора (администраторов) и Пользователей АПК.

3 УСТАНОВКА И ПОДГОТОВКА К РАБОТЕ АПК «ЗАСТАВА-150»

3.1 Шаги, необходимые для безопасной приемки и настройки

АПК поставляется с полностью установленным ПО.

Подготовка АПК к работе включает следующие операции:

– сборку и подключение АПК;
– проверку настроек BIOS;
– проверку контрольной суммы образа ОС;
– настройку сетевых параметров (при необходимости);
– установку персонального и доверенного сертификатов;
– настройку получения политики безопасности.

3.1.1 Сборка и подключение АПК

Порядок подключения АПК (см. Рисунок 2**Ошибка! Источник ссылки не найден.**):

1) подключить к системному блоку монитор, клавиатуру;
2) подключить АПК к сети Интернет с помощью сетевого кабеля (поз. 4 - 9);
3) подключить блок питания к разъему электропитания (поз. 1);
4) подключить монитор и системный блок к сети питания.

3.1.2 Проверка настроек BIOS

Для проверки настроек BIOS необходимо:

1) Включить АПК кнопкой питания . Для входа в меню BIOS до начала загрузки программной составляющей надо нажимать клавишу <Del> до появления запроса на ввод пароля.
2) При появлении запроса на ввод пароля ввести пароль на BIOS. Пароль, установленный производителем: **Tonk123!@#**.

Рекомендуется сменить установленный производителем пароль.

3) После появления на экране меню BIOS проверить и, при необходимости, изменить настройки следующих параметров BIOS:

– в разделе «Main» (см. Рисунок 3) дата (параметр «System Date») и время (параметр «System time») должны совпадать с текущими;

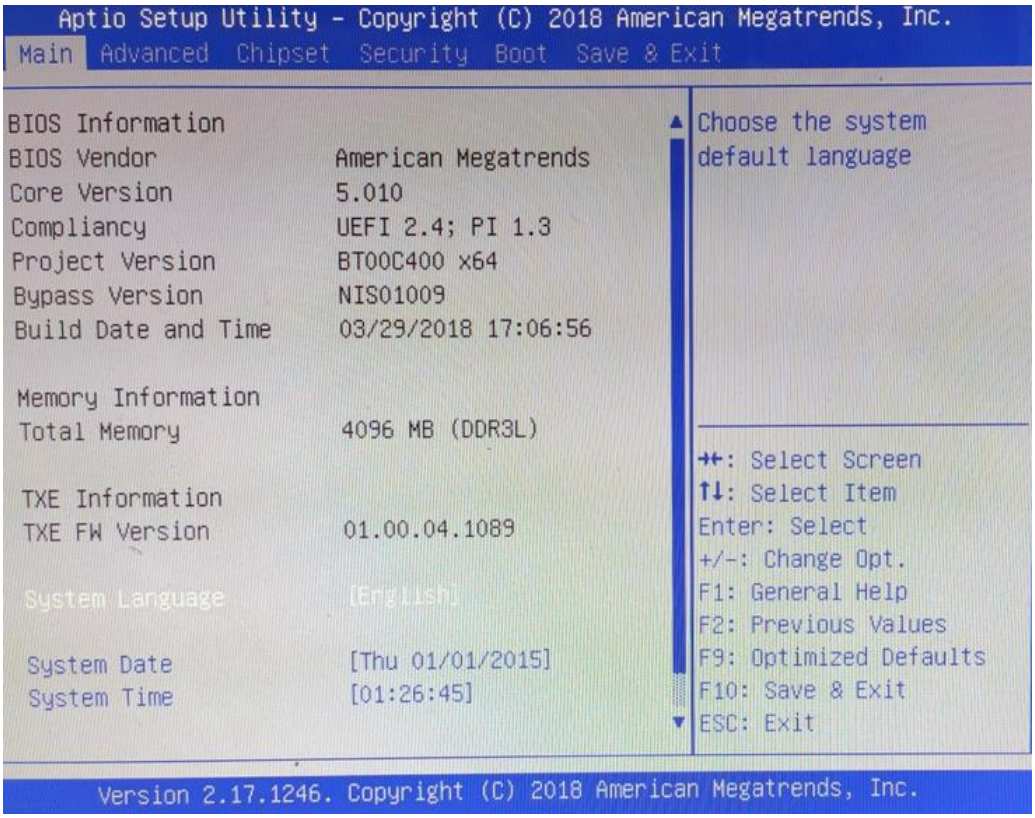

Рисунок 3 – Раздел «Main»

– в разделе «Advanced/LAN Configuration» (см. Рисунок 4) параметр «LAN PXE Boot» должен иметь значение «Disabled»;

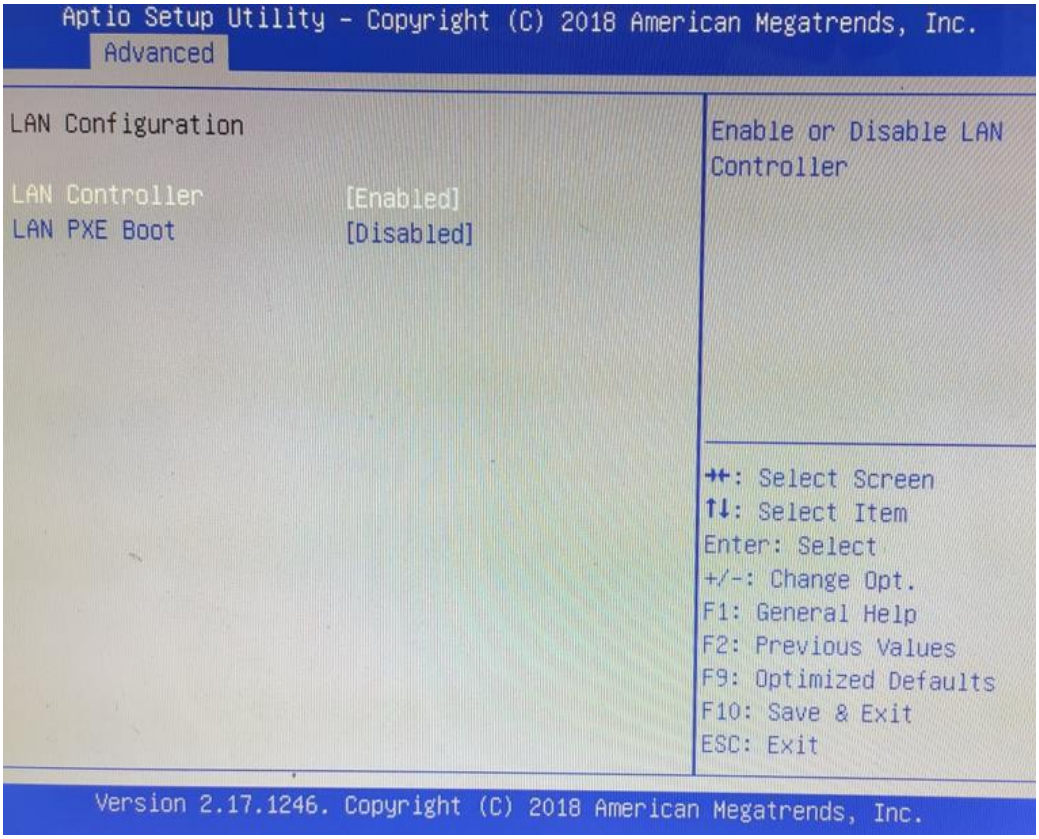

Рисунок 4 – Раздел «LAN Configuration»

