УТВЕРЖДЕН
МКЕЮ.00689-01 32 01-ЛУ

ПРОГРАММНО-АППАРАТНЫЙ КОМПЛЕКС «VPN/FW «ЗАСТАВА-КЛИЕНТ», ВЕРСИЯ 8 КС3» (ИСПОЛНЕНИЕ ZC8-AS64-VF-03)

РУКОВОДСТВО СИСТЕМНОГО ПРОГРАММИСТА

МКЕЮ.00689-01 32 01

Листов 107

Инв. №подл.	Подп. и дата	Взам. инв. №	Инв. №дубл.	Подп. и дата
10099				

2025

АННОТАЦИЯ

Документ МКЕЮ.00689-01 32 01 «Программно-аппаратный комплекс «VPN/FW «ЗАСТАВА-Клиент», версия 8 КС3» (исполнение ZC8-AS64-VF-03). Руководство системного программиста» содержит инструкции для работы пользователя с правами учётной записи администратора (далее – администратор) с программно-аппаратным комплексом «VPN/FW «ЗАСТАВА-Клиент», версия 8 КС3» (исполнение ZC8-AS64-VF-03) (далее – ПАК «ЗАСТАВА-Клиент»).

В документе приведены перечень доступных пользователю функций, описание графического интерфейса ПАК «ЗАСТАВА-Клиент» и принципов безопасной работы с ним, указаны параметры безопасности с указанием безопасных значений, а также описание режимов работы и действий пользователя при возникновении нештатных ситуаций.

СОДЕРЖАНИЕ

1. ОБЩИЕ СВЕДЕНИЯ

1.1. Назначение

ПАК «ЗАСТАВА-Клиент» предназначен для защиты и фильтрации входящего и исходящего трафика на средстве вычислительной техники (СВТ) пользователя. ПАК «ЗАСТАВА-Клиент» обеспечивает контроль и фильтрацию сетевого трафика, взаимную криптографическую защиту абонентов при установлении соединения, шифрование и контроль целостности IP-пакетов в корпоративной информационной системе.

ПАК «ЗАСТАВА-Клиент» предоставляет следующие возможности по защите и фильтрации трафика:

- фильтрация сетевого трафика для отправителей и получателей данных и всех операций перемещения контролируемой ПАК «ЗАСТАВА-Клиент» информации к узлам информационной системы и от них;
- осуществление фильтрации, основанной на следующих типах атрибутов безопасности субъектов: сетевой адрес узла отправителя, сетевой адрес узла получателя;
- фильтрация, основанная на следующих типах атрибутов безопасности информации: сетевой протокол, который используется для взаимодействия; транспортный протокол, который используется для взаимодействия, порты источника и получателя в рамках сеанса (сессии); разрешенные (запрещенные) команды, разрешенный (запрещенный) мобильный код; разрешенные (запрещенные) протоколы прикладного уровня;
- разрешение или запрет информационного потока в соответствии с установленными администратором ПАК «ЗАСТАВА-Клиент» наборе правил фильтрации, основанном на идентифицированных атрибутах;
- осуществление политики фильтрации пакетов с учетом управляющих команд от взаимодействующих с ПАК «ЗАСТАВА-Клиент» средств защиты информации (СЗИ) перечень которых приведён в приложении (см. Приложение 1);
- проверка каждого пакета на соответствие таблице состояний (статус, тип);
- проверка использования сетевых ресурсов, содержащих мобильный код, для которого администратором ПАК «ЗАСТАВА-Клиент» установлены разрешительные или запретительные атрибуты безопасности;
- разрешение или запрет информационного потока на основании результатов проверок;
- фильтрация пакетов с учетом управляющих команд от взаимодействующих с ПАК «ЗАСТАВА-Клиент» СЗИ других видов, основанную на атрибутах, указывающих на признаки нарушения безопасности в информации сетевого трафика;

— разрешение информационного потока, если значения атрибутов безопасности, установленные взаимодействующими СЗИ для контролируемого сетевого трафика, указывают на отсутствие нарушений безопасности информации;
— запрет информационного потока, если значения атрибутов безопасности, установленные взаимодействующими СЗИ для контролируемого сетевого трафика, указывают на наличие нарушений безопасности информации.

ПАК «ЗАСТАВА-Клиент» обеспечивает защиту информации конфиденциального характера, не содержащей сведений, составляющих государственную тайну: сведений для служебного пользования, персональных данных, сведений, составляющих коммерческую, банковскую тайну и других видов конфиденциальной информации.

Использование ПАК «ЗАСТАВА-Клиент» позволяет осуществлять защищенное сетевое взаимодействие с агентами в информационно-телекоммуникационной сети. Агентом для ПАК «ЗАСТАВА-Клиент» являются:

— СВТ с установленным программными изделиями «ЗАСТАВА-Офис», перечень которых приведён в приложении (см. Приложение 1);
— аппаратно-программными комплексами линейки «ЗАСТАВА», перечень которых приведён в приложении (см. Приложение 1).

ПАК «ЗАСТАВА-Клиент» является, согласно действующим нормативным правовым актам Российской Федерации, средством криптографической защиты информации (СКЗИ).

1.2. Системные требования

1.2.1. Требования к аппаратному обеспечению

Аппаратное обеспечение СВТ, на котором устанавливается ПАК «ЗАСТАВА-Клиент», должно отвечать минимальным требованиям, представленным в таблице (см. Таблица 1).

Таблица 1 – Требования к аппаратному обеспечению исполнений ПАК «ЗАСТАВА-Клиент»

Исполнение	Требования к аппаратному обеспечению
ZC8-AS64-VF-03	– процессор Intel N100; – 1 ГБ оперативной памяти; – 1 ГБ свободного дискового пространства; – наличие сетевого интерфейса Ethernet; – наличие устройства для чтения компакт-дисков; – аппаратно-программный модуль доверенной загрузки (АПМДЗ), сертифицированный в установленном порядке

1.2.2. Требования к программному обеспечению

На СВТ, на котором устанавливается ПАК «ЗАСТАВА-Клиент», должна быть установлена операционная система (ОС), указанная в таблице (см. Таблица 2).

Таблица 2 – ОС, поддерживаемые исполнениями ПАК «ЗАСТАВА-Клиент»

Исполнение	Поддерживаемая ОС
ZC8-AS64-VF-03	ОС Astra Linux Special Edition 1.7

В случае наличия на СВТ установленных антивирусных программных средств необходимо добавление vpndmn в список доверенных программ.

1.2.3. Ключевой носитель

В качестве носителей ключевой информации для ПАК должны использоваться сертифицированные ФСБ России (персональные идентификаторы) функциональные ключевые носители (ФКН):

- RU.63793390.00003-01 ESMART Token ГОСТ;
- КБДЖ.01558 Рутокен 3.0.

Использование совместно с ПАК «ЗАСТАВА-Клиент» носителей ключевой информации, не рекомендованных эксплуатационной документацией к ПАК «ЗАСТАВА-Клиент» или не имеющих действующего заключения ФСБ России, запрещается!

1.3. Ролевая модель

Ролевая модель ПАК «ЗАСТАВА-Клиент» приведена в таблице (см. Таблица 3).

Таблица 3 - Ролевая модель ПАК «ЗАСТАВА-Клиент»

Роль	Описание
Оператор[1)]	Локальный непривилегированный пользователь, имеющий непосредственный доступ к СВТ с установленным ПАК «ЗАСТАВА-Клиент», осуществляющий функции мониторинга, включая: – просмотр локального журнала аудита; – просмотр настроек ПАК «ЗАСТАВА-Клиент»; – просмотр таблицы состояния активных соединений
Администратор безопасности СКЗИ	Локальный привилегированный пользователь, имеющий непосредственный доступ к СВТ с установленным ПАК «ЗАСТАВА-Клиент» и осуществляющий: – настройку СВТ и функционал СКЗИ; – ввод и смену криптографических ключей; – проведение периодических регламентных работ и технического обслуживания СВТ и СКЗИ
Удалённый администратор	Удалённый привилегированный пользователь, имеющий доступ к СВТ с установленным ПАК «ЗАСТАВА-Клиент» посредством подключения к СВТ по защищённому каналу связи и осуществляющий: – формирование, доставку и активацию локальной политики безопасности (ЛПБ) СКЗИ; – формирование и доставку данных, необходимых для обновления ПАК «ЗАСТАВА-Клиент»; – формирование и доставку команд на смену действующих ключевой пары СКЗИ и соответствующего им цифрового сертификата; – проведение периодического удалённого мониторинга состояния СКЗИ, просмотра локальных журналов регистрации системных событий ПАК «ЗАСТАВА-Клиент» и тестирования их работоспособности
[1)] Описание принципов работы пользователя с правами учётной записи оператора с ПАК «ЗАСТАВА-Клиент» приведено в документе МКЕЮ.00689-01 34 01 «Программно-аппаратный компелекс «VPN/FW «ЗАСТАВА-Клиент», версия 8 КС3». Руководство оператора».	

1.4. Процедура приемки ПАК «ЗАСТАВА-Клиент»

Описание действий при получении ПАК «ЗАСТАВА-Клиент» эксплуатирующей организацией приведено в документе МКЕЮ.00689-01 30 01 «Программно-аппаратный комплекс «VPN/FW «ЗАСТАВА-Клиент», версия 8 КС3». Формуляр».

После выполнения приёмки необходимо выполнить подготовку ПАК «ЗАСТАВА-Клиент» к использованию в соответствии с указаниями раздела 3.

2. СПЕЦИАЛЬНЫЕ СВЕДЕНИЯ

2.1. Меры безопасности для среды информационных технологий

Для того чтобы ПАК «ЗАСТАВА-Клиент» выполняло все заявленные функции по защите информации от несанкционированного доступа (НСД) из внешней сети, необходимы организационно-распорядительные и технические меры, приведенные в документе МКЕЮ.00689-01 30 01 «Программно-аппаратный комплекс «VPN/FW «ЗАСТАВА-Клиент», версия 8 КС3». Формуляр».

2.2. Интерфейсы взаимодействия с функциями безопасности

В ПАК «ЗАСТАВА-Клиент» реализованы следующие интерфейсы взаимодействия с функциями безопасности:

- графический пользовательский интерфейс, предоставляющий механизм взаимодействия с подсистемами аудита, контроля доступа, управления безопасностью, защиты функций безопасности и подсистемой сигнализации о нарушении безопасности;
- интерфейс командной строки, предоставляющий механизм взаимодействия с подсистемами управления безопасностью и контроля доступа;
- интерфейс взаимодействия с ПО «ЗАСТАВА-Управление», предоставляющий механизм взаимодействия с подсистемой управления безопасностью.

2.3. Описание мер безопасности для среды функционирования

Для того чтобы ПАК «ЗАСТАВА-Клиент» выполняло все заявленные функции по защите информации от НСД из внешней сети, необходимо выполнение следующих организационно-распорядительных и технических мер, применимых к среде функционирования (ПО «ЗАСТАВА-Управление»):

- при задании политики безопасности по умолчанию использовать параметры «Блокировать все», «Блокировать все, включая предназначенное другим»;
- при задании правил межсетевого экранирования должны использоваться следующие уровни журналирования: «События», «Подробный», «Отладочный».

2.4. Принципы безопасной работы с интерфейсами взаимодействия

Администратор имеет доступ к интерфейсу командной строки.

Администратору рекомендуется обеспечивать следующие меры безопасности при работе с интерфейсом локальной консоли:

- запрет на установку уровня журналирования, равного «Disabled», для параметров журналирования «Log Level» и «Log Level kernel» в ПАК «ЗАСТАВА-Клиент»;

- запрет на установку уровня журналирования, равного «Disabled», при получении политики от программных изделий «ЗАСТАВА-Управление», перечень которых приведён в приложении (см. Приложение 1);
- запрет на отключение системного журнала ПАК «ЗАСТАВА-Клиент»;
- запрет на установку политики безопасности, полученную из файла;
- запрет на установку «Политики драйвера по умолчанию» в значение «Pass»;
- выполнять выход из учётной записи по завершении работы с ПАК «ЗАСТАВА-Клиент».

Необходимо устанавливать параметр «Политика драйвера по умолчанию» в значение «Сбрасывать все» (`dropall`). Необходимо учесть, что в этом случае сеть не будет доступна, если СВТ не присвоен статический IP-адрес. Если СВТ получает IP-адрес по DHCP, то нужно 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 СВТ IP-адреса).

Администратору ПАК «ЗАСТАВА-Клиент» рекомендуется обеспечивать запрет передачи политик безопасности по открытому каналу связи при работе с интерфейсом взаимодействия с ПО «ЗАСТАВА-Управление».

2.5. Описание доступных для администратора функций и интерфейсов с указанием безопасных значений

Меры по обеспечению безопасной работы со средой функционирования приведены в подразделе 2.3.

Описание доступных для администратора функций ПАК «ЗАСТАВА-Клиент» приведено в разделах 4 и 5.

Администратор ПАК «ЗАСТАВА-Клиент» обязан использовать только безопасные значения при задании политики безопасности для ПАК «ЗАСТАВА-Клиент». Безопасными значениями являются:

- при задании политики драйвера по умолчанию (DDP) – использование параметров «Сбрасывать все, кроме DHCP» («DROP»), «Сбрасывать все» («DROP ALL»);
- при задании получения политики безопасности с ПО «ЗАСТАВА-Управление» должны использоваться следующие уровни журналирования: «Отключен», «События», «Подробный», «Отладочный»;

При задании настроек политики безопасности в ПО «ЗАСТАВА-Управление» администратор обязан руководствоваться следующими безопасными значениями:

- при задании политики безопасности по умолчанию – использовать параметры «Блокировать все», «Блокировать все, включая предназначенное другим»;
- при задании правил межсетевого экранирования должны использоваться следующие уровни журналирования: «События», «Подробный», «Отладочный».

2.6. Типы событий, имеющих значение для безопасности

Перечень событий, имеющих значение для безопасности ПАК «ЗАСТАВА-Клиент», приведён в таблице (см. Таблица 4).

Таблица 4 - Перечень событий, имеющих значение для безопасности

Событие	Условия возникновения события
Вход в ПАК «ЗАСТАВА-Клиент» с использованием корректных данных	Ввод правильных логина, пароля, а также ПИН-кода персонального идентификатора администратора ПАК «ЗАСТАВА-Клиент»
Выход из ПАК «ЗАСТАВА-Клиент»	Выполнение команды `logout`
Попытка входа в ПАК «ЗАСТАВА-Клиент» с использованием некорректных данных	Ввод неправильных логина, пароля или ПИН-кода персонального идентификатора администратора ПАК «ЗАСТАВА-Клиент», либо попытка входа с использованием некорректного идентификатора
Изменение параметров безопасности и управление настройками	Изменение уровня журналирования событий при изменении способа задания ЛПБ
Запуск программ и порождение процессов, относящихся ПАК «ЗАСТАВА-Клиент»	Перезапуск или запуск модулей, относящихся к ПАК «ЗАСТАВА-Клиент»
Очистка журнала ПАК «ЗАСТАВА-Клиент»	Очистка журнала при помощи команды `vpnconfig clear log` или в графическом интерфейсе во вкладке «Журнал»
Активация ЛПБ	Событие возникает, когда указанная политика безопасности распознается без ошибок (в случае задания политики из файла) и успешно доставляется и прогружается (в случае получения политики от центра управления политиками (ЦУП)
Выполнение процедуры контроля целостности	Событие возникает при использовании утилиты icv_checker, а также при старте ПАК «ЗАСТАВА-Клиент»

2.7. Режимы функционирования

ПАК «ЗАСТАВА-Клиент» имеет следующие режимы функционирования:

— аварийный режим;

— штатный режим.

ПАК «ЗАСТАВА-Клиент» работает в штатном режиме, когда указанная политика безопасности распознается без ошибок (в случае задания политики из файла) и успешно доставляется и прогружается (в случае получения политики от ЦУП).

ПАК «ЗАСТАВА-Клиент» поддерживает возможность перехода в режим аварийной поддержки, который предоставляет возможность возврата к штатному режиму функционирования. Процесс восстановления работы ПАК «ЗАСТАВА-Клиент» приведён в подразделе 3.1.4.

