УТВЕРЖДЕН

МКЕЮ.00627-01 32 01-ЛУ

«Программный комплекс защиты корпоративных вычислительных ресурсов на сетевом уровне с использованием технологий VPN и распределенного межсетевого экранирования на основе интернет-протоколов семейства IPsec/IKE «VPN/FW «ЗАСТАВА-Офис», версия 6 КС1»

(«VPN/FW «ЗАСТАВА-Офис», версия 6 КС1»)

Руководство системного программиста

МКЕЮ.00627-01 32 01

Листов 166

Инв.№ подл.	Подп. и дата	Взам. инв. №	Инв.№ дубл.	Подп. и дата
7410				

2021

Содержание

1. Введение

1.1. О данном документе

Этот документ описывает функциональные возможности, особенности конфигурирования и применения МКЕЮ.00627-01 «Программный комплекс защиты корпоративных вычислительных ресурсов на сетевом уровне с использованием технологий VPN и распределенного межсетевого экранирования на основе интернет-протоколов семейства IPsec/IKE «VPN/FW «ЗАСТАВА-Офис», версия 6 КС1» (далее – «VPN/FW «ЗАСТАВА-Офис», версия 6 КС1», *ЗАСТАВА-Офис* или *Агент*).

1.1.1. Типографские соглашения

Курсив	*Курсив* используется, чтобы выделить названия компонентов *ЗАСТАВА.* Он используются, чтобы указать строку данных, которая будет введена в поле. Курсив также может использоваться для акцента.
«Кавычки»	Текст, заключенный в кавычки, используется, чтобы указать выбор из списка в данном поле (то есть выбор из предопределенного списка в окне), названия окон программы, всплывающих окон, выбора из меню, а также параметров и атрибутов объектов.
МАЛЫЕ ПРОПИСНЫЕ	Малые прописные используются для названий документов (стандарты, монографии, бумаги, технические и пользовательские документы по программным продуктам, интерактивные справочные системы, и т.д.), а также для ссылок на разделы документов.
`Непропорциональный`	Непропорциональный шрифт используется для ссылок на системные папки и каталоги, последовательности пунктов меню, файлы и пути, и команды в интерфейсе командной строки.
<Угловые скобки>	Угловые скобки используются в именах клавиш на клавиатуре компьютера, а также в описаниях параметров.

1.1.2. Как использовать данный документ

Для того чтобы узнать, как инсталлировать и подготовить к работе *ЗАСТАВА-Офис* и ознакомиться с работой *ЗАСТАВА-Офис*, обратитесь к разделу 2 Подготовка к использованию *ЗАСТАВА-Офис*.

Для того чтобы узнать, как осуществлять навигацию по структуре окон *ЗАСТАВА-Офис,* обратитесь к разделу 3 Работа в графическом интерфейсе *ЗАСТАВА-Офис*.

За информацией о том, как регистрируются сертификаты и ключи в *ЗАСТАВА-Офис,* обратитесь к подразделу 3.4 Окно «Сертификаты и ключи». В этом подразделе Вы также найдете информацию относительно того, как создать Запрос Регистрации Сертификата (ЗРС) и как импортировать список отозванных сертификатов (СОС) в *ЗАСТАВА-Офис*.

Чтобы узнать, как конфигурировать локальные установки *ЗАСТАВА-Офис,* обратитесь к разделу 3 Работа в графическом интерфейсе *ЗАСТАВА-Офис*.

За информацией по использованию токенов для хранения конфиденциальных данных обратитесь к подразделу 3.6 Окно «Токены».

Для того чтобы узнать, как конфигурировать *ЗАСТАВА-Офис*, используя интерфейс командной строки, и просмотреть список доступных команд, обратитесь к разделу 5 Интерфейс командной строки.

Описание работы с модулем управления криптобиблиотеками приведено в п. 3.1.7 Работа с плагинами.

1.2. О компоненте «*ЗАСТАВА-Офис*»

1.2.1. Назначение

Компонент *ЗАСТАВА-Офис* может поставляться в варианте межсетевого экрана (МЭ), обеспечивающего контроль и фильтрацию проходящих через него сетевых пакетов или варианте VPN (СКЗИ + МЭ), обеспечивающего, как контроль и фильтрацию сетевого трафика, так и взаимную криптографическую защиту абонентов при установлении соединения, шифрование и контроль целостности IP-пакетов в корпоративной информационной системе.

В варианте VPN (СКЗИ + МЭ) *ЗАСТАВА-Офис*, версия 6 предназначен для работы в качестве шлюза, осуществляющего защиту и фильтрацию трафика между внутренней (защищаемой) сетью и внешними локальными сетями (ЛВС) или глобальными сетями (WANs). Наиболее распространены следующие два сценария использования компонента *ЗАСТАВА-Офис* (могут применяться совместно):

- "Site-to-Site" - организация защищенного соединения (VPN-туннеля) между двумя и более удаленными офисами одной компании, связанными через потенциально опасную сеть (например, Интернет). В этом случае в каждом офисе компании устанавливается *ЗАСТАВА-Офис*.
- "Host-to-Site" - организация VPN-туннеля между мобильными пользователями в сети Интернет и корпоративным офисом. В этом случае на компьютерах

пользователей должен быть установлен МКЕЮ.00626-01 «Программный комплекс защиты корпоративных вычислительных ресурсов на сетевом уровне с использованием технологий VPN и распределенного межсетевого экранирования на основе интернет-протоколов семейства IPsec/IKE «VPN/FW «ЗАСТАВА-Клиент», версия 6 КС1» («VPN/FW «ЗАСТАВА-Клиент», версия 6 КС1») (далее – *ЗАСТАВА-Клиент*), а в корпоративном офисе – соответственно, *ЗАСТАВА-Офис*.

Обеспечение контроля и фильтрации сетевого трафика, а также взаимной криптографической защиты абонентов при установлении соединения, шифрования и контроля целостности передаваемых данных производится в соответствии с загружаемой в *ЗАСТАВА-Офис* Локальной Политикой Безопасности (ЛПБ), созданной с помощью МКЕЮ.00631-01 «Программный комплекс «VPN/FW ЗАСТАВА-Управление», версия 6 КС3» («VPN/FW ЗАСТАВА-Управление», версия 6 КС3») (далее – *ЗАСТАВА-Управление*).

В состав ПК в варианте VPN (СКЗИ + МЭ) входит СКЗИ ЖТЯИ.00087-01 «КриптоПро CSP», версия 4.0КС1 производства ООО «КРИПТО-ПРО» (г. Москва).

1.2.2. Область применения

Компонент *ЗАСТАВА-Офис* предназначен для применения (в роли *шлюза*) в локальных, корпоративных и глобальных сетях, где в качестве протокола сетевого уровня используется протокол IP.

Компонент *ЗАСТАВА-Офис* предназначен для работы на компьютерах под управлением операционных систем (ОС) ALT Linux 6/7 платформы ia32, x64.

Используемая ОС должна иметь установленную и активизированную поддержку сети и стека TCP/IP.

Компьютер, на котором устанавливается компонент *ЗАСТАВА-Офис*, должен иметь два и более сетевых интерфейса с запущенной службой «Маршрутизация и удаленный доступ». Трафик обрабатывается на интерфейсах, указанных при инсталляции.

1.2.3. Характеристики

1.2.3.1. Защита трафика и фильтрация

Компонент *ЗАСТАВА-Офис* предоставляет следующие возможности по защите и фильтрации трафика:

– Защита трафика на сетевом уровне при помощи протоколов IPsec ESP;

- Обеспечение двусторонней криптографической аутентификации при установлении соединений с другими хостами защищенной корпоративной сети на базе протоколов IKEv2, контроля целостности данных и конфиденциальности информации путем ее шифрования;
- Пакетная фильтрация трафика, основанная на использовании полей заголовков транспортных и сетевых протоколов:
  - На сетевом уровне - через IPv4-адрес и/или поле заголовка IP-протокола;
  - На транспортном уровне - по направлению TCP-соединения и по протоколам сервисов (TCP/UDP-портам);

— Расширенная фильтрация пакетов (применение конечных автоматов для большого числа сетевых протоколов);

— Осуществление определенной политики взаимодействия (имитозащита и/или шифрование трафика) для каждого защищенного соединения; параметры трафика определяются сетевыми адресами, портами и/или идентификационной информацией конечного отправителя и получателя;

— Возможность применения различных степеней защиты трафика;

— Сокрытие топологии защищаемой сети (поддержка режима туннелирование трафика);

— Возможность использования конфигурируемых туннельных адресов для IPsec-протоколов;

— Поддержка «горячего» резервирования Шлюзов Безопасности (компьютеров с *ЗАСТАВА-Офис* или маршрутизаторов Cisco) так, что один из этих шлюзов является активным, а остальные шлюзы будут использованы как резервные при выходе из строя основного активного шлюза.

1.2.3.2. Дополнительные возможности

В *ЗАСТАВА-Офис* предусмотрены:

- Поддержка работы при наличии в сети промежуточных устройств с трансляцией сетевых адресов (NAT) путем инкапсуляции IPsec в UDP.
- Выполнение функций NAT-устройства (трансляция сетевых адресов NAT/PAT в соответствии с правилами в ЛПБ);
- При дополнительной инсталляции соответствующего модуля поддерживается фильтрация по шаблонам (Application Proxy) для следующих прикладных протоколов: Telnet, FTP, SMTP, HTTP, SOCKS;

– Управление качеством обслуживания (QoS): осуществляется путем модификации поля DiffServ при туннелировании IP-пакетов. Данная функциональность полезна для протоколов, чувствительных к задержкам (VoIP и т. п.).

1.2.3.3. Сертификаты и обмен ключами

Для установления защищенных соединений с использованием протокола IKE в *Агентах* (*ЗАСТАВА-Клиент*, *ЗАСТАВА-Офис* - обычно употребляется собирательный термин *Агенты*) используются X.509 V3 сертификаты в соответствии с RFC5280.

Хранение и защита контейнеров ключей персональных сертификатов осуществляется СКЗИ «КриптоПро CSP» версии 3.6.1, «КриптоПро CSP» версии 3.9, «КриптоПро CSP» версии 4.0.

В *ЗАСТАВА-Офис* предусмотрены использование СОС и поддержка получения сертификатов и СОС через протокол LDAP и HTTP.

1.2.3.4. Инсталляция и конфигурирование

ЗАСТАВА-Офис может быть сконфигурирован удаленно, получив ЛПБ от *ЗАСТАВА-Управление* - по сети через протокол управления политикой (Policy Management Protocol).

Для доступа к компьютеру посредством протокола Telnet, необходимо сделать следующие шаги при инсталляции *ЗАСТАВА-Офис*:

1) Включить автоматический запуск сервиса Telnet (использование логинов по умолчанию и пустых паролей является потенциальной угрозой в этом случае).

2) Отключить NTLM-аутентификацию, включенную по умолчанию. Для этого возможны два варианта:

— запустить tlntadmn.exe, используя интерактивное меню установить NTLM в значение «0» и перезапустить сервис;

— исправить соответствующие настройки в реестре и перезапустить сервис.

1.2.3.5. Регистрация событий и статистика

Регистрация событий и статистика обеспечивается:

– Возможностью ведения локального журнала регистрации событий с централизованной или локальной настройкой уровня детализации;

– Возможностью ведения удаленного журнала регистрации событий (syslog);

– Отправка SNMP-трапов (сообщений) на NMS-систему.

1.2.3.6. Стандарты и совместимость с другими продуктами

ЗАСТАВА-Офис обеспечивает совместимость с другими продуктами и поддержку Стандартов благодаря:

- Поддержке работы с сертификатами открытых ключей и персональных закрытых ключей через интерфейс внешних криптопровайдеров поддерживающих интерфейс PKCS #11 версии 2.10 и выше;
- Поддержке персональных сертификатов и сертификатов УЦ в формате X509v3;
- Поддержке возможности работы с СОС в формате CRLv2;
- Поддержке режимов аутентификации IKE посредством предварительно распределенного ключа (preshared key);
- Поддержке протоколов семейства IPsec и IKE (версий 1 и 2). Протоколы описаны подробно в нижеприведённых документах:

Общие стандарты группы IPsec

RFC 4301	Security Architecture for the Internet Protocol	http://www.ietf.org/rfc/rfc4301.txt

IPsec: протоколы ESP

RFC 4303	IP Encapsulating Security Payload (ESP)	http://www.ietf.org/rfc/rfc4303.txt

IPsec: обмен ключами

RFC 2408	Internet Security Association and Key Management Protocol (ISAKMP)	http://www.ietf.org/rfc/rfc2408.txt
RFC 2409	Internet Key Exchange (IKE)	http://www.ietf.org/rfc/rfc2409.txt
RFC 5996	Internet Key Exchange Protocol Version 2 (IKEv2)	http://www.ietf.org/rfc/rfc5996.txt
RFC 6290	A Quick Crash Detection Method for the Internet Key Exchange Protocol (IKE)	http://www.ietf.org/rfc/rfc6290.txt
RFC 6311	Protocol Support for High Availability of IKEv2/IPsec	http://www.ietf.org/rfc/rfc6311.txt
RFC 5723	Internet Key Exchange Protocol Version 2 (IKEv2) Session Resumption	http://www.ietf.org/rfc/rfc5723.txt

RFC 5685	Redirect Mechanism for the Internet Key Exchange Protocol Version 2 (IKEv2)	http://www.ietf.org/rfc/rfc5685.txt

PKI

RFC 5280	Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile	http://www.ietf.org/rfc/rfc2459.txt

Другие протоколы

RFC 0792	Internet Control Message Protocol (ICMP)	http://www.ietf.org/rfc/rfc792.txt
RFC 1777	Lightweight Directory Access Protocol (LDAP)	http://www.ietf.org/rfc/rfc1777.txt
RFC 1155	Structure and Identification of Management Information for TCP/IP-based Internets	http://www.ietf.org/rfc/rfc1155.txt
RFC 1157	Simple Network Management Protocol (SNMP)	http://www.ietf.org/rfc/rfc1157.txt
RFC 2138	Remote Authentication Dial-in User Service (RADIUS)	http://www.ietf.org/rfc/rfc2138.txt
RFC 4357	Additional Cryptographic Algorithms for Use with GOST 28147-89, GOST R 34.10-94, GOST R 34.10-2001, and GOST R 34.11-94 Algorithms	http://www.ietf.org/rfc/rfc4375.txt
RFC 4490	Using the GOST 28147-89, GOST R 34.11-94, GOST R 34.10-94, and GOST R 34.10-2001 Algorithms with Cryptographic Message Syntax (CMS)	http://www.ietf.org/rfc/rfc4490.txt
RFC 4491	Using the GOST R 34.10-94, GOST R 34.10-2001, and GOST R 34.11-94 Algorithms with the Internet X.509 Public Key Infrastructure Certificate and CRL Profile	http://www.ietf.org/rfc/rfc4491.txt

Термины и определения

RFC 2828	Internet Security Glossary	http://www.ietf.org/rfc/rfc2828.txt

1.2.4. Минимальные системные требования

Аппаратное обеспечение компьютера, на котором устанавливается компонент *ЗАСТАВА-Офис*, должно удовлетворять следующим минимальным требованиям:

- Процессор, эквивалентный Intel Pentium 4, с частотой 1400 МГц;
- Оперативная память – от 512 Мбайт;
- 50 Мбайт свободного дискового пространства;
- Разрешение монитора не менее 1024×768 пикселей.

На компьютере, на который устанавливается компонент *ЗАСТАВА-Офис*, должна быть уставлена одна из следующих ОС:

- ОС ALT Linux 6/7 платформы ia32, x64.

2. Подготовка к использованию *ЗАСТАВА-Офис*

Перед началом установки убедитесь в том, что Вы устанавливаете соответствующую версию *ЗАСТАВА-Офис* в соответствующей версии ОС.

Перед установкой *ЗАСТАВА-Офис* необходимо инсталлировать на компьютер СКЗИ «КриптоПро CSP» версии 3.6.1, «КриптоПро CSP» версии 3.9 или «КриптоПро CSP» версии 4.0, в зависимости от комплектации и исполнения *ПК «VPN/FW «ЗАСТАВА», версия 6*.

	Чтобы инсталлировать и деинсталлировать *ЗАСТАВА-Офис* Вы должны иметь привилегии администратора ОС
	Удостоверьтесь в том, что на компьютере правильно установлены дата, время и настройки часового пояса. Необходимо правильно определить эти параметры, иначе может оказаться, что срок действия сертификатов истек, и Вы не можете установить *ЗАСТАВА-Офис*.
	Длина пароля администратора ОС, на которой устанавливается *ЗАСТАВА-Офис*, должна быть не меньше шести буквенно-цифровых символов.
	СКЗИ «КриптоПро CSP» должно быть установлено с поддержкой уровня ядра, для этого при установке приложения необходимо выбрать тип установки Custom и установить модуль Kernel mode CSP.

2.1. ОС Семейства ALT Linux

Инсталляционные пакеты *ЗАСТАВА-Офис* для ОС ALT Linux 6 представляются в виде файлов с расширением *.rpm*. Предоставляемые инсталляционные пакеты собираются под все ядра версий ОС LINUX. Список поддерживаемых платформ указан в п. 1.2.4. Предоставляемые инсталляционные пакеты собираются под ядра:

- 2.6.32-el-smp-alt31.M60C.1,
- 2.6.32-ovz-el-alt40.M60P.2,
- 3.0.26-alt0.M60P.1.

Для сборки инсталляционного пакета под отличные ядра см. п. 2.1.4.

2.1.1. Инсталляция *ЗАСТАВА-Офис*

Инсталляция *ЗАСТАВА-Офис* производится на компьютер, который не содержит среду компиляции и сборки и работает на той версией ядра ОС ALT Linux 6, для которой был получен инсталляционный пакет. Инсталляция запускается командой:

`rpm -i` <путь к инсталляционному пакету>.

2.1.2. Обновление *ЗАСТАВА-Офис*

Обновление *ЗАСТАВА-Офис* запускается командой:

`rpm –U` <путь к инсталляционному пакету>

Более подробное описание обновления *ЗАСТАВА-Офис* см. в п. **Ошибка! Источник ссылки не найден.**.

2.1.3. Деинсталляция *ЗАСТАВА-Офис*

Деинсталляция *ЗАСТАВА- Офис* запускается командой:

`rpm –e` <путь к инсталляционному пакету>.

2.1.4. Руководство по сборке инсталляционного пакета

Для сборки инсталляционного пакета драйвера `vpnpcap` и криптоплагина из исходных кодов используется среда сборки RPM. Исходные коды драйвера `vpnpcap` и криптоплагина предоставляются в виде файла с расширением src.rpm: ZASTAVAoffice-drv-<version>.src.rpm. После установки с компакт-диска ОС ALT Linux 6 необходимо настроить соответствующие APT-репозитории, обновить список доступных из них пакетов, и установить пакеты `rpm-build` и `kernel-headers-modules` (устанавливается пакет `kernel-headers-modules` той версии ядра ОС ALT Linux 6, для которой собирается инсталляционный пакет драйвера `vpnpcap` и криптоплагинов). Также необходимо установить собранный пакет драйвера СКЗИ «КриптоПро CSP» в зависимости от комплектации и исполнения *ПК «VPN/FW «ЗАСТАВА»* и добавить в таблицу экспортируемых символов ядра ОС, символы экспортируемые из модуля ядра провайдера CryptoPro CSP (`drvcsp.ko`), например, так:

```
cd /opt/cprocsp/src/drtcsp; bash ./gensyms.sh
```

Сборка инсталляционного пакета драйвера `vpnpcap` и криптоплагина запускается командой:

```
rpmbuild --define "autostart_mode " --define "cpro_symbols " --define "kernel_release " --define "pcap_smp " --define “cpro_release “ ZASTAVAoffice-drv-<version>.src.rpm
```

Параметры сборки:

`autostart_mode` – управляет запуском после инсталляции, принимаемые значения:

1 – не устанавливать криптоплагин и не загружать драйвер vpnpcap (например, для установки под chroot),

2 – устанавливать принудительно криптоплагин и загружать драйвер vpnpcap.

Без параметра autostart_mode автоматически определяется необходимость установки криптоплагина и запуска драйвера vpnpcap.

cpro_symbols – указывает полный путь к символам экспортируемым из модуля ядра провайдера CryptoPro CSP (drvcsp.ko), например, /opt/cprocsp/src/drtcsp/Module.symvers.

kernel_release – указывает версию ядра ОС ALT Linux 6, для которой собирается инсталляционный пакет драйвера vpnpcap и криптоплагина.

pcap_smp – указывает собирать драйвер vpnpcap с тредами или без них, принимаемые значения:

0 – без тредов,

1 – с тредами.

При любом другом значении параметра pcap_smp или его отсутствии автоматически определяется необходимость сборки драйвера vpnpcap с тредами или без них. Если ядро собрано с поддержкой SMP – то драйвер vpnpcap будет с тредами, если без поддержки SMP – то драйвер vpnpcap будет без тредов.

cpro_release - указывает суффикс драйвера cp_plg_cpro в зависимости от версии CryptoPro CSP, принимаемые значения:

- 36r2 для CryptoPro CSP 3.6 R2
- 36r3 для CryptoPro CSP 3.6 R3
- 40 для для CryptoPro CSP 3.6 R4, 3.9, 4.0

Если значение cpro_release не задано, то по умолчанию, cpro_release равен 40.

Пример сборки драйвера vpnpcap и криптоплагина:

```
rpmbuild --rebuild --define "autostart_mode 2" --define "cpro_symbols /opt/cprocsp/src/drtcsp/Module.symvers" --define "kernel_release 2.6.32-ovz-smp-alt8" --define "pcap_smp 0" --define “cpro_release 36r3” ZASTAVAoffice-drv-<version>.src.rpm
```

В результате будет собран драйвер vpnpcap и криптоплагин без тредов с функцией принудительной установки криптоплагина и загрузки драйвера vpnpcap для ядра 2.6.32-ovz-smp-alt8 ОС ALT Linux 6 и CryptoPro CSP 3.6 R3.

Инсталляция собранного пакета запускается командой:

```
rpm –i <путь к собранному пакету>
```

2.1.5. Интеграция *ЗАСТАВА-Офис* с системным SNMP-сервисом

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

– Определить путь к файлу snmpd.conf. Если файла нет, то необходимо его создать (обратитесь к документации по snmpd).

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 "

Также для корректной работы необходимо установить snmp-браузер. В зависимости от производителя настройки snmpd могут различаться (обратитесь к документации по snmpd).

2.2. Восстановление *ЗАСТАВА-Офис*

Проверка целостности программного обеспечения (ПО) осуществляется путем сравнения значения контрольной суммы, которое записано в файле filelist.hash, для данного файла, с текущим значением. При несовпадении значений выдается соответствующее предупреждение. Расчет контрольной суммы производится по алгоритму.

Проверка контрольных сумм производится в процессе загрузки службы vpndmn, при проверке целостности ПО производится регистрация событий в системном журнале и в файле vpn_init.log.

При нарушении целостности служба *ЗАСТАВА-Офис* не запустится, что свидетельствует о нарушении целостности ПО.

Проверить контрольные суммы можно, запустив в командном интерпретаторе cmd.exe утилиту `icv_checker`, находящуюся в главной директории *ЗАСТАВА-Офис*. Для проверки целостности ПО необходимо выполнить команду `icv_checker filelist.hash`, где: filelist.hash - файл с текущим значением контрольных сумм.

Для восстановления работоспособности *ЗАСТАВА-Офис* необходимо произвести деинсталляцию с последующей инсталляцией *ЗАСТАВА-Офис*.

Более подробная информация о применении утилит icv_checker и icv_writer находится в разделе 5.5 Утилиты icv_writer и icv_checker.

2.3. Запуск графического интерфейса *ЗАСТАВА*-Офис

Системные модули *ЗАСТАВА-Офис* запускаются автоматически при загрузке ОС и работают постоянно в фоновом режиме.

1) При необходимости, Вы можете открыть графический интерфейс *ЗАСТАВА-Офис* следующим образом:

   – В ОС ALT Linux выполнить команду `/opt/ZASTAVAoffice/bin/vpnagent`

Для успешного отображения графического модуля компонента *ЗАСТАВА-Офис* в ОС ALT Linux, необходимо использовать ОС с установленным графическим окружением.

2) Появится *Панель управления*, с помощью которой Вы можете устанавливать параметры *ЗАСТАВА-Офис*.

Подробности о *Панели управления* и её особенностях, см. в подразделе 3.1.

2.4. Конфигурирование *ЗАСТАВА-Офис*

Возможности *ЗАСТАВА-Офис* при конфигурировании:

— *ЗАСТАВА-Офис* может быть сконфигурирован после установки с помощью Графического интерфейса (GUI – Graphical User Interface) *ЗАСТАВА-Офис*, как описано в разделе 3 или с помощью командной строки, как описано в разделе 5.

2.5. Быстрое включение *ЗАСТАВА-Офис* в работу с помощью графического интерфейса

Для быстрого запуска *ЗАСТАВА-Офис* в работу необходимо выполнить следующее:

— Получить и подключить носитель с персональным сертификатом;

— Зарегистрировать цифровой сертификат формата X.509, выпущенный Удостоверяющим центром (УЦ – издатель персонального сертификата), или всю доверенную цепочку сертификатов, если персональный сертификат издан Подчиненным УЦ;

— Согласовать идентификаторы интерфейсов с идентификаторами в ЦУП;

— Создать и активировать конфигурацию для подключения к ЦУП.

К этому моменту Ваш *Агент* должен быть создан в ЦУП как security объект с оттранслированной и активированной ЛПБ. Вы должны иметь носитель с контейнером Вашего персонального цифрового сертификата, в котором должен быть содержаться Ваш открытый ключ и файлы цифровых сертификатов. СКЗИ «КриптоПро CSP» в зависимости от комплектации и исполнения *ПК «VPN/FW «ЗАСТАВА», версия 6*, установленное на Вашем компьютере, должно обеспечивать поддержку носителя с Вашим персональным сертификатом.

Порядок быстрого включения в работу *ЗАСТАВА-Офис* следующий:

1) Подключить носитель с контейнером к компьютеру. Убедиться в том, что Ваш сертификат появился в *ЗАСТАВА-Офис*. Для этого необходимо открыть окно «Токены» и убедиться в том, что в дереве Builtin CryptoPro Module появился Ваш носитель (см. Рисунок 1).

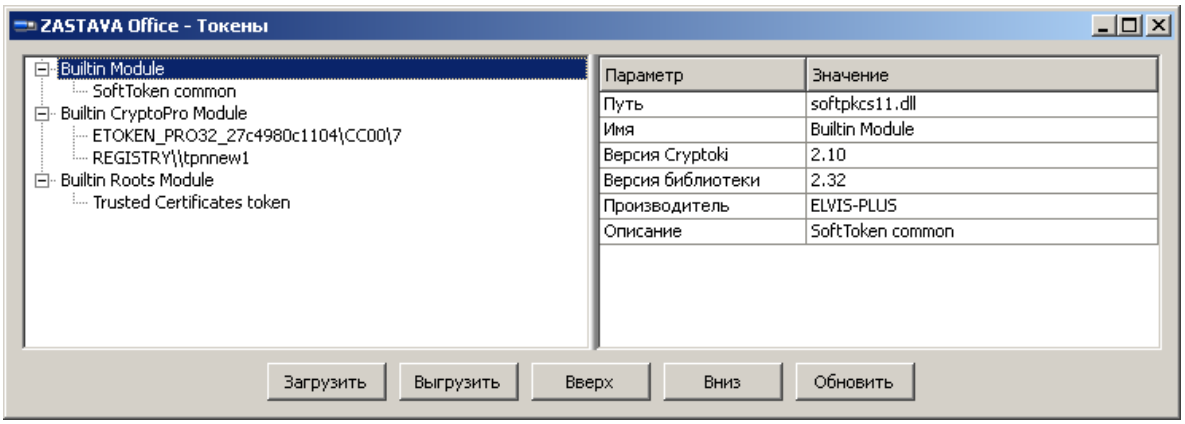

Рисунок 1 – Подключение носителя с сертификатом и ключами

Одновременно в окне «Сертификаты и ключи» появился Ваш персональный сертификат во вкладке «Персональные» (см. Рисунок 2).

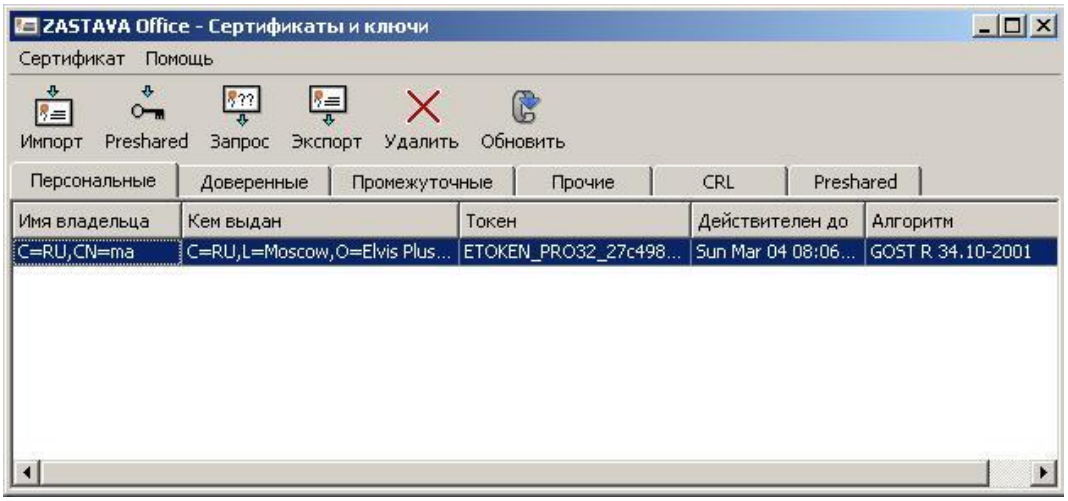

Рисунок 2 – Автоматическое добавление сертификата из носителя

2) Зарегистрировать сертификаты УЦ:

а) Открыть окно «Сертификаты и ключи» и нажать кнопку «Импорт».

б) В открывшемся окне навигатора открыть файл с корневым сертификатом УЦ. Корневой сертификат УЦ должен быть зарегистрирован как «Доверенный» на устройстве Trusted certificate token (см. Рисунок 3).

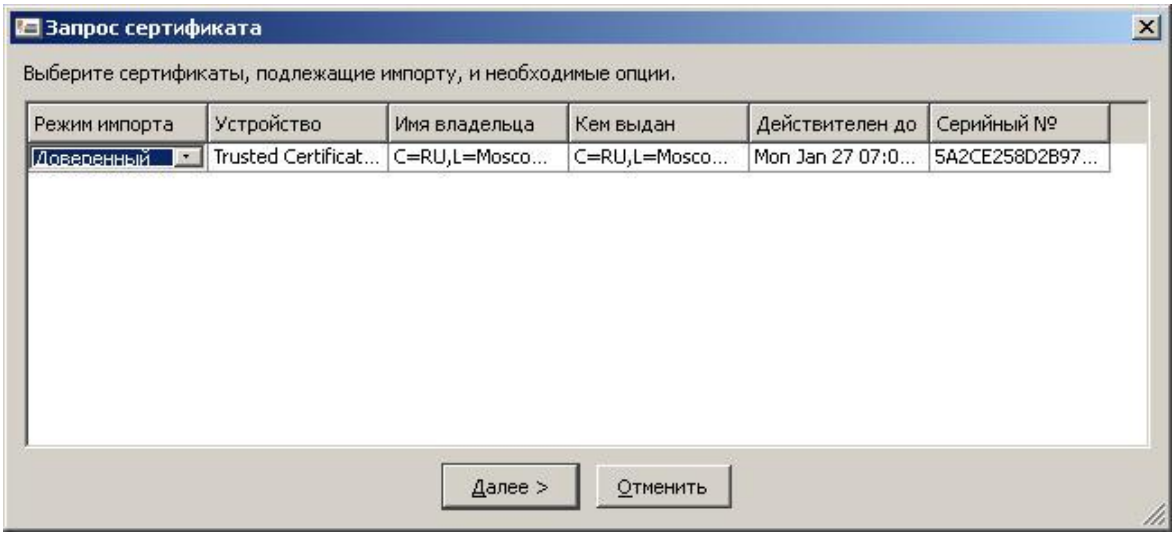

Рисунок 3 – Настройки в окне «Сертификат/Мастер ключей» при импорте сертификата УЦ

в) В следующем окне диалога ввести PIN-код Trusted Certificate токена (см. Рисунок 4).

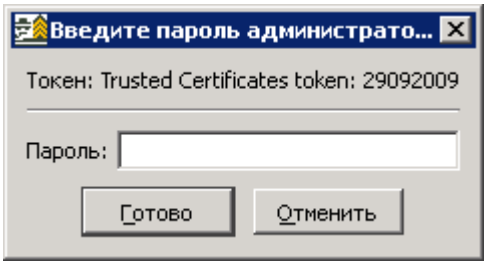

Рисунок 4 – Окно для ввода пароля токена

	Предустановленное значение PIN-кода токена – 12345678.
	Если персональный сертификат издан корневым УЦ то этого достаточно, если подчиненным УЦ, то в любой последовательности командой «Импорт» зарегистрировать все промежуточные сертификаты. При этом *ЗАСТАВА-Офис* определяет тип сертификата и кладет его в нужное хранилище.

3) Подключиться к ЦУП, для этого надо:

   а) Открыть окно «Управление политиками», нажав кнопку «Политика» на *Панели управления*.

   б) В окне «Управление политиками» выделить название системной политики и дважды нажать левой клавишей мыши или нажать кнопку «Правка». Откроется окно «Опции политики». Исправить действующую политику:

   – В поле «Источник» выбрать в качестве источника прогрузки политики – «Сервер + Сертификат».
   – В поле «Сертификат» выбрать Ваш персональный сертификат.
   – В поле «Сервер(ы) политик» ввести адрес(а) сервера политики (см. Рисунок 5) и порт, с которого будет получена политика. Если порт сервера не указан, то берется значение по умолчанию (500).
     Если серверов несколько, IP-адреса указываются через запятую. Номер порта указывается через двоеточие.

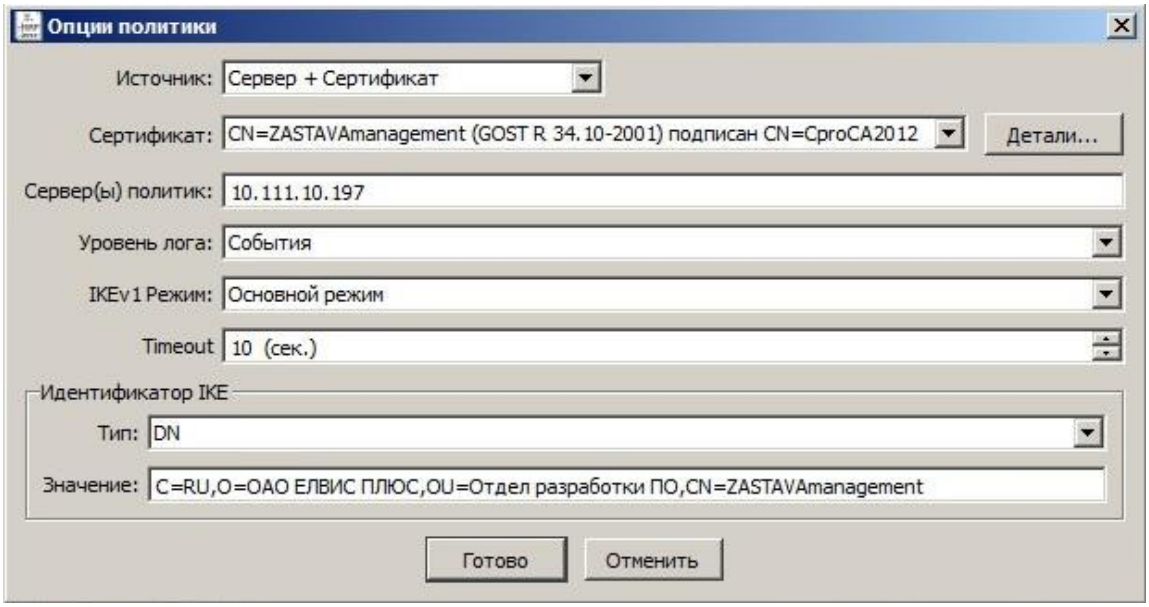

Рисунок 5 – Добавление сервера(ов) политики для прогрузки ЛПБ в окне «Опции политик»

   – Выбрать режим установления соединения IKE v1: основной или агрессивный в поле «IKE v1 Режим».

– Отметить время в поле «Timeout», через которое необходимо обращаться к серверу за ЛПБ.
– В секции «Идентификатор IKE» выбрать тип идентификатора для прогрузки политики, который должен быть согласован с ЦУП.

в) После внесения изменений нажать кнопку «Готово».

г) Выбрать созданную политику и нажать кнопку «Активировать».

д) *Агент* начинает инициировать создание защищенного соединения с сервером ЦУП. В процессе создания соединения при обращении к персональному сертификату будет запрошен пароль (PIN-код токена) хранилища персонального сертификата (см. Рисунок 6).

При первом обращении для доступа к хранилищу контейнера выдается окно ввода пароля (PIN-кода) с флагом «сохранить пароль для дальнейших соединений». Если не установить флаг, то введенный им пароль будет сохранен, и не будет запрашиваться при установлении последующих соединений до перезапуска службы vpndmn.exe *Агента*. Если установить флаг, то пароль больше запрашиваться не будет.
Если не установить флаг, то введенный пароль не будет сохранен и будет запрашиваться при установке последующих соединений.

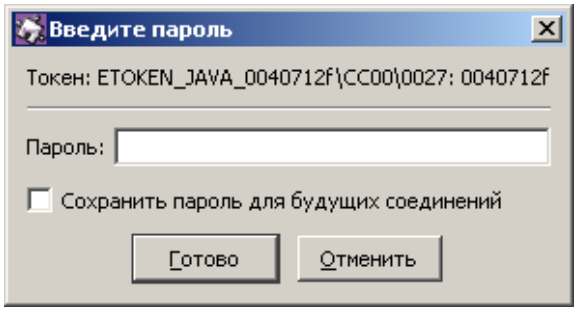

Рисунок 6 – Ввод пароля токена при создании защищенного соединения

е) Ввести требуемый пароль (PIN-код токена).

ж) После установления соединения в информационной строке *Панели управления* появится информация о прогрузке политики из ЦУП (см. Рисунок 7).

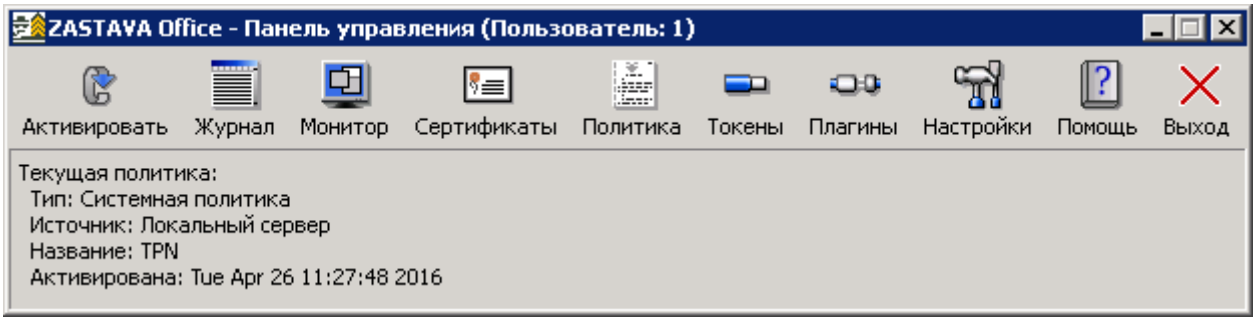

Рисунок 7 – Текущий статус ЛПБ *ЗАСТАВА-Офис* (источник ЛПБ и дата ее активации)

3. РАБОТА В ГРАФИЧЕСКОМ ИНТЕРФЕЙСЕ *ЗАСТАВА-ОФИС*

3.1. *Панель управления*

Основным элементом управления ЗАСТАВА-Офис является *Панель Управления* (Рисунок 8).