– в разделе «Boot \\ Boot Option Properties» параметры Boot Option # 2 установить в состояние «Disabled»;

– в разделе «Boot» (см. Рисунок 5) параметр «Boot Option #1» должен иметь значение «(штатный) загрузочный диск»;

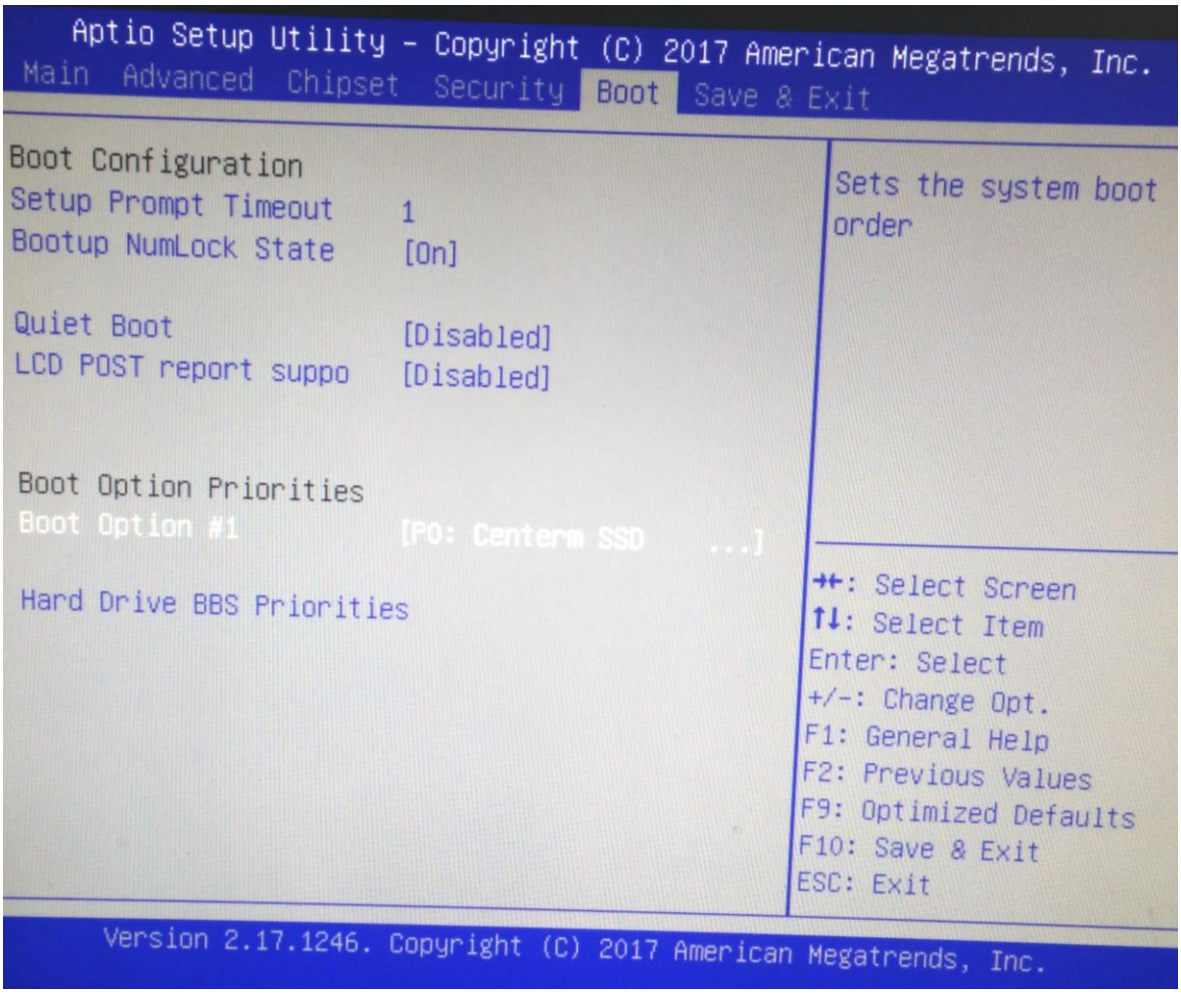

Рисунок 5 – Раздел «Boot»

– в разделе «Boot \\ USB Device BBS Priorieties» параметр Boot Option # 1 установить в состояние «(штатный) загрузочный диск»;
– в разделе «Advanced \\ Network Bypass Configuration» параметр Network bypass BIOS s установить в состояние «Disabled»;
– в разделе «Advanced \\ CPU Configuration» параметр Intel Virtualization Technology установить в состояние «Disabled»;
– в разделе «Advanced \\ PPM Configuration» параметр EIST установить в состояние «Disabled»;
– в разделе «Advanced \\ PPM Configuration» параметр CPU C state Report установить в состояние «Disabled»;
– в разделе «Advanced \\ USB Configuration» параметр USB Configuration XHCI Mode установить в состояние «Disabled».

Примечание – В случае выхода из строя батареи питания CMOS на системной плате АПК осуществляется замена батареи, повторная установка вышеперечисленных параметров

BIOS и смена пароля на вход в меню BIOS. Периодичность смены батареи – один раз в пять лет.

4) В случае изменения настроек следует сохранить изменения, выбрав в разделе «Save & Exit» параметр «Save Changes and Exit».

5) Выключить АПК кнопкой питания .

3.1.3 Сброс настроек датчика вскрытия корпуса

Для сброса датчика вскрытия корпуса АПК необходимо:

1) Зайти в BIOS нажатием клавиши <DELETE>.

2) Перейти в раздел Advanced -> Caseopen Configuration (см. Рисунок 6).