3. ПОДГОТОВКА К ИСПОЛЬЗОВАНИЮ ПАК «ЗАСТАВА-КЛИЕНТ»

Перед началом установки ПАК «ЗАСТАВА-Клиент» необходимо убедиться в том, что на СВТ установлена ОС, поддерживаемая устанавливаемым дистрибутивом ПАК «ЗАСТАВА-Клиент». Перечень поддерживаемых ОС приведён в подразделе 1.2.

	Чтобы инсталлировать и деинсталлировать ПАК «ЗАСТАВА-Клиент», пользователь должен иметь привилегии администратора ОС.
	Необходимо удостовериться в том, что на СВТ правильно установлены дата, время и настройки часового пояса, иначе может оказаться, что срок действия сертификатов истек, и установить ПАК «ЗАСТАВА-Клиент» невозможно.
	Длина пароля администратора ОС, на которой устанавливается ПАК «ЗАСТАВА-Клиент», должна быть не меньше восьми буквенно-цифровых символов.
	Служба удаленного доступа должна быть отключена (удаленный помощник, удаленный рабочий стол) (для ОС семейства Windows).
	В ЛПБ должен быть включен параметр Сервер сети Microsoft: использовать цифровую подпись (всегда) (для ОС семейства Windows).

3.1. ОС семейства Linux

3.1.1. Установка ПАК «ЗАСТАВА-Клиент»

Инсталляция ПАК «ЗАСТАВА-Клиент» на ОС Astra Linux Special Edition 1.7 запускается командой:

```
dpkg –i <путь к инсталляционному пакету ZASTAVAclient формата deb>
```

Данные сообщения выводятся, т.к. при установке плагины, входящие в состав ПАК «ЗАСТАВА-Клиент», инсталлируются последовательно. На те алгоритмы, которые уже включены в плагин, выдается предупреждение.

	После установки ПАК «ЗАСТАВА-Клиент» необходимо выполнить команды от имени суперпользователя root:
	`systemctl enable vpnclient_pcap`
	`systemctl enable vpnclient`
	и выполнить перезагрузку.

3.1.2. Удаление ПАК «ЗАСТАВА-Клиент»

Деинсталляция ПАК «ЗАСТАВА-Клиент» для ОС Astra Linux Special Edition 1.7 запускается командой:

```
dpkg -r ZASTAVAclient
```

3.1.3. Интеграция ПАК «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 необходимо:

1) определить путь к файлу «snmpd.conf». Например, «/etc/snmp/snmpd.conf». Если файла нет, необходимо его создать (обратитесь к документации по snmpd);
2) в конец файла «snmpd.conf» добавить строку, выполнив команду:

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

3) дать команду «snmpd» для подгрузки модуля расширения:

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

3.1.4. Настройка динамического контроля целостности

Для ПАК «ЗАСТАВА-Клиент» в исполнении ZC8-AS64-VF-03 должен быть настроен динамический контроль целостности путём выпонения задания периодической проверки в соответствии с настроенным сценарием проверки.

Для создания сценария периодической проверки выполнить шаги:

1) в программе эмулятора терминала выполнить авторизацию с использованием данных учётной записи с правами суперпользователя (root);
2) создать сценарий периодической проверки, выполнив команду:

```
vim.tiny /usr/sbin/regular_check_control_sum.sh
```

3) добавить в файл текст:

```
#!/bin/sh
if /opt/ZASTAVAclient/bin/icv_checker
/opt/ZASTAVAclient/bin/filelist.hash > /var/log/skzi_exist_checksum;
then
        echo -en "Динамический контроль СКЗИ пройден успешно " |
systemd-cat -t ZASTAVA
else
        echo -en "Динамический контроль СКЗИ не пройден " | systemd-
cat -t ZASTAVA
        /sbin/poweroff
fi
```

4) сохранить изменения и закрыть файл;
5) в программе эмулятора терминала выполнить команду:

```
chmod +x /usr/sbin/regular_check_control_sum.sh
```

Для настройки задания на выполнение периодической проверку выполнить шаги:

1) в программе эмулятора терминала выполнить авторизацию с использованием данных учётной записи с правами суперпользователя (root);
2) создать сценарий периодической проверки, выполнив команду:

```
crontab -e
```

3) указать периодичность проверки:

```
1    */3    *    *    *    /usr/sbin/regular_check_control_sum.sh    >>
/var/spool/cron/root
```

4) сохранить изменения и закрыть файл.

3.2. Восстановление ПАК «ЗАСТАВА-Клиент»

Проверка целостности ПАК «ЗАСТАВА-Клиент» осуществляется путем сравнения значения контрольных сумм (КС), приведённых в файле filelist.hash для данного файла, с его

текущим значением. При несовпадении значений выдается соответствующее предупреждение. Расчет КС производится по алгоритму ГОСТ 34.11-2012.

Проверка КС производится в процессе загрузки службы vpndmn, при проверке целостности ПАК «ЗАСТАВА-Клиент» производится регистрация событий в системном журнале и в файле vpn_init.log.

При нарушении целостности служба ПАК «ЗАСТАВА-Клиент» не запустится, что свидетельствует о нарушении целостности ПАК.

Проверить КС можно, запустив в командном интерпретаторе cmd.exe утилиту «icv_checker», входящую в комплект поставки ПАК «ЗАСТАВА-Клиент». Для проверки целостности ПАК необходимо выполнить команду:

```
icv_checker filelist.hash
```

где: filelist.hash - файл с текущим значением КС.

Во время работы ПАК «ЗАСТАВА-Клиент» проверяет доступность ЦУП. В случае, если ЦУП не доступен, ПАК «ЗАСТАВА-Клиент» переходит режим, который предполагает применение политики аварийного состояния, определенной в настройках драйвера vpnpcap.

Для восстановления работоспособности ПАК «ЗАСТАВА-Клиент», администратор может вручную перезапустить службу, настроить на автоматический запуск службы после сбоя или вернуть к заводским параметрам (произвести деинсталляцию с последующей инсталляцией ПАК «ЗАСТАВА-Клиент»). Если данные действия не привели к восстановлению функционирования, необходимо обратиться к предприятию-изготовителю ПАК «ЗАСТАВА-Клиент».

Более подробная информация о применении утилиты «icv_checker» приведена в подразделе 5.5.

3.3. Конфигурирование ПАК «ЗАСТАВА-Клиент»

ПАК «ЗАСТАВА-Клиент» может быть сконфигурировано после установки как с помощью графического интерфейса (подробные инструкции приведены в разделе 4), так и с помощью командной строки (подробные инструкции приведены в разделе 5).

При подготовке к работе необходимо настроить в ПАК «ЗАСТАВА-Клиент» параметры получения политики безопасности.

3.3.1. Настройка получения политики безопасности

	Настройку получения политики безопасности осуществляет администратор ОС.
	Политика безопасности не должна задаваться из файла! Политика безопасности должна быть прогружена строго с сервера ПО «ЗАСТАВА-Управление».

При поставке в ПАК «ЗАСТАВА-Клиент» в качестве текущей ЛПБ установлена политика, сохраненная в драйвере по умолчанию. При этом значок ПАК «ЗАСТАВА-Клиент» в системной информационной панели синего цвета .

Необходимо установить в качестве текущей ЛПБ политику пользователя. Политика пользователя создается в ПО «ЗАСТАВА-Управление» и загружается на ПАК «ЗАСТАВА-Клиент» по сети.

Настройка получения политики пользователя производится с помощью ПАК «ЗАСТАВА-Клиент». Для настройки параметров получения пользовательской политики безопасности необходимо:

1) открыть панель управления ПАК «ЗАСТАВА-Клиент», нажав правой клавишей мыши на значок в системной информационной панели и выбрав элемент «Панель управления»;
2) открыть окно «Управление политиками», нажав кнопку «Политика» (см. Рисунок 1);

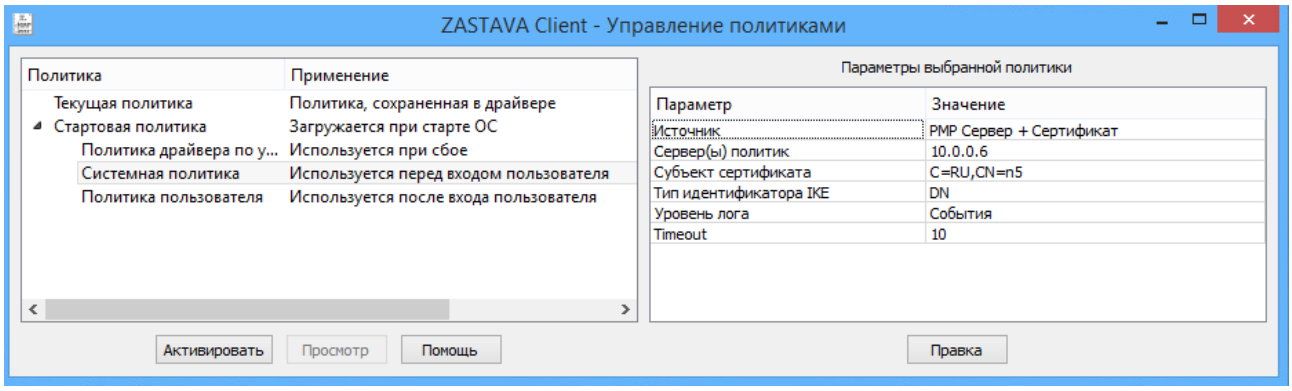


Рисунок 1 – Окно управления политиками

3) в открывшемся окне выбрать пункт «Политика пользователя» и нажать клавишу <Enter>. Откроется окно «Опции политики» (см. Рисунок 2);

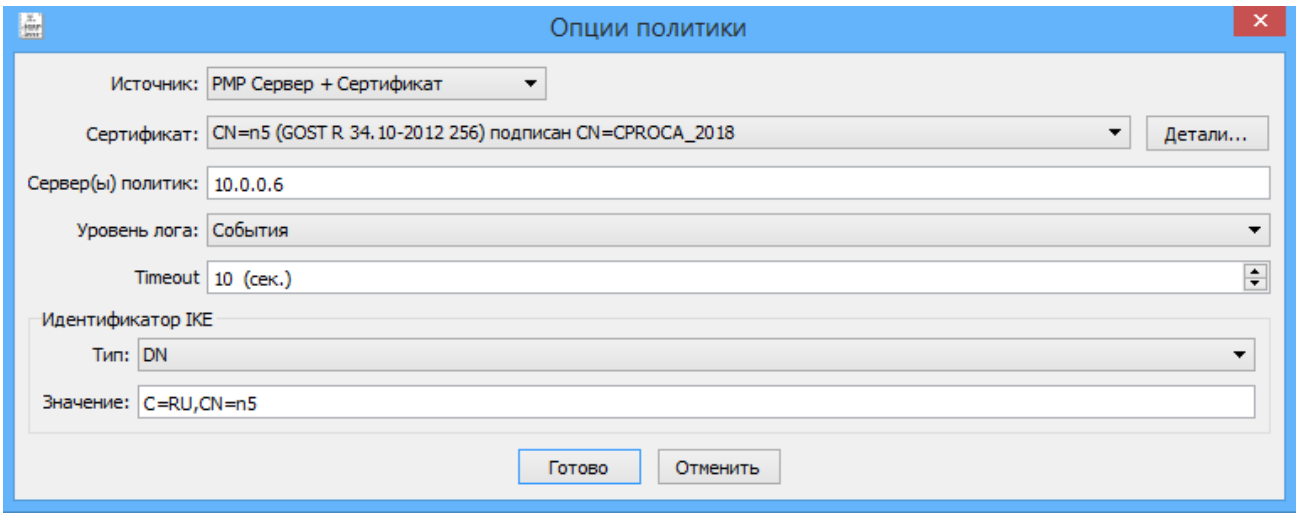


Рисунок 2 – Окно «Опции политики». Настройка политики пользователя

4) в окне «Опции политики» выполнить следующие настройки:

— в поле «Источник» выбрать «Сервер + Сертификат» для загрузки ЛПБ с сервера ПО «ЗАСТАВА-Управление» и установки SA IPsec с помощью сертификата;

— в поле «Сервер(ы) политик» указать IP-адрес или имя сервера и порт, с которого будет получена политика. Если номер порта не указан, то будет взято значение по умолчанию (500). Если серверов несколько, IP-адреса указываются через запятую. Номер порта указывается через двоеточие;

— в секции «Идентификатор IKE» выбрать из раскрывающегося списка значение «DN»;

— остальные настройки оставить без изменений:

  — «Сертификат» – «Любой персональный сертификат»;

  — «Уровень лога» – «События»;

  — «Timeout» – 10 (сек);

5) нажать кнопку «Готово». В появившемся запросе на активацию измененной политики выбрать «Да» (см. Рисунок 3).

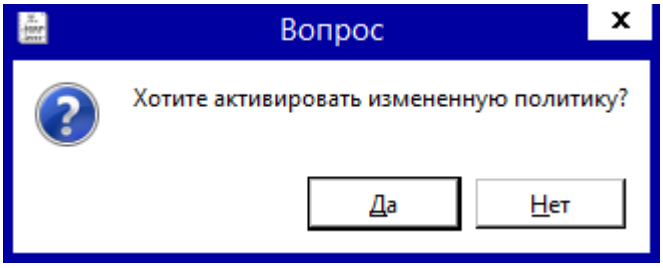


Рисунок 3 – Запрос на активацию политики

В результате будет загружена и активирована пользовательская политика. При успешной загрузке значок программы в системной информационной панели изменит свой цвет на зеленый «».

3.3.2. Настройка журнала

Настройка параметров регистрации событий производится из окна «Прочие настройки», которое открывается кнопкой «Настройки». Окно «Прочие настройки» содержит вкладку «Журнал», в которой производится настройка параметров регистрации событий.

Параметры ведения журнала «Максимальный размер файла (КБ)» и «Число резервных копий» настраиваются индивидуально, но должны быть не менее следующих значений:

— 10240 для параметра «Максимальный размер файла (КБ)»;

— 5 для параметра «Число резервных копий».

Запрещается деактивировать параметр «Вести запись в файл»!

3.4. Конфигурирование модуля vpnpcap

Существует возможность конфигурировать поведение модуля vpnpcap с помощью задания параметров:

- filth_max_count - размер хэш-таблицы фильтров (по умолчанию 8192). Хэш-Таблица обеспечивает быстрый поиск фильтра при точном соответствии записи в ней параметрам пакета;
- threads_mask - битовая маска, определяющая на каких процессорах будет выполняться код драйвера. По умолчанию - все нули, что означает «на всех, установленных в системе». Если маска отлична от нуля, то установленные биты разрешают выполнение кода драйвера на соответствующих CPU, а сброшенные – запрещают;
- pcap_defcfg - политика драйвера, действующая во время загрузки программной составляющей с момента загрузки драйвера vpnpcap в оперативную память СВТ и до момента запуска службы vpndmn, может принимать значения:
  - 2 - PASS(default);
  - 1 – DROP (all,except DHCP);
  - 0 – DROP (all);
- diffserv – параметр, отвечающий за включение функции приоритизации трафика на основании поля ToS заголовка IP-пакета. diffserv=1 – приоритизация трафика включена. По умолчанию установлено значение «0»;
- параметр, опередеяющий размер очереди обрабатываемых пакетов.

3.4.1. Изменение параметров запуска vpnpcap в ОС семейства Linux

Параметры запуска vpnpcap задаются в конфигурационном файле /etc/vpnagent/vpnpcap.conf pkt_queue в формате: <параметр>=<значение>

После изменения конфигурационного файла необходимо перезапустить службу ПАК «ЗАСТАВА-Клиент»:

```
service stop vpnclient
service stop vpnclient_pcap
service start vpnclient_pcap
service start vpnclient
```

или перезагрузить ОС.

Для изменения параметров без перезагрузки необходимо выполнить команду:

```
echo <значение> > /sys/modules/vpnpcap/<параметр>
```

3.5. Процедура обновления

Сведения о процедуре обновления приведены в документе МКЕЮ.00689-01 30 01 «Программно-аппаратный комплекс «VPN/FW «ЗАСТАВА-Клиент», версия 8 КС3». Формуляр».

3.5.1. Обновление ПАК «ЗАСТАВА-Клиент»

Процессы скачивания и установки обновлений не выполняются автоматически, а могут выполняться в зависимости от настроек в ЛПБ ПО «ЗАСТАВА-Управление»:

- обновление по команде с сервера обновления;
- не обновлять.