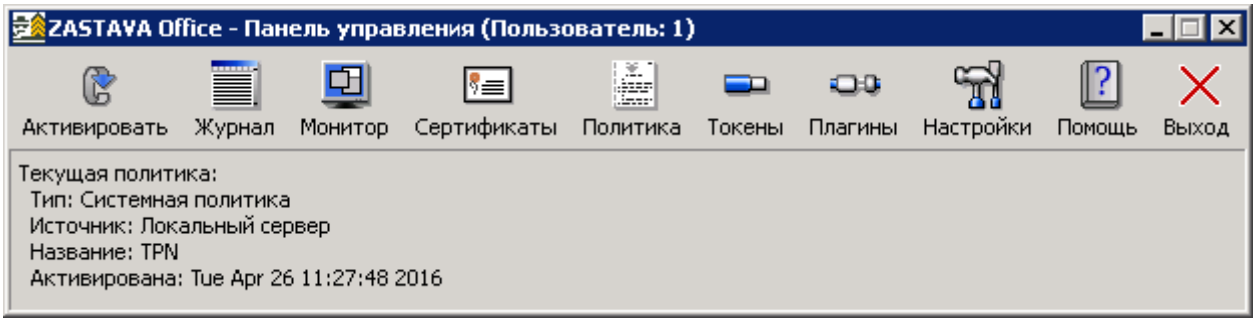

Рисунок 8 – *Панель управления*

Панель управления содержит кнопки, при помощи которых можно выполнить необходимую операцию или открыть дополнительное окно.

В нижней части *Панели управления* находится окно состояния, отображающее текущую ЛПБ *ЗАСТАВА-Офис* (тип активированной ЛПБ, источник ЛПБ, дата и время ее активации).

3.1.1. Перезагрузка ЛПБ

Чтобы перезагрузить ЛПБ, которая загружена в *ЗАСТАВА-Офис,* нужно нажать кнопку «Активировать». После этого будет заново загружена текущая ЛПБ. Если Вы хотите загрузить ЛПБ из файла или с сервера, используйте кнопку «Активировать» на вкладке системной политики с настроенными параметрами окна «Управление политиками» (см. подраздел 3.5).

Обычно перегружать ЛПБ принудительно не требуется. Исключением являются ситуации, когда возникают ошибки конфигурирования *ЗАСТАВА-Офис* или ошибки при установлении защищенных соединений.

Удостовериться в том, что на компьютере правильно установлены дата, время и настройки часового пояса. Необходимо правильно определить эти параметры, иначе может оказаться, что срок действия сертификатов истек, и Вы не можете установить VPN-соединения.

3.1.2. Просмотр событий

Вы можете просматривать файл регистрации событий *ЗАСТАВА-Офис* при помощи кнопки «Журнал» на *Панели управления*. При нажатии этой кнопки появится окно «Журнал», отображающее информацию о системных событиях.

3.1.3. Монитор

Окно «Монитор», доступное нажатием на кнопку «Монитор», предоставляет обзор активных в настоящее время защищенных соединений, установленных с данным компьютером. Кроме того, окно «Монитор» позволяет провести фильтрацию защищённых соединений, просмотреть статистику по пакетам, список выделенных адресов ike-cfg, а также параметры шлюзов прикладного уровня.

3.1.4. Сертификаты

Цифровые сертификаты и предварительно распределенные ключи (pre-shared)[1] необходимы, чтобы проверять подлинность объектов политики, с которыми Вы взаимодействуете. Сертификаты (включая сертификаты УЦ), предварительно распределенные ключи, СОС регистрируются в *ЗАСТАВА-Офис* через окно «Сертификаты и Ключи».

3.1.5. Работа с политикой

ЛПБ является текстовым файлом, описывающим правила, которые определяют, как взаимодействуют объекты в защищённой среде. Для настройки параметров необходимо нажать кнопку «Политика» на *Панели управления*. Окно «Управление Политиками» предназначено для редактирования списка ЛПБ и установки опций ЛПБ. Для сохранения измененных опций ЛПБ требуется введение пароля администратора. Для активации выбранной из списка политики введение пароля администратора не требуется.

3.1.6. Работа с токенами

ЗАСТАВА-Офис позволяет использовать токены как среду транспортировки важной информации (хранение и поиск паролей, сертификатов, закрытых ключей). Для настройки параметров необходимо нажать кнопку «Токены» на *Панели управления*. Окно «Токены» предназначено для редактирования списка токенов и выполнения ряда доступных действий: загрузки, входа, смены пароля, инициализации и обновления токенов.

---

[1] Предварительно распределенные ключи поддерживаются в *ЗАСТАВА-Офис* при наличии токена *PKCS #11*, который обладает возможностью хранить предварительно распределенные ключи.

3.1.7. Работа с плагинами

При помощи модуля криптоплагинов можно регистрировать и активировать криптобиблиотеки, а также управлять отдельными криптоалгоритмами, входящими в состав библиотек.

Работа с модулем криптоплагинов может производиться, либо при помощи графического интерфейса в окне «Плагины» - для этого необходимо нажать кнопку «Плагины» на *Панели управления*, либо из командной строки - см. раздел 5.

3.1.8. Настройки *ЗАСТАВА-Офис*

Пользователи имеют доступ к средствам конфигурирования настроек *ЗАСТАВА-Офис*. Для этого необходимо нажать кнопку «Настройки» на *Панели управления*.

3.1.9. Помощь

Выбрать «Помощь», чтобы отобразилось меню, с помощью которого можно вызвать справочную систему *ЗАСТАВА-Офис*, а также получить информацию о программе.

3.1.9.1. Информация о программе

Для получения информации о программе необходимо нажать кнопку «Помощь» на *Панели управления* и в выпадающем меню выбрать пункт «О ZASTAVA Office...».

3.1.9.2. Справочная система *ЗАСТАВА-Офис*

Интерактивная справочная система может использоваться для получения ответов на вопросы по работе *ЗАСТАВА-Офис*. Если Вы испытываете трудности с созданием или редактированием объектов или у Вас есть вопросы относительно параметров, Вы можете воспользоваться справочной системой. Для вызова системы надо нажать кнопку «Помощь» на *Панели управления* и в выпадающем меню выбрать пункт «Помощь», откроется окно «Помощь», подробнее см. подраздел 3.9.

3.1.10. Закрытие

Нажатие кнопки «Выход» закрывает только графический интерфейс *ЗАСТАВА-Офис.* При этом служба vpndmn и *ЗАСТАВА-Офис* будут продолжать работать, но вместо политики пользователя будет загружена системная политика.

3.1.11. Строка статуса ЛПБ

В нижней части *Панели управления* находится строка (см. Рисунок 8), отображающая текущий статус ЛПБ *ЗАСТАВА-Офис* (источник ЛПБ и дата и время ее активации, название конфигурации).

3.1.12. Ввод пароля токена

Когда *Агент* начинает инициировать создание защищенного соединения с сервером ЦУП. В процессе создания соединения при обращении к персональному сертификату будет запрошен пароль (PIN-код токена) хранилища персонального сертификата (см. Рисунок 9).

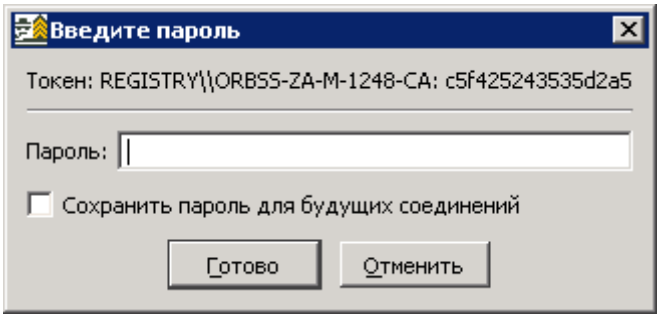

Рисунок 9 – Ввод пароля токена при создании защищенного соединения

Также пароль запрашивается при любом обращении к персональному сертификату, например, при импорте персонального сертификата, удалении его из *ЗАСТАВА-Офис* и т. д.

Удостовериться в том, что у Вас запущен графический интерфейс *ЗАСТАВА-Офис*, в противном случае окно с запросом на ввод пароля токена не появится и защищенное соединение с сервером ЦУП не создастся.

3.2. Окно «Журнал»

Окно «Журнал» (см. Рисунок 10) открывается нажатием кнопки «Журнал» на Панели управления. В журнале отображается содержимое файла регистрации событий *ЗАСТАВА-Офис*.

В верхней части окна расположена панель управления.

Основную часть окна занимает таблица с описанием системных событий. Уровень детализации настраивается пользователем (подробнее см. п. 3.8.1).

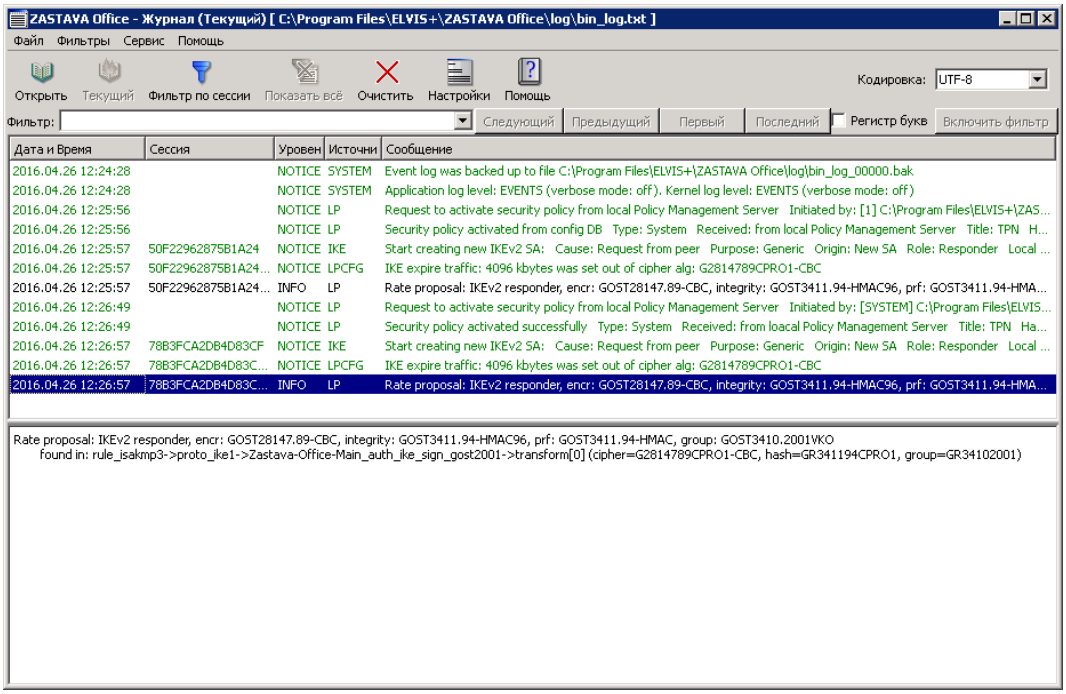

Рисунок 10 – Окно с зарегистрированными событиями

Системные события в таблице разбиты по следующим параметрам:

– Дата и Время – время регистрации события.

– Сессия – шестнадцатеричное выражение, составленное из: cookie Initiator; cookie Responder; Messenger ID. Причем любое из двух первых выражений служит идентификатором IKE-сессии.

– Уровень – значимость события (INFO, WARNING, ERROR и т. д.).

– Источник – программный модуль, в котором произошло событие.

– Сообщение – текстовое представление произошедшего системного события.

В нижней части окна в более удобном виде отображается информация из столбца «Сообщение» выделенной строки журнала.

Вы можете копировать текст из нижней части поля окна «Журнал» регистрации в Буфер Обмена (Clipboard), выделяя его при помощи мыши или нажимая клавиши <Ctrl>+<C>. При необходимости, можно послать эту информацию администратору безопасности, для анализа возникших проблем с *ЗАСТАВА-Офис*.

3.2.1. Структура окна «Журнал»

3.2.1.1. Строка меню окна «Журнала»

Строка меню содержит следующие меню: «Файл», «Фильтры», «Сервис», «Помощь». Команды меню представлены в таблице (см. Таблица 1).

Таблица 1 – Команды меню окна «Журнал»

Команда	Характеристика
Файл	
Открыть	Открывает событий, выбранный пользователем.
Открыть текущий журнал	Открывает текущий журнал событий.
Открыть новый журнал	Открывает новое окно «Журнал».
Фильтр	
Фильтр по сессии IKE	Отфильтровывает в журнале все события по выбранной сессии (cookie Initiator; cookie Responder).
Фильтр по обмену IKE	Отфильтровывает в журнале все события по полной выбранной сессии (cookie Initiator; cookie Responder; Messenger ID).
Фильтр по уровню	Отфильтровывает события по выбранному значению значимости (столбец «Уровень»).
Фильтр по источнику	Отфильтровывает события по выбранному значению программного модуля, в котором произошло событие (столбец «Источник»).
Показать все	Отменяет параметры фильтрации и отображает весь журнал системных событий.
Сервис	
Копировать в буфер обмена	Копирует информацию из выделенных строк журнала событий в буфер обмена.
Копировать в поле фильтра	Копирует содержание выделенной ячейки журнала событий в поле «Фильтр».
Очистить	Очищает текущее содержимого окна «Журнал» и файла регистрации системных событий.
Настройки	Открывает окно «Параметры лога» для настройки параметров регистрации и представления системных событий.
Помощь	
Справка по журналу	Открывает раздел «Справки», поясняющий работу с журналом регистрации системных событий.
Помощь	Вызов общей Справочной системы *ЗАСТАВА-Офис*

3.2.1.2. Панель инструментов окна «Журнала»

Описание элементов Панели инструментов окна «Журнал» приведено в таблице (см. Таблица 2).

Таблица 2 – Описание кнопок панели инструментов окна «Журнал»

Кнопка	Описание
 Открыть	Открывает журнал событий, выбранный пользователем.
 Текущий	Открывает текущий журнал событий. Кнопка неактивна при просмотре текущего журнала событий.
 Фильтр по сессии IKE	Отфильтровывает в журнале все события по выбранной сессии (cookie Initiator; cookie Responder).
 Показать все	Отменяет параметры фильтрации и позывает весь журнал системных событий.
 Очистить	Очищает текущее содержимого окна «Журнал» и файла регистрации системных событий.
 Настройки	Открывает окно «Параметры лога» для настройки параметров регистрации и представления системных событий.
 Помощь	Открывает раздел «Справки», поясняющий работу с журналом регистрации системных событий.
Кодировка	Выбор кодировки, в которой информация отображается в журнале.
Фильтр	Ввод текста, по которому будет производиться фильтрация
Следующий	Следующая строка журнала, соответствующая заданному фильтру.
Предыдущий	Предыдущая строка журнала, соответствующая заданному фильтру.
Первый	Первая строка журнала, соответствующая заданному фильтру.
Последний	Последняя строка журнала, соответствующая заданному фильтру.
Регистр букв	Если флажок установлен, фильтрация производится с учетом регистра. Если флажок не установлен, фильтрация производится без учета регистра.
Включить фильтр	Отфильтровывает строки, в которых присутствует тест из поля «Фильтр».
Убрать фильтрацию	Отображает полный журнал. Кнопка отображается, когда включена фильтрация по какому-либо параметру.

3.2.1.3. Контекстное меню окна «Журнал»

Команды контекстного меню окна «Журнал» и их описание приведены в таблице (см. Таблица 3).

Таблица 3 – Команды контекстного меню окна «Журнал»

Команда	Характеристика
Фильтр по сессии IKE	Выделяет в журнале все события по выбранной сессии (cookie Initiator; cookie Responder).
Фильтр по обмену IKE	Выделяет в журнале все события по полной выбранной сессии (cookie Initiator; cookie Responder; Messenger ID).
Фильтр по уровню	Выделяет в журнале все события по их значимости (INFO, WARNING, ERROR).
Фильтр по источнику	Выделяет в журнале все события относительно программного модуля, в котором произошло событие (поле «Источник»).
Копировать в буфер обмена	Копирует информацию из выделенных строк журнала событий в буфер обмена.
Копировать в поле фильтра	Копирует содержание выделенной ячейки журнала событий в поле «Фильтр».

3.2.2. Фильтрация отображаемых событий

Отфильтровать информацию в журнале можно либо по одному из предустановленных фильтров (меню «Фильтры»), либо по произвольно заданному тексту.

Для фильтрации с помощью предустановленных фильтров следует выделить в таблице строку с требуемым значением параметра и затем выбрать в меню нужный фильтр. Например, чтобы отфильтровать все события уровня «INFO», следует выделить в журнале любую строку, в столбце «Уровень» которой стоит значение INFO, затем выбрать команду меню «Фильтры» → «Фильтр по уровню». В результате в журнале будут отображаться только строки с уровнем INFO.

Чтобы отфильтровать события по произвольно заданному тексту, введите нужный текст в поле «Фильтр». Результаты поиска подсвечиваются настроенным цветом по мере ввода текста. При нажатии кнопки «Включить фильтр» в журнале будут отображаться только отфильтрованные строки, содержащие введенный текст.

Чтобы скопировать в поле «Фильтр» содержимое какой-либо ячейки журнала, щелкните правой клавишей мыши на нужной ячейке и в появившемся контекстном меню выберите команду «Копировать в поле фильтра».

3.2.3. Настройка параметров регистрации событий

Настройка параметров регистрации событий производится из окна «Параметры лога», которое открывается кнопкой «Настройки». Окно «Параметры лога» содержит две вкладки: «Обработка» и «Отображение».

На вкладке «Обработка» (см. Рисунок 11) производится настройка параметров регистрации событий. Содержание вкладки полностью дублирует вкладку «Журнал» окна «Прочие настройки» и настраивается аналогичным образом (см. п. 3.8.1).

Некоторые параметры уровней регистрации хранятся также в ЛПБ, созданной для *ЗАСТАВА-Офис*

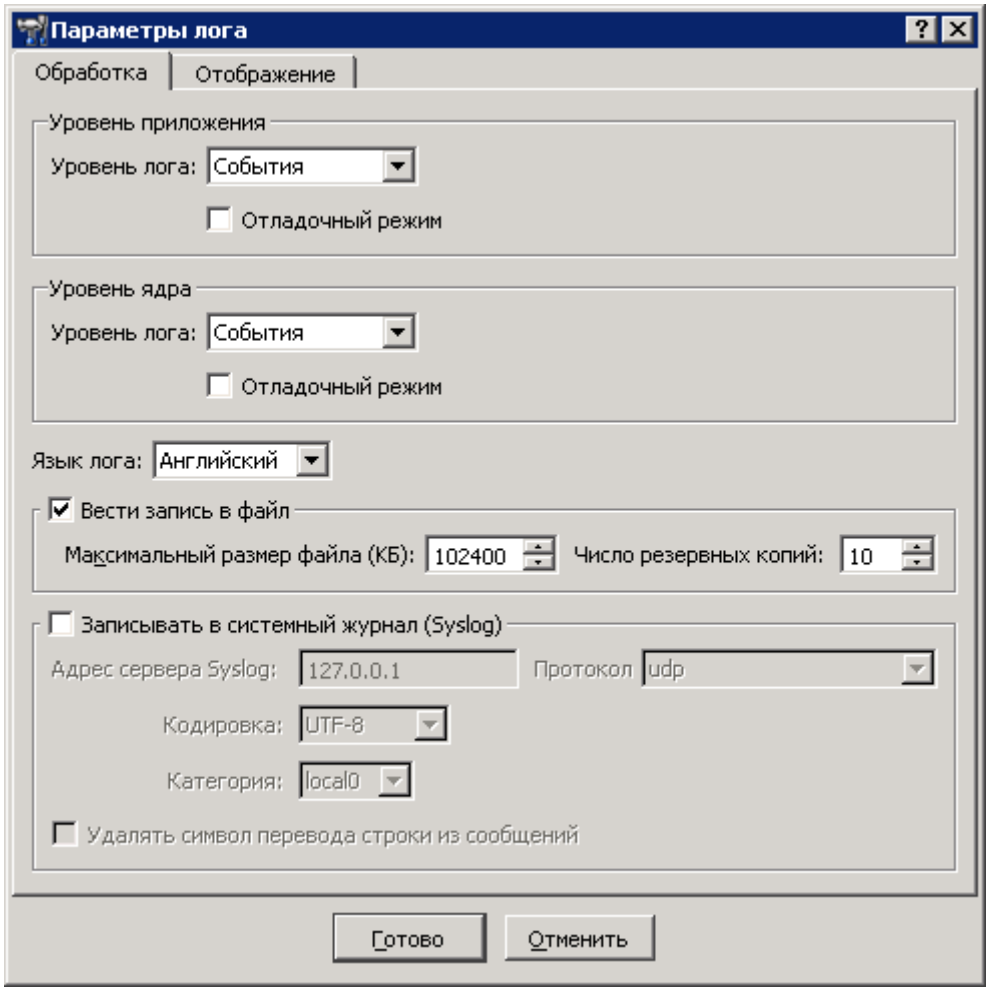

Рисунок 11 – Окно настройки параметров регистрации событий

Параметры представления журнала системных событий настраиваются на вкладке «Отображение» (см. Рисунок 12).

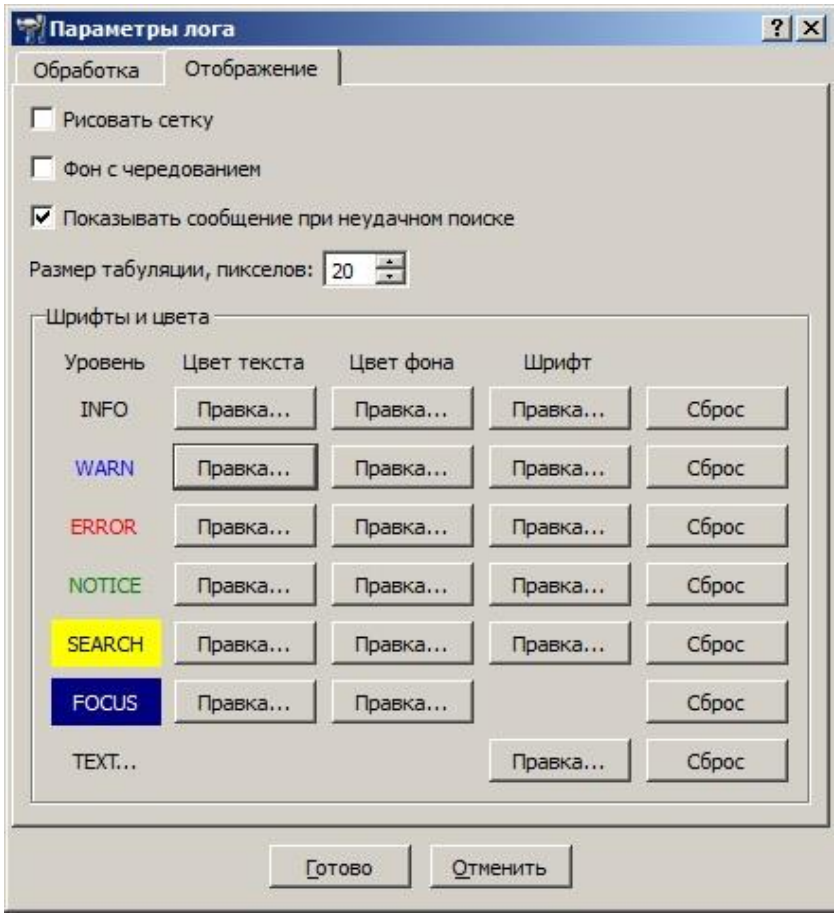

Рисунок 12 – Настройка параметров представления журнала системных событий

Вы можете настроить цвет текста, цвет фона и шрифт для отображения сообщений каждого из уровней. Для настройки параметра следует нажать соответствующую кнопку «Правка» и в появившемся окне изменить значения параметра. Кнопка «Сброс» позволяет сбросить пользовательские настройки на настройки по умолчанию.

По окончании настройки следует нажать кнопку «Готово» для применения сделанных изменений.

Для отмены настроек следует нажать кнопку «Отменить».

3.2.4. Копирование описания событий

Для копирования информации необходимо:

1) Выделить одну или несколько строк в журнале. Выделение нескольких строк производится стандартным образом, с помощью клавиш <Shift> или <Ctrl>.
2) Скопировать выделенные строки в буфер обмена одним из способов:
   - выбрав в контекстном меню команду «Копировать в буфер обмена»;
   - выбрав команду меню «Сервис» → «Копировать в буфер обмена»;
   - нажав сочетание клавиш <Ctrl + C>;

Выделенные строки будут скопированы в буфер обмена.

Информация из буфера обмена может быть вставлена в выбранное приложение стандартным образом.

3.2.5. Файл регистрации системных событий

Содержимое окна «Журнал» хранится в файле `bin_log.txt`.

Вы можете открыть для просмотра другие журналы регистрации событий ЗАСТАВА-Клиент при помощи кнопки «Открыть» на панели инструментов окна «Журнал».

3.2.6. Очистка журнала и файла регистрации системных событий

Для очистки текущего содержимого окна «Журнал» и файла регистрации системных событий следует нажать кнопку «Очистить». В результате очистки произойдет следующее:

- Журнал будет очищен;
- Событие очистки журнала будет зарегистрировано и размещено в начале файла регистрации событий, а также появится вверху списка в окне «Журнал».
- «Старый» список зарегистрированных событий будет переименован в файл с расширением **.bak* и с именем вида *bin_log_<номер по порядку>*.

3.3. Окно «Монитор»

Окно «Монитор», доступное нажатием на кнопку «Монитор», предоставляет обзор активных в настоящее время защищенных соединений, установленных с данным компьютером.

Кроме того, окно «Монитор» позволяет провести фильтрацию защищённых соединений, просмотреть статистику по пакетам, список выделенных адресов ike-cfg, а также параметры шлюзов прикладного уровня. Окно содержит несколько вкладок, как показано на рисунке (см. Рисунок 13).

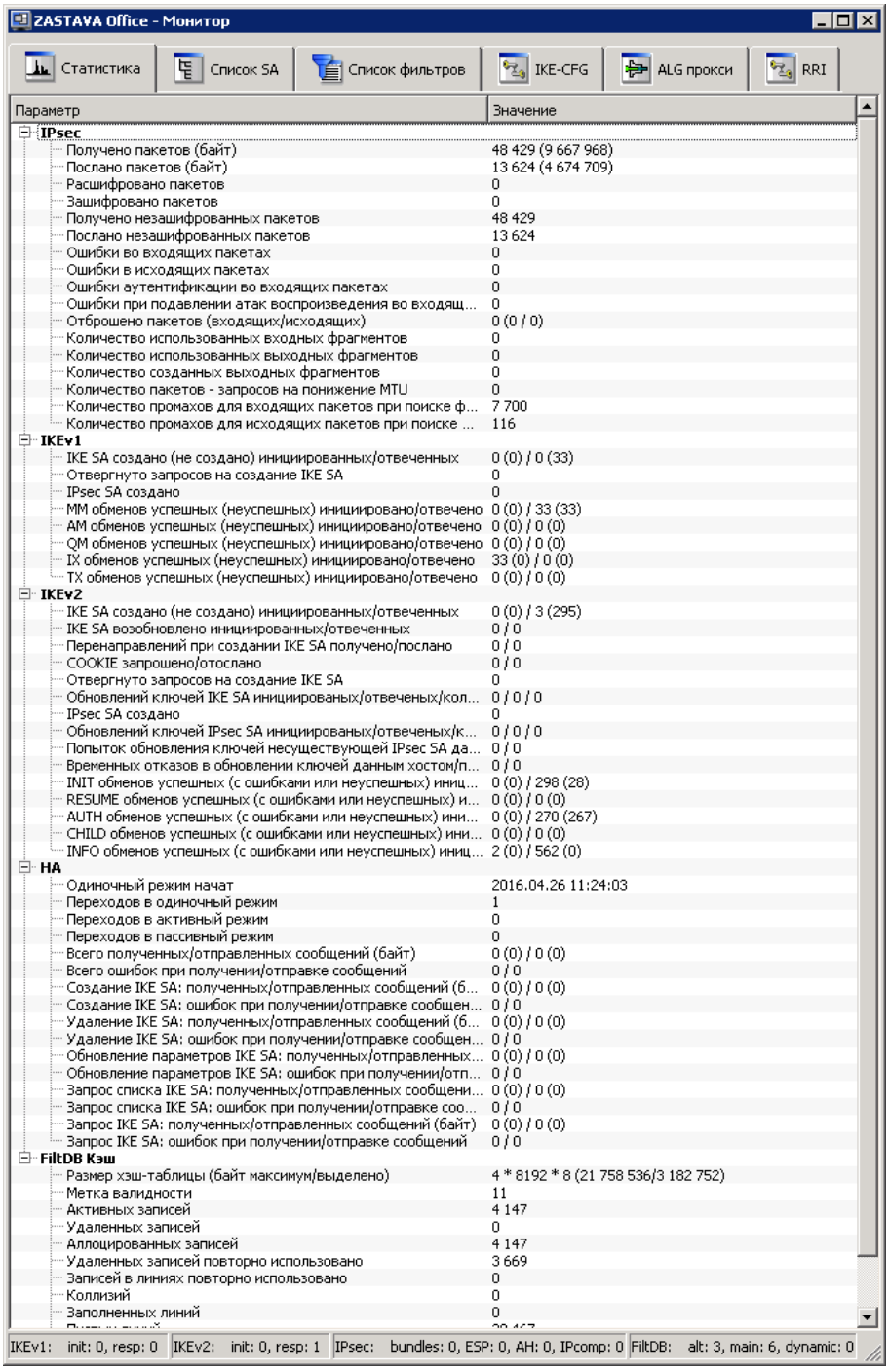

Рисунок 13 – Окно «Монитор», вкладка «Статистика»

3.3.1. Вкладка «Статистика»

На вкладке «Статистика» можно получить статистическую информацию по всем пакетам прошедшим через драйвер *Агента* (например, по протоколу IPsec) (см. Таблица 4).

Таблица 4 – Описание параметров вкладки «Статистика»

Параметр	Описание
IPsec	

Параметр	Описание
Получено пакетов (байт)	Количество пакетов, полученное с момента запуска *Агента*
Послано пакетов (байт)	Количество пакетов, посланное с момента запуска *Агента*
Расшифровано пакетов	Количество пакетов, расшифрованных *Агентом*
Зашифровано пакетов	Количество пакетов, зашифрованных *Агентом*
Получено незашифрованных пакетов	Количество полученных *Агентом* незашифрованных пакетов
Послано незашифрованных пакетов	Количество отправленных незашифрованных пакетов
Ошибки во входящих пакетах	Количество ошибок во входящих пакетах
Ошибки в исходящих пакетах	Количество ошибок в исходящих пакетах
Ошибки аутентификации во входящих пакетах	Количество ошибок аутентификации во входящих пакетах
Ошибки при подавлении атак воспроизведения во входящих пакетах	Количество ошибок при подавлении атак воспроизведения во входящих пакетах
Отброшено пакетов (входящих/исходящих)	Количество отброшенных пакетов или фрагментов
Количество использованных входных фрагментов	Количество IP-фрагментов, использованных при реассемблировании входного пакета
Количество использованных выходных фрагментов	Количество IP-фрагментов, использованных при реассемблировании выходного пакета
Количество созданных выходных фрагментов	Количество IP-фрагментов, созданных при фрагментации выходного пакета
Количество пакетов – запросов на понижение MTU	Количество пакетов – запросов на понижение MTU
Количество промахов для входящих пакетов при поиске фильтра в хэш-таблице	Количество промахов для входящих пакетов при поиске фильтра в хэш-таблице
Количество промахов для исходящих пакетов при поиске фильтра в хэш-таблице	Количество промахов для исходящих пакетов при поиске фильтра в хэш-таблице
IKEv2	
IKE SA создано (не создано) инициированных/отвеченных	Количество созданных (не созданных) инициированных/отвеченных IKE SA в формате x(x)/x(x)

Параметр	Описание
IKE SA возобновлено инициированных/отвеченных	Количество возобновленных IKE SA инициированных/отвеченных
Перенаправлений при создании IKE SA получено/послано	Количество перенаправлений IKE SA получено/послано
COOKIE запрошено/отослано	Количество запрошенных/отправленных токенов COOKIE
Отвергнуто запросов на создание IKE SA	Количество отвергнутых запросов на создание IKE SA
Обновлений ключей IKE SA инициированных/отвеченных/ коллизий	Количество обновлений ключей IKE SA инициированных/отвеченных/коллизий в формате x/x/x
IPsec SA создано	Количество созданных IPsec SA
Обновлений ключей IPsec SA инициированных/отвеченных/ коллизий	Количество обновлений ключей IPsec SA инициированных/полученных/коллизий в формате x/x/x
Попыток обновления ключей несуществующей IPsec SA данным хостом/партнером	Количество попыток обновления ключей несуществующей IPsec SA данным хостом/партнером
Временных отказов в обновлении ключей данным хостом/партнером	Количество временных отказов в обновлении ключей данным хостом/партнером
INIT обменов успешных (с ошибками или неуспешных) инициировано/отвечено	Количество обменов INIT_IKE_SA успешных (с ошибками или неуспешных) инициировано/отвечено в формате x(x)/x(x)
RESUME обменов успешных (с ошибками или неуспешных) инициировано/отвечено	Количество обменов RESUME_IKE_SA успешных (с ошибками или неуспешных) инициировано/отвечено в формате x(x)/x(x)
AUTH обменов успешных(с ошибками или неуспешных) инициировано/отправлено	Количество успешных (с ошибками или неуспешных) обменов IKE_AUTH инициировано/отправлено в формате x(x)/x(x)
CHILD обменов успешных(с ошибками или неуспешных) инициировано/отправлено	Количество успешных (с ошибками или неуспешных) обменов CREATE_CHILD_SA инициировано/отправлено в формате x(x)/x(x)
INFO обменов успешных(с ошибками или неуспешных) инициировано/отправлено	Количество успешных (с ошибками или неуспешных) обменов INFORMATIONAL инициировано/отправлено в формате x(x)/x(x)
HA	
Одиночный режим начат	Время старта одиночного режима
Переходов в одиночный режим	Количество переходов в одиночный режим
Переходов в активный режим	Количество переходов в активный режим
Переходов в пассивный режим	Количество переходов в пассивный режим
Всего полученных/ отправленных сообщений (байт)	Объем полученных/ отправленных сообщений в байтах

Параметр	Описание
Всего ошибок при получении/отправке сообщений	Количество ошибок при получении/отправке сообщений
Неизвестных сообщений (байт) получено	Объем полученных неизвестных сообщений в байтах
Создание IKE SA: полученных/ отправленных сообщений (байт)	Объем полученных/ отправленных сообщений в байтах при создании IKE SA
Создание IKE SA:ошибок при получении/отправке сообщений	Количество ошибок при создании IKE SA
Удаление IKE SA: полученных/ отправленных сообщений (байт)	Объем полученных/ отправленных сообщений в байтах при удалении IKE SA
Удаление IKE SA: ошибок при получении/отправке сообщений	Количество ошибок при удалении IKE SA
Обновление параметров IKE SA: полученных/ отправленных сообщений (байт)	Объем полученных/ отправленных сообщений в байтах при обновлении параметров IKE SA
Обновление параметров IKE SA:ошибок при получении/ отправке сообщений	Количество ошибок при обновлении параметров IKE SA
Запрос списка IKE SA: полученных/ отправленных сообщений (байт)	Объем полученных/ отправленных сообщений в байтах при запросе списка IKE SA
Запрос списка IKE SA: ошибок при получении/ отправке сообщений	Количество ошибок при запросе списка IKE SA
Запрос IKE SA: полученных/ отправленных сообщений (байт)	Объем полученных/ отправленных сообщений в байтах при запросе IKE SA
Запрос IKE SA: ошибок при получении/ отправке сообщений	Количество ошибок при запросе IKE SA
IKE-CFG обновление записей: полученных/отправленных сообщений (байт)	Объем полученных/ отправленных сообщений в байтах при обновлении записей IKE-CFG
IKE-CFG обновление записей: ошибок при получении/ отправке сообщений	Количество ошибок в полученных/ отправленных сообщениях при обновлении записей IKE-CFG
IKE-CFG удаление записей: полученных/отправленных сообщений (байт)	Объем полученных/ отправленных сообщений в байтах при удалении записей IKE-CFG
IKE-CFG удаление записей: ошибок при получении/ отправке сообщений	Количество ошибок в полученных/ отправленных сообщениях при удалении записей IKE-CFG
IKE-CFG сброс всех записей: полученных/отправленных сообщений (байт)	Объем полученных/ отправленных сообщений в байтах при обновлении сбросе записей IKE-CFG
IKE-CFG сброс всех записей: ошибок при получении/ отправке	Количество ошибок в полученных/ отправленных сообщениях при сбросе записей IKE-CFG

Параметр	Описание
сообщений	
FiltDB Кэш	
Размер хэш-таблицы (байт максимум/выделено)	Размер хэш-таблицы (байт максимум/выделено) в формате x*x*x(x/x)
Метка валидности	Текущее значение метки, служащей для определения возможности использования записей в хэш-таблице
Активных записей	Количество активных записей
Удаленных записей	Количество удаленных записей
Аллоцированных записей	Количество записей выделенных из памяти
Удалённых записей повторно использовано	Количество повторно использованных удалённых записей
Записей в линиях повторно использовано	Количество использованных записей в линиях
Коллизий	Количество попыток добавления одинаковых записей
Заполненных линий	Количество заполненных линий
Пустых линий	Количество пустых линий
Остальных линий	Количество остальных линий
Средняя длина непустых линий	Средняя длина непустых линий

3.3.2. Вкладка «Список SA»

Вкладка «Список SA» в левой части содержит древовидную структуру (см. Рисунок 14) активных защищённых соединений, установленных с данным компьютером, а также создающихся защищённых соединений. В правой части окна содержится детальная информацию о выбранном в левой части окна активном соединении.

Рядом с кнопкой «Фильтр» в правом верхнем углу окна «Монитор» вкладки «Список SA» расположены две кнопки «Удалить» и «Удалить все из списка», позволяющие удалить активное защищённое соединение.