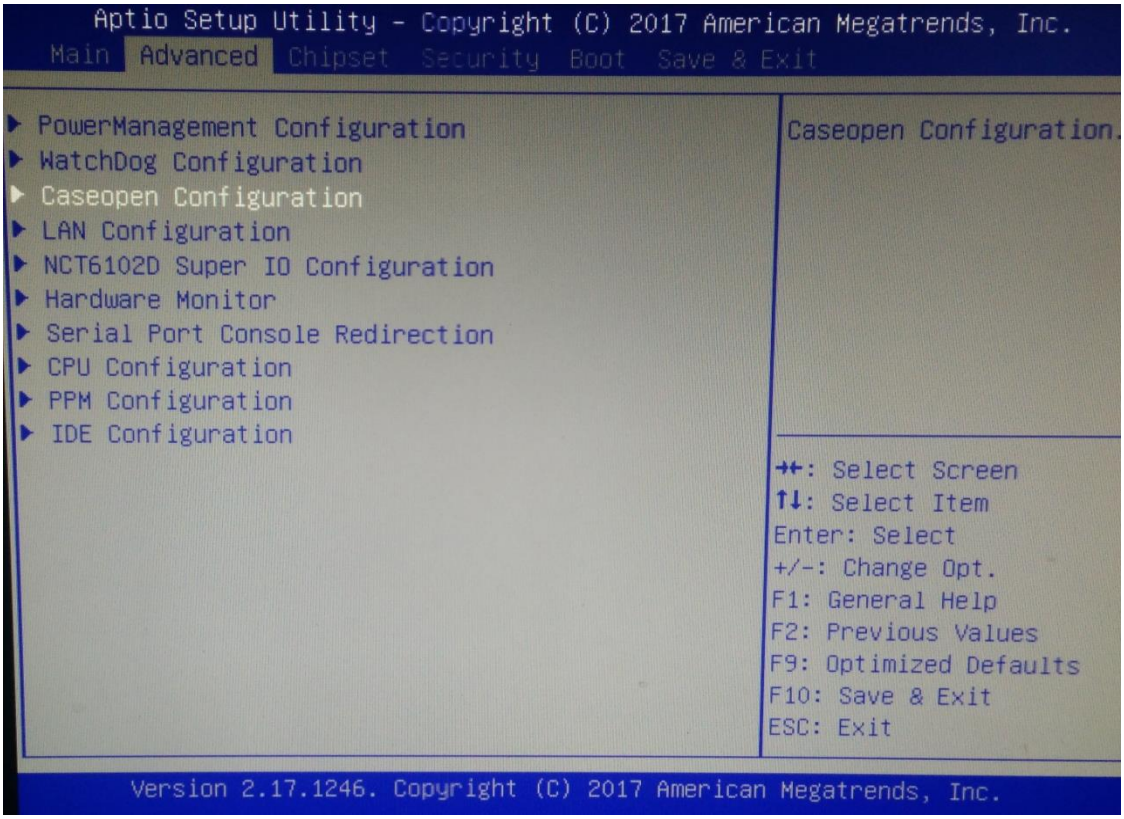

Рисунок 6 – Выбор раздела

3) Для отключения датчика вскрытия корпуса АПК необходимо в параметре Caseopen Support выставить значение «Disabled» (см. Рисунок 7).

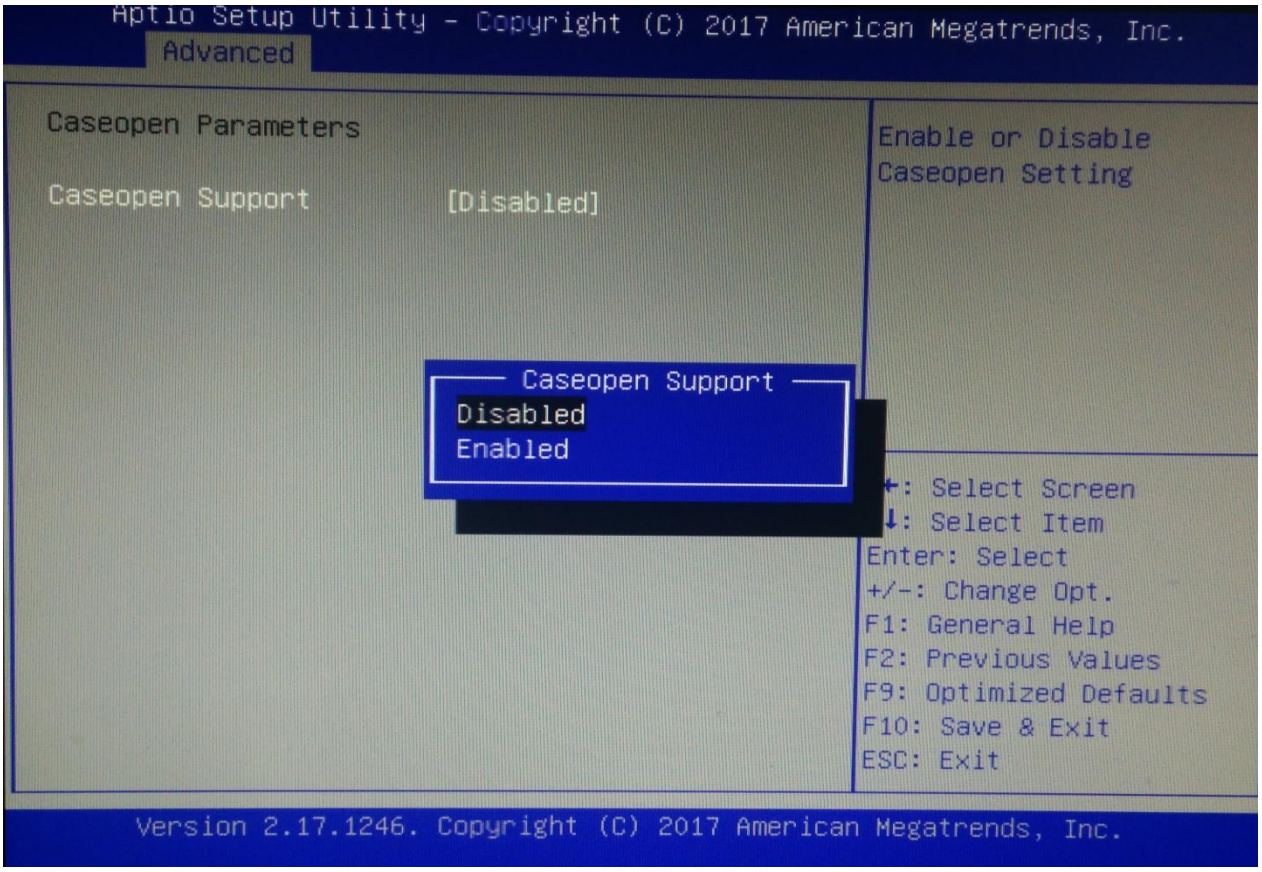

Рисунок 7 – Отключение датчика вскрытия корпуса

4) Для сброса датчика вскрытия корпуса (при изменении аппаратной конфигурации), необходимо убедиться в том, что датчик включен (Caseopen Support -> Enabled), и в параметре Clear Caseopen Status выставить значение «Clear Status» (см. Рисунок 8).