Обращение к серверу обновлений производится по открытому протоколу HTTP. При необходимости защиты данного соединения можно воспользоваться штатными средствами ПО «ЗАСТАВА-Управление», установив правило для защищенного соединения между данным ПАК «ЗАСТАВА-Клиент» и сервером обновления.

На сервере обновлений должна быть выложена сертифицированная версия ПАК «ЗАСТАВА-Клиент». Использование несертифицированной версии запрещено.

Для обновления ПАК «ЗАСТАВА-Клиент» необходимо выполнить команду:

```
dpkg –i <путь к инсталляционному пакету ZASTAVAclient формата deb>
```

3.6. Рекомендации по безопасной настройке и конфигурированию

Рекомендации по безопасной настройке и конфигурированию ПАК «ЗАСТАВА-Клиент»:

1) установка, настройка и конфигурирование ПАК «ЗАСТАВА-Клиент» на аппаратную платформу персонального СВТ должны осуществляться исключительно администратором безопасности СКЗИ в соответствии с требованиями настоящего Руководства системного программиста и требованиями документа МКЕЮ.00689-01 93 01 «Программно-аппаратный комплекс «VPN/FW «ЗАСТАВА-Клиент», версия 8 КС3» (исполнение ZC8-AS64-VF-03). Правила пользования»;
2) перед установкой и настройкой ПАК «ЗАСТАВА-Клиент» на персональные СВТ, предназначенные для его размещения, должны быть установить все последние обновления ОС, используемой на этом СВТ;
3) перед установкой и настройкой ПАК «ЗАСТАВА-Клиент» на персональные СВТ, предназначенные для его размещения, должны быть проверены на отсутствие вредоносного программного кода. Должна быть организована постоянная антивирусная защита персонального СВТ, на котором установлен ПАК «ЗАСТАВА-Клиент». Рекомендуется использовать для указанных целей сертифицированные в Российской Федерации антивирусные средства. Антивирусные базы данных должны регулярно обновляться. При конфигурировании средств антивирусной защиты, размещаемых на СВТ с установленным ПАК «ЗАСТАВА-Клиент» необходимо, чтобы системная служба ***vpndmn*** была внесена в список доверенных приложений (исключений);
4) на персональных СВТ, предназначенных для установки и эксплуатации ПАК «ЗАСТАВА-Клиент», должно быть **ЗАПРЕЩЕНО** размещение и/или наличие средств разработки и отладки программного обеспечения;

5) установка ПАК «ЗАСТАВА-Клиент» на СВТ должна производиться только с дистрибутивов, полученных по доверенному каналу одним из способов, описанных в документе МКЕЮ.00689-01 93 01 «Программно-аппаратный комплекс «VPN/FW «ЗАСТАВА-Клиент», версия 8 КС3» (исполнение ZC8-AS64-VF-03). Правила пользования»;
6) на СВТ, предназначенных для установки и эксплуатации ПАК «ЗАСТАВА-Клиент», должен быть настроен режим замкнутой программной среды для ОС в соответствии с документацией на ОС Astra Linux 1.7;
7) в ПАК «ЗАСТАВА-Клиент» должен быть настроен механизм автоматического контроля целостности программных модулей путём запуска по расписанию утилиты ***icv_checker*** с файлом шаблона контроля целостности;
8) на СВТ, предназначенных для установки и эксплуатации ПАК «ЗАСТАВА-Клиент», должен быть установлен аппаратно-программный модуль доверенной загрузки (АПМДЗ), сертифицированный в установленном порядке и имеющий действующий сертификат ФСБ России;
9) для обеспечения защиты ПАК «ЗАСТАВА-Клиент» от НСД при реализации ролевой модели должен быть настроен режим двухфакторной аутентификации, при котором доступ к загрузке ОС предоставляется на основании сертификата X.509, хранящегося на ключевом носителе и PIN-кода к этому носителю;
10) настройка параметров мониторинга, протоколирования, аудита и анализа системных событий в ПАК «ЗАСТАВА-Клиент» должны осуществляться в соответствии с требованиями и рекомендациями настоящего Руководства системного программиста;
11) при настройке, конфигурировании и создании политики безопасности администратор безопасности СКЗИ ПАК «ЗАСТАВА-Клиент» должен руководствоваться следующими требованиями:

— атрибуту cipher в структуре proto_ike должно быть присвоено одно из следующих значений: «GR3412_2015_KD-H96-MGM» или «GR3412_2015_MD-H64-MGM»;
— атрибуту group в структуре proto_ike должно быть присвоено значение «GR34102012_256» при использовании атрибуту cipher со значением «GR3412_2015_MD-H64-MGM»;
— атрибуту group в структуре proto_ike должно быть присвоено значение «GR34102012_256» или «GR34102012_512» при использовании атрибуту cipher со значением «GR3412_2015_KD-H64-MGM»;
— атрибуту prf в структуре proto_ike должно быть присвоено значение «GR34112012_512-HMAC»;

— атрибуту expiry_time в структуре proto_ike должно быть присвоено цифровое значение в диапазоне от 180 до 28800;

— атрибуту cipher в структуре proto_esp должно быть присвоено значение: «GR3412_2015_KD-H96-MGM» или «GR3412_2015_MD-H64-MGM»;

Примечания. 1. При установке значения ***0*** атрибуту ***expiry_time*** в структуре ***proto_ike***, атрибуту ***expiry_traffic*** должно быть присвоено цифровое значение в диапазоне от ***1*** до ***4096***.

2. При установке значения ***0*** атрибуту ***expiry_time*** в структуре ***proto_esp***, атрибуту ***expiry_traffic*** должно быть присвоено цифровое значение в диапазоне от ***1*** до ***4096***.

12) при необходимости обеспечить совместимость ПАК «ЗАСТАВА-Клиент» с сертифицированными программными, программно-аппаратными и аппаратно-программными изделиями типа «VPN/FW «ЗАСТАВА», версия 6»[1)] производства АО «ЭЛВИС-ПЛЮС» при настройке, конфигурировании и создании политики безопасности администратор безопасности СКЗИ должен руководствоваться следующими требованиями:

— атрибуту cipher в структуре proto_ike должно быть присвоено одно из следующих значений: «GR2814789-CTR»;

— атрибуту group в структуре proto_ike должно быть присвоено значение «GR34102012_256»;

— атрибуту prf в структуре proto_ike должно быть присвоено значение «GR34112012_256-HMAC» или «GR34112012_512-HMAC»

— атрибуту expiry_time в структуре proto_ike должно быть присвоено цифровое значение в диапазоне от 180 до 28800;

— атрибуту cipher в структуре proto_esp должно быть присвоено значение: «GR2814789D-CTR»;

— атрибут integrity в структуре proto_esp должен всегда присутствовать и ему должно быть присвоено значение: «GR2814789-IMIT»;

[1)] СКЗИ семейства «VPN/FW «ЗАСТАВА», версия 6» используют для шифрования и имитостойкого шифрования данных российский государственный стандарт ГОСТ 28147-89 «Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования», использование которого возможно на основании разрешения ЦЗИиСС ФСБ России.

— атрибут cipher со значением «GR2814789D-CTR» совместно с атрибутом integrity со значением GR2814789-IMIT в структуре proto_esp должен использоваться только в режиме туннелирования;

— атрибуту expiry_time в структуре proto_esp должно быть присвоено цифровое значение в диапазоне от 180 до 28800;

Примечания. 1. При установке значения ***0*** атрибуту ***expiry_time*** в структуре ***proto_ike***, атрибуту ***expiry_traffic*** должно быть присвоено цифровое значение в диапазоне от ***1*** до ***4096***.

2. При установке значения ***0*** атрибуту ***expiry_time*** в структуре ***proto_esp***, атрибуту ***expiry_traffic*** должно быть присвоено цифровое значение в диапазоне от ***1*** до ***4096***.

13) при настройке, конфигурировании и создании политики безопасности средств межсетевого экранирования ПАК «ЗАСТАВА-Клиент» **ЗАПРЕЩАЕТСЯ** использовать режим ***«Pass All»*** по умолчанию;

14) средства контроля за вскрытием корпуса, если таковыми оборудованы системные блоки персональных СВТ с размещенным ПАК «ЗАСТАВА-Клиент», должны быть приведены в рабочее состояние. Размещение средств контроля на системных блоках должно позволять визуально контролировать вскрытие системного блока и исключать возможность бесконтрольного изменения аппаратной части данного СВТ.

4. ГРАФИЧЕСКИЙ ИНТЕРФЕЙС ПАК «ЗАСТАВА-КЛИЕНТ»

4.1. Запуск графического интерфейса ПАК «ЗАСТАВА-Клиент»

Системные модули ПАК «ЗАСТАВА-Клиент» запускаются автоматически при загрузке ОС и работают постоянно в фоновом режиме. При работе ПАК «ЗАСТАВА-Клиент» в системной информационной панели присутствует значок программы «».

Открыть графический интерфейс ПАК «ЗАСТАВА-Клиент» можно одним из способов:

— левой клавишей мыши дважды нажать на значок «» в системной информационной панели;

— нажать правой клавишей мыши на значок «» в системной информационной панели и в появившемся контекстном меню (см. Рисунок 4) выбрать требуемый элемент. Из контекстного меню можно открыть панель управления или одно из окон ПАК «ЗАСТАВА-Клиент».

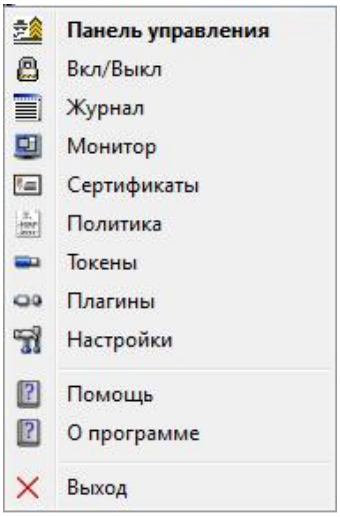


Рисунок 4 – Контекстное меню значка ПАК «ЗАСТАВА-Клиент» в системной информационной панели

4.2. Индикация текущего статуса

Текущий статус ЛПБ ПАК «ЗАСТАВА-Клиент» отображается цветом значка в системной информационной панели, кроме того, текущий статус можно просмотреть в нижней части Панели управления ПАК «ЗАСТАВА-Клиент» (см. подраздел 4.1).

Для просмотра подробной информации о текущем статусе ЛПБ необходимо поместить курсор поверх значка в системной информационной панели и подождать несколько секунд, в результате будет показана подсказка с подробной информацией. Та же самая информация отображается в строке состояния панели управления.

Статусы ПАК «ЗАСТАВА-Клиент» представляются разными графическими символами (см. Таблица 5).

Таблица 5 – Перечень графических символов статусов ЛПБ

Статус ПАК «ЗАСТАВА-Клиент»	Цвет значка
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 политики из файла (или отсутствие активации); предыдущая политика будет восстановлена	(жёлтый)
Активирована «Политика драйвера по умолчанию»	(синий)
Системная служба ПАК «ЗАСТАВА-Клиент» `vpndmn` не запущена	(серый)
При загрузке политики ПАК «ЗАСТАВА-Клиент» с ПО «ЗАСТАВА-Управление» (сервер доступен)	(темно зеленый с ярко зеленой рамкой)
При загрузке политики ПАК «ЗАСТАВА-Клиент» с ПО «ЗАСТАВА-Управление» (сервер недоступен)	(желтый с красной рамкой)
Обращение к политике ПАК «ЗАСТАВА-Клиент»	(серый с песочными часами)

4.3. Ввод пароля токена

Ввод пароля ключевого носителя (токена) требуется тогда, когда ПАК «ЗАСТАВА-Клиент» начинает инициировать создание защищенного соединения с сервером ПО «ЗАСТАВА-Управление». В процессе создания соединения при обращении к персональному сертификату будет запрошен пароль (ПИН-код токена) ключевого носителя (см. Рисунок 5).

Также пароль запрашивается при любом действии с персональным сертификатом, например, удалении его из ПАК «ЗАСТАВА-Клиент» и т.д.

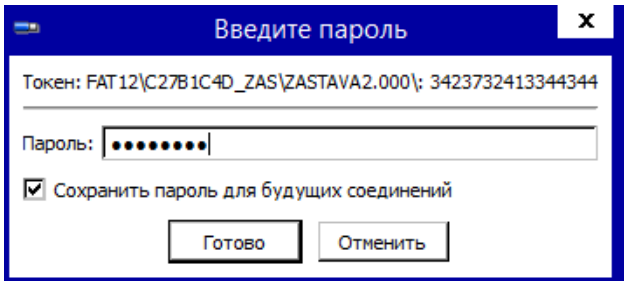


Рисунок 5 – Ввод пароля токена при создании защищенного соединения

Необходимо удостовериться в запуске графического интерфейса ПАК «ЗАСТАВА-Клиент», в противном случае окно с запросом на ввод пароля токена не появится, и защищенное соединение с сервером ПО «ЗАСТАВА-Управление» не создастся.

4.4. Панель управления

Панель управления ПАК «ЗАСТАВА-Клиент» (см. Рисунок 6) содержит кнопки, при помощи которых можно выполнить необходимую операцию или открыть дополнительное окно.

В нижней части панели управления находится поле, отображающее текущий статус ЛПБ ПАК «ЗАСТАВА-Клиент» (тип активированной ЛПБ, источник ЛПБ, название конфигурации, дата и время ее активации).

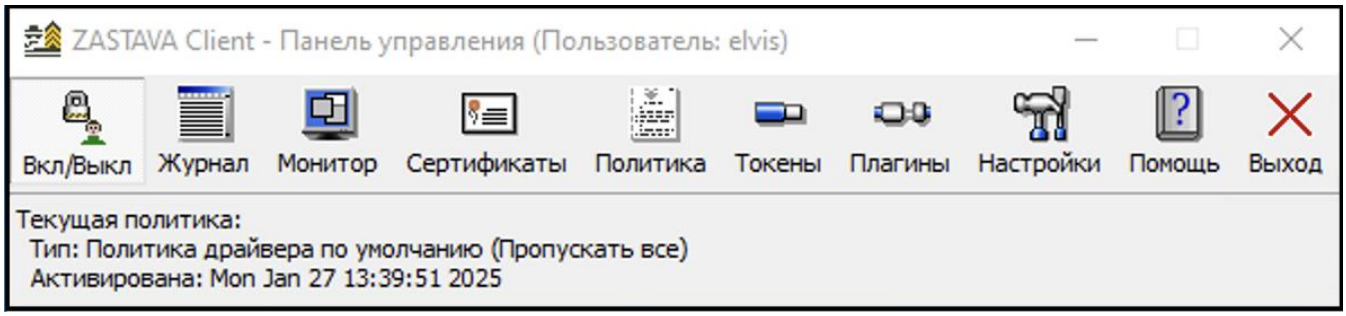


Рисунок 6 – Панель управления

Описание кнопок панели управления приведено в таблице (см. Таблица 6).

Таблица 6 - Кнопки панели управления

Кнопка	Описание
Вкл/Выкл	Переключение между пользовательской и системной политиками безопасности: «Вкл» – прогружается пользовательская политика; «Выкл» – удаляются все созданные ПАК «ЗАСТАВА-Клиент» защищенные соединения (SA) и прогружается системная политика, либо, если отсутствует системная политика, политика драйвера по умолчанию, настраиваемая в окне «Управление политиками» (см. подраздел 4.8). Текущее состояние ЛПБ отображается в нижней части панели управления
Журнал	Открывает Журнал событий, в котором отображается информация о системных событиях
Монитор	Открывает окно «Монитор», в котором представлен обзор активных защищенных соединений, установленных с данным СВТ
Сертификаты	Открывает окно «Сертификаты и Ключи», предназначенное для регистрации в ПАК «ЗАСТАВА-Клиент» сертификатов (включая сертификаты удостоверяющего центра (УЦ)), предварительно распределенных ключей и списки отозванных сертификатов (СОС)
Политика	Открывает окно «Управление политиками», предназначенное для редактирования списка ЛПБ и установки опций ЛПБ
Токены	Открывает окно «Токены», предназначенное для редактирования списка токенов, а также смены пароля, инициализации, обновления токенов
Плагины	Открывает окно «Плагины», с помощью которого можно регистрировать и активировать криптобиблиотеки
Настройки	Открывает окно «Прочие настройки», предназначенное для изменения локальных установок ПАК «ЗАСТАВА-Клиент». Изменять настройки может только администратор ПАК «ЗАСТАВА-Клиент». Остальным пользователям изменение настроек запрещено
Помощь	Отображает меню, содержащее следующие команды: – «Помощь» – вызывает справочную систему ПАК «ЗАСТАВА-Клиент»; – «О ZASTAVA Client» – отображает окно с информацией о программе.
Выход	Закрывает графический интерфейс ПАК «ЗАСТАВА-Клиент». При этом будет отключена политика пользователя и загружена системная политика, сервис vpndmn будет продолжать работать

4.5. Окно «Журнал»

Окно «Журнал» (см. Рисунок 7) открывается нажатием кнопки «Журнал» на панели управления. В журнале отображается содержимое файла регистрации событий ПАК «ЗАСТАВА-Клиент».