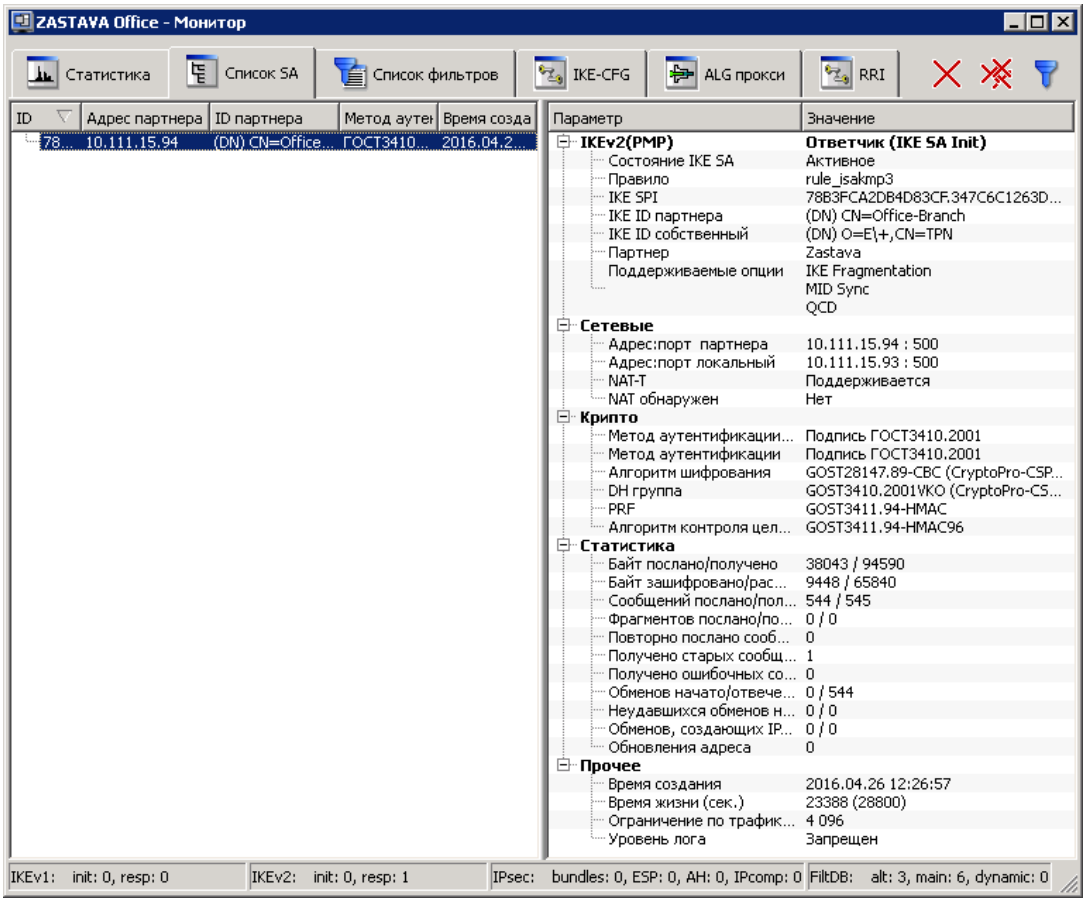

Рисунок 14 - Окно «Монитор», вкладка «Список SA»

Таблица в левой части окна содержит следующую информацию о защищенных соединениях (IPsec SAs) (см. Таблица 5).

Таблица 5 – Информация об активных защищенных соединениях

Параметр	Характеристика
ID	ID IKE SA (IKE SPI) или внутренний идентификатор IPsec SA
Адрес партнера	IP-адрес партнера
ID партнера	Идентификатор партнера (часто DN сертификата партнера)
Метод аутентификации	Используемый в защищенном соединении метод аутентификации для IKE SA и имя правила в LSP для IPsec SA
Время создания	Время создания SA

В правой части экрана отображаются параметры и их значения для данного соединения.

Информация о защищенном соединении появляется только после выбора соответствующего соединения в левой части окна.

Отфильтровать защищённые соединения можно с помощью кнопки «Фильтр», расположенной в верхнем правом углу окна. Таблицы в нижней части окна с параметрами фильтрации несут ту же смысловую нагрузку, что и таблицы в правой части окна «Список

SA». В верхней части окна «Список SA –> Фильтр» можно задать различные параметры фильтрации протоколов IKE и IPsec. Вкладка «Фильтр» показана на рисунке (см. Рисунок 15).

Эта вкладка позволяет отфильтровать все существующие защищенные соединения по ряду параметров.

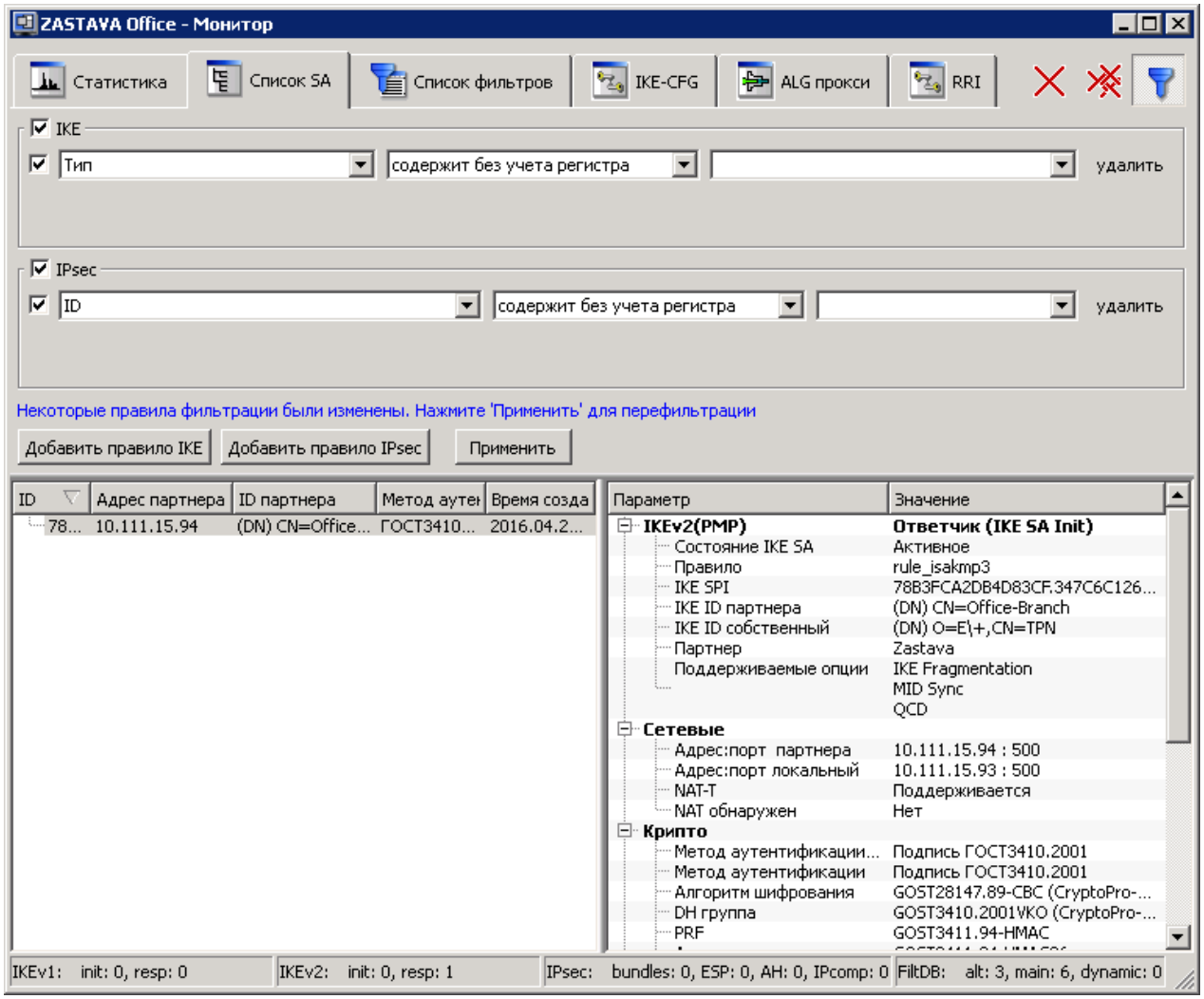

Рисунок 15 - Окно «Монитор», активный «Фильтр»

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

Таблица 6 – Параметры фильтрации протокола IKE SA

Параметр	Характеристика
Тип	Тип создания SA
Режим	Режим создания SA
Роль	Роль локальной машины при создании SA
Состояние IKE SA	Состояние IKE SA
EAP ID собственный	Свой EAP ID
IKE ID собственный	IKE ID данного компьютера

Параметр	Характеристика
EAP ID партнера	EAP ID, присланный партнером
IKE ID партнера	IKE ID партнера
ID партнера	ID партнера (IKE ID или EAP ID в зависимости от метода аутентификации)
Правило	Имя правила
Алгоритм шифрования	Алгоритм шифрования
Хэш-функция	Алгоритм хэширования
DH группа	DH группа
Алгоритм контроля целостности	Алгоритм контроля целостности
PRF	Псевдослучайная функция
Локальный адрес	IP-адрес данного компьютера, использованный при создании защищенного соединения
Локальный порт	UDP-порт на данном компьютере, использованный при создании защищенного соединения
Адрес партнера	IP компьютера, с которым создано защищенное соединение
Порт партнера	UDP-порт компьютера, с которым создано защищенное соединение
Перенаправлен с адреса	IP компьютера, с которого произошло перенаправление на данный
Метод аутентификации	Метод аутентификации данного компьютера
Метод аутентификации партнера	Метод аутентификации партнера
IKE SPI	IKEv2 SPI
Уровень лога	Уровень подробности регистрации событий
Поддерживаемые опции	Список поддерживаемых опций

Параметры фильтрации протокола IPsec SA приведены в таблице (см. Таблица 7).

Таблица 7 – Параметры фильтрации протокола IPsec SA

Тип	Характеристика
ID	Идентификационный номер
Ссылка на IKE SA	Ссылка на IKE SA
IKE SA ID партнера	IKE SA ID компьютера, с которым создано защищенное соединение

Тип	Характеристика
Режим	Режим создания SA
Роль	Роль при создании SA
Id партнера	ID компьютера партнёра
Id локальный	ID данного компьютера
Адрес партнера	IP-адрес компьютера, с которым создано защищенное подключение
Порт партнера	UDP-порт компьютера, с которым создано защищенное подключение
Адрес локальный	IP-адрес данного компьютера, использованный при создании защищенного соединения
Порт локальный	UDP-порт на данном компьютере, использованный при создании защищенного соединения
IKE-CFG адрес (сервер)	IKE CFG адрес, выданный клиенту
DH группа	DH группа
Фильтр	Фильтр
Правило	Правило
(ESP) Правило	(ESP) Правило
(ESP) SPI in	Значение SPI для входящей SA (ESP)
(ESP) SPI out	Значение SPI для исходящей SA (ESP)
(ESP) Rekey SPI in	Значение SPI для входящей SA, ключи которой были обновлены (ESP)
(ESP) Уровень лога	(ESP) Уровень подробности регистрации событий
(ESP) PMTU	(ESP) значение MTU, которое установлено на промежуточном шлюзе
(ESP) Состояние	(ESP) Состояние
(ESP) Преобразование	(ESP) Алгоритм шифрования
(ESP) Аутентификация	(ESP) Алгоритм имитозащиты
(ESP) Исходный адрес партнера	(ESP) Исходный адрес партнера
(ESP) Исходный адрес локальный	(ESP) Исходный адрес данного компьютера

Тип	Характеристика
(ESP) Декапсулировано пакетов	(ESP) Декапсулировано пакетов
(ESP) Декапсулировано байт	(ESP) Декапсулировано байт
(ESP) Ошибки дешифрации (пакетов)	(ESP) Ошибки дешифрации (пакетов)
(ESP) Ошибки аутентификации (пакетов)	(ESP) Ошибки аутентификации (пакетов)
(ESP) Ошибки атак воспроизведения (пакетов)	(ESP) Ошибки атак воспроизведения (пакетов)
(ESP) Ошибки ограничения трафика (пакетов)	(ESP) Ошибки ограничения трафика (пакетов)
(ESP) Прочие ошибки декапсуляции (пакетов)	(ESP) Прочие ошибки декапсуляции (пакетов)
(ESP) Инкапсулировано пакетов	(ESP) Инкапсулировано пакетов
(ESP) Инкапсулировано байт	(ESP) Инкапсулировано байт
(ESP) ошибки шифрации (пакетов)	(ESP) ошибки шифрации (пакетов)
(IPcomp) Правило	(IPcomp) Правило
(IPcomp) CPI in	Значение CPI для входящей SA (IPcomp)
(IPcomp) CPI out	Значение CPI для исходящей SA (IPcomp)
(IPcomp) Rekey CPI in	Значение CPI для входящей SA, ключи которой были обновлены (IPcomp)
(IPcomp) Уровень лога	(IPcomp) Уровень подробности регистрации событий
(IPcomp) PMTU	(IPcomp) значение MTU, которое установлено на промежуточном шлюзе

Тип	Характеристика
(IPcomp) Состояние	(IPcomp) Состояние
(IPcomp) Преобразование	(IPcomp) Алгоритм сжатия

Фильтрация может осуществляться как среди IKE SA, так и по IPsec SA. Выбор осуществляется с помощью переключателя в левой верхней части экрана.

Для задания операции для фильтрации необходимо выбрать параметр из выпадающего списка второго поля строки для задания параметров фильтрации (см. Таблица 8), операции специфичны для каждого из параметров.

Таблица 8 – Описание типов операций фильтрации

Команда	Характеристика
Операции для фильтрации по типу обмена	
равен	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)
не равен	значение поля не равно эталону
Операции для фильтрации по роли в процессе обмена	
равен	значение поля равно эталону (значение может быть: initiator, responder)
не равен	значение поля не равно эталону
Операции для фильтрации по содержанию строк	
содержит без учета регистра	поле содержит подстроку (эталон), игнорируя регистр букв
не содержит без учета регистра	поле не содержит подстроку (эталон), игнорируя регистр букв
содержит	поле содержит подстроку (эталон), учитывая регистр букв
не содержит	поле не содержит подстроку (эталон), учитывая регистр букв
равняется без учета регистра	поле равняется эталону, игнорируя регистр букв
не равняется без учета регистра	поле не равняется эталону, игнорируя регистр букв
равняется	поле равняется эталону, учитывая регистр букв
не равняется	поле не равняется эталону, учитывая регистр букв
Операции для фильтрации по полю IP-адрес	
в диапазоне	значение поля (IP-адрес) входит в диапазон, заданный эталоном, в качестве эталона можно указать просто IP-адрес (10.1.1.1) или диапазон

Команда	Характеристика
	(10.1.1.1..10.1.1.255) или подсеть (10.1.1.0/24 или 10.1.1.0/255.255.255.0)
не в диапазоне	значение поля (IP-адрес) не входит в диапазон
равен	значение поля (IP-адрес) равен эталону (IP-адрес)
не равен	значение поля (IP-адрес) не равен эталону(IP-адресу)
Операции для фильтрации по полю IP-порт	
равен	значение поля (порт) равно эталону
не равен	значение поля не равно эталону
в диапазоне	значение поля входит в диапазон заданный эталоном, в качестве эталона можно указать просто порт (8080) или диапазон (0...65535)
не в диапазоне	значение поля не входит в диапазон заданный эталоном
Операции для фильтрации по полю уровень лога	
равен	значение поля равно эталону (возможные значения: disabled, events, details, verbose)
не равен	значение поля не равно эталону
больше чем	значение поля больше эталона (disabled < events < details < verbose)
меньше чем	значение поля меньше эталона
больше или равен	значение поля больше или равно эталону
меньше или равен	значение поля меньше или равно эталону
Операции для фильтрации по IPsec-соединению по полю протокол	
равен	значение поля равно эталону (возможные значения: esp, pcp)
не равен	значение поля не равно эталону
Операции для фильтрации по IPsec-соединению по полю mode	
равен	значение поля равно эталону(возможные значения: tunnel, transport)
не равен	значение поля не равно эталону
Операции для фильтрации по IP-протоколу	
равен	значение поля (протокол) равно эталону
не равен	значение поля не равно эталону
в диапазоне	значение поля входит в диапазон, заданный эталоном, в качестве эталона можно указать просто протокол (6) или диапазон (0...255)
не в диапазоне	значение поля не входит в диапазон, заданный эталоном
Операции для фильтрации по диапазону IP-адресов	
содержит	значение поля (IP-диапазон) содержит IP-адрес, заданный эталоном
не содержит	значение поля (IP-диапазон) не содержит IP-адрес, заданный эталоном
в диапазоне	значение поля (IP-диапазон) входит в другой IP-диапазон, заданный эталоном

Команда	Характеристика
не в диапазоне	значение поля (IP-диапазон) не входит в другой IP-диапазон, заданный эталоном
равен	значение поля (IP-диапазон) совпадает с IP-диапазоном, заданный эталоном
не равен	значение поля (IP-диапазон) не совпадает с IP-диапазоном, заданный эталоном

После выбора параметра стейта и выбора, какую операцию применить необходимо, надо указать значение, по которому будет производиться сравнение, в крайнем правом поле строки фильтрации и нажать кнопку «Применить». В таблице будут показаны отфильтрованные события. Количество событий, удовлетворяющих правилу фильтрации, будет показано правее кнопки «Применить».

Во вкладке «Список SA» существует контекстное меню с командами (см. Таблица 9).

Таблица 9 – Команды контекстного меню вкладки «Список SA»

Команда	Характеристика
Показать журнал	Переход в окно «Монитор» для просмотра событий
Выделить первый	Выделение первого SA в окне записи
Выделить последний	Выделение последнего SA в окне записи
Развернуть все	Отображает содержимое состояний SA-соединений
Показывать все SA	Показывать все SA
Показывать только IKE SA	Показывать только IKE SA
Показывать только IPsec SA	Показывать только IPsec SA
Показывать синхронизированные SA	Показывать синхронизированные SA
Показывать удаленные SA	Показывать удаленные SA
Искать только в дереве SA	Искать только в дереве SA
Сменить ключ	Запустить процесс обновления ключей
Удалить	Удалить выделенную сессию
Удалить все из списка	Удалить все соединения
Сохранить	Сохранить выделенную сессию
Сохранить ветвь	Сохранить выделенную ветвь
Сохранить все	Сохранить все

3.3.3. Вкладка «Список Фильтров»

3.3.3.1. Основные элементы

Вкладка «Список Фильтров» позволяет просмотреть как статические, так и динамические фильтры, прогруженные в драйвер (список фильтров определяется ЛПБ) (см. Рисунок 16).

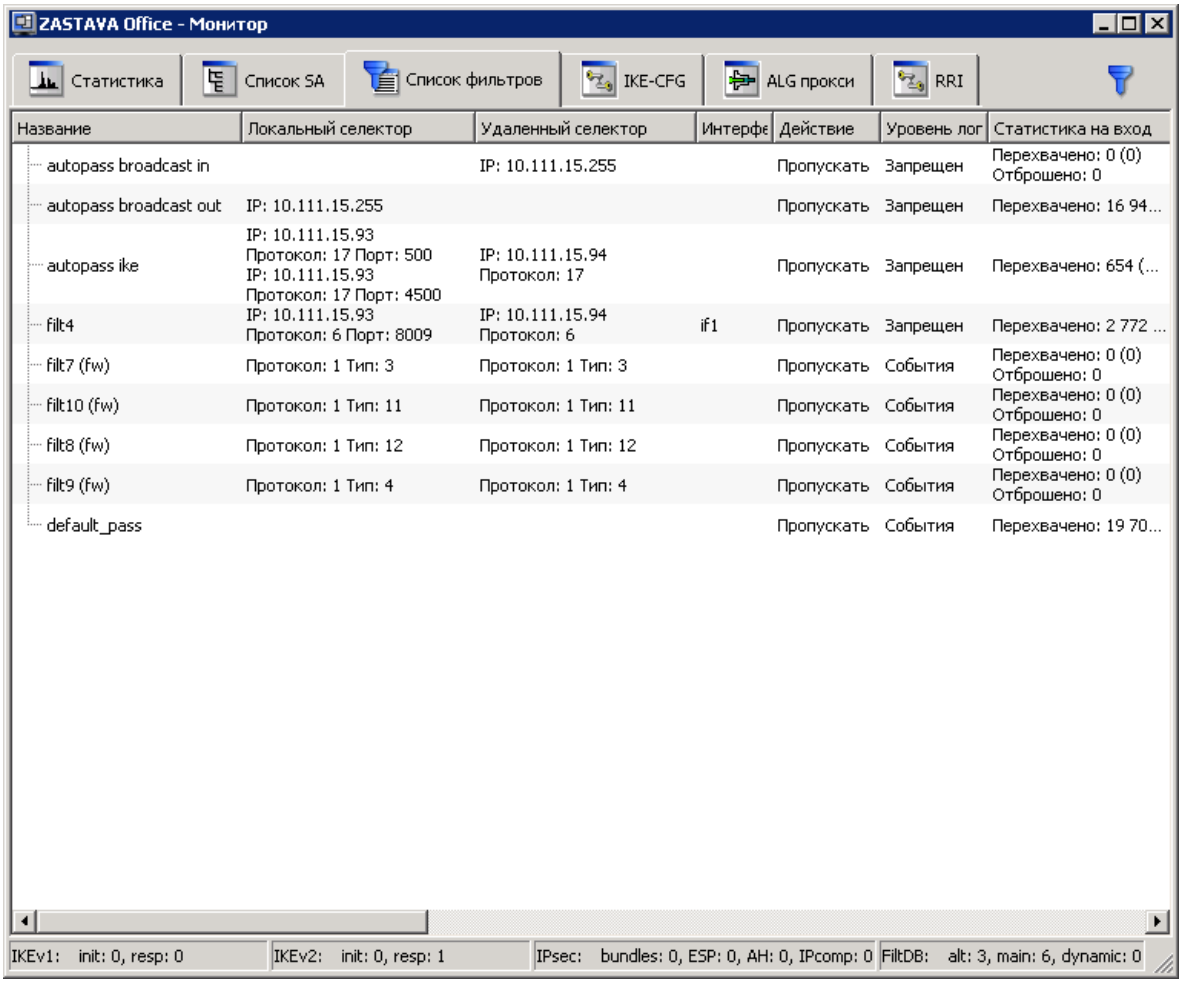

Рисунок 16 – Окно «Монитор», вкладка «Список фильтров»

Основную часть вкладки занимает список фильтров, который включает в себя статистику по параметрам фильтрации (см. Таблица 10).

Таблица 10 – Параметры фильтров

Параметр	Характеристика
Название	Параметр фильтрации по полю «Название»
Локальный селектор	Адрес, протокол и порт локального селектора
Удаленный селектор	Адрес, протокол и порт удаленного селектора
Интерфейс	Интерфейс, на котором установлен фильтр
Действие	Действие для фильтрации

Параметр	Характеристика
Уровень лога	Уровень подробности регистрации событий
Статистика на вход	Статистика входящих пакетов
Статистика на выход	Статистика исходящих пакетов
Входящих пакетов в секунду	Статистика входящих пакетов в секунду
Входящих байт в секунду	Статистика входящих байт в секунду
Исходящих пакетов в секунду	Статистика исходящих пакетов в секунду
Исходящих байтов в секунду	Статистика исходящих байт в секунду
Входящих промахов в кэше	Статистика промахов после проверки входящих пакетов на соответствие с фильтрами в кэше
Исходящих промахов в кэше	Статистика промахов после проверки исходящих пакетов на соответствие с фильтрами в кэше
Входящих промахов в кэше в секунду	Статистика промахов в секунду после проверки входящих пакетов на соответствие с фильтрами в кэше
Исходящих промахов в кэше в секунду	Статистика промахов в секунду после проверки исходящих пакетов на соответствие с фильтрами в кэше
Записей в кэше	Статистика записей в кэше
Фаервольные процедуры	Фаервольные процедуры
Комментарий	Комментарий (например, описание фильтра)

На вкладке «Список фильтров» существует контекстное меню с командами, приведенными в таблице (см. Таблица 11).

Таблица 11 – Команды контекстного меню вкладки «Список фильтров»

Команда	Характеристика
Копировать	Копирует содержимое ячейки, на которой стоит курсор, в буфер обмена
Копировать всю строку	Копирует содержимое текущей строки в буфер обмена
Показать журнал	Открывает текущий журнал

3.3.3.1. Фильтрация

Для задания правил фильтрации следует:

1) Открыть панель фильтров кнопкой  .
2) Нажать кнопку «Добавить правило», появится строка задания правила фильтрации (см. Рисунок 17).
3) Задать правило фильтрации:
   а) Выбрать из первого списка параметр фильтрации (см. Таблица 12).

б) Выбрать из второго списка условие фильтрации.

в) В третьем поле задать или выбрать из списка значение, по которому будет производиться сравнение.

	Для удаления фильтра следует нажать кнопку «Удалить» справа от фильтра.
	Чтобы отключить применение фильтра, следует снять флажок слева от фильтра.

4) При необходимости, добавить еще одно или несколько правил фильтрации, нажав кнопку «Добавить правило».

5) После задания всех требуемых правил фильтрации, нажать кнопку «Применить», в результате в таблице будут отображаться только фильтры, соответствующие заданным правилам.

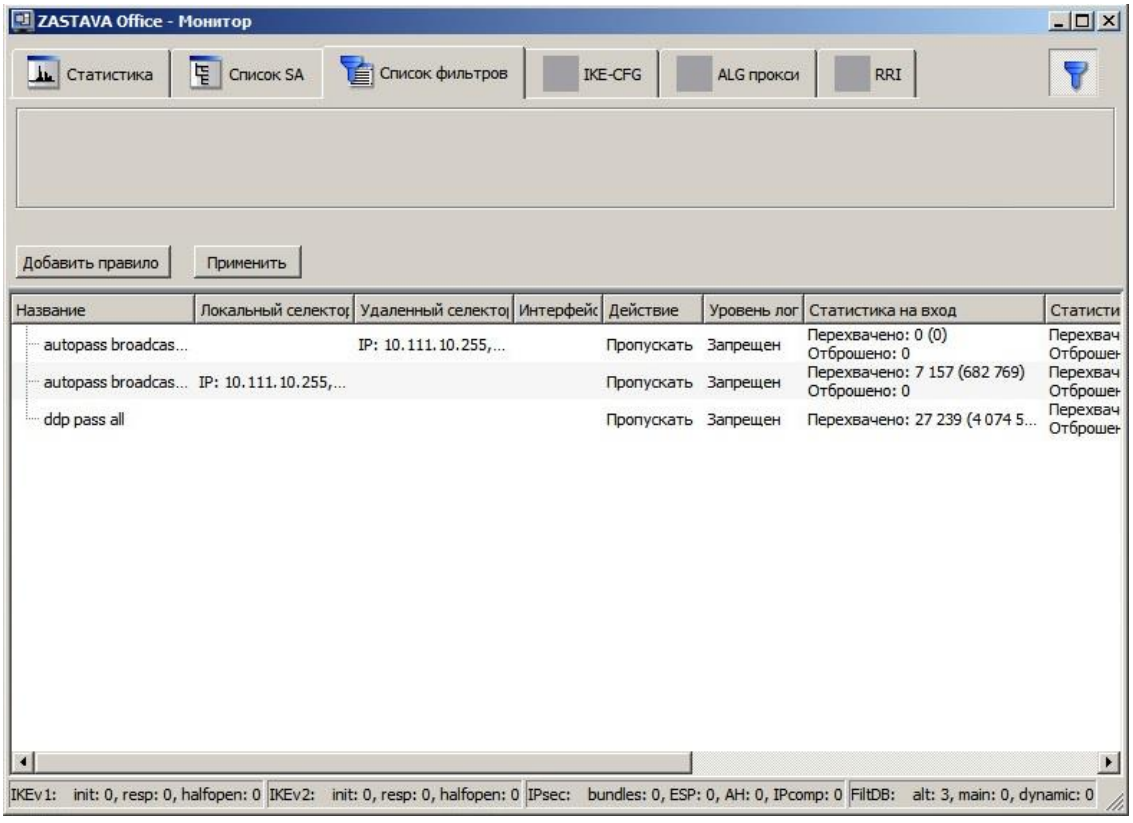

Рисунок 17 – Окно «Монитор», вкладка «Список фильтров». Открыта панель фильтрации

Таблица 12 – Параметры фильтрации

Параметр	Характеристика
Тип	Параметр фильтрации по полю «Тип»
Название	Параметр фильтрации по полю «Название»
Действие	Параметр фильтрации по полю «Действие»
Уровень лога	Параметр фильтрации по полю «Уровень лога»

Параметр	Характеристика
Флаги	Параметр фильтрации по времени жизни
Комментарий	Параметр фильтрации по полю «Комментарий»
Интерфейс	Параметр фильтрации по полю «Интерфейс»
Локальный селектор	Параметр фильтрации по полю «Локальный селектор»
Адрес из локального селектора	Фильтрация поля «Локальный селектор» по IP-адресу
Порт из локального селектора	Фильтрация поля «Локальный селектор» по порту
Удаленный селектор	Параметр фильтрации по полю «Удаленный селектор»
Адрес из удаленного селектора	Фильтрация поля «Удаленный селектор» по IP-адресу
Порт из удаленного селектора	Фильтрация поля «Удаленный селектор» по порту
Входящих пакетов	Фильтрация поля «Входящие пакеты»
Исходящих пакетов	Фильтрация поля «Исходящие пакеты»
Входящих байт	Фильтрация поля «Входящих байт»
Исходящих байт	Фильтрация поля «Исходящих байт»
Входящих байт отброшено	Фильтрация поля «Входящих байт отброшено»
Исходящих байт отброшено	Фильтрация поля «Исходящих байт отброшено»
Входящих промахов в кэше	Фильтрация поля «Входящих промахов в кэше»
Исходящих промахов в кэше	Фильтрация поля «Исходящих промахов в кэше»
Записей в кэше	Фильтрация поля «Записей в кэше»
Фаервольные процедуры	Параметр фильтрации по полю «Фаервольные процедуры»

3.3.4. Вкладка «IKE-CFG»

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

Вкладка «IKE-CFG» позволяет получить информацию об установленных соединениях на основе протокола IKE-CFG (см. Рисунок 18).

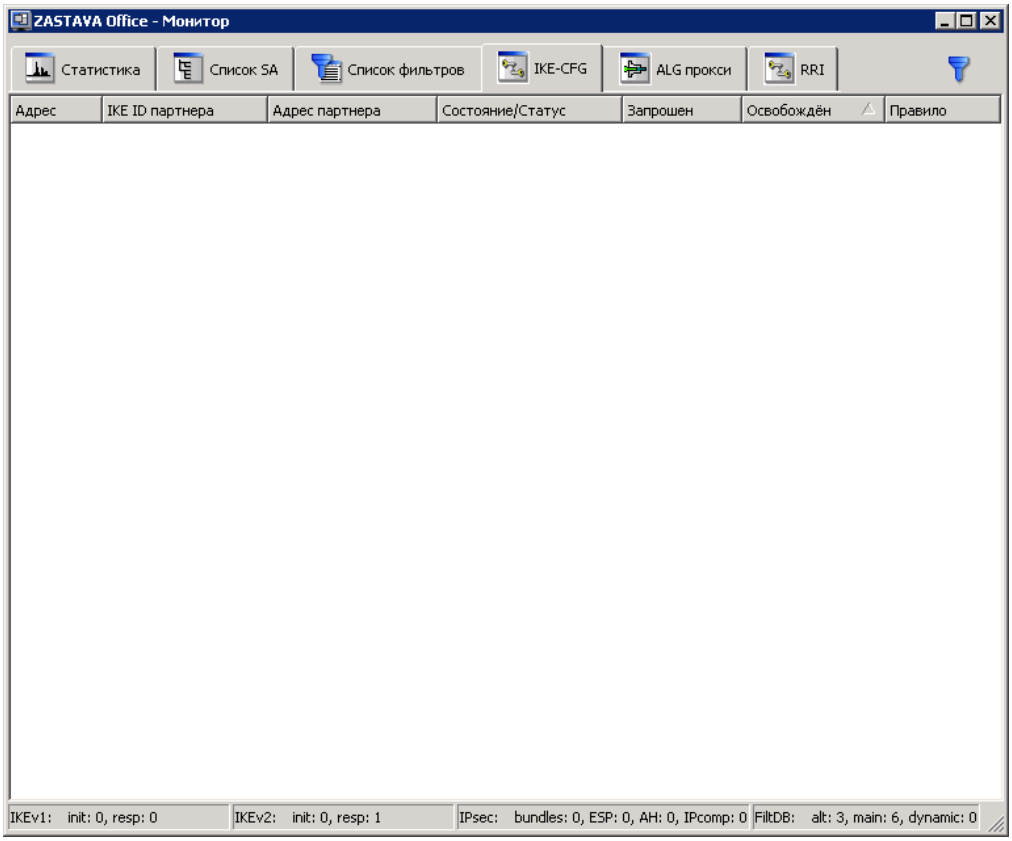

Рисунок 18 – Вкладка «IKE-CFG»

Информация, доступная для просмотра в данной вкладке, представлена в таблице (см. Таблица 13).

Таблица 13 – Вкладка IKE-CFG

Параметр	**Характеристика**
Адрес	Выделенный адрес
Ike idref	Идентификационный номер соединения
IKE ID партнера	IKE ID первой фазы партнера
Адрес партнера	IP-адрес партнера
Состояние/Статус	Текущий статус выделенного адреса
Запрошен	Дата и время запроса адреса
Освобожден	Дата и время освобождения адреса
Правило	Правило IKE CFG

Существует возможность произвести фильтрацию в окне «IKE-CFG», для этого необходимо в правом верхнем углу нажать кнопку «Фильтр», в появившемся окне (см. Рисунок 19) выбрать необходимые параметры фильтрации.

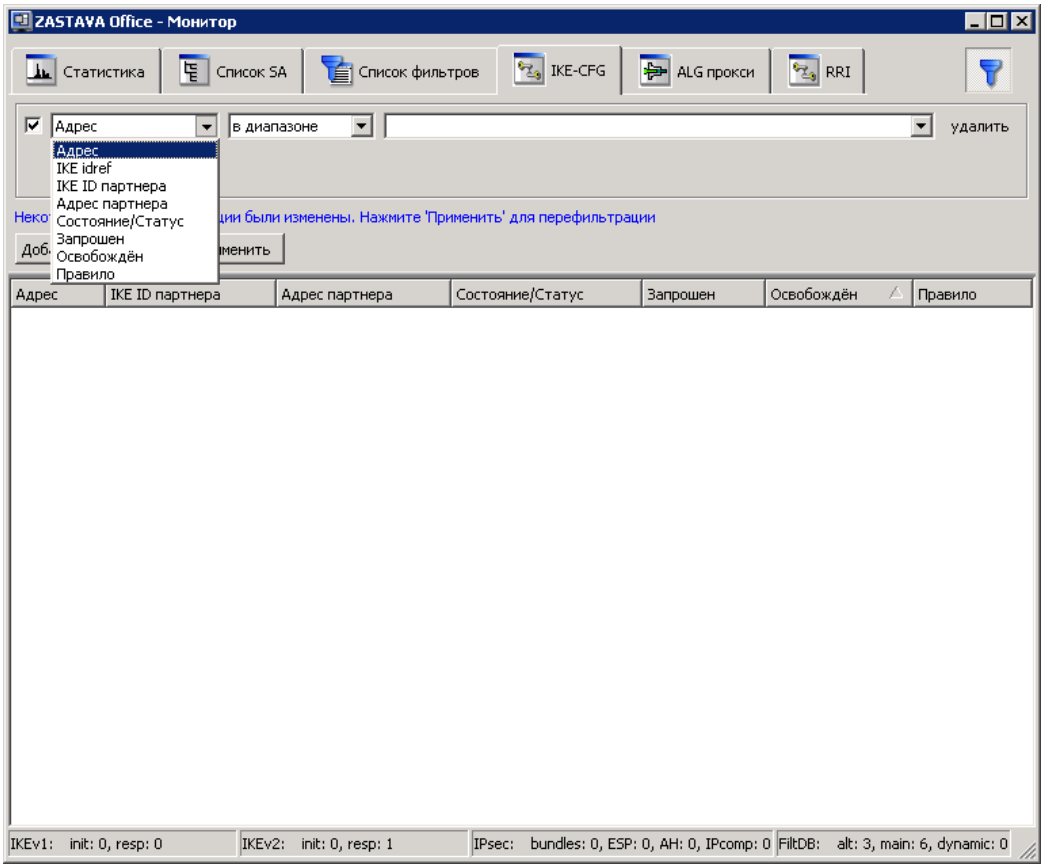

Рисунок 19 – Вкладка «IKE-CFG»

Параметры фильтрации вкладки «IKE-CFG» представлены в таблице (см. Таблица 14).

Таблица 14 – Параметры фильтрации вкладки «IKE-CFG»

Параметр	Характеристика
Адрес	Фильтрация по параметру «Адрес»
Ike idref	Фильтрация по идентификационному номеру соединения
IKE ID партнера	IKE ID первой фазы партнера
Адрес партнера	Фильтрация по параметру «Состояние/Статус»
Состояние	Фильтрация по дате и времени освобождения адреса
Освобожден	Дата и время освобождения адреса
Запрошен	Дата и время запроса адреса
Правило	Правило IKE CFG

После выбора параметра фильтрации и выбора, какую операцию применить, необходимо указать значение, по которому будет производиться сравнение, в крайнем правом поле строки фильтрации, и нажать кнопку «Применить». В таблице будут показаны отфильтрованные события. Количество событий, удовлетворяющих правилу фильтрации, будет показано правее кнопки «Применить».

3.3.5. Вкладка «ALG proxy»

На вкладке «ALG proxy» представлена информация о прокси-серверах, установленных на данном *ЗАСТАВА-Офис* (см. Рисунок 20).

На этом рисунке представлен пример отображения содержимого вкладки «ALG proxy» с запущенным SMTP прокси-сервером.

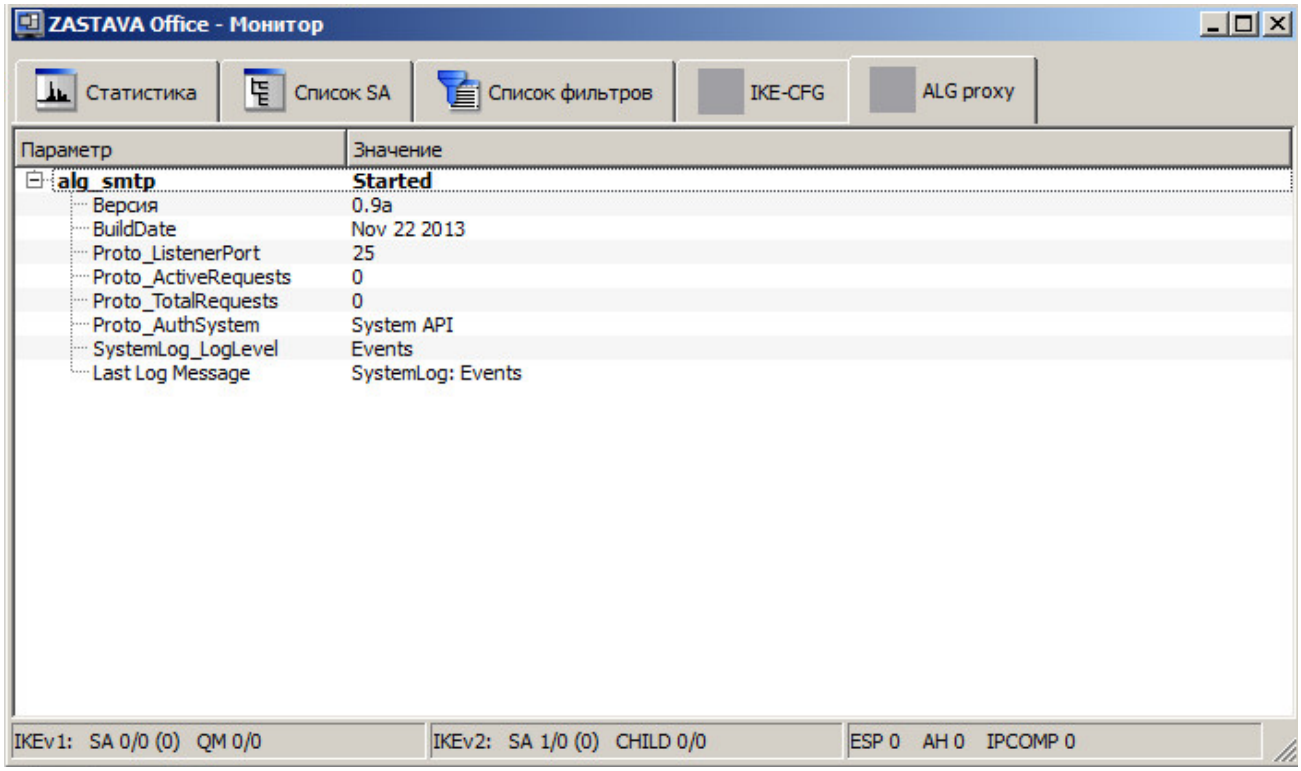

Рисунок 20 – Вкладка «ALG proxy»

3.3.6. Вкладка «RRI» (Reverse Route Injection)

В *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 *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 *ЗАСТАВА-Офис* удаляется.