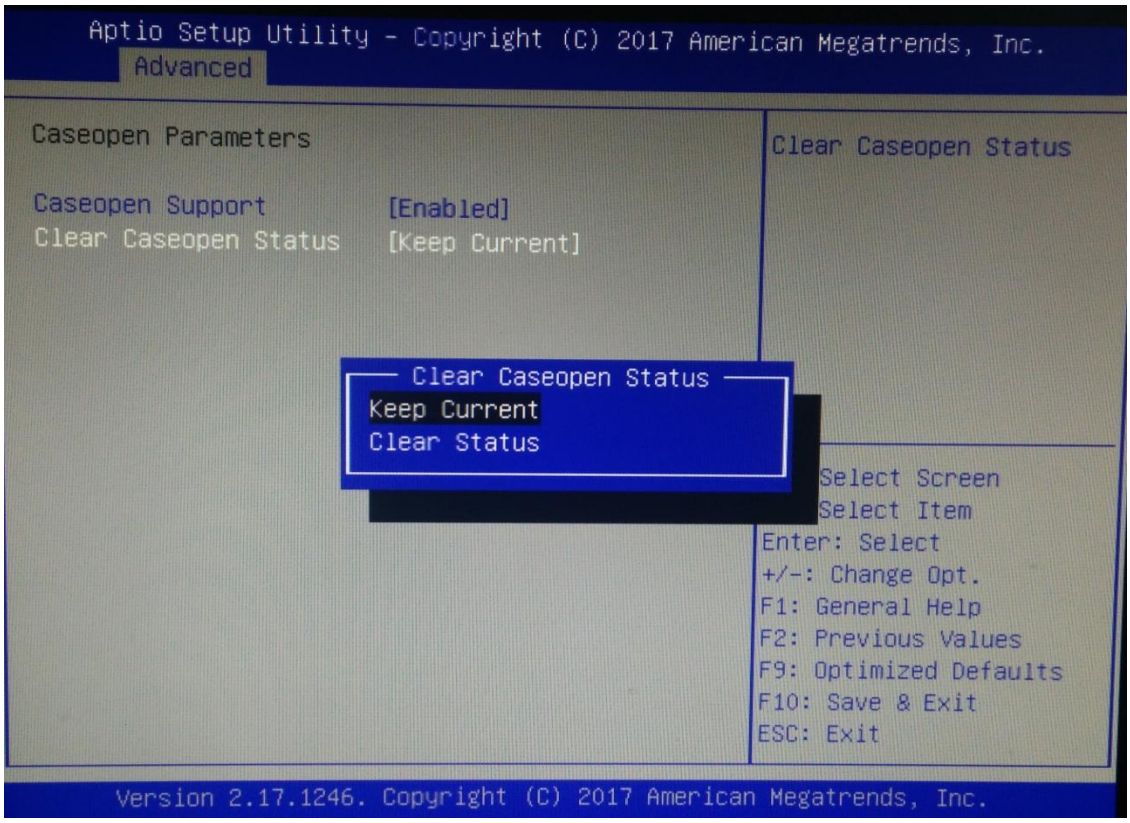

Рисунок 8 – Сброс конфигурации датчика вскрытия

5) Сохранить изменения и выйти из BIOS нажатием клавиши <F10>.

3.1.4 Проверка контрольной суммы

При первом включении необходимо проверить контрольную сумму образа программной составляющей. Процедура проверки приведена в подразделе 3.2.2.

3.1.5 Настройка сетевых параметров

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

Процедура настройки сетевых параметров приведена в подразделе 3.2.8.

3.1.6 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.

3.2 Описание операций

Основные операции, выполняемые в АПК:

- включение (см. подраздел 3.2.1);
- просмотр локальных журналов событий (см. подраздел 3.2.5);
- проверка контрольной суммы программной составляющей (см. подраздел 3.2.2);
- смена PIN-кода ключевого носителя (см. подраздел 0);
- обновление (см. подраздел 3.2.5);
- автоматический контроль целостности (см. подраздел 3.2.19);
- выключение (см. подраздел 3.2.19).

3.2.1 Включение

Для включения АПК необходимо:

1) Включить АПК нажатием кнопки питания. Дождаться загрузки программной составляющей;
2) Подключить ключевой носитель к USB-разъему;
3) Ввести логин пользователя, в появившемся запросе ввести PIN-код пользователя ключевого носителя администратора АПК. Будет выполнен вход в систему.

Внимание! После ввода PIN-кода не допускается оставлять ключевой носитель без контроля, в том числе при уходе с рабочего места.

3.2.2 Проверка контрольной суммы

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

- при первом включении АПК;
- один раз в месяц;
- каждый раз после обновления ПО АПК.

Результаты проверки заносятся в формуляр АПК.

Процедура проверки контрольной суммы:

1) Включить АПК, нажав кнопку питания , дождаться появления меню выбора вариантов загрузки «Boot menu for ZASTAVA-150».
2) Выбрать пункт меню «Controll sum check» 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 АПК, нажав кнопку питания.

3.2.3 Смена пароля на BIOS

Для смены пароля на BIOS необходимо:

1) Включить АПК кнопкой питания . Для входа в меню BIOS до начала загрузки программной составляющей надо нажимать клавишу <Del> до появления запроса на ввод пароля;
2) При появлении запроса на ввод пароля ввести пароль на BIOS. Пароль, установленный производителем: **Tonk123!@#;**
3) В разделе «Security» (см. Рисунок 9) выбрать «Administrator Password» и нажать клавишу <Enter>;
4) Ввести новый пароль и подтверждение.

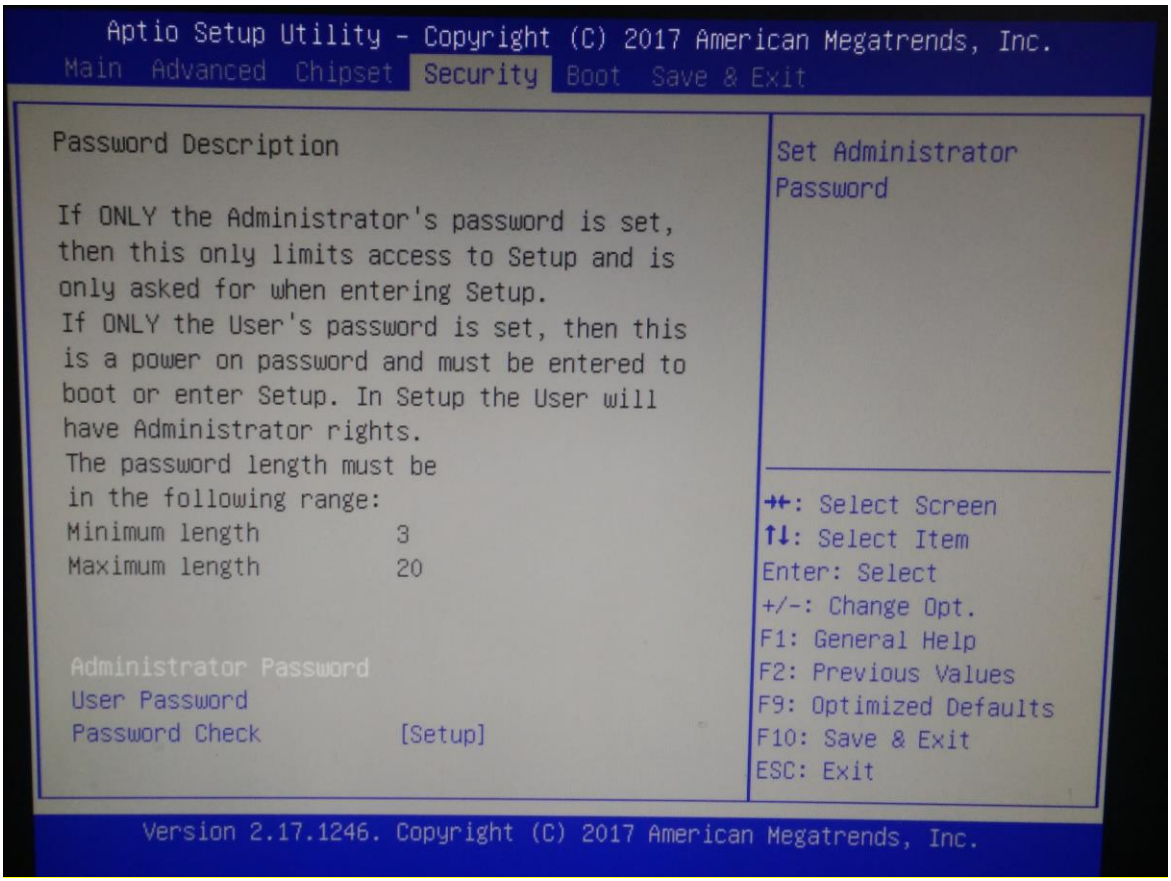

Рисунок 9 – Раздел «Security»

Запрещается использование установленного производителем пароля BIOS. Установленный пароль требуется держать в секрете.