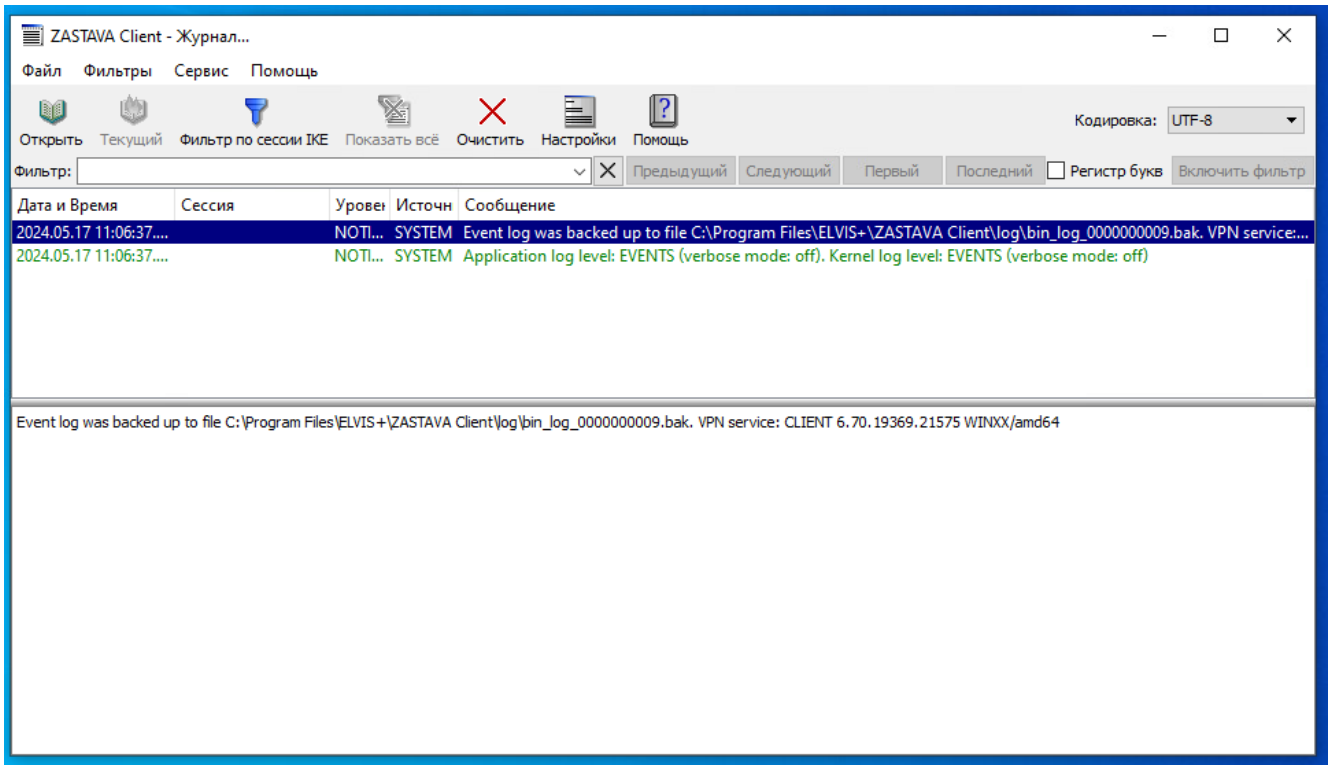


Рисунок 7 – Окно с зарегистрированными событиями

В верхней части окна расположена панель управления.

Основную часть окна занимает таблица с описанием системных событий. Уровень детализации настраивается пользователем (подробнее см. п. 4.5.2.3).

В журнале регистрируются следующие события:

- запуск и завершение выполнения функций аудита (запуск и остановка службы vpndmn);
- действия, предпринимаемые ПАК «ЗАСТАВА-Клиент» в ответ на нарушения безопасности (журналирование DROP правил фильтрации или запрет команд в прокси);
- получение доступа и факт изменения локального журнал аудита (факт удаления журнала bin_log);
- внесение изменений в список информации, подлежащей аудиту (изменение уровня журналирования);
- все решения по запросам на информационные потоки (создание и удаление стейтов межсетевых экранов);

- все попытки подключения к субъектам защищаемого сегмента сети из неконтролируемого сегмента сети, включая любые атрибуты безопасности (использование логов FW-процедур на установление соединения либо разрешение потока в прокси);
- все попытки подключения субъектов, находящихся в защищаемом сегменте сети, к ресурсам, расположенным в неконтролируемом сегменте сети (использование логов FW-процедур на установление соединения либо разрешение потока в прокси);
- все модификации списка типов контролируемого сетевого трафика (журналирование активации политики);
- изменение настроек ПАК «ЗАСТАВА-Клиент»;
- изменение настроек получения политики безопасности;
- назначение приоритета обслуживания информационных потоков;
- сообщения синхронизации при использовании кластеризации;
- удачный вход пользователей в ПАК «ЗАСТАВА-Клиент»;
- неудачный вход пользователей в ПАК «ЗАСТАВА-Клиент»;
- запуск и остановка службы ПАК «ЗАСТАВА-Клиент», реализующей функции безопасности (запуск и останов службы vpndmn);
- неудачный запуск и остановка службы ПАК «ЗАСТАВА-Клиент», реализующей функции безопасности (неудачный запуск службы vpndmn);
- результат проверки КС ПАК «ЗАСТАВА-Клиент».

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 отображается информация из столбца «Сообщение» выделенной строки журнала.

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

4.5.1. Строка меню окна «Журнала»

Строка меню содержит следующие меню: «Файл», «Фильтры», «Сервис», «Помощь». Команды меню представлены в таблице (см. Таблица 7).

Таблица 7 – 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
Помощь	
Справка по журналу	Открывает раздел «Справки», поясняющий работу с журналом регистрации системных событий
Помощь	Вызов интерактивной справочной системы ПАК «ЗАСТАВА-Клиент»

4.5.2. Панель инструментов окна «Журнал»

Описание элементов панели инструментов окна «Журнал» приведено в таблице (см. Таблица 8).

Таблица 8 – 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)

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

4.5.2.1. Контекстное меню окна «Журнал»

Команды контекстного меню окна «Журнал» и их описание приведены в таблице (см. Таблица 9).

Таблица 9 – 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»

4.5.2.2. 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 необходимо выделить в таблице строку с требуемым значением параметра и затем выбрать в меню нужный фильтр. Например, чтобы отфильтровать все события уровня «INFO», надо 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, нужно ввести 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, необходимо нажать правой клавишей мыши на нужной ячейке и в появившемся контекстном меню выбрать команду «Копировать в поле фильтра».

4.5.2.3. 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 8) производится настройка параметров регистрации событий. Содержание вкладки полностью дублирует вкладку «Журнал» окна «Прочие настройки» и настраивается аналогичным образом.

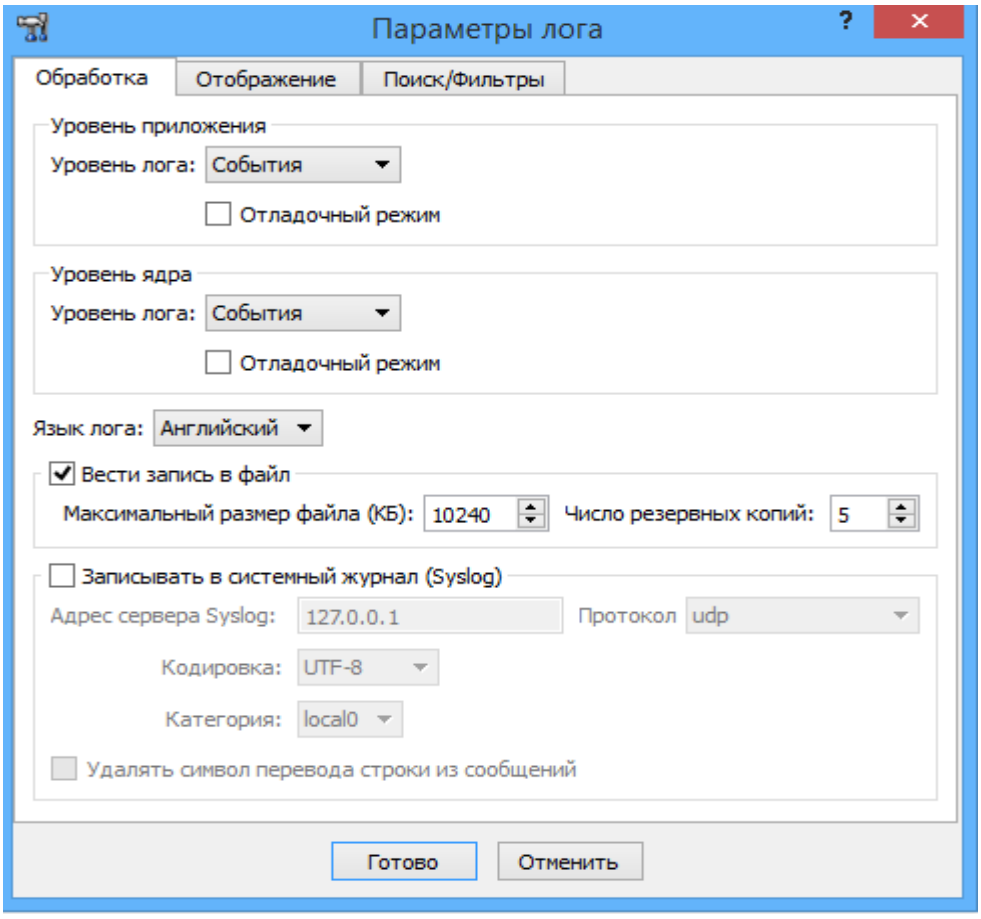


Рисунок 8 – Окно настройки параметров регистрации событий

Параметры представления журнала настраиваются на вкладке «Отображение» (см. Рисунок 9).

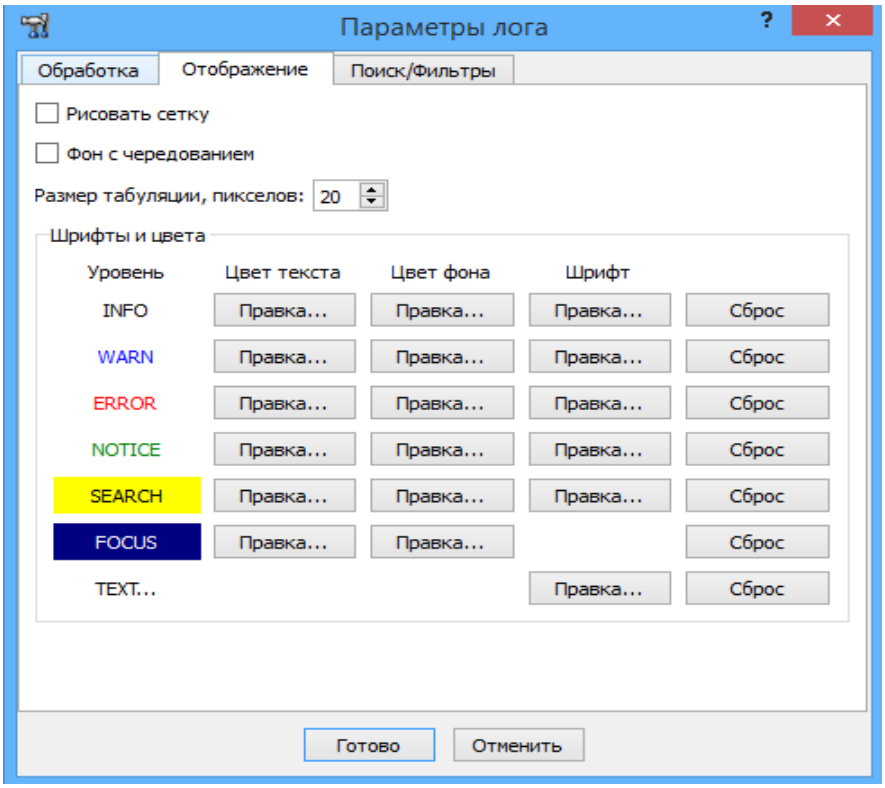


Рисунок 9 – Настройка параметров представления журнала

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

Для применения изменений по окончании настройки нажать кнопку «Готово». Для отмены настроек нажать кнопку «Отменить».

Параметры поиска и фильтрации по журналу настраиваются на вкладке «Поиск/Фильтры» (см. Рисунок 10).

ПАК «ЗАСТАВА-Клиент» поддерживает возможность настройки отображения сообщений при неудачном поиске и префиксов для ID-сессий.

Для применения изменений по окончании настройки нажать кнопку «Готово». Для отмены настроек нажать кнопку «Отменить».

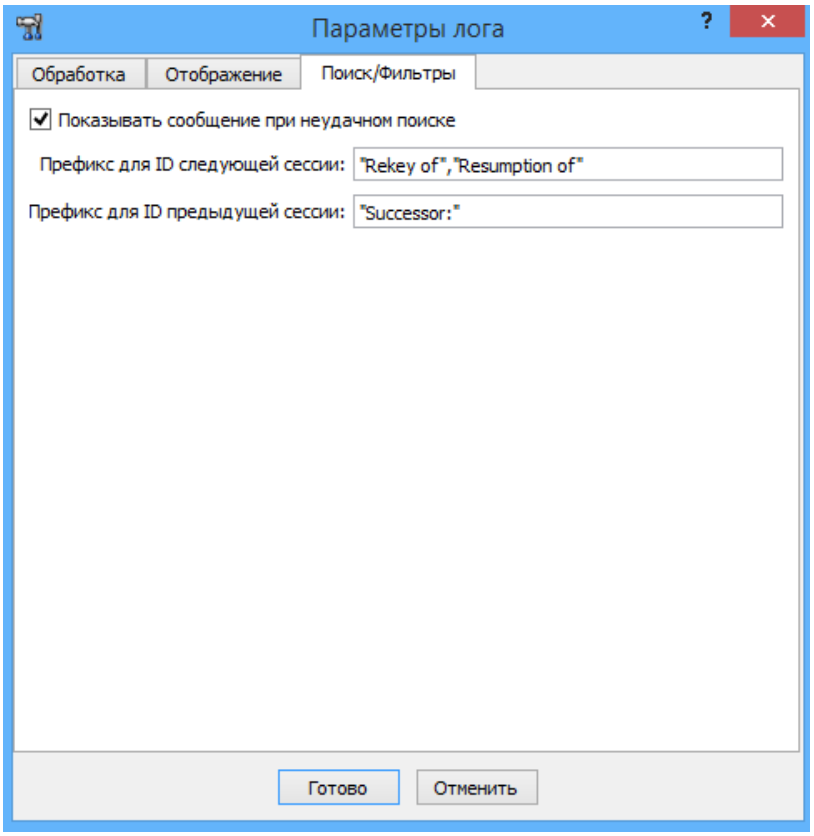


Рисунок 10 – Настройка параметров поиска/фильтрации журнала

4.5.2.4. 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.

4.5.2.5. Файл регистрации системных событий

Содержимое окна «Журнал» для ОС Astra Linux Special Edition 1.7 хранится в файле «/var/vpnagent/log/bin_log.txt».

Для просмотра других журналов регистрации событий ПАК «ЗАСТАВА-Клиент» надо нажать кнопку «Открыть» на панели инструментов окна «Журнал».