На вкладке «RRI» представлена информация о маршрутах, установленных на данном *ЗАСТАВА-Офис* (см. Рисунок 21).

Для включения RRI необходимо открыть окно «Прочие настройки», перейти на вкладку «IKE» и поставить флажок в поле «Reverse Route Injection», в поле «Reverse Route

Injection Table Id» задается название таблицы для сохранения информации о маршрутизации (по умолчанию 111). Для просмотра информации о маршрутах, необходимо выполнить команду в консоли (см. п. 5.2.10).

Вкладка RRI отображает связи между топологией VPN и системой маршрутизации. После создания защищенного соединения IPsec SA, в таблицу маршрутизации *ЗАСТАВА-Офис* с включенным RRI автоматически вносится запись о маршруте к удаленной сети партнера или клиенту.

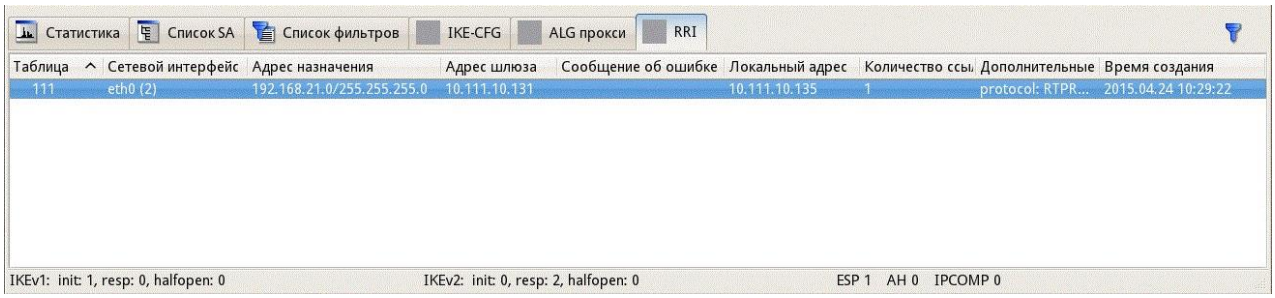

Рисунок 21 – Вкладка «RRI»

При журналировании информации о маршрутизации в столбце «Сообщения об ошибке» могут отображаться информационные сообщения или сообщения об ошибке (см. Таблица 15).

Таблица 15 – Конфликтные ситуации и журналирование маршрутизации при них

N	Ситуация	Поведение ЗАСТАВА-Офис

1.	Строится IPsec SA, если при этом ID партнера второй фазы IKE можно преобразовать в подсеть (содержит диапазон IP-адресов, порты и/или протоколы).	Маршрут RR не добавляется и выдается предупреждение в журнал:
		`LOG_MSG_RRI_NOTADD_FULLRANGE`
		`LOG_MSG_RRI_NOTADD_BADRANGE`
		При наличии портов и протоколов маршрут создается, но с предупреждением в журнал:
		`LOG_MSG_RRI_WARNING_PORTPROTOCOL`

2.	Имеется построенный IPsec SA и в таблицу внесен вычисленный RR по нему. Строится другой IPsec SA и по нему также вычисляется RR. Оба IPsec SA имеют разные локальные ID, но одинаковые ID партнеров. Если при этом отличаются туннельные адреса, то для двух таких SA могут потребоваться разные маршруты, а добавить второй маршрут невозможно.	Маршрут RR создается только для первого из конфликтующих SA, а при создании второго SA в журнал выдается предупреждение: `LOG_MSG_RRI_ADD_FAIL`

N	Ситуация	Поведение ЗАСТАВА-Офис
3.	При создании IPsec SA вычисляется маршрут RR, который вступает в конфликт с существующими маршрутами	Если в таблице есть такой же маршрут (адрес назначения совпадает), маршрут RR не добавляется. В журнал выдается сообщение: `LOG_MSG_RRI_ADD_FAIL`. Если есть более приоритетный маршрут, пересекающийся, но не совпадающий с маршрутом RR, то маршрут RR добавляется в таблицу маршрутизации.
4.	Конфликт с более узкими фильтрами без RRI.	Маршрут создается без учета таких конфликтов, то есть через pass или ipsec фильтр без RRI пакет может уйти не туда.
5.	При построении IPsec SA в транспортном или туннельном режиме, ID партнера совпадает с туннельным адресом. Маршрут будет как бы рекурсивным – адрес назначения совпадает с адресом шлюза.	Маршрут не создается. В журнале фиксируется сообщение: `LOG_MSG_RRI_NOTADD_GATE_EQUAL_TO_DST`

Сообщения протоколирования, при которых не создается маршрут RR для SA описан в таблице (см. Таблица 15), стоит также отметить индикацию других системных событий при которых не создался RR для SA:

- Не получилось получить таблицу маршрутизации:

  LOG_MSG_RRI_SYS_ENUM_ERROR SYSTEM ERROR EVENTS

  rus:RRI\tНе удалось зачитать таблицу маршрутов из системных настроек: %s

  eng:RRI\tFail to read route table from system settings: %s

- Не удалось добавить маршрут в системную таблицу:

  LOG_MSG_RRI_ADD_FAIL SYSTEM ERROR EVENTS

  rus:RRI\tОшибка при добавлении маршрута. Интерфейс: %s (%d), подсеть: %s/%s, шлюз: %s, Таблица %u, локальный адрес: %s. %s

  eng:RRI\tRoute entry add fail. Interface: %s (%d), subnet: %s/%s, gateway: %s, table %u, local ip: %s. %s

Ошибка удаления правила из системной таблицы маршрутизации (эти ошибки не приводят к каким-либо дополнительным действиям кроме выдачи данного сообщения):

LOG_MSG_RRI_DEL_FAIL SYSTEM ERROR EVENTS

rus:RRI\tОшибка при удалении маршрута. Интерфейс: %s (%d), подсеть: %s/%s, шлюз: %s, Таблица %u, локальный адрес: %s, счетчик: %d. %s

eng:RRI\tRoute entry del fail. Interface: %s (%d), subnet: %s/%s, gateway: %s, table %u, local ip: %s, refcount: %d. %s

Добавление нового RR:

LOG_MSG_RRI_ADD_OK SYSTEM NOTICE EVENTS

rus:RRI\tМаршрут добавлен. Интерфейс: %s (%d), подсеть: %s/%s, шлюз: %s, Таблица %u, локальный адрес: %s, счетчик: %d

eng:RRI\tRoute entry add. Interface: %s (%d), subnet: %s/%s, gateway: %s, table %u, local ip: %s, refcount: %d

Удаление RR (сообщение выводится при удалении записи из системной таблицы. То есть, когда удалены все SA, использующие данный маршрут):

LOG_MSG_RRI_DEL_OK SYSTEM NOTICE EVENTS

rus:RRI\tМаршрут удален. Интерфейс: %s (%d), подсеть: %s/%s, шлюз: %s, Таблица %u, локальный адрес: %s, счетчик: %d

eng:RRI\tRoute entry del. Interface: %s (%d), subnet: %s/%s, gateway: %s, table %u, local ip: %s, refcount: %d

3.4. Окно «Сертификаты и ключи»

Сертификаты (включая сертификаты УЦ), предварительно распределенные ключи, СОС регистрируются в *ЗАСТАВА-Офис* через окно «Сертификаты и Ключи». Вызовите это окно, выбрав «Сертификаты» на *Панели управления.*

ЗАСТАВА-Офис поддерживает два типа сертификатов X.509 V3: сертификаты УЦ и сертификаты конечных пользователей. Среди сертификатов конечных пользователей выделяют (с точки зрения данного хоста) персональные сертификаты, прочие сертификаты и промежуточные сертификаты. Ниже описаны особенности этих четырех групп сертификатов:

1. **Доверенный сертификат –** принадлежат доверенным третьим сторонам (организациям), которые занимаются выпуском цифровых сертификатов. При помощи сертификата УЦ можно проверить подлинность любого сертификата, изданного данным УЦ. Сертификаты УЦ могут быть импортированы в *ЗАСТАВА-Офис* с целью проверки подлинности всех сертификатов, присылаемых партнерами по связи в процессе установления защищенных соединений.
2. **Персональный сертификат** – это сертификат, принадлежащий данному компьютеру *ЗАСТАВА-Офис*. Отличительной особенностью является то, что локальный сертификат хранится на токене вместе с соответствующим ему закрытым ключом. Наличие закрытого ключа позволяет *ЗАСТАВА-Офис* осуществлять двустороннюю криптографическую аутентификацию при

установлении соединений с другими хостами защищенной корпоративной сети на основе протоколов IKEv2.

3. **Прочие сертификаты** - это сертификаты, принадлежащие данному *ЗАСТАВА-Офис*. Отличительной особенностью является то, что данные сертификаты выкладываются без соответствующего закрытого ключа и их нельзя отнести к обозначенным типам сертификатов.

4. **Промежуточные сертификаты** - это сертификаты, принадлежащие данному *ЗАСТАВА-Офис*. Отличительной особенностью является то, что это цифровые сертификаты промежуточных УЦ, выданные промежуточным сертифицирующим органом (CA - certification authority).

Предварительно распределенные ключи могут использоваться в *ЗАСТАВА-Офис* в качестве альтернативы использования сертификатов. Для получения более полной информации см. п. 3.4.7.

В окне «Сертификаты и Ключи» Вы можете также создать ЗРС, если вы используете токены, которые поддерживают генерацию ключевой пары. ЗРС можно послать в УЦ, где на его основании будет издан сертификат. Для получения более полной информации см. п 3.4.6. *ЗАСТАВА-Офис* поддерживает СОС. Для получения более полной информации см. п. 3.4.8.

3.4.1. Структура окна «Сертификаты и Ключи»

Чтобы открыть окно «Сертификаты и Ключи» необходимо на *Панель управления* нажать кнопку «Сертификаты». Окно «Сертификаты и Ключи» показывает краткий обзор сертификатов. Окно содержит меню, *Панель инструментов* и вкладки, разделенные по типам сертификатов (см. Рисунок 22).

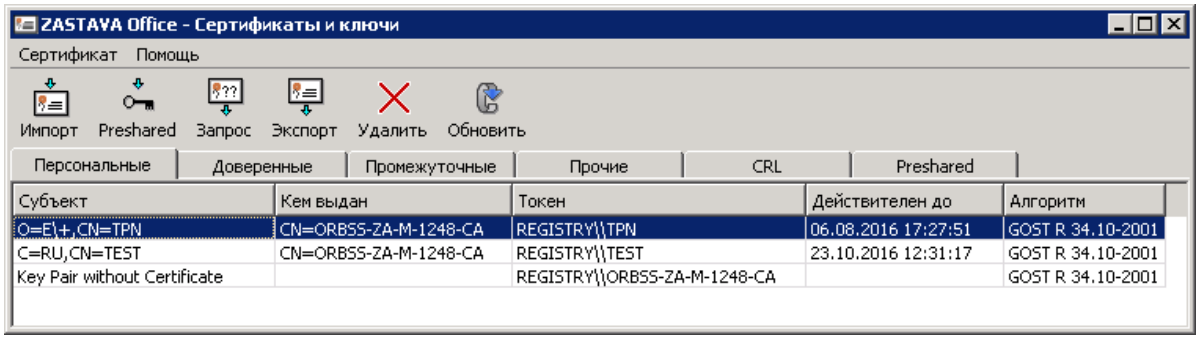

Рисунок 22 – Окно «Сертификаты и Ключи»

3.4.1.1. Вкладки окна «Сертификаты и ключи»

Окно «Сертификаты и ключи» содержит вкладки с зарегистрированными сертификатами, разделенными по типам сертификатов: Персональные, Доверенные, Промежуточные, Прочие, CRL, Preshared. Окно «Сертификаты и ключи» отображает все экземпляры объектов в соответствии с типом выбранной вкладки (см. Таблица 16).

Таблица 16 – Вкладки окна «Сертификаты и ключи» и их содержание

Тип объекта	Характеристика
Персональные	Персональные сертификаты (обычно один), а также ЗРС
Доверенные	Сертификаты УЦ
Промежуточные	Сертификаты между сертификатом УЦ и сертификатами конечных пользователей
Прочие	Все остальные сертификаты, которые нельзя отнести к обозначенным типам сертификатов
CRL	Списки отозванных сертификатов (СОС)
Preshared	Предварительно распределенные ключи

3.4.1.2. Строка меню

Строка меню содержит следующие пункты: «Сертификат», «Помощь». Команды меню представлены в таблице (см. Таблица 17).

Таблица 17 – Команды меню

Команда	Действие
Сертификат	
Импорт сертификата	Запускает мастер «Сертификат/Мастер ключей», который помогает импортировать сертификат, СОС из файловой системы или из токена
Импорт предварительно распределенного ключа	Запускает мастер «Сертификат/Мастер ключей», который помогает импортировать предварительно распределенный ключ (также параметры предварительно распределенного ключа могут быть введены вручную)
Генерация запроса сертификата	Запускает мастер «Сертификат/Мастер ключей», который помогает создавать ЗРС
Экспорт сертификата	Запускает мастер «Сертификат/Мастер ключей», который помогает вам экспортировать любой сертификат
Обновить	Обновляет список объектов, зарегистрированных в базе данных (БД). Если окно «Сертификаты и ключи» открыто, когда активизирована ЛПБ, то сертификаты, полученные в течение IKE-обмена, не показываются автоматически. СОС, полученные автоматически от сервера LDAP, также не показываются. Нажатие кнопки «Обновить» гарантирует то, что Вы видите наиболее свежую информацию о БД.

Команда	Действие
Помощь	
Работа с сертификатами и ключами	Открывает раздел «Справки», поясняющий работу с сертификатами и ключами
Помощь	Вызов общей Справочной системы *ЗАСТАВА-Офис*

3.4.1.3. Панель инструментов окна «Сертификаты и ключи»

Описание кнопок панели инструментов приведено в таблице (см. Таблица 18). Функции этих кнопок соответствуют функциям пунктов меню (см. п. 3.4.1.2).

Таблица 18 – Кнопки панели инструментов окна «Сертификаты и ключи»

Кнопка	Действие
 Импорт	Запускает мастер импорта сертификатов
 Preshared	Запускает мастер импорта предварительно распределенных ключей
 Запрос	Запускает мастер Генерации запроса сертификата
 Экспорт	Запускает мастер Экспорта сертификатов
 Удалить	Удаляет выбранный сертификат
 Обновить	Обновляет список сертификатов, зарегистрированных в базе данных.

3.4.2. Характеристики сертификатов

3.4.2.1. Свойства сертификата

Характеристики сертификата приведены в таблице (см. Таблица 19).

Таблица 19 – Характеристики сертификата

Параметр	Характеристика
Версия	Версия формата сертификата
Серийный номер	Серийный номер сертификата
Издатель	Кем выдан сертификат
Субъект	Содержит отличительное имя субъекта, то есть владельца закрытого

Параметр	Характеристика
	ключа, соответствующего открытому ключу данного сертификата. Субъектом сертификата может выступать Удостоверяющий Центр (УЦ), Регистрационный Центр (РЦ) или конечный субъект
Алгоритм подписи	Алгоритм цифровой подписи сертификата
Алгоритм ключа	Тип открытого ключа (алгоритм цифровой подписи и длина)
Публичный ключ	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 (CDP)	Точки распространения СОС, указанные в данном сертификате. Для каждой точки распространения отображается следующая информация: DP[N] "<DP Value>", CRLI[N] "<Issuer Value>", где: – N – номер точки распространения; – <DP Value>- месторасположение точки, где можно получить СОС; – <Issuer Value>- имя организации, выпустившей СОС
Authority Info Access	Способ доступа к информации УЦ
Issuer Alt Name	Альтернативное имя издателя сертификата
Subject Alt Name	Альтернативное имя субъекта сертификата
Fingerprint (md5)	Хеш-сумма сертификата, вычисляемая по алгоритму md5
Fingerprint (sha1)	Хеш-сумма сертификата, вычисляемая по алгоритму sha1

Если в строке DN (поля «Владелец», «Издатель») присутствуют национальные символы, то для корректного отображения в графическом интерфейсе они должны быть заданы (в теле сертификата) в кодировке UTF-8 (см. RFC 2459, RFC 3280).

3.4.2.2. Свойства Запроса на Регистрацию Сертификата

Характеристики ЗРС приведены в таблице (см. Таблица 20).

Таблица 20 – Характеристики ЗРС

Параметр	Характеристика
Устройство	Устройство, на котором будет сохранены сертификат и ключи
Алгоритм	Тип открытого ключа (алгоритм цифровой подписи)

Параметр	Характеристика
Длина ключа	Тип открытого ключа (длина)
Хэш-алгоритм	Алгоритм хеширования
Имя владельца	Информацию о владельце сертификата
Код страны	Код страны
Организация	Наименование организации
Подразделение	Наименование подразделения
Название	Наименование файла сертификата
Альтернативное имя владельца	Характеризует издателя сертификата
IP-адрес	IP-адрес владельца
DNS	DNS
E-mail	Адрес электронной почты владельца
Флажок «Пометить закрытый ключ как экспортируемый»	Закрытый ключ сертификата помечается как экспортируемый

3.4.2.3. Состав предварительно распределенных ключей

Состав предварительно распределенных ключей приведен в таблице (см. Таблица 21).

Таблица 21 – Состав предварительно распределенных ключей

Параметр	Характеристика
Устройство	Устройство, на котором будут сохранены ключи
Имя	Имя предварительно распределенного ключа (назначенное пользователем)
Значение	Алфавитно-цифровое значение предварительно распределенного ключа
Шестнадцатеричное значение	Шестнадцатеричная трансляция алфавитно-цифрового значения предварительно распределенного ключа

3.4.2.4. Состав CRL (Список Отозванных Сертификатов)

Отображается следующая информация о СОС в окне «Сертификаты и ключи» (см. Таблица 22).

Таблица 22 – Информация о СОС

Параметр	Характеристика
Кем выдан	Имя УЦ, который издал данный сертификат
Токен	Устройство, на котором будет сохранен СОС

Параметр	Характеристика
Последнее обновление	Дата и время издания CRL (дата его последнего обновления УЦ), время задано по Гринвичу (GMT)
Следующее обновление	Дата и время очередного планового обновления СОС УЦ, время по GMT. По истечении данной даты/времени СОС будет считаться недействительным.
Алгоритм	Тип открытого ключа (алгоритм цифровой подписи)

3.4.3. Генерация сертификатов

Для генерирования сертификатов могут применяться различные PKI-продукты третьих производителей. ЛПБ для *ЗАСТАВА-Офис* формируются при помощи ЦУП. Для получения дополнительной информации об этих продуктах нужно смотреть соответствующую документацию и встроенные справочные системы продуктов.

Если вы используете токены, которые поддерживают генерацию ключевой пары, создайте ЗРС *ЗАСТАВА-Офис*, как описано в п. 3.4.6.1. ЗРС будет создан и сохранен в *ЗАСТАВА-Офис* вместе с соответствующим личным ключом, который генерируется в момент создания ЗРС. Отправьте созданный запрос в УЦ (в зависимости от требований УЦ используйте электронную почту, веб-браузер или другие средства). После получения сертификата из УЦ импортируйте его в *ЗАСТАВА-Офис*, как описано в п. 3.4.4. После того, как сертификат будет импортирован, он заменит собой соответствующий ЗРС в окне «Сертификаты и ключи» *ЗАСТАВА-Офис* и будет автоматически связан со своим закрытым ключом.

3.4.4. Регистрация и удаление сертификата

3.4.4.1. Регистрация сертификата

Вы можете регистрировать два типа X.509 сертификатов в *ЗАСТАВА-Офис*: Доверенные и Персональные. Для получения информации о типах сертификатов см п. 3.4.1.1.

Чтобы зарегистрировать новый сертификат (Доверенные и Персональные) в БД *ЗАСТАВА-Офис* необходимо сделать следующее:

1) Нажать кнопку  «Импорт» или «Импорт сертификата» из меню «Сертификат». Запустится программный Мастер.

2) В появившемся окне выбрать необходимый для установки сертификат и нажать кнопку «Открыть» (см. Рисунок 23).

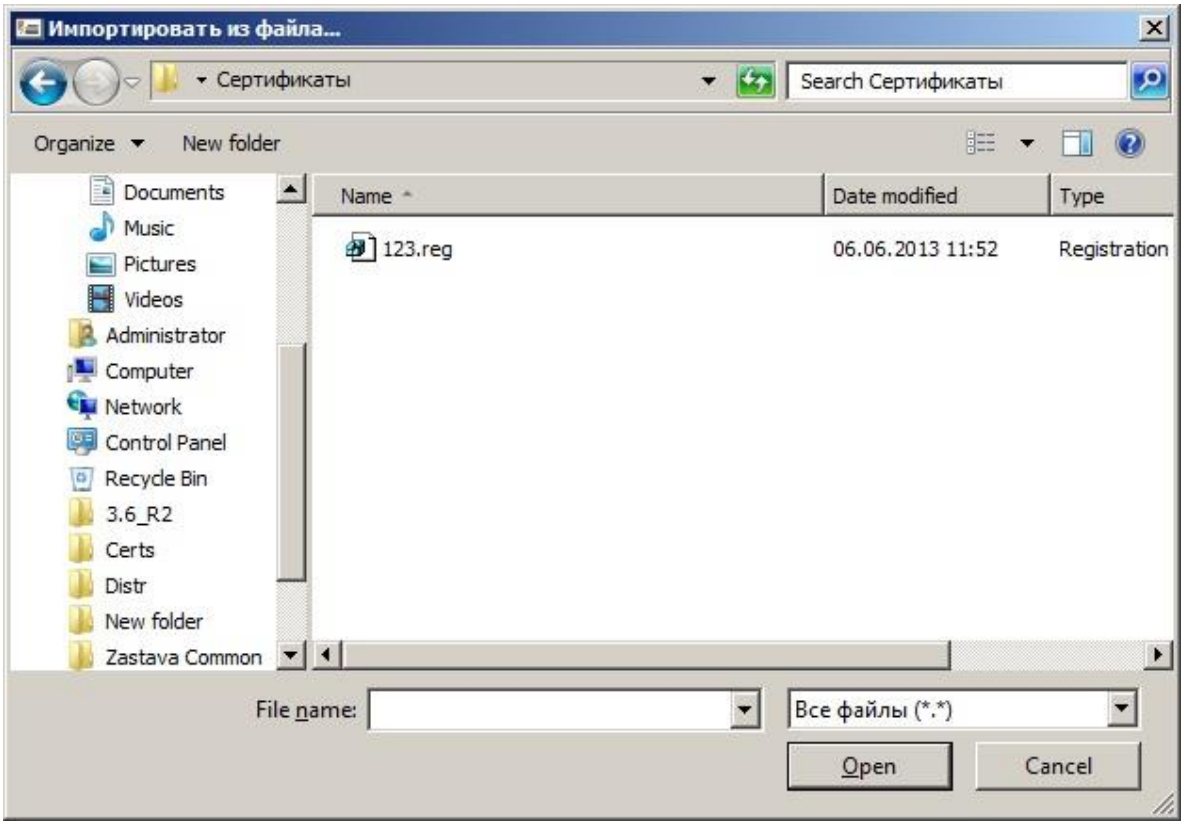

Рисунок 23 – Выбор импортированного объекта

3) Выбрать необходимый «Режим импорта» сертификата, например «Импортировать» (см. Рисунок 24) либо оставить режим импорта, выбранный по умолчанию и нажать кнопку «Далее».

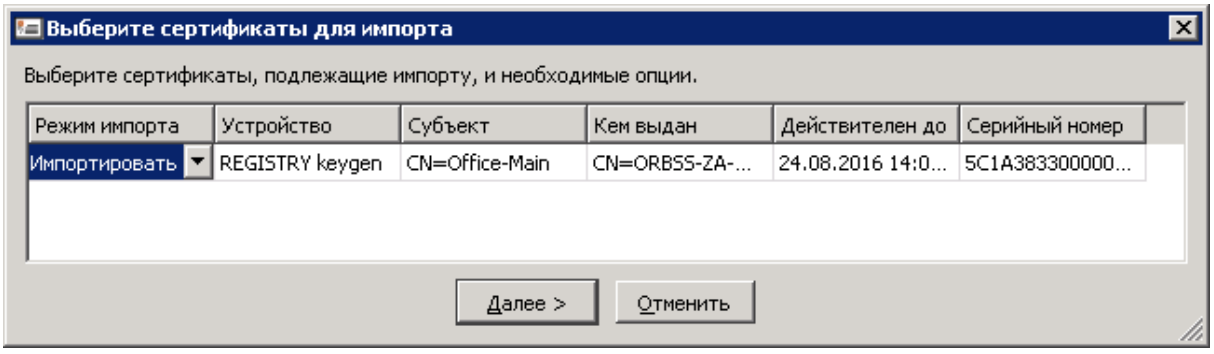

Рисунок 24 – Выбор режима импорта сертификата

4) При успешном импортировании появится индикатор  (см. Рисунок 25). Теперь Мастер сертификатов показывает импортированный сертификат, необходимо нажать кнопку «Готово».

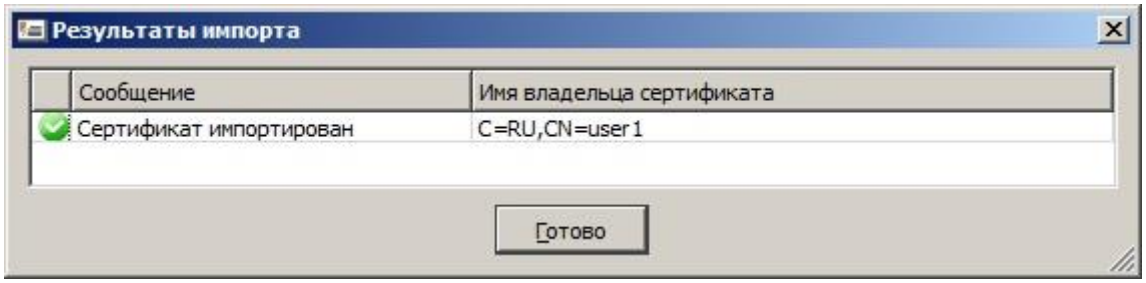

Рисунок 25 – Окно результата импортирования сертификата

5) Зарегистрированный сертификат теперь включен в таблицу окна «Сертификаты и Ключи».

Перед чтением сертификата из файла удостовериться в том, что ОС настроена для показа файлов всех типов.

6) При импорте одного или более сертификатов из файла в формате PKCS#12, необходимо ввести пароль для доступа к этому файлу. В некоторых случаях на данном этапе необходимо вводить PIN-код токена, на котором хранится контейнер с сертификатом(-ами). Мастер теперь показывает сертификат, который Вы собираетесь зарегистрировать:

   – Если Вы регистрируете сертификат УЦ, нужно в поле «Режим импорта» (см. Рисунок 26**)** назначить этому сертификату соответствующий статус - «Доверенный»**.** После чего нажать кнопку «Далее».

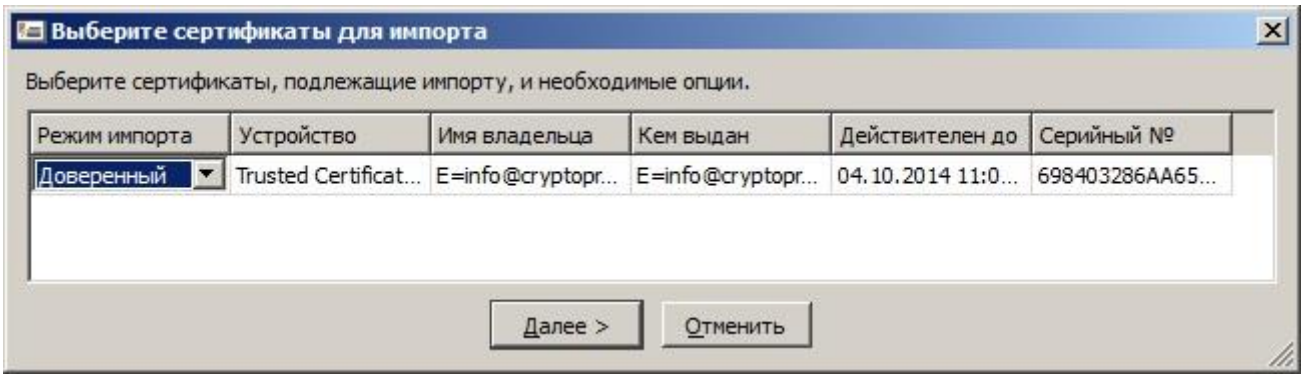

Рисунок 26 – Выбор режима импорта сертификата для регистрации Доверенного сертификата

   – Необходимо ввести PIN-код токена (см. Рисунок 27), в котором будет содержаться сертификат. После ввода PIN-кода нужно нажать кнопку «Готово».

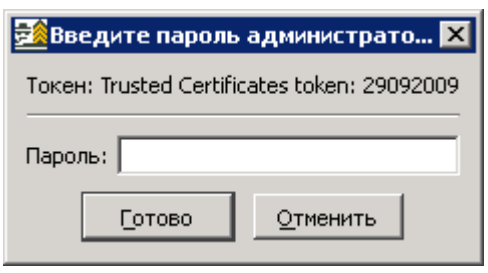

Рисунок 27 – Ввод пароля токена

	Если сертификат УЦ был получен через незащищённый канал (например, по электронной почте) и Вы хотите сохранить его, как «Доверенный», следует 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 1, которая отображается в полях «Fingerprint» в таблице сертификатов *ЗАСТАВА-Офис*. Если сигнатуры не совпадают, немедленно удалите сертификат из *ЗАСТАВА-Офис*.
	Режим импорта «Доверенный» отображается только для сертификатов УЦ. Персональным сертификатам автоматически назначается статус «Доверенный» (если сертификат имеет закрытый ключ, этому сертификату доверяют по умолчанию). Промежуточные сертификаты не могут сохраняться со статусом «Доверенный»; они всегда проверяются по цепочке доверия.
	При импорте доверенного сертификата необходимо вводить пароль администратора, установленный для токена.
	Если открыта сессия связи с токеном, в окне «Сертификаты и ключи» автоматически отображает объекты сертификата, содержащиеся на токене. Все эти сертификаты имеют статус «Доверяемый». Вы можете сохранять сертификат УЦ как «Доверяемый». Сертификаты партнёров по связи, импортированные из токенов, будут всегда проверяться по цепочке доверия.

– Нажать кнопку «Готово». Зарегистрированный сертификат теперь включен в таблицу с зарегистрированными сертификатами окна «Сертификаты и Ключи».

	Чтобы создать локальный сертификат при помощи внешнего УЦ надо создать ЗРС, см. п. 3.4.6.1. ЗРС будет создан и сохранён в *ЗАСТАВА-Офис* вместе с соответствующим личным ключом (он генерируется одновременно с созданием ЗРС). Перешлите созданный ЗРС в УЦ. Когда Вы будете импортировать сертификат, полученный из УЦ, в *ЗАСТАВА-Офис*, этот сертификат заменит соответствующий ЗРС и будет автоматически связан с личным ключом.

3.4.4.2. Удаление сертификата

Для удаления сертификата из *ЗАСТАВА-Офис* следует:

1) Выделить сертификат, который требуется удалить;
2) Нажать на *Панели инструментов* кнопку «Удалить»;
3) В появившемся запросе на удаление нажать кнопку «Да»;
4) Ввести пароль. Сертификат будет удален из *ЗАСТАВА-Офис*.

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

3.4.5. Экспорт сертификата

Для того чтобы выполнить процедуру экспорта сертификата необходимо:

– Выбрать требуемый сертификат в окне «Сертификаты и ключи».
– Нажать кнопку  «Экспорт» или выбрать команду меню «Сертификат» → «Экспорт сертификата». Запустится программный Мастер.
– В появившемся окне выбрать формат экспортируемого сертификата (см. Рисунок 28). Ввести пароль на ключевую информацию, если сертификат экспортируется в PKCS #12 формате. Нажать кнопку «Готово». При необходимости поставить флаг в поле «По возможности включить все сертификаты из иерархии».
– В появившемся окне выбрать необходимый для сохранения сертификата путь и нажать кнопку «Сохранить». Появится информационное окно с сообщением о результатах экспорта.

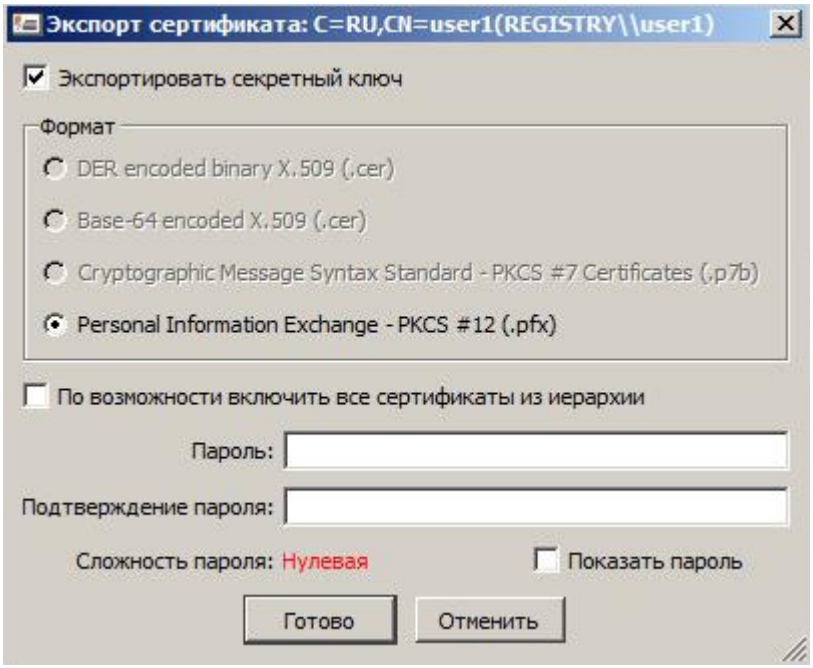

Рисунок 28 – Параметры экспорта сертификата

3.4.6. Запросы на Регистрацию Сертификата

Существует несколько способов получить локальный сертификат для *ЗАСТАВА-Офис*. Например, можно импортировать сертификат вместе с его личным ключом из файловой системы, как описано в п. 3.4.4.1. Кроме того, можно зарегистрировать токен, содержащий сертификат с его личным ключом, как описано в п. 3.6.1.

Также можно создать ЗРС в окне «Сертификаты и Ключи». Созданный запрос отправляется затем в УЦ, который преобразовывает полученный запрос в сертификат.

3.4.6.1. Создание Запроса на Регистрацию Сертификата

Для того чтобы создать ЗРС, нужно выполнить следующие операции:

1) Нажать кнопку  «Запрос» или выбрать команду меню «Сертификат» → «Генерация запроса сертификата».

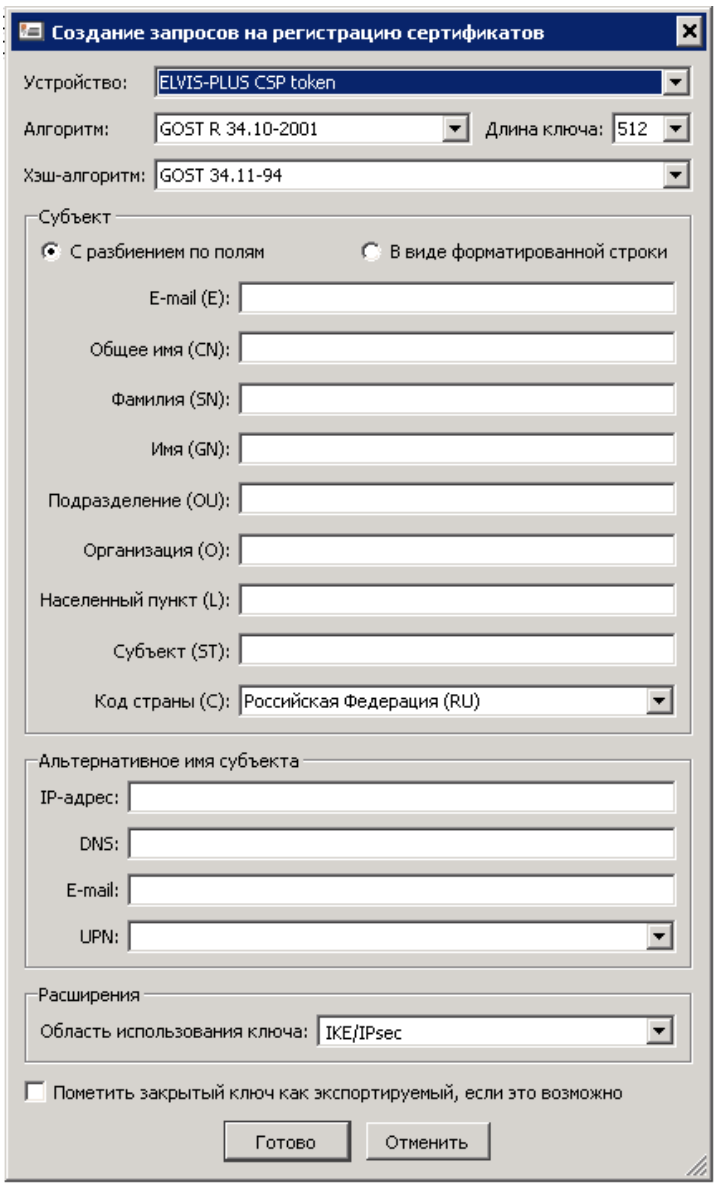

Рисунок 29 – Ввод информации для создания ЗРС

2) В появившемся окне «Создание запросов на регистрацию сертификатов» заполнить необходимые поля (см. Рисунок 29):
   - Выбрать устройство, на котором будет храниться закрытый ключ;
   - Выбрать алгоритм шифрования;
   - Задать длину ключа;
   - Выбрать хэш-алгоритм;

– Ввести информацию о владельце сертификата, заполнив соответствующие поля раздела «Субъект». Информацию можно задавать либо с разбиением по полям, либо в виде форматированной строки (см. п. 3.4.6.1.1 на стр. 68). Обязательным является «Код страны», кроме того, необходимо заполнить как минимум одно из остальных полей в соответствии с их названием.

  Незаполненные поля не будут включены в ЗРС.

