УТВЕРЖДЕН

МКЕЮ.00626-01 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 «ПК «ЗАСТАВА-Клиент»», версия 6 КС1»

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

Руководство системного программиста

МКЕЮ.00626-01 32 01

Листов 168

Инв.№ подл.	Подп. и дата	Взам. инв. №	Инв.№ дубл.	Подп. и дата
7390				

2021

Содержание

1.Введение

1.1. О данном документе

Настоящий документ описывает функциональные возможности, особенности конфигурирования и применения 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 «ПК «ЗАСТАВА-Клиент»», версия 6 КС1» («VPN/FW «ПК «ЗАСТАВА-Клиент»», версия 6 КС1») (далее – ПК «ПК «ЗАСТАВА-Клиент»» 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 компонента, 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 компонентам, 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 ПК «ПК «ЗАСТАВА-Клиент»» и ознакомиться с работой компонента, надо обратиться к разделу 2 Подготовка к использованию *ПК «ЗАСТАВА-Клиент»*.

Для того чтобы узнать, как осуществлять навигацию по структуре окон ПК «ПК «ЗАСТАВА-Клиент»», надо обратиться к разделу 3 Работа в графическом интерфейсе *ПК «ЗАСТАВА-Клиент»*.

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

Чтобы узнать, как конфигурировать локальные установки *ПК «ЗАСТАВА-Клиент»*, надо обратиться к разделу 3 Работа в графическом интерфейсе *ПК «ЗАСТАВА-Клиент»*.

Для получения информации по использованию токенов для хранения конфиденциальных данных надо обратиться к подразделу 3.6 Окно «Токены».

Для того чтобы узнать, как конфигурировать *ПК «ЗАСТАВА-Клиент»*, используя интерфейс командной строки и просмотреть список доступных команд, надо обратиться к разделу 5 Интерфейс командной строки.

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

1.2. О *ПК «ЗАСТАВА-Клиент»*

1.2.1. Назначение

ПК *«ЗАСТАВА-Клиент»* предназначен для защиты корпоративных вычислительных ресурсов на сетевом уровне модели взаимодействия OSI/ISO (на уровне TCP/IP-протокола) с использованием технологий VPN и распределенного межсетевого экранирования на основе интернет - протоколов семейства IPsec.

ПК *«ЗАСТАВА-Клиент»* обеспечивает выполнение криптографических функций: шифрования, контроля целостности данных, имитозащиту данных, открытого распределения криптографических ключей.

ПК *«ЗАСТАВА-Клиент»* обеспечивает контроль и фильтрацию сетевых пакетов в соответствии с заданными правилами, а также защиту криптографическими методами передаваемой по каналам связи информации конфиденциального характера.

В качестве СКЗИ ПК *«ЗАСТАВА-Клиент»* обеспечивает выполнение криптографических функций: шифрования, контроля целостности данных, имитозащиту данных, открытого распределения криптографических ключей, что обеспечивает:

- конфиденциальность передаваемой в корпоративной информационно-телекоммуникационной сети (ИТКС) информации, за счет ее шифрования с использованием режима гаммирования (CTR) и зацепления блоков (CBC), согласно ГОСТ 28147-89;
- защиту доступа к корпоративным вычислительным ресурсам за счет использования протоколов двухсторонней криптографической аутентификации при установлении соединений на базе протокола IKEv2 с использованием алгоритмов подписи в соответствии с ГОСТ Р 34.10-2012;
- контроль целостности данных посредством вычисления значения их хэш-функции в соответствии с ГОСТ Р 34.11-2012;
- имитозащиту данных на основе применения ГОСТ 28147-89 в режиме имитовставки;
- поддержку схемы открытого распределения ключей Диффи-Хеллмана на основе алгоритма ГОСТ Р 34.10-2012 VKO в 256-битном режиме.

1.2.2. Область применения

Компонент *ПК «ЗАСТАВА-Клиент»* предназначен для работы на компьютерах с операционной системой (ОС) Windows XP SP3, ОС Windows 7, ОС Windows 8 платформы ia32 и x64, ALT Linux 6.0 платформы ia32, x64, ALT Linux 7.0 платформы ia32, x64, находящихся в локальных, корпоративных и глобальных сетях, где в качестве протокола сетевого уровня используется протокол IP v4, и необходим для защиты информации при передаче ее через сети общего пользования.

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

1.2.3. Характеристики

1.2.3.1. Защита трафика и фильтрация

Компонент *ПК «ЗАСТАВА-Клиент»* 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 IKEv1 и 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 IP v4-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 работы в режиме «мобильного пользователя» (когда IP-адрес компьютера назначается динамически, т. е. заранее неизвестен);

— Поддержка «горячего» резервирования Шлюзов Безопасности (компьютеров с установленным компонентом МКЕЮ.00627-01 «ЗАСТАВА-Офис», версия 6 (далее - *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 *ПК «ЗАСТАВА-Клиент»* предусмотрены:

— Поддержка работы при наличии в сети промежуточных устройств с трансляцией сетевых адресов (NAT) путем инкапсуляции IPsec в UDP. Для протокола IKEv1 поддерживаются следующие версии NAT-Traversal:

1) draft-huttunen-ipsec-esp-in-udp-01;

2) draft-ietf-ipsec-nat-t-ike-02;

3) draft-ietf-ipsec-nat-t-ike-03;

4) RFC3947.

— 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* (*ПК «ЗАСТАВА-Клиент», ЗАСТАВА-Офис* - обычно употребляется собирательный термин *Агенты*) используются X.509 V3 сертификаты в соответствии с RFC 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 *ПК «ЗАСТАВА-Клиент»* предусмотрены использование СОС и поддержка получения сертификатов и СОС через протокол LDAP и HTTP.

1.2.3.4. Инсталляция и конфигурирование

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

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);

— Отправкой SNMP-трапов (сообщений) на NMS-систему.

1.2.3.6. Стандарты и совместимость с другими продуктами

ПК «ЗАСТАВА-Клиент» 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

Psec: 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

RFC5280	Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile	http://www.ietf.org/rfc/rfc5280.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

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 *ПК «ЗАСТАВА-Клиент»* должно удовлетворять следующим минимальным требованиям:

- Процессор, эквивалентный Intel Pentium III, с частотой 600 МГц;
- Оперативная память – от 512 Мбайт;
- Разрешение монитора 1024×768 пикселей.

На компьютере, на который устанавливается *ПК «ЗАСТАВА-Клиент»,* должна быть уставлена одна из следующих ОС:

- ОС Windows XP SP3, ОС Windows 7, ОС Windows 8 платформы ia32 и x64;
- ОС ALT Linux 6.0 платформы ia32, x64, ALT Linux 7.0 платформы ia32, x64.

2.Подготовка к использованию *ПК «ЗАСТАВА-Клиент»*

Перед началом установки надо убедиться в том, что устанавливаемая версия *ПК «ЗАСТАВА-Клиент»* соответствует версии ОС.

Перед установкой ПК «ЗАСТАВА-Клиент» необходимо инсталлировать на компьютер СКЗИ «КриптоПро CSP».

	Чтобы инсталлировать и деинсталлировать *ПК «ЗАСТАВА-Клиент»* Вы должны иметь права администратора ОС
	Удостовериться в том, что дата, время и настройки часового пояса правильно установлены на Вашем компьютере. Необходимо правильно определить эти параметры, иначе может оказаться, что срок действия сертификатов истек, и Вы не можете установить *ПК «ЗАСТАВА-Клиент»*
	Длина пароля администратора ОС, на которой устанавливается *ПК «ЗАСТАВА-Клиент»,* 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.

При настройке, конфигурировании и создании политики безопасности в части шифрования, контроля целостности и взаимной аутентификации администратор безопасности должен руководствоваться требованиями настоящего документа.

2.1. ОС семейства Windows

2.1.1. Установка ПК «ЗАСТАВА-Клиент»

Для инсталляции *ПК «ЗАСТАВА-Клиент»* необходимо произвести следующие действия:

1) Закрыть все открытые программы.
2) Вставить в CD-привод инсталляционный диск, найти папку с дистрибутивом *ПК «ЗАСТАВА-Клиент»* и запустить программу установки (zastavaclient.exe). Запустится Мастер установки (см. Рисунок 1).

Для запуска установки *ПК «ЗАСТАВА-Клиент»* в режиме журналирования необходимо воспользоваться интерфейсом командной строки и с помощью средств Windows Installer выполнить команду:

<путь к инсталляционному дистрибутиву> /l*v <путь к файлу журнала>, где: l – указатель для журналирования при установке, v – уровень регистрации событий «verbose». Файл журналирования процедуры установки обычно сохраняется в директории c:\Program Files\ELVIS+\ZASTAVA Client с именем vpn_agent_install.log.

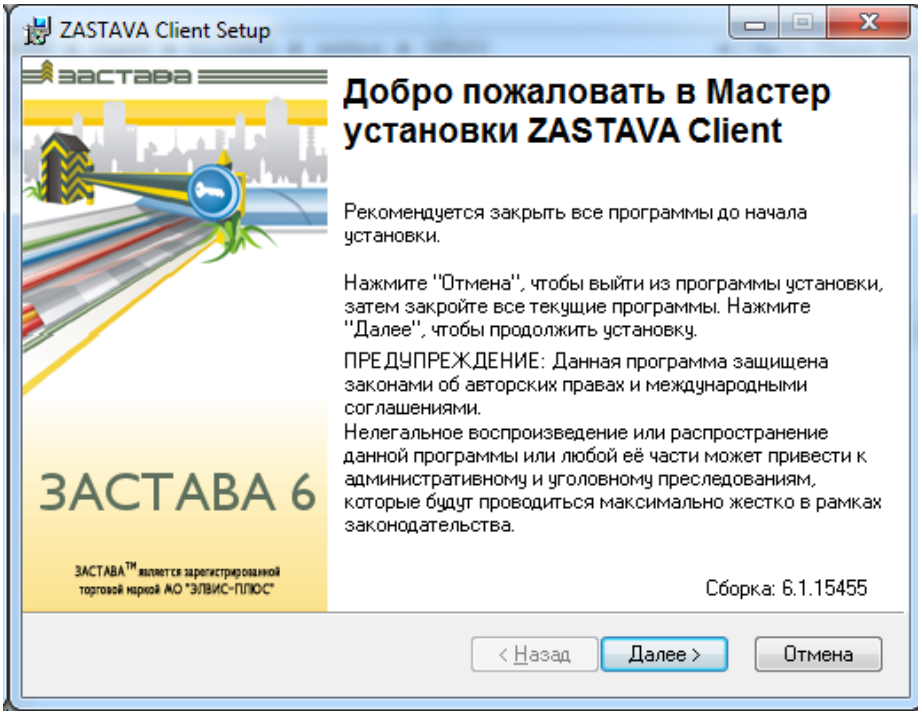

Рисунок 1 – Запуск Мастера установки

3) Подтвердить согласие с приведенным в окне лицензионным соглашением (см. Рисунок 2).

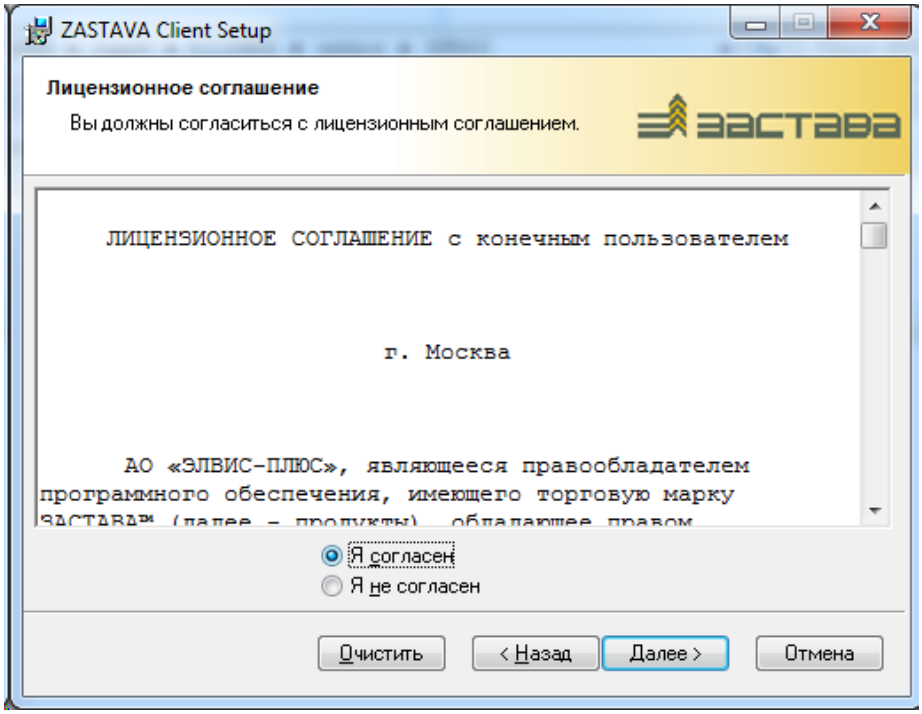

Рисунок 2 – Окно с лицензионным соглашением

4) Для указания папки, в которую будет установлен *ПК «ЗАСТАВА-Клиент»*, надо нажать кнопку «Изменить» и сделать выбор (см. Рисунок 3).

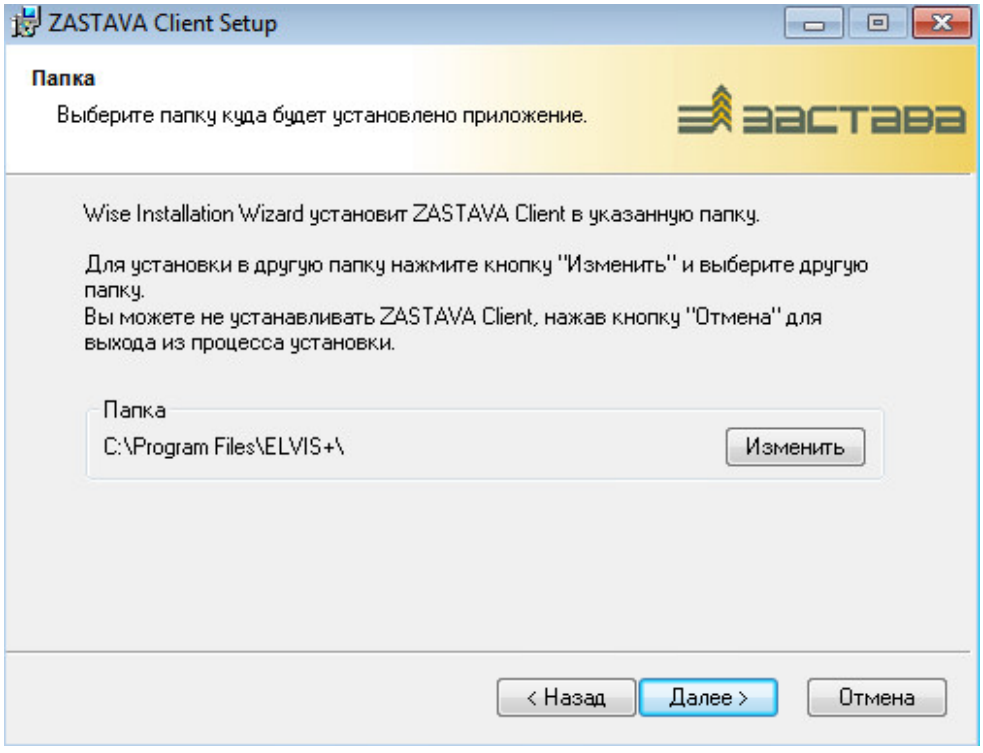

Рисунок 3 – Выбор папки для установки *ПК «ЗАСТАВА-Клиент»*

5) В окне «Выбор компонент» выбрать программные модули, которые Вы хотите инсталлировать, или оставить все значения по умолчанию (см. Рисунок 4).

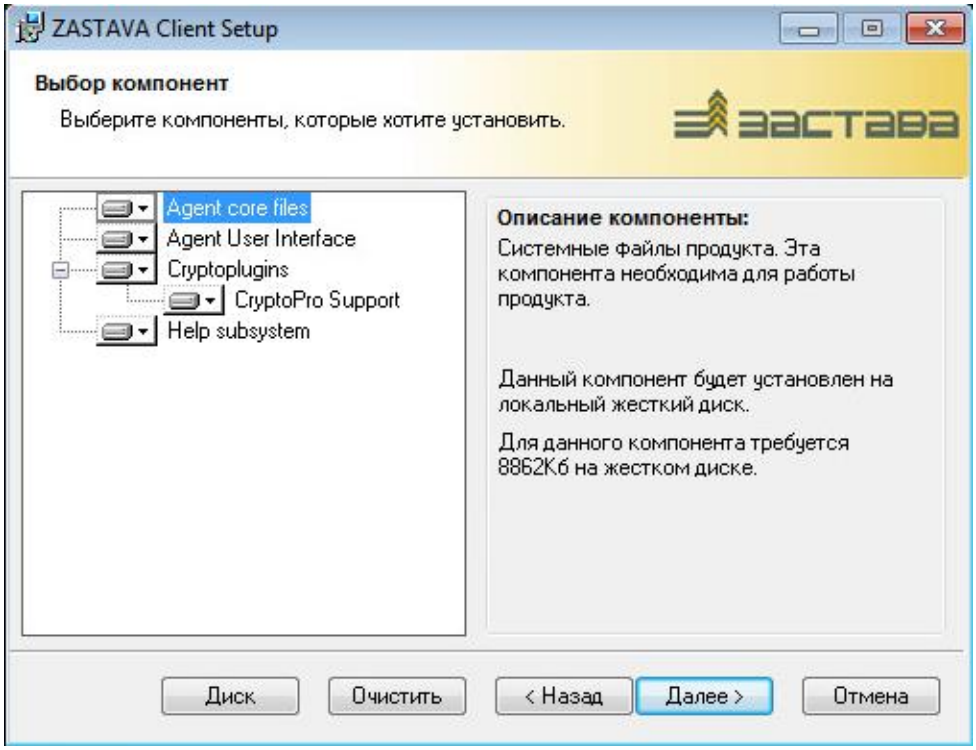

Рисунок 4 – Выбор устанавливаемых компонентов *ПК «ЗАСТАВА-Клиент»*

6) Если в ОС не установлен компонент SNMP (Simple Network Management Protocol), то появится окно с соответствующим предупреждением (см. Рисунок 5). Можно продолжить инсталляцию, нажав кнопку «ОК», либо, при необходимости использования SNMP-функций центра управления политиками (ЦУП), прервать инсталляцию и установить требуемые компоненты ОС согласно инструкции в окне.

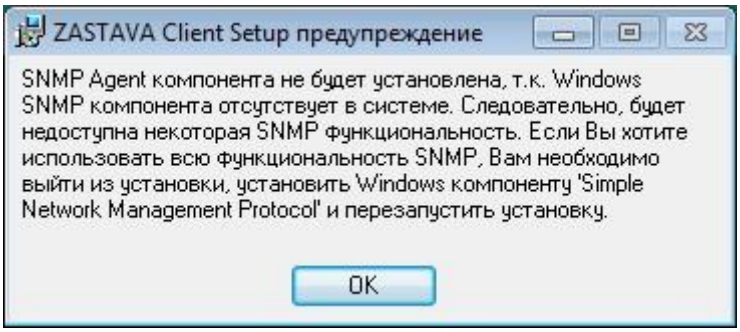

Рисунок 5 – Предупреждение о неустановленном компоненте SNMP

7) Если в ОС активен Брандмауэр Windows, то необходимо добавить компонент *ПК «ЗАСТАВА-Клиент»* в список его исключений, для этого надо отметить соответствующий флаг и нажать кнопку «Далее» (см. Рисунок 6).

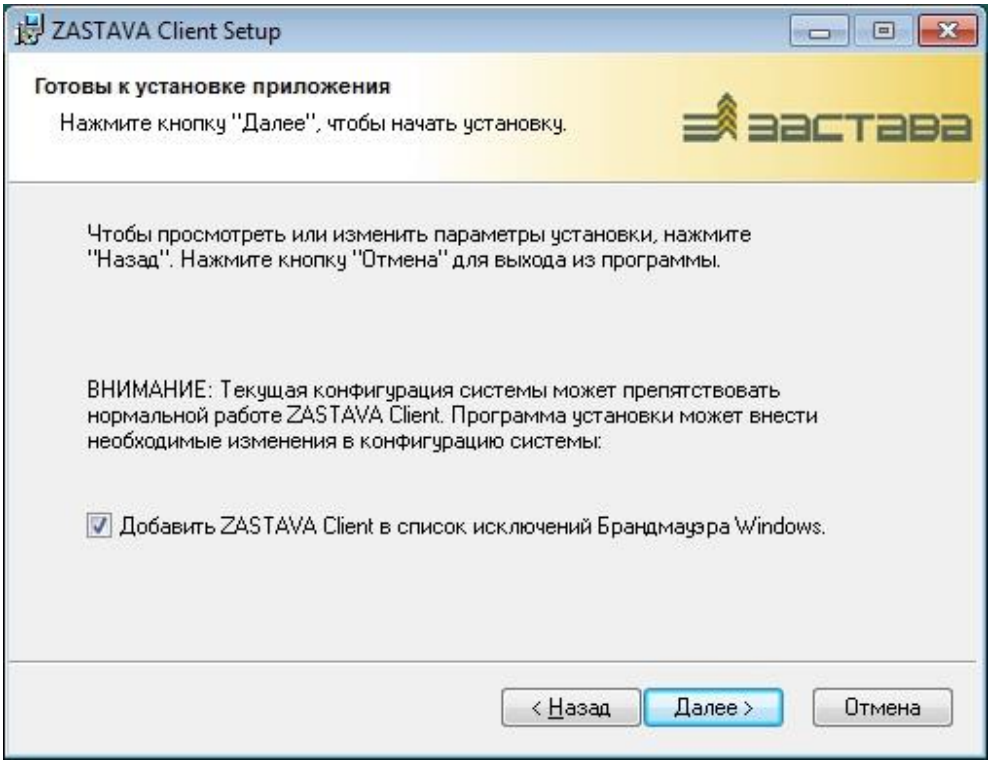

Рисунок 6 - Добавление *ПК «ЗАСТАВА-Клиент»* в список исключений Брандмауэра Windows

8) После завершения инсталляции нажать кнопку «Готово» (см. Рисунок 7).

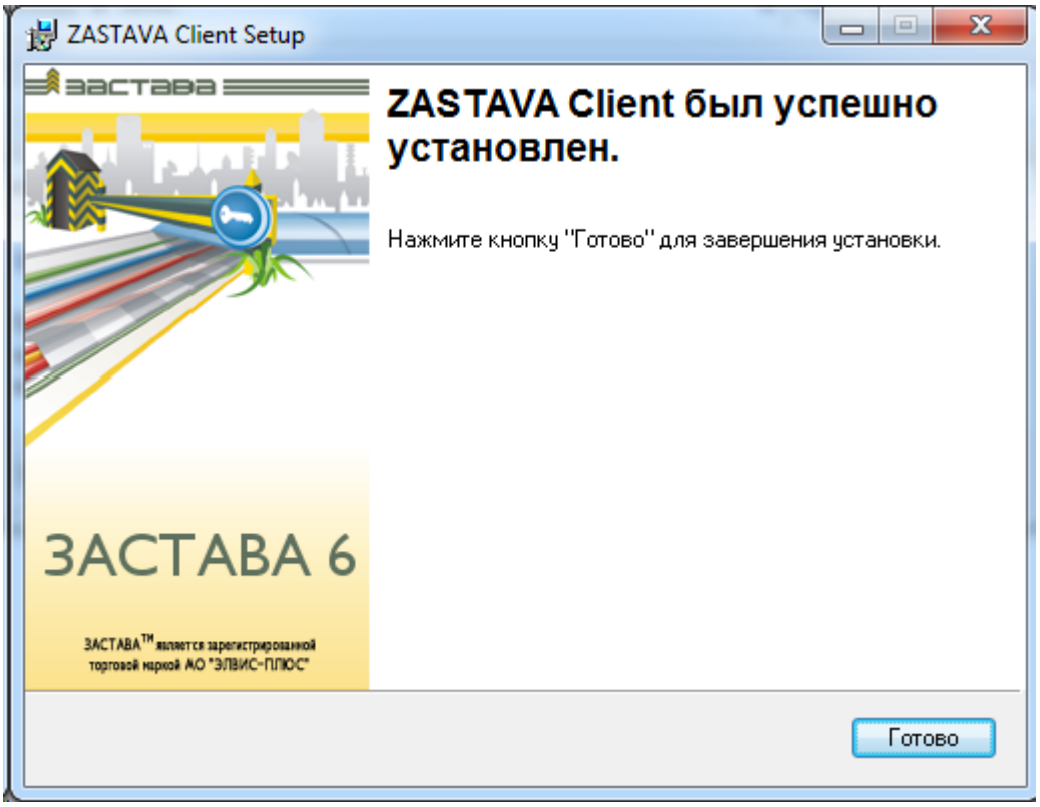

Рисунок 7 – Завершение установки

9) При необходимости перезагрузить компьютер.

В течение инсталляции *ПК «ЗАСТАВА-Клиент»*, содержимое самоизвлекающегося файла zastavaclient.exe извлекается во временный каталог. Обычно, этот каталог c:\Documents and Settings\<user_name>\ Local Settings\Temp; Вы можете проверить этот путь, используя Start→Settings→Control Panel→ System→Advanced→Environment Variables. Обычно, эти извлеченные файлы автоматически не удаляются после инсталляции. Вы можете удалить эти файлы вручную, когда инсталляция будет закончена.

ПК «ЗАСТАВА-Клиент» содержит Application Proxy модули для нескольких протоколов (FTP, SOCKS, HTTP). Поэтому, если в Вашей ОС уже присутствуют серверы для данных протоколов, то после инсталляции *ПК «ЗАСТАВА-Клиент»* возможен конфликт портов, из-за чего данные серверы или Application Proxy серверы *ПК «ЗАСТАВА-Клиент»* могут оказаться неработоспособными.

2.1.2. Обновление ПК «ЗАСТАВА-Клиент»

ПК «ЗАСТАВА-Клиент» поддерживает процедуру автоматического обновления (настройки данной процедуры в графическом интерфейсе *ПК «ЗАСТАВА-Клиент»* описаны в п.3.8.4, настройка с помощью утилиты командной строки описана в п. 5.3.9), которая позволяет загружать и устанавливать свежие версии *ПК «ЗАСТАВА-Клиент»*. Конфигурирование автоматического обновления может выполняться как через локальные настройки *ПК «ЗАСТАВА-Клиент»*, так и централизованно – через *ЗАСТАВА-Управление*, когда настройки указываются в ЛПБ *ПК «ЗАСТАВА-Клиент»*.

При включении режима автоматического обновления *ПК «ЗАСТАВА-Клиент»* будет периодически связываться с указанным сервером, содержащим обновления (данный сервер может располагаться в локальной сети или в сети Интернет). Если на сервере выложена новая версия *ПК «ЗАСТАВА-Клиент»*, то будет запущен процесс обновления (скачивание файла обновления, деинсталляция текущей версии и инсталляция новой, с сохранением всей информации о настройках).

В зависимости от настроек в ЛПБ *ПК «ЗАСТАВА-Клиент»* процессы скачивания и инсталляции обновлений могут выполняться либо полностью автоматически, либо по команде пользователя или сервера обновления. Кроме того, поддерживается инсталляция обновлений по расписанию.

Для успешного автоматического обновления *ПК «ЗАСТАВА-Клиент»* под управлением ОС Windows XP необходимо выбрать соответствующие параметры подписывания драйверов:

1) Открыть меню «Пуск», выбрать свойства папки «Мой компьютер».

2) Выбрать вкладку «Оборудование», в разделе «Драйверы» выбрать «Подписывание драйверов».

3) В окне «Подписывание драйверов» выбрать пункт «Пропускать – устанавливать программное обеспечение и не запрашивать утверждения» (см. Рисунок 8).