3.2.4 Смена PIN-кода ключевого носителя

Смена PIN-кода пользователя ключевого носителя производится перед началом его использования. В дальнейшем смену PIN-кода следует производить не реже, чем один раз в 6 месяцев. Смена PIN-кода производится с помощью ПО «ЗАСТАВА-Офис».

Внимание! Администратор и пользователи АПК обязаны хранить PIN-код доступа к своим ключевым носителям в тайне, и не имеют права сообщать PIN-код никому.

Для смены пароля необходимо воспользоваться командой:

`vpnconfig -password token <token_id> <old_pin> <new_pin> [save] [admin]`, где

`<token_id>` - идентификатор токена, который можно получить с помощью команды `vpnconfig – list token`;

`<old_pin>` - старый пароль;

`<new_pin>` - новый пароль;

`[save]` – дополнительный параметр, который позволяет сохранить пароль для последующих соединений;

[admin] – дополнительный параметр, указывающий на смену пароля администратора, а не пользователя.

3.2.5 Смена пароля пользователя

Для смены пароля пользователя в ОС установлена утилита passwd.

Для входа в ОС необходимо:

- предоставить токен, содержащий закрытый ключ и сертификат пользователя;
- ввести логин пользователя;
- ввести пароль пользователя;
- дождаться проверки *pam_pkcs11* и ввести PIN-код токена.

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.

3.2.6 Создание запроса PKCS10 на выпуск сертификата

Для создания запроса на выпуск сертификата используются встроенные в ПО «ЗАСТАВА-Офис» возможности. 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 в системе токенов необходимо ввести команду:

vpnconfig -list token (см. Рисунок 10).

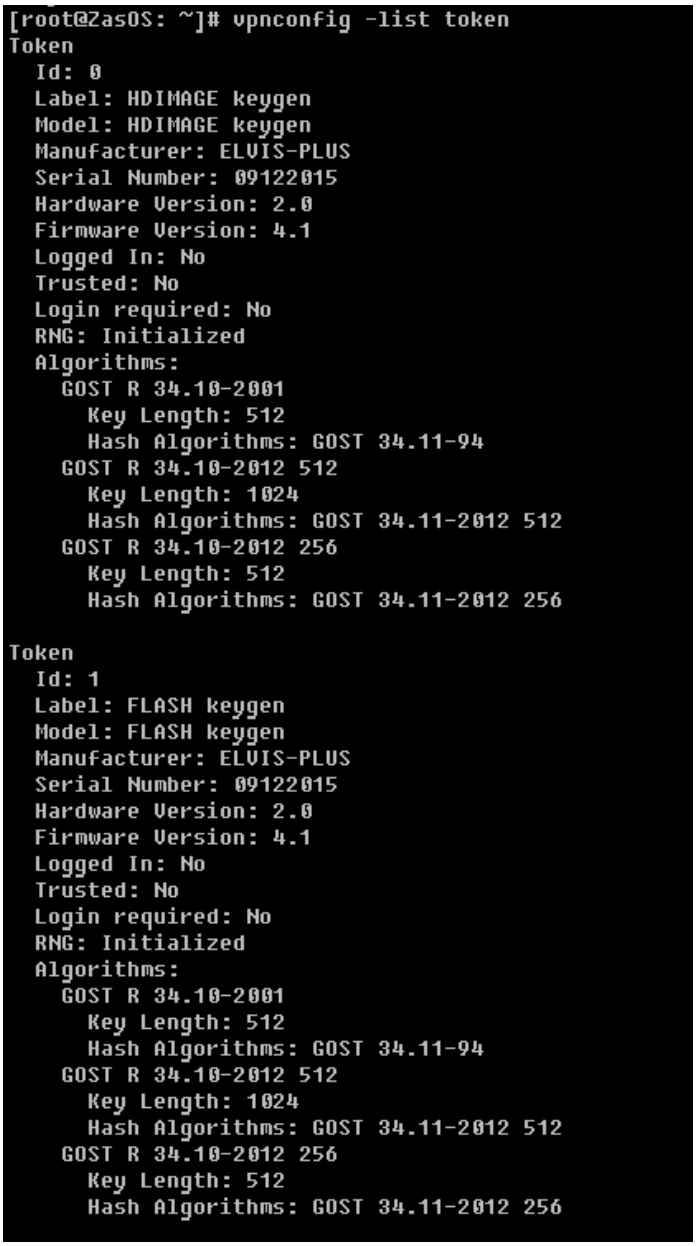

Рисунок 10 - Пример вывода команды *vpnconfig -list token*

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 11).

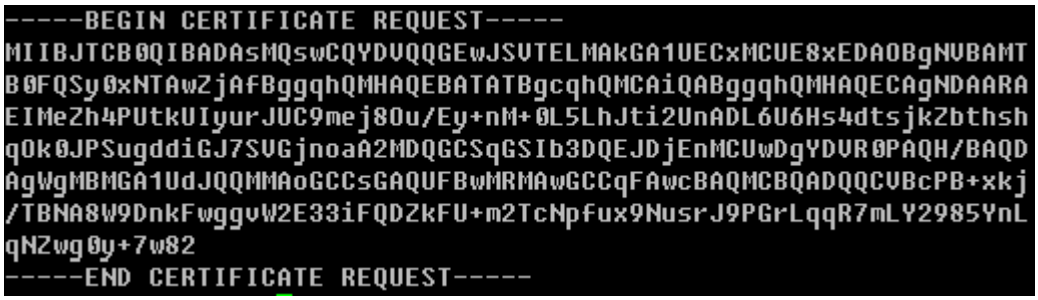

Рисунок 11 – Пример запроса на выпуск сертификата

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>

3.2.7 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 12).

```
#minute (0-59),
#|      hour (0-23),
#|      |       day of the month (1-31),
#|      |       |       month of the year (1-12),
#|      |       |       |       day of the week (0-6 with 0=Sunday).
#|      |       |       |       |       commands
```

Рисунок 12 – 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.

3.2.8 Настройка сетевых соединений

Для настройки сетевых параметров рекомендуется использовать средства, предоставляемые утилитой NetworkManager (далее –NM) т.к. она является универсальной, и её нотация не зависит от дистрибутива. Далее будет приведены команды NM по настройке различных сетевых аспектов из CLI (утилита nmcli), но возможность настройки при помощи редактирования системных фалов доступна также, нотация при этом схожа с debian-based дистрибутивами.

У nmcli много опций, также есть параметры, начинающиеся с + или – (например, +ipv4.routes для добавления статического маршрута), поэтому рекомендуется пользоваться автодополнением т.к. в ОС имеются дополнения bash-completion для множества утилит, включая и NetworkManager

3.2.9 Просмотр доступных физических устройств

Для того чтобы посмотреть физические устройства, доступные для настройки, необходимо ввести команду *nmcli devices* (см. Рисунок 13).

```
[root@ZasOS: ~]# nmcli device
УСТРОЙСТВО  ТИП       СОСТОЯНИЕ       СОЕДИНЕНИЕ
eth0        ethernet  подключено      eth0
eth1        ethernet  недоступен      --
eth2        ethernet  недоступен      --
eth3        ethernet  недоступен      --
eth4        ethernet  недоступен      --
eth5        ethernet  недоступен      --
```

Рисунок 13 – Пример вывода команды *nmcli device*

3.2.10 Создание соединения

Соединение является набором сетевых параметров (DNS, IP-адрес, маршруты и т.д.), которые могут быть применены к физическому устройству. Одномоментно к физическому устройству может быть применено только одно соединение. Можно создать несколько соединений и производить переключение на одно из них, при необходимости.