– При необходимости, заполнить поля в разделе «Альтернативное имя субъекта» (IP-адрес, адрес электронной почты, DNS-имя, UPN). Эти поля являются необязательными;
– В разделе «Расширения» выбрать область использования ключа;
– При необходимости, установить флажок «Пометить закрытый ключ как экспортируемый, если это возможно».

3) Нажать кнопку «Готово».
4) По запросу ввести PIN-код (пароль) устройства на котором генерируется ключевая пара.
5) Появится окно со сформированным запросом на получение сертификата (Рисунок 30). ЗРС и соответствующий ему закрытый ключ будут сохранены в *ЗАСТАВА-Офис* – в таблице появится соответствующая строка с именем субъекта «Key Pair without Certificate».

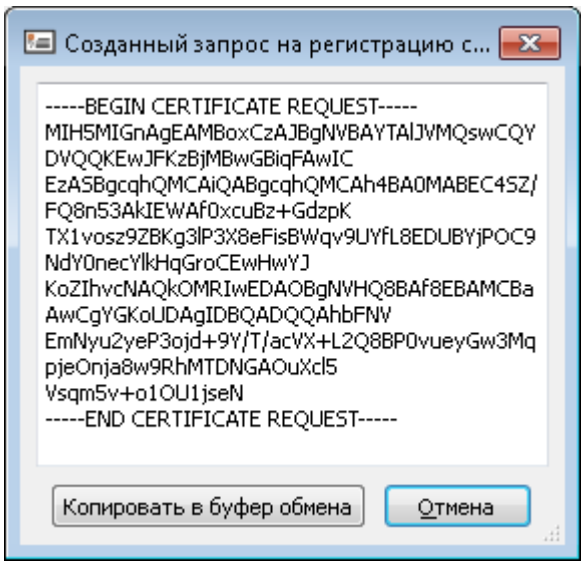

Рисунок 30 – Созданный запрос на регистрацию сертификата

6) Скопировать текст запроса в буфер обмена, нажав кнопку «Копировать в буфер обмена».

7) Отправить созданный запрос в УЦ (с помощью веб-браузера, электронной почты или других средств).
8) После получения сертификата от УЦ, его следует импортировать в *ЗАСТАВА-Офис,* как это описано в п. 3.4.4.1. После того, как сертификат будет импортирован, он заменит собой соответствующий ЗРС в окне «Сертификаты и ключи» *ЗАСТАВА-Офис* и будет автоматически связан со своим закрытым ключом.

3.4.6.1.1. Формат строки Индивидуального Имени (DN)

При использовании Уникального Имени (DN) в ЗРС необходимо ввести значения DN в формате, описанном в этом пункте. Используйте только те значения, которые необходимы для создания ЗРС.

```
attr1=attr1_value,attr2=attr2_value,...,
```

где: `attrN=attrN_value,`

`attr1,attr2,...,attrN – имена атрибутов DN;`

`attr1_value,attr2_value,...,attrN_value_-` значения соответствующих атрибутов.

Например, строка DN может выглядеть следующим образом:

```
O=Test,OU= Marketing,CN= Ivanov
```

Типы атрибутов, обычно использующихся в строках DN, представлены в таблице (см. Таблица 23).

Таблица 23 – Типы атрибутов

Типы атрибутов	Наименование	Расшифровка
CN	Subject Common Name	Общее имя*
C	Subject Country	Страна
L	Subject Locality	Район расположения
ST	Subject State or Province	Область расположения
O	Subject Organization	Название организации
OU	Subject Organizational Unit	Название отдела организации
SN	Subject Surname	Фамилия
GN	Subject Given Name	Имя
I	Subject Initials	Инициалы
T	Subject Title Unit	Должность
Примечание * – Все перечисленные атрибуты относятся к владельцу сертификата (поле «Субьект»)		

При определении значений атрибутов DN рекомендуется использовать только буквы латинского алфавита и цифры. Некоторые символы имеют специальное значение в строке DN и должны писаться с обратной наклонной чертой перед ними. Например, в названии отдела (OU) можно использовать запятые следующим образом:

```
O=Test,OU=Marketing\, Management, CN=Ivanov
```

Любой специальный символ можно заменить обратной наклонной чертой и двумя шестнадцатеричными цифрами, которые представляют собой код символа.

Например, строка DN, в которой указан перевод каретки, выглядит так:

```
O=Test,CN=Ivanov\0DPetr
```

Возможно также добавление произвольных атрибутов в строку DN, используя «точечно-десятичный» формат типа атрибута,

Например, `1.2.840.113549.1.9.1=ivanov@test.com`

Порядок размещения атрибутов DN в сертификате зависит от порядка размещения атрибутов в запросе и от УЦ, выдающего сертификат. Некоторые ВЧС-агенты третьих производителей распознают сертификаты удаленных партнеров по связи, только если атрибуты DN расположены в определенном порядке (например, продукты Check Point могут работать только с теми Индивидуальными именами, у которых атрибут CN расположен в конце строки). После получения сертификата от УЦ надо убедиться в том, что *ЗАСТАВА-Офис* способен корректно взаимодействовать со всеми видами *Агентов*, необходимыми для работы.

В компонентах *ПК «VPN/FW «ЗАСТАВА» версия 6* атрибуты DN сертификатов расположены в том же порядке, в котором они указаны в сертификате. Во многих аналогичных продуктах третьих производителей используется реверсивное отображение атрибутов DN.

Если в строке DN (поля «Владелец», «Издатель») присутствуют национальные символы, то для корректного отображения в графическом интерфейсе они должны быть заданы (в теле сертификата) в кодировке UTF-8 (см. RFC 2459, RFC 3280).

3.4.6.2. Удаление Запроса на Регистрацию Сертификата

Для того чтобы удалить ЗРС из *ЗАСТАВА-Офис* надо выделить ЗРС, который нужно удалить в окне «Сертификаты и ключи», нажать на панели инструментов окна «Сертификаты и ключи» кнопку «Удалить». Запрос будет удален из *ЗАСТАВА-Офис*.

3.4.7. Предварительно Распределенные Ключи

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 партнером заранее). Если ключи не совпадают, защищённое подключение не будет установлено.

3.4.7.1. Регистрация предварительно распределенного ключа

Чтобы зарегистрировать предварительно распределенный ключ в *ЗАСТАВА-Офис* необходимо сделать следующее:

– Нажать кнопку  «Preshared» или «Импорт сертификата» из меню «Сертификат». Запустится программный Мастер.
– В появившемся окне «Preshared Key» заполнить необходимые поля (см. Рисунок 31).
– В появившемся окне ввести уникальное имя ключа в поле «Имя ключа». Это имя будет использовано в качестве идентификатора в ЛПБ.

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

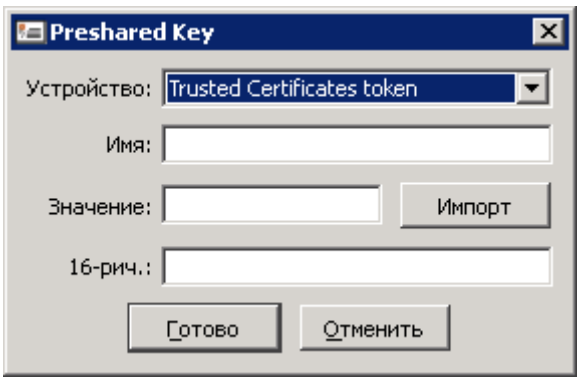

Рисунок 31 – Ввод параметров предварительно распределенного ключа

– Ввести значение ключа в поле «Значение» или «16-рич.» или нажать кнопку «Импортировать значение ключа» и указать файл со значением предварительно распределенного ключа.
– Теперь Мастер ключей показывает предварительно распределенный ключ, который Вы собираетесь регистрировать. Нажать кнопку «Готово». Зарегистрированный предварительно распределенный ключ теперь включен в таблицу вкладки «Preshared Key» окна «Сертификаты и Ключи».

3.4.7.2. Удаление предварительно распределенного ключа

Для удаления предварительно распределенного ключа из *ЗАСТАВА-Офис* надо выделить ключ, который требуется удалить, в таблице вкладки «Preshared Key» окна «Сертификаты и Ключи», нажать на панели инструментов окна «Сертификаты и ключи» кнопку «Удалить». Ключ будет удален из таблицы и из *ЗАСТАВА-Офис*.

3.4.8. Списки Отозванных Сертификатов

COC(CRL) – это список отозванных сертификатов, которые с данного момента времени не имеют силы и не должны использоваться для формирования Защищенных Соединений (SA) в течение сеанса безопасного соединения.

Каждый COC выпускается определенным УЦ и содержит только сертификаты, аннулированные данным УЦ. Любой COC имеет силу в течение периода времени, указанного в нем: с даты (и времени) создания COC до даты (и времени) следующей намеченной коррекции. Значения времени заданы по Гринвичу. Ваш часовой пояс будет принят во внимание при вычислении периода действия COC.

COC может быть импортирован в *ЗАСТАВА-Офис* автоматически или вручную.

Проверка сертификатов управляется локальными настройками *ЗАСТАВА-Офис.* Доступны три варианта:

- Обработка CRL выключена
- Обработка CRL включена, отзывать, если CRL недоступен
- Обработка CRL включена, не отзывать, если CRL недоступен

Локальные настройки *ЗАСТАВА-Офис* описаны в разделе 3.8 Окно «Прочие настройки».

3.4.8.1. Обработка COC

При проверке сертификата *ЗАСТАВА-Офис* путем просмотра COC удостоверяется в том, что сертификат не отозван.

Если в локальных настройках *ЗАСТАВА-Офис* выбрана опция «Обработка CRL выключена», то проверка на наличие сертификата и всей цепочки в списке отозванных не производится.

Если выбрана опция «Обработка CRL включена, отзывать, если CRL недоступен», то сертификат будет признан отозванным, если COC не найден. Соединение с использованием такого сертификата не будет установлено.

Если выбрана опция «Обработка CRL включена, не отзывать, если CRL недоступен», то сертификат будет признан действительным, даже если СОС не найден. Установление соединения с использованием такого сертификата возможно.

Для поиска СОС используется следующий алгоритм:

– Если в сертификате не указан CDP, то поиск СОС и проверка сертификата не производится;
– Если CDP указан, то *ЗАСТАВА-Офис* проверяет, был ли загружен СОС ранее. Если СОС не был загружен, или период его действительности истек, то выполняется загрузка с источника, указанного в CDP. Если загрузить СОС не удалось, то выполняется поиск СОС среди импортированных на токены.

3.4.9. Проверка сертификата

Вы можете проверить сертификат, зарегистрированный в *ЗАСТАВА-Офис*, просматривая его *цепочку доверия* (т. е. список УЦ, подтверждающих подлинность сертификата). Цепочку сертификата можно просмотреть в окне «Параметры сертификата», выбрав требуемый для проверки сертификат, и, нажав на нем дважды левой кнопкой мыши. В верхней части окна «Параметры сертификата» будет показана *Иерархия сертификата.*

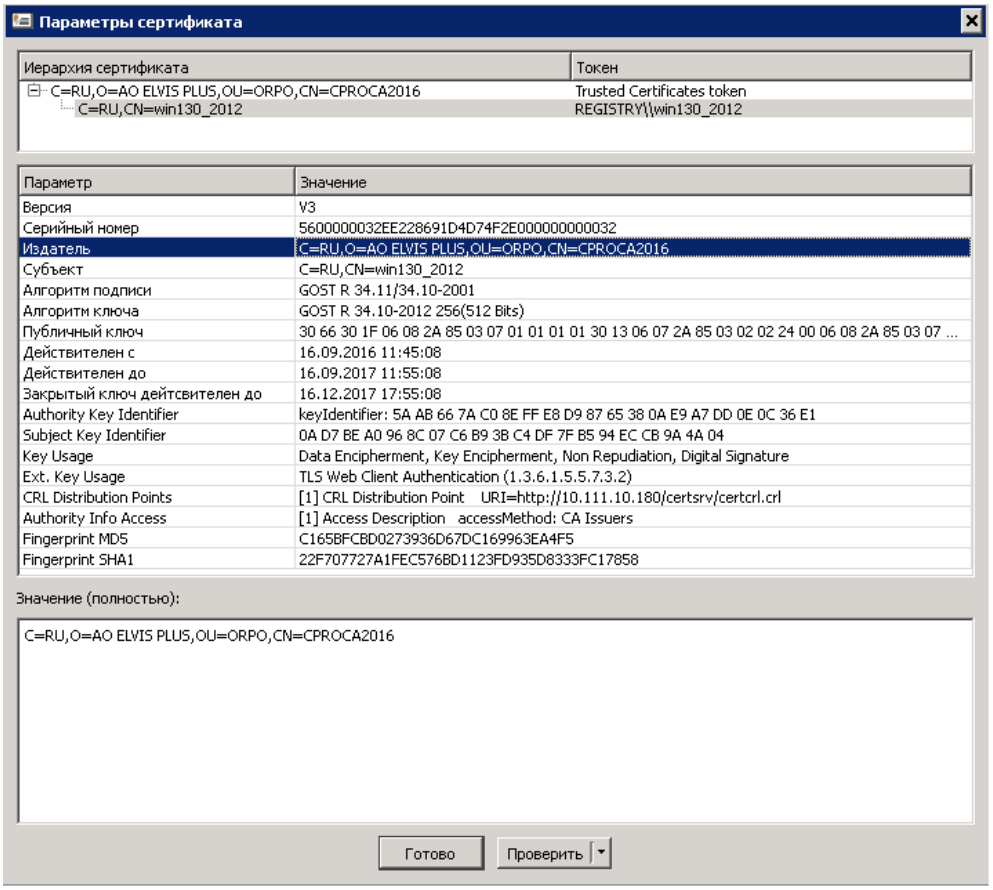

Рисунок 32 – Окно «Параметры сертификата»

Кнопка «Проверить» внизу окна «Параметры сертификата» позволяет проверить сертификат на его актуальность по периоду действительности и присутствию в списке отозванный сертификатов. Настройки проверки по СОС задаются нажатием на символ «стрелка вниз» на кнопке «Проверить» и выбором соответствующего пункта из выпадающего меню.

Убедитесь в том, что на компьютере правильно установлены дата, время и настройки часового пояса. Неправильная установка данных параметров может привести к тому, что сертификаты или CRL будут помечены как недействительные.

3.5. Окно «Управление политиками»

Окно «Управление политиками» предназначено для редактирования списка ЛПБ и установки опций ЛПБ (см. Рисунок 33). Для получения информации об ЛПБ см. п. 3.5.2. Для получения информации об особенностях создания ЛПБ см. п. 3.5.5.

ЛПБ является текстовым файлом, описывающим правила, которые определяют, как *ЗАСТАВА-Офис* связывается с другими объектами в защищённой среде.

ЛПБ может быть добавлена, активирована и просмотрена.

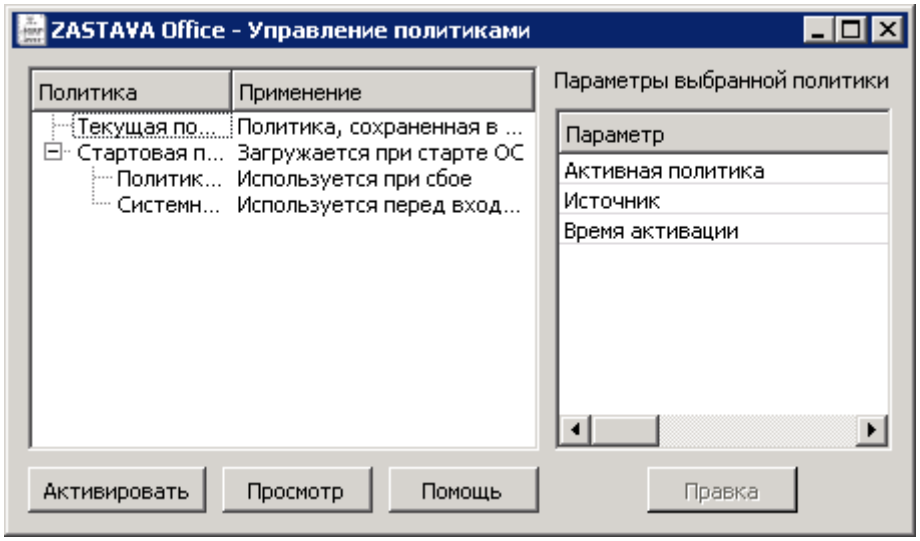

Рисунок 33 – Окно «Управление политиками»

3.5.1. Структура окна «Управление политиками»

Окно «Управление политиками» состоит из двух полей:

– Поле с деревом политик;

– Параметры выбранной политики.

Поле «Политика» содержит дерево существующих политик. При выделении политики в дереве политик в поле «Параметры выбранной политики» отображаются параметры

политики. Поле «Политика» содержит также кнопки «Активировать», «Просмотр» и «Помощь». Для стартовой политики также доступна кнопка «Правка» для редактирования параметров политики.

3.5.2. Типы политик

В поле «Политика» существуют следующие типы политик:

- Текущая – политика, сохраняемая в драйвере *Агента.*
- Стартовая – политика, загружаемая при старте ОС:
  - Политика Драйвера по умолчанию (DDP) – политика, загружаемая при сбое;
  - Системная – политика, используемая перед входом и после выхода пользователя.

3.5.3. Параметры политик *ЗАСТАВА-Офис*

3.5.3.1. Системная ЛПБ

Системная политика может быть получена из файла, с сервера или отсутствовать.

Для изменения параметров системной политики необходимо на системной политике в поле «Политика» нажать дважды левой кнопкой мыши и выбрать необходимые параметры в окне «Опции политики» (см. Рисунок 34).

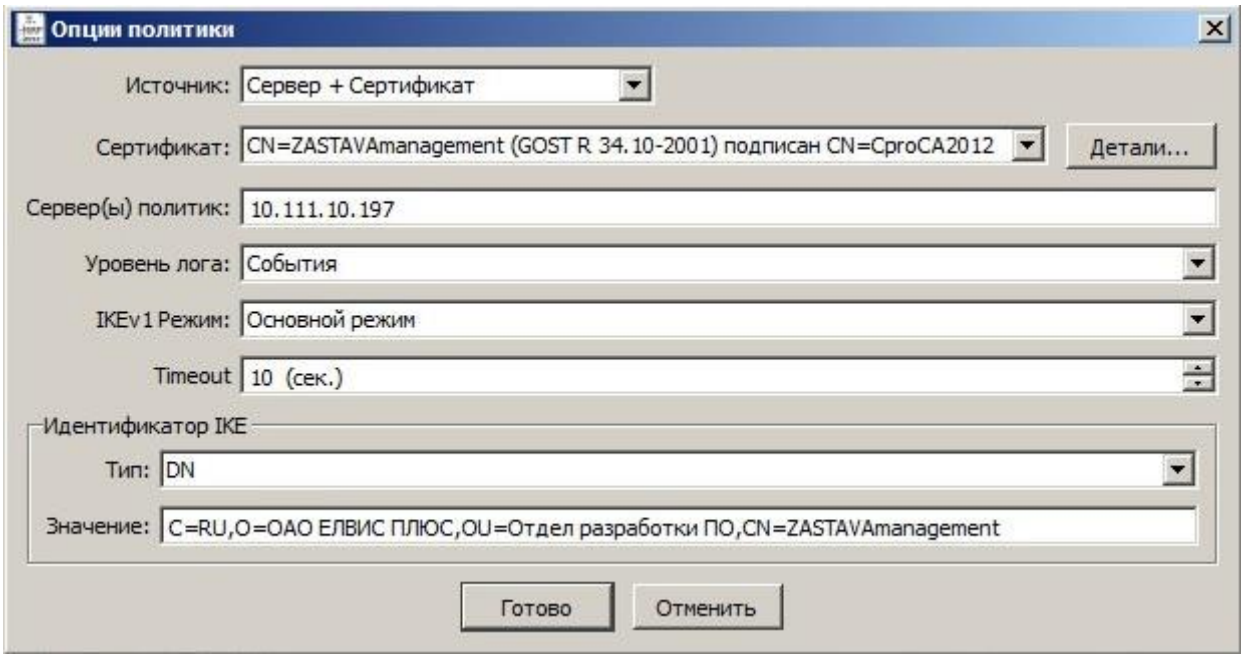

Рисунок 34 – Настройка параметров системной политики

Для настройки системной политики необходимо:

1) Выбрать тип метода активации из поля «Источник» и определить параметры данного метода:
   – При выборе метода прогрузки из файла необходимо в поле «Путь» указать путь к файлу с политикой или выбрать необходимый файл, нажав кнопку «…».

С помощью кнопки «Редактировать» при выборе метода активации из файла можно произвести изменение файла политики в окне «Редактор».

   – При выборе метода прогрузки с сервера необходимо в поле «Источник» выбрать из раскрывающегося списка необходимый параметр для установки SA. Раскрывающийся список содержит следующие значения: «Сервер+Сертификат», «Сервер+Ключ». Для настройки прогрузки политики с сервера необходимо:
     а) Выбрать из выпадающего списка поля «Сертификат» или «Ключ» зарегистрированный сертификат или Preshared Key:
     б) В окне «Опции политик» доступны также параметры: Уровень лога, Сервер(ы), IKE Режим. Чтобы настроить получение ЛПБ с сервера политики необходимо ввести в поле «Сервер(ы) политик» IP-адрес(а) или имя сервера и порт, с которого будет получена политика, если не указать порт, то берется значение по умолчанию (500). Если серверов несколько, IP-адреса указываются через запятую. Номер порта указывается через двоеточие.
     в) Для журналирования сообщений при передаче ЛПБ с сервера политики необходимо выбрать уровень подробности регистрации событий в поле «Уровень лога», подробнее об уровне регистрации событий см. в п. 3.8.1.1.
     г) Отметить в поле «Timeout» время, через которое необходимо обращаться к серверу за ЛПБ.
     д) В секции «Идентификатор IKE» выбрать тип IKE-идентификатора для прогрузки политики, согласованного с ЦУП.

2) Нажать кнопку «Готово».
3) Нажать в появившемся после сохранения параметров политики информационном окне кнопку «Да» – если Вы хотите активировать данную политику, «Нет» – если

не хотите активировать данную политику.

Сохранение опций политики требует введения пароля администратора.

3.5.3.2. Политика драйвера по умолчанию

В *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 в поле «Политика» окна «Управление политиками» нажать дважды левой кнопкой мыши и выбрать необходимые параметры в окне «Опции политик» (см. Рисунок 35). «Политика драйвера по умолчанию» может быть установлена, либо в «Сбрасывать все» (DROP ALL), либо в «Сбрасывать все, кроме DHCP» (DROP ALL EXCEPT DHCP), либо в «Пропускать все» (PASS ALL). После выбора необходимых настроек нажать кнопку «Готово» для сохранения настроек в *ЗАСТАВА-Офис*.

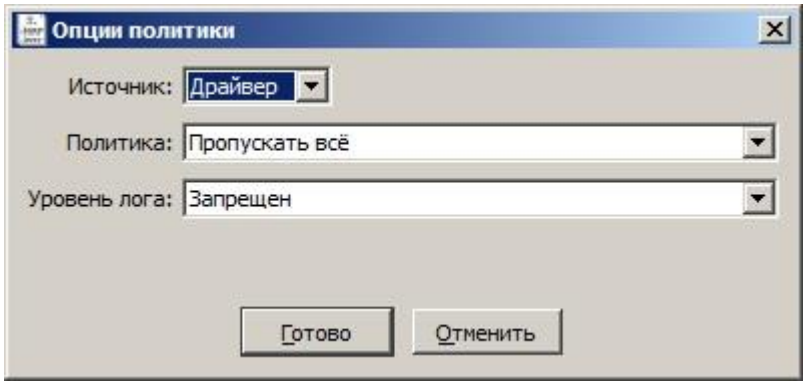

Рисунок 35 – Настройка параметров «Политика драйвера по умолчанию»

Из соображений безопасности рекомендуется устанавливать «Политика драйвера по умолчанию» в значение «Сбрасывать все». 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». В этом случае сеть будет недоступна до момента активации рабочей ЛПБ (исключение составляет только трафик DHCP, необходимый для назначения компьютеру IP-адреса).

Если на компьютере с *ЗАСТАВА-Офис* настроена удаленная аутентификация при входе пользователя в систему (например, аутентификация посредством домен-контроллера), то для ее правильной работы «Политика драйвера по умолчанию» должна быть: «Пропускать все».

3.5.4. Изменение параметров ЛПБ

Для изменения параметров выбранной политики из дерева политик поля «Политика» необходимо нажать дважды левой кнопкой мыши на требуемой политике. В появившемся окне «Опции политик» изменить необходимые параметры.

Для изменения доступны параметры следующих политик:

– Политика Драйвера по умолчанию (DDP) – политика, загружаемая при сбое.
– Системная политика – используется перед входом пользователя.

Параметры «Системной политики» и «Политики Драйвера по умолчанию» можно также изменить, выделив в дереве политик требуемую политику и нажав на правую кнопку мыши, из выпадающего меню выбрать параметр «Правка». В появившемся окне «Опции политик» изменить необходимые параметры. Сохранение измененных параметров требует ввода пароля администратора.

3.5.5. Создание ЛПБ

ЛПБ, созданная в *ЗАСТАВА-Управление,* сохраняется как текстовый файл. Данный режим задается в *ЗАСТАВА-Управление*.

Создание ЛПБ в *ЗАСТАВА-Управление*:

— Добавить соответствующий *ЗАСТАВА-Офис* объект в глобальную политику безопасности;
— Определить правила для данного объекта;
— Оттранслировать глобальную политику безопасности в ЛПБ или сохранить ЛПБ как файл;
— Зарегистрировать ЛПБ в *ЗАСТАВА-Офис.* За дополнительной информацией надо обратиться к п. 3.5.5.1.

3.5.5.1. Регистрация новой системной ЛПБ

ЛПБ может быть зарегистрирована в окне «Управление политиками». ЛПБ может находиться в файловой системе. При активации указанной политики *ЗАСТАВА-Офис* обратится к заданному источнику и скопирует политику в драйвер *Агента*, после чего эта политика будет активирована:

1) Нажать кнопку «Правка».
2) Выбрать один из способов добавления ЛПБ из поля «Источник» окна «Опции политик»:
   – Загрузить из файла;

     Для загрузки ЛПБ из файла необходимо указать файл ЛПБ в текстовом формате, или ввести вручную путь к файлу.
   – Загрузить с сервера ЦУП.

     Для загрузки ЛПБ с сервера необходимо выполнить следующие действия:
     а) Выбрать один из параметров:
        – «Сервер+Сертификат» – для загрузки ЛПБ с сервера и установки IPsec SA с помощью сертификата;
        – «Сервер+Ключ» – для загрузки ЛПБ с сервера и установки IKE;
     б) Выбрать из выпадающего списка зарегистрированный сертификат или Preshared Key, в соответствии с выбранным методом прогрузки с сервера.
     в) Ввести адрес или имя сервера и порт в строке «Сервер(ы) политик» поля «Общие параметры для всех политик», с которого будет получена политика. Если порт не указан, то берется значение по умолчанию (500). В качестве адреса сервера политик можно использовать DNS. Если серверов несколько, IP-адреса указываются через запятую. Номер порта указывается через двоеточие.
     г) Выбрать уровень подробности регистрации событий при передаче ЛПБ с сервера политики в поле «Уровень лога».
     д) Выбрать режим установления соединения IKE v1: основной или агрессивный в поле «IKE v1 Режим».
     е) В поле «Timeout» установить время, через которое необходимо обращаться к серверу за получением ЛПБ.
     ж) В секции «Идентификатор IKE» выбрать тип IKE-идентификатора для прогрузки политики, согласованного с ЦУП.
3) Нажать кнопку «Сохранить».
4) Ответить на вопрос об активации политики. Для активации зарегистрированной политики после сохранения параметров нажать кнопку «Да».

Перед чтением ЛПБ из файла удостовериться в том, что ОС настроена для показа всех типов файлов, иначе нужные файлы могут оказаться скрытыми.

3.5.6. Просмотр ЛПБ

В поле с деревом политик окна «Управление политиками» можно произвести просмотр текущей ЛПБ, для этого необходимо выбрать из дерева политик строку «Текущая политика» и нажать кнопку «Просмотр» окна «Управление политиками». В появившемся окне «Редактор» можно просмотреть код политики, произвести изменения или поиск необходимых параметров, выполнить переход на определенную строку политики, воспользовавшись для этого меню «Вид» окна «Редактор» и, при необходимости, сохранить данную политику в файловой системе, выбрав в меню «Файл» команду «Сохранить» и определив путь для сохранения.

3.5.7. Активация ЛПБ

Для активации ЛПБ (т.е. для загрузки в драйвер *Агента*) необходимо выделить нужную политику в дереве политик окна «Управление политиками» *ЗАСТАВА-Офис* и нажать кнопку «Активировать». ЛПБ загрузится в драйвер *Агента* и правила, определённые в ЛПБ, вступят в действие.

Если активация прошла успешно, ЛПБ загружается в драйвер *Агента* и активируется, это означает, что IP-трафик будет обрабатываться в соответствии с правилами, описанными в ЛПБ.

3.6. Окно «Токены»

ЗАСТАВА-Офис позволяет Вам использовать токены как среду транспортировки важной информации (сертификатов, закрытых ключей). *ЗАСТАВА-Офис* поддерживает работу с PKCS#11-совместимыми токенами версии 2.10 и выше, для работы необходимо наличие соответствующих динамически подключаемых библиотек. Также дополнительно поставляется эмулятор модуля токена на жестком диске.

В окне «Токены» (см. Рисунок 36) Вы можете зарегистрировать PKCS#11 модули для заданного типа токена (USB-ключ, смарт-карта, эмулятор токена на гибком/жёстком диске). Это окно содержит список всех зарегистрированных модулей токенов.

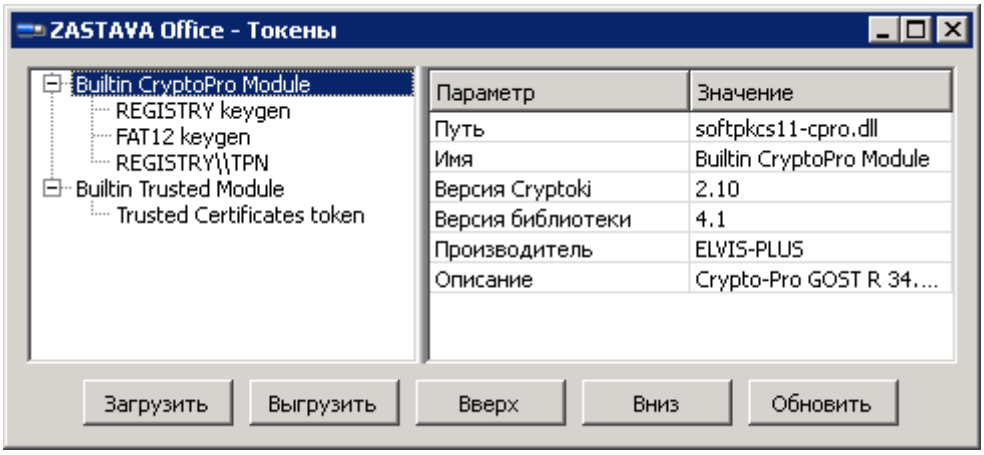

Рисунок 36 – Окно «Токены»

3.6.1. Добавление модулей токенов

Для регистрации модуля PKCS#11 в окне «Токены» необходимо:

– Нажать кнопку «Загрузить» в окне «Токены» в появившемся окне «Загрузить модуль» ввести требуемые данные (см. Рисунок 37).

– Ввести Имя модуля PKCS#11.

– Указать путь к динамической библиотеке модуля PKCS#11 и нажать кнопку «Открыть».

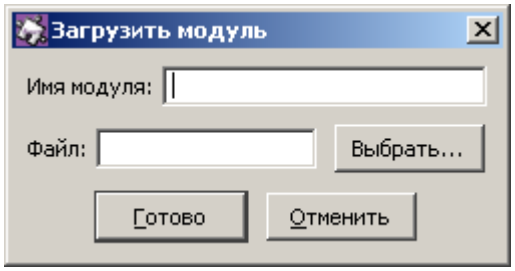

Рисунок 37 – Окно «Загрузить модуль»

Библиотеки модулей токенов *ЗАСТАВА-Офис* (для дискеты и эмуляторов токена на жестком диске) копируются в соответствующие каталоги во время инсталляции *ЗАСТАВА-Офис*.

Если Вы используете в качестве токена смарт-карту или USB-брелок, тогда требуемое ПО должно входить в комплект поставки токена. Имена библиотечных модулей PKCS#*11, которые входят в состав *ЗАСТАВА-Офис*, приведены в таблице (см. Таблица 24). Обратите внимание, что другие PKCS#11 библиотеки могут поставляться с другим ПО для токенов. Чтобы найти имя требуемой библиотеки обратитесь к документации по токенам.

Таблица 24 – Имена библиотечных модулей PKCS#*11

Тип токена	Имя библиотеки модуля PKCS#11
SoftToken common	`softpkcs11.dll*`

CryptoPro SoftToken	`softpkcs11-cpro.dll`
Trusted Certificates token	`softpkcs11-trusted.dll`
*Данный модуль, входит в дополнительный пакет установки *ЗАСТАВА-Офис*.	

– Нажать кнопку «Готово».

3.6.2. Смена PIN-кода токена

Если Вы хотите изменить PIN-код текущего токена, то в окне «Токены» необходимо выбрать токен из списка, затем нажать кнопку «Сменить пароль». Ввести текущий пароль в поле «Текущий пароль». Ввести новый пароль в поля «Новый пароль» и «Повтор пароля» и нажать кнопку «Готово».

	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).
	Кнопка «Сменить пароль» будет недоступна, если нет токенов, зарегистрированных в *ЗАСТАВА-Офис.*
	Если для доверенного токена задан пароль пользователя, то импорт сертификата на этот токен производиться с вводом пароля администратора, а удаление сертификата – с паролем пользователя.

3.6.3. Инициализация токена

Для инициализации токена в окне «Токены» необходимо:

– Нажать кнопку «Инициализировать» в окне «Токены» в появившемся окне «Инициализация токена» вписать данные (см. Рисунок 38).

– Ввести пароль администратора токена.

– В поле «Также установить пароль пользователя» в поле «Новый пароль» ввести новый пароль пользователя и повторить введенный пароль в поле «Повтор пароля».

– Параметр «Сохранить пароль для будущих соединений» – необязательный параметр, который отвечает за сохранение пароля пользователя.

– Нажать кнопку «Готово».

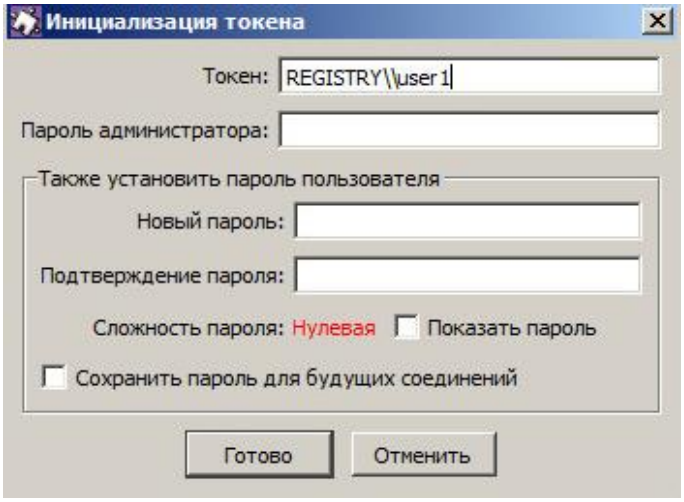

Рисунок 38 – Окно «Инициализация токена»

3.6.4. Удаление модуля токена

Чтобы удалить модуль PKCS#11 из *ЗАСТАВА-Офис* Вы должны выбрать его в таблице и нажать кнопку «Выгрузить».

3.7. Окно «Плагины»

Модуль управления криптобиблиотек (модуль криптоплагинов) – встроенный программный модуль, предназначенный для подключения криптобиблиотек, используемых в *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 компонентам ПК «VPN/FW «ЗАСТАВА», версия 6 как отдельный модуль (плагин). По умолчанию, в состав компонентов ПК «VPN/FW «ЗАСТАВА», версия 6 входит набор штатных криптобиблиотек (см. Таблица 25).

Таблица 25 – Состав криптобиблиотек

Наименование	Описание
`crypto_cpro_user`	Криптоалгоритмы ГОСТ для шифрования

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 ОС для защиты сетевого трафика;
- выполнение криптографических процедур на прикладном уровне.

Работа с модулем криптоплагинов может производиться либо при помощи графического интерфейса в окне «Плагины», либо из командной строки - см. раздел 5.

3.7.1. Просмотр криптобиблиотек и криптоалгоритмов

Криптобиблиотеки, зарегистрированные в модуле криптоплагинов, просматриваются в главном окне программы в виде списка. Плюс (+) рядом с именем криптобиблиотеки означает, что она содержит криптоалгоритмы. Чтобы просмотреть криптоалгоритмы, содержащиеся в любой зарегистрированной криптобиблиотеке, необходимо нажать на плюс рядом с именем. Список алгоритмов, содержащихся в криптобиблиотеке, расширится, как показано на рисунке (см. Рисунок 39).

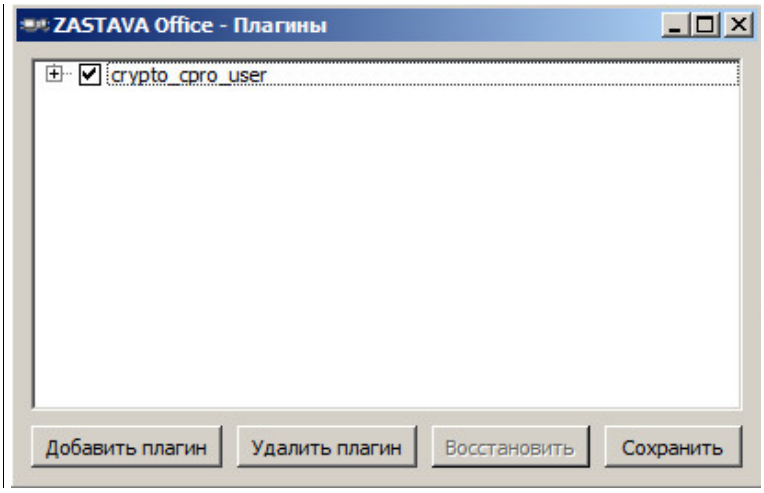

Рисунок 39 – Окно модуля криптоплагинов

По умолчанию в *ЗАСТАВА-Офис* установлены следующие криптобиблиотеки, представленные в таблице (см. Таблица 24).

Если имя криптобиблиотеки выделено серым цветом, значит при загрузке данной криптобиблиотеки произошла ошибка и она не доступна для использования.

3.7.2. Регистрация криптобиблиотеки

Модуль криптоплагинов может управлять криптобиблиотеками (регистрировать и активировать), которые используются в компонентах ПК «VPN/FW «ЗАСТАВА», версия 6, чтобы обеспечивать защиту информационных обменов. Криптобиблиотеки – это подключаемые программные модули, которые содержат криптоалгоритмы; любая криптобиблиотека может быть зарегистрирована в модуле криптоплагинов и может использоваться в компонентах ПК «VPN/FW «ЗАСТАВА», версия 6.

Для регистрации новой криптобиблиотеки:

– нажать кнопку «Добавить плагин»;

– В окне «Добавить плагин» найти требуемый файл криптобиблиотеки, и выбрать «Открыть».