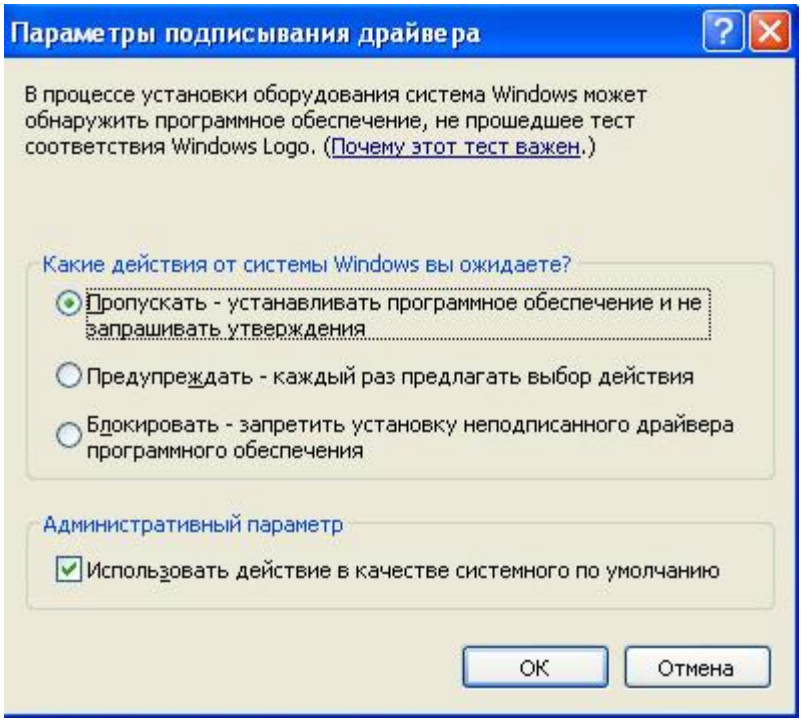

Рисунок 8 – Параметры подписывания драйверов

Обращение к серверу обновлений производится по открытому протоколу HTTP. При необходимости защиты данного соединения можно воспользоваться штатными средствами «ЗАСТАВА» (создать в Центре Управления политиками (ЦУП) *ЗАСТАВА-Управления* правило для защищенного соединения между данным *ПК «ЗАСТАВА-Клиент»* и сервером обновления).

2.1.3. Деинсталляция *ПК «ЗАСТАВА-Клиент»*

Для удаления *ПК «ЗАСТАВА-Клиент»* из ОС Windows надо закрыть все программные окна *ПК «ЗАСТАВА-Клиент»* и затем произвести деинсталляцию *ПК «ЗАСТАВА-Клиент»*, используя инструмент «Установка и удаление программ» в Панели управления. Все компоненты *ПК «ЗАСТАВА-Клиент»* будут полностью удалены, перезагрузить компьютер.

2.2. ОС семейства ALT Linux

Инсталляционные пакеты *ПК «ЗАСТАВА-Клиент»* для ОС ALT Linux 6 представляются в виде файлов с расширением .rpm: ZASTAVAclient-<version>-alt27.i386.rpm – 32-битная версия, ZASTAVAclient-<version>-alt31.x86_64.rpm – 64-битная версия. 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 от приведенных выше ядер, надо обратиться к п. 2.2.4.

2.2.1. Инсталляция ПК «ЗАСТАВА-Клиент»

Инсталляция *ПК «ЗАСТАВА-Клиент»* 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>
```

2.2.2. Обновление ПК «ЗАСТАВА-Клиент»

Обновление *ПК «ЗАСТАВА-Клиент»* запускается командой:

```
rpm –U <путь к инсталляционному пакету>
```

2.2.3. Деинсталляция *ПК «ЗАСТАВА-Клиент»*

Деинсталляция *ПК «ЗАСТАВА-Клиент»* запускается командой:

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

2.2.4. 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: ZASTAVAclient-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 провадера 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 “ ZASTAVAclient-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 провадера CryptoPro CSP (drvcsp.ko), например, /opt/cprocsp/src/drtcsp/Module.symvers.

kernel_release – указывает версию ядра ОС ALTLinux 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 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" ZASTAVA-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 ALTLinux 6 и CryptoPro CSP 3.6 R3.

Инсталляция собранного пакета запускается командой:

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

2.2.5. Интеграция *ПК «ЗАСТАВА-Клиент»* с системным SNMP-сервисом

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

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

В файл `snmpd.conf` добавить строку:

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

Дать команду `snmpd` для подгрузки модуля расширения:

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

2.3. Восстановление *ПК «ЗАСТАВА-Клиент»*

Проверка целостности программного обеспечения (ПО) компонента *ПК «ЗАСТАВА-Клиент»* осуществляется путем сравнения значения контрольной суммы, которое записано в файле filelist.hash, для данного файла, с текущим значением. При несовпадении значений выдается соответствующее предупреждение.

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 *ПК «ЗАСТАВА-Клиент»* не запустится, что свидетельствует о нарушении контрольных сумм программной части.

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

Для восстановления работоспособности *ПК «ЗАСТАВА-Клиент»* необходимо произвести деинсталляцию с последующей инсталляцией *ПК «ЗАСТАВА-Клиент»*.

2.4. Запуск графического интерфейса (GUI) *ПК «ЗАСТАВА-Клиент»*

Системные модули *ПК «ЗАСТАВА-Клиент»* запускаются автоматически при загрузке ОС и работают постоянно в фоновом режиме.

1) При необходимости, Вы можете открыть графический интерфейс *ПК «ЗАСТАВА-Клиент»* следующим образом:

– В ОС Windows выполнить команду через меню:

  – Пуск → Программы → ELVIS+ → ZASTAVA Client → VPN Agent, либо нажать дважды на иконке  в системном трее.

  – В ОС Linux выполнить команду `/opt/ZASTAVAclient/bin/vpnagent`

Для успешного отображения графического модуля компонента *ПК «ЗАСТАВА-Клиент»* в ОС Linux необходимо использовать ОС с установленным графическим окружением.

2) Появится *Панель инструментов*, с помощью которой Вы можете устанавливать параметры *ПК «ЗАСТАВА-Клиент»*.

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

2.5. Конфигурирование *ПК «ЗАСТАВА-Клиент»*

Возможности *ПК «ЗАСТАВА-Клиент»* при конфигурировании:

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

При сохранении настроек требуется ввести логин и пароль пользователя, входящего в группу администраторы.

В ОС Linux существуют ограничения на конфигурирование *ПК «ЗАСТАВА-Клиент»*: изменять настройки могут только пользователь root и пользователи, добавленные системными средствами в группу «admin». Остальным пользователям изменение настроек запрещено.

2.6. Быстрое включение *ПК «ЗАСТАВА-Клиент»* в работу с помощью графического интерфейса

Для быстрого запуска *ПК «ЗАСТАВА-Клиент»* в работу необходимо выполнить следующее:

— Получить и подключить носитель с персональным сертификатом к компьютеру с установленным компонентом *ПК «ЗАСТАВА-Клиент»*;

— Зарегистрировать сертификат Удостоверяющего центра (УЦ) – издатель персонального сертификата или всю трастовую цепочку сертификатов, если персональный сертификат издан Подчиненным УЦ;

— Создать и активировать конфигурацию для подключения к ЦУП.

К этому моменту *Агент* должен быть создан в ЦУП как Хост безопасности или пользователь с сертификатом, с оттранслированной и активированной ЛПБ. Администратором безопасности Вам должен быть выдан носитель с контейнером Вашего персонального сертификата, в котором должен быть инсталлирован Ваш открытый ключ и файлы сертификатов. СКЗИ, установленное на компьютере, должно обеспечивать поддержку носителя с персональным сертификатом.

Порядок быстрого включения в работу *ПК «ЗАСТАВА-Клиент»* следующий:

1) Подключить носитель с контейнером к компьютеру. Убедиться в том, что Ваш сертификат появился в *ПК «ЗАСТАВА-Клиент»*. Для этого необходимо открыть окно «Токены» и убедиться в том, что в дереве Builtin CryptoPro Module появился Ваш носитель (см. Рисунок 9).

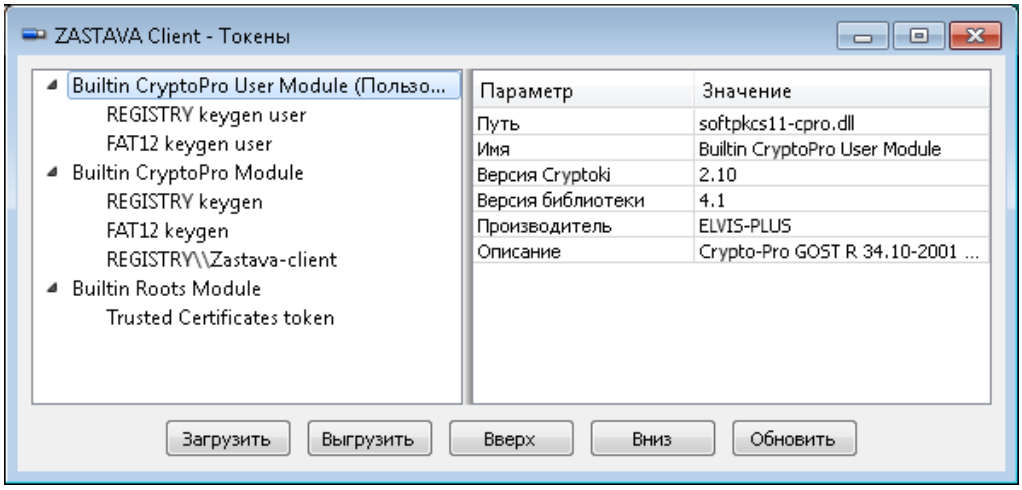

Рисунок 9 – Подключение носителя с сертификатом и ключами

Одновременно в окне «Сертификаты и ключи» появился Ваш персональный сертификат на вкладке «Персональные» (см. Рисунок 10).

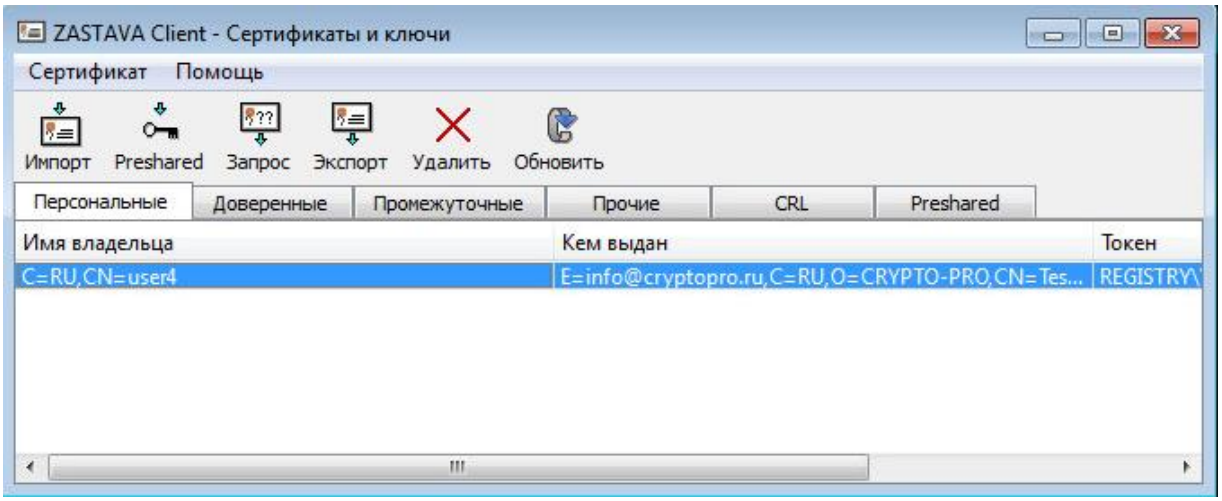

Рисунок 10 – Автоматическое добавление сертификата из носителя

2) Зарегистрировать сертификаты УЦ:

— Открыть окно «Сертификаты и ключи» и нажать кнопку «Импорт».

— 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 11).

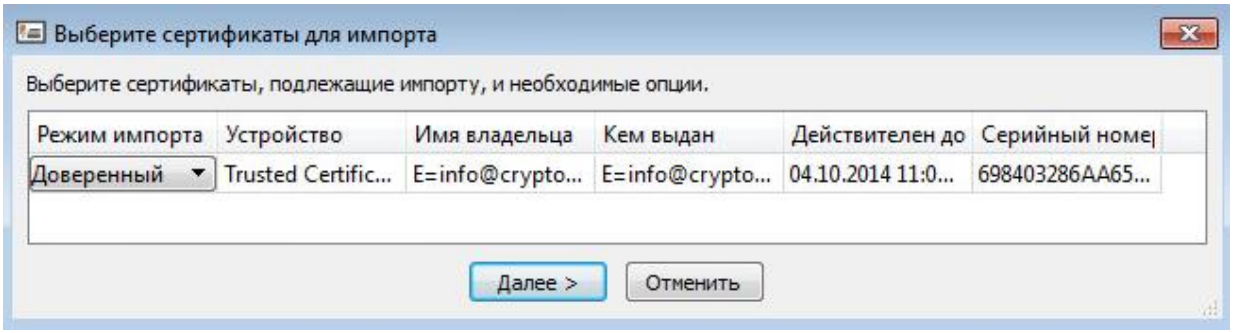

Рисунок 11 – Настройки в окне «Сертификат/Мастер ключей» при импорте сертификата УЦ

— В следующем окне диалога ввести PIN-код Trusted Certificate токена (см. Рисунок 12).

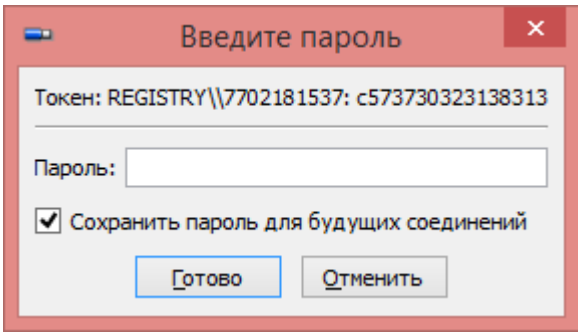

Рисунок 12 – Окно для ввода пароля токена

	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 *ПК «ЗАСТАВА-Клиент»* 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 инструментов* (см. Рисунок 37).

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 источник прогрузки политики – «Сервер+Сертификат».

– В поле «Сертификат» выбрать Ваш персональный сертификат (см. Рисунок 13).

– В поле «Сервер(ы) политик» ввести адрес сервера политики. Если не указать порт сервера, то берется значение по умолчанию (500).

Если серверов несколько, IP-адреса указываются через запятую. Номер порта указывается через двоеточие.

– Если персональный сертификат один, то можно в этом поле оставить значение «Любой персональный сертификат».
– Чтобы настроить получение ЛПБ с сервера политики необходимо ввести в поле «Сервер(ы) политик» IP-адрес(а) сервера, с которого будет получена политика.
– Для регистрации сообщений при передаче ЛПБ с сервера политики необходимо выбрать уровень регистрации событий в поле «Уровень лога», подробнее об уровне регистрации событий см. п. 3.8.1.1.

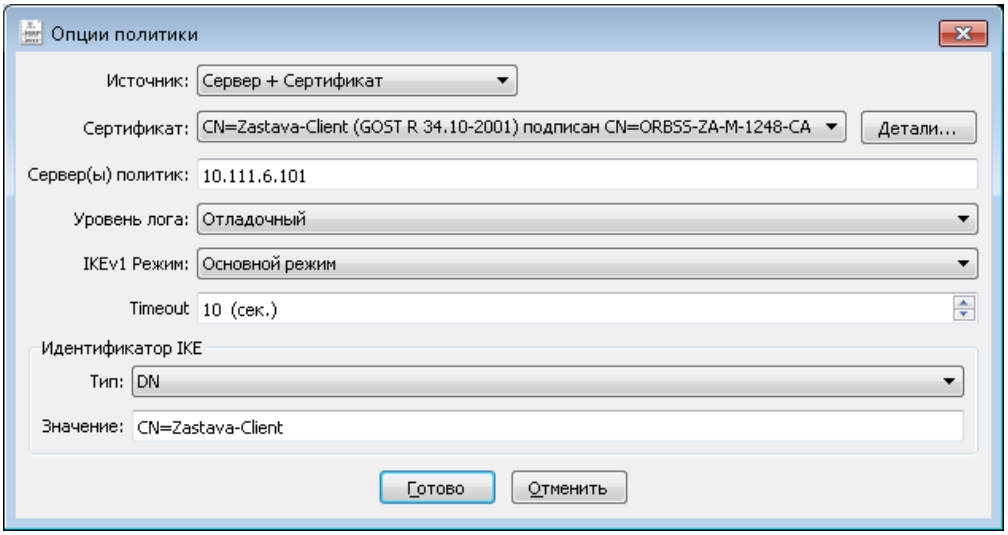

Рисунок 13 – Добавление параметров политики для прогрузки ЛПБ в окне «Опции политик»

— 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» на *Инструментальной панели*.

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 14).

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.

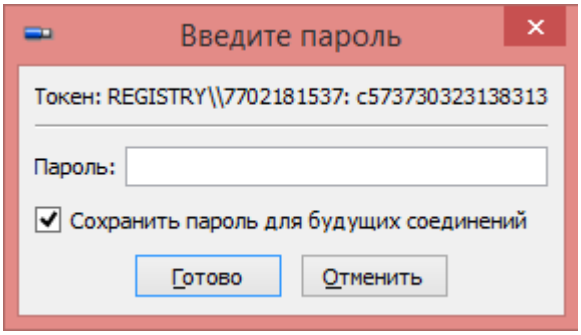

Рисунок 14 – Ввод пароля токена при создании защищенного соединения

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

ж) После установления соединения в информационной строке *Панели инструментов* появится информация о прогрузке политики из ЦУП (см. Рисунок 15).

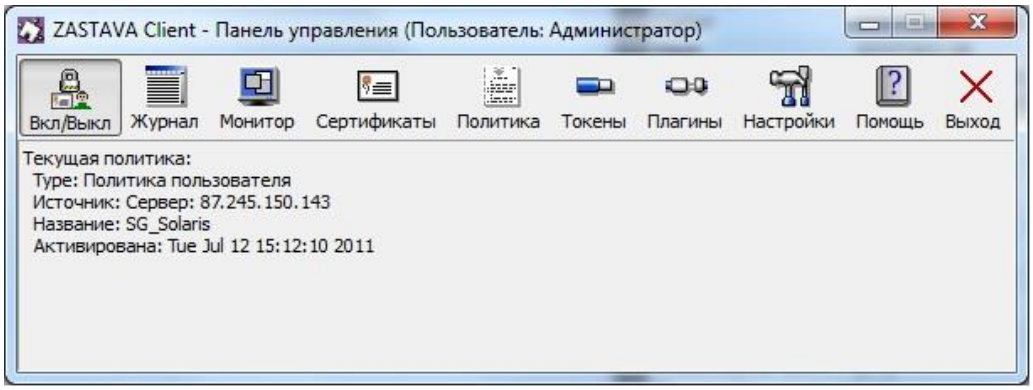

Рисунок 15 – Текущий статус ЛПБ *ПК «ЗАСТАВА-Клиент»* (источник ЛПБ и дата ее активации)

3. РАБОТА В ГРАФИЧЕСКОМ ИНТЕРФЕЙСЕ *ПК «ЗАСТАВА-КЛИЕНТ»*

3.1. Панель управления

Панель управления содержит кнопки, при помощи которых можно выполнить необходимую операцию или открыть дополнительное окно. После запуска *ПК «ЗАСТАВА-Клиент»*, на *Панели управления* отображаются кнопки: «Вкл/Выкл», «Журнал», «Монитор», «Сертификаты», «Политика», «Токены», «Плагины», «Настройки», «Помощь» и «Выход».

В нижней части *Панели управления* находится поле (см. Рисунок 16), отображающее текущую ЛПБ *ПК «ЗАСТАВА-Клиент»* (тип активированной ЛПБ, источник ЛПБ, дата и время ее активации).

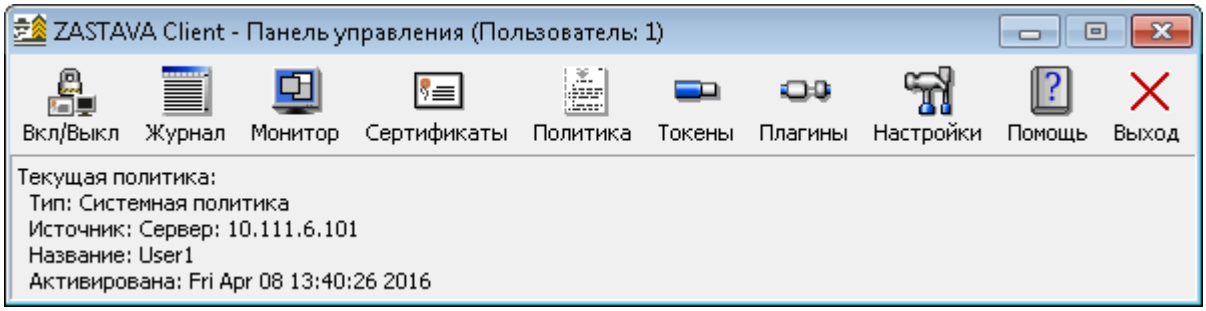

Рисунок 16 – *Панель управления* после входа в систему

3.1.1. Перезагрузка ЛПБ

При переходе в состояние «Выкл» удаляются все созданные *Агентом* защищенные соединения (SA) и прогружается системная политика либо DDP, настраиваемая в окне «Управление политиками» (см. подраздел 3.5) если отсутствует системная политика.

При переходе в состояние «Вкл» в *Агенте* прогружается пользовательская политика.

3.1.2. Просмотр событий

Вы можете просматривать файл регистрации событий *ПК «ЗАСТАВА-Клиент»* 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 и ключи

Сертификаты (включая сертификаты УЦ), предварительно распределенные ключи (pre-shared)[1]. СОС регистрируются в *ПК «ЗАСТАВА-Клиент»* через окно «Сертификаты и Ключи». Вызовите это окно, выбрав «Сертификаты» на *Панели управления*. Окно «Сертификаты и Ключи» показывает краткий обзор сертификатов.

3.1.5. Работа с политикой

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

3.1.6. Работа с токенами

ПК «ЗАСТАВА-Клиент» позволяет Вам 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 из командной строки, либо при помощи графического интерфейса окна «Плагины», для этого необходимо нажать кнопку «Плагины» на *Панели управления*, либо из командной строки - см. раздел 5.

3.1.8. Настройки ПК «ЗАСТАВА-Клиент»

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

В ОС Linux изменять настройки могут только пользователь root и пользователи, добавленные системными средствами в группу «admin». Остальным пользователям изменение настроек запрещено.

3.1.9. Помощь

Выбрать «Помощь», чтобы отобразилось меню, с помощью которого можно вызвать справочную систему *ПК «ЗАСТАВА-Клиент»*, 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 Client».

3.1.9.2. Справочная система ПК «ЗАСТАВА-Клиент»

Интерактивная справочная система может использоваться для получения ответов на вопросы по работе *ПК «ЗАСТАВА-Клиент»*. 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 *ПК «ЗАСТАВА-Клиент»*. При этом служба vpndmn и *ПК «ЗАСТАВА-Клиент»* 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 16), отображающая текущий статус ЛПБ *ПК «ЗАСТАВА-Клиент»* (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 17).

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

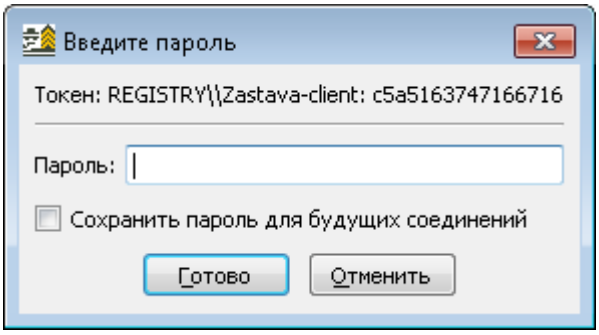

Рисунок 17 – Ввод пароля токена при создании защищенного соединения

Удостовериться в том, что у Вас запущен *Графический интерфейс ПК «ЗАСТАВА-Клиент»*, 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 18) открывается нажатием кнопки «Журнал» на Панели управления. В журнале отображается содержимое файла регистрации событий ЗАСТАВА-Управление.

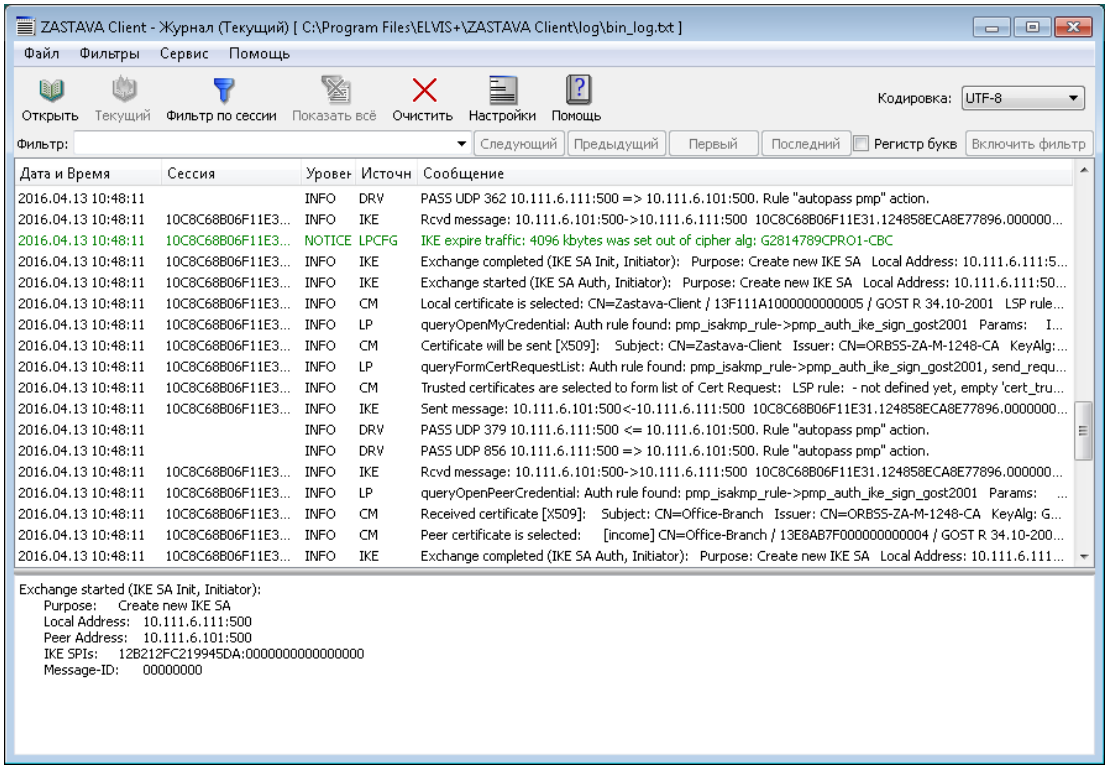

Рисунок 18 – Окно с зарегистрированными событиями

В верхней части окна расположена панель управления.

Основную часть окна занимает таблица с описанием системных событий. Уровень детализации настраивается пользователем (подробнее см. п. 3.2.3 на стр. 36).

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.

Текст из нижней части окна «Журнал» можно скопировать в буфер обмена (Clipboard), выделив его при помощи мыши и нажав клавиши <Ctrl+C>. При необходимости, можно послать эту информацию администратору безопасности для анализа возникших проблем с *ПК «ЗАСТАВА-Клиент»*.

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 журнал событий, выбранный пользователем.
Открыть текущий журнал	Открывает текущий журнал событий.
Открыть новый журнал	Открывает новое окно «Журнал».
Фильтры	
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.

Команда	Характеристика
Помощь	
Справка по журналу	Открывает раздел «Справки», поясняющий работу с журналом регистрации системных событий.
Помощь	Вызов общей Справочной системы *ПК «ЗАСТАВА-Клиент»*

3.2.1.2. Панель инструментов окна «Журнал»

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.

Кнопка	Описание
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 19) производится настройка параметров регистрации событий. Содержание вкладки полностью дублирует вкладку «Журнал» окна «Прочие настройки» и настраивается аналогичным образом (см. п. 3.8.1 на стр. 92).

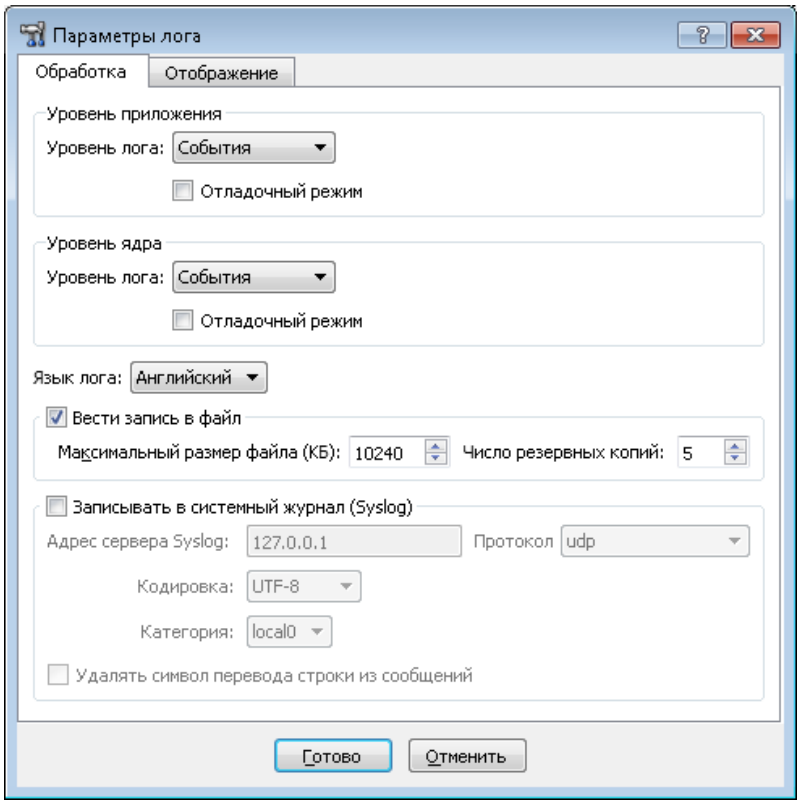

Рисунок 19 – Окно настройки параметров регистрации событий

Параметры представления журнала системных событий настраиваются на вкладке «Отображение» (см. Рисунок 20).

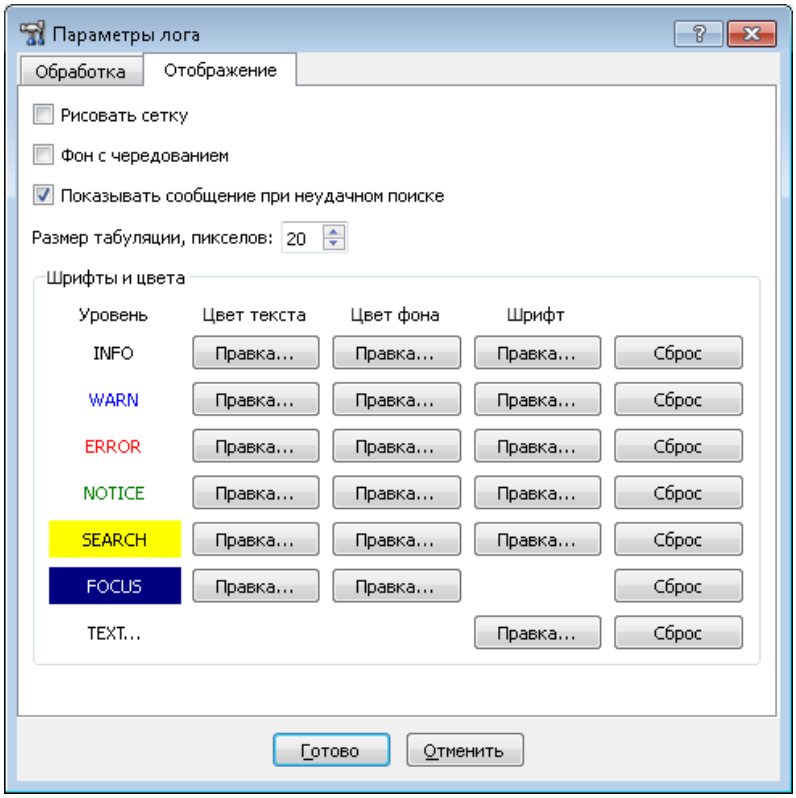

Рисунок 20 – Настройка параметров представления журнала системных событий

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 ПК «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 21).

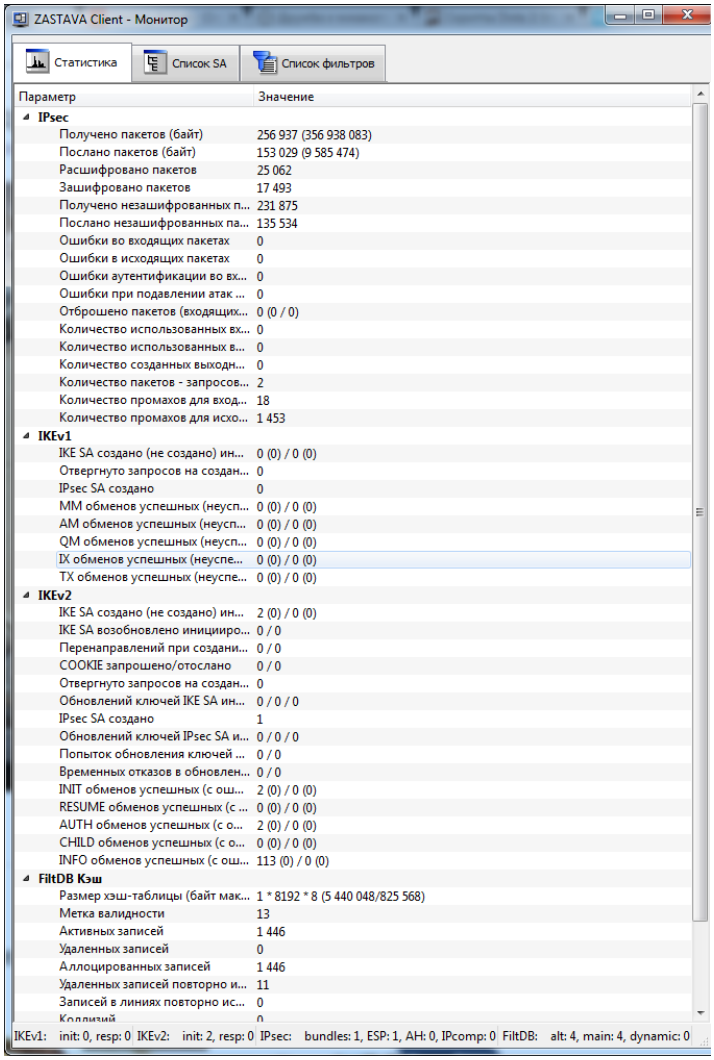

Рисунок 21 – Окно «Монитор», вкладка «Статистика»

3.3.1. Вкладка «Статистика»

На вкладке «Статистика» (см. Рисунок 21) 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	
Получено пакетов (байт)	Количество пакетов, полученных с момента запуска *Агента*
Послано пакетов (байт)	Количество пакетов, отправленных с момента запуска *Агента*

Параметр	Описание
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
IKEv1	
IKE SA создано (не создано) инициированных/отвеченных	Количество созданных (не созданных) инициированных/ отвеченных IKE SA в формате x(x)/x(x)

Параметр	Описание
Отвергнуто запросов на создание IKE SA	Количество отвергнутых запросов на создание IKE SA
IPsec SA создано	Количество созданных IPsec SA
MM обменов успешных (неуспешных) инициировано/отвечено	Количество успешных (неуспешных) обменов MainMode инициировано/отвечено в формате x(x)/x(x)
AM обменов успешных (неуспешных) инициировано/отвечено	Количество успешных (неуспешных) обменов Aggressive Mode инициировано/отвечено в формате x(x)/x(x)
QM обменов успешных (неуспешных) инициировано/отвечено	Количество успешных (неуспешных) обменов Quick Mode инициировано/отвечено в формате x(x)/x(x)
IX обменов успешных(неуспешных) инициировано/отвечено	Количество успешных (неуспешных) обменов Informational Exchange инициировано/отвечено в формате x(x)/x(x)
TX обменов успешных (неуспешных) инициировано/отвечено	Количество успешных (неуспешных) обменов Transaction Exchange инициировано/отвечено принятых запросов на создание IX в формате x(x)/x(x)
IKEv2	
IKE SA создано (не создано) инициированных/отвеченных	Количество созданных (не созданных) инициированных/ отвеченных IKE SA в формате x(x)/x(x)
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

Параметр	Описание
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/отвечено	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/отвечено	Количество успешных (с ошибками или неуспешных) обменов CREATE_CHILD_SA обменов инициировано/отправлено в формате x(x)/x(x)
INFO обменов успешных(с ошибками или неуспешных) инициировано/отвечено	Количество успешных (с ошибками или неуспешных) обменов INFORMATIONAL инициировано/отправлено в формате x(x)/x(x)
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

Параметр	Описание
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 22) 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.

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)
Метод аутентификации	Используемый в защищенном соединении метод аутентификации для IKE SA и имя правила в LSP для IPsec SA
Время создания	Время создания соединения

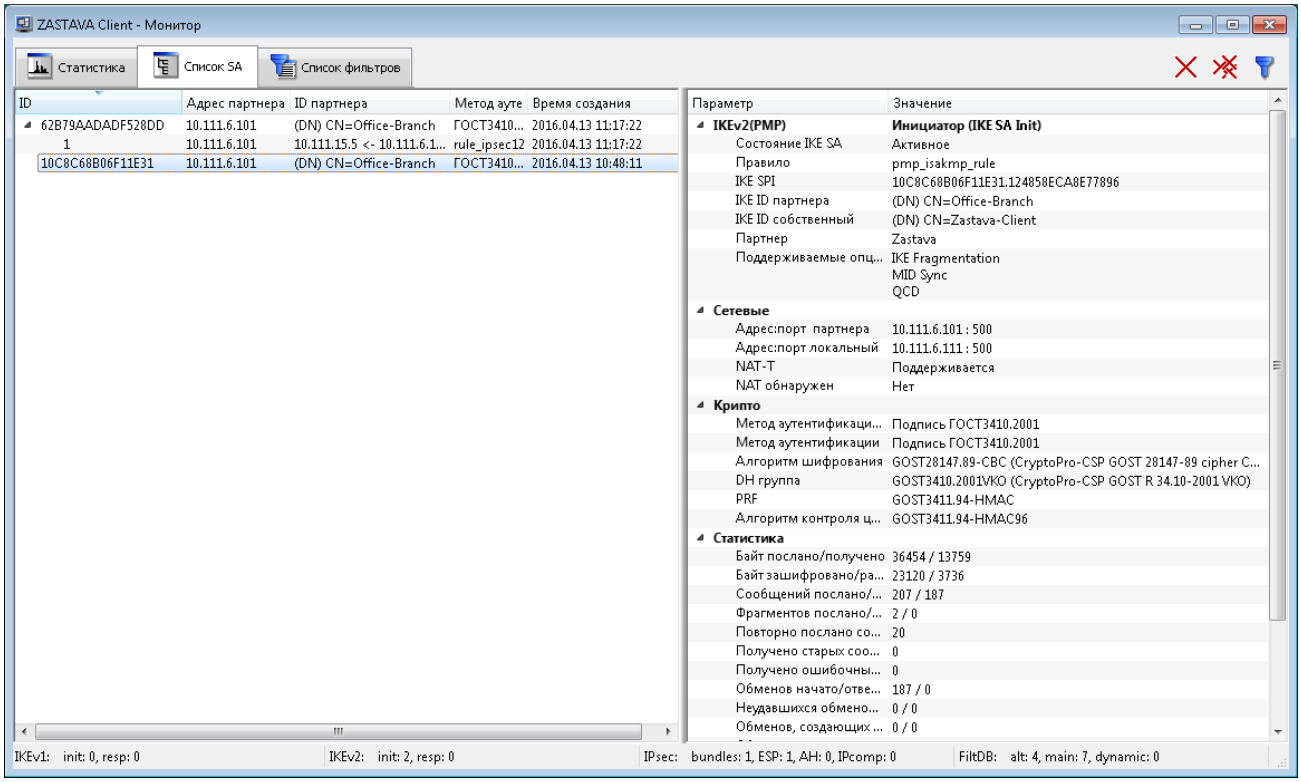

Рисунок 22 – Окно «Монитор», вкладка «Список SA»

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 23).

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

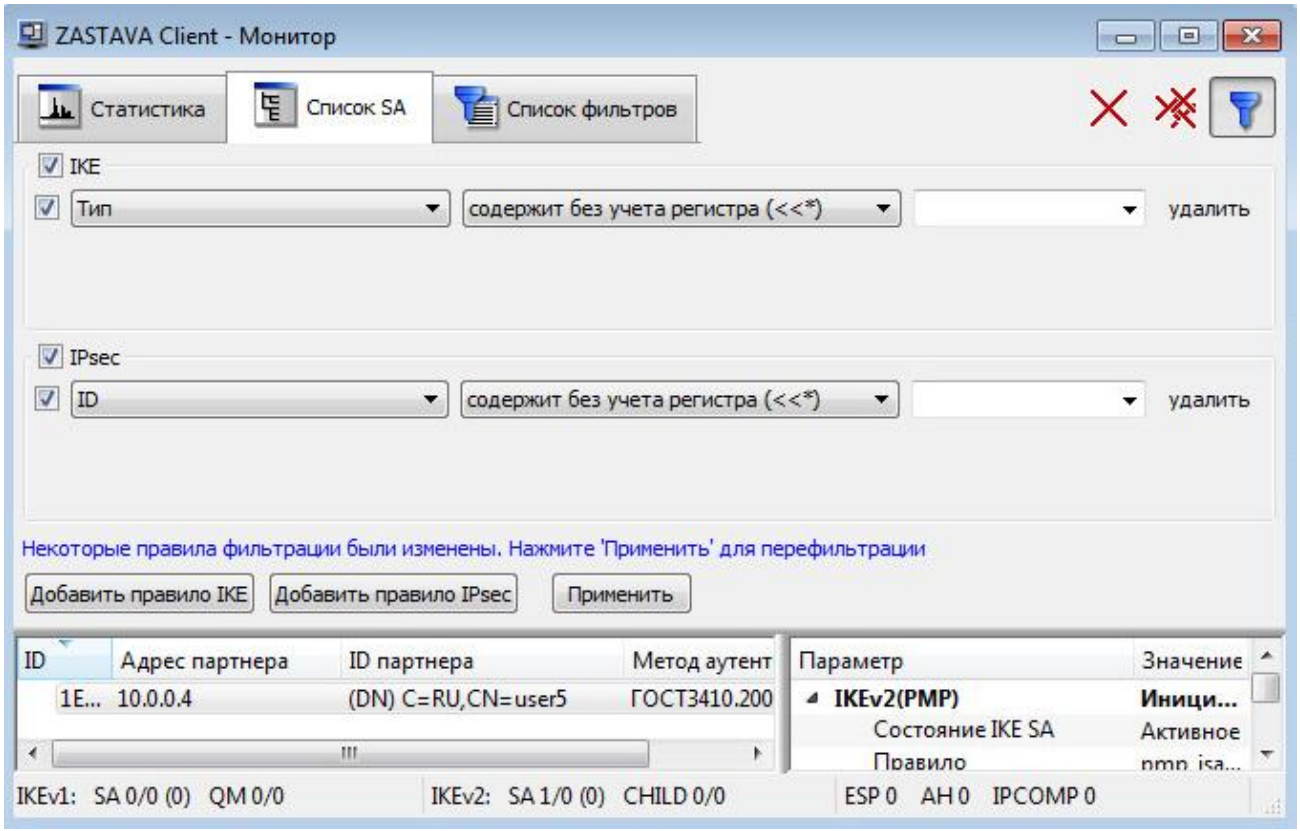

Рисунок 23 - Окно «Монитор», активный «Фильтр»

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

Таблица 6 – Параметры фильтрации протокола IKE

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
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

Параметр	Характеристика
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 партнера	Метод аутентификации партнера
Метод аутентификации	Метод идентификации данного компьютера
IKE SA cookie	IKEv1 SA cookie