Команда, создающая соединение, может сразу иметь очень много параметров, разделенных пробелом. Также можно создать соединение с минимально необходимым набором параметров, а затем модифицировать его с помощью дополнительных параметров

Пример команды для создания соединения типа Ethernet:

nmcli connection add con-name eth1 ifname eth1 type ethernet ipv4.addresses 10.0.0.1/24 gw4 10.0.0.254 ipv4.method manual autoconnect on

В данном примере выделяются следующие параметры:

- *con-name* – указывает понятное человеку имя соединения;
- *ifname* – задает физическое устройство для которого будет применимо данное соединение;
- *type* – тип настраиваемого соединения. Список всех доступных типов можно посмотреть с помощью автодополнения;
- *ipv4.addresses* – задает IP-адрес для соединения;
- *gw4* – задает шлюз по умолчанию для данного соединения;
- *ipv4.method* – способ получения адреса, может быть auto или manual (DHCP или Static);
- *autoconnect* – автоматическое применение соединения при старте системы.

Пример команды для создания соединения типа VLAN:

nmcli connection add con-name eth1.90 type vlan vlan.id 9 vlan.parent eth1 ipv4.addresses 10.0.0.1/24 ipv4.method manual

В данном примере выделяются следующие параметры:

– *type* – тип vlan;

– *vlan.id* – номер тега для vlan;

– *vlan.parent* – физическое устройство на котором будет создан vlan.

Остальные параметры идентичны параметрам в предыдущем примере.

Для оперативного просмотра настроек VLAN (физическое устройство, тэг) можно воспользоваться командой: *cat /proc/net/vlan/config* (см. Рисунок 14).

```
[root@ZasOS: ~]# cat /proc/net/vlan/config
VLAN Dev name    | VLAN ID
Name-Type: VLAN_NAME_TYPE_RAW_PLUS_VID_NO_PAD
eth1.9          | 9  | eth1
eth1.11         | 11  | eth1
[root@ZasOS: ~]#
```

Рисунок 14 – Пример вывода команды *cat /proc/net/vlan/config*

3.2.11 Изменение\добавление IP-адреса у существующего соединения

Пример команды для изменения или добавления текущего IP-адреса соединения:

nmcli connection modify eth2 ipv4.addresses 10.0.0.1/24

В данном примере ключевой параметр - *modify*, после которого идет название соединения, параметры которого необходимо подвергнуть изменениям.

Если необходимо добавить дополнительный IP-адрес для соединения (т.н. alias), то необходимо поставить знак + перед адресом, например,

nmcli connection modify eth2 +ipv4.addresses 172.16.0.1/28

3.2.12 Настройка параметров маршрутизации для соединения

Под параметром маршрутизации в данном руководстве понимается:

– добавление шлюза по умолчанию;

– удаление шлюза по умолчанию;

– добавление маршрута для сети;

– удаление маршрута для сети.

Пример команды для добавления шлюза по умолчанию:

nmcli connection modify eth2 ipv4.gateway 10.11.1.25

В данном примере ключевой параметр *ipv4.gateway,* после которого задается IP-адрес шлюза по умолчанию.

Пример команды для добавления шлюза по умолчанию:

*nmcli connection modify eth2 ipv4.gateway **0.0.0.0***

В данном примере ключевой параметр - *ipv4.gateway,* после которого задается IP-адрес ***0.0.0.0.*** Такой IP-адрес является указанием для nmcli того, что шлюз по умолчанию необходимо удалить.

Пример команды для добавления маршрута к сети:

nmcli connection modify eth2 +ipv4.routes "192.168.0.0/24 10.111.1.11"

В данном примере ключевой параметр - *+ipv4.routes,* после которого, в кавычках, задается IP-адрес сети и через пробел шлюз, через который данная сеть доступна (т.н. next hop).

Таким образом, можно указывать множество маршрутов за один раз, просто перечисляя через пробел параметр и значение, например,

+ipv4.routes "192.168.0.0/24 10.111.1.11" +ipv4.routes "32.0.0.0/24 10.111.1.11" и т.д.

Пример команды для удаления маршрута к сети:

nmcli connection modify eth2 -ipv4.routes "192.168.0.0/24 10.111.1.11"

В данном примере ключевой параметр - *-ipv4.routes,* после которого в кавычках задается IP-адрес сети и через пробел шлюз, через который данная сеть доступна (т.н. next hop).

Так же, как и добавление, можно проводить и удаление множества маршрутов за один раз.

3.2.13 Добавление\изменение DNS серверов для соединения

Пример команды для добавления/изменения DNS серверов:

nmcli connection modify eth2 ipv4.dns 8.8.8.8

В данном примере ключевой параметр *ipv4.dns,* после которого задается IP-адрес DNS сервера для соединения. Возможно задавать несколько DNS серверов через запятую или при помощи параметра + *ipv4.dns.*

Удалить DNS серверы можно при помощи параметра *-ipv4.dns.*

3.2.14 Просмотр настроек соединения

Пример команды для просмотра настроек соединения:

nmcli connection show eth2

В данном примере ключевой параметр *show,* после которого задается имя соединения.

3.2.15 Применение соединения

Для применения соединения необходимо ввести команду: *nmcli connection up <имя>*.

3.2.16 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`.

3.2.17 Обновление

После установки обновления необходимо проверить контрольную сумму, как описано в подразделе 3.2.2. Результат проверки занести в формуляр.

3.2.18 Регламент обновления

3.2.18.1 Процедуры получения обновления

Для обновления АПК потребитель должен самостоятельно получить на предприятии-поставщике (изготовителе) АПК согласно договору на поставку и/или техническую поддержку образ обновления на CD/DVD-диске или USB-носителе 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 АПК должна производиться только по доверенному каналу.

3.2.18.2 Процедуры контроля целостности обновления

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

3.2.18.3 Типовые процедуры тестирования обновления

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

3.2.18.4 Процедуры установки и применения обновления

Для установки нового сертифицированного обновления АПК, 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*.

---

* «Специальными требованиями и рекомендациями по технической защите конфиденциальной информации (СТР-К)», утвержденного приказом Гостехкомиссии России от 30.08.2002 № 282;

3.2.18.5 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.

3.2.19 Автоматический контроль целостности

В АПК реализован автоматический запуск контроля целостности ПО «ЗАСТАВА-Офис».

По умолчанию контроль целостности запускается один раз в три часа (не с момента запуска АПК, а в час, кратный трем).

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

В случае отрицательного прохождения контроля целостности в системный журнал messages, записывается событие о нарушении целостности «Целостность СКЗИ нарушена».

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

В случае нарушения целостности АПК выключается.

3.2.20 Настройка параметров запуск автоматического контроля целостности

Для изменения параметров запуска автоматического контроля целостности необходимо:

1) авторизоваться с правами учетной записи root;

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 не с момента запуска АПК, а в час, кратный трем).

«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.

Автоматический контроль целостности запускается скриптом regular_check_control_sum.sh

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

3.2.21 Выключение

Для выключения АПК необходимо нажать кнопку питания  .

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 4).

Таблица 4 – 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 5).