Если регистрация прошла успешно в окне «Плагины» будет показана информация о зарегистрированной криптобиблиотеке. Чтобы выйти из программы надо нажать кнопку «Сохранить».

3.7.3. Удаление криптобиблиотеки

Удаление криптобиблиотеки:

– Выделить зарегистрированную криптобиблиотеку, которую нужно удалить;
– Нажать кнопку «Удалить плагин»;
– Подтвердить решение удалить криптобиблиотеку в окне «Плагины», нажать кнопку «Да» и перезапустить ОС, чтобы завершить процесс удаления криптобиблиотеки.

3.7.4. Активация криптобиблиотеки

Криптоалгоритмы, содержащиеся в специальных криптобиблиотеках, могут быть активированы или деактивированы.

Чтобы активировать криптоалгоритм надо найти его в списке и нажать кнопку «Восстановить».

Нажать кнопку «Сохранить», чтобы сохранить результаты.

Перед активацией криптоалгоритма убедиться в том, что данный алгоритм не был активирован ни в какой другой криптобиблиотеке. Если алгоритм был активирован в другой криптобиблиотеке, его нужно сначала деактивировать, прежде чем этот криптоалгоритм будет активирован в новой криптобиблиотеке.

3.8. Окно «Прочие настройки»

Все параметры, которые определяют работу *ЗАСТАВА-Офис*, можно разделить на две группы:

– локальные установки;
– параметры в ЛПБ.

Окно «Прочие настройки» предназначено для изменения локальных установок *ЗАСТАВА-Офис*. При штатной работе *ЗАСТАВА-Офис* изменение локальных установок обычно не требуется, и управление производится централизованно при помощи ЦУП (путем внесения изменений в ЛПБ).

Чтобы получить доступ к окну «Прочие настройки», необходимо на *Панели управления* нажать кнопку «Настройки» (см. Рисунок 40).

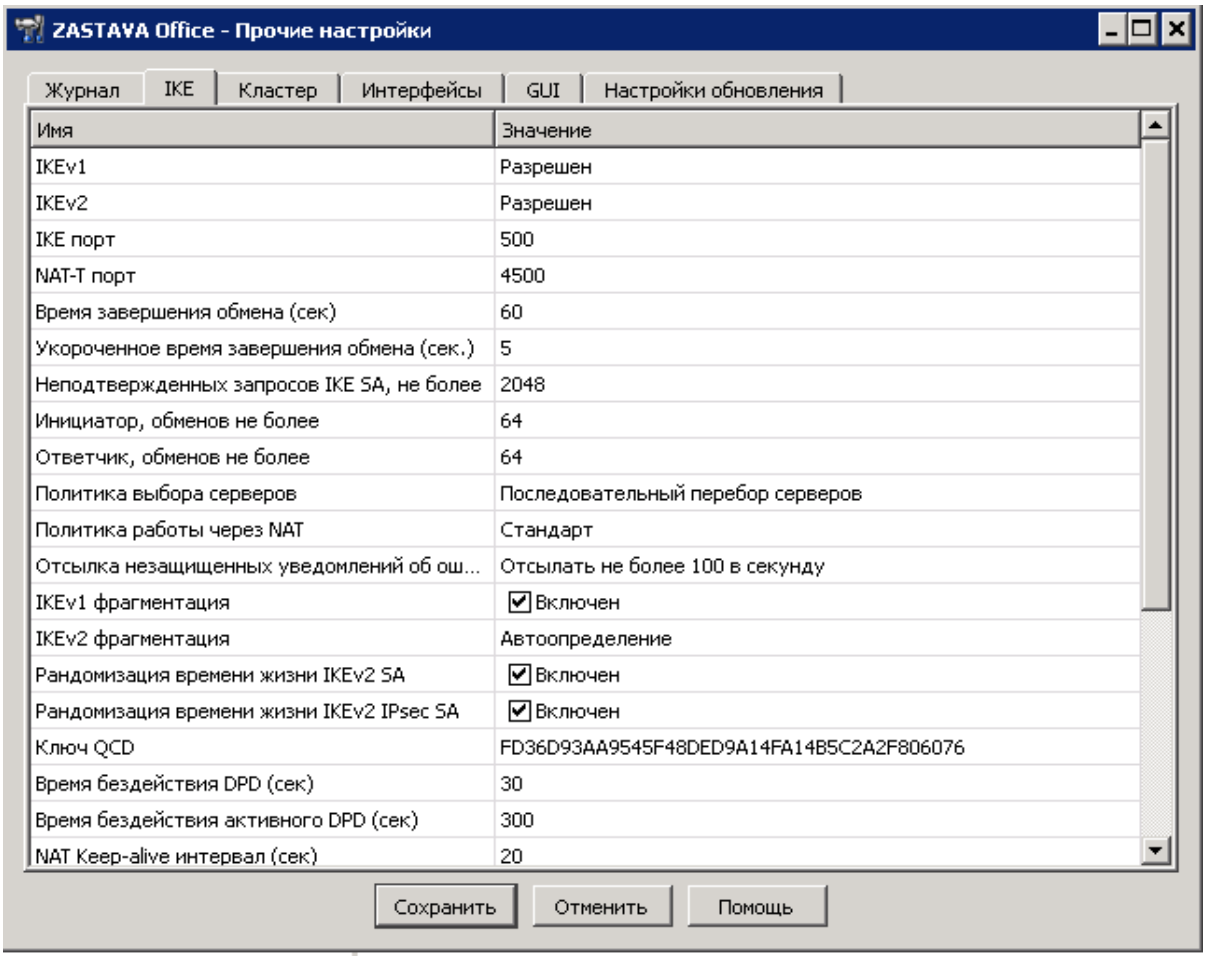

Рисунок 40 – Окно «Прочие настройки» с отображением вкладки «IKE»

После редактирования параметров окна «Прочие настройки» необходимо нажать кнопку «Сохранить», чтобы сохранить изменения.

	Некоторые изменения вступают в силу только после того, как будет перезагружена ЛПБ.
	Некоторые изменения, например, активация ЛПБ, не могут быть отменены.

Окно «Прочие настройки» имеет закладки для следующих параметров, приведенных в таблице (см. Таблица 26).

Таблица 26 – Параметры окна «Прочие настройки»

Наименование вкладки	**Параметры**

Наименование вкладки	Параметры
Журнал	Установка параметров журнала регистрации событий
IKE	Установка значений параметров протокола IKE
Кластер	Настройки кластера
Интерфейсы	Редактирование имен сетевых интерфейсов, на которых ставится драйвер перехвата пакетов.
GUI	Установка параметров представления информации в графическом интерфейсе *ЗАСТАВА-Офис*
Настройки обновления	Управление механизмом автоматического обновления

3.8.1. Вкладка «Журнал»

Регистрация событий позволяет сохранять хронологию системных событий, происходящих в *ЗАСТАВА-Офис.* Настройку системы регистрации событий можно произвести на вкладке «Журнал» окна «Прочие настройки» для выбора вкладки «Журнал» необходимо на *Панели управления* нажать кнопку «Настройки» и в появившемся окне выбрать вкладку «Журнал» (см. Рисунок 41). На вкладке «Журнал» окна «Прочие настройки» можно изменить язык регистрации системных событий, для этого необходимо выбрать нужное значение в поле «Язык лога» и нажать кнопку «Сохранить», для сохранения изменений.

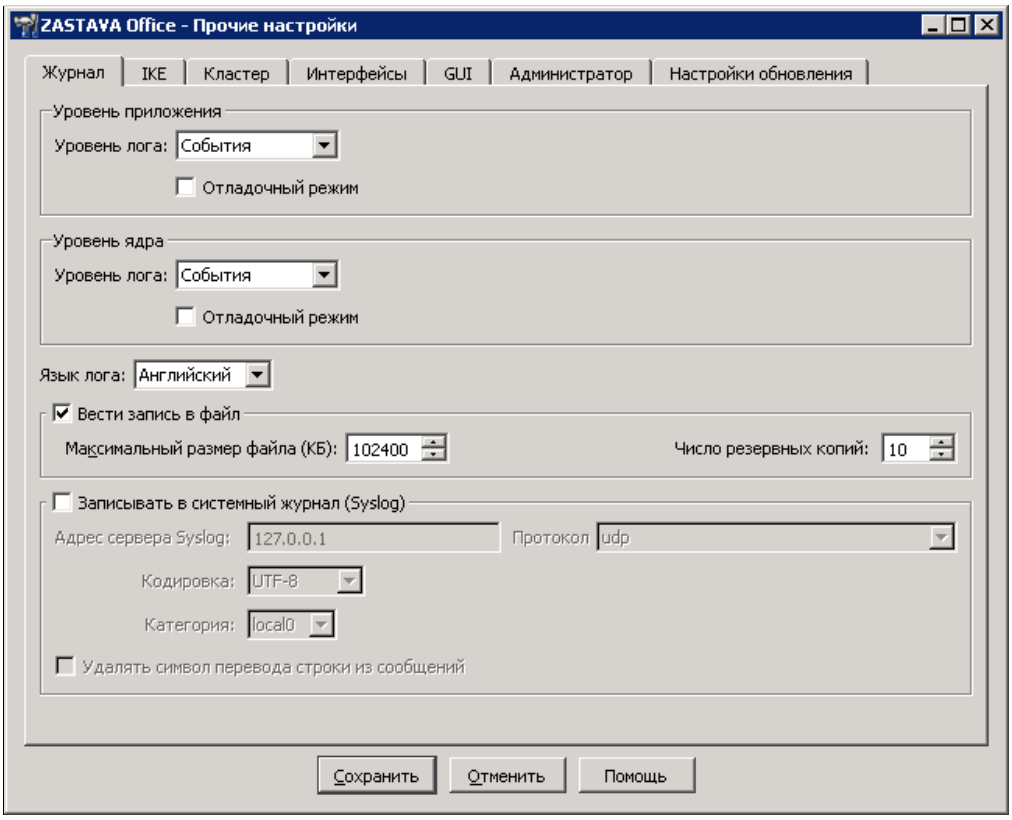

Рисунок 41 – Вкладка «Журнал» окна «Прочие настройки»

3.8.1.1. Уровень регистрации событий

Задать уровень регистрации событий можно для двух уровней: Уровень приложения и Уровень ядра (см. Рисунок 41). На Уровне приложения генерируются сообщения от службы (процессы и т.д.), на Уровне ядра – сообщения от драйвера. Сообщения уровня ядра в журнале помечаются как «DRV».

Уровень регистрации событий (поле «Уровень лога») может быть установлен, в зависимости от требуемой степени подробности, в одно из четырех значений: «Заблокирован», «События», «Подробный», «Отладочный» (в порядке от наименьшего количества информации к наибольшему). Если Вы не хотите регистрировать события, следует выбрать значение «Заблокирован».

Если установлен флажок «Отладочный режим» (см. Рисунок 41) уровни регистрации событий, заданные в политике, будут игнорироваться.

Описание уровней регистрации событий приведено в таблице (см. Таблица 27).

Таблица 27 – Значения для уровня регистрации событий

Уровень регистрации событий	Параметры
Заблокирован	События не будут регистрироваться
События	Будет регистрироваться минимальное количество информации об операциях, а также все сообщения об ошибках.
Подробный	Будет регистрироваться полная информация об операциях (для поиска неисправностей).
Отладочный	Все события будут зарегистрированы; уровень используется, в основном, для отладки.

При установке уровня регистрации «Отладочный» (Verbose) генерируется огромное количество сообщений. К примеру, информация об установлении одного защищенного соединения (SA) может занимать в журнале сообщений более 20 страниц. Используйте этот уровень только для обнаружения и детализации ошибок при работе клиента *ЗАСТАВА-Офис*.

Параметры уровня регистрации могут также указываться в ЛПБ, созданной *ЗАСТАВА-Управление* для *ЗАСТАВА-Офис*. В этом случае установки из ЛПБ будут иметь преимущество перед локальными установками. Вы можете посмотреть текущий реальный уровень регистрации событий, нажав кнопку «Информация об уровне лога» в окне «Журнал» (при этом «Уровень лога» не должен быть в состоянии «Заблокирован»).

Настройки системы регистрации событий (название архивных файлов журнала, их количество, максимальный размер файла журнала, настройки Syslog) хранятся в секции /LOG

файла localsettings.ini, который располагается в основной директории *ЗАСТАВА-Офис*. Некоторые из этих параметров могут также настраиваться через графический интерфейс *ЗАСТАВА-Офис* – см. вкладку «Журнал» окна «Прочие настройки».

3.8.1.2. Параметры файла регистрации событий

Файл регистрации событий (`bin_log.txt`) может стать чрезвычайно большим и в итоге содержать старую, ненужную информацию. Чтобы установить максимальный размер файла надо отредактировать значение в поле «Макс размер файла (МБ)». Когда размер файла превысит заданное значение, текущий файл будет перемещен в архивный файл, после чего будет начат новый файл. Количество сохраняемых резервных копий журнала (предустановленное – 5) устанавливается в поле «Число резервных копий».

	Сам журнал может просматриваться по нажатию кнопки «Журнал» на *Панели управления* (см. подраздел 3.2).
	Параметры SYSTEM, LP, LDAP, CM управляются как из *ЗАСТАВА-Офис,* так и централизовано из ЦУП при условии, что уровень регистрации событий данных модулей в ЦУП установлен в значение DEFAULT.

3.8.1.3. Параметры журнала Syslog

ЗАСТАВА-Офис позволяет настроить регистрацию событий с помощью системного средства журналирования – Syslog. При этом syslog-сервер может находиться как на локальном, так и на удалённом компьютере. Для регистрации событий с системном журнале следует установить флажок «Записывать в системный журнал (Syslog)». Доступны следующие настройки, указанные в таблице (см. Таблица 28).

Таблица 28 – Настройка параметров записи в системный журнал

Настройки	Параметры
Адрес сервера Syslog	Задаёт значение адреса syslog-сервера.
Протокол	Протокол, в соответствии с которым будет происходить передача данных
Кодировка	Кодировка, в которой будут формироваться сообщения для системного журнала.
Категория	Оно из предопределённых значений от 0 до 7. Позволяет идентифицировать сообщения от *ЗАСТАВА-Офис* в общем журнале.
Удалять символ перевода строки из сообщений	Параметр для склеивания строчек в многострочном сообщении

3.8.1.3.1. Удалённая регистрация событий для ОС ALT Linux

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 *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`

3.8.2. Вкладка «IKE»

ЗАСТАВА-Офис позволяет настроить параметры протокола IKE, для этого надо воспользоваться вкладкой «IKE» окна «Прочие настройки» (см. Рисунок 42).

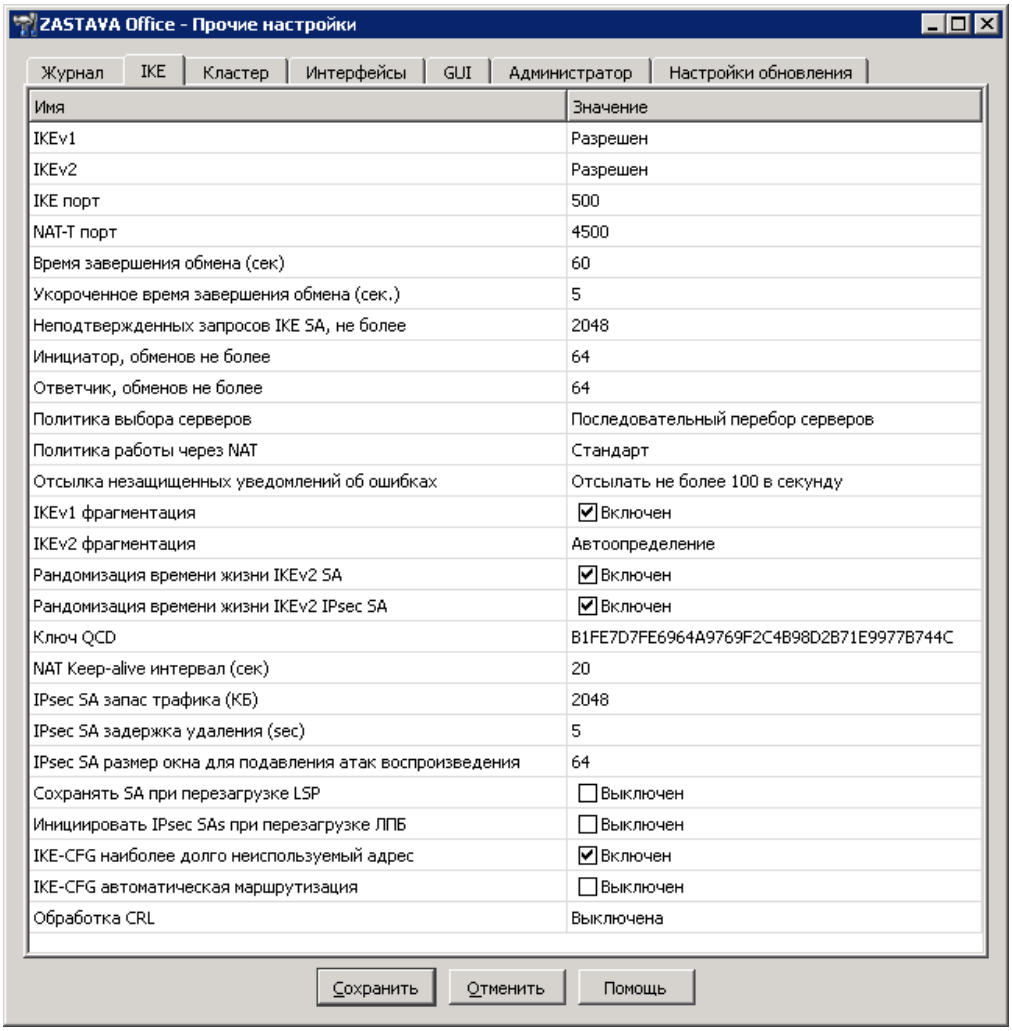

Рисунок 42 – Окно «Прочие настройки» вкладка «IKE»

3.8.2.1. Изменение параметров

Изменение значений параметров производится стандартным образом, в зависимости от типа поля:

- выбрать из списка;
- дважды нажать мышью на поле со значением параметра, ввести новое значение с клавиатуры. Недопустимые символы не отображаются в поле;
- установить/снять флажок.

Чтобы сохранить изменения необходимо нажать кнопку «Сохранить».

3.8.2.2. 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 29).

Таблица 29 – Параметры IKE

Параметр	Расшифровка
IKEv2	Управление режимом работы IKEv2 (по умолчанию - Разрешен) Режимы: — Разрешен; — Только ответчик; — Запрещен.
IKE порт	Номер порта для IKE-соединения (1-65535, по умолчанию 500)
NAT-T порт	Порт для работы алгоритма NAT-Traversal. Трафик IKE будет переключен на этот порт, когда при установлении соединения между партнерами обнаруживается присутствие NAT-устройств. Значение по умолчанию: (1-65535, по умолчанию 4500)
Время завершения обмена (сек)	Максимальное время для создания защищенного соединения (SA). (5-600, по умолчанию 60)
Укороченное время для завершения обмена (сек)	Укороченное время для завершения обмена (3-60, по умолчанию 5)

Параметр	Расшифровка
Неподтвержденных запросов IKE SA, не более	Максимальное количество стейтов IKE 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 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. Стейт 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 реальный, то инициатор повторно посылает запрос, включая в него COOKIE. Такие запросы считаются ответчиком подтвержденными и минуют проверку на превышение описываемого параметра
Ответчик, обменов не более	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.
Политика выбора серверов	Политика выбора серверов. Режимы: — Соединяться только с первым сервером из списка; — Последовательный перебор серверов (используется по умолчанию); — Перебор серверов в 2 потока; — Перебор серверов в 4 потока; — Перебор серверов в 8 потоков.
Политика работы через NAT	Политика выбора метода работы через NAT (по умолчанию – Стандарт)
Отсылка незащищенных уведомлений об ошибках	Частота отправки незащищенных сообщений об ошибках (по умолчанию – Отсылать не более 100 в секунду). Возможные значения: отключить, отправлять через 1 сек, отправлять через 10 сек, отправлять через 100 сек, отправлять через 1000 сек, постоянно отправлять.
IKE v2 фрагментация	Управление режимом фрагментации (IKEv2). Значения: — Не использовать; — Автоопределение (используется по умолчанию); — Всегда фрагментировать.
Рандомизация времени жизни IKEv2 IPsec SA	Рандомизация времени жизни IPsec SA (по умолчанию включена)
Рандомизация времени жизни IKEv2 SA	Рандомизация времени жизни IKE SA (IKEv2) (по умолчанию включена)
IKEv2 возобновление	Возобновление IKE SA (IKEv2) (по умолчанию включено)

Параметр	Расшифровка
Ключ QCD	Ключ для выработки токена для метода Quick Crash Detection (по умолчанию генерируется автоматически или может быть 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 сторонними агентами.
NAT Keep-alive интервал (сек)	Интервал в секундах для отправки UDP пакета для поддержания трансляции на NAT устройстве (1-60, по умолчанию 20)
IPsec SA Запас трафика (КБ)	Запас трафика IPsec, по достижении которого запускается процесс обновления ключей (0-16384, по умолчанию 2048)
IPsec SA Задержка удаления (сек)	Задержка до удаления IPsec
IPSec SA размер окна для подавления атак воспроизведения	IPSec размер окна для подавления атак воспроизведения (по умолчанию 64). Возможные значения: 32, 64, 128, 264, 512, отключено.
Сохранить SA при перезагрузке LSP	Сохранение SA при перезагрузке ЛПБ (по умолчанию выключено)
Инициировать IPsec Sas при перезагрузке ЛПБ	Управление режимом инициации IPsec SAs при загрузке ЛПБ (по умолчанию выключен).
IKE-CFG автоматическая маршрутизация	Параметр, контролирующий использование IKE-CFG
IKE-CFG наиболее долго неиспользуемый адрес	Параметр, контролирующий использование IKE-CFG
Обработка CRL	Параметр, регулирующий режимы обработки CRL Режимы: — Выключена (используется по умолчанию); — Включена, отзывать, если CRL недоступен; — Включена, не отзывать, если CRL недоступен. Режимы обработки CRL описаны в разделе 3.4.8 Списки Отозванных Сертификатов.

Некоторые дополнительные параметры протокола IKE хранятся в ЛПБ, создаваемой для *ЗАСТАВА-Офис* в *ЗАСТАВА-Управление*.

3.8.2.3. Политика работы через NAT

Управление политикой выбора метода работы через NAT осуществляется из локальных настроек *ЗАСТАВА-Офис* на вкладке «IKE» параметр «Политика работы через NAT». Политика может быть одной из представленных в таблице (см. Таблица 30).

Таблица 30 – Управление политикой выбора метода работы через NAT

Параметр	Расшифровка
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.
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.
Все методы	Использовать все методы. Будучи инициатором, предлагаются все варианты UDP-инкапсуляции, будучи респондентом приоритетным считается метод Стандарт.
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).
Автовыбор	Режим характеризуется тем, что, будучи инициатором, в Main Mode *Агент* пытается сам выбрать подходящий метод UDP-инкапсуляции.
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.
Все методы (Принудительно)	Режим «Все методы» с принудительной инкапсуляцией. Полностью аналогичен режиму «Все методы», за тем исключением, что инкапсуляция используется всегда, не зависимо от наличия или отсутствия NAT-а между партнерами.
Huttunen (Принудительно)	Режим Huttunen с принудительной инкапсуляцией. Полностью аналогичен режиму Huttunen, за тем исключением, что инкапсуляция используется всегда, не зависимо от наличия или отсутствия NAT-а между партнерами
Автовыбор (Принудительно)	Автоопределение с принудительной инкапсуляцией. Режим полностью аналогичен режиму Автовыбор, за тем исключением, что инкапсуляция используется всегда, не зависимо от наличия или отсутствия NAT-а между партнерами.

Некоторые настройки IKE не отображаются в интерфейсе, но могут быть изменены в секции IKE файла локальных настроек localsettings.ini:

CERT_IGNORE_KEY_USAGE_BITS:
=0 – атрибут сертификата «key usage» будет проверяться;
=1 – атрибут сертификата «key usage» **не будет** проверяться;

CERT_IMPORT_WITH_UNKNOWN_CRITICAL:
=0 – запрещает импортировать сертификаты с неизвестными критическими расширениями;
=1 – **позволяет** импортировать сертификаты с неизвестными критическими расширениями;

CERT_IGNORE_EXT_KEY_USAGE:
=0 – позволяет использовать для установления SA IKE/IPSec **только** сертификат с OID 1.3.6.1.5.5.7.3.17 в поле «Extended Key Usage»;
=1 – не проверяет наличие OID 1.3.6.1.5.5.7.3.17 в поле EKU.

3.8.3. Вкладка «Кластер»

ЗАСТАВА-Офис может быть установлен на кластерную информационную систему. Поддержка кластера позволяет построить высоконадёжную отказоустойчивую систему.

Вкладка «Кластер» содержит настройки для включения кластерной информационной системы (см. Рисунок 43, Рисунок 44).

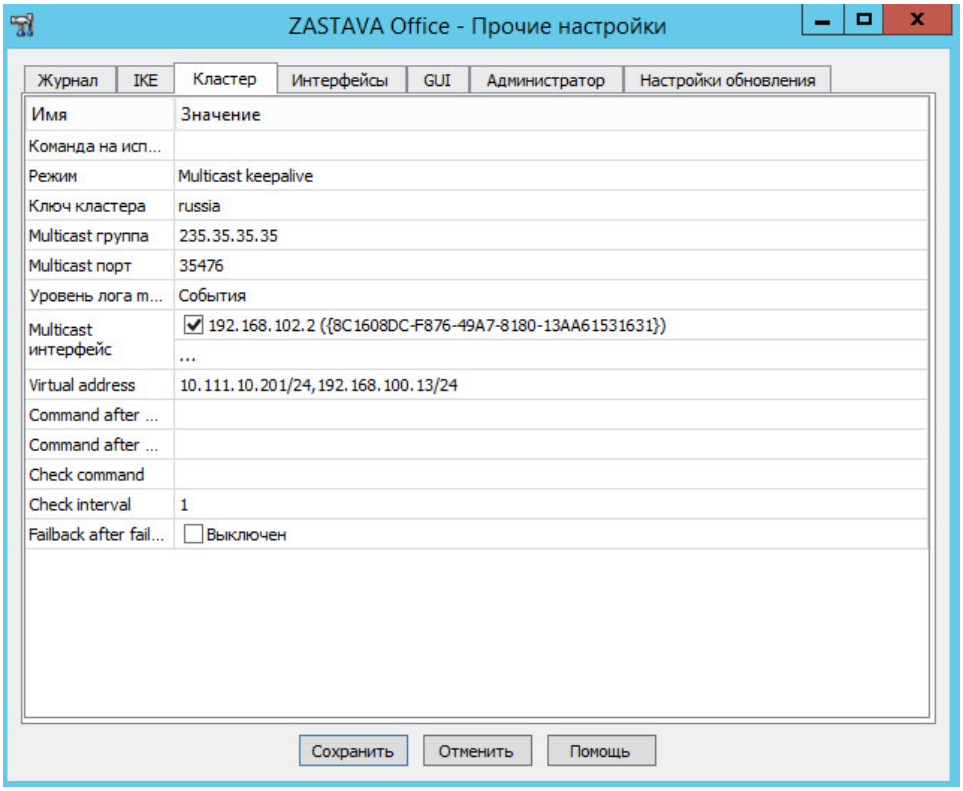

Рисунок 43 – Вкладка «Кластер» окна «Прочие настройки»

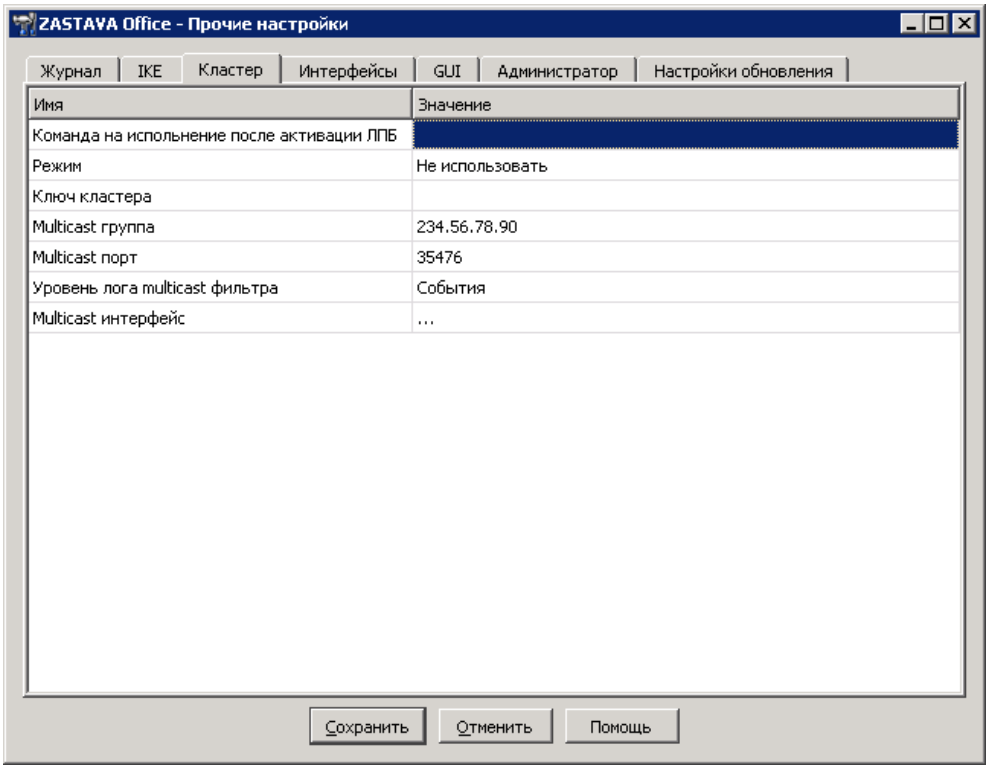

Рисунок 44 – Вкладка «Кластер» окна «Прочие настройки» для ОС Linux

Вкладка «Кластер» содержит следующие настройки (см. Таблица 31).

Таблица 31 – Параметры вкладки «Кластер»

Имя	**Значение**
Команда на исполнение после активации ЛПБ	Системная команда, которая должна быть выполнена после активации ЛПБ (не обязательное поле)
Режим	Режим работы *ЗАСТАВА-Офис*: Не использовать – режим кластера не используется; Multicast – позволяет работать в кластерном режиме (используется в ОС Linux); Multicast keepalive – позволяет работать в кластерном режиме
Ключ кластера	Буквенно-цифровая последовательность, использующаяся для шифрации трафика между узлами кластера
Multicast группа	Групповой адрес режима Multicast из диапазона 224.0.0.0 до 239.255.255.255.
Multicast порт	Порт режима Multicast (любое десятичное целое число).

Имя	Значение
Уровень лога Multicast фильтра	Уровень регистрации событий режима Multicast: – Заблокирован – События не будут регистрироваться; – События – Будет регистрироваться минимальное количество информации об операциях, а также все сообщения об ошибках; – Подробный – Будет регистрироваться полная информация об операциях (для поиска неисправностей); – Отладочный – Все события будут зарегистрированы; уровень используется, в основном, для отладки
Multicast интерфейс	Интерфейс, использующийся в режиме Multicast

Более подробную информацию о конфигурировании *ЗАСТАВА-Офис* в режиме высокой надежности можно найти в Приложении 1. «*ЗАСТАВА-Офис* высокой надежности».

3.8.4. Вкладка «Интерфейсы»

Таблица на вкладке «Интерфейсы» окна «Прочие настройки» показывает данные относительно сетевых интерфейсов компьютера, трафик на которых контролируется *ЗАСТАВА-Офис*. Для каждого интерфейса представлена информация (см. Рисунок 45).

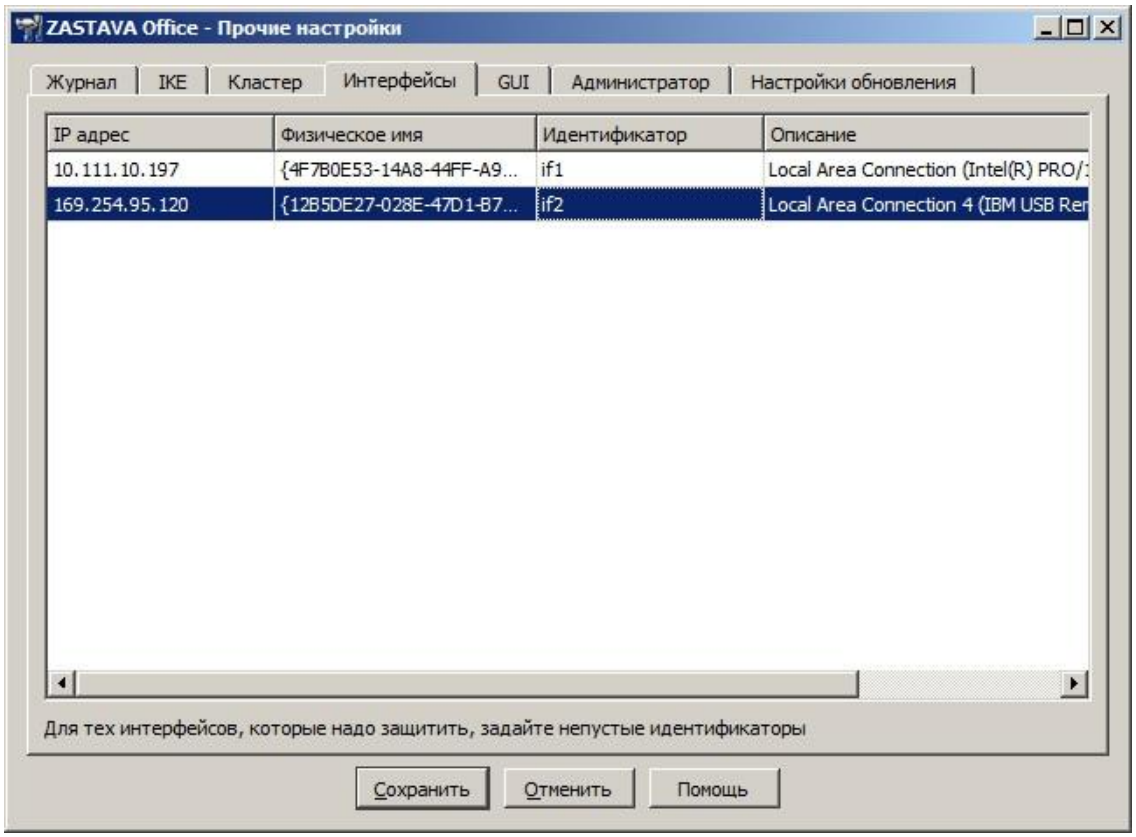

Рисунок 45 – Вкладка «Интерфейсы» окна «Прочие настройки»

Во вкладке «Интерфейсы» информация по интерфейсам разделена по параметрам (см. Таблица 32).

Таблица 32 – Параметры локальных интерфейсов

Параметры	Расшифровка
IP-адрес	IP-адрес интерфейса. Не редактируется.
Физическое имя	Физическое имя интерфейса. Не редактируется.
Идентификатор	Идентификатор интерфейса. Редактируется.
Описание	Описание интерфейса. Не редактируется.

Те интерфейсы, которые были зарегистрированы при установке *ЗАСТАВА-Офис* (активные интерфейсы), имеют непустое значение в поле «Идентификатор». Эти интерфейсы контролируются/управляются *ЗАСТАВА-Офис*. Драйвер *ЗАСТАВА-Офис*, перехватывающий сетевые пакеты, установлен на этих интерфейсах, и они могут быть включены в правила ЛПБ.

Список активных интерфейсов можно изменять. Для ввода/редактирования *Идентификатора интерфейса* нужно:

— Нажать дважды левой кнопкой мыши в соответствующей строке таблицы поля «Идентификатор».
— Изменить значение в поле «Идентификатор». Не используйте запятые, кавычки, апострофы или пробелы. Идентификаторы должны соответствовать описанию Объектов в ЦУП.

При помощи вышеописанной процедуры можно также изменить идентификаторы зарегистрированных интерфейсов. Кроме того, можно удалить интерфейс из списка активных интерфейсов – для этого нужно очистить поле «Идентификатор» таким же способом.

После внесения изменений на вкладке «Интерфейсы», следует перезагрузить ЛПБ.

3.8.5. Вкладка «GUI»

Вкладка «GUI» окна «Прочие настройки» позволяет настроить представление графического интерфейса *ЗАСТАВА-Офис* (см. Рисунок 46).

В поле «Стиль Toolbar» можно изменить представление графического интерфейса, для этого необходимо отметить одно из видов представлений: «Только надписи», «Только картинки», «Картинки и надписи»,

Также можно изменить представление иконок на *Панели управления ЗАСТАВА-Офис,* для этого необходимо поставить флаг в поле «Большие иконки в toolbar». Язык GUI также можно поменять на этой вкладке.

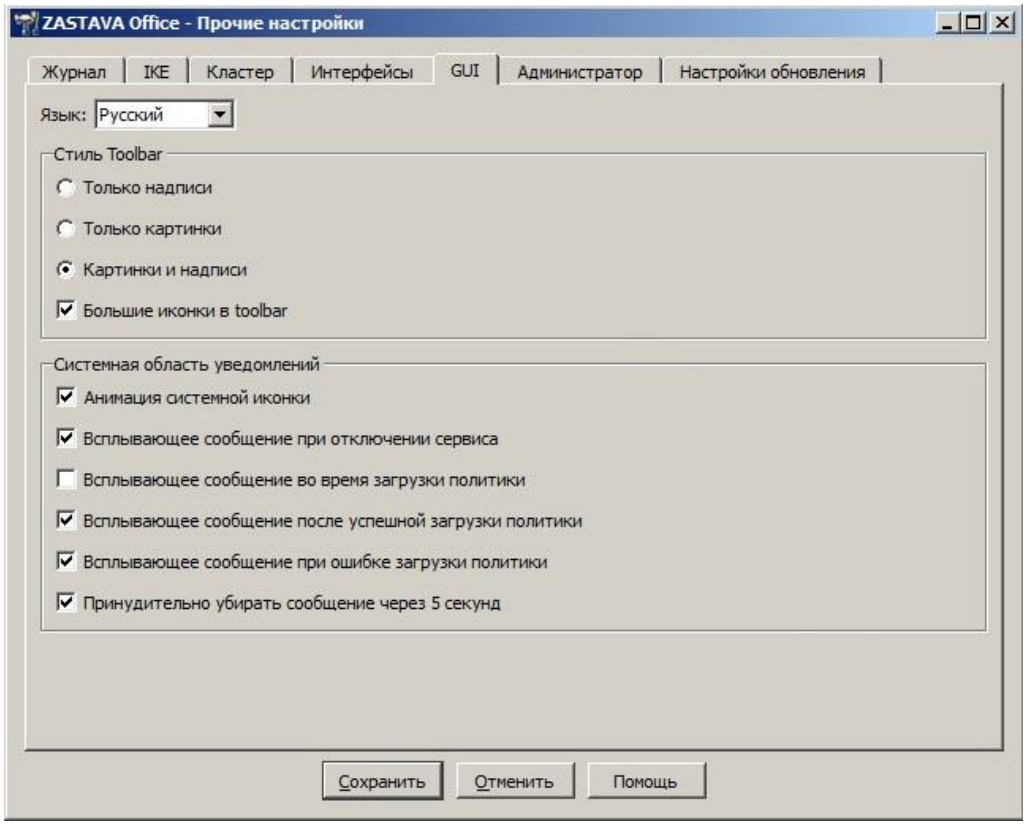

Рисунок 46 – Вкладка «GUI» окна «Прочие настройки»

Параметры вкладки «GUI» представлены в таблице (см. Таблица 33).