4.5.2.6. Очистка журнала и файла регистрации системных событий

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

— журнал будет очищен;

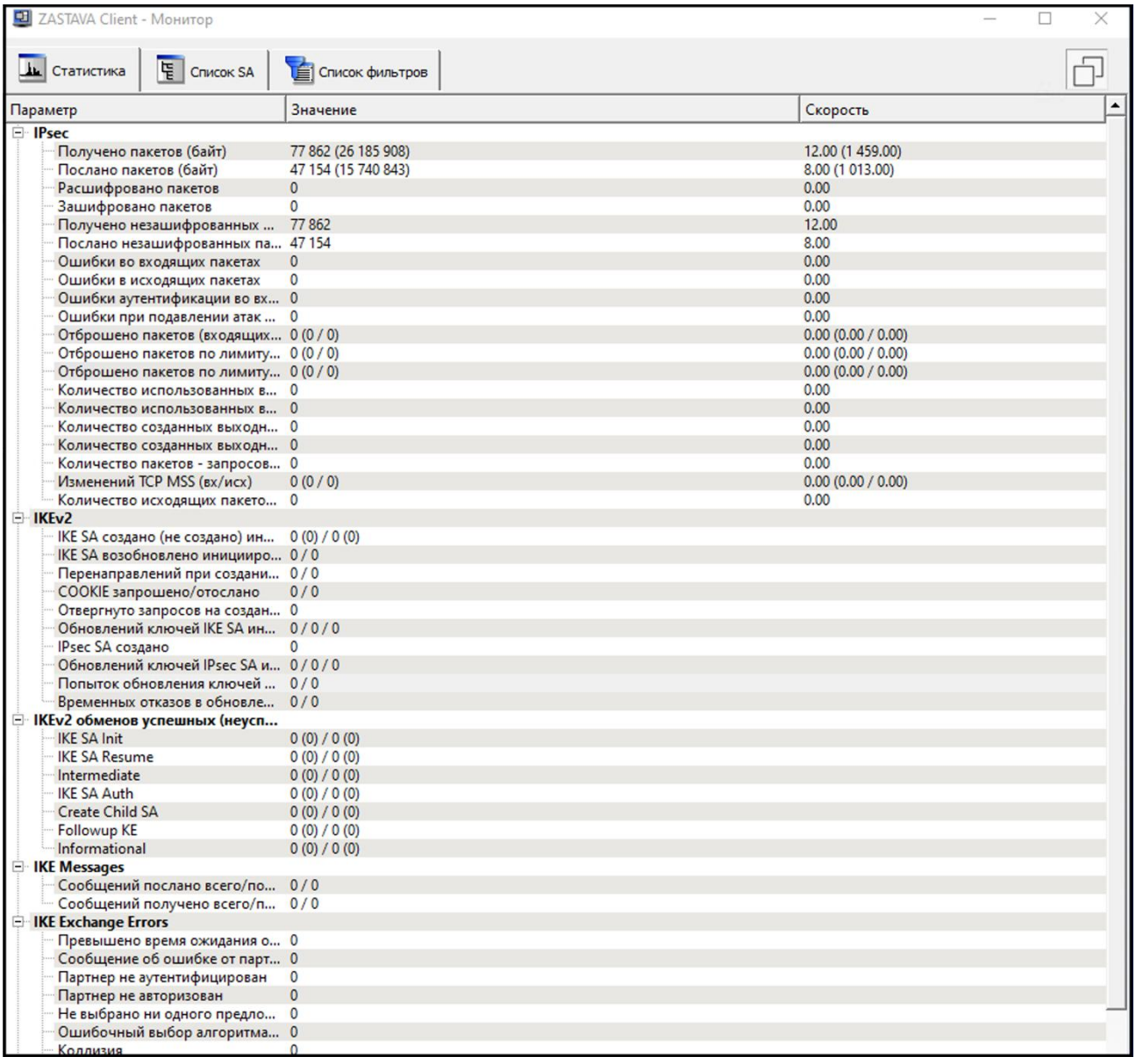
— событие очистки журнала будет зарегистрировано и размещено в начале файла регистрации событий, а также появится вверху списка в окне «Журнал»;

— предыдущий («старый») список зарегистрированных событий будет переименован в файл с именем вида «bin_log_<номер по порядку>» и с расширением *.bak.

4.6. Окно «Монитор»

Окно «Монитор», доступное по нажатии кнопки «Монитор», предоставляет обзор активных в настоящее время защищенных соединений, установленных с данным СВТ.

Кроме того, окно «Монитор» позволяет провести фильтрацию защищённых соединений, просмотреть статистику по пакетам, список выделенных адресов «ike-cfg», а также параметры агентов прикладного уровня. Окно содержит несколько вкладок, как показано на рисунке (см. Рисунок 11).



Параметр	Значение	Скорость
IPsec		
Получено пакетов (байт)	77 862 (26 185 908)	12.00 (1 459.00)
Послано пакетов (байт)	47 154 (15 740 843)	8.00 (1 013.00)
Расшифровано пакетов	0	0.00
Зашифровано пакетов	0	0.00
Получено незашифрованных ...	77 862	12.00
Послано незашифрованных па...	47 154	8.00
Ошибки во входящих пакетах	0	0.00
Ошибки в исходящих пакетах	0	0.00
Ошибки аутентификации во вх...	0	0.00
Ошибки при подавлении атак ...	0	0.00
Отброшено пакетов (входящих...	0 (0 / 0)	0.00 (0.00 / 0.00)
Отброшено пакетов по лимиту...	0 (0 / 0)	0.00 (0.00 / 0.00)
Отброшено пакетов по лимиту...	0 (0 / 0)	0.00 (0.00 / 0.00)
Количество использованных в...	0	0.00
Количество использованных в...	0	0.00
Количество созданных выходн...	0	0.00
Количество созданных выходн...	0	0.00
Количество пакетов - запросов...	0	0.00
Изменений TCP MSS (вх/исх)	0 (0 / 0)	0.00 (0.00 / 0.00)
Количество исходящих пакето...	0	0.00
IKEv2		
IKE SA создано (не создано) ин...	0 (0) / 0 (0)	
IKE SA возобновлено инициро...	0 / 0	
Перенаправлений при создани...	0 / 0	
COOKIE запрошено/отослано	0 / 0	
Отвергнуто запросов на создан...	0	
Обновлений ключей IKE SA ин...	0 / 0 / 0	
IPsec SA создано	0	
Обновлений ключей IPsec SA и...	0 / 0 / 0	
Попыток обновления ключей ...	0 / 0	
Временных отказов в обновле...	0 / 0	
IKEv2 обменов успешных (неусп...		
IKE SA Init	0 (0) / 0 (0)	
IKE SA Resume	0 (0) / 0 (0)	
Intermediate	0 (0) / 0 (0)	
IKE SA Auth	0 (0) / 0 (0)	
Create Child SA	0 (0) / 0 (0)	
Followup KE	0 (0) / 0 (0)	
Informational	0 (0) / 0 (0)	
IKE Messages		
Сообщений послано всего/по...	0 / 0	
Сообщений получено всего/п...	0 / 0	
IKE Exchange Errors		
Превышено время ожидания о...	0	
Сообщение об ошибке от парт...	0	
Партнер не аутентифицирован	0	
Партнер не авторизован	0	
Не выбрано ни одного предло...	0	
Ошибочный выбор алгоритма...	0	
Коллизия	0	

Рисунок 11 – Окно «Монитор», вкладка «Статистика»

4.6.1. Вкладка «Статистика»

На вкладке «Статистика» (см. Рисунок 11) можно получить статистическую информацию по всем пакетам, прошедшим через драйвер ПАК «ЗАСТАВА-Клиент» (например, по протоколу IPsec) (см. Таблица 10).

Таблица 10 – Описание параметров вкладки «Статистика»

Параметр	Описание
IPsec	
Получено пакетов (байт)	Количество пакетов, полученных с момента запуска
Послано пакетов (байт)	Количество пакетов, отправленных с момента запуска
Расшифровано пакетов	Количество расшифрованных пакетов
Зашифровано пакетов	Количество зашифрованных пакетов
Получено незашифрованных пакетов	Количество полученных 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 восстановлеии фрагментированных входных пакетов
Количество использованных выходных фрагментов	Количество IP-фрагментов, использованных при восстановлении фрагментированных выходных пакетов
Количество созданных выходных фрагментов	Количество IP-фрагментов, созданных при фрагментации выходного пакета
Количество пакетов – запросов на понижение MTU	Количество пакетов – запросов на понижение MTU
Количество промахов для входящих пакетов при поиске фильтра в хэш-таблице	Количество промахов для входящих пакетов при поиске фильтра в хэш-таблице
Количество промахов для исходящих пакетов при поиске фильтра в хэш-таблице	Количество промахов для исходящих пакетов при поиске фильтра в хэш-таблице
IKEv2	
IKE SA создано (не создано) инициированных/отвеченных	Количество созданных (не созданных) инициированных/ отвеченных IKE SA в формате x(x)/x(x)
IKE SA возобновлено инициированных/отвеченных	Количество возобновленных IKE SA инициированных/отвеченных
Перенаправлений при создании IKE SA получено/послано	Количество перенаправлений IKE SA получено/послано
COOKIE запрошено/отослано	Количество запрошенных/отправленных токенов COOKIE
Отвергнуто запросов на создание IKE SA	Количество отвергнутых запросов на создание IKE SA
Обновлений ключей IKE SA инициированных/отвеченных/ коллизий	Количество обновлений ключей IKE SA инициированных/ отвеченных/коллизий в формате x/x/x
IPsec SA создано	Количество созданных IPsec SA
Обновлений ключей IPsec SA инициированных/отвеченных/ коллизий	Количество обновлений ключей IPsec SA инициированных/ полученных/коллизий в формате x/x/x

Параметр	Описание
Попыток обновления ключей несуществующей IPsec SA данным хостом/партнером	Количество попыток обновления ключей несуществующей IPsec SA данным хостом/партнером по связи
Временных отказов в обновлении ключей данным хостом/партнером	Количество временных отказов в обновлении ключей данным хостом/партнером по связи
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
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

4.6.2. Вкладка «Список SA»

Вкладка «Список SA» в левой части окна содержит древовидную структуру активных защищённых соединений, установленных с данным СВТ, а также создающихся защищённых соединений. В правой части окна содержится детальная информация о выбранном в левой части окна активном соединении. Изображение окна со вкладкой «Список SA» приведено на рисунке (см. Рисунок 12).

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 информацию о защищенных соединениях (IPSec SAs), параметры и характеристики приведены в таблице (см. Таблица 11).

Таблица 11 – Информация об активных защищенных соединениях

Параметр	Характеристика
ID	ID IKE SA (IKE SPI) или внутренний идентификатор IPsec SA
Адрес партнера	IP-адрес партнера по связи
ID партнера	Идентификатор партнера по связи (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

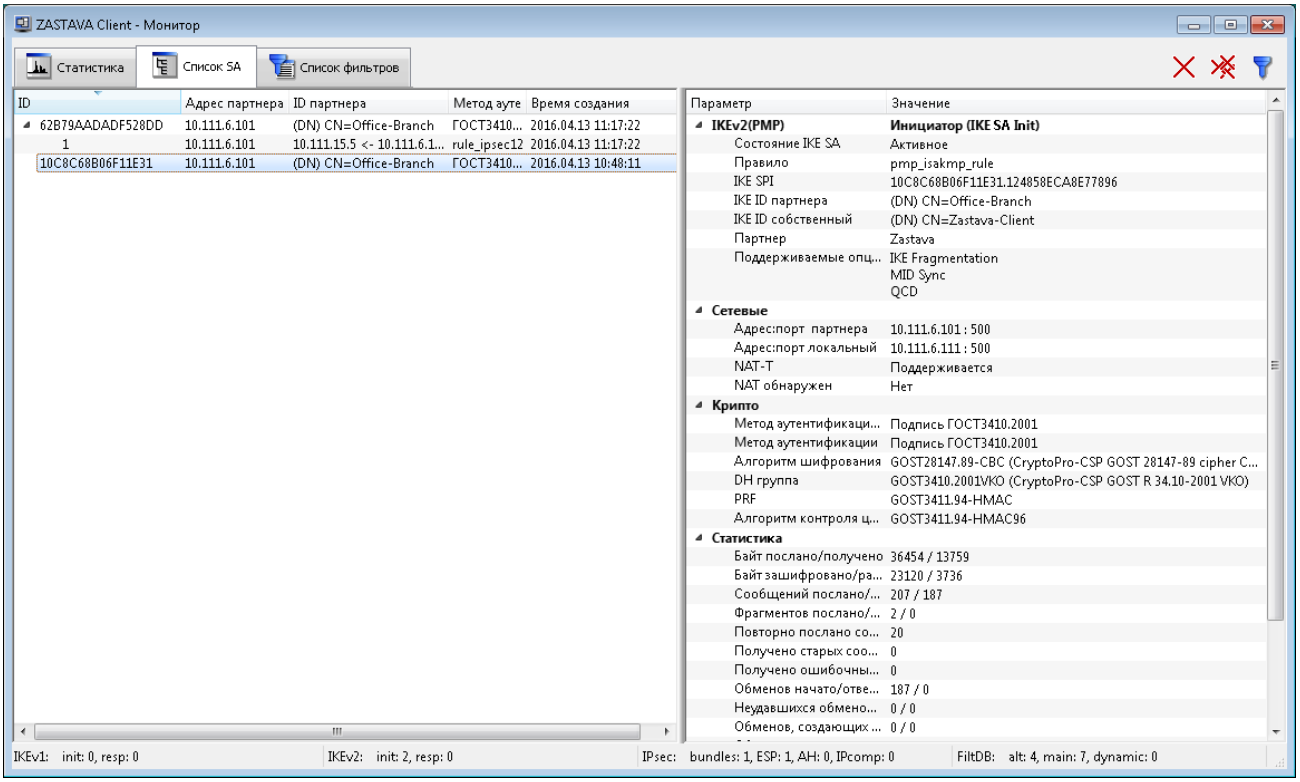


Рисунок 12 – Окно «Монитор», вкладка «Список SA»

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 13).

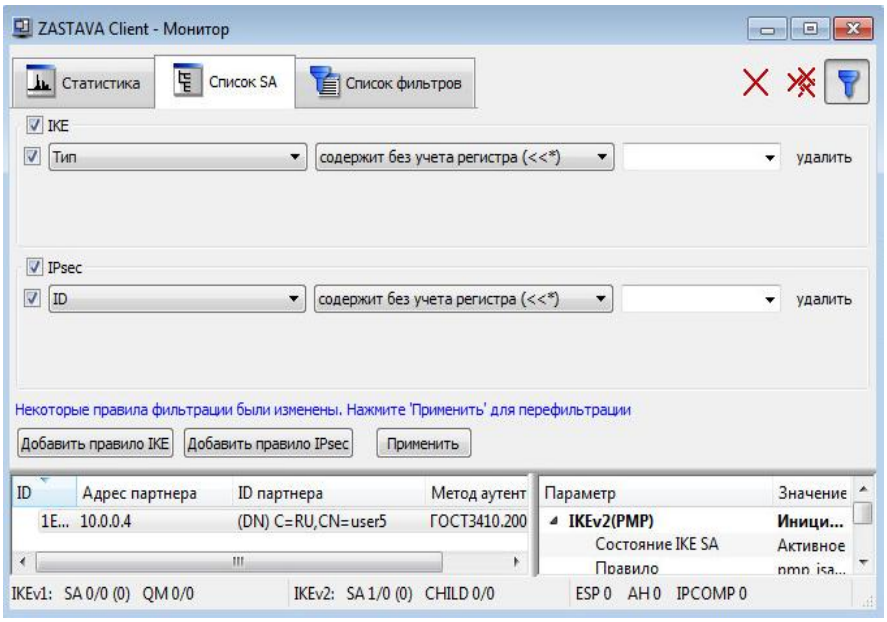


Рисунок 13 – Окно «Монитор», активный «Фильтр»

Параметры фильтрации протокола IKE приведены в таблице (см. Таблица 12).