Таблица 5 – 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	Количество промахов для исходящих пакетов при поиске

Параметр	Описание
hash table	фильтра в хэш-таблице
IKEv2	
IKE SAs created (failed) initiated/responded	Количество созданных (не созданных) инициированных/ отвеченных IKE SA в формате x(x)/x(x)
Resumed IKE SA initiated/responded	Количество возобновленных IKE SA инициированных/ отвеченных
IKE SA redirections received/sent	Количество перенаправлений IKE SA получено/послано
COOKIE requested/sent	Количество запрошенных/отправленных токенов COOKIE
Denied IKE SA requests	Количество отвергнутых запросов на создание IKE SA
IKE SA rekeys initiated/responded/collisions	Количество обновлений ключей IKE SA инициированных/отвеченных/коллизий в формате x/x/x
IPsec SA bundless created	Количество созданных IPsec SA
IPsec SA rekeys initiated/responded/collisions	Количество обновлений ключей IPsec SA инициированных/полученных/коллизий в формате x/x/x
Attempts to rekey non-existend IPsec SA by this host/by peer	Количество попыток обновления ключей несуществующей IPsec SA данным хостом/партнером
Temporary rekey failures on this host/on peer	Количество временных отказов в обновлении ключей данным хостом/партнером
INIT exchanges completed (with errors or failed) initiated/responded	Количество обменов INIT_IKE_SA успешных (с ошибками или неуспешных) инициировано/отвечено в формате x(x)/x(x)
RESUME exchanges completed (with errors or failed) initiated/responded	Количество обменов RESUME_IKE_SA успешных (с ошибками или неуспешных) инициировано/отвечено в формате x(x)/x(x)
AUTH exchanges completed (with errors or failed) initiated/responded	Количество успешных (с ошибками или неуспешных) обменов IKE_AUTH инициировано/отправлено в формате x(x)/x(x)
CHILD exchanges completed (with errors or failed) initiated/responded	Количество успешных (с ошибками или неуспешных) обменов CREATE_CHILD_SA инициировано/отправлено в формате x(x)/x(x)
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

Параметр	Описание
Unknown messages(bytes) recv	Количество неизвестных сообщений (байт) при получении сообщений
Create IKE SA: recv/sent messages (bytes)	Объем полученных/ отправленных сообщений в байтах при создании IKE SA
Create IKE SA: errors in recv/sent messages	Количество ошибок в полученных/ отправленных сообщениях при создании IKE SA
Delete IKE SA: recv/sent messages (bytes)	Объем полученных/ отправленных сообщений в байтах при удалении IKE SA
Delete IKE SA: errors in recv/sent messages	Количество ошибок в полученных/ отправленных сообщениях при удалении IKE SA
Update IKE SA: recv/sent messages (bytes)	Объем полученных/ отправленных сообщений в байтах при обновлении параметров IKE SA
Update IKE SA: errors in recv/sent messages	Количество ошибок в полученных/ отправленных сообщениях при обновлении параметров IKE SA
Request IKE SA list: recv/sent messages (bytes)	Объем полученных/ отправленных сообщений в байтах при запросе списка IKE SA
Request IKE SA list: errors in recv/sent messages	Количество ошибок в полученных/ отправленных сообщениях при запросе списка IKE SA
Get IKE SA list: recv/sent messages (bytes)	Объем полученных/ отправленных сообщений в байтах при запросе IKE SA
Get IKE SA list: errors in recv/sent messages	Количество ошибок в полученных/ отправленных сообщениях при запросе IKE SA
IKE-CFG sync: recv/sent messages (bytes)	Объем полученных/ отправленных сообщений в байтах при обновлении записей IKE-CFG
IKE-CFG sync: errors in recv/sent messages	Количество ошибок в полученных/ отправленных сообщениях при обновлении записей IKE-CFG
IKE-CFG del: recv/sent messages (bytes)	Объем полученных/ отправленных сообщений в байтах при удалении записей IKE-CFG
IKE-CFG del: errors in recv/sent messages	Количество ошибок в полученных/ отправленных сообщениях при удалении записей IKE-CFG
IKE-CFG clear: recv/sent messages (bytes)	Объем полученных/ отправленных сообщений в байтах при обновлении сбросе записей IKE-CFG
IKE-CFG clear: errors in recv/sent messages	Количество ошибок в полученных/ отправленных сообщениях при сбросе записей IKE-CFG
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

Параметр	Описание
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: 560000008093053836OCC5729B000000000080
          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 6 и Таблица 7),

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.

Параметры фильтрации протокола IKE SA приведены в таблице (см. Таблица 6).

Таблица 6 – 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

Параметр	Характеристика
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
spi	IKEv2 SPI
log_level	Уровень регистрации событий
features	Список поддерживаемых опций

Параметры фильтрации и описание типов операций фильтрации протокола IPsec SA приведены в таблицах (см. Таблица 7, Таблица 8).

Таблица 7 – Параметры фильтрации протокола IPsec SA

Тип	Характеристика
idstr	Идентификационный номер
ike_saref_str	Ссылка на IKE SA
ike_id_remote	IKE SA ID партнера
mode	Режим создания SA
role	Роль при создании SA
peer_id	ID партнёра
local_id	ID локальный
peer_ip	IP-адрес партнера
peer_port	UDP-порт партнера
local_ip	IP-адрес локальный
local_port	UDP-порт на локальном компьютере
Ike_cfg_server	IKE CFG адрес, выданный клиенту
dhgroup	DH группа
filter	Фильтр
rule	Правило
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)

Тип	Характеристика
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 8 – Описание типов операций фильтрации

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

Команда	Характеристика
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 -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, за исключением 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 11).

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 9),

`operation` – операция для произведения сравнения по выбранному полю с эталоном (см. Таблица 10),

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

Таблица 9 – Параметры фильтрации протокола

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

Таблица 10 – 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

Команда	Характеристика
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 11 – 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 12).

Таблица 12 – 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 Algproxy

Команда `vpnmonitor -algproxy` позволяет просмотреть информацию о прокси-серверах, установленных на данном ПО «ЗАСТАВА-Офис».

4.1.2.10 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 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.