Таблица 33 – Параметры окна «GUI»

Параметр	**Описание**
Только картинки	Отображает/скрывает иконки на *Панели управления* и га *панелях инструментов* всех окон *ЗАСТАВА-Офис.*
Только надписи	Отображает/скрывает имена кнопок на *Панели управления* и в представлении всех окон *ЗАСТАВА-Офис.*
Картинки и надписи	Отображает/скрывает имена кнопок на *Панели управления* и в представлении всех окон *ЗАСТАВА-Офис.*
Большие рисунки	Изменяет размер иконок на *Панели управления* и в представлении всех окон *ЗАСТАВА-Офис.*
Язык	Изменяет язык интерфейса (пункты «Русский», «English») представления GUI *ЗАСТАВА-Офис.*
Анимация системной иконки	Отображает/скрывает анимацию системной иконки на панели инструментов рабочего стола.
Всплывающие сообщения при отключении сервиса	Включает трансляцию всплывающих сообщений при отключении сервиса
Всплывающие сообщения во время загрузки политики	Включает трансляцию всплывающих сообщений во время загрузки политики
Всплывающие сообщения после успешной загрузки	Включает трансляцию всплывающих сообщений после успешной загрузки политики

Параметр	Описание
политики	
Всплывающие сообщения при ошибке загрузки политики	Включает трансляцию всплывающих сообщений при ошибке загрузки политики
Принудительно убрать сообщения через 5 секунд	Закрывает тултипы через 5 секунд, даже если пользователь не двигает мышкой (по умолчанию – включена)

3.8.6. Вкладка «Администратор»

Вкладка «Администратор» окна «Прочие настройки» предназначена для добавления и удаления учетных записей администраторов настроек СКЗИ. Также возможно установить время истечения сессии логина и сменить пароль.

Параметры конфигурирования настроек представлены в таблице (см. Таблица 34).

Таблица 34 – Описание элементов интерфейса вкладки «Администратор»

Элемент	Описание
Кнопка «Добавить»	Добавление нового администратора и указание срока действия пароля
Кнопка «Удалить»	Удаление учетной записи администратора
Кнопка «Logout»	Выход из учетной записи текущего администратора. Для активации новой ЛПБ потребуется авторизация
Кнопка «Сменить пароль»	Смена пароля администратора и срока его действия

3.8.7. Вкладка «Настройки обновления»

Вкладка «Настройки обновления» окна «Прочие настройки» предназначена для локального конфигурирования автоматических обновлений (подробнее см. п. 3.8.7.1).

3.8.7.1. Описание элементов интерфейса

ЗАСТАВА-Офис позволяет произвести настройки обновлений. На вкладке «Настройки обновления» окна «Прочие настройки» (см. Рисунок 47) можно выбрать метод конфигурации обновлений, режим обновлений, а также проверить наличие новых обновлений, загрузить и установить их. Параметры конфигурирования настроек обновления представлены в таблице (см. Таблица 35).

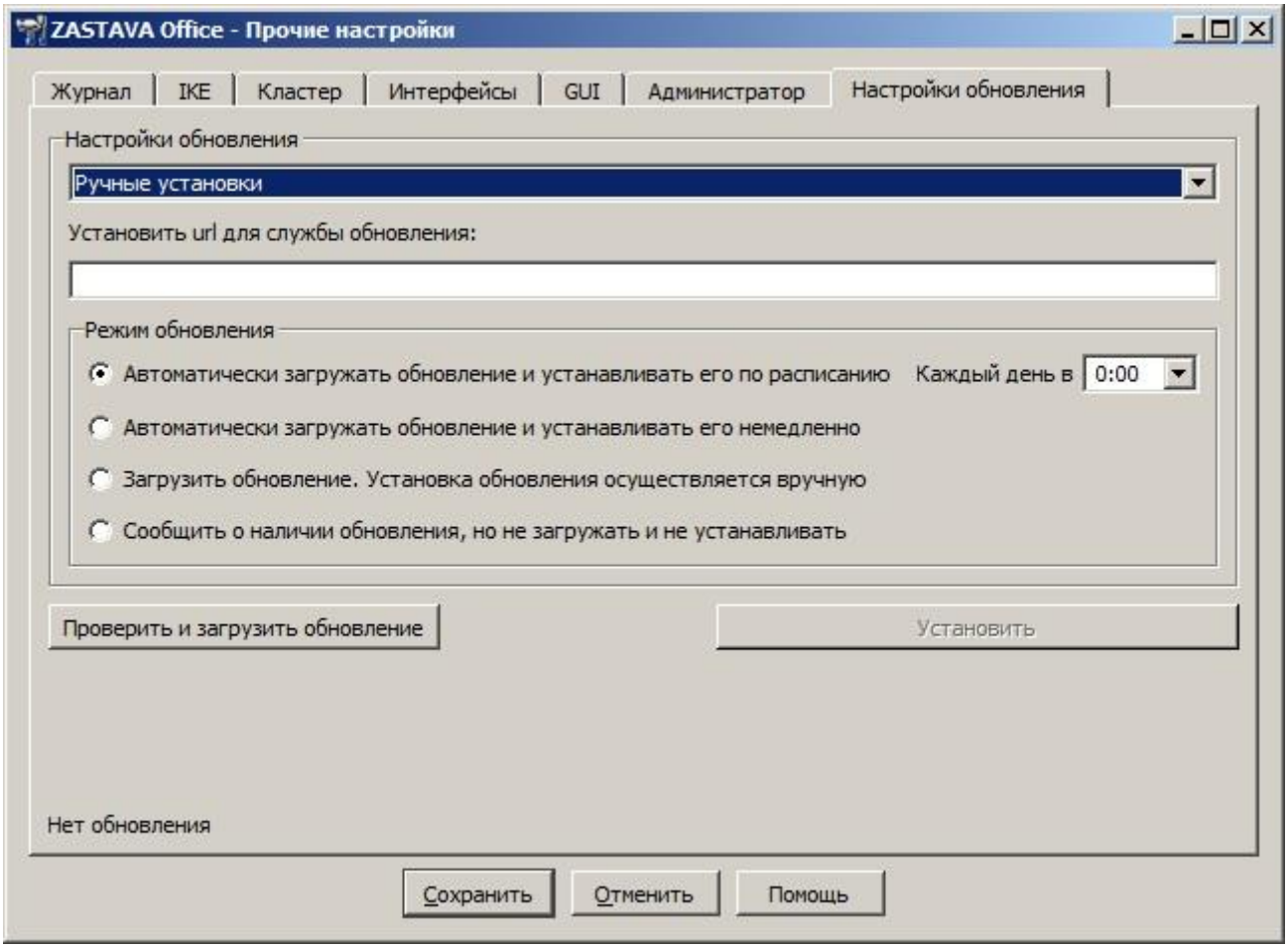

Рисунок 47 – Окно «Прочие настройки» с отображением вкладки «Настройки обновления»

Таблица 35 – Описание элементов интерфейса вкладки «Настройки обновления»

Элемент	Описание
Выпадающий список	Метод конфигурирования обновлений **Отключить автообновление** – автоматические обновления отключены. **Локальная политика безопасности** – конфигурирование обновлений выполняется централизованно, через *ЗАСТАВА-Управление* (параметры будут считываться *Агентом* из ЛПБ). **Ручные установки** – конфигурирование обновлений проводится вручную (т.е. в данном окне).
Установить url для службы обновления	(Учитывается только в методе конфигурирования **Ручные установки**) Адрес ресурса, к которому будет обращаться *Агент* при проверке обновлений.
Режим обновления	(Учитывается только в методе конфигурирования **Ручные установки**) Режим скачивания и инсталляции обновлений (4 варианта). Примечание. Формат строки расписания приведен в п. 3.8.7.2.
Кнопка «Проверить и загрузить обновление»	При нажатии кнопки проверяется соединение с указанным сервером и наличие свежей версии *ЗАСТАВА-Офис*. В случае успеха будет выведено соответствующее сообщение и можно будет запустить скачивание обновления.

Элемент	Описание
Кнопка «Установить»	Инсталлировать скаченное обновление.

3.8.7.2. Описание формата представления расписания

При выборе метода обновления по расписанию необходимо во всплывающем списке указать время, когда будет происходить обновление. Обновления будут происходить каждый день.

3.9. Окно «Помощь»

Интерактивная справочная система может использоваться для получения ответов на вопросы по работе с *ЗАСТАВА-Офис*. Если Вы испытываете трудности с созданием или редактированием объектов или у Вас есть вопросы относительно параметров, Вы можете воспользоваться справочной системой. Для вызова системы нажать кнопку «Помощь» на *Панели управления* и в выпадающем меню выбрать пункт «Помощь». В окнах *ЗАСТАВА-Офис* справочная система может быть вызвана с помощью клавиши <F1>, кнопки «Помощь» или команд «Помощь меню» (если возможно).

4. Интерфейс *Панели управления* рабочего стола

Текущий статус ЛПБ *ЗАСТАВА-Офис* можно просмотреть в нижней части *Панели управления ЗАСТАВА-Офис* (см. подраздел 3.1), также текущий статус отображается иконкой, расположенной на панели задач.

Имеются восемь иконок, каждая со своим собственным цветом, указывающим на текущий статус ЛПБ. Статус всегда показывается, независимо от того, открыт на Вашем рабочем столе *ЗАСТАВА-Офис* или нет.

При двойном нажатии на иконке левой кнопкой мыши открывается графический интерфейс *ЗАСТАВА-Офис*.

4.1. Контекстное меню

С помощью однократного нажатия правой кнопкой мыши на иконке статуса, расположенной на панели инструментов рабочего стола, можно запустить контекстное меню (см. Рисунок 48), выбрав параметр «Панель управления», получить справку по *ЗАСТАВА-Офис,* выбрав в выпадающем меню параметр «Помощь», открыть необходимое окно *Панели управления*, для настройки параметров, либо закрыть интерфейс *Панели управления* рабочего стола, выбрав параметр «Выход». *Панель управления ЗАСТАВА-Офис* можно запустить двойным нажатием на иконке статуса левой кнопкой мыши. на , или.

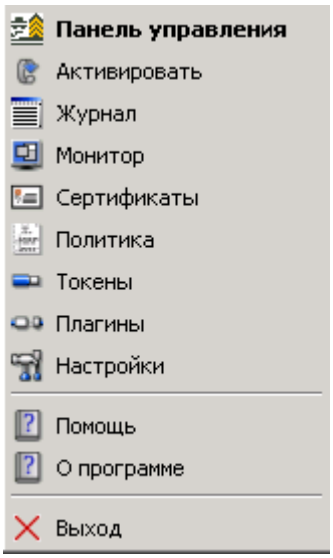

Рисунок 48 – Контекстное меню иконки статуса на панели инструментов рабочего стола

4.2. Ввод пароля токена

Когда *Агент* начинает инициировать создание защищенного соединения с сервером ЦУП. В процессе создания соединения при обращении к персональному сертификату будет запрошен пароль (PIN-код токена) хранилища персонального сертификата (см. Рисунок 49).

Также пароль запрашивается при любом обращении к персональному сертификату, например, при импорте персонального сертификата, удалении его из *ЗАСТАВА-Офис* и т.д.

Удостовериться в том, что у Вас запущен графический интерфейс *ЗАСТАВА-Офис*, в противном случае окно с запросом на ввод пароля токена не появится и защищенное соединение с сервером ЦУП не создастся.

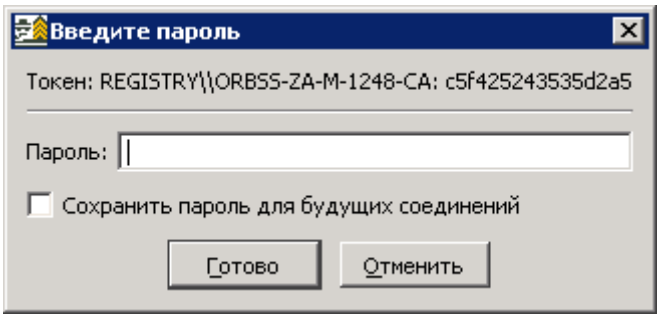

Рисунок 49 – Ввод пароля токена при создании защищенного соединения

4.3. Индикация текущего статуса

Поместив курсор поверх иконки и подождав несколько секунд, будет показана подсказка с подробной информацией о текущем статусе ЛПБ. Та же самая информация будет отображена в строке состояния *Панели управления*. Иконки и статусы представляются разными графическими символами (см. Таблица 36).

Таблица 36 – Перечень графических символов статусов ЛПБ

Статусы *ЗАСТАВА-Офис*	**Иконка (цвет)**
Ошибка активации; предыдущая политика не будет восстановлена. Прогружена любая другая политика, например, «Политика драйвера по умолчанию»	(красный)
Активирована текущая системная ЛПБ	(темно зеленый)
Ошибка активации; предыдущая политика будет восстановлена	(жёлтый)
Активирована «Политика драйвера по умолчанию»	(синий)
Системная служба *ЗАСТАВА-Офис* `vpndmn` остановлена	(серый)
При загрузки политики *ЗАСТАВА-Офис* с ЦУП (сервер доступен)	(темно зеленый с ярко зеленой рамкой)
При загрузки политики *ЗАСТАВА-Офис* с ЦУП (сервер не доступен)	(желтый с красной рамкой)

Также, в зависимости от текущего статуса ЛПБ, могут представляться следующие иконки (см. Таблица 37), иконка со статусом «Системная служба *ЗАСТАВА-Офис* `vpndmn` остановлена» никаких дополнительных статусов не имеет.

Таблица 37 – Иконка статуса. Дополнительные изображения к цвету иконки

Дополнительные статусы *ЗАСТАВА-Офис*	**Иконка (изображение внутри)**
Доступно обновление *ЗАСТАВА-Офис**	 (восклицательный знак)
Примечание. * – актуально для всех цветов кроме красного цвета иконки статуса	

5. Интерфейс командной строки

Интерфейс командной строки позволяет администратору автоматизировать процесс конфигурирования *ЗАСТАВА-Офис*. Интерфейс командной строки может также использоваться, если по некоторым причинам Вам более удобно работать с консольными приложениями, чем в оконной среде, или если оконный интерфейс отсутствует.

5.1. Мониторинг работы *ЗАСТАВА-Офис*

5.1.1. Обзор средств мониторинга

Для возможности осуществления мониторинга работы *ЗАСТАВА-Офис* используются следующие средства:

- Журналы регистрации событий (bin_log.txt, vpndmn_init.log);
- Dmesg, syslog
- Утилиты конфигурирования и мониторинга активности, входящие в комплект поставки *ЗАСТАВА-Офис.*

5.1.1.1. Файл регистрации системных событий

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

5.1.1.2. 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. 5.3.5. Это событие будет зарегистрировано и размещено в начале файла журнала.

5.2. 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.

5.2.1. Справочная система по работе с утилитой

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

5.2.2. 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 38).

Таблица 38 – 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 39). Подробное описание параметров статистики представлено в подразделе 3.3 (см. Таблица 4).

Таблица 39 – 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 Агентом 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

Параметр	Описание
Incoming anti-replay errors	Количество ошибок при подавлении атак воспроизведения во входящих пакетах
Dropped packets (in/out)	Отброшено пакетов (входящих/исходящих)
Input frags consumed	Количество использованных входных фрагментов
Output frags consumed	Количество использованных выходных фрагментов
Output frags created	Количество созданных выходных фрагментов
Decrease MTU requests	Количество пакетов-запросов на понижение MTU
Incoming packets not found in hash table	Количество промахов для входящих пакетов при поиске фильтра в хэш-таблице
Outgoing packets not found in hash table	Количество промахов для исходящих пакетов при поиске фильтра в хэш-таблице
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	Количество успешных (с ошибками или неуспешных)

Параметр	Описание
errors or failed) initiated/responded	обменов CREATE_CHILD_SA инициировано/отправлено в формате x(x)/x(x)
INFO exchanges completed (with errors or failed) initiated/responded	Количество успешных (с ошибками или неуспешных) обменов INFORMATIONAL инициировано/отправлено в формате x(x)/x(x)
HA	
Single start at	Время старта одиночного режима
Single start count	Количество переходов в одиночный режим
Active start count	Количество переходов в активный режим
Passive start count	Количество переходов в пассивный режим
Total recv/sent messages (bytes)	Объем полученных/ отправленных сообщений в байтах
Total errors in recv/sent messages	Количество ошибок при получении/отправке сообщений
Unknown messages(bytes) recv	Количество неизвестных сообщений (байт) при получении сообщений
Create IKE SA: recv/sent messages (bytes)	Объем полученных/ отправленных сообщений в байтах при создании IKE SA
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	Объем полученных/ отправленных сообщений в байтах

Параметр	Описание
(bytes)	при удалении записей IKE-CFG
IKE-CFG del: errors in recv/sent messages	Количество ошибок в полученных/ отправленных сообщениях при удалении записей IKE-CFG
IKE-CFG clear: recv/sent messages (bytes)	Объем полученных/ отправленных сообщений в байтах при обновлении сбросе записей IKE-CFG
IKE-CFG clear: errors in recv/sent messages	Количество ошибок в полученных/ отправленных сообщениях при сбросе записей IKE-CFG
FiltDB Cache	
Hash table size (bytes max/alloc)	Размер хэш-таблицы (байт максимум/выделено) в формате x*x*x(x/x)
Validity tag	Текущее значение метки, служащей для определения возможности использования записей в хэш-таблице
Live entries	Количество активных записей
Dead entries	Количество удаленных записей
Allocated entries	Количество записей выделенных из памяти
Dead reused	Количество повторно использованных удалённых записей
Line reused	Количество использованных записей в линиях
Collisions	Количество попыток добавления одинаковых записей
Full lines	Количество заполненных линий
Empty lines	Количество пустых линий
Other lines	Количество остальных линий
Avarage length of non-empty lines	Средняя длина непустых линий

Пример вывода результата команды `vpnmonitor -s`:

```
param                          |value
-------------------------------|------------------------------
IPsec                          |
Packets (bytes) recieved       |398 774 (69 396 140)
Packets (bytes) sent           |79 362 (15 988 088)
Decapsulated packets           |0
Encapsulated packets           |0
Packets recieved unsecure      |398 774
Packets sent unsecure          |79 362
Incoming errors                |0
Outgoing errors                |0
Incoming auth errors           |0
Incoming anti-replay errors    |0
Dropped packets (in/out)       |0 (0 / 0)
Input frags consumed           |0
```

```
Output frags consumed        |0
Output frags created         |0
Decrease MTU requests        |0
Incoming packets not found i~|45 171
n hash table                 |
Outgoing packets not found i~|842
n hash table                 |

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

HA mode: single

vpndmn started at: 2016.04.26 11:23:58
       worked: 23 hours 37 minutes 35 seconds
```

5.2.3. Вывод информации об активированной политике

Для просмотра информации об активированной на *ЗАСТАВА-Офис* 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 команду: 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: 56000000809305383 60CC5729B000000000080
            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

5.2.4. Просмотр информации по созданным 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
```

5.2.5. 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 40 и Таблица 41),

operation – операция для произведения сравнения по выбранному полю с эталоном (см. Таблица 41),

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 42).

Таблица 40 – Параметры фильтрации протокола IKE SA

Параметр	Характеристика
type	Тип создания SA
mode	Режим создания SA
role	Роль локальной машины при создании SA
state	Состояние IKE SA
eapid_local	Локальный EAP ID
ikeid_local	Локальный IKE ID
eapid_remote	EAP ID партнера
ikeid_remote	IKE ID партнера
id_remote	ID партнера
rule_name	Имя правила
algcipher	Алгоритм шифрования
alghash	Алгоритм хэширования
dhgroup	DH группа
algintegrity	Алгоритм контроля целостности
algprf	Псевдослучайная функция
local_ip	IP-адрес локального компьютера, использованный при создании защищенного соединения
local_port	UDP-порт на локальном компьютере, использованный при создании защищенного соединения
peer_ip	IP-адрес партнера, с которым создано защищенное соединение
peer_port	UDP-порт партнераа, 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 протокола IPsec SA приведены в таблице (см. Таблица 41).

Таблица 41 – 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)
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 42 – 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

Команда	Характеристика
	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) равен эталону (IP-адрес)
not_equal	значение поля (IP-адрес) не равен эталону (IP-адресу)
Операции для фильтрации по полю IP-порт	
equal	значение поля (порт) равно эталону
not_equal	значение поля не равно эталону
inrange	значение поля входит в диапазон заданный эталоном, в качестве эталона можно указать просто порт (8080) или диапазон (0...65535)
not_inrange	значение поля не входит в диапазон заданный эталоном
Операции для фильтрации по полю уровень лога	
equal	значение поля равно эталону (возможные значения: disabled, events, details, verbose)
not_equal	значение поля не равно эталону
gt	значение поля больше эталона (disabled < events < details < verbose)
lt	значение поля меньше эталона
gteq	значение поля больше или равно эталону
lteq	значение поля меньше или равно эталону

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

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

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

Существует возможность фильтрации списка установленных соединений по ID:

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

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

Пример:

```
vpnmonitor -i -view details dhgroup.not_contain(test1) or
local_ip.equal(test2)-ipsec-sa log_level.gt(test3) and
transform.not_iequal(test4)
```

5.2.6. Команды применимые к отфильтрованным SA

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

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

Для удаления всех SA используется команда:

```
vpnmonitor -i -clearikesa delpmp
```

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

5.2.7. 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 45).

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 (см. ниже);

– `orderby <field>` - сортировка по заданному полю;

– `delay <num>` - вывод команды с задержкой в заданное количество секунд;

– `tail <num>` - вывод последних <num> строк;

– `cmd <delete>` - удалить отфильтрованные значения (только для динамических фильтров).

Для задания правил фильтраций следует воспользоваться командой:

`vpnmonitor –f <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 43),

`operation` – операция для произведения сравнения по выбранному полю с эталоном (см. Таблица 44),

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

Таблица 43 – Параметры фильтрации протокола

Параметр	Характеристика
type	Параметр фильтрации по полю «Тип»
name	Параметр фильтрации по полю «Название»
action	Параметр фильтрации по полю «Действие»

Параметр	Характеристика
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 44 – Описание типов операций фильтрации

Команда	Характеристика
Операции для фильтрации по типу обмена	
equal	значение поля равно эталону
not_equal	значение поля не равно эталону
Операции для фильтрации по содержанию строк	
icontain	поле содержит подстроку (эталон), игнорируя регистр букв
not_icontain	поле не содержит подстроку (эталон), игнорируя регистр букв
contain	поле содержит подстроку (эталон), учитывая регистр букв
not_contain	поле не содержит подстроку (эталон), учитывая регистр букв
iequal	поле равняется эталону, игнорируя регистр букв
not_iequa	поле не равняется эталону, игнорируя регистр букв
equal	поле равняется эталону, учитывая регистр букв
not_equal	поле не равняется эталону, учитывая регистр букв

Команда	Характеристика
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 45 – 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.

5.2.8. 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 46).

Таблица 46 – 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
```

5.2.9. Просмотр статистики Algproxy

Команда `vpnmonitor –algproxy` позволяет просмотреть информацию о прокси-серверах, установленных на данном *ЗАСТАВА-Офис*.

5.2.10. Просмотр статистики RRI

В *ЗАСТАВА-Офис* для ОС ALT Linux 6 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 *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 *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`.

5.3. Утилита vpnconfig

Утилита конфигурирования `vpnconfig` предназначена для изменения и просмотра локальных установок *ЗАСТАВА-Офис*. При штатной работе *ЗАСТАВА-Офис* изменение локальных установок обычно не требуется и управление *ЗАСТАВА-Офис* производится централизованно при помощи ЦУП (путем внесения изменений в ЛПБ).

	В ОС Linux пользоваться утилитой vpnconfig могут только пользователь root и пользователи, добавленные системными средствами в группу, указанную в файле /var/vpnagent/localsettings.iniв параметре ADMIN_GROUP.
	Некоторые изменения вступают в силу только после того, как будет перезагружена ЛПБ.
	Некоторые изменения, например, активация ЛПБ, не могут быть отменены.

5.3.1. Справочная система по работе с утилитой

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

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

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

Также существует возможность получить подробную справку с примерами и описанием команд для этого ввести команду `vpnconfig -h all`.

5.3.2. Просмотр информации о *ЗАСТАВА-Офис*

Для получения информации о *ЗАСТАВА-Офис* необходимо воспользоваться командой:

```
vpnconfig -ver
```

Пример вывода команды `vpnmonitor -ver`:

```
Product name: ZASTAVA Office
Vendor name: AO ELVIS-PLUS
Product build: 6.1.16253
Product release: 6.1
Build date: 2016/03/30 17:35
Product/platform information: GATE WINXX amd64
```

5.3.3. Работа с сертификатами и ключами

Цифровые сертификаты и предварительно распределенные ключи необходимы, чтобы проверять подлинность партнеров по взаимодействию. Сертификаты (включая сертификаты УЦ), предварительно распределенные ключи, СОС регистрируются в *ЗАСТАВА-Офис*. Описание видов сертификатов и их параметров приведено в подразделе 3.4.

Предварительно распределённые ключи могут использоваться с *ЗАСТАВА-Офис* в качестве альтернативы использования сертификатов. Для получения более полной информации надо обратиться к п. 5.3.3.3.

ЗАСТАВА-Офис поддерживает СОС. Для получения более полной информации надо обратиться к п. 3.4.8.

5.3.3.1. Свойства Сертификата и его проверка

Для просмотра всех свойств сертификата необходимо узнать id сертификата, для этого 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 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 47).

Таблица 47 – 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. Субъектом сертификата может выступать УЦ, РЦ или конечный субъект
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 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
```

5.3.3.2. Регистрация и удаление Сертификатов

5.3.3.2.1. Регистрация сертификата

Вы можете регистрировать два типа X.509 сертификатов в *ЗАСТАВА-Офис:* сертификаты УЦ и сертификаты конечных пользователей (локальные и партнёров по связи). Для получения информации о типах сертификатов (см. п. 5.3.3).

Чтобы зарегистрировать новый сертификат УЦ в *ЗАСТАВА-Офис* необходимо произвести следующие действия:

1) Выполнить команду `vpnconfig –list token`, найти в появившемся списке токен `Trusted Certificates token` и запомнить его ID.
2) Выполнить команду `vpnconfig –add cert <file> password <password> pin <pin> ca token <token_id>`, где: `<password>` – пароль доступа к закрытому ключу, `<pin>` – пароль доступа к токену, `<token_id>` - ID для `Trusted Certificates token`.
3) В случае ввода корректного PIN-кода и пароля появится следующее сообщение, сигнализирующее об успешной регистрации сертификата:

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

Чтобы зарегистрировать новый персональный сертификат в *ЗАСТАВА-Офис* необходимо произвести следующие действия:

1) Выполнить команду `vpnconfig –add cert <path> [<password>]`, где: `[<password>]` – пароль доступа к контейнеру.
2) При импортировании Персонального сертификата необходимо ввести PIN-код токена в появившемся окне. После ввода PIN-кода нужно нажать кнопку «Готово».
3) Поставить флаг в поле «Save password for future requests», если требуется сохранить пароль токена для будущих соединений.
4) В случае ввода корректного PIN-кода появится следующее сообщение, сигнализирующее об успешной регистрации сертификата:

   `Password OK.`

```
Certificate is imported.
```

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

1) Скопировать содержимое контейнера, содержащего закрытый ключ и сертификат, можно с помощью СКЗИ «КриптоПро CSP» в реестр или на носитель.
2) *ЗАСТАВА-Офис* автоматически определит сертификат как «Персональный», по наличию ключа. Но, необходимо помнить, что для того чтобы была возможность использовать персональный сертификат необходимо, чтобы сеанс с токеном был открыт.

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

5.3.3.2.2. 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>]`.

5.3.3.2.3. Удаление сертификата

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

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

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

5.3.3.3. 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.

5.3.3.3.1. Регистрация предварительно распределенного ключа

Чтобы зарегистрировать предварительно распределенный ключ в *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:

   4) `token <token id>` – устройство для хранения предварительно распределенного ключа;
   5) `file <path>` – путь к файлу, содержащему значение ключа;
   6) `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.
```

5.3.3.3.2. 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
```

5.3.3.3.3. Удаление предварительно распределенного ключа

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

5.3.3.4. Списки отозванных сертификатов

СОС – 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. Подробное описание СОС представлено в п. 3.4.8. Списки Отозванных Сертификатов.

Для того чтобы просмотреть зарегистрированный СОС, следует выполнить команду `vpnconfig -list cert crl`.

5.3.3.4.1. Импортирование СОС вручную

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

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

СОС не может быть удален из *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 СОС вручную, импортируя файл.

5.3.4. 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.

5.3.4.1. Установка списка ЛПБ

ЛПБ может быть добавлена, изменена и активирована.

5.3.4.2. Настройка параметров политик

5.3.4.2.1. Системная ЛПБ

Системная политика может быть получена из файла, с сервера или отсутствовать.

Для изменения параметров системной политики необходимо воспользоваться утилитой `vpnconfig`.

Для настройки системной политики необходимо:

1) Выбрать тип метода активации из поля «Источник» и определить параметры данного метода:
2) При выборе метода прогрузки из файла необходимо выполнить команду `vpnconfig -set lsp system file <path>`, где: `path` – путь к файлу конфигурации.
3) При выборе метода прогрузки с сервера необходимо выполнить команду `vpnconfig -set lsp system pmp [<cert_id> <id_type> <server_ip> <log level> [<timeout>]]`, где:
   - `cert_id` – идентификатор сертификата; для просмотра `id` сертификата можно воспользоваться командой `vpnconfig -list cert personal;`
   - `<id_type>` – тип идентификатора для прогрузки политики, который должен быть согласован с ЦУП;

- `<server_ip>|<server_name>` – адрес сервера прогрузки|имя компьютера и порт. Если порт не указан, то берется значение по умолчанию (500). Если серверов несколько, IP-адреса указываются через запятую. Номер порта указывается через двоеточие. После регистрации ЛПБ *ЗАСТАВА-Офис* будет обращаться к заданному источнику всякий раз, когда политика активируется;
- `<log level>` – уровень журналирования событий;
- `<timeout>` – временной промежуток между обращениями к серверу.

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

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]`.

5.3.4.2.2. Политика драйвера по умолчанию

В *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).

Если на компьютере с *ЗАСТАВА-Офис* настроена удаленная аутентификация при входе пользователя в систему (например, аутентификация посредством домен-контроллера), то для ее правильной работы «Политика драйвера по умолчанию» должна быть: «Пропускать все».

5.3.4.2.3. Изменения сертификата/предварительно распределенного ключа 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`.

5.3.4.2.4. Уровень 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.

Для просмотра возможных уровней журнала надо выполнить команду `vpnconfig -set lsp loglevel`.

5.3.4.2.5. IKE идентификатор

Чтобы настроить получение ЛПБ с сервера политики необходимо указать IKE id, для этого нужно выполнить команду `vpnconfig -set lsp system|user idtype <id_type>`. Для изменения значения идентификатора нужно выполнить команду `vpnconfig -set lsp system idvalue <id_value>`.

5.3.4.2.6. Серверы политик

Чтобы настроить получение ЛПБ с сервера политики, необходимо указать IP-адрес(а) сервера, с которого будет получена политика для этого нужно выполнить команду `vpnconfig -set lsp system server <server_ip>`.

После регистрации ЛПБ *ЗАСТАВА-Офис* будет обращаться к заданному источнику всякий раз, когда политика активируется.

5.3.4.3. Активация ЛПБ

Для активации ЛПБ (т.е. для загрузки в драйвер *Агента*), необходимо узнать ее `<id>`, который содержится в выводе команды `vpnconfig –list lsp`. После этого необходимо выполнить команду `vpnconfig -activate lsp <id>`. ЛПБ загрузится в драйвер *Агента* и правила, определённые в ЛПБ, вступят в действие.

5.3.4.4. Просмотр ЛПБ

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

5.3.5. Регистрация событий

Конфигурирование регистрации событий происходит с помощью команды `vpnconfig -set log`, параметры команды представлены числами от 0 до 15 (см. Таблица 48).

Таблица 48 – Параметры команды `vpnconfig –set log`

Числовой параметр	Описание	Расшифровка
0	Log Level	Уровень регистрации событий
1	Log Level kernel	Уровень регистрации событий для уровня драйвера
2	File log	Включение или отключение параметра записи системных событий в файл
3	Max Log Size	Установка максимального размера файла записи системных событий
4	Backup Depth	Установка количества создаваемых резервных копий файла записи системных событий
5	Syslog	Включение или отключение параметра записи системных событий на syslog-сервер
6	Destination	Задание адреса удаленного syslog-сервера
7	Protocol	Протокол
8	Put msg len when use tcp	Выводить сообщение при использовании протокола tcp
9	Encoding from	Выбор алгоритма кодировки для открытия журнала событий
10	Encoding to	Выбор алгоритма кодирования сообщений записи системных событий
11	Facility	Настойка уровня протоколирования Syslog
12	Language	Установка языка журналирования

Числовой параметр	Описание	Расшифровка
13	Broadcast messages to terminals from vpndmn	Широковещательные сообщения терминалам от службы *ЗАСТАВА-Офис*
14	Verbose mode for application level	Установить отладочный уровень регистрации событий для уровня приложения
15	Verbose mode for kernel level	Установить отладочный уровень регистрации событий для уровня драйвера
16	Syslog Singleline	Удалять символы новой линии из сообщений

Регистрация событий позволяет сохранять хронологию системных событий, происходящих в *ЗАСТАВА-Офис*. Уровень регистрации событий может быть установлен командой `vpnconfig -set log 0 (Log Level) <0 (Disabled), 1 (Events), 2 (Details), 4 (Verbose)>`. Установить значение параметра «Disabled», если вы вообще не хотите регистрировать события.

Доступны следующие значения для уровня регистрации событий (в порядке от наименьшего количества информации к наибольшему):

- Заблокирован (Disabled) – События не будут регистрироваться;
- События (Event) – Будет регистрироваться минимальное количество информации об операциях, а также все сообщения об ошибках;
- Подробный (Details) – Будет регистрироваться полная информация об операциях (для поиска неисправностей);
- Отладочный (Verbose) – Все события будут зарегистрированы; уровень используется, в основном, для отладки.

При установке уровня регистрации «Отладочный» (Verbose) генерируется огромное количество сообщений. К примеру, информация об установлении одного защищенного соединения (SA) может занимать в журнале сообщений более 20 страниц. Используйте этот уровень с осторожностью.

Параметры уровня регистрации могут также указываться в ЛПБ, созданной *ЗАСТАВА-Управление* для *ЗАСТАВА-Офис*. В этом случае установки из ЛПБ будут иметь преимущество перед локальными установками. Посмотреть текущий реальный уровень регистрации событий можно, выполнив команду `vpnconfig -list log`, в выводе этой команды будет содержаться вся информация о настройках системы регистрации событий *ЗАСТАВА-Офис*.

Настройки системы регистрации событий (название архивных файлов журнала, их количество, максимальный размер файла журнала, настройки Syslog) хранятся в секции /LOG файла localsettings.ini, который располагается в одной из основных директорий *ЗАСТАВА-Офис*.

5.3.5.1. Файл регистрации событий

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

Записи о регистрируемых системных событиях хранятся в файле `bin_log.txt` в директории `C:\Program Files\ELVIS+\ZASTAVA Office\log`.

Для ОС Linux файлы регистрации событий располагаются в директории `/var/vpnagent/log/` (например: `bin_log.txt` и `vpndmn_init.log`).

Файл регистрации событий (`bin_log.txt`) может стать чрезвычайно большим и в итоге содержать устаревшую, ненужную информацию. Чтобы установить максимальный размер файла необходимо выполнить команду `vpnconfig -set log "3"`. Когда размер файла превысит заданное значение, текущий файл будет переименован в файл с другим именем, после чего будет начат новый файл.

Для задания количества создаваемых резервных копий необходимо выполнить команду `vpnconfig -set log "4" <value>`.

Для установки языка журналирования необходимо выполнить команду `vpnconfig -set log "12" <value>`. Возможные значения: 0 – Английский, 1 – Русский.

Для выбора алгоритма кодировки для открытия журнала регистрации событий необходимо выполнить команду `vpnconfig -set log "9" <value>`, где: `<value>` - алгоритм кодировки сообщений, возможные значения: KOI8-R, DOS-866, Win-1251, UTF-8.

Некоторые параметры уровней регистрации хранятся также в ЛПБ, созданной для *ЗАСТАВА-Офис*

5.3.5.2. Параметры журнала Syslog

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

Для включения или отключения параметра записи системных событий на syslog-сервер необходимо выполнить команду `vpnconfig -set log "5" <value>`, где: `<value>1/0/on/off/true/false/Enabled/ Disabled`.

Для выбора алгоритма кодирования сообщений необходимо выполнить команду `vpnconfig -set log "10" <value>`, где: `<value>` - алгоритм кодировки сообщений, возможные значения: KOI8-R, DOS-866, Win-1251, UTF-8.

Для задания адреса удаленного syslog-сервера необходимо выполнить команду `vpnconfig -set log "6" <value>,<value>` – адрес удалённого syslog-сервера.

Для настойки уровня протоколирования Syslog необходимо выполнить команду `vpnconfig -set log "11" <value>,<value>` - одно из значений от 0 до 7.

5.3.5.3. Удалённая регистрация событий

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

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

где: `<facility>` – одно из значений local0...local7, заданное в настройках *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`

5.3.6. 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>`.

5.3.6.1. 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 49).

Таблица 49 – Параметры протокола IKE

Номер параметра	Параметр	Расшифровка
0	IKEv1	Управление режимом работы IKEv1. Возможные значения: – Disabled – Enabled (используется по умолчанию) – Responder only
1	IKEv2	Управление режимом работы IKEv2 Возможные значения: – Disabled – Enabled (используется по умолчанию) – Responder only
2	IKE port	Номер порта для IKE-соединения (1-65535, по умолчанию 500)
3	NAT-T port	Порт для работы алгоритма NAT-Traversal. Трафик IKE будет переключен на этот порт, когда при установлении соединения между партнерами обнаруживается присутствие NAT-устройств. Значение по умолчанию: (1-65535, по умолчанию 4500)
4	Time to complete exchange (sec)	Максимальное время для создания защищенного соединения (SA). (5-600, по умолчанию 60)
5	Shortened time to complete exchange	Укороченное время для завершения обмена (3-60, по умолчанию 5)
6	Max half-open states	Максимальное количество стейтов IKE 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 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. Стейт 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 реальный, то инициатор повторно посылает запрос, включая в него COOKIE. Такие запросы считаются ответчиком подтвержденными и минуют проверку на превышение описываемого параметра

Номер параметра	Параметр	Расшифровка
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)
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 сторонними агентами.
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)

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

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

Некоторые дополнительные параметры протокола IKE хранятся в ЛПБ, создаваемой для *ЗАСТАВА-Офис* в *ЗАСТАВА-Управление*.

5.3.6.1.1. 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 50.

Таблица 50 – Режимы работы обработки CRL

Числовое значение	**Режим работы обработки CRL**
0	Disabled. Обработка CRL выключена. Поиск и проверка CRL не производятся ни для какого сертификата
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.

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

5.3.6.1.2. Политика выбора метода работы через NAT

Управление политикой выбора метода работы через NAT осуществляется из локальных настроек *ЗАСТАВА-Офис*. В зависимости от выбранного числового значения параметра с id = 15 политика может быть следующей (см. Таблица 51).

Таблица 51 – 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).

Числовое значение	Политика
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 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.

5.3.7. Настройка кластера

ЗАСТАВА-Офис может быть установлен на кластерную информационную систему. Поддержка кластера позволяет построить высоконадёжную отказоустойчивую систему. ОС, на основе которой реализован кластер, узлом кластера может быть любой из компьютеров, на которых функционирует *ЗАСТАВА-Офис*. Кластерное ПО должно быть соответствующим образом настроено.

Для просмотра установленных настроек кластерной системы необходимо выполнить команду vpnconfig –list ha. Вывод результата выполнения данной команды будет содержать информацию об установленных настройках кластера.

Пример вывода для ОС Linux:

```
# |Parameter                          |Value
0 |Command to execute after LSP activation|
1 |Mode                               |Disabled
2 |Cluster Key                        |
3 |Multicast group                    |234.56.78.90
4 |Multicast port                     |35476
5 |Multicast filter log level         |Events
6 |Multicast interface                |
```

Параметры кластера приведены в таблице (см. Таблица 52).

Таблица 52 – Параметры для настройки кластера

№	Имя	Значение

№	Имя	Значение
0	Command to execute after LSP activation	Системная команда, которая должна быть выполнена после активации ЛПБ (не обязательное поле)
1	Mode	Режим работы *ЗАСТАВА-Офис*: 1 (Disabled) – режим кластера не используется; 2 (Multicast) – позволяет работать в кластерном режиме (используется в ОС Linux); 3 (Multicast keepalive) – позволяет работать в кластерном режиме
2	Cluster Key	Буквенно-цифровая последовательность, использующаяся для шифрации трафика между узлами кластера
3	Multicast group	Групповой адрес режима Multicast из диапазона 224.0.0.0 до 239.255.255.255.
4	Multicast port	Порт режима Multicast (любое десятичное целое число).
5	Multicast filter log level	Уровень регистрации событий режима Multicast: – Запрещен – События не будут регистрироваться; – События – Будет регистрироваться минимальное количество информации об операциях, а также все сообщения об ошибках; – Подробный – Будет регистрироваться полная информация об операциях (для поиска неисправностей); – Отладочный – Все события будут зарегистрированы; уровень используется, в основном, для отладки
6	Multicast interface	Интерфейс, использующийся в режиме Multicast

5.3.7.1. Настройка режима кластера для ОС Linux

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

1) Для включения режима кластера необходимо *для каждого узла кластера* выполнить следующие настройки:
   - Установить режим «Multicast», выполнив команду `vpnconfig –set ha 1 multicast`.
   - Задать одинаковое для всех узлов кластера значение ключа (Cluster Key), выполнив команду `vpnconfig –set ha 2 <значение ключа>`.
   - Определить групповой адрес режима «Multicast» из диапазона 224.0.0.0 до 239.255.255.255, выполнив команду `vpnconfig –set ha 3 <адрес>`.
   - Указать порт для режима «Multicast», выполнив команду `vpnconfig –set ha 4 <port_id>`.

– Ввести одинаковое для всех узлов кластера значение ключа QCD, выполнив команду `vpnconfig –set ike 16 <ключ в 16-ричном формате>`.

2) Для настройки синхронизации *для каждого узла кластера* необходимо указать адрес интерфейса, который будет использоваться для синхронизации кластерных узлов, выполнив команду выполнив команду `vpnconfig –set ha 6 <interface_id>`.
3) Указать уровень регистрации событий для фильтра Multicast, выполнив команду `vpnconfig –set ha 5 <log_level>`.

5.3.8. Модули токенов

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

5.3.8.1. Просмотр модулей токенов

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

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

5.3.8.2. Добавление Модулей токенов

Для регистрации модуля PKCS#11 в *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.

Если Вы используете в качестве токена смарт-карту или USB-брелок, требуемое ПО должно входить в комплект поставки токена.

5.3.8.3. Удаление Модуля токена

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

5.3.9. Работа с токенами

5.3.9.1. Просмотр зарегистрированных токенов

Для просмотра всех зарегистрированных токенов необходимо выполнить команду `vpnconfig –list token`. Будет выведена информация о каждом токене. Пример вывода результата данной команды:

```
Token
  Id: 5
  Label: REGISTRY\\TEST
  Model: \TEST
  Manufacturer: ELVIS-PLUS
  Serial Number: c545543545
  Hardware Version: 2.0
  Firmware Version: 4.1
  Logged In: No
  Trusted: No
  Login required: Yes
  Algorithms:
    GOST R 34.10-2001
      Key Length: 512
      Hash Algorithms: GOST 34.11-94
    GOST R 34.10-2012 512
      Key Length: 1024
      Hash Algorithms: GOST 34.11-2012 512
    GOST R 34.10-2012 256
      Key Length: 512
      Hash Algorithms: GOST 34.11-2012 256

Token
  Id: 6
  Label: Trusted Certificates token
  Model: Trusted Token
  Manufacturer: ELVIS-PLUS
  Serial Number: 29092009
  Hardware Version: 2.0
```

```
Firmware Version: 2.0
Logged In: Yes
Trusted: Yes
Login required: Yes
```

5.3.9.2. 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 (см. п. 5.3.9.1), `<pin>` – PIN-код токена, `[save]` – необязательный параметр, если его не установить, то *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>`.

5.3.9.3. 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 *ЗАСТАВА-Офис.*

5.3.10. 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.

5.3.11. Настройки обновления

С помощью утилиты `vpnconfig` можно выполнить настройку автоматического обновления. Для просмотра всех параметров автоматического обновления необходимо выполнить команду `vpnconfig –list update`.

Для ввода/редактирования параметров обновления следует выполнить команду и задать <id> необходимого параметра и его значение `vpnconfig -set update <id> <value>`. Где: `<id>` - идентификатор параметра обновлений, `<value>` - значение выбранного параметра.

Параметры обновления приведены в таблице (см. Таблица 53).

Таблица 53 – Параметры обновления

Номер параметра	**Параметр**	**Расшифровка**
0	Check Inetval (sec)	Интервал запроса обновления с сервера. Доступные значения 0 до 4294967295 Значение по умолчанию 1800
1	Path	Путь для сохранения загруженного обновления
2	Available Update Version	Версия доступного обновления
3	Downloaded Update Version	Версия загруженного обновления
4	Update Version	Версия для обновления
5	Schedule	Параметр для установки расписания обновлений (Учитывается только в методе конфигурирования Ручные установки)
6	Setting	Метод конфигурирования обновлений Возможные значения: 13 Disable - Отключить автообновление – автоматические обновления отключены. 14 LSP - ЛПБ – конфигурирование обновлений выполняется централизованно, через *ЗАСТАВА-Управление* (параметры будут считываться *Агентом* из ЛПБ) . 15 Local - Ручные установки – конфигурирование обновлений проводится вручную.
7	URL	(Учитывается только в методе конфигурирования Ручные установки) Адрес ресурса, к которому будет обращаться *Агент* при проверке обновлений.

Номер параметра	Параметр	Расшифровка
8	Mode	(Учитывается только в методе конфигурирования Ручные установки) Режим скачивания и инсталляции обновлений (4 варианта).
9	Available Update Name	Имя доступного обновления
10	Download path	Путь к папке с обновлениями (при конфигурировании обновлений через *ЗАСТАВА-Управление*)
11	Update URI	Адрес ресурса, к которому будет обращаться *Агент* при проверке обновлений (при конфигурировании через *ЗАСТАВА-Управление*)
12	Always verify downloaded files	Включение/отключение проверки хэш-сумм при загрузке обновлений: true – проверять 0 – не проверять (не рекомендуется)

5.4. Утилита plg_ctl

Модуль управления криптобиблиотеками (криптоплагинами) – встроенный программный модуль, предназначенный для подключения криптобиблиотек, используемых в *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 *ЗАСТАВА-Офис* как отдельный модуль (плагин). По умолчанию в состав *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 ОС 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.

5.4.1. 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.

5.4.1.1. Действия

Утилита `plg_ctl` поддерживает следующие действия, представленные в таблице (см. Таблица 54).

Таблица 54 – Действия, поддерживаемые утилитой `plg_ctl`

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

5.4.1.2. Опции

Утилита `plg_ctl` поддерживает следующие опции, представленные в таблице (см. Таблица 55).

Таблица 55 – Опции, поддерживаемые утилитой `plg_ctl`

Ключ	Название	Описание
-k	Kernel (уровень ядра)	Выполнить операции только с криптобиблиотеками уровня ядра ОС. 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`.

Ключ	Название	Описание
-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`

5.4.2. 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`

5.4.3. 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.

5.4.4. 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`

5.4.5. Примеры команд в интерфейсе командной строки

Примеры команд в интерфейсе командной строки приведены в таблице (см. Таблица 56).

Таблица 56 – 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.

5.5. 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
```

ПРИЛОЖЕНИЕ 1. *ЗАСТАВА-ОФИС* ВЫСОКОЙ НАДЁЖНОСТИ (С ПОДДЕРЖКОЙ HIGH AVAILABILITY)

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 *ЗАСТАВА-Офис* в составе кластера, необходимо произвести следующие настройки:

- синхронизировать время на всех узлах;
- установить *ЗАСТАВА-Офис* на все узлы кластера;
- настроить прогрузку политики (из файла или по PMPv2);
- включить и настроить режим кластера в графическом интерфейсе *ЗАСТАВА-Офис* (см. ниже), либо через интерфейс командной строки (см. п. 5.3.7);
- для настройки кластера на ОС ALT Linux установить ПО «keepalived» и описать виртуальные интерфейсы кластера в файле keepalived.conf.

Настройка кластера в ОС Linux

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

1) Для включения режима кластера необходимо *для каждого узла кластера* выполнить следующие настройки (см. Рисунок 44):
   - На вкладке «Кластер» установить для параметра «Режим» значение «Multicast».
   - На вкладке «Кластер» в поле «Ключ кластера» ввести одинаковое для всех узлов кластера значение ключа.
   - На вкладке «IKE». В поле «Ключ QCD» ввести одинаковое для всех узлов кластера значение ключа в 16-ричном формате.
2) Для настройки синхронизации, необходимо *для каждого узла кластера* на вкладке «Кластер» в строке «Milticast интерфейс» указать адрес интерфейса, который будет использоваться для синхронизации кластерных узлов.

3) Указать уровень регистрации событий для фильтра Multicast, выбрав соответствующее значение параметра «Multicast интерфейс».
4) Нажать кнопку «Сохранить» для применения сделанных изменений.

ПРИЛОЖЕНИЕ 2. КОНФИГУРИРОВАНИЕ МОДУЛЯ ТОКЕНОВ

Существует возможность конфигурировать поведение Softtoken common с помощью конфигурационного файла pkcs11.cfg. Файл pkcs11.cfg расположен в директории /etc/vpnagent (для ОС ALT Linux).

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» версии 3.6.1, «КриптоПро CSP» версии 3.9 или «КриптоПро CSP» версии 4.0 в зависимости от комплектации и исполнения *ПК «VPN/FW «ЗАСТАВА», версия 6,* (по умолчанию) 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.

ПРИЛОЖЕНИЕ 3. КОНФИГУРИРОВАНИЕ МОДУЛЯ VPNPCAP

Существует возможность конфигурировать поведение модуля vpnpcap в ОС ALT Linux 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 при отсутствии связи с сервисом:
  - 2 - PASS(default);
  - 1 – DROP.

Для задания этих параметров необходимо выполнить следующе команды:

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

ПРИЛОЖЕНИЕ 4. КОНФИГУРИРОВАНИЕ МОДУЛЯ CP_PLG_CPRO

Для конфигурирования модуля cp_plg_cpro-36r2 используется параметр max_handles. Параметр Max_handles - максимальное количество хэндлов СКЗИ «КриптоПро CSP» версии 3.6.1, «КриптоПро CSP» версии 3.9 или «КриптоПро CSP» версии 4.0 в зависимости от комплектации и исполнения *ПК «VPN/FW «ЗАСТАВА», версия 6*, параметр влияет на максимальное количество IPsec SA, которые могут быть установлены. По умолчанию данный параметр равен 262140.

Для изменения этого параметра необходимо выполнить следующие команды:

- в ОС ALT Linux:
  - /etc/init.d/vpngate stop
  - /sbin/rmmod cp_plg_cpro36;
  - /sbin/modprobe cp_plg_cpro-36r2 max_handles=120000;
  - /etc/init.d/vpngate start

Аналогичные операции необходимо выполнить для настройки модуля `cp_plg_cpro-40`.

В ОС ALT Linux x32-битной версии есть ограничение на количество SA около 16000, при этом количество хэндлов СКЗИ «КриптоПро CSP» версии 3.6.1, «КриптоПро CSP» версии 3.9 или «КриптоПро CSP» версии 4.0 в зависимости от комплектации и исполнения *ПК «VPN/FW «ЗАСТАВА», версия 6* не обязательно менять (по умолчанию стоит 256000 или 0x40000), максимальный предел количества хендлов установлен в 0x01000000, что соответствует 1 млн. SA.

Для многопоточной обработки с использованием 8 ядер количество SA приблизительно в 60 раз меньше и составляет 200 SA для 32-битной версии, и 16 тысяч, для 64-битной версии

ПРИЛОЖЕНИЕ 5. ИНИЦИАЛИЗАЦИИ ДСЧ «КРИПТОПРО CSP» ВНЕШНЕЙ ГАММОЙ

Для корректной работы «КриптоПро CSP» требуется инициализация встроенного датчика случайных чисел. При наличии аппаратного ДСЧ инициализация встроенного датчика происходит автоматически при инициализации криптоплагина crypto_cpro_user. При использовании «КриптоПро CSP» КС1 и отсутствии аппаратного ДСЧ необходимо инициализировать встроенный ДСЧ с помощью внешней гаммы.

Для инициализации встроенного ДСЧ с помощью внешней гаммы необходимо:

1) На АРМ выработки внешней гаммы необходимо сгенерировать внешнюю гамму, согласно документации «ЖТЯИ.00050-02 90 04. КриптоПро CSP. АРМ выработки внешней гаммы». Необходимое количество случайных отрезков гаммы должно быть два
2) На АРМ с «ЗАСТАВА-Офис» запустить «КриптоПро CSP» от имени администратора, перейти во вкладку «Оборудование» и выбрать пункт «Настроить ДСЧ»

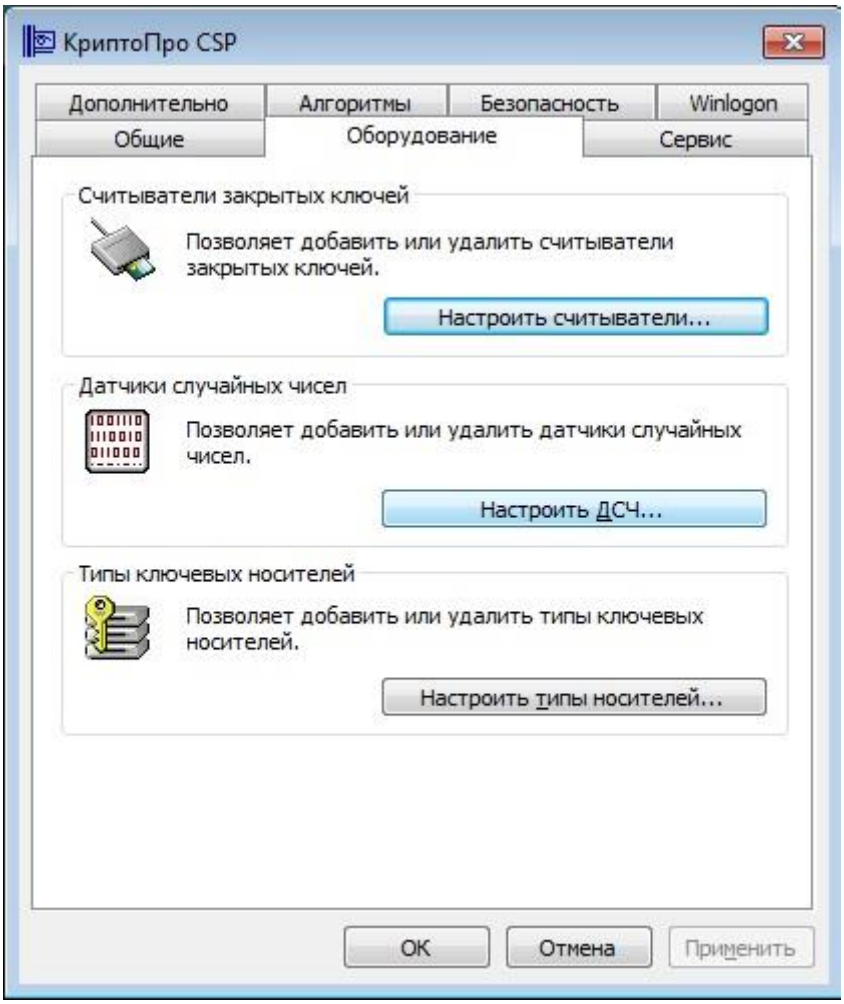

Рисунок 50 – «КриптоПро CSP» вкладка Оборудование

3) В появившемся окне выбрать «Добавить»

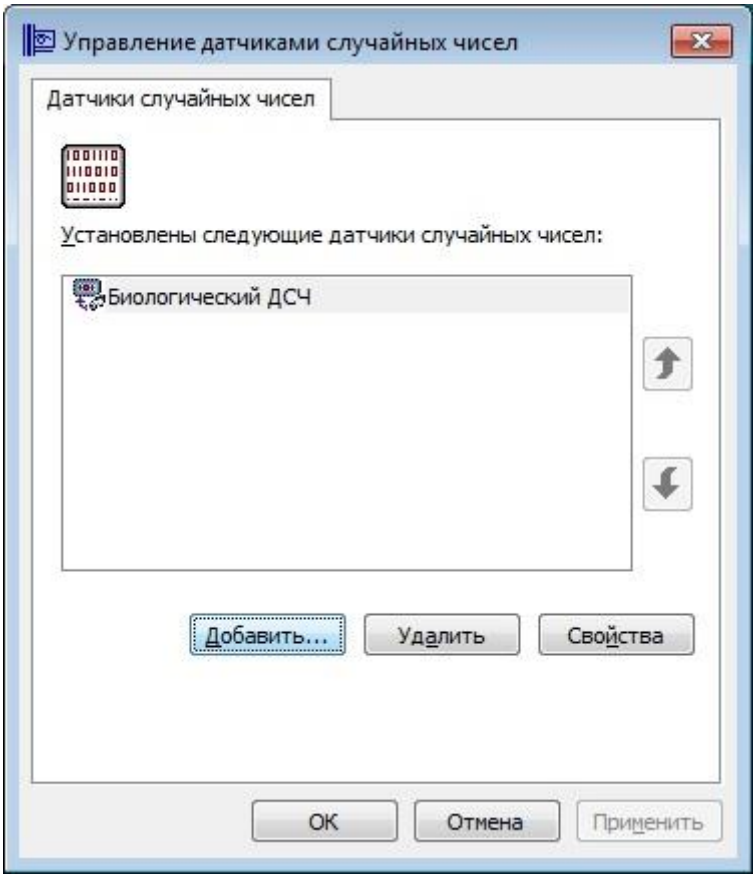

Рисунок 51 – «КриптоПро CSP» Управление датчиками случайных чисел

4) В запустившемся мастере установки ДСЧ нажать «Далее»

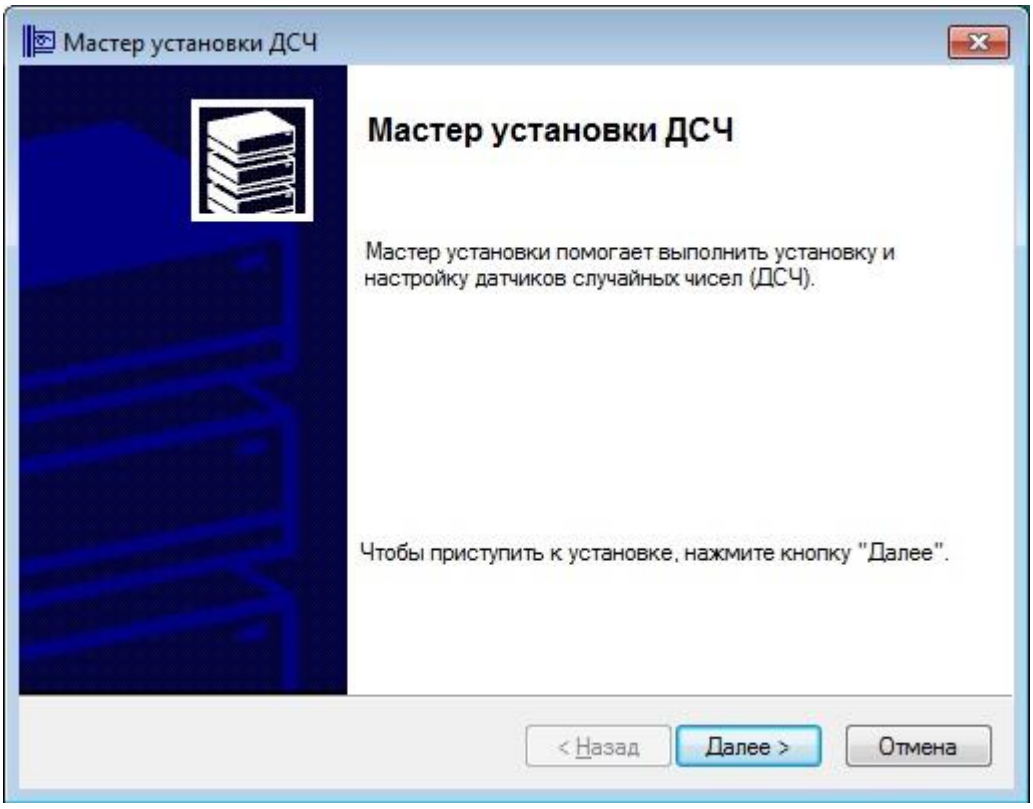

Рисунок 52 – «КриптоПро CSP» Запуск мастера установки ДСЧ

5) Выбрать «КриптоПро исходный материал», нажать «Далее»

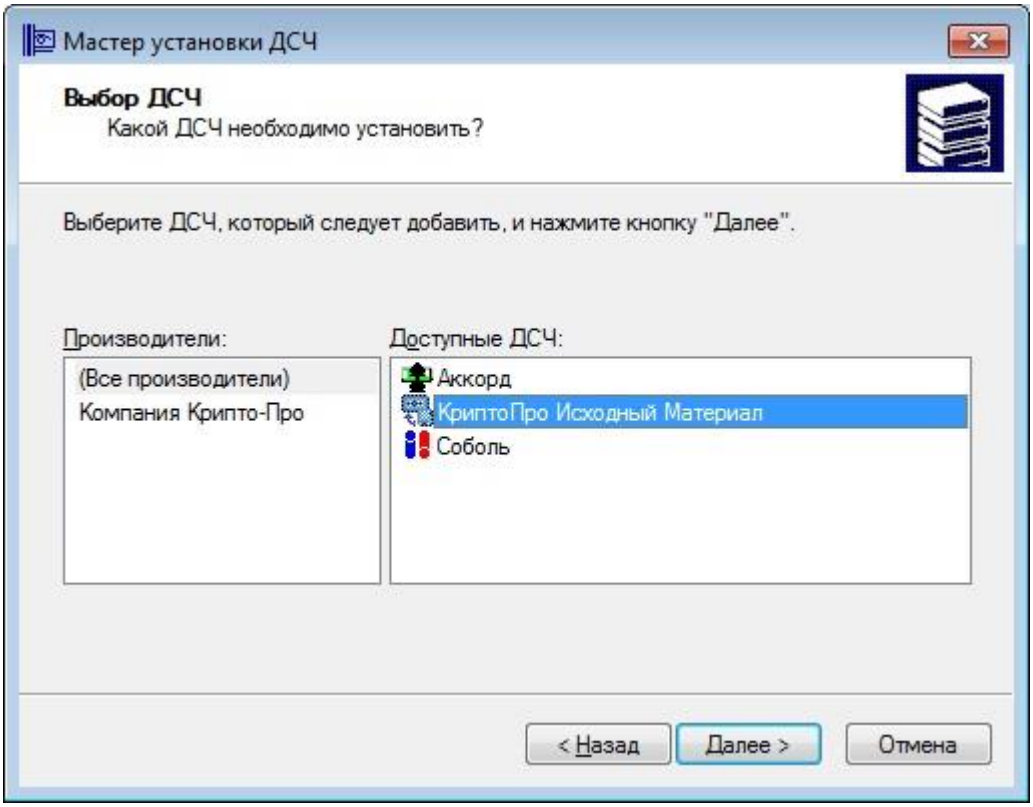

Рисунок 53 – «КриптоПро CSP» Выбор ДСЧ

6) Ввести имя ДСЧ, нажать «Далее»

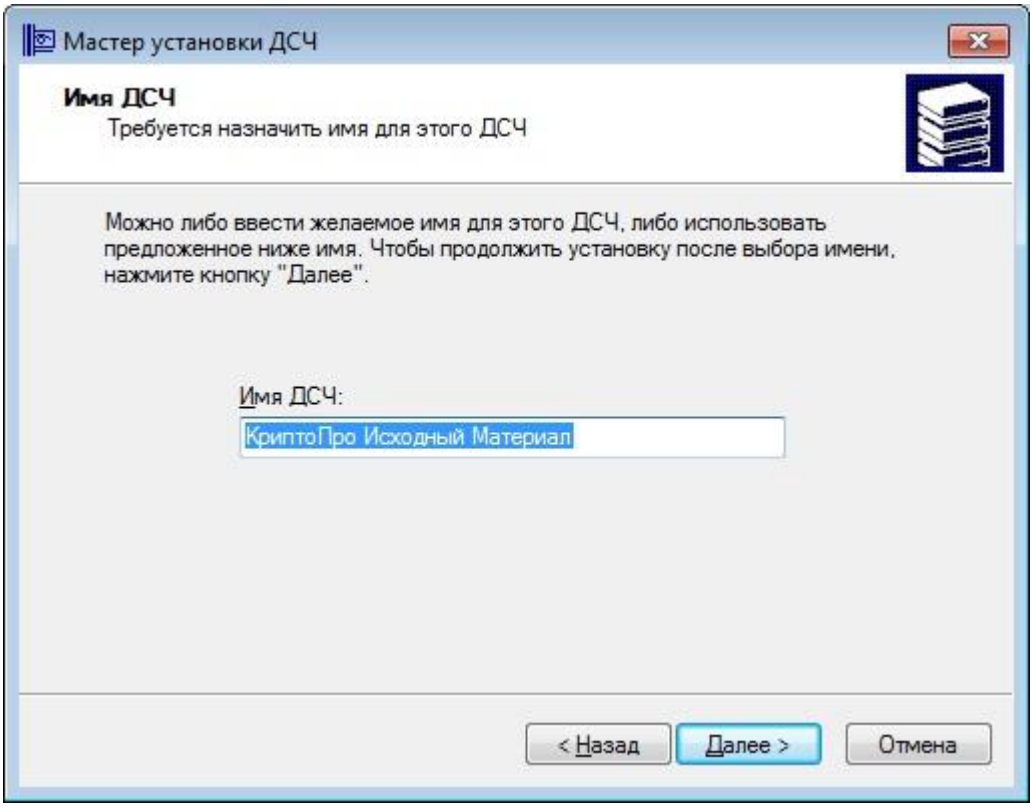

Рисунок 54 – «КриптоПро CSP» Ввод имени ДСЧ

7) Указать путь к папкам, где находятся папки db

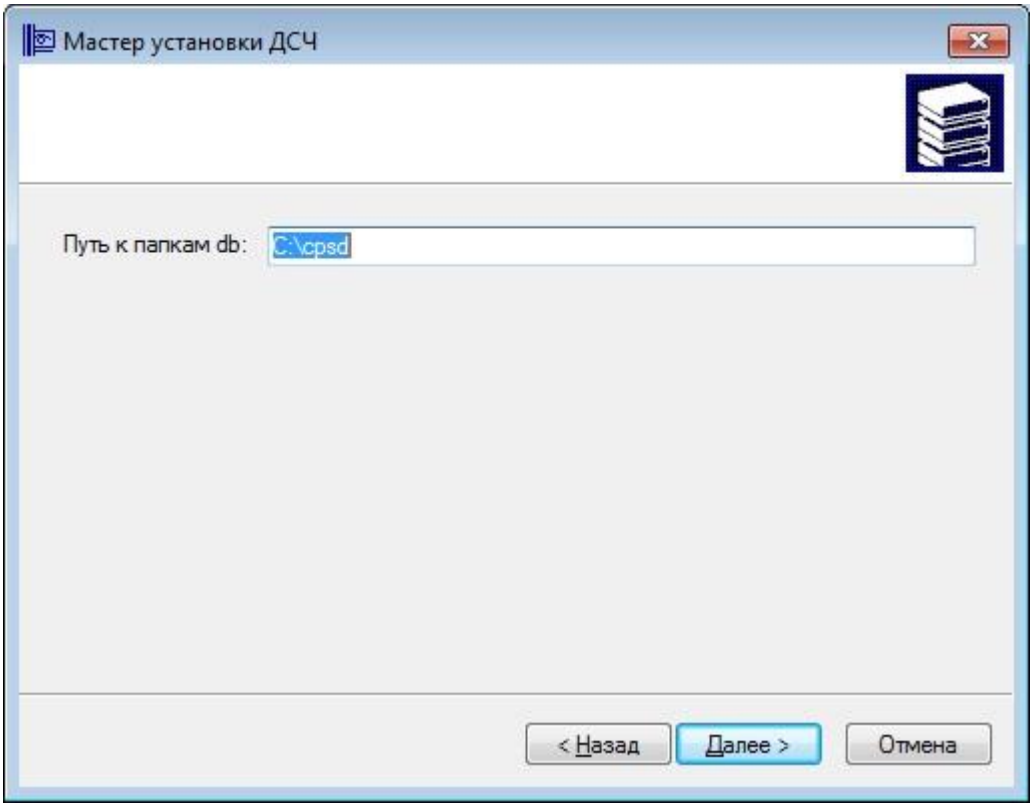

Рисунок 55 – «КриптоПро CSP» Указание путик папке

8) Нажать «Готово», перезагрузить компьютер

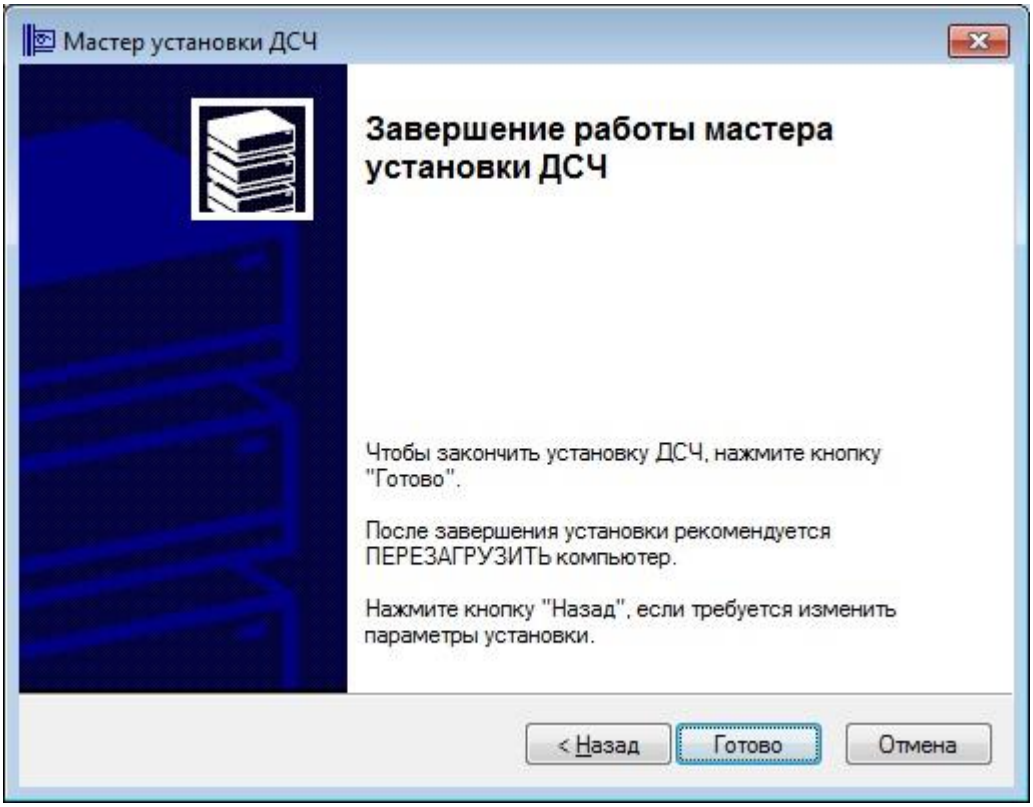

Рисунок 56 – «КриптоПро CSP» Завершение работы мастера ДСЧ

9) Убедиться, что после перезагрузки компьютера в журнале «ЗАСТАВА-Офис» присутствует запись: [crypto_cpro_user] CryptoPro info: Ver: 3.9, PKZI: 8227, SKZI: 8001, Type: RELEASE(0), Arch: AMD64(4), OS: WINDOWS(0), RNG: Hardware

Для инициализации встроенного ДСЧ с помощью внешней гаммы на ОС семейства Linux необходимо:

1) На АРМ выработки внешней гаммы необходимо сгенерировать внешнюю гамму, согласно документации «ЖТЯИ.00050-02 90 04. КриптоПро CSP. АРМ выработки внешней гаммы». Необходимое количество случайных отрезков гаммы должно быть два
2) На АРМ с «ЗАСТАВА-Офис» разместить файлы с данными, полученными на АРМ выработки внешней гаммы, по следующему пути: /var/opt/cprocsp/dsrf/
3) Выполнить следующие команды КриптоПро CSP:

```
./cpconfig -hardware rndm -add cpsd -name 'cpsd rng' -level 3
./cpconfig -hardware rndm -configure cpsd -add string /db1/kis_1 /var/opt/cprocsp/dsrf/db1/kis_1
./cpconfig -hardware rndm -configure cpsd -add string /db2/kis_1 /var/opt/cprocsp/dsrf/db2/kis_1
```

4) Перезагрузить компьютер
5) Убедиться, что после перезагрузки компьютера в журнале «ЗАСТАВА-Офис» присутствует запись: [crypto_cpro_user] CryptoPro info: Ver: 3.9, PKZI: 8227, SKZI: 8001, Type: RELEASE(0), Arch: AMD64(4), OS: WINDOWS(0), RNG: Hardware

Приложение 6. Устранение неисправностей

п/н	Описание неисправностей	Решение
1	Конфигурирование «КриптоПро CSP» 3.6.1 Смена исполнения провайдера - KC1, KC2.	*/opt/cprocsp/sbin/<arch>/cpconfig -defprov -view -provtype 75 :* показать список установленных провайдеров СКЗИ «КриптоПро CSP» типа 75 (ГОСТ Р 34.10-2001) */opt/cprocsp/sbin/<arch>/cpconfig -ini '\cryptography\Defaults\Provider Types\Type 075\Name' -view:* показать провайдер по умолчанию типа 75 */opt/cprocsp/sbin/<arch>/cpconfig -defprov -setdef -provtype 75 -provname 'Crypto-Pro GOST R 34.10-2001 KC2 CSP':* установить провайдер по умолчанию типа Crypto-Pro GOST R 34.10-2001 KC2 CSP */opt/cprocsp/sbin/<arch>/cpconfig -license -set <license> :* Установить лицензию СКЗИ «КриптоПро CSP» */opt/cprocsp/bin/<arch>/csptest -keys -verifycontext :* показать версию СКЗИ «КриптоПро CSP» */opt/cprocsp/sbin/amd64/cpconfig -hardware reader -del FLASH :* Удалить аппаратный считыватель "FLASH"

Перечень принятых терминов и сокращений

Ниже приведен список русско- и англоязычных сокращений и отдельных специальных терминов, используемых в компонентах ПК «VPN/FW «ЗАСТАВА», версия 6. Некоторые (в основном, англоязычные) сокращения и термины употребляются только во внутренних идентификаторах программ и приведены здесь для справки.

БД – база данных

ВЧС - виртуальная частная сеть

Агенты – собирательное название для линейки управляемых агентов безопасности (*ЗАСТАВА-Клиент, ЗАСТАВА-Офис*)

ЗРС - Запрос Регистрации Сертификата

ЛВС - локальная вычислительная сеть

ЛПБ - локальная политика безопасности (в контексте ПК «VPN/FW «ЗАСТАВА», версия 6)

ОС - операционная система

ПК – программный комплекс

ПО - программное обеспечение

РЦ - Регистрационный центр

СКЗИ - средство криптографической защиты информации

СОС - список отозванных сертификатов

УЦ – Удостоверяющий центр

ЦУП - Центр управления политиками безопасности *ЗАСТАВА-Управление*

CA (Certification Authority) - см. УЦ

CER (Certificate Enrollment Request) - см. ЗРС

CLI (Command Line Interface) - интерфейс командной строки

CRL (Certificate Revocation List) – см. СОС

CRL Distribution Point - Точки распространения СОС

DHCP - стандартный протокол получения клиентами IP-адреса и другой информации от централизованного DHCP-сервера

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

ESP (Encapsulated Security Payload) - протокол из группы IPsec

GMT – время по Гринвичу

GUI (Graphical User Interface) - графический интерфейс пользователя

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»)

Log - журнал регистрации

Log level - уровень детализации при регистрации событий

LSP (Local Security Policy) - см. ЛПБ

MIB (Management Information Base) - структурированный (в виде дерева) набор параметров, используемых протоколом SNMP

NAT (Network Address Translation) – трансляция сетевых адресов

PKI (Public Key Infrastructure) – инфраструктура открытых ключей (комплекс программных средств и методик для работы с цифровыми сертификатами)

PMP (Policy Management Protocol) - протокол распределения политики безопасности (в контексте ПК «VPN/FW «ЗАСТАВА», версия 6)

RRI (Reverse Route Injection) – механизм сязей и управления топологией VPN

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

SNMP (Simple Network Management Protocol) - протокол управления в IP-сетях

TCP – сетевой протокол транспортного уровня (с гарантированной доставкой) в IP-сетях

UDP – сетевой протокол транспортного уровня (без гарантированной доставки) в IP-сетях

VPN (Virtual Private Network) - см. ВЧС

Перечень ссылочных документов

[1] МКЕЮ.00626-01 32 01 «Программный комплекс защиты корпоративных вычислительных ресурсов на сетевом уровне с использованием технологий VPN и распределенного межсетевого экранирования на основе интернет-протоколов семейства IPsec/IKE «VPN/FW «ЗАСТАВА-Клиент», версия 6 КС1» («VPN/FW «ЗАСТАВА-Клиент», версия 6 КС1») Руководство системного программиста».

[2] МКЕЮ.00631-01 32 01 «Программный комплекс «VPN/FW ЗАСТАВА-Управление», версия 6 КС3» («VPN/FW ЗАСТАВА-Управление», версия 6 КС3») (исполнение ZM-WS64-VO-03) Руководство системного программиста».

Лист регистрации изменений

Изм.	Номера листов (страниц)				Всего листов (страниц) в документе	Номер документа	Входящий номер сопроводительного документа и дата	Подпись	Дата
	изме–ненных	заме–ненных	новых	изъя–тых					