IKE SPI	IKEv2 SPI
Уровень лога	Уровень подробности регистрации событий
Поддерживаемые опции	Список поддерживаемых опций

Параметры фильтрации протокола IPsec 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
Режим	Режим создания SA
Роль	Роль при создании SA
Id партнера	ID компьютера партнёра
Id локальный	ID данного компьютера

Тип	Характеристика
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	IKE-CFG адрес, выданный клиенту
DH группа	DH группа
Фильтр	Фильтр
Правило	Название применяемого правила
(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
(ESP) Декапсулировано	(ESP) Декапсулировано пакетов

Тип	Характеристика
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 среди 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, операции специфичны для каждого из параметров (см. Таблица 8).

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, create child SA, 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

Команда	Характеристика
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 (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) равно эталону (IP-адрес)
не равен	значение поля (IP-адрес) не равно 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

Команда	Характеристика
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
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 указать значение, по которому будет производиться сравнение, в крайнем правом поле строки фильтрации, и нажать кнопку «Применить». В нижней 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	Показывает все SA-соединения

Команда	Характеристика
Показывать только IKE SA	Показывает только IKE SA
Показывать только IPsec SA	Показывает только IPsec SA
Показывать удаленные SA	Показывает удаленные SA
Искать только в дереве SA	Поиск 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 24).

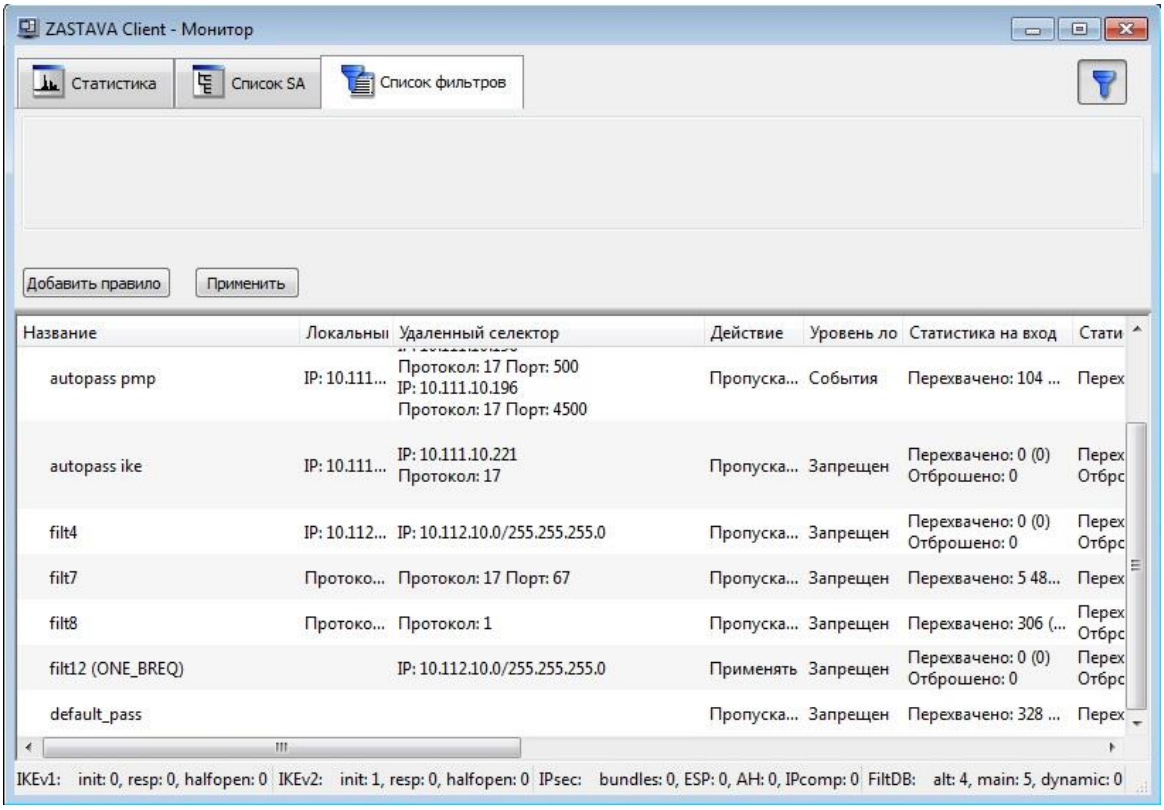

Рисунок 24 - Окно «Монитор», вкладка «Список фильтров»

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
Действие	Действие для фильтрации
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

Параметр	Характеристика
Входящих промахов в кэше в секунду	Статистика промахов после проверки входящих пакетов в секунду на соответствие с фильтрами в кэше
Исходящих промахов в кэше в секунду	Статистика промахов после проверки исходящих пакетов в секунду на соответствие с фильтрами в кэше
Записей в кэше	Статистика промахов после проверки исходящих пакетов на соответствие с фильтрами в кэше
Фаервольные процедуры	Параметр фильтрации по полю «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

3.3.3.2. Фильтрация

Для задания правил фильтрации следует:

1) Открыть панель фильтров кнопкой  .
2) Нажать кнопку «Добавить правило», появится строка задания правила фильтрации (см. Рисунок 25).
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.

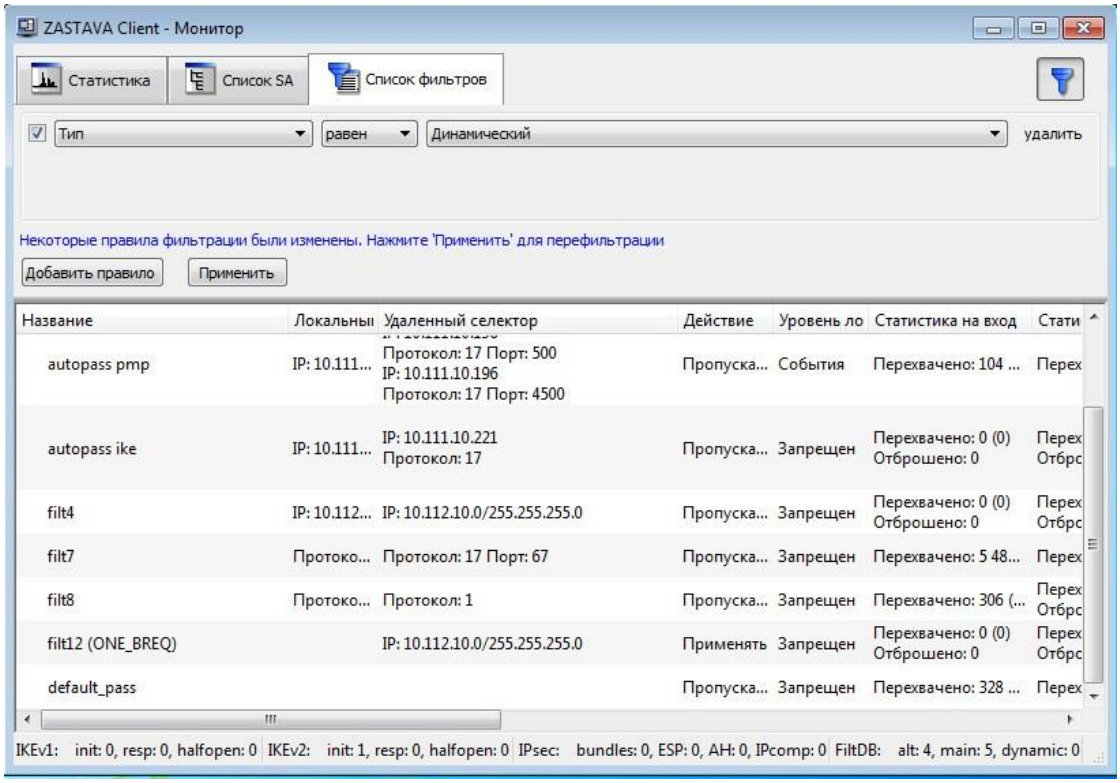

Рисунок 25 – Окно «Монитор», вкладка «Список фильтров». Открыта панель фильтрации

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»
Флаги	Параметр фильтрации по полю «Название»
Комментарий	Параметр фильтрации по полю «Комментарий»
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
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»

Параметр	Характеристика
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»

3.4. Окно «Сертификаты и ключи»

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

ПК «ЗАСТАВА-Клиент» 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:

- **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 *ПК «ЗАСТАВА-Клиент»* с целью проверки подлинности всех сертификатов, присылаемых партнерами по связи в процессе установления защищенных соединений (см. «сертификаты партнёров»).
- **Персональный сертификат** – это сертификат, используемый данным пользователем *ПК «ЗАСТАВА-Клиент»*. Отличительной особенностью является то, что локальный сертификат хранится на токене вместе с соответствующим закрытым ключом. Наличие закрытого ключа позволяет *ЗАСТАВА-Офис* осуществлять двустороннюю криптографическую аутентификацию при установлении соединений с другими хостами защищенной корпоративной сети на базе протоколов IKEv1 и IKEv2.

— **Прочие сертификаты** – это сертификаты, используемые данным *ПК «ЗАСТАВА-Клиент»*. Отличительной особенностью является то, что данные сертификаты выкладывается без соответствующего закрытого ключа и их нельзя отнести к обозначенным типам сертификатов.

— **Промежуточные сертификаты –** это сертификаты, используемые данным *ПК «ЗАСТАВА-Клиент»*. Отличительной особенностью является то, что это CA-сертификаты промежуточных УЦ, выданные промежуточным сертифицирующим органом (CA – certification authority).

Предварительно распределенные ключи могут использоваться в *ПК «ЗАСТАВА-Клиент»* в качестве альтернативы использования сертификатов. Для получения более полной информации надо обратиться к 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. *ПК «ЗАСТАВА-Клиент»* поддерживает СОС. Для получения более полной информации надо обратиться к п. 3.4.8.

3.4.1. Структура окна «Сертификаты и Ключи»

Чтобы открыть окно «Сертификаты и Ключи» необходимо на *Панели управления* нажать кнопку «Сертификаты». Окно «Сертификаты и Ключи» показывает краткий обзор сертификатов. Окно содержит меню, инструментальную панель и вкладки, разделенные по типам сертификатов (см. Рисунок 26).

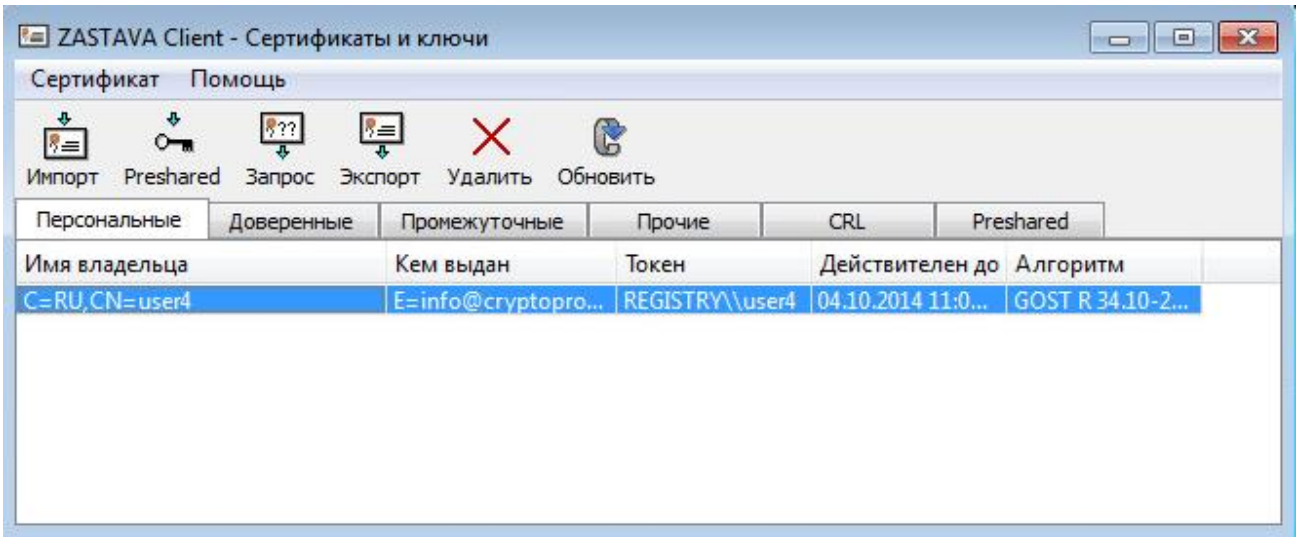

Рисунок 26 – Окно «Сертификаты и Ключи»

3.4.1.1. Вкладки окна «Сертификаты и ключи»

Окно «Сертификаты и ключи» содержит вкладки с зарегистрированными сертификатами разделенных 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 13).

Таблица 13 – 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	СОС
Preshared	Предварительно распределенные ключи

3.4.1.2. Строка меню

Строка меню содержит следующие меню: «Сертификаты», «Помощь». Команды меню представлены в таблице (см. Таблица 14).

Таблица 14 – Команды меню

Команда	Действие
Сертификаты	
Импорт сертификата	Запускает мастер Импорта сертификатов, который помогает Вам импортировать сертификат, СОС из файловой системы или из токена
Импорт предопределенного ключа	Запускает мастер Импорта предварительно распределенных ключей, который помогает импортировать предварительно распределенный ключ (также параметры предварительно распределенного ключа могут быть введены вручную)
Генерация запроса сертификата	Запускает мастер Генерации запроса сертификата, который помогает создавать ЗРС
Экспорт сертификата	Запускает мастер Экспорта сертификатов, который помогает экспортировать любой сертификат.
Обновить	Обновляет список сертификатов, зарегистрированных в базе данных (БД). Если окно «Сертификаты и ключи» открыто, когда активизирована ЛПБ, то сертификаты, полученные в течение IKE-обмена, не обновляются автоматически. СОС, полученные автоматически от сервера LDAP, также не показываются. Нажатие

Команда	Действие
	кнопки «Обновить» гарантирует то, что Вы видите наиболее свежую информацию о БД
Помощь	
Работа с сертификатами и ключами	Открывает раздел «Работа с сертификатами и ключами», поясняющий работу с сертификатами и ключами
Помощь	Вызов общей Справочной системы *ПК «ЗАСТАВА-Клиент»*

3.4.1.3. Инструментальная панель окна «Сертификаты и ключи»

Описание кнопок панели инструментов приведено в таблице (см. Таблица 15). Функции этих кнопок соответствуют функциям пунктов меню (см. п. 3.4.1.2).

Таблица 15 – 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.

Работа в окне «Сертификаты» подробнее описана в разделе 4.

3.4.2. Характеристики сертификатов

3.4.2.1. Свойства сертификата

Для просмотра свойств сертификата нужно выбрать его в соответствующей вкладке (Персональные, Доверенные и т. д.) и дважды нажать на него правой кнопкой мыши или воспользоваться клавишей <Enter>.

Характеристики сертификата приведены в таблице (см. Таблица 16).

Таблица 16 – Характеристики сертификата

Параметр	Характеристика
Version	Версия 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 Удостоверяющий Центр (УЦ), Регистрационный Центр (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)	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 17).

Таблица 17 – Характеристики ЗРС

Параметр	Характеристика
Устройство	Устройство, на котором будет сохранены сертификат и ключи
Алгоритм	Тип открытого ключа (алгоритм цифровой подписи)
Длина ключа	Длина открытого ключа
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
DNS	DNS
E-mail	E-mail
Флаг «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 18).

Таблица 18 – Состав предварительно распределенных ключей

Параметр	Характеристика
Устройство	Устройство, на котором будет сохранены ключи.

Параметр	**Характеристика**
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 (Списка Отозванных Сертификатов)

Отображается следующая информация о СОС в окне «Сертификаты и ключи» (см. Таблица 19).

Таблица 19 – Информация о СОС

Параметр	**Характеристика**
Кем выдан	Имя УЦ, который издал данный сертификат
Токен	Устройство, на котором будет сохранен СОС
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 *ПК «ЗАСТАВА-Клиент»*

Для генерирования сертификатов могут применяться различные PKI-продукты третьих производителей. ЛПБ для *ПК «ЗАСТАВА-Клиент»* 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 *ПК «ЗАСТАВА-Клиент»*, как описано в п. 3.4.6.1. ЗРС будет создан и сохранен в *ПК «ЗАСТАВА-Клиент»* 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 *ПК «ЗАСТАВА-Клиент»*, как описано в п. 3.4.4.1. После того, как сертификат будет импортирован, он заменит собой соответствующий ЗРС в окне

«Сертификаты и ключи» *ПК «ЗАСТАВА-Клиент»* 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 *ПК «ЗАСТАВА-Клиент»:* Доверенные и Персональные (для получения информации о типах сертификатов см. п. 3.4.1.1).

Чтобы зарегистрировать новый сертификат (Доверенные и Персональные) в *ПК «ЗАСТАВА-Клиент»* 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 27).

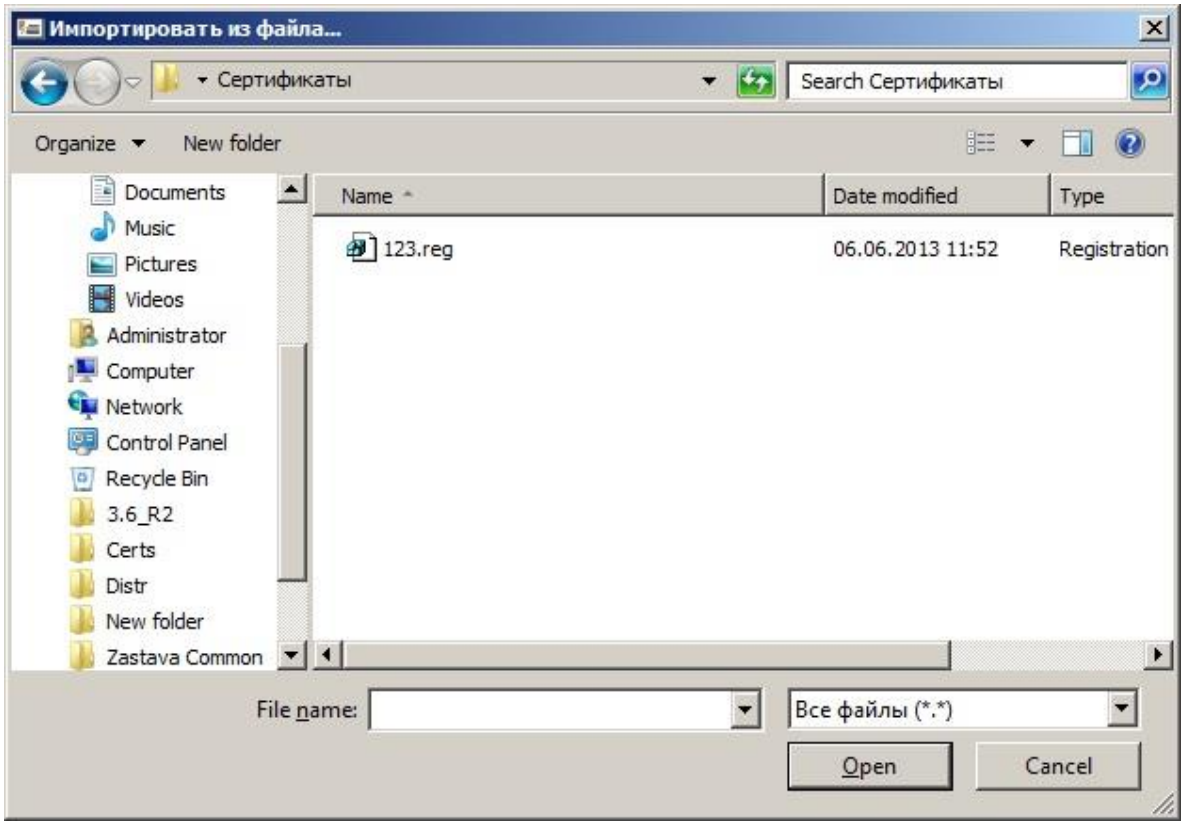

Рисунок 27 – Выбор импортированного объекта

3) Выбрать необходимый «Режим импорта» сертификата, например: «Импортировать», либо оставить режим по умолчанию (см. Рисунок 28) и нажать кнопку «Далее».

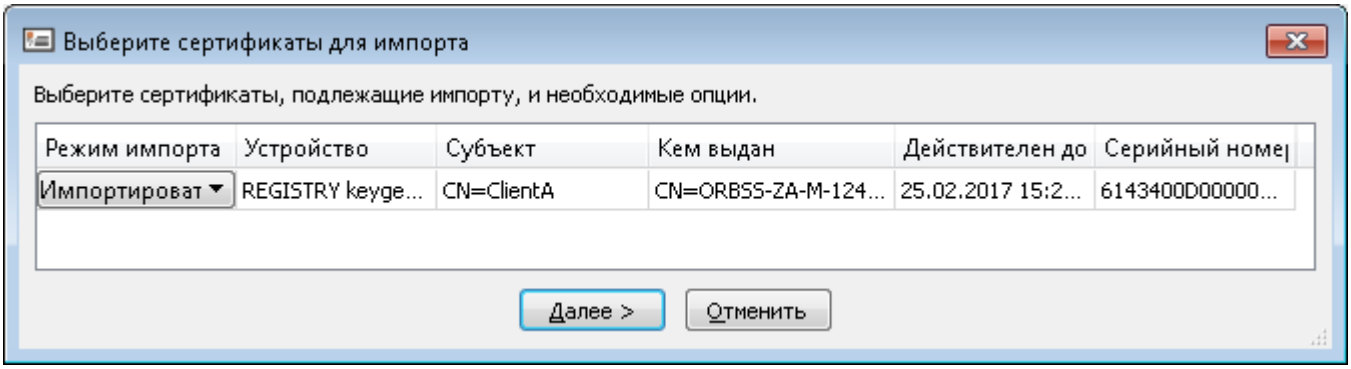

Рисунок 28 – Выбор режима импорта сертификата

4) При успешном импортировании появится индикатор (см. Рисунок 29). Теперь Мастер сертификатов показывает импортированный сертификат, нажать кнопку «Готово».

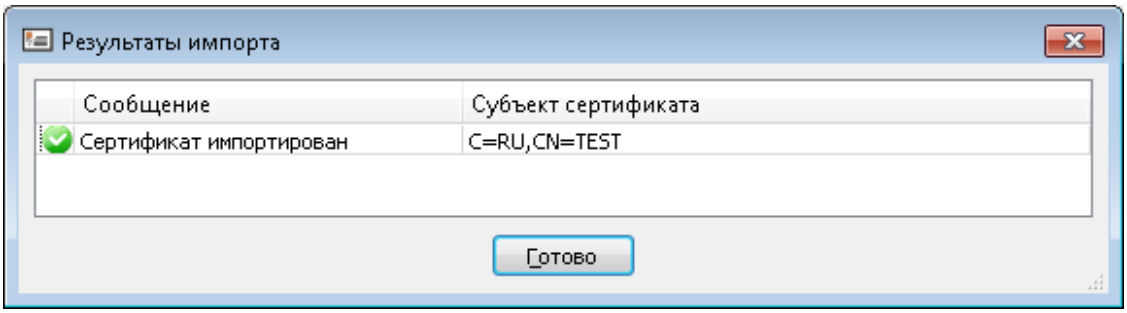

Рисунок 29 – Окно результата импортирования сертификата

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

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

6) Если Вы импортируете один 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 30) назначить этому сертификату соответствующий статус - «Доверенный». После чего нажать кнопку «Далее».

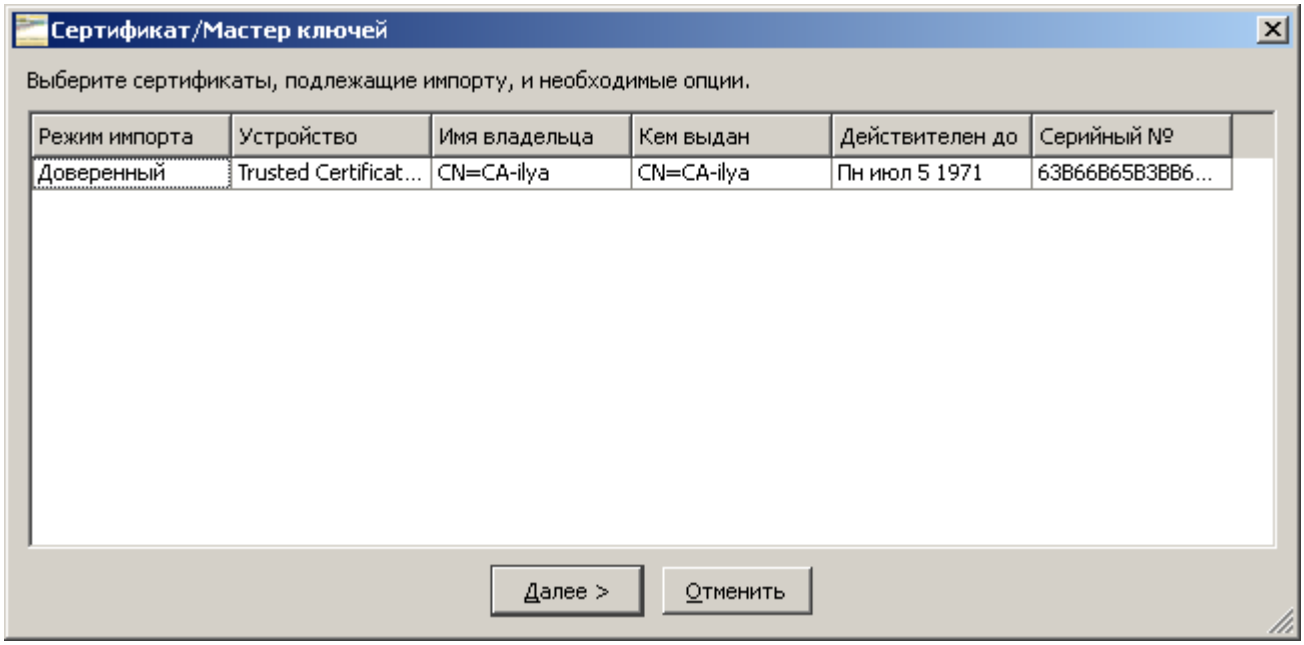

Рисунок 30 – Выбор режима импорта сертификата для регистрации Доверенного сертификата

- Необходимо ввести PIN-код токена (см. Рисунок 31), в котором будет содержаться сертификат. После ввода PIN-кода нужно нажать кнопку «Готово».

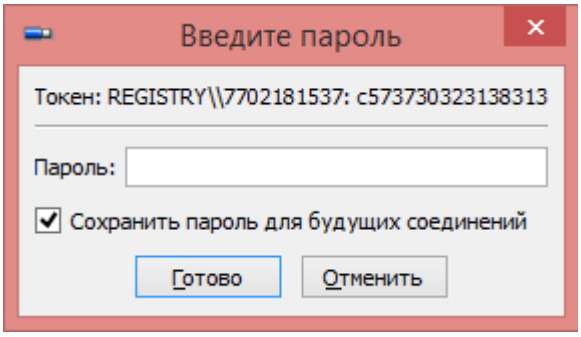

Рисунок 31 – Ввод пароля токена

	Если сертификат УЦ был послан Вам через незащищённый канал (например, по электронной почте) и Вы хотите сохранить его, как «Доверенный», Вы должны проверить подлинность этого сертификата вручную.
	Непосредственно после регистрации его в *ПК «ЗАСТАВА-Клиент»* свяжитесь с администратором УЦ, чтобы сравнить сигнатуру (fingerprint) оригинального сертификата УЦ с сигнатурой полученного сертификата, которая отображается в полях «Fingerprint» в таблице сертификатов *ПК «ЗАСТАВА-Клиент»*. Если сигнатуры не совпадают, немедленно удалите сертификат из *ПК «ЗАСТАВА-Клиент»*.
	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 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 *ПК «ЗАСТАВА-Клиент»* 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 *ПК «ЗАСТАВА-Клиент»*, этот сертификат заменит соответствующий ЗРС и будет автоматически связан с личным ключом.

3.4.4.2. Удаление сертификата

Для удаления сертификата из *ПК «ЗАСТАВА-Клиент»* 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 *ПК «ЗАСТАВА-Клиент»*.

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:

1) Выбрать требуемый сертификат в окне «Сертификаты и ключи».
2) Нажать кнопку  «Экспорт» или «Экспорт сертификата» из меню «Сертификат». Запустится программный Мастер.
3) В появившемся окне выбрать формат экспортируемого сертификата (см. Рисунок 32). 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».

4) В появившемся окне выбрать необходимый для сохранения сертификата путь и нажать кнопку «Сохранить». Появится информационное окно с сообщением о результатах экспорта.

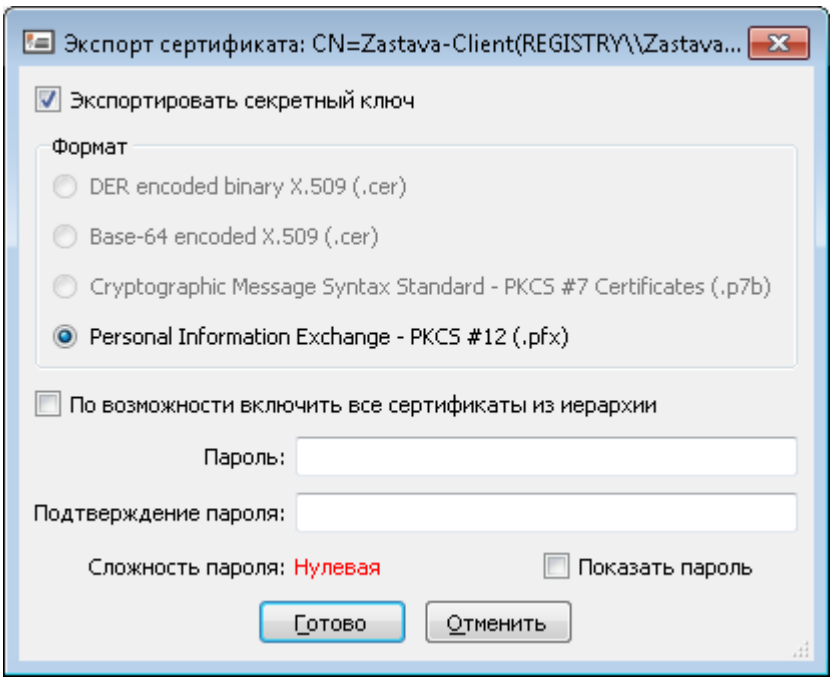

Рисунок 32 – Параметры экспорта сертификата

3.4.6. Запросы на Регистрацию Сертификата

Существует несколько способов получить локальный сертификат для *ПК «ЗАСТАВА-Клиент»*. 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».

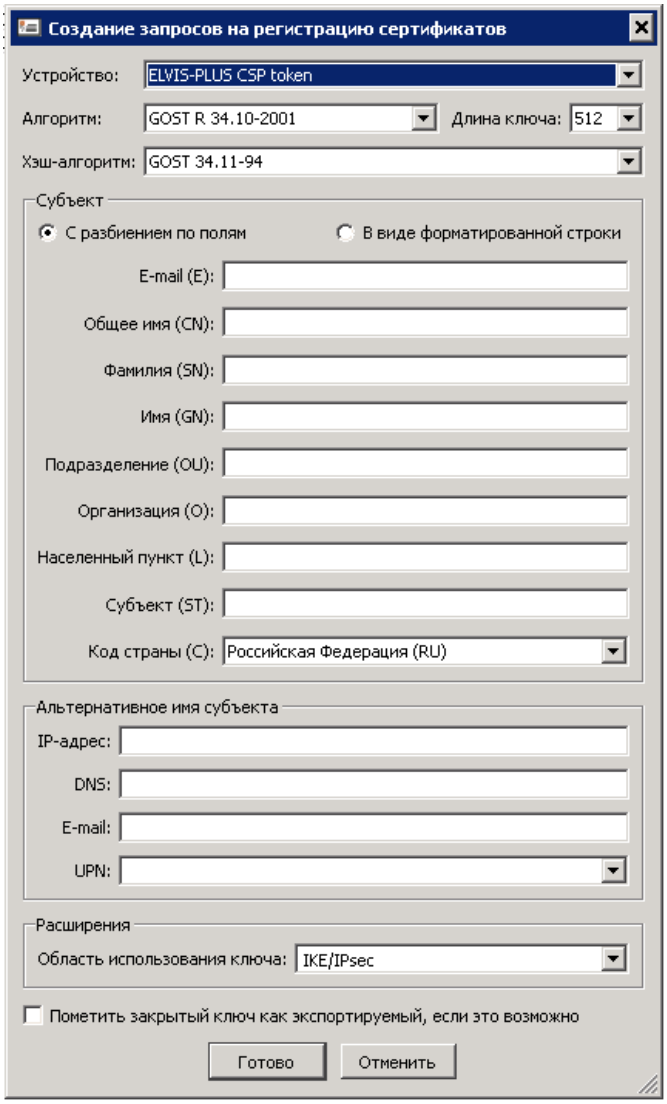

Рисунок 33 – Ввод информации для создания ЗРС

2) В появившемся окне «Создание Запроса на Регистрацию Сертификатов» заполнить необходимые поля (см. Рисунок 33):

   – 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. 70). 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 (см. Рисунок 34). ЗРС и соответствующий ему закрытый ключ будут сохранены в *ЗАСТАВА-Офис* – в таблице появится соответствующая строка с именем субъекта «Key Pair without Certificate».

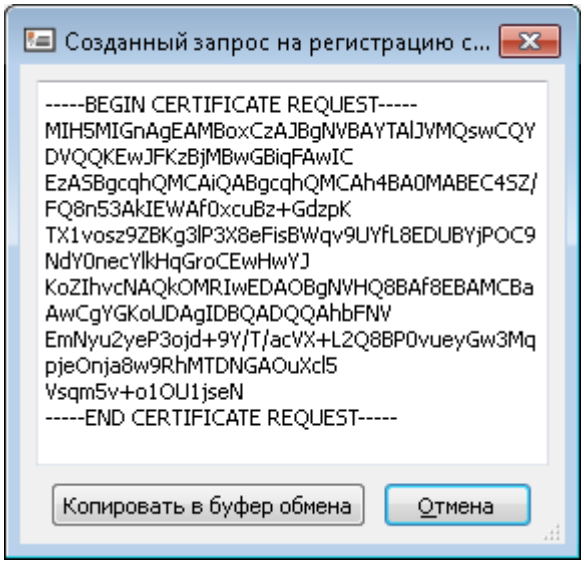

Рисунок 34 – Копирование ЗРС в буфер обмена

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» *ПК «ЗАСТАВА-Клиент»* 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 20).

Таблица 20 – 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. После получения сертификата от УЦ убедитесь в том, что *ПК «ЗАСТАВА-Клиент»* способен корректно взаимодействовать со всеми видами *Агентов*, необходимыми для работы.

В компонентах ПК «VPN/FW «ЗАСТАВА» версии 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 *ПК «ЗАСТАВА-Клиент»* надо выделить ЗРС, который Вы хотите удалить в окне «Сертификаты и ключи», нажать на *Инструментальной панели* окна «Сертификаты и ключи» кнопку «Удалить». Запрос будет удален из *ПК «ЗАСТАВА-Клиент»*.

3.4.7. 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 партнером заранее). Если Ваши 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.

Когда используются предварительно распределенные ключи, Вы должны зарегистрировать, по крайней мере, сертификаты, используемые для проверки целостности ЛПБ.

3.4.7.1. Регистрация предварительно распределенного ключа

Чтобы зарегистрировать предварительно распределенный ключ в *ПК «ЗАСТАВА-Клиент»* необходимо сделать следующее:

1) Нажать кнопку  «Preshared» из меню «Сертификат». Запустится программный Мастер.

2) В появившемся окне «Preshared Key» заполнить необходимые поля (см. Рисунок 35).

3) 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 (“_”).

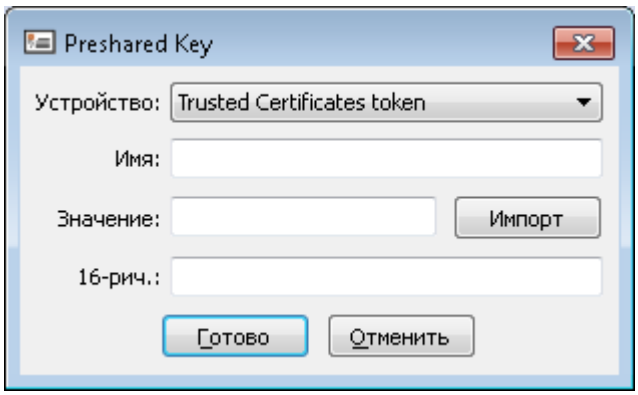

Рисунок 35 – Ввод параметров предварительно распределенного ключа

4) Ввести значение ключа в поле «Значение» или «16-рич.» или нажать кнопку «Импортировать значение ключа» и указать файл со значением предварительно распределенного ключа.

5) 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 *ПК «ЗАСТАВА-Клиент»* надо выделить ключ, который Вы хотите удалить, в таблице вкладки «Preshared Key» окна «Сертификаты и Ключи», нажать на *Инструментальной панели* окна «Сертификаты и ключи» кнопку «Удалить». Запрос будет удален из таблицы и из *ПК «ЗАСТАВА-Клиент»*.

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 *ПК «ЗАСТАВА-Клиент»* автоматически или вручную.

Проверка сертификатов управляется локальными настройками *ПК «ЗАСТАВА-Клиент»*. Доступны три варианта:

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