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: 6.4.21617
Product release: 6.4
Build date: 2021/09/20 20:01
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 могут требовать ввода пароля администратора при удаленном подключении Администратора АПК. Для этого перед командой следует указать опцию –login admin <username> <password>. Пример:

```
vpnconfig -login admin admin 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 13).

Таблица 13 – 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

В ПО «ЗАСТАВА Офис» можно регистрировать два типа X.509 сертификатов: 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 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» 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 (необходимо выполнить команду: `vpnconfig -login token <token_id> <pin> save`).

Если сертификат УЦ был получен через незащищённый канал (например, по электронной почте) и необходимо сохранить его как «Доверяемый», необходимо 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 необходимо 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 устройстве.

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:

Password OK.

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»

4.2.2.5.1.1 Системная ЛПБ

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

Для настройки системной политики необходимо:

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

7) 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 ПК «ЗАСТАВА-Управление»;

– `<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.

8) 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]`.

4.2.2.5.1.2 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.

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 настройки 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 14).

Таблица 14 – Параметры протокола IKE

Идентификатор 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

Идентификатор параметра	Параметр	Расшифровка
		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 exchanges	Максимальное количество параллельных обменов, которые данный хост готов принимать в качестве ответчика в рамках одной IKE SA (1 – 16, по умолчанию – 4). Для IKEv2 этот же параметр (но заданный у партнера) будет определять максимальное количество параллельных обменов, которые могут быть инициированы данным хостом в рамках одной IKE SA.
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)

Идентификатор параметра	Параметр	Расшифровка
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 настройках ПО (RRI table id), в противном случае те маршруты, которые прописываются в таблицу с номером `<table id>`, система не распознает. Пример команды: `ip rule add from all lookup 111`

Идентификатор параметра	Параметр	Расшифровка
		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 15).

Таблица 15 – 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, 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.

Числовое значение	Режим работы обработки CRL
	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 16) (под Агентом понимается ПО «ЗАСТАВА-Офис»).

Таблица 16 – 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 партнерами.
130 (Все методы (Принудительно))	Режим "Все методы с принудительной инкапсуляцией. Полностью аналогичен режиму Все методы, за тем исключением, что инкапсуляция

Числовое значение	Политика
	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:

Provider

Name: Builtin Trusted Module

Path: softpkcs11-trusted.dll

Cryptoki Version: 2.20

Library Version: 2.32

Manufacturer: ELVIS-PLUS

Description: Trusted Certificates

Tokens: 1

Token: Trusted Certificates token

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 17).

Таблица 17 – Действия, поддерживаемые утилитой `plg_ctl`

Ключ	Название	Описание
`-e`	Enable	Активировать криптобиблиотеку или криптоалгоритм
`-d`	Disable	Деактивировать криптобиблиотеку или криптоалгоритм

Ключ	Название	Описание
-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

4.2.3.1.2Опции

Утилита plg_ctl поддерживает следующие опции, представленные в таблице (см. Таблица 18).

Таблица 18 – 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 19).

Таблица 19 – 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 «КриптоПро CSP» 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 следующие 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 «КриптоПро CSP», 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 с ПК «ЗАСТАВА-Управление»);
- 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 папку /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 необходимо:

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 НЕШТАТНЫЕ СИТУАЦИИ

5.1 Некорректная работа АПК после обновления ОС

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

Для возврата к эталону необходимо предварительно запросить у производителя пароль доступа к эталону.

Возврат к эталону выполняется следующим образом:

1) Включить АПК, нажав кнопку питания , дождаться появления меню выбора вариантов загрузки «Boot menu for ZASTAVA-150».
2) Выбрать пункт меню «Factory Reset» и нажать клавишу <Enter>.
3) В появившемся окне «Password required» ввести полученный у производителя пароль доступа к эталону. Нажать клавишу <Enter>.
4) На экране появится сообщение о проверке контрольной суммы заводского образа ОС. Дождаться окончания проверки.
5) По окончании проверки в случае совпадения контрольных сумм будет загружена эталонная программная составляющая, АПК 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 Изготовителю (Поставщику).

5.2 Обнаружение несанкционированного вскрытия корпуса (срабатывания датчика вскрытия корпуса)

В случае обнаружения срабатывания датчика вскрытия корпуса необходимо:

- отключить АПК от каналов передачи данных;
- выполнить перезагрузку и сверить контрольные суммы с зафиксированными в формуляре (см. подраздел 3.2.2);
- назначить ответственного за расследование инцидента. Всю ключевую информацию считать скомпрометированной;
- если в результате расследования выяснилось, что действия нарушителя не несли злого умысла, то необходимо выполнить откат в эталон (см. подраздел 5.1) и выпустить новую ключевую информацию для VPN (см. подраздел 3.2.6);

– если в результате расследования выяснилось, что действия нарушителя несли злой умысел, то необходимо отправить АПК Изготовителю (Поставщику) на восстановление.

5.3 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 5.1) и выпустить новую ключевую информацию для VPN (см. подраздел 3.2.6);
– в случае если действия, которые привели к инциденту, являются угрозой безопасности, то необходимо отправить АПК Изготовителю (Поставщику) на восстановление.

5.4 Автоматическое отключение АПК

Автоматическое отключение АПК происходит в следующих случаях

– в случае неуспешного прохождения автоматического контроля целостности (см. подраздел 3.2.19). В случае автоматического отключения необходимо включить АПК заново (см. подраздел 3.2.1). Если после включения обнаружится нарушение целостности образа АПК необходимо выполнить действия, описанные в подразделе 5.3;
– в случае неуспешного прохождения контроля целостности ПО СКЗИ «ESMART Token ГОСТ», который запускается при каждом старте ОС АПК и при предъявлении ключевого носителя.

5.5 Компрометация ключей аутентификации

В случае компрометации ключей аутентификации необходимо:

– назначить ответственного за расследование инцидента;
– в случае компрометации ключей для VPN необходимо выпустить новую ключевую информацию для VPN (см. подраздел 3.2.6);
– в случае компрометации ключей для входа в ОС необходимо отправить АПК Изготовителю (Поставщику) на восстановление.

6 ВОЗМОЖНЫЕ НЕИСПРАВНОСТИ И СПОСОБЫ ИХ УСТРАНЕНИЯ

Возможные неисправности и способы их устранения приведены в таблице (см. Таблица 20).

Таблица 20 – Возможные неисправности и способы их устранения

Описание	Способы устранения
Не работает мышь	Последовательно выполнить действия до устранения неисправности: 1. Проверить подключение мыши к USB-порту системного блока. 2. Проверить кабель на наличие повреждений, заломов, разрезов. 3. Обратить внимание на наличие световой индикации сенсора мыши (нижняя сторона, сенсор должен излучать красный свет). 4. Проверить сенсор мыши на наличие инородных предметов (пыль, грязь, крошки и пр.); при наличии загрязнения - извлечь (продуть) и проверить работу. 5. При наличии повреждений кабеля, отсутствии световой индикации или невозможности прочистить сенсор обратиться в службу технической поддержки.
Не работает клавиатура	Последовательно выполнить действия до устранения неисправности: 1. Проверить подключение клавиатуры к USB-порту системного блока. 2. Проверить кабель на наличие повреждений, заломов, разрезов. 3. Проверить наличие световой индикации на клавиатуре в верхнем правом углу, нажав несколько раз клавишу <Num Lock>. 4. При наличии повреждений кабеля или отсутствии световой индикации обратиться в службу технической поддержки.
На экране входа в систему «Не удалось выполнить вход»	Последовательно выполнить действия до устранения неисправности: 1. Проверить правильность выбранной учётной записи (admin или user). 2. Проверить наличие смарт-карты в считывателе карт. 3. Убедиться в том, что смарт-карта вставлена до конца в слот. 4. Если после выполнения действий вы не получили приглашения к вводу PIN-кода - обратитесь в службу технической поддержки.
Сбой настроек BIOS	Проверить и, при необходимости, изменить настройки BIOS (см. п. 3.1.2).
Ключевой носитель утерян	Сообщить в УЦ о факте утери.

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
CRL	–	Certificate Revocation List – см. COC
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)
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)
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
АПК	–	Аппаратно-программный комплекс
ГОСТ	–	Государственный стандарт

ГПБ	–	Глобальная политика безопасности
ЛПБ	–	Локальная политика безопасности
ОС	–	Операционная система
ПО	–	Программное обеспечение
ПК	–	Программный комплекс
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

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

Подп. и дата

Инв. № дубл.

Взам. инв. №

Подп. и дата

Инв. № подл. 7434

Изм.	Лист	№ докум.	Подп.	Дата	МКЕЮ.00630.ИЗ	Лист
						81