Таблица 12 – Параметры фильтрации протокола IKE

Параметр	Характеристика
Тип	Тип создания SA
Режим	Режим создания SA
Роль	Роль локальной СВТ при создании SA
Состояние IKE SA	Состояние IKE SA
EAP ID собственный	Свой EAP ID
IKE ID собственный	IKE ID данного СВТ
EAP ID партнера	EAP ID, присланный партнером по связи
IKE ID партнера	IKE ID партнера по связи
ID партнера	ID партнера по связи (IKE ID или EAP ID в зависимости от метода аутентификации)
Правило	Имя правила
Алгоритм шифрования	Алгоритм шифрования
Хэш-функция	Алгоритм хэширования
DH группа	DH-группа
Алгоритм контроля целостности	Алгоритм контроля целостности
PRF	Псевдослучайная функция
Локальный адрес	IP-адрес данного СВТ, использованный при создании защищенного соединения
Локальный порт	UDP-порт на данном СВТ, использованный при создании защищенного соединения
Адрес партнера	IP-адрес СВТ, с которым создано защищенное соединение
Порт партнера	UDP-порт СВТ, с которым создано защищенное соединение
Перенаправлен с адреса	IP-адрес СВТ, с которого произошло перенаправление на данный
Метод аутентификации партнера	Метод аутентификации партнера по связи
Метод аутентификации	Метод идентификации данного СВТ

Параметр	Характеристика
IKE SPI	IKEv2 SPI
Уровень лога	Уровень подробности регистрации событий
Поддерживаемые опции	Список поддерживаемых опций

Параметры фильтрации протокола IPsec приведены в таблице (см. Таблица 13).

Таблица 13 – 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 СВТ, с которым создано защищенное соединение
Режим	Режим создания SA
Роль	Роль при создании SA
Id партнера	ID СВТ партнёра по связи
Id локальный	ID данного СВТ
Адрес партнера	IP-адрес СВТ, с которым создано защищенное подключение
Порт партнера	UDP-порт СВТ, с которым создано защищенное подключение
Адрес локальный	IP-адрес данного СВТ, использованный при создании защищенного соединения
Порт локальный	UDP-порт на данном СВТ, использованный при создании защищенного соединения
IKE-CFG адрес	IKE-CFG адрес, выданный ПАК «ЗАСТАВА-Клиент»
DH группа	DH группа
Фильтр	Фильтр
Правило	Название применяемого правила
(AH) Правило	(AH) Правило
(AH) SPI in	Значение SPI для входящей SA (AH)
(AH) SPI out	Значение SPI для исходящей SA (AH)
(AH) Rekey SPI in	Значение SPI для входящей SA, ключи которой были обновлены
(AH) Уровень лога	(AH) Уровень подробности регистрации событий
(AH) PMTU	(AH) значение MTU, которое установлено на промежуточном агенте
(AH) Состояние	(AH) Состояние
(AH) Аутентификация	(AH) Алгоритм имитозащиты
(AH) Декапсулировано пакетов	(AH) Декапсулировано пакетов
(AH) Декапсулировано байт	(AH) Декапсулировано байт
(AH) Ошибки дешифрации (пакетов)	(AH) Ошибки дешифрации (пакетов)
(AH) Ошибки аутентификации (пакетов)	(AH) Ошибки аутентификации (пакетов)
(AH) Ошибки атак воспроизведения (пакетов)	(AH) Ошибки атак воспроизведения (пакетов)
(AH) Ошибки ограничения трафика (пакетов)	(AH) Ошибки ограничения трафика (пакетов)
(AH) Прочие ошибки декапсуляции (пакетов)	(AH) Прочие ошибки декапсуляции (пакетов)
(AH) Инкапсулировано пакетов	(AH) Инкапсулировано пакетов
(AH) Инкапсулировано байт	(AH) Инкапсулировано байт

Тип	Характеристика
(AH) Ошибки шифрации (пакетов)	(AH) Ошибки шифрации (пакетов)
(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 агенте
(ESP) Состояние	(ESP) Состояние
(ESP) Преобразование	(ESP) Алгоритм шифрования
(ESP) Аутентификация	(ESP) Алгоритм имитозащиты
(ESP) Исходный адрес партнера	(ESP) Исходный адрес партнера по связи
(ESP) Исходный адрес локальный	(ESP) Исходный адрес данного СВТ
(ESP) Декапсулировано пакетов	(ESP) Декапсулировано пакетов
(ESP) Декапсулировано байт	(ESP) Декапсулировано байт
(ESP) Ошибки дешифрации (пакетов)	(ESP) Ошибки дешифрации (пакетов)
(ESP) Ошибки аутентификации (пакетов)	(ESP) Ошибки аутентификации (пакетов)
(ESP) Ошибки атак воспроизведения (пакетов)	(ESP) Ошибки атак воспроизведения (пакетов)
(ESP) Ошибки ограничения трафика (пакетов)	(ESP) Ошибки ограничения трафика (пакетов)
(ESP) Прочие ошибки декапсуляции (пакетов)	(ESP) Прочие ошибки декапсуляции (пакетов)
(ESP) Инкапсулировано пакетов	(ESP) Инкапсулировано пакетов
(ESP) Инкапсулировано байт	(ESP) Инкапсулировано байт
(ESP) Ошибки шифрации (пакетов)	(ESP) ошибки шифрации (пакетов)
(IPcomp) Правило	(IPcomp) Правило
(IPcomp) CPI in	Значение CPI для входящей SA (IPcomp)
(IPcomp) CPI out	Значение CPI для исходящей SA (IPcomp)
(IPcomp) Rekey CPI in	Значение CPI для входящей SA, ключи которой были обновлены (IPcomp)
(IPcomp) Уровень лога	(IPcomp) Уровень подробности регистрации событий
(IPcomp) PMTU	(IPcomp) значение MTU, которое установлено на промежуточном агенте
(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 14).

Таблица 14 – 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
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 TCP/UDP 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: ah, esp, pcp)
не равен	значение поля не равно эталону
Операции для фильтрации по IPsec-соединению по полю mode	
равен	значение поля равно эталону (возможные значения: tunnel, transport)
не равен	значение поля не равно эталону
Операции для фильтрации по IP-протоколу	

Команда	Характеристика
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, в крайнем правом поле строки фильтрации необходимо указать значение, по которому будет производиться сравнение, и нажать кнопку «Применить». В нижней таблице будут показаны отфильтрованные события. Количество событий, удовлетворяющих правилу фильтрации, будет показано правее кнопки «Применить».

На вкладке «Список SA» существует контекстное меню с командами, которое раскрывается по нажатии правой клавиши мыши (см. Таблица 15).

Таблица 15 – 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
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

4.6.3. Вкладка «Список фильтров»

4.6.3.1. Основные элементы

Вкладка «Список Фильтров» позволяет просмотреть как статические, так и динамические фильтры, прогруженные в драйвер (список фильтров определяется ЛПБ) (см. Рисунок 14).

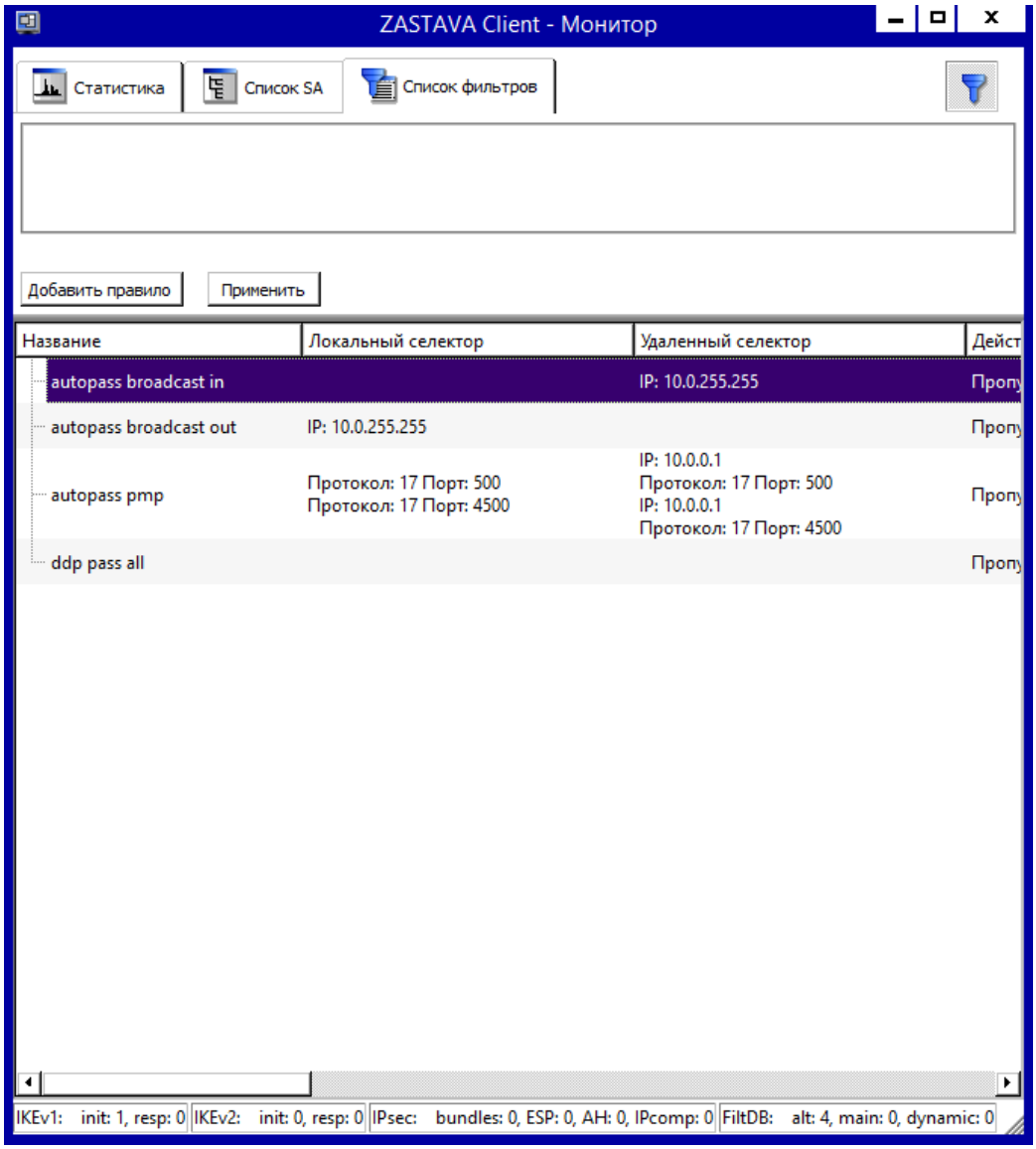


Рисунок 14 – Окно «Монитор», вкладка «Список фильтров»

Основную часть вкладки занимает список фильтров, который включает в себя статистику по параметрам фильтрации (см. Таблица 16).

Таблица 16 – 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	Текущая скорость входящих пакетов
Исходящих пакетов в секунду	Статистика исходящих пакетов в секунду
Исходящих байтов в секунду	Текущая скорость исходящих пакетов

Параметр	Характеристика
Входящих промахов в кэше	Статистика промахов после проверки входящих пакетов на соответствие с фильтрами в кэше
Исходящих промахов в кэше	Статистика промахов после проверки исходящих пакетов на соответствие с фильтрами в кэше
Входящих промахов в кэше в секунду	Статистика промахов 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 17).

Таблица 17 – Команды контекстного меню вкладки «Список фильтров»

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

4.6.3.2. Фильтрация

Для задания правил фильтрации необходимо:

1) открыть панель фильтров кнопкой «  »;
2) нажать кнопку «Добавить правило», появится строка задания правила фильтрации (см. Рисунок 15);
3) задать правило фильтрации:

— выбрать из первого списка параметр фильтрации (см. Таблица 18);
— выбрать из второго списка условие фильтрации;
— в третьем поле задать или выбрать из списка значение, по которому будет производиться сравнение;

 Для удаления фильтра нажать кнопку «Удалить» справа от фильтра.

 Чтобы отключить применение фильтра, 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.

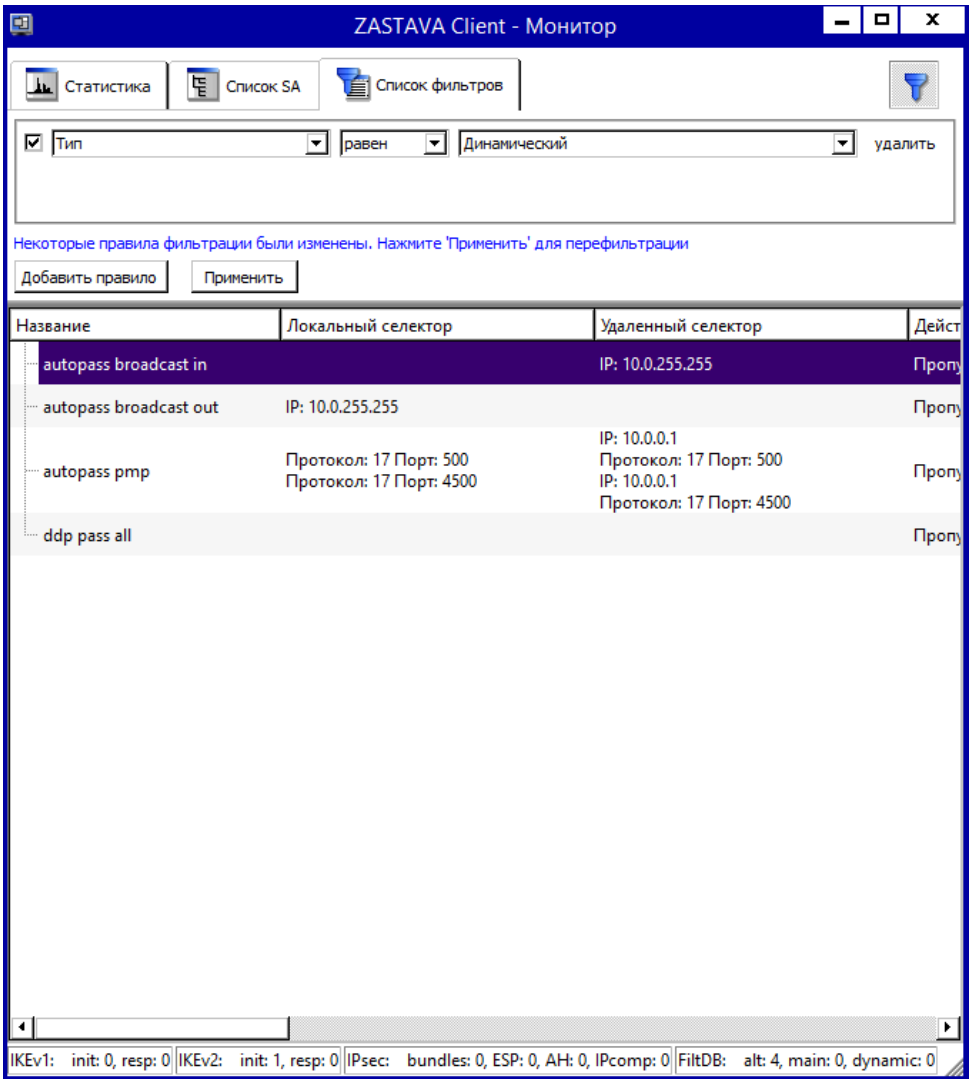


Рисунок 15 – Окно «Монитор», вкладка «Список фильтров». Открыта панель фильтрации

Таблица 18 – 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»
Входящих байт	Фильтрация поля «Входящих байт»
Исходящих байт	Фильтрация поля «Исходящих байт»
Входящих байт отброшено	Фильтрация поля «Входящих байт отброшено»

Параметр	Характеристика
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»

4.7. Окно «Сертификаты и ключи»

Сертификаты (включая сертификаты УЦ), предварительно распределенные ключи и СОС регистрируются в ПАК «ЗАСТАВА-Клиент» через окно «Сертификаты и Ключи». Вызвать это окно можно, нажав кнопку «Сертификаты» на панели управления.

ПАК «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 ПАК «ЗАСТАВА-Клиент» с целью проверки подлинности всех сертификатов, присылаемых партнерами по связи в процессе установления защищенных соединений.
- Персональный сертификат – сертификат, используемый данным пользователем ПАК «ЗАСТАВА-Клиент». Отличительной особенностью является то, что локальный сертификат хранится на токене вместе с соответствующим закрытым ключом. Наличие закрытого ключа позволяет осуществлять двустороннюю криптографическую аутентификацию при установлении соединений с другими хостами защищенной корпоративной сети на базе протокола IKEv2.
- Прочие сертификаты – сертификаты, используемые данным ПАК «ЗАСТАВА-Клиент». Отличительной особенностью является то, что данные сертификаты выкладывается без соответствующего закрытого ключа и их нельзя отнести к обозначенным типам сертификатов.
- Промежуточные сертификаты – сертификаты, используемые данным ПАК «ЗАСТАВА-Клиент». Отличительной особенностью является то, что это CA-сертификаты промежуточных УЦ, выданные промежуточным сертифицирующим органом (CA – certification authority).