3.4.8.1. Обработка COC

При проверке сертификата *ПК «ЗАСТАВА-Клиент»* путем просмотра COC удостоверяется в том, что сертификат не отозван.

Если в локальных настройках *ПК «ЗАСТАВА-Клиент»* 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 COC не найден. Установление соединения с использованием такого сертификата возможно.

Для поиска COC используется следующий алгоритм:

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

3.4.9. Проверка сертификата

Вы можете проверить сертификат, зарегистрированный в *ПК «ЗАСТАВА-Клиент»*, 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.*

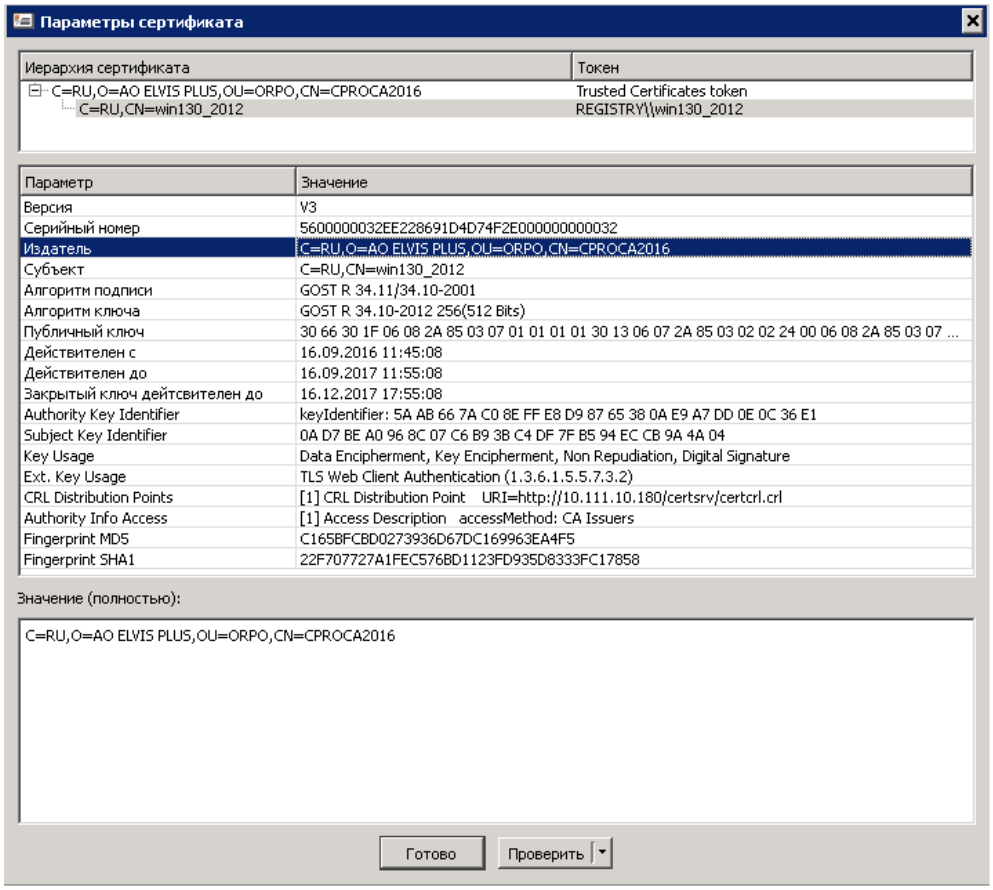

Рисунок 36 – Окно «Параметры сертификата»

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 дата, время и настройки часового пояса правильно установлены на Вашем компьютере. 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 37). Для получения информации об ЛПБ см. п. 3.5.3. Для получения информации об особенностях создания ЛПБ см. п. 3.5.5.

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

ЛПБ может быть установлена, активирована и просмотрена.

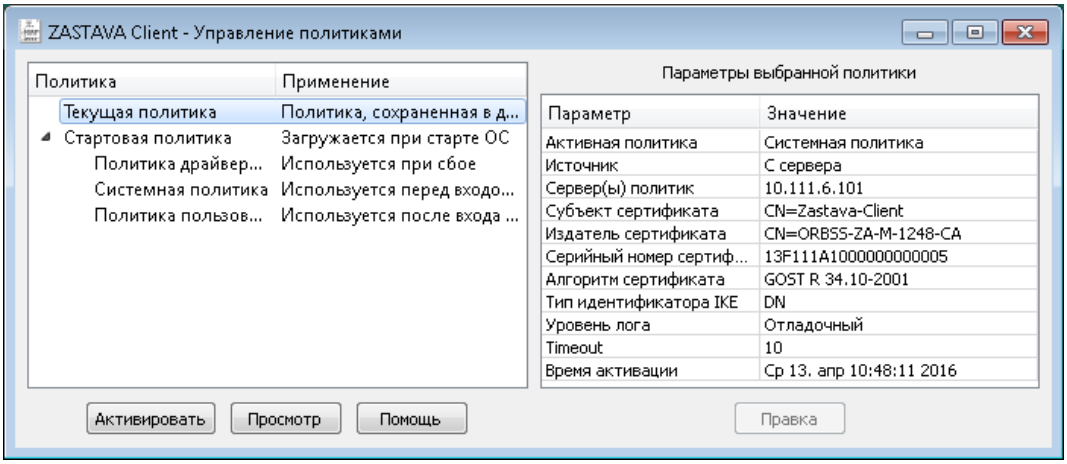

Рисунок 37 – Окно «Управление политиками»

3.5.1. Структура окна «Управление политиками»

Окно «Управление политиками» состоит двух разделов:

– Раздел с деревом политик;
– Раздел с параметрами 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».

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;
  – Политика пользователя – политика, используемая после входа пользователя в ОС.

3.5.3. Параметры политик *ПК «ЗАСТАВА-Клиент»*

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 политик» (см. Рисунок 38).

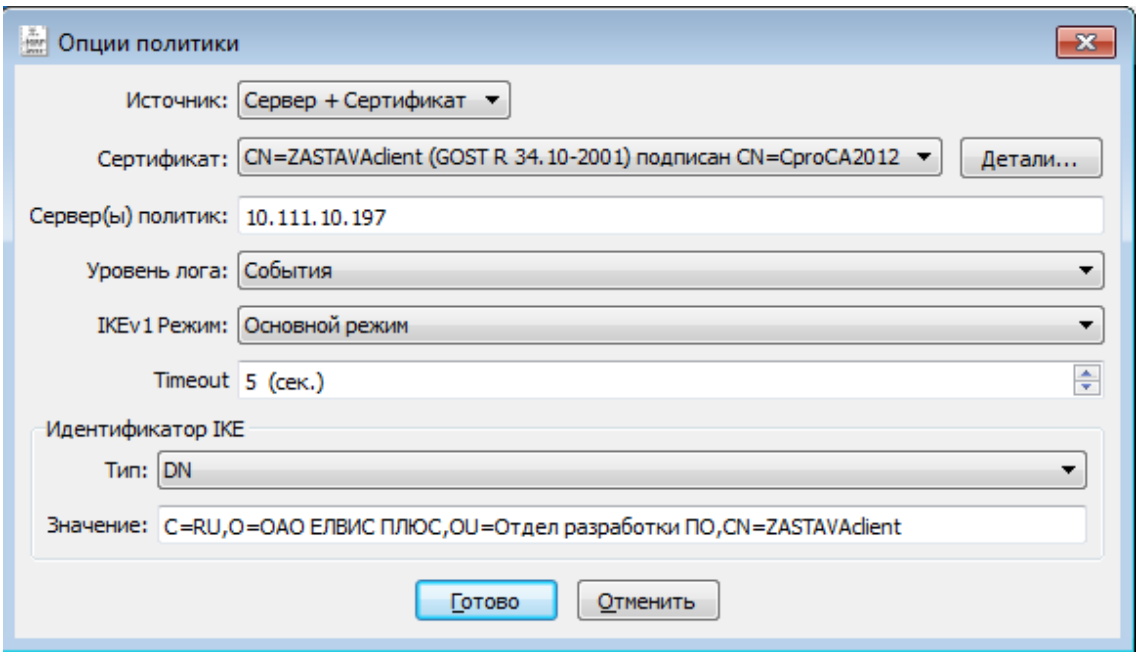

Рисунок 38 – Настройка параметров системной политики

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.

С помощью кнопки «Детали» при выборе метода активации с сервера можно просмотреть параметры выбранного сертификата в окне «Параметры сертификата».

б) Чтобы настроить получение ЛПБ с сервера политики необходимо ввести в поле «Сервер(ы) политик» IP-адрес(а) 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. п. 3.8.1.1.

г) Выбрать режим установления соединения IKEv1: основной или агрессивный в поле «IKEv1 Режим».

д) Отметить время, через которое необходимо обращаться к серверу за ЛПБ, в поле «Timeout».

е) В секции «Идентификатор IKE» выбрать тип IKE идентификатора для прогрузки политики, согласованного с ЦУП.

2) Нажать кнопку «Готово». Сохранение опций политики требует введения логина и пароля пользователя, который входит в группу администраторы.

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.

3.5.3.2. Политика пользователя

Политика, используемая после входа пользователя в ОС. Политика пользователя может быть получена из файла или с сервера политик.

Для изменения параметров пользовательской политики необходимо на политике пользователя в поле «Политика» нажать дважды левой кнопкой мыши и выбрать необходимые параметры в окне «Опции политик» (см. Рисунок 39).

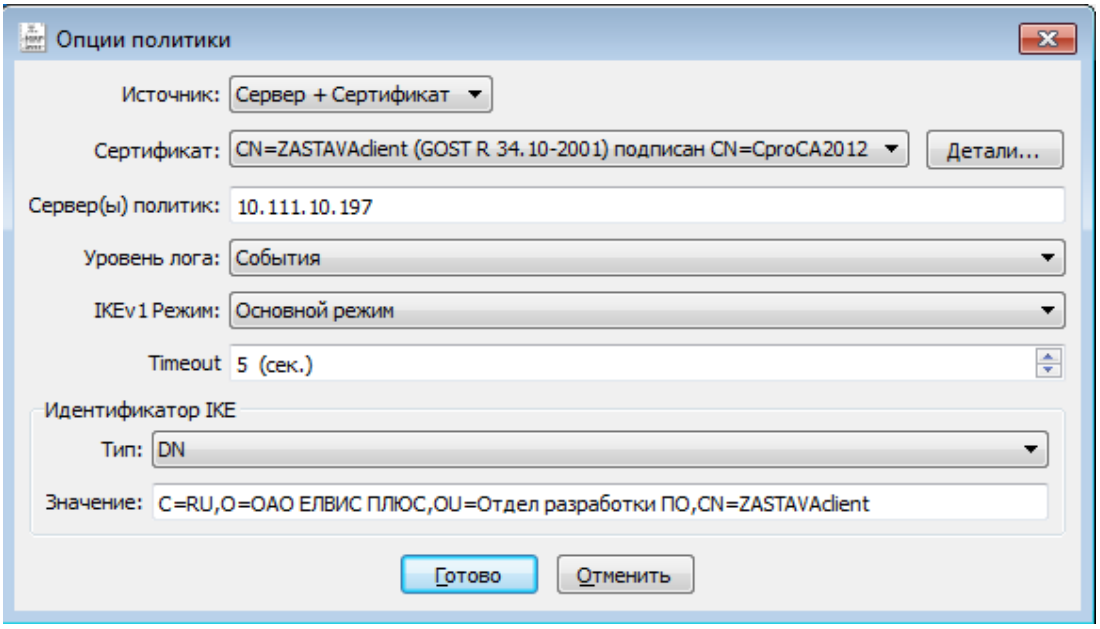

Рисунок 39 - Настройка параметров политики пользователя

Для настройки *политики пользователя* 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 нажав кнопку «Выбрать» выбрать необходимый файл из файловой системы, затем нажать кнопку «Готово» (см. Рисунок 40). Сохранение опций политики требует введения логина и пароля пользователя, который входит в группу администраторы.

– При выборе метода прогрузки «Отсутствует» в случае ошибки при прогрузке пользовательской политики, будет прогружаться системная политика.

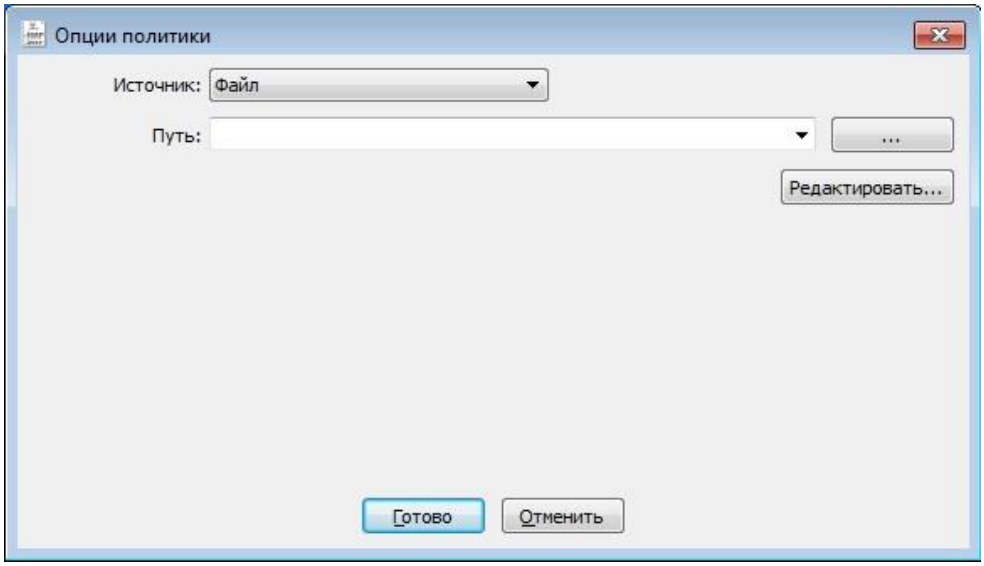

Рисунок 40 – Настройки политики пользователя при прогрузки политики из файла

– При выборе метода прогрузки с сервера (для загрузки ЛПБ с сервера и установки IPsec SA с помощью сертификата) необходимо в поле «Источник» выбрать значение «Сервер+Сертификат» (см. Рисунок 41). Для настройки прогрузки пользовательской политики с сервера необходимо:

  – Выбрать из выпадающего списка поля «Сертификат» зарегистрированный сертификат.

	С помощью кнопки «Редактировать» при выборе метода активации из файла можно произвести изменение файла политики в окне «Редактор».
	С помощью кнопки «Детали» при выборе метода активации с сервера можно просмотреть параметры выбранного сертификата в окне «Параметры сертификата».
	При выборе метода прогрузки «Сервер+Сертификат» можно указать значение «Любой персональный сертификат» в поле «Сертификат» при этом для активации будет использован сертификат, который не указан в параметрах системной политики.

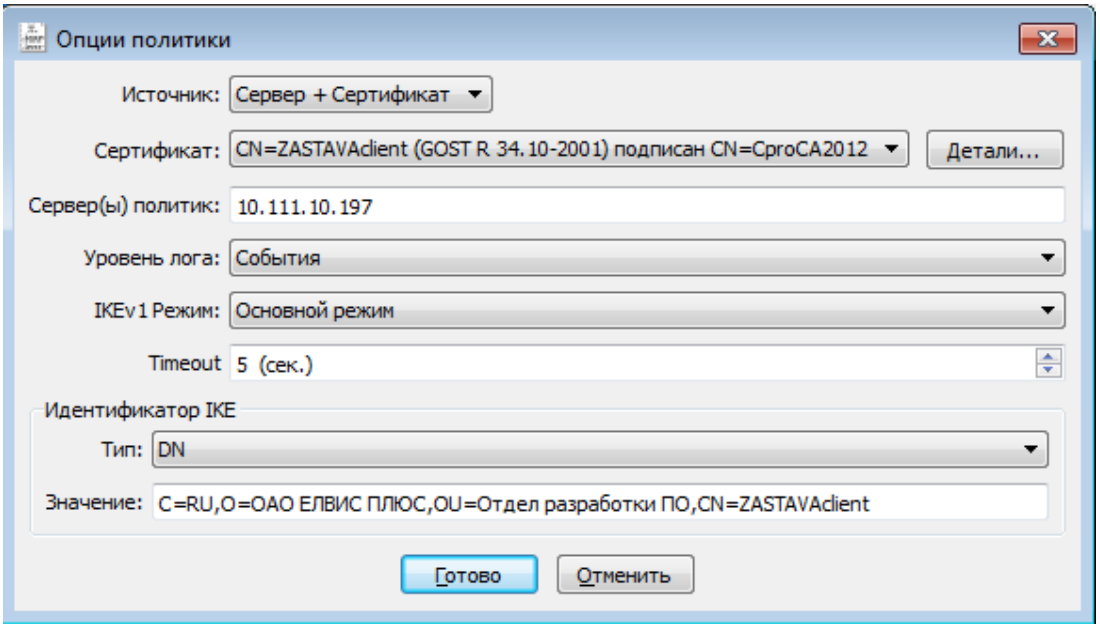

Рисунок 41 – Настройки политики пользователя при выборе метода прогрузки с сервера

- Ввести адрес сервера в строке «Сервер(ы) политик» и указать порт, с которого будет получена политика, если не указать порт, 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.
- 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. п. 3.8.1.1.
- Выбрать режим установления соединения IKE v1: основной или агрессивный в поле «IKE v1 Режим».
- Отметить время, через которое необходимо обращаться к серверу за ЛПБ, в поле «Time out».
- В секции «Идентификатор IKE» выбрать тип IKE идентификатора для прогрузки политики, согласованного с ЦУП.

2) Нажать кнопку «Готово». Сохранение опций политики требует введения логина и пароля пользователя, который входит в группу администраторы.

3) В появившемся после сохранения параметров политики информационном окне нажать кнопку «Да», если Вы хотите активировать данную политику, «Нет», если не хотите активировать данную политику.

3.5.3.3. Политика драйвера по умолчанию

В *ПК «ЗАСТАВА-Клиент»* имеется простая политика обработки трафика, которая используется 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 42). «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 «Сохранить» для сохранения настроек в *ПК «ЗАСТАВА-Клиент»*.

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).

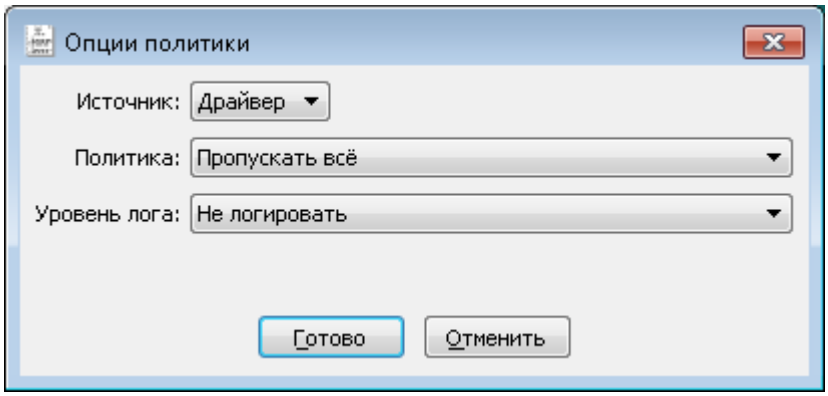

Рисунок 42 – Настройка параметров «Политика драйвера по умолчанию»

	Если на компьютере с *ПК «ЗАСТАВА-Клиент»* 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, используемая перед входом пользователя.
- Политика пользователя – политика, используемая после входа пользователя в ОС.

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

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 *ПК «ЗАСТАВА-Клиент»* объект в глобальную политику безопасности (ГПБ);
- Определить правила для данного объекта;
- Оттранслировать ГПБ в ЛПБ или сохранить ЛПБ как файл;
- Зарегистрировать ЛПБ в *ПК «ЗАСТАВА-Клиент»*. За дополнительной информацией надо обратиться к п. 3.5.5.1.

Файл с ЛПБ нужно перенести на компьютер *ПК «ЗАСТАВА-Клиент»* и затем зарегистрировать, согласно инструкциям в п. 3.5.3.1 и п. 3.5.3.2, или зарегистрировать ее с помощью команды `vpnconfig -set lsp user/system file <path>`.

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 *ПК «ЗАСТАВА-Клиент»*

обратится к заданному источнику и скопирует политику в драйвер *Агент*а, после чего эта политика будет активирована. Для регистрации новой ЛПБ необходимо:

- Нажать кнопку «Правка».
- 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:

  - Выбрать один из параметров:
    - Параметр «Сервер+Сертификат» (для загрузки ЛПБ с сервера и установки IPsec SA с помощью сертификата),
    - Параметр «Сервер+Ключ» (для загрузки ЛПБ с сервера и установки IPsec SA с помощью Preshared Key, только для системной ЛПБ);
  - Выбрать из выпадающего списка зарегистрированный сертификат или Preshared Key, в соответствии с выбранным методом прогрузки с сервера.
  - Ввести адрес сервера в строке «Сервер(ы) политик» 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.
  - Выбрать режим установления соединения IKE v1: основной или агрессивный в поле «IKE v1 Режим».
  - Отметить время, через которое необходимо обращаться к серверу за ЛПБ, в поле «Time out».
  - Выбрать тип идентификатора в секции «Идентификатор IKE» для прогрузки политики, который должен быть согласован с ЦУП.
- Нажать кнопку «Сохранить».
- 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 Вам файлы могут оказаться скрытыми.

3.5.5.2. Регистрация новой пользовательской ЛПБ

Регистрация пользовательской ЛПБ производится также как регистрация системной политики см. п. 3.5.5.1.

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» *ПК «ЗАСТАВА-Клиент»* и нажать кнопку «Активировать», ввести логин и пароль администратора. 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»

ПК «ЗАСТАВА-Клиент» позволяет использовать токены как среду транспортировки важной информации (сертификатов, закрытых ключей). *ПК «ЗАСТАВА-Клиент»* 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 43) 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. Доступна возможность загружать модули токенов как пользовательские.

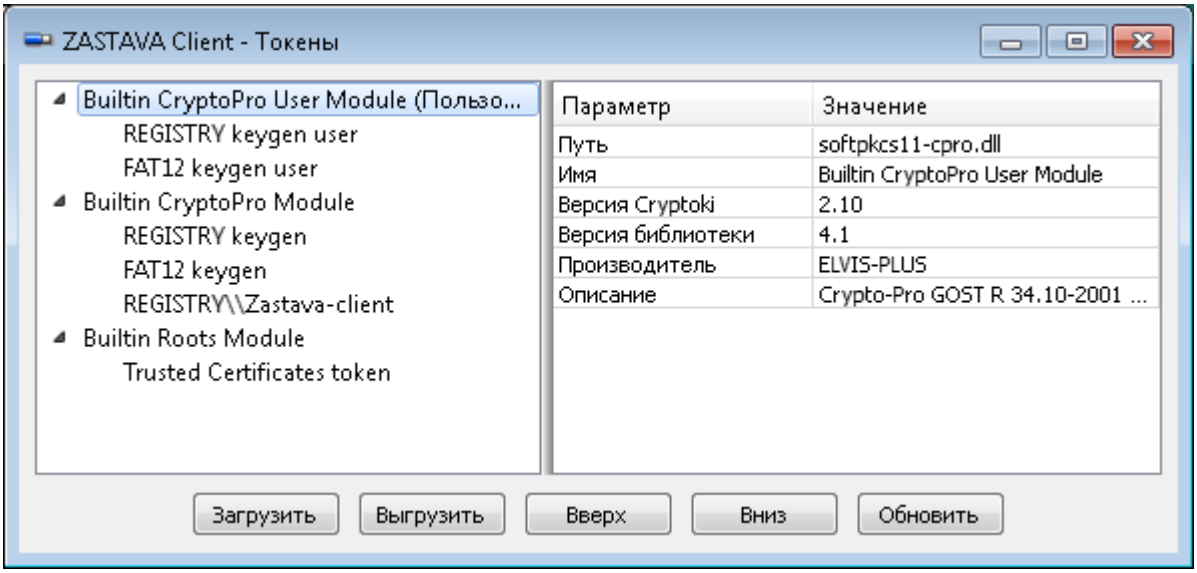

Рисунок 43 – Окно «Токены»

3.6.1. Добавление модулей токенов

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

1) Нажать кнопку «Загрузить» в окне «Токены», в появившемся окне «Загрузить модуль» ввести требуемые данные (см. Рисунок 44).

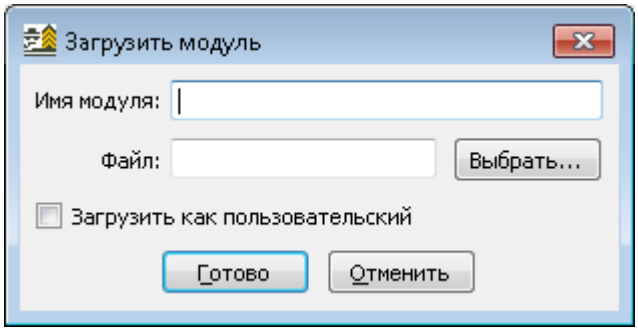

Рисунок 44 – Окно «Загрузить модуль»

2) Ввести Имя модуля PKCS#11.

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

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

Если Вы используете в качестве токена смарт-карту или USB-носитель, тогда требуемое ПО должно входить в комплект поставки токена. Имена библиотечных модулей PKCS#*11, которые входят в состав *ПК «ЗАСТАВА-Клиент»*, приведены в таблице (см. Таблица 21). Обратите внимание на то, что другие PKCS#11 библиотеки могут поставляться с другим

ПО для токенов. Чтобы найти имя требуемой библиотеки обратитесь к документации по токенам.

Таблица 21 – 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 *ПК «ЗАСТАВА-Клиент»*	

При необходимости отметить флаг «Загрузить как пользовательский», определив загружаемый модуль токена определенному пользователю.

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 *ПК «ЗАСТАВА-Клиент»*.
	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 закладке «Модули Токенов» необходимо:

1) Нажать кнопку «Инициализировать» в окне «Токены», в появившемся окне «Инициализация токена» вписать данные (см. Рисунок 45).

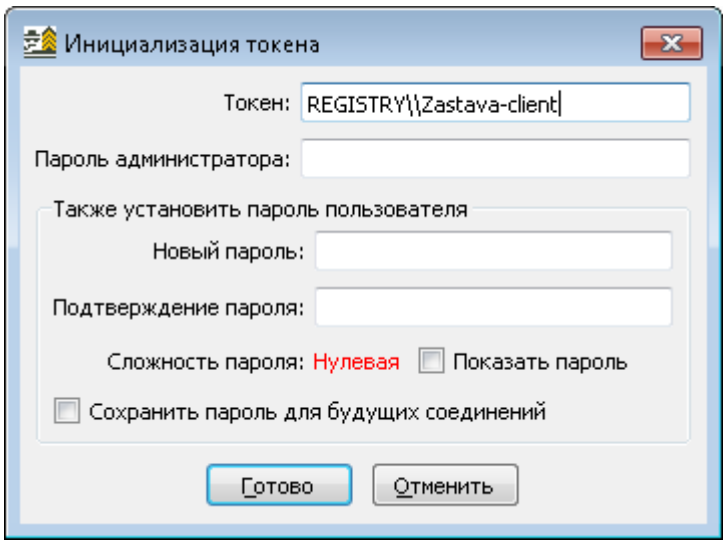

Рисунок 45 – Окно «Инициализация токена»

2) Ввести пароль администратора токена.

3) В поле «Также установить пароль пользователя» в поле «Новый пароль» ввести новый пароль пользователя и повторить введенный пароль в поле «Подтверждение пароля».

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

5) Нажать кнопку «Готово».

3.6.4. Удаление модуля токена

Чтобы удалить модуль PKCS#11 из *ПК «ЗАСТАВА-Клиент»* 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 во всех компонентах ПК «VPN/FW «ЗАСТАВА», версия 6 (компонент *ЗАСТАВА-Управление*, версия 6, компонент *ПК «ЗАСТАВА-Клиент»*, версия 6 и компонент *ЗАСТАВА-Офис*, версия 6). 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 ПК «VPN/FW «ЗАСТАВА», версия 6 как отдельный модуль (плагин). По

умолчанию, в состав ПК «VPN/FW «ЗАСТАВА», версия 6 входит набор штатных криптобиблиотек (см. Таблица 22).

Таблица 22 – 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. Значок раскрывающегося списка (►) рядом с именем криптобиблиотеки означает, что она содержит криптоалгоритмы. Чтобы просмотреть криптоалгоритмы, содержащиеся в любой зарегистрированной криптобиблиотеке, необходимо нажать на значок раскрывающегося списка рядом с именем. Список алгоритмов, содержащихся в криптобиблиотеке, расширится, как показано на рисунке (см. Рисунок 46).

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

По умолчанию в *Агентах* установлены следующие криптобиблиотеки, представленные в таблице (см. Таблица 22).

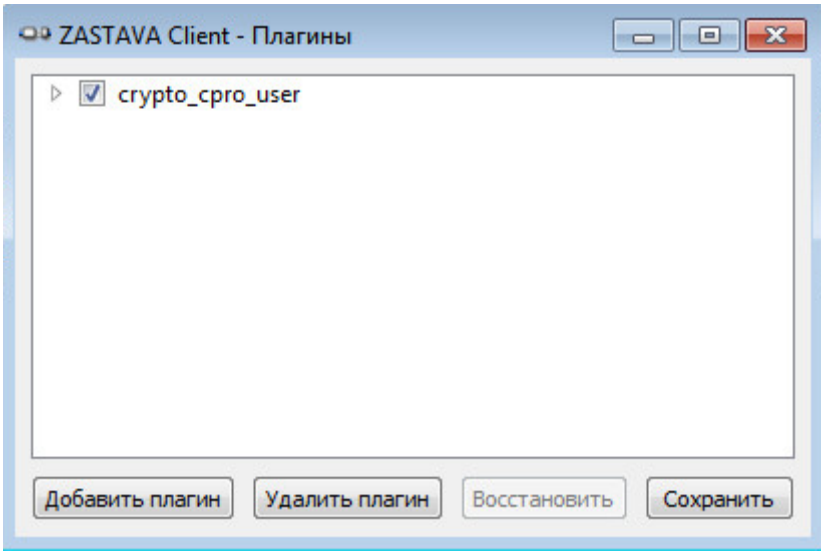

Рисунок 46 – Окно модуля криптоплагинов

3.7.2. Регистрация криптобиблиотеки

Модуль криптоплагинов может управлять криптобиблиотеками (регистрировать и активировать), которые используются 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 ПК «VPN/FW «ЗАСТАВА», версия 6.

Для регистрации новой криптобиблиотеки необходимо:

- 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 убедитесь 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 *Агентов*, можно разделить на две группы:

- локальные установки;
- параметры в ЛПБ.

Окно «Прочие настройки» предназначено для изменения локальных установок *ПК «ЗАСТАВА-Клиент»*. При штатной работе *ПК «ЗАСТАВА-Клиент»* изменение локальных установок обычно не требуется и управление *ПК «ЗАСТАВА-Клиент»* 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 47).

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.

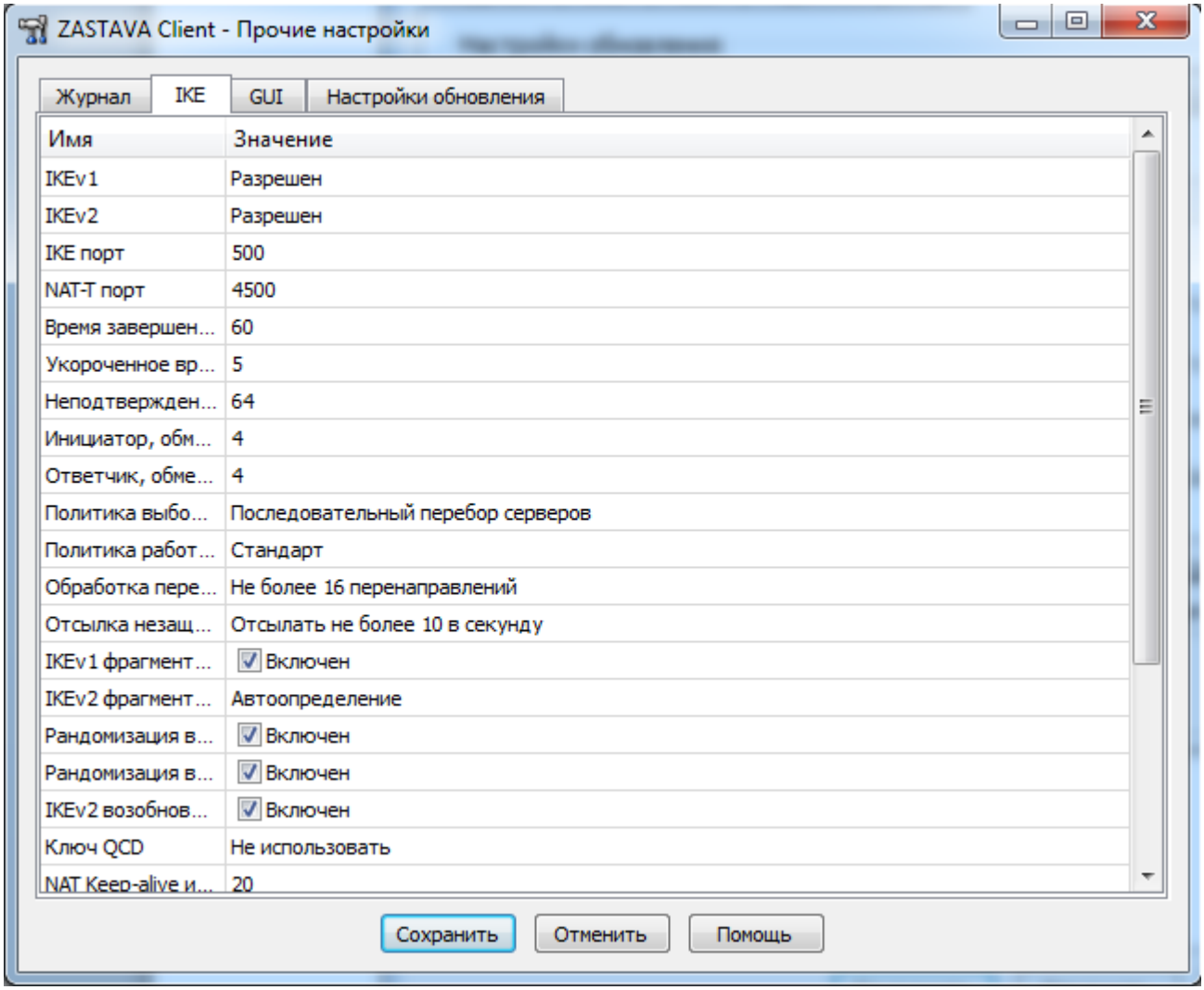

Рисунок 47 – Окно «Прочие настройки» с отображением закладки «IKE»

Окно «Прочие настройки» имеет закладки для следующих параметров, приведенных в таблице (см. Таблица 23).

Таблица 23 – Параметры окна «Прочие настройки»

Наименование вкладки	Параметры
Журнал	Установка параметров журнала регистрации событий
IKE	Установка значений параметров протокола IKE
GUI	Установка параметров представления информации в графическом интерфейсе *ПК «ЗАСТАВА-Клиент»*
Настройки обновления	Управление механизмом автоматического обновления

3.8.1. Вкладка «Журнал»

Регистрация событий позволяет сохранять хронологию системных событий, происходящих в *ПК «ЗАСТАВА-Клиент»*. Настройку системы регистрации событий можно произвести во 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 48). 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.

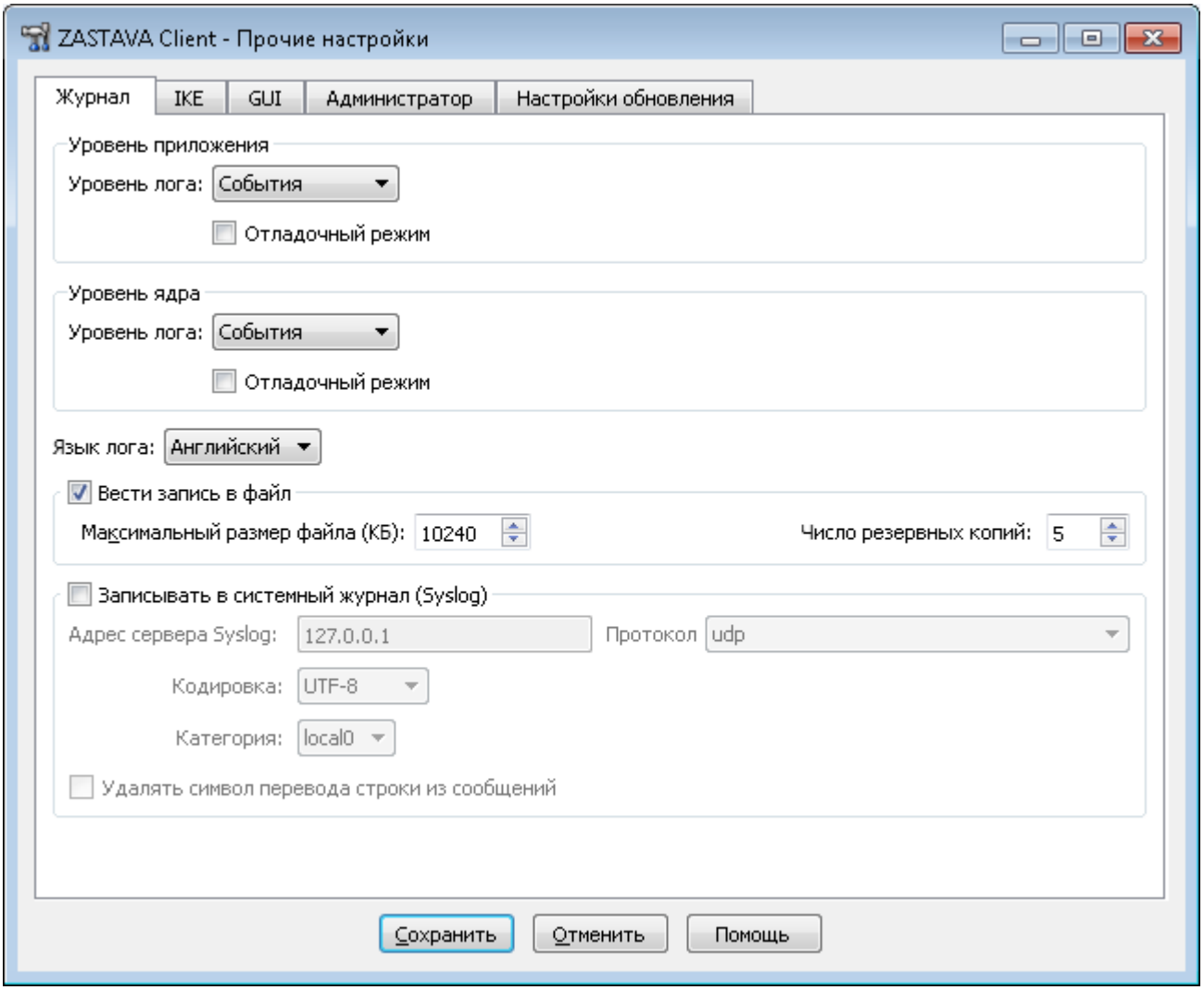

Рисунок 48 – Вкладка «Журнал» окна «Прочие настройки»

3.8.1.1. Уровень регистрации событий

Задать уровень регистрации событий можно для двух уровней: Уровень приложения и Уровень ядра (см. Рисунок 48). 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 48) уровни регистрации событий, заданные в политике, будут игнорироваться.

Описание уровней регистрации событий приведено в таблице (см. Таблица 24).

Таблица 24 – 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 *ПК «ЗАСТАВА-Клиент»*.

Параметры уровня регистрации могут также указываться в ЛПБ, созданной *ЗАСТАВА-Управление* для *ПК «ЗАСТАВА-Клиент»*. 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 *ПК «ЗАСТАВА-Клиент»* для ОС Windows, в секции /var/vpnagent/ для ОС ALT Linux. Некоторые из этих параметров могут также настраиваться через графический интерфейс *ПК «ЗАСТАВА-Клиент»* – 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 отредактируйте значение в поле «Максимальный размер файла (КБ)». 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 *ПК «ЗАСТАВА-Клиент»*, 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

ПК «ЗАСТАВА-Клиент» 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 25).

Таблица 25 – 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
Категория	Оно из предопределённых значений от local0 до local7. Позволяет идентифицировать сообщения от *ПК «ЗАСТАВА-Клиент»* в общем журнале
Кодировка	Кодировка, в которой будут формироваться сообщения для системного журнала
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 в ОС Linux необходимо также отредактировать файл `/etc/syslog.conf`, добавив строку вида:

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

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

`<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»

ПК «ЗАСТАВА-Клиент» позволяет настроить параметры протокола IKE для этого необходимо воспользоваться закладкой «IKE» окна «Прочие настройки» (см. Рисунок 49).

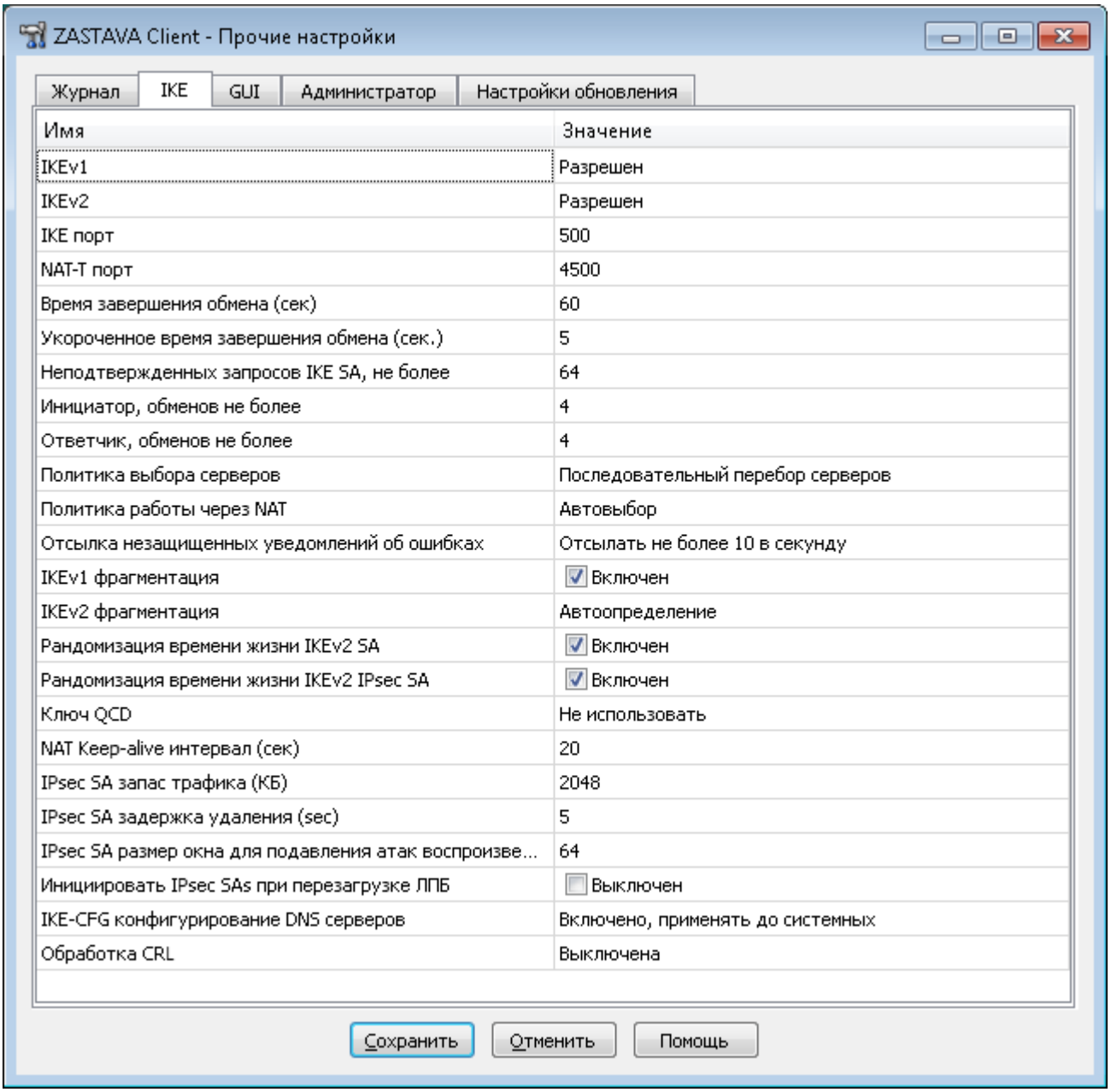

Рисунок 49 - Окно «Прочие настройки» вкладка «IKE»

3.8.2.1. Изменение параметров

Все параметры в закладках изменяются одинаково:

1) Выделив параметр и двойным нажатием левой кнопкой мыши на параметре ввести необходимое значение параметра, либо убрать флаг с параметра или выбрать значение из выпадающего списка.

Ввести информацию. Недопустимые символы не отображаются в поле.

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 26).

Таблица 26 – Параметры IKE

Параметр	Расшифровка
IKEv1	Управление режимом работы IKEv1 (по умолчанию - Разрешен) Режимы: — Разрешен; — Только ответчик; — Запрещен.
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)
Неподтвержденных запросов IKE	Максимальное количество стейтов IKE в процессе создания SA, в которых нет подтверждения IP-адреса партнера (0-

Параметр	Расшифровка
SA, не более	256, по умолчанию 64) Если количество запросов от неподтвержденных IP-адресов превышает этот параметр, то дальнейшие действия зависят от версии протокола IKE. Для IKEv1 любой новый запрос игнорируется. Для IKEv2 любой новый запрос также игнорируется, но при этом запускается процедура подтверждения IP-адреса. Эта процедура заключается в отправке инициатору специального значения – COOKIE, которое тот должен вернуть. 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
Инициатор, обменов не более	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.
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 (по умолчанию – Последовательный перебор серверов) Режимы: — Соединяться только с первым сервером из списка; — Последовательный перебор серверов; — 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 - Автовыбор)
Отсылка незащищенных уведомлений об ошибках	Частота отправки незащищенных сообщений об ошибках (по умолчанию – Отсылать не более 10 в секунду). Возможные значения: не отсылать, Отсылать не более 1 сек, Отсылать не более 10 сек, Отсылать не более 100 сек, Всегда отсылать.
IKE v1 фрагментация	Включение/отключение режима фрагментации (IKEv1) (по умолчанию включен)

Параметр	Расшифровка
IKE v2 фрагментация	Управление режимом фрагментации (IKEv2) (по умолчанию – Автоопределение) Значения: — Не использовать; — Автоматический; — Всегда фрагментировать.
Рандомизация времени жизни IKE v2 IPsec SA	Рандомизация времени жизни IPsec SA (по умолчанию включена)
Рандомизация времени жизни IKE v2 SA	Рандомизация времени жизни IKE SA (IKEv2) (по умолчанию включена)
Ключ QCD	Ключ для выработки токена для метода Quick Crash Detection (генерируется автоматически или может быть отключен, по умолчанию «Не использовать»). 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) (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 (по умолчанию 5)
Инициировать IPsec SA при перезагрузке ЛПБ	При включенном режиме на каждое IPSec правило в политике создается IKE и IPsec SA при перегрузке политики.
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.
Инициировать IPsec SAs при загрузке ЛПБ	Управление режимом инициации IPsec SAs при загрузке ЛПБ (по умолчанию выключен).
IKE-CFG конфигурирование DNS серверов	Параметр, регулирующий режимы обработки IKE-CFG. При установлении SA, на интерфейсе, через который оно установлено, прописывается DNS-сервер в зависимости от настроек: — Выключено – используется системный DNS. DNS, указанный в политике, не используется; — Включено – используется DNS, указанный в политике, системный DNS не используется;

Параметр	Расшифровка
	— Включено, применять до системных (используется по умолчанию) – используется DNS, указанный в политике, и он применяется в первую очередь; — Включено, применять после системных – DNS, указанный в политике, используется после неудачной попытки использования системного DNS. После разрыва SA соответствующая запись о DNS-сервере удаляется.
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 *ПК «ЗАСТАВА-Клиент»* в *ЗАСТАВА-Управление*.

3.8.2.3. Политика работы через NAT

Управление политикой выбора метода работы через NAT осуществляется из локальных настроек *ПК «ЗАСТАВА-Клиент»* в закладке «IKE» параметр «Политика работы через NAT». Политика может быть такой, как представленная в таблице (см. Таблица 27).

Таблица 27 – Управление политикой выбора метода работы через NAT

Параметр	Расшифровка
Не использовать	*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).

Параметр	Расшифровка
Автовыбор	Этот режим устанавливается по умолчанию после установки *Агента*. 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, независимо 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, независимо 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, независимо 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 «GUI»

Закладка «GUI» окна «Прочие настройки» позволяет настроить представление графического интерфейса *ПК «ЗАСТАВА-Клиент»* (см. Рисунок 50).

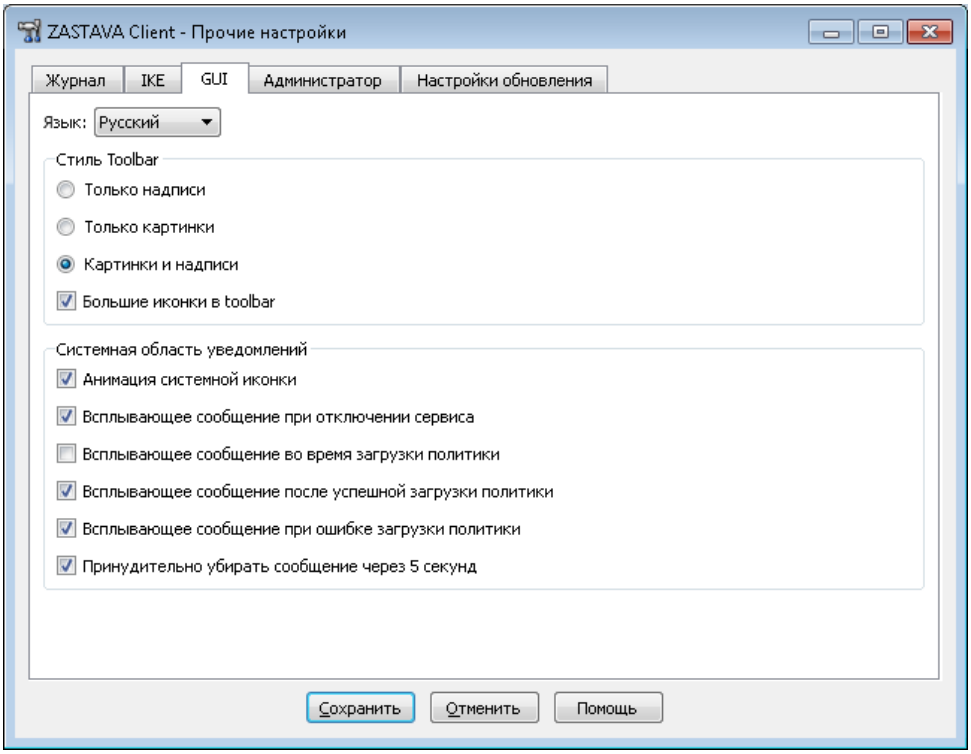

Рисунок 50 – Закладка «GUI» окна «Прочие настройки»

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 ПК «ЗАСТАВА-Клиент»*, для этого необходимо поставить флаг в поле «Большие иконки в toolbar». Язык GUI также можно поменять в этой закладке.

В поле «Системная область уведомлений» можно настроить отображение всплывающих окон в качестве реакции на события в системе, а также включить анимацию системной иконки.

Параметры закладки «GUI» представлены в таблице (см. Таблица 28).

Таблица 28 – Параметры окна «GUI»

Параметр	Описание
Только картинки	Отображает/скрывает Панель управления в виде иконок и в представлении всех окон *ПК «ЗАСТАВА-Клиент»*.
Только надписи	Отображает/скрывает имена кнопок на *Панели управления* и в представлении всех окон *ПК «ЗАСТАВА-Клиент»*.
Картинки и надписи	Отображает/скрывает имена кнопок на *Панели управления* и в представлении всех окон *ПК «ЗАСТАВА-Клиент»*.
Большие иконки в toolbar	Изменяет размер иконок на *Панели управления* и в представлении всех окон *ПК «ЗАСТАВА-Клиент»*.
Язык	Изменяет язык интерфейса (пункты «Русский», «English»)

Параметр	Описание
	представления GUI *ПК «ЗАСТАВА-Клиент»*.
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 политики	Включает трансляцию всплывающих сообщений после успешной загрузки 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 используется - включен)

3.8.4. 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 29).

Таблица 29 – 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

3.8.5. Вкладка «Настройки обновления»

Закладка «Настройки обновления» окна «Прочие настройки» предназначена для локального конфигурирования автоматических обновлений (подробнее см. в п. 3.8.5.1).

3.8.5.1. Описание элементов интерфейса

ПК «ЗАСТАВА-Клиент» позволяет Вам произвести настройки обновлений. В закладке «Настройки обновления» окна «Прочие настройки» (см. Рисунок 51) Вы можете 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 30).

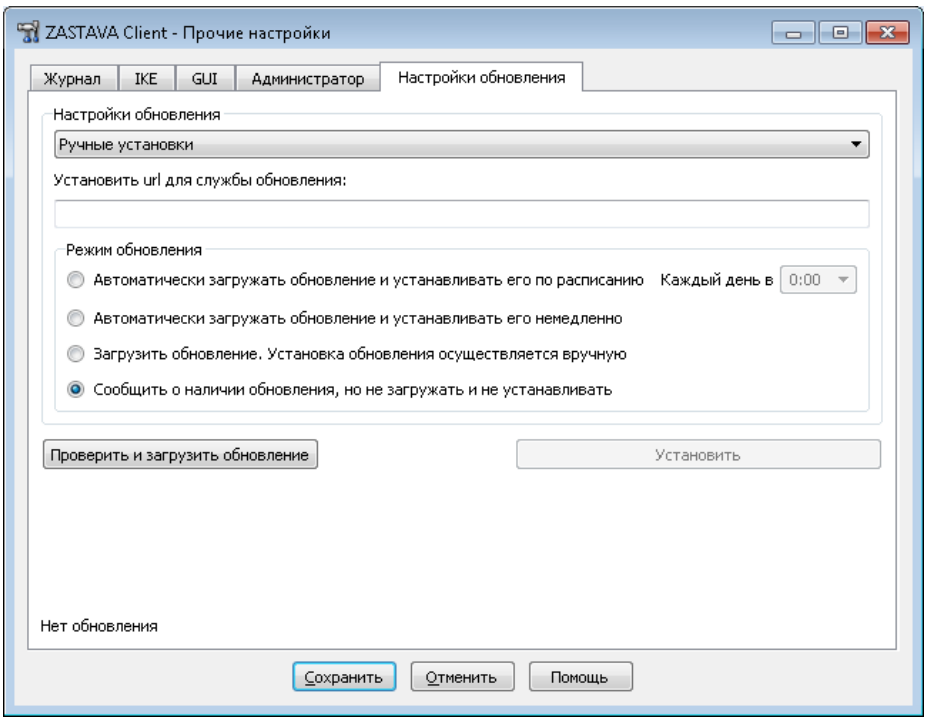

Рисунок 51 – Окно «Прочие настройки» с отображением закладки «Настройки обновления»

Таблица 30 – Описание элементов интерфейса вкладки «Настройки обновления»

Элемент	Описание
Выпадающий список	Метод конфигурирования обновлений. Доступные значения: **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 (четыре варианта). Примечание. Формат строки расписания приведен в п. 3.8.5.2.
Кнопка «Проверить и загрузить обновление»	При нажатии кнопки проверяется соединение с указанным сервером и наличие свежей версии *ПК «ЗАСТАВА-Клиент»*. В случае успеха будет выведено соответствующее сообщение и можно будет запустить скачивание обновления.

Элемент	Описание
Кнопка «Установить»	Инсталлировать скачанное обновление.

3.8.5.2. 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 *ПК «ЗАСТАВА-Клиент»*. 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». В окнах *ПК «ЗАСТАВА-Клиент»* справочная система может быть вызвана с помощью клавиши <F1>, кнопки «Помощь» или команд «Помощь меню» (если возможно).

Навигационная область справочной системы отображается при запуске окна «Help» и содержит оглавление «ПК «ЗАСТАВА-Клиент» 6. Справочная система» (см. Рисунок 52).

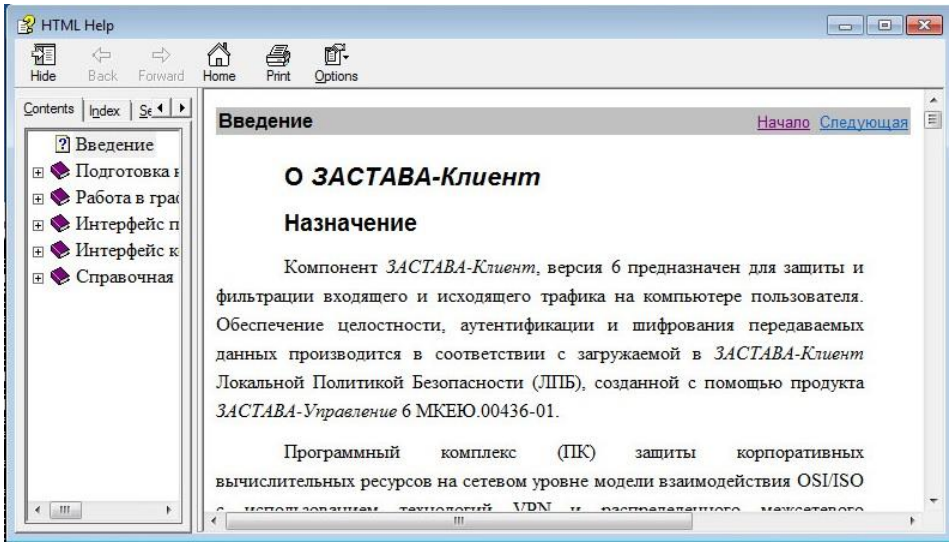

Рисунок 52 – Навигационная область справочной системы

Для просмотра справки по определенным интересующим настройкам необходимо нажать ссылку на необходимый Вам раздел для его просмотра. При выборе раздела из списка, этот раздел будет отображен в новом окне (см. Рисунок 53).

Навигационные кнопки «Previous» (Предыдущая), «Top» (Начало) и «Next» (Следующая) расположены справа вверху раздела. Используя эти кнопки, Вы можете передвигаться по разделам в их логической последовательности.

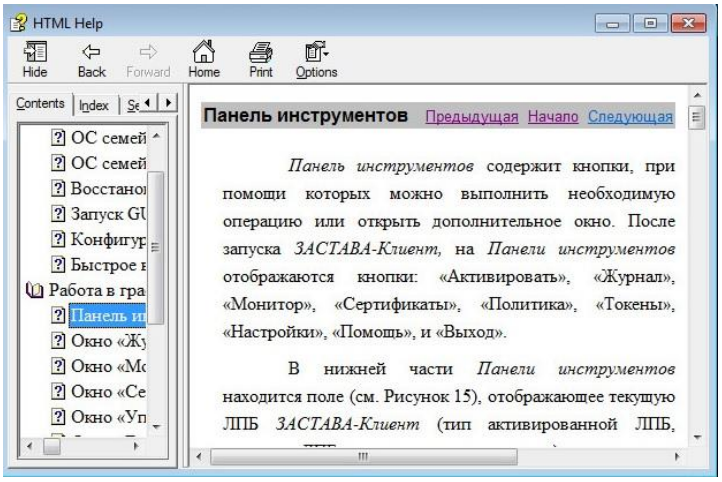

Рисунок 53 – Инструментальная панель справочной системы

4. ИНТЕРФЕЙС *ПАНЕЛИ УПРАВЛЕНИЯ* РАБОЧЕГО СТОЛА

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

Для отображения текущего статуса ЛПБ *ПК «ЗАСТАВА-Клиент»* существуют пять иконок, каждая со своим собственным цветом. Статус всегда показывается, независимо от того, открыт на Вашем рабочем столе *ПК «ЗАСТАВА-Клиент»* или нет.

При двойном нажатии на иконке левой кнопкой мыши открывается графический интерфейс *ПК «ЗАСТАВА-Клиент»*.

4.1. Контекстное меню

С помощью контекстного меню иконки на панели инструментов рабочего стола (см. Рисунок 54) можно двойным нажатием на иконке левой кнопкой мыши запустить *Панель инструментов ПК «ЗАСТАВА-Клиент»*, или однократным нажатием правой кнопкой мыши на иконке запустить контекстное меню, выбрав параметр «Панель управления», получить справку по *ПК «ЗАСТАВА-Клиент»,* выбрав в выпадающем меню параметр «Помощь», открыть необходимое окно *Панели управления*, для настройки параметров, либо закрыть интерфейс панели инструментов рабочего стола, выбрав параметр «Выход».

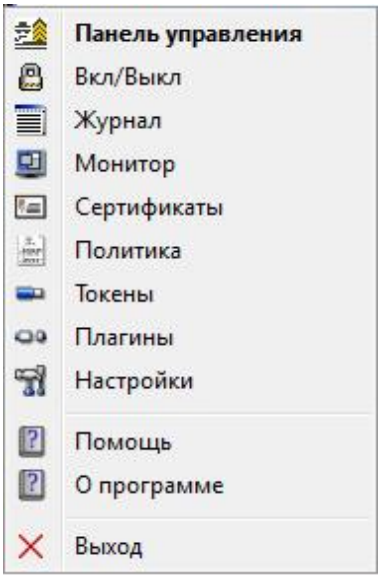

Рисунок 54 – Контекстное меню иконки статуса на панели инструментов рабочего стола

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 55).

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

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

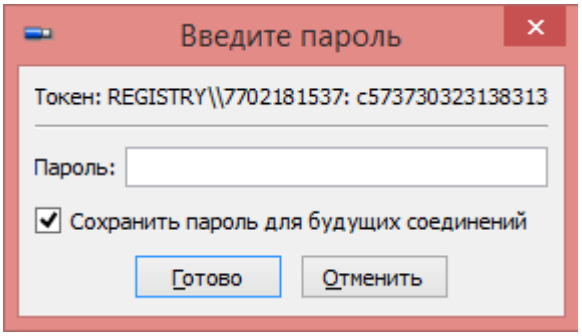

Рисунок 55 – Ввод пароля токена при создании защищенного соединения

4.3. Индикация текущего статуса

Поместив курсор поверх иконки, подождите 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 31).

Таблица 31 – Перечень графических символов статусов ЛПБ

Статусы *ПК «ЗАСТАВА-Клиент»*	**Иконка (цвет)**
Ошибка активации; предыдущая политика не будет восстановлена. Прогружена любая другая политика, например, «Политика драйвера по умолчанию»	(красный)
Активирована текущая пользовательская ЛПБ	(зелёный)
Активирована текущая системная ЛПБ	(темно зеленый)
Ошибка активации; предыдущая политика будет восстановлена	(жёлтый)
Активирована «Политика драйвера по умолчанию»	(синий)
Системная служба *ПК «ЗАСТАВА-Клиент»* `vpndmn` не запущена	(серый)

Статусы *ПК «ЗАСТАВА-Клиент»*	**Иконка (цвет)**
При загрузке политики *ПК «ЗАСТАВА-Клиент»* с ЦУП (сервер доступен)	 (темно зеленый с ярко зеленой рамкой)
При загрузке политики *ПК «ЗАСТАВА-Клиент»* с ЦУП (сервер не доступен)	 (желтый с красной рамкой)

Также, в зависимости от текущего статуса ЛПБ, могут представляться следующие иконки (см. Таблица 32), иконка со статусом «Системная служба *ПК «ЗАСТАВА-Клиент»* `vpndmn` остановлена» никаких дополнительных статусов не имеет.

Таблица 32 – Иконка статуса. Дополнительные изображения к цвету иконки

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

5. Интерфейс командной строки

Интерфейс командной строки позволяет администратору автоматизировать процесс конфигурирования *ПК «ЗАСТАВА-Клиент»*. 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 *ПК «ЗАСТАВА-Клиент»*

5.1.1. Обзор средств мониторинга

Для возможности осуществления мониторинга работы *ПК «ЗАСТАВА-Клиент»* используются следующие средства:

- Журналы регистрации событий (bin_log.txt, vpndmn_init.log);
- Утилиты конфигурирования и мониторинга активности, входящие в комплект поставки *ПК «ЗАСТАВА-Клиент»*.

5.1.1.1. Файл регистрации системных событий

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

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

В ЛПБ для каждой группы системных событий ([POLICY] (политика безопасности), [CERTS] (сертификаты) и т.д.) может содержаться настройка уровня детализации. Если уровень детализации для соответствующей группы событий отсутствует в ЛПБ, то в этом случае будут использованы локальные настройки уровня 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 выполнить команду (см. Таблица 33):

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

Таблица 33 – Параметры команды `vpnmonitor -s`

Параметр	Описание
all	Просмотр полной статистики
ipsec	Просмотр статистики IPsec
ike	Просмотр статистики IKE (IKE v1 и IKE v2)
ike1	Просмотр статистики IKE v1
ike2	Просмотр статистики IKE v2
fcache	Просмотр статистики fcache

Список параметров выводимой статистики представлен в таблице (см. Таблица 34).

Таблица 34 – Печень параметров статистики

Параметр	Описание
IPsec	
Packets (bytes) recieved	Количество пакетов, полученное с момента запуска *Агента*
Packets (bytes) sent	Количество пакетов, посланное с момента запуска *Агента*
Decapsulated packets	Количество пакетов, расшифрованных *Агентом*
Encapsulated packets	Количество пакетов, зашифрованных *Агентом*

Параметр	Описание
Packets recieved unsecure	Количество полученных *Агентом* незашифрованных пакетов
Packets sent unsecure	Количество отправленных незашифрованных пакетов
Incoming errors	Количество ошибок во входящих пакетах
Outgoing errors	Количество ошибок в исходящих пакетах
Incoming auth errors	Количество ошибок аутентификации во входящих пакетах
Incoming anti-replay errors	Количество ошибок при подавлении атак воспроизведения во входящих пакетах
Dropped packets (in/out)	Количество отброшенных пакетов или фрагментов
Input frags consumed	Количество IP-фрагментов, использованных при реассемблировании входного пакета
Output frags consumed	Количество IP-фрагментов, использованных при реассемблировании выходного пакета
Output frags created	Количество IP-фрагментов, созданных при фрагментации выходного пакета
Decrease MTU requests	Количество пакетов – запросов на понижение MTU
Incoming packets not found in hash table	Количество промахов для входящих пакетов при поиске фильтра в хэш-таблице
Outgoing packets not found in hash table	Количество промахов для исходящих пакетов при поиске фильтра в хэш-таблице
IKEv1	
IKE SAs created (failed) initiated/responded	Количество созданных (не созданных) инициированных/отвеченных IKE SA в формате x(x)/x(x)
Denied IKE SAs requests	Количество отвергнутых запросов на создание IKE SA
IPsec SA bundless created	Количество созданных IPsec SA
MM exchanges completed (failed) initiated/responded	Количество успешных (неуспешных) обменов MainMode инициировано/отвечено в формате x(x)/x(x)
AM exchanges completed (failed) initiated/responded	Количество успешных (неуспешных) обменов Aggressive Mode инициировано/отвечено в формате x(x)/x(x)

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

Параметр	Описание
INFO exchanges completed (with errors or failed) initiated/responded	Количество успешных (с ошибками или неуспешных) обменов INFORMATIONAL инициировано/отправлено в формате x(x)/x(x)
FiltDB Кэш	
Hash table size (bytes max/alloc)	Размер хэш-таблицы (байт максимум/выделено) в формате x*x*x(x/x)
Validity tag	Текущее значение метки, служащей для определения возможности использования записей в хэш-таблице
Live entries	Количество активных записей
Dead entries	Количество удаленных записей
Allocated entries	Количество записей выделенных из памяти
Dead reused	Количество повторно использованных удалённых записей
Line reused	Количество использованных записей в линиях
Collisions	Количество попыток добавления одинаковых записей
Full lines	Количество заполненных линий
Empty lines	Количество пустых линий
Other lines	Количество остальных линий
Average length of non-empty lines	Средняя длина непустых линий

Пример вывода результата команды `vpnmonitor –s ipsec` представлен ниже:

```
param                          |value
-------------------------------|------------------------------
IPsec                          |
Packets (bytes) recieved       |979 847 (159 993 099)
Packets (bytes) sent           |87 331 (18 829 527)
Decapsulated packets           |4
Encapsulated packets           |4
Packets recieved unsecure      |979 843
Packets sent unsecure          |87 327
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~|72 662
n hash table                  |
Outgoing packets not found i~|337
n hash table                  |

IKEv1:  init: 0, resp: 1
IKEv2:  init: 0, resp: 0
IPsec:  bundles: 0, ESP: 0, AH: 0, IPcomp: 0
FiltDB: alt: 3, main: 10, dynamic: 0

vpndmn started at: 2015.12.11 10:07:03
       worked: 59 days 3 hours 42 minutes 52 seconds
```

5.2.3. Вывод информации о политике, активированной на *ПК «ЗАСТАВА-Клиент»*

Для просмотра информации об активированной на *ПК «ЗАСТАВА-Клиент»* политики необходимо выполнить команду: `vpnmonitor -p`. Пример вывода результата данной команды:

```
Current Policy:
Type: User Policy
Source: Server: 10.111.10.184
Title: client3
Activated: Fri Mar 31 13:07:10 2017
```

Для просмотра подробной информации о параметрах прогруженной политики используется команду: vpnmonitor –pp.

Пример вывода подробной информации о политике:

```
LSP request:
        type: User PMP
        user:
        file path:
        pmp servers: 10.111.10.131
        cert subject: C=RU,CN=Client132_EPCSP
        log level: EVENTS

LSP active:
        type: User PMP
        user:
        file path:
        pmp servers: 10.111.10.131
        pmp cert subject: C=RU,CN=Client132_EPCSP
        pmp cert issuer: C=RU,O=AO ELVIS PLUS,OU=ORPO,CN=CPROCA2016
        pmp cert serial: 560000007F8591F2256C830A6900000000007F
        pmp cert key alg: GOST R 34.10-2001
        pmp log level: EVENTS
        title: Client132
        hash: 1115288B2944A1435B974A301AE03186
        time: Mon Jun 19 14:06:20 2017
        in progress: false
        from DB: false
        cert present: true
```

```
        connected to TPN: true
        last error:
        diagnostic: User policy: 'Client132' activated at Mon Jun 19
14:06:20 2017
```

5.2.4. Просмотр информации по созданным 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 вывода команды `vpnmonitor -i` представлен ниже:

```
3E7F533AF88B3180.680772825362DB66       10.111.10.131   (DN)
C=RU,CN=GateWin131_CPROCA2016      GOST3410.2001-Sig / GOST3410.2001-Sig
        1       ESP(Tunnel) Initiator   192.168.21.0..192.168.21.255 <-
        10.111.10.132   rule_ipsec1
        6
E0DE20B215FBBC85.B82D26E6655783EE       10.111.10.131   (DN)
C=RU,CN=GateWin131_CPROCA2016      GOST3410.2001-Sig / GOST3410.2001-Sig
IKE states count 2
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 | table | list | 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 SA;
  - 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 table -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 35 и Таблица 36), `operation` – операция для произведения сравнения по выбранному полю с эталоном (см. Таблица 37), `etalon` – эталонное значение выбранного поля, по которому будет произведено сравнение в соответствии с выбранной операцией.

Таблица 35 – Параметры фильтрации протокола IKE

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 IDпартнера
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
peer_port	UDP-порт партнера
redirect_ip	IP компьютера, с которого произошло перенаправление на данный
peer_auth_method	Метод аутентификации партнера
auth_method	Метод и аутентификации локальный
cookie	IKEv1 SA cookie
spi	IKEv2 SPI

Параметр	Характеристика
log_level	Уровень регистрации событий
features	Список поддерживаемых опций

Таблица 36 – Параметры фильтрации протокола IPsec

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, с которым создано защищенное подключение
peer_port	UDP-порт партнера, с которым создано защищенное подключение
local_ip	IP-адрес локального компьютера, использованный при создании защищенного соединения
local_port	UDP-порт на локальном компьютере, использованный при создании защищенного соединения
ike_cfg_server	IKE CFG адрес, выданный клиенту
dhgroup	DH группа
filter	Фильтр
rule	Название применяемого правила
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	Состояние

Тип	Характеристика
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 37 – Описание типов операций фильтрации

Команда	Характеристика
Операции для фильтрации по типу обмена	
equal	значение поля равно эталону (значение может быть: mm (Main Mode), am

Команда	Характеристика
	(Aggressive Mode), qm (Quick Mode), ix (Informational), tx (Transaction), для IKEv2: resume, init, auth, child, info)
not_equal	значение поля не равно эталону
Операции для фильтрации по роли в процессе обмена	
equal	значение поля равно эталону (значение может быть: initiator, responder)
not_equal	значение поля не равно эталону
Операции для фильтрации по содержанию строк	
icontain	поле содержит подстроку (эталон), игнорируя регистр букв
not_icontain	поле не содержит подстроку (эталон), игнорируя регистр букв
contain	поле содержит подстроку (эталон), учитывая регистр букв
not_contain	поле не содержит подстроку (эталон), учитывая регистр букв
iequal	поле равняется эталону, игнорируя регистр букв
not_iequa	поле не равняется эталону, игнорируя регистр букв
equal	поле равняется эталону, учитывая регистр букв
not_equal	поле не равняется эталону, учитывая регистр букв
Операции для фильтрации по полю IP-адрес	
inrange	значение поля (IP-адрес) входит в диапазон заданный эталоном, в качестве эталона можно указать просто IP-адрес (10.1.1.1) или диапазон (10.1.1.1…10.1.1.255) или подсеть (10.1.1.0/24 или 10.1.1.0/255.255.255.0)
not_inrange	значение поля (IP-адрес) не входит в диапазон
equal	значение поля (IP-адрес) равно эталону (IP-адрес)
not_equal	значение поля (IP-адрес) не равно эталону (IP-адресу)
Операции для фильтрации по полю IP-порт	
equal	значение поля (порт) равно эталону
not_equal	значение поля не равно эталону
inrange	значение поля входит в диапазон заданный эталоном, в качестве эталона можно указать просто порт (8080) или диапазон (0…65535)
not_inrange	значение поля не входит в диапазон заданный эталоном
Операции для фильтрации по полю уровень лога	
equal	значение поля равно эталону (возможные значения: disabled, events,

Команда	Характеристика
	details, verbose)
not_equal	значение поля не равно эталону
gt	значение поля больше эталона (disabled < events < details < verbose)
lt	значение поля меньше эталона
gteq	значение поля больше или равно эталону
lteq	значение поля меньше или равно эталону
Операции для фильтрации по IPsec-соединению по полю mode	
equal	значение поля равно эталону (возможные значения: tunnel, transport)
not_equal	значение поля не равно эталону

В некоторых командных оболочках запрещено использование некоторых символов (например, в bash '(', ')', '*', кавычки и т.д.), поэтому перед этими символами нужно ставить знак '\' или использовать другие служебные символы данной командной оболочки либо 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 поиска стейта по его ID:

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

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

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 IKE стейтов 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 40).

Для просмотра определенного фильтра, можно воспользоваться командами

```
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>` – показывать информацию:

- `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 послендих <num> строк;

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

Таблица 38 – Параметры фильтрации протокола

Параметр	Характеристика
type	Параметр фильтрации по полю «Тип»
name	Параметр фильтрации по полю «Название»
action	Параметр фильтрации по полю «Действие»
log_level	Параметр фильтрации по полю «Уровень лога»
flags_ttl_str	Параметр фильтрации по времени жизни
comment	Параметр фильтрации по полю «Комментарий»

if-names	Параметр фильтрации по полю «Интерфейс»
srcsel_as_str	Параметр фильтрации по полю «Локальный селектор»
srcsel_ip	Фильтрация поля «Локальный селектор» по IP-адресу
srcsel_port	Фильтрация поля «Локальный селектор» по порту
dstsel_as_str	Параметр фильтрации по полю «Удаленный селектор»
dstsel_ip	Фильтрация поля «Удаленный селектор» по IP-адресу
dstsel_port	Фильтрация поля «Удаленный селектор» по порту
pkt_in	Параметр фильтрации по полю «Входящие пакеты»
pkt_out	Параметр фильтрации по полю «Исходящие пакеты»
bytes_in	Параметр фильтрации по полю «Входящих байт»
bytes_out	Параметр фильтрации по полю «Исходящих байт»
drop_in	Параметр фильтрации по полю «Входящих байт отброшено»
drop_out	Параметр фильтрации по полю «Исходящих байт отброшено»
miss_in	Параметр фильтрации по полю «Входящих промахов в кэше»
miss_out	Параметр фильтрации по полю «Исходящих промахов в кэше»
fh_count	Параметр фильтрации по полю «Записей в кэше»
fwprocs	Параметр фильтрации по полю «Фаервольные процедуры»

Таблица 39 – Описание типов операций фильтрации

Команда	**Характеристика**
Операции для фильтрации по типу обмена	
equal	значение поля равно эталону
not_equal	значение поля не равно эталону
Операции для фильтрации по содержанию строк	
icontain	поле содержит подстроку (эталон), игнорируя регистр букв
not_icontain	поле не содержит подстроку (эталон), игнорируя регистр букв
contain	поле содержит подстроку (эталон), учитывая регистр букв
not_contain	поле не содержит подстроку (эталон), учитывая регистр букв
iequal	поле равняется эталону, игнорируя регистр букв
not_iequa	поле не равняется эталону, игнорируя регистр букв
equal	поле равняется эталону, учитывая регистр букв
not_equal	поле не равняется эталону, учитывая регистр букв
Операции для фильтрации по полю уровень лога	
equal	значение поля равно эталону (возможные значения: disabled, events, details, verbose)
not_equal	значение поля не равно эталону

gt	значение поля больше эталона (disabled < events < details < verbose)
lt	значение поля меньше эталона
gteq	значение поля больше или равно эталону
lteq	значение поля меньше или равно эталону
Операции для фильтрации по полю IP-адрес	
contain	значение поля (IP-адрес) содержит эталон (IP-адрес)
not_ contain	значение поля (IP-адрес) не содержит эталон (IP-адрес)
Операции для фильтрации по полю IP-порт	
contain	значение поля (порт) содержит эталон
not_ contain	значение поля не содержит эталон
Unsigned int operation	
equal	значение поля равно эталону (возможные значения: disabled, events, details, verbose)
not_equal	значение поля не равно эталону
gt	значение поля больше эталона (disabled < events < details < verbose)
lt	значение поля меньше эталона
gteq	значение поля больше или равно эталону
lteq	значение поля меньше или равно эталону

Пример:

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

Таблица 40 – 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` представлен ниже:

```
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.

5.3. Утилита vpnconfig

Утилита конфигурирования `vpnconfig` предназначена для изменения и просмотра локальных установок *ПК «ЗАСТАВА-Клиент»*.

	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.

При штатной работе *ПК «ЗАСТАВА-Клиент»* изменение локальных установок обычно не требуется и управление *ПК «ЗАСТАВА-Клиент»* производится централизованно при помощи ЦУП (путем внесения изменений в ЛПБ).

	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 *ПК «ЗАСТАВА-Клиент»*

Для получения информации о *ПК «ЗАСТАВА-Клиент»* необходимо воспользоваться командой:

```
vpnconfig –ver.
```

Пример вывода команды `vpnconfig –ver`:

```
Product name: ZASTAVA Client
```

```
Vendor name: AO ELVIS-PLUS
Product build: 6.1.16122
Product release: 6.1
Build date: 2016/01/29 8:26
Product/platform information: CLIENT WINXX i386
```

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 *ПК «ЗАСТАВА-Клиент»*. Описание видов сертификатов и их параметров приведено в подразделе 3.4.

Предварительно распределенные ключи могут использоваться с *ПК «ЗАСТАВА-Клиент»* в качестве альтернативы использования сертификатов. Для получения более полной информации обращайтесь к п. 3.4.7.

ПК «ЗАСТАВА-Клиент» поддерживает СОС. Для получения более полной информации обращайтесь 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 надо выполнить команду `vpnconfig –list cert`. Затем выполнить команду `vpnconfig –view cert <id>`.

Будет выведена полная информация о свойствах сертификата, а также выведена его *цепочка доверия*, т. е. список 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 41).

Таблица 41 – Свойства сертификата

Свойство	Описание
Version	Версия 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.

Свойство	Описание
Sign Algorithm	Алгоритм цифровой подписи сертификата
Key Algorithm	Тип открытого ключа (алгоритм цифровой подписи и длина)
Public Key	Значение открытого ключа.
Valid From	Начальная дата действия сертификата
Valid To	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)	Хеш-сумма сертификата, вычисляемая по алгоритму md5.
Fingerprint (sha1)	Хеш-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 *ПК «ЗАСТАВА-Клиент»:* 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 *ПК «ЗАСТАВА-Клиент»* необходимо произвести следующие действия:

1) Выполнить команду `vpnconfig –list token` и найти в появившемся списке токен `Trusted Certificates token` и запоминить 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 *ПК «ЗАСТАВА-Клиент»* 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 бедующих 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 *ПК «ЗАСТАВА-Клиент»* необходимо сделать следующее:

1) Скопировать содержимое контейнера, содержащего закрытый ключ и сертификат, можно с помощью СКЗИ в реестр или на носитель.

2) *ПК «ЗАСТАВА-Клиент»* 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 послан Вам 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 *ПК «ЗАСТАВА-Клиент»* свяжитесь с администратором УЦ, чтобы сравнить сигнатуру (fingerprint) оригинального сертификата УЦ с сигнатурой полученного сертификата УЦ, которая отображается в полях «Fingerprint» в таблице сертификатов *ПК «ЗАСТАВА-Клиент»*. Если сигнатуры не совпадают, немедленно удалите сертификат из *ПК «ЗАСТАВА-Клиент»*.

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 *ПК «ЗАСТАВА-Клиент»* 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 *ПК «ЗАСТАВА-Клиент»*, закончился, данный сертификат будет автоматически удалён из *ПК «ЗАСТАВА-Клиент»* после проверки. Однако это не относится к локальным сертификатам (с закрытыми ключами). Поэтому удостоверьтесь 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 Ваши 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 *ПК «ЗАСТАВА-Клиент»* необходимо произвести следующие действия:

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

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

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

2) Если опции `file` и `inline` не использовались, то в консоли появится сообщение для ввода значение предварительно распределенного ключа вида `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 *ПК «ЗАСТАВА-Клиент»* 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, необходимо 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 *ПК «ЗАСТАВА-Клиент»* необходимо выполнить команду `vpnconfig -add cert <file>`.

Как только СОС будет успешно импортирован, все сертификаты, зарегистрированные в *ПК «ЗАСТАВА-Клиент»*, будут сверены с СОС. Если сертификат, который зарегистрирован в *ПК «ЗАСТАВА-Клиент»*, 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 *ПК «ЗАСТАВА-Клиент»*. 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 удалена, изменена и активирована. Во время активации ЛПБ необходимо ввести логин и пароль администратора.

5.3.4.2. Настройка параметров политик ПК «ЗАСТАВА-Клиент»

5.3.4.2.1. Системная ЛПБ

Системная политика может быть получена из файла, либо с сервера.

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:

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

   – 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`, либо указать значение `any` при использовании для соединения любого зарегистрированного локального сертификата;

      – `<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 *ПК «ЗАСТАВА-Клиент»* будет обращаться к заданному источнику всякий раз, когда политика активируется.

- `<log level>` – уровень журналирования событий.
- `<timeout>` – временной промежуток между обращениями к серверу.

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

Для активации политики необходимо воспользоваться командой `vpnconfig -login admin <admin login> <admin password> -activate lsp system [file <path>]` *или* `vpnconfig -login admin <admin login> <admin password> -activate lsp system [pmp <cert_id>]` *или* `vpnconfig -login admin <admin login> <admin password> -activate lsp system [pmp <key_id>]`.

5.3.4.2.2. Политика пользователя

Политика, используемая после входа пользователя в ОС. Политика пользователя может быть получена из файла или с сервера политик.

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

Для настройки *политики пользователя* необходимо:

- При выборе метода прогрузки из файла необходимо выполнить команду `vpnconfig -set lsp user file <path>`, где: `path` – путь к файлу конфигурации.
- При выборе метода прогрузки с сервера необходимо выполнить команду `vpnconfig -set lsp user pmp any|<cert_id> <id_type> <server_ip> [<log level>]`, где:
  - `cert_id`, идентификатор сертификата; для просмотра `id` сертификата можно воспользоваться командой `vpnconfig -list cert personal`, либо указать значение `any` при использовании для соединения любого зарегистрированного локального сертификата;
  - `<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 *ПК «ЗАСТАВА-Клиент»* будет обращаться к заданному источнику всякий раз, когда политика активируется;

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

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

Для настройки параметров политики и ее активации можно воспользоваться одной командой `vpnconfig -login admin <admin login> <admin password> -activate lsp user [file <path>]` или `vpnconfig -login admin <admin login> <admin password> -activate lsp user [pmp any|<cert_id>]`.

5.3.4.2.3. Политика драйвера по умолчанию

В *ПК «ЗАСТАВА-Клиент»* 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 -login admin <admin login> <admin password> -activate lsp 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 *ПК «ЗАСТАВА-Клиент»* 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».

5.3.4.2.4. Изменение 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|user cert any|<cert_id>`, где: `<cert_id>` - идентификатор сертификата. Для просмотра `<cert_id>` можно воспользоваться командой `vpnconfig -list cert personal`, либо указать значение `any` при использовании для соединения любого зарегистрированного локального сертификата.

Для изменения предварительно распределенного ключа, с помощью которого будет устанавливаться соединение с сервером политики, нужно выполнить команду `vpnconfig -set lsp system key any|<key_id>`, где: `<key_id>` – идентификатор предварительно распределенного ключа. Для просмотра `<key_id>` можно воспользоваться командой `vpnconfig -list cert preshared`, либо указать значение `any` при использовании для соединения любого зарегистрированного ключа.

5.3.4.2.5. 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|user loglevel <log level>`, где: `<log level>` – уровень регистрации событий при передаче ЛПБ с сервера политики.

5.3.4.2.6. 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>`.

5.3.4.2.7. 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|user server <server_ip>`.

После регистрации ЛПБ *ПК «ЗАСТАВА-Клиент»* 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 `тип`, который содержится в выводе команды `vpnconfig –list lsp`. После этого необходимо указать логин и пароль администратора, выполнив команду `vpnconfig -login admin <admin login> <admin password> -activate lsp system`. 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 42).