ПАК «ЗАСТАВА-Клиент» поддерживает СОС. Более полная информация приведена в п. 4.7.7.

4.7.1. 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, панель инструментов и вкладки, разделенные по типам сертификатов (см. Рисунок 16).

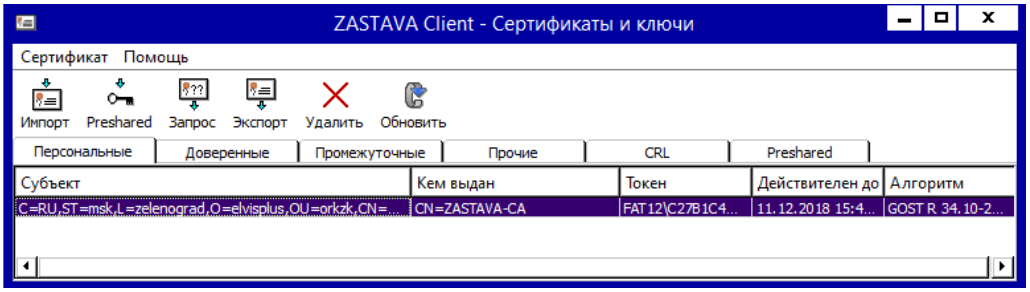


Рисунок 16 – Окно «Сертификаты и Ключи»

4.7.1.1. Вкладки окна «Сертификаты и ключи»

Окно «Сертификаты и ключи» содержит вкладки с зарегистрированными сертификатами, разделенные 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 19).

Таблица 19 – Вкладки окна «Сертификаты и ключи» и их содержание

Тип объекта	Характеристика
Персональные	Персональные сертификаты (обычно один)
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

4.7.1.2. Строка меню

Строка меню содержит следующие меню: «Сертификаты», «Помощь». Команды меню представлены в таблице (см. Таблица 20).

Таблица 20 – Команды меню

Команда	Действие
Сертификаты	
Импорт сертификата	Запускает мастер Импорта сертификатов, который помогает импортировать сертификат, СОС из файловой системы или из токена
Импорт предопределенного ключа	Запускает мастер Импорта предварительно распределенных ключей
Генерация запроса сертификата	Запускает мастер Генерации запроса сертификата
Экспорт сертификата	Запускает мастер Экспорта сертификатов, который помогает экспортировать любой сертификат.
Обновить	Обновляет список сертификатов, зарегистрированных сертификатов. Если окно «Сертификаты и ключи» открыто, когда активизирована ЛПБ, то

Команда	Действие
	сертификаты, полученные в течение IKE-обмена, не обновляются автоматически. СОС, полученные автоматически от сервера LDAP, также не показываются. Нажатие кнопки «Обновить» гарантирует то, что Вы видите наиболее свежую информацию
Помощь	
Работа с сертификатами и ключами	Открывает раздел справки «Работа с сертификатами и ключами»
Помощь	Вызов общей Справочной системы ПАК «ЗАСТАВА-Клиент»

4.7.1.3. Панель инструментов окна «Сертификаты и ключи»

Описание кнопок панели инструментов приведено в таблице (см. Таблица 21). Функции этих кнопок соответствуют функциям элементов меню (см. п. 4.7.1.2).

Таблица 21 – 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 зарегистрированных сертификатов

4.7.2. Характеристики сертификатов

4.7.2.1. Свойства сертификата

Для просмотра свойств сертификата нужно выбрать его в соответствующей вкладке (Персональные, Доверенные и т.д.) и дважды нажать на него правой клавишей мыши или воспользоваться клавишей <Enter>. Характеристики сертификата приведены в таблице (см. Таблица 22).

Таблица 22 – Характеристики сертификата

Параметр	Характеристика
Версия	Версия сертификата
Серийный номер	Серийный номер сертификата
Издатель	Кем выдан сертификат
Субъект	Содержит отличительное имя субъекта, то есть, владельца закрытого ключа, соответствующего открытому ключу данного сертификата. Субъектом сертификата может выступать УЦ, регистрационный центр (РЦ) или конечный субъект
Алгоритм подписи	Алгоритм цифровой подписи сертификата
Key Algorithm	Тип открытого ключа (алгоритм цифровой подписи и длина)

Параметр	Характеристика
Алгоритм ключа	Значение открытого ключа
Действителен с	Начальная дата действия сертификата
Действителен до	Конечная дата действия сертификата
Закрытый ключ действителен до	Конечная дата действия закрытого ключа
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).

4.7.2.2. Свойства запроса на регистрацию сертификата

Характеристики запроса на регистрацию сертификата приведены в таблице (см. Таблица 23).

Таблица 23 – Характеристики запроса на регистрацию сертификата

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
Раздел «Субъект» (информация о владельце сертификата)	
E-mail (E)	Адрес электронной почты
Название (CN)	Псевдоним УЦ
Фамилия (SN)	Фамилия физического лица, действующего от имени юридического лица владельца сертификата
Имя (GN)	Имя физического лица, действующего от имени юридического лица владельца сертификата
Подразделение (OU)	Наименование подразделения организации
Организация (O)	Наименование организации
Населенный пункт (L)	Наименование населенного пункта по адресу местонахождения организации
Субъект (ST)	Область расположения
Код страны (C)	Страна
Раздел «Альтернативное имя субъекта» (характеризует издателя сертификата)	

Параметр	Характеристика
IP-адрес	IP-адрес
DNS	DNS-сервер
E-mail	Адрес электронной почты
UPN	Дополнительное имя субъекта
Область использования ключа	Область использования ключа
Флаг «Пометить закрытый ключ как экспортируемый, если это возможно»	Закрытый ключ сертификата помечается как экспортируемый
Флаг «Подписать запрос с помощью сертификата»	Запрос подписывается выбранным сертификатом

4.7.2.3. Состав предварительно распределенных ключей

Состав предварительно распределенных ключей приведен в таблице (см. Таблица 24).

Таблица 24 – Состав предварительно распределенных ключей

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

4.7.2.4. Состав списка отозванных сертификатов

В окне «Сертификаты и ключи» во вкладке CRL отображается информация о COC, параметры и характеристики приведены в таблице (см. Таблица 25).

Таблица 25 – Информация о COC

Параметр	Характеристика
Кем выдан	Имя УЦ, который издал данный сертификат
Токен	Устройство, на котором будет сохранен COC
Последнее обновление	Дата и время издания COC (дата его последнего обновления УЦ), время задано по Гринвичу (GMT)
Следующее обновление	Дата и время очередного планового обновления COC УЦ, время по GMT. По истечении данной даты/времени COC будет считаться недействительным
Алгоритм	Тип открытого ключа (алгоритм цифровой подписи)

4.7.3. Регистрация и удаление сертификата

4.7.3.1. Регистрация сертификата

В ПАК «ЗАСТАВА-Клиент» может регистрироваться два типа X.509 сертификатов: Доверенные и Персональные (для получения информации о типах сертификатов см. п. 4.7.1.1).

Чтобы зарегистрировать новый сертификат (Доверенный или Персональный) в ПАК «ЗАСТАВА-Клиент», необходимо сделать следующее:

1) нажать кнопку  «Импорт» или выбрать элемент «Импорт сертификата» из меню «Сертификат». Запустится программный Мастер;
2) в появившемся окне выбрать необходимый для установки сертификат и нажать кнопку «Открыть» (см. Рисунок 17);

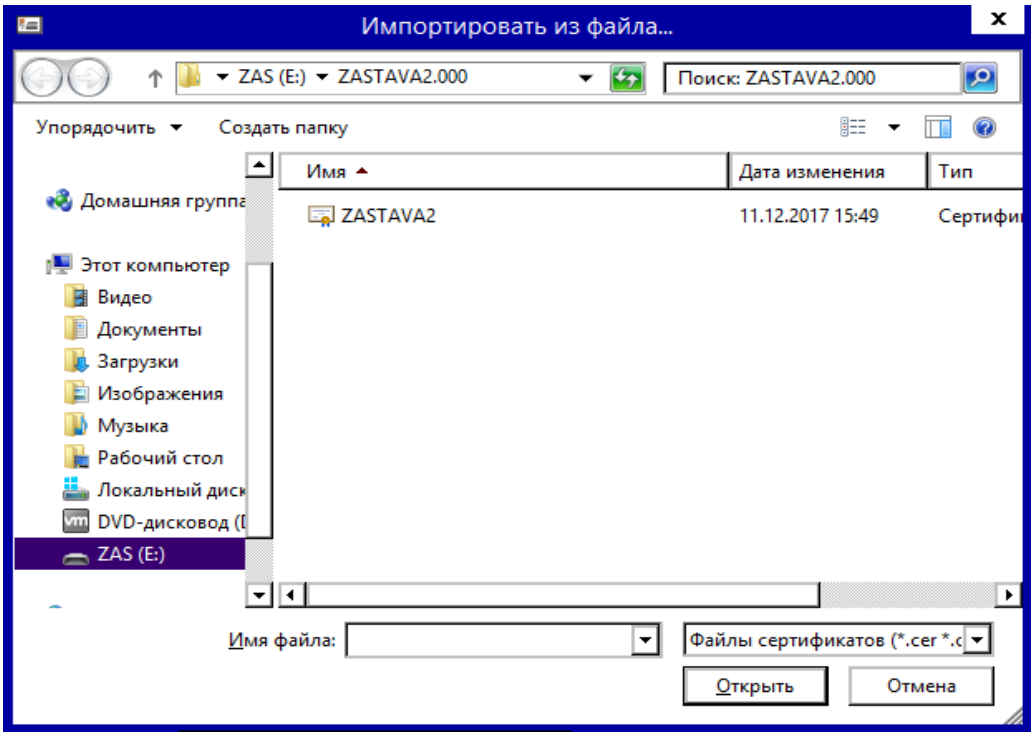


Рисунок 17 – Выбор импортированного объекта

3) режим импорта будет выбран автоматически, в соответствии с типом сертификата. Нажать кнопку «Далее» (см. Рисунок 18);

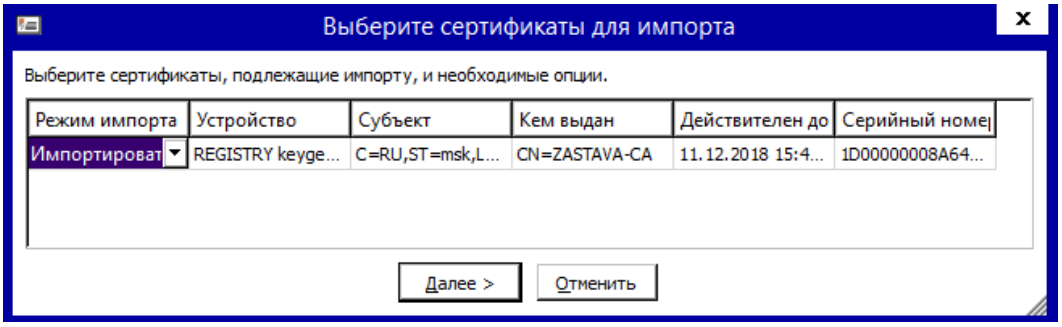


Рисунок 18 – Выбор режима импорта сертификата

4) при успешном импортировании появится индикатор (см. Рисунок 19), а в окне результатов импорта будет отображён импортированный сертификат. Нажать кнопку «Готово»;

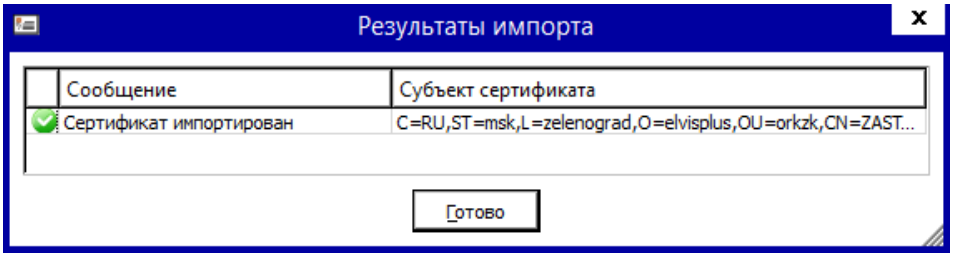


Рисунок 19 – Окно результата импортирования сертификата

5) зарегистрированный сертификат теперь включен в таблицу окна «Сертификаты и Ключи»;

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

6) при импорте одного или более сертификатов из файла в формате PKCS#12 необходимо ввести пароль для доступа к этому файлу. В некоторых случаях на данном этапе необходимо вводить ПИН-код токена, на котором хранится контейнер с сертификатом (-ами). Мастер будет отображать сертификат, который выбран для регистрации:

— при регистрации сертификата УЦ в поле «Режим импорта» (см. Рисунок 20) необходимо назначить статус «Доверенный», после чего нажать кнопку «Далее»;

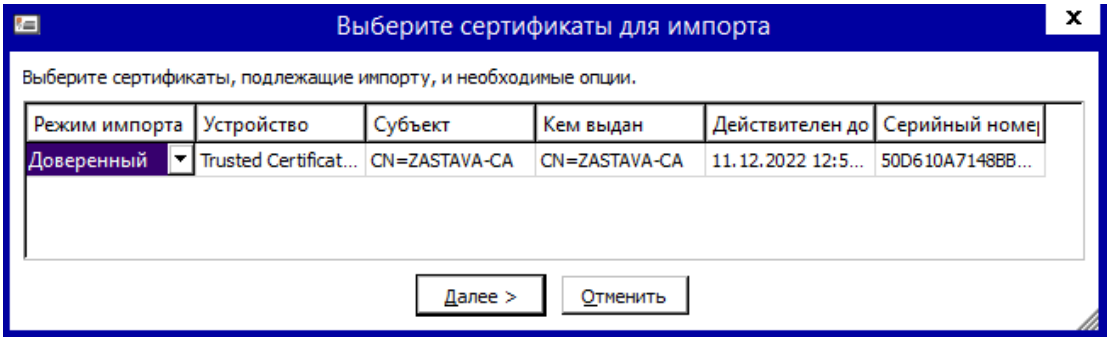


Рисунок 20 – Выбор режима импорта сертификата для регистрации Доверенного сертификата

— необходимо ввести ПИН-код токена (см. Рисунок 21), в котором будет содержаться сертификат. После ввода ПИН-кода нажать кнопку «Готово».

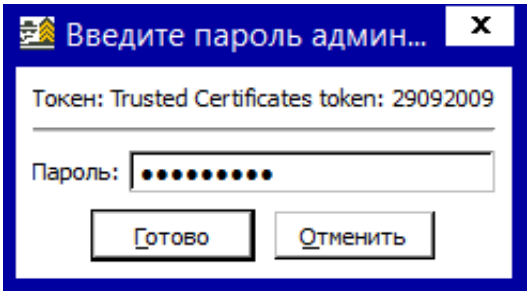


Рисунок 21 – Ввод пароля токена

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

Если сертификат УЦ был получен через незащищённый канал (например, по электронной почте) и Вы хотите сохранить его, как «Доверенный», необходимо проверить подлинность этого сертификата вручную. Непосредственно после регистрации сертификата в ПАК «ЗАСТАВА-Клиент» надо связаться с уполномоченным представителем УЦ, чтобы сравнить сигнатуру (fingerprint) оригинального сертификата УЦ с сигнатурой полученного сертификата, которая отображается в полях «Fingerprint» в таблице сертификатов ПАК «ЗАСТАВА-Клиент». Если сигнатуры не совпадают, надо немедленно удалить сертификат из ПАК «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.

Если открыта сессия связи с токеном, в окне «Сертификаты и ключи» автоматически отображаются объекты сертификата, содержащиеся на токене. Все эти сертификаты имеют статус «Доверенный». Вы можете сохранять сертификат УЦ как «Доверенный». Сертификаты партнёров по связи, импортированные из токенов, будут всегда проверяться по цепочке доверия.

Чтобы создать локальный сертификат при помощи внешнего УЦ, необходимо создать запрос на регистрацию сертификата, см. п. 4.7.5.1. Запрос на регистрацию сертификата будет создан и сохранён в ПАК «ЗАСТАВА-Клиент» вместе с соответствующим личным ключом (генерируется одновременно с созданием запроса). Перешлите созданный запрос на регистрацию сертификата в УЦ. Когда Вы будете импортировать сертификат, полученный из УЦ, в ПАК «ЗАСТАВА-Клиент» этот сертификат заменит соответствующий запрос на регистрацию сертификата и будет автоматически связан с личным ключом.