Таблица 42 – Параметры команды `vpnconfig –set log`

Числовой параметр	Описание	Расшифровка
0	Log Level	Уровень регистрации событий
1	Log Level kernel	Уровень регистрации событий уровня ядра
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
13	Broadcast messages to terminals from vpndmn	Широковещательные сообщения терминалам от службы *ПК «ЗАСТАВА-Клиент»*
14	Verbose mode for application level	Установить отладочный уровень регистрации событий для уровня приложения

Числовой параметр	Описание	Расшифровка
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 *ПК «ЗАСТАВА-Клиент»*. Уровень регистрации событий может быть установлен командой `vpnconfig -set log 0 (Log Level)`, где `Log Level` может принимать значения `<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):

- Журнал отключен (Disabled) – События не будут регистрироваться;
- События (Event) – Будет регистрироваться минимальное количество информации об операциях, а также все сообщения об ошибках;
- Детальный (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 *ПК «ЗАСТАВА-Клиент»*. В этом случае установки из ЛПБ будут иметь преимущество перед локальными установками. Вы можете посмотреть текущий реальный уровень регистрации событий, выполнив команду `vpnconfig -list log`, в выводе этой команды будет содержаться вся информация о настройках системы регистрации событий *ПК «ЗАСТАВА-Клиент»*.

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 *ПК «ЗАСТАВА-Клиент»*.

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 Client\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" <value>`. 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 *ПК «ЗАСТАВА-Клиент»*

5.3.5.2. Параметры журнала Syslog

ПК «ЗАСТАВА-Клиент» 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 необходимо отредактировать файл `/etc/syslog.conf`, добавив строку вида:

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

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

`<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 протокола 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 43).

Таблица 43 – 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 (sec)	Укороченное время для завершения обмена (3-60, по умолчанию 5)

Номер параметра	Параметр	Расшифровка
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 дальнейшие действия зависят от версии протокола IKE. Для IKEv1 любой новый запрос игнорируется. Для IKEv2 любой новый запрос также игнорируется, но при этом запускается процедура подтверждения IP-адреса. Эта процедура заключается в отправке инициатору специального значения – COOKIE, которое тот должен вернуть. 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
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)

Номер параметра	Параметр	Расшифровка
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)
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	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)
22	IKE-CFG configure DNS servers	Параметр, регулирующий режимы обработки IKE-CFG. При установлении SA, на интерфейсе, через который оно установлено, прописывается DNS-сервер в зависимости от настроек: — Выключено – используется системный DNS. DNS, указанный в политике, не используется; — Включено – используется DNS, указанный в политике, системный DNS не используется; — Включено, применять до системных (используется по умолчанию) – используется DNS, указанный в политике, и он применяется в первую очередь; — Включено, применять после системных – DNS, указанный в политике, используется после неудачной попытки использования системного DNS. После разрыва SA соответствующая запись о DNS-сервере удаляется.

Номер параметра	Параметр	Расшифровка
23	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 *ПК «ЗАСТАВА-Клиент»* в *ЗАСТАВА-Управление*.

5.3.6.1.1. Политика выбора метода работы через NAT

Управление политикой выбора метода работы через NAT осуществляется из локальных настроек *ПК «ЗАСТАВА-Клиент»*. В зависимости от выбранного числового значения параметра с id = ike_nat_t_policy политика может быть следующей (см. Таблица 44).

Таблица 44 – 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)	Будучи инициатором, предлагаются все варианты UDP-инкапсуляции, кроме метода Huttunen, будучи респондентом приоритетным считается метод Стандарт.
2 (Все методы)	Использовать все методы. Будучи инициатором, предлагаются все варианты UDP-инкапсуляции, будучи респондентом приоритетным считается метод Стандарт.
3 (Huttunen)	Этот метод делает вариант Huttunen более приоритетным. Будучи инициатором, *Агент* предлагает только его. Будучи респондером метод Huttunen считается более приоритетным (но не единственно возможным).
4 (Автовыбор)	Этот режим устанавливается по умолчанию после установки *Агента*. 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	Режим Huttunen с принудительной инкапсуляцией. Полностью аналогичен

Числовое значение	Политика
(Принудительно))	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.

5.3.6.1.2. Описание режимов обработки CRL

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

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

Для изменения значения этого параметра с помощью утилиты командной строки нужно выполнить команду: `vpnconfig -s ike crl_processing <id-parameter>`. В зависимости от выбранного значения id-parameter, обработка CRL будет производиться в режимах, приведенных в Таблице 45.

Таблица 45 – 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,

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

5.3.7. Токены

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

5.3.7.1. Просмотр Модулей токенов

Для просмотра всех зарегистрированных Модулей токенов необходимо выполнить команду `vpnconfig –list provider`. Вывод результата выполнения данной команды будет содержать информацию о 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
```

5.3.7.2. Добавление Модулей токенов

Для регистрации модуля PKCS#11 в *ПК «ЗАСТАВА-Клиент»* 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.

5.3.7.3. Удаление Модуля токена

Чтобы удалить модуль PKCS#11 из *ПК «ЗАСТАВА-Клиент»* необходимо определить его Имя (Name), для этого воспользуйтесь командой `vpnconfig –list provider`.

Для удаления Модуля токена следует выполнить команду:

`vpnconfig –remove provider <name>`.

5.3.8. Работа с токенами

5.3.8.1. 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
```

5.3.8.2. 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. 5.3.8.1);

`<pin>` – PIN-код токена;

`[save]` – необязательный параметр, если его не установить, то *ПК «ЗАСТАВА-Клиент»* 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>`.

5.3.8.3. 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 *ПК «ЗАСТАВА-Клиент»*.

5.3.9. 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 IKE приведены в таблице (см. Таблица 46).

Таблица 46 – 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	Settings	Метод конфигурирования обновлений Возможные значения: 13 Disable - Отключить автообновление – автоматические обновления отключены. 14 LSP - Локальная политика безопасности – конфигурирование обновлений выполняется централизованно, через *ЗАСТАВА-Управление* (параметры будут считываться *Агентом* из ЛПБ).

Номер параметра	Параметр	Расшифровка
		15 Manual Settings - 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.
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 *ПК «ЗАСТАВА-Клиент»*. 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 *ПК «ЗАСТАВА-Клиент»* как отдельный модуль (плагин). По умолчанию в состав *ПК «ЗАСТАВА-Клиент»* 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 47).

Таблица 47 – 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 48).

Таблица 48 – 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 49).

Таблица 49 – 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 в 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. Конфигурирование модуля токенов

Существует возможность конфигурировать поведение Softtoken common с помощью конфигурационного файла pkcs11.cfg. Файл pkcs11.cfg расположен в директории /var/vpnagent (для ОС Linux) или в главной директории *Агента* (для ОС Windows).

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» (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 2. Конфигурирование модуля vpnpcap

Существует возможность конфигурировать поведение модуля vpnpcap в ОС Linux с помощью задания параметров:

- filth_max_count - размер хеш-таблицы фильтров (по умолчанию 8192). Хеш-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 3. КОНФИГУРИРОВАНИЕ МОДУЛЯ CP_PLG_CPRO

Для конфигурирования модуля cp_plg_cpro-36r2 используется параметр max_handles. Параметр Max_handles - максимальное количество хэндлов КриптоПро, 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/vpnclient stop;
  - /sbin/rmmod cp_plg_cpro36;
  - /sbin/modprobe cp_plg_cpro-36r2 max_handles=120000;
  - /etc/init.d/vpnclient start.
- в ОС Windows:
  - Задать в реестре (HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\vpnpcap\Parameters) пользовательский параметр MaxHandles, тип = DWORD. После задания параметра необходимо перезапустить сервис «VPN Service for Windows».

Аналогичные операции необходимо выполнить для настройки модуля cp_plg_cpro-36r3 и cp_plg_cpro-40.

Приложение 4. 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 «ПК «ЗАСТАВА-Клиент»» запустить «КриптоПро CSP» от имени администратора, перейти во вкладку «Оборудование» и выбрать пункт «Настроить ДСЧ»

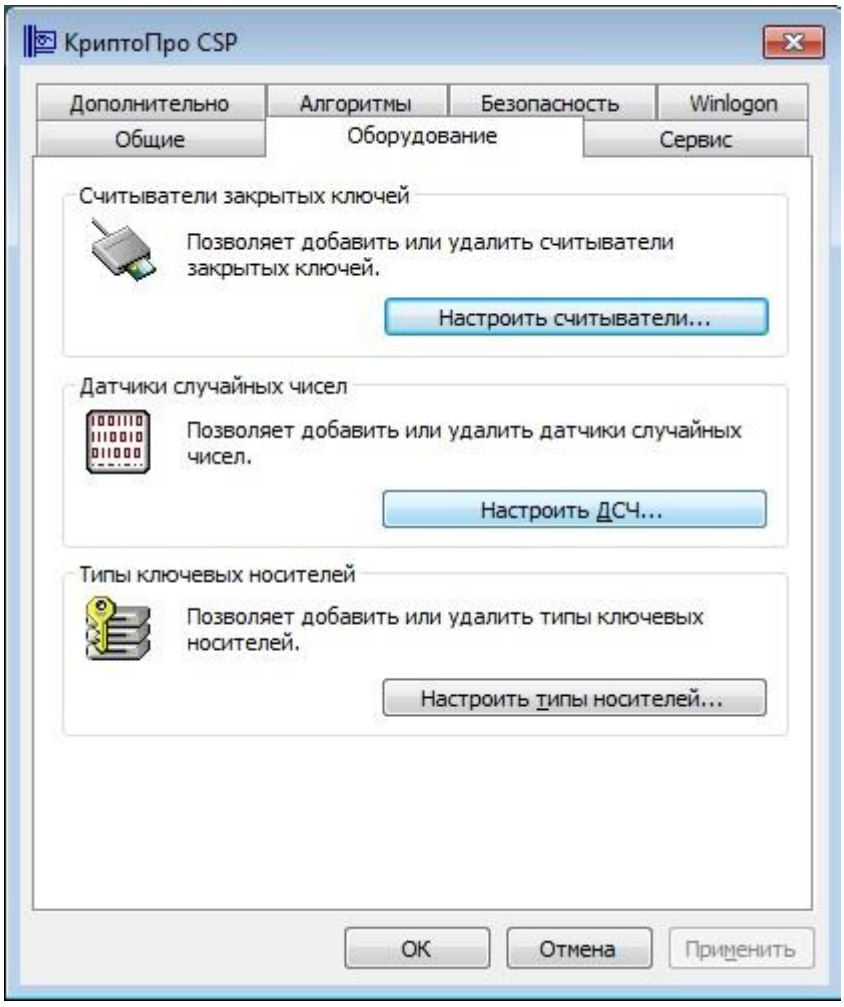

Рисунок 56 – «КриптоПро CSP» закладка Оборудование

3) В появившемся окне выбрать «Добавить»

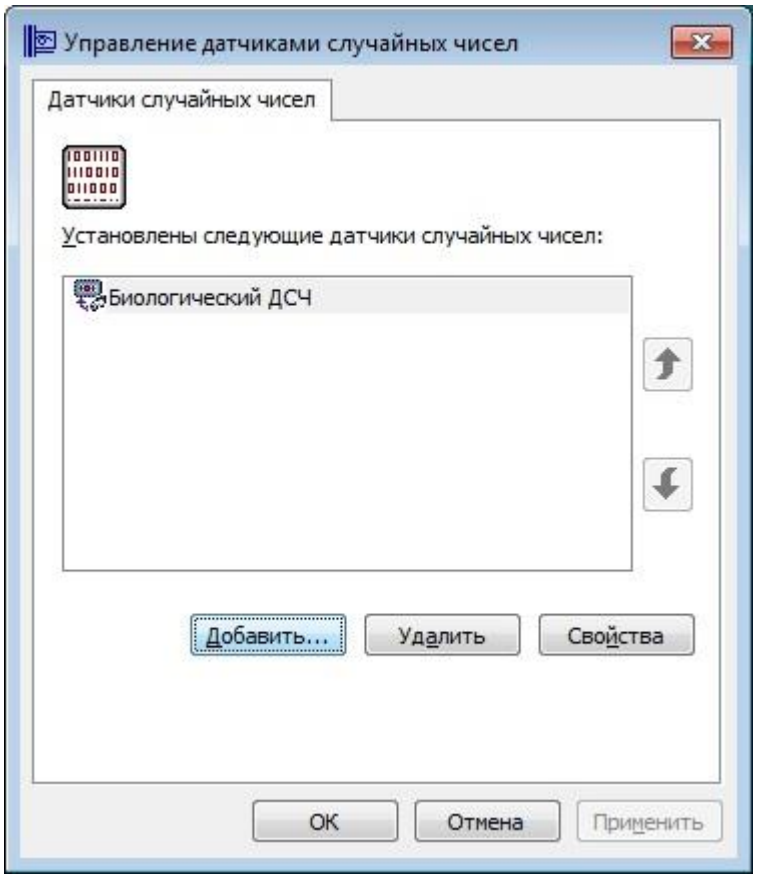

Рисунок 57 – «КриптоПро CSP» Управление датчиками случайных чисел

4) В запустившемся мастере установки ДСЧ нажать «Далее»

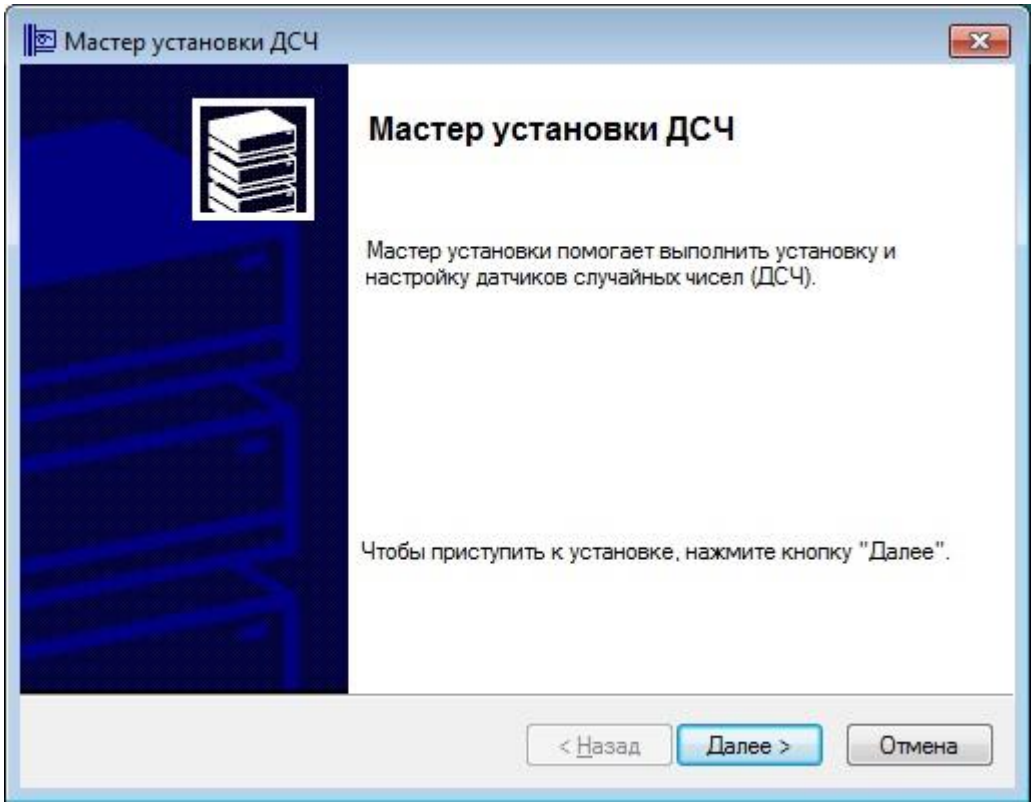

Рисунок 58 – «КриптоПро CSP» Запуск мастера установки ДСЧ

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

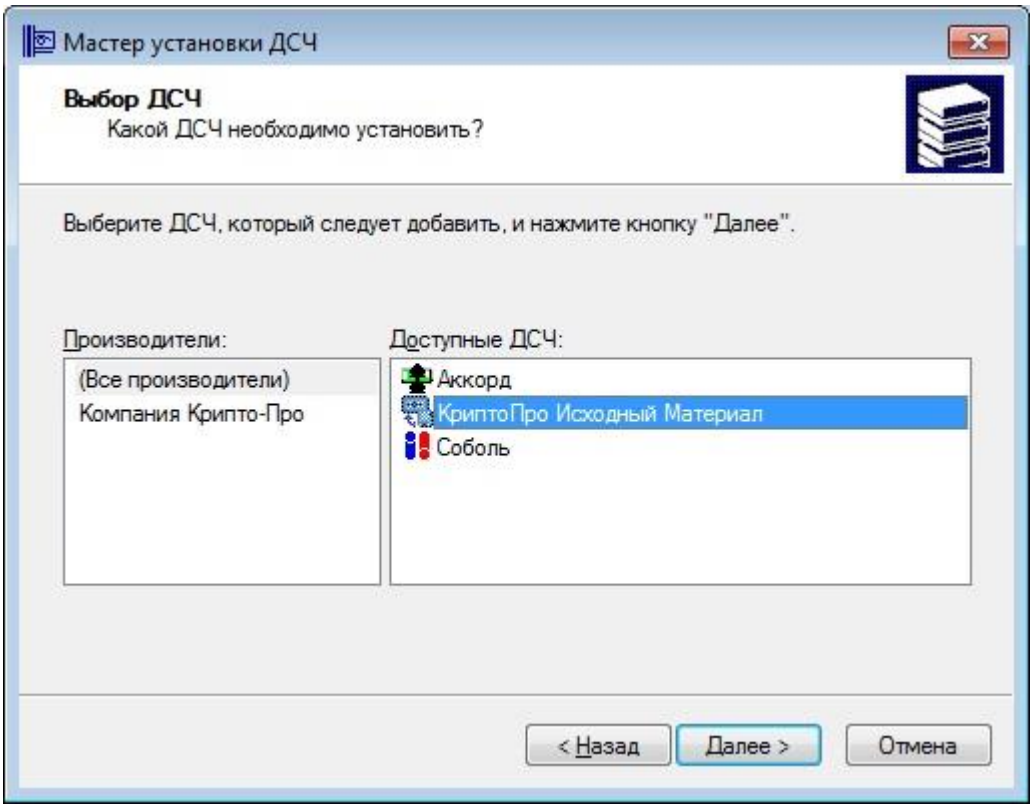

Рисунок 59 – «КриптоПро CSP» Выбор ДСЧ

6) Ввести имя ДСЧ, нажать «Далее»

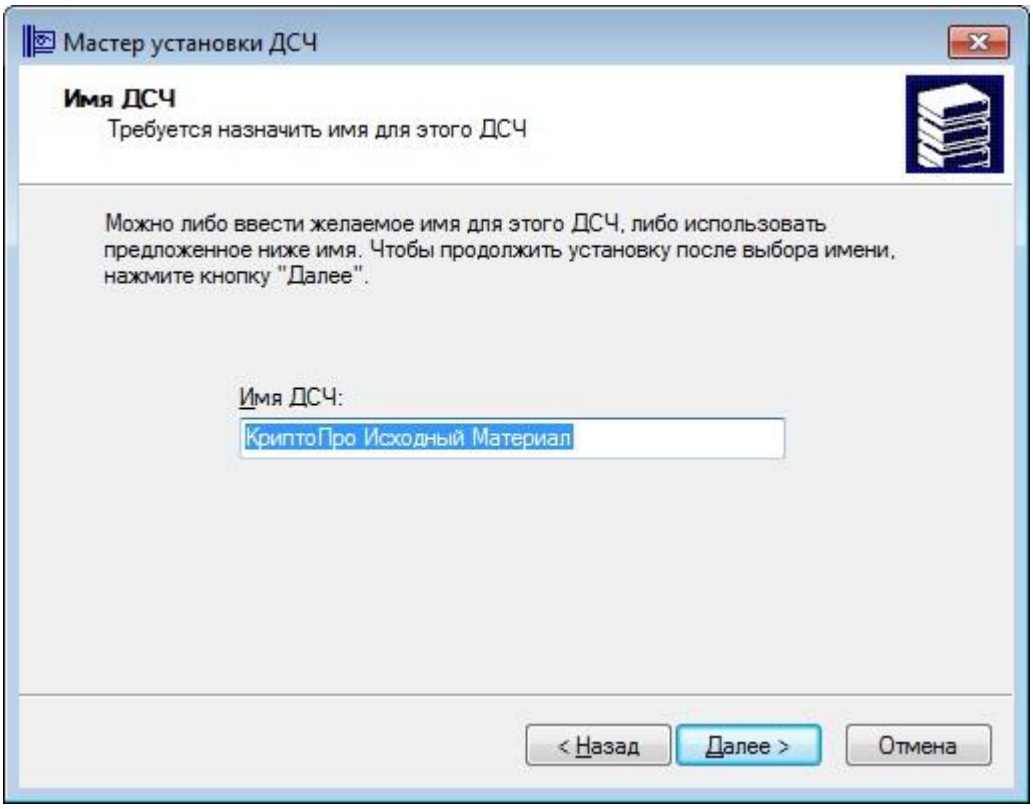

Рисунок 60 – «КриптоПро CSP» Ввод имени ДСЧ

7) Указать путь к папкам, где находятся папки db

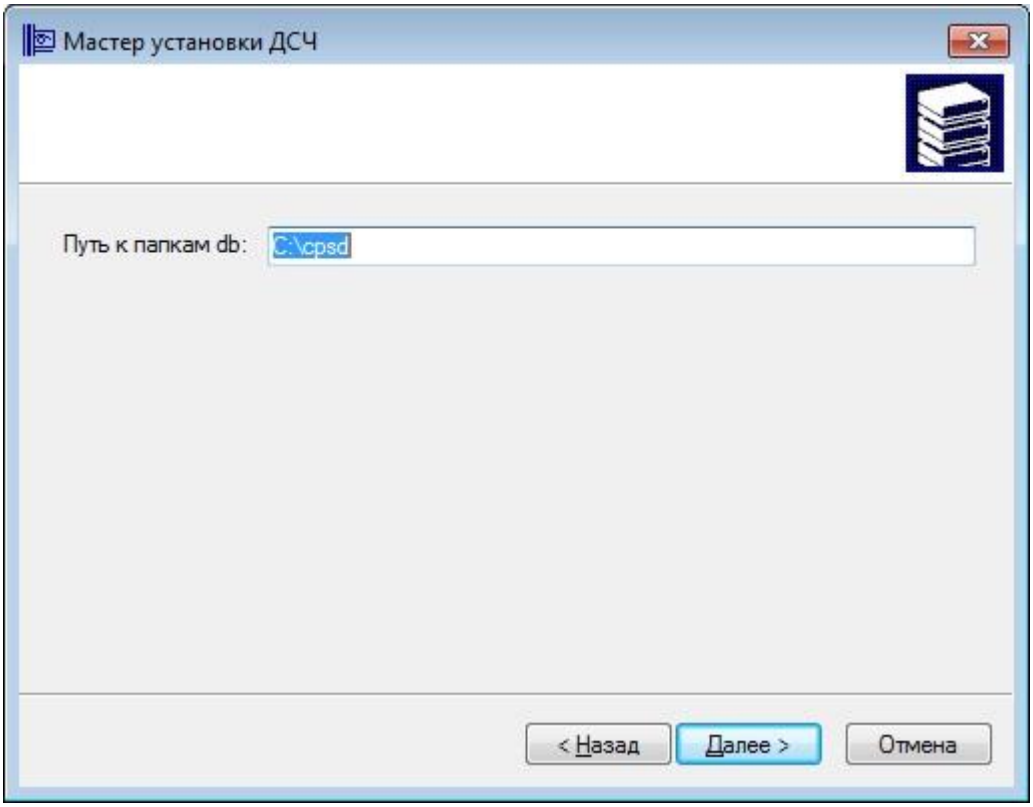

Рисунок 61 – «КриптоПро CSP» Указание путик папке

8) Нажать «Готово», перезагрузить компьютер

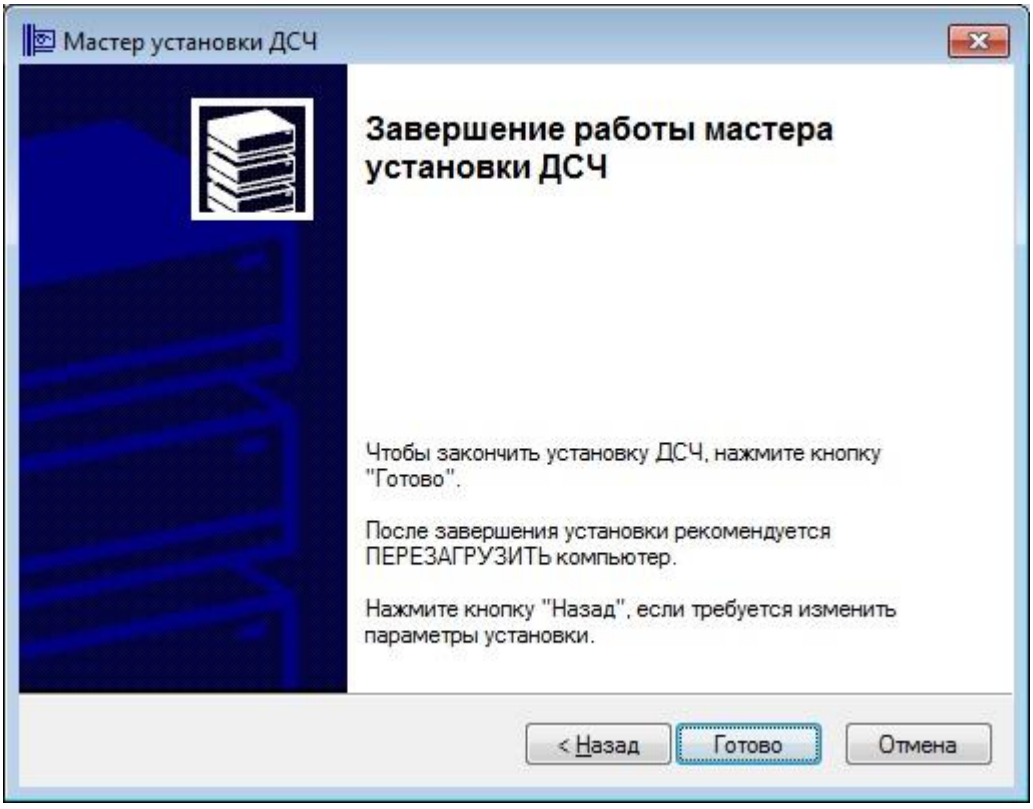

Рисунок 62 – «КриптоПро CSP» Завершение работы мастера ДСЧ

9) Убедиться, что после перезагрузки компьютера в журнале «ПК «ЗАСТАВА-Клиент»» 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 5. Устранение неисправностей

п/н	Описание неисправностей	Решение
1	Конфигурирование «КриптоПро CSP». 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 КриптоПро */opt/cprocsp/bin/<arch>/csptest -keys -verifycontext :* показать версию «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 ПК «VPN/FW «ЗАСТАВА», версия 6. Некоторые (в основном, англоязычные) сокращения и термины употребляются только во внутренних идентификаторах программ и приведены здесь для справки.

Агент – собирательное название для линейки управляемых агентов безопасности (компонент «*ПК «ЗАСТАВА-Клиент»*», версия 6,компонент *«ЗАСТАВА-Офис»*, версия 6)

БД – база данных

ВЧС - виртуальная частная сеть

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

ЗРС - Запрос Регистрации Сертификата

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

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 IPsecGMT - 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

NMS (Network Management System) - система управления и мониторинга сети (обычно на основе протокола SNMP)

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 ПК «VPN/FW «ЗАСТАВА», версия 6)

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.00627 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-Офис», версия 6 КС1» («VPN/FW «ЗАСТАВА-Офис», версия 6 КС1») (исполнения: ZO6-L32-VF-01, ZO6-L64-VF-01). Руководство системного программиста».

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

[3] МКЕЮ.00626-01 91 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») (исполнения: ZC6-WX64-VF-01, ZC6-L32-VF-01, ZC6-L64-VF-01). Правила пользования».

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					