4.7.3.2. Удаление сертификата

Для удаления сертификата из ПАК «ЗАСТАВА-Клиент» надо выделить сертификат, который требуется удалить, в окне «Сертификаты и ключи» нажать на панели инструментов в окне «Сертификаты и ключи» кнопку «Удалить». Сертификат будет удален из ПАК «ЗАСТАВА-Клиент».

Если срок действия сертификата, находящегося в ПАК «ЗАСТАВА-Клиент», закончился, данный сертификат будет автоматически удалён из окна «Сертификаты и ключи» после проверки. Однако это не относится к локальным сертификатам (с личными ключами).

4.7.4. Экспорт сертификата

Для 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 22). 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»;

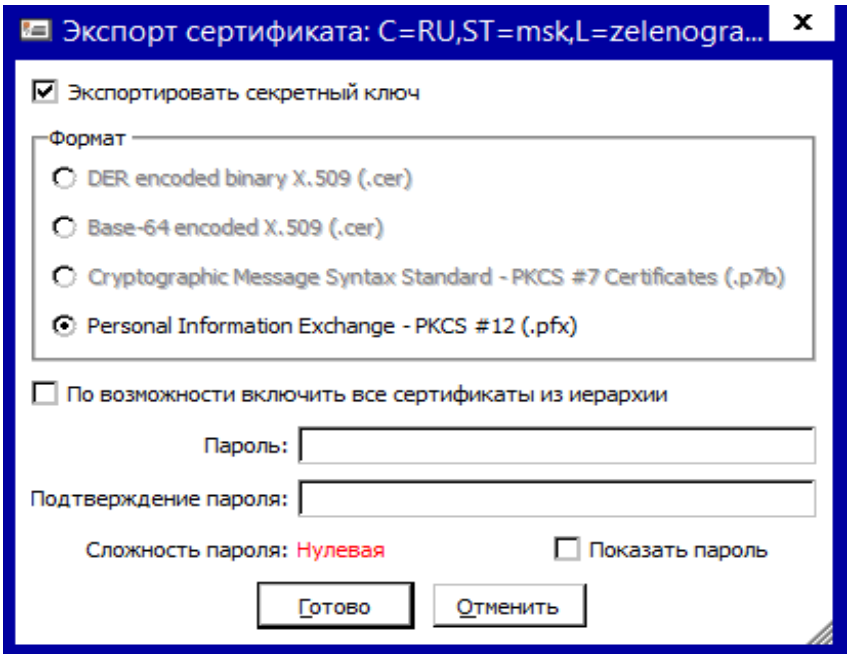


Рисунок 22 – Параметры экспорта сертификата

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

4.7.5. Запросы на регистрацию сертификата

Существует несколько способов получить локальный сертификат для ПАК «ЗАСТАВА-Клиент». Например, можно импортировать сертификат вместе с его личным ключом из файловой системы, как описано в п. 4.7.3.1.

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

4.7.5.1. Создание запроса на регистрацию сертификата

Для того чтобы создать запрос на регистрацию сертификата, необходимо выполнить следующие операции:

1) нажать кнопку  «Запрос» или выбрать команду меню «Сертификат» → «Генерация запроса сертификата»;
2) в появившемся окне «Создание Запроса на Регистрацию Сертификатов» заполнить необходимые поля (см. Рисунок 23):

— 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. 4.7.5.2). 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 запрос на регистрацию сертификата;
— 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»;
— нажать кнопку «Готово»;

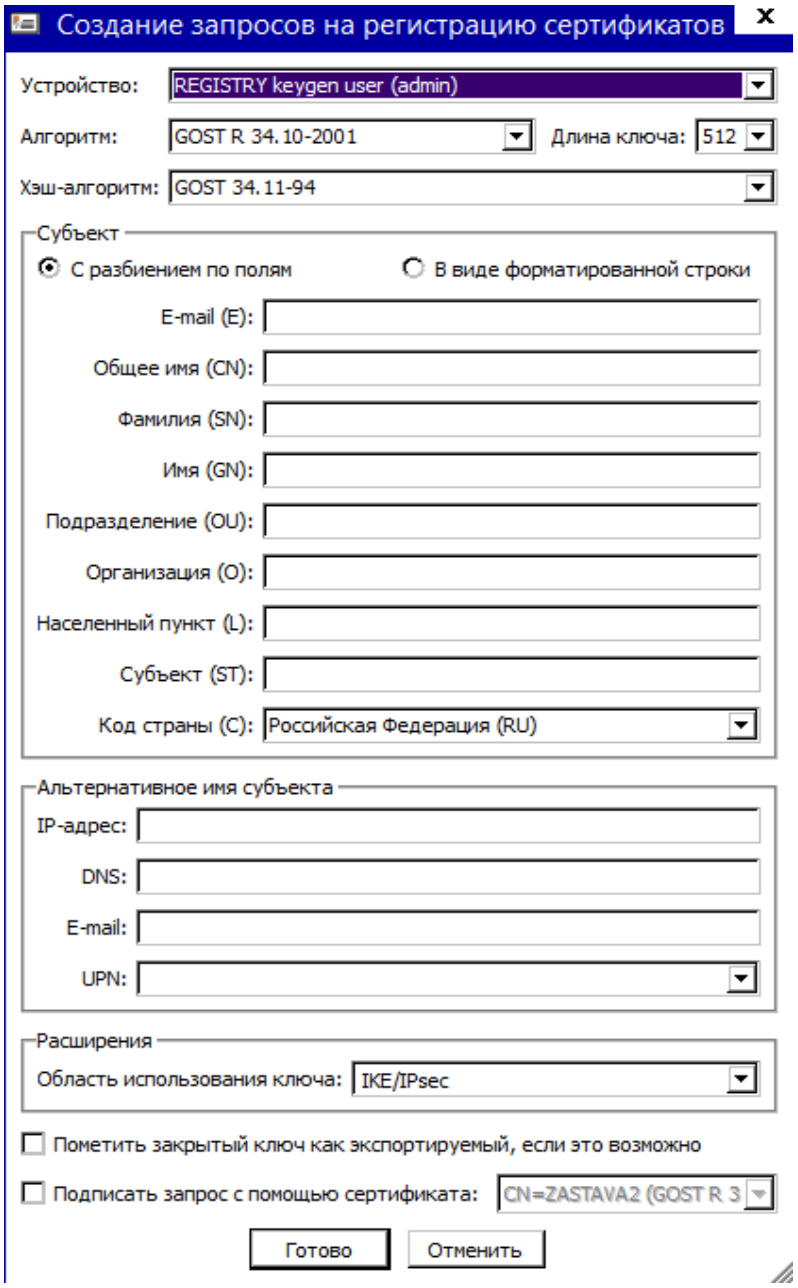


Рисунок 23 – Ввод информации для создания запроса на регистрацию сертификата

3) по запросу ввести ПИН-код (пароль) устройства, на котором генерируется ключевая пара;
4) появится окно со сформированным запросом на получение сертификата (см. Рисунок 24). Запрос на регистрацию сертификата и соответствующий ему закрытый ключ будут сохранены в ПАК «ЗАСТАВА-Клиент», в таблице появится соответствующая строка с именем субъекта «Key Pair without Certificate»;

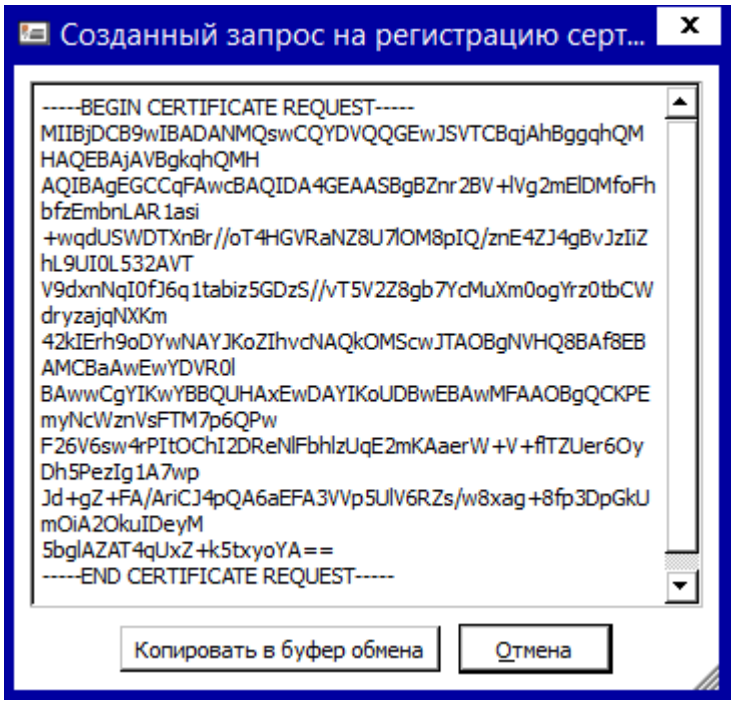


Рисунок 24 – Копирование запроса на регистрацию сертификата в буфер обмена

5) скопировать текст запроса в буфер обмена, нажав кнопку «Копировать в буфер обмена»;
6) отправить созданный запрос в УЦ (с помощью веб-браузера, электронной почты или других средств);
7) после получения сертификата от УЦ его необходимо импортировать в ПАК «ЗАСТАВА-Клиент», как это описано в п. 4.7.3.1. После того, как сертификат будет импортирован, он заменит собой соответствующий запрос на регистрацию сертификата в окне «Сертификаты и ключи» ПАК «ЗАСТАВА-Клиент» и будет автоматически связан со своим закрытым ключом.

4.7.5.2. Формат строки уникального имени (DN)

При использовании Уникального Имени (DN) в запросе на регистрацию сертификата необходимо ввести значения DN в формате, описанном в этом подпункте. Должны быть использованы только те значения, которые необходимы для создания запроса на регистрацию сертификата, в следующем формате:

```
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 26).

Таблица 26 – Типы атрибутов

Типы атрибутов	Наименование	Расшифровка
E	E-mail	Адрес электронной почты*
CN	Subject Common Name	Общее имя (псевдоним УЦ)
SN	Subject Surname	Фамилия
GN	Subject Given Name	Имя
OU	Subject Organizational Unit	Название подразделения организации
O	Subject Organization	Название организации
L	Subject Locality	Район расположения
ST	Subject State or Province	Область расположения
C	Subject Country	Страна
Примечание. * – Все перечисленные атрибуты относятся к владельцу сертификата (поле «Субъект»).		

При определении значений атрибутов DN рекомендуется использовать только буквы латинского алфавита и цифры. Некоторые символы имеют специальное значение в строке DN и должны использоваться 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-децимальный» 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 VPN-агенты иных производителей распознают сертификаты удаленных партнеров по связи, только если атрибуты DN расположены в определенном порядке. После получения сертификата от УЦ необходимо убедиться в том, что ПАК «ЗАСТАВА-Клиент» способно корректно взаимодействовать со всеми видами Агентов, необходимыми для работы.

В ПАК «ЗАСТАВА-Клиент» атрибуты DN-сертификатов расположены в том же порядке, в котором они указаны в сертификате. Во многих аналогичных программных изделиях иных 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).

4.7.5.3. Удаление запроса на регистрацию сертификата

Для того чтобы удалить из ПАК «ЗАСТАВА-Клиент» запрос на регистрацию сертификата, необходимо выделить его в окне «Сертификаты и ключи», затем нажать на панели инструментов в окне «Сертификаты и ключи» кнопку «Удалить». Запрос будет удален из ПАК «ЗАСТАВА-Клиент».

4.7.6. Предварительно распределенные ключи

Как и сертификаты, предварительно распределенные ключи позволяют проводить аутентификацию при установлении защищенного соединения с удаленным партнером по связи. Эта процедура аутентификации будет успешной, если партнеры по информационному обмену имеют предварительно распределенный ключ с одинаковым значением (эти значения должны быть согласованы с партнером заранее). Если ключи не совпадают, защищённое соединение 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 по связи.

При использовании предварительно распределённых ключей должны быть зарегистрированы, как минимум, сертификаты, используемые для проверки целостности ЛПБ.

4.7.6.1. Регистрация предварительно распределенного ключа

Чтобы зарегистрировать предварительно распределенный ключ в ПАК «ЗАСТАВА-Клиент», необходимо выполнить следующее:

1) нажать кнопку «» «Preshared» из меню «Сертификат». Запустится программный Мастер;
2) в появившемся окне «Preshared Key» (см. Рисунок 25) в поле «Имя ключа» ввести уникальное имя ключа. Это имя будет использовано в качестве идентификатора в ЛПБ;

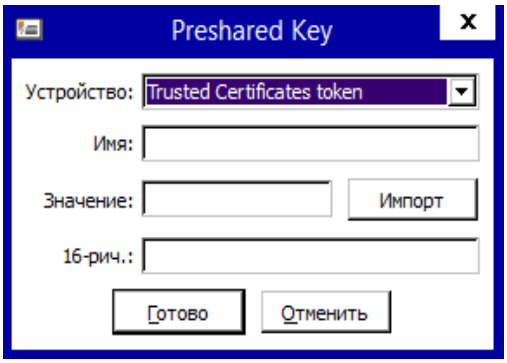


Рисунок 25 – Ввод параметров предварительно распределенного ключа

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

3) ввести значение ключа в поле «Значение» или в поле «16-рич.», нажать кнопку «Импорт» и выбрать файл и сохранить значение предварительно распределенного ключа;
4) теперь в Мастере ключей отображается предварительно распределенный ключ, готовый к регистрации. Нажать кнопку «Готово». Зарегистрированный предварительно распределенный ключ теперь включен в таблицу вкладки «Preshared Key» окна «Сертификаты и Ключи».

4.7.6.2. Удаление предварительно распределенного ключа

Для удаления предварительно распределенного ключа из ПАК «ЗАСТАВА-Клиент» необходимо выделить его в таблице вкладки «Preshared Key» окна «Сертификаты и Ключи», нажать на панели инструментов в окне «Сертификаты и ключи» кнопку «Удалить». Ключ будет удален из таблицы и из ПАК «ЗАСТАВА-Клиент».

4.7.7. 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.

Каждый СОС выпускается определенным УЦ и содержит только сертификаты, аннулированные данным УЦ. Любой СОС имеет силу в течение периода времени, указанного в СОС: с даты (и времени) создания СОС до даты (и времени) следующего намеченного изменения СОС. Значения времени заданы по Гринвичу; текущий часовой пояс будет принят во внимание при вычислении периода действия СОС. Как только этот период закончится, ПАК «ЗАСТАВА-Клиент» должно получить новый СОС. СОС может быть импортирован в ПАК «ЗАСТАВА-Клиент» либо автоматически (из внешнего сервера, при помощи протокола LDAP), либо вручную.

В большинстве случаев ПАК «ЗАСТАВА-Клиент» автоматически сверяет сертификаты с СОС. Всякий раз, когда сертификат получен от партнёра по связи по протоколу IKE, ПАК «ЗАСТАВА-Клиент» сначала попытается найти необходимый СОС. При отсутствии СОС или в случае, если срок действия имеющегося СОС истек, ПАК «ЗАСТАВА-Клиент» соединится с LDAP ПАК «ЗАСТАВА-Клиент», чтобы получить обновленный СОС. Если сертификат партнёра по связи или соответствующий сертификат УЦ указан в СОС, или требуемый СОС недоступен, связь с партнером не будет установлена. Если в текущей ЛПБ обработка СОС выключена, сертификаты не будут проверяться по СОС. Для получения информации о проверке сертификатов по СОС см. п. 4.7.7.2.

4.7.7.1. Обработка СОС

При проверке валидности сертификата ПАК «ЗАСТАВА-Клиент» путем просмотра СОС (CRL) удостоверяется то, что сертификат не аннулирован. СОС может быть импортирован в ПАК «ЗАСТАВА-Клиент» или автоматически (из внешнего ПАК «ЗАСТАВА-Клиент», используя протокол LDAP), или вручную.

Если в текущей ЛПБ обработка СОС выключена, эта проверка не будет выполняться (сертификат получит статус «Проверенный», если он действительно подтвержден сертификатом УЦ и может быть проверен по цепочке доверия). Если активная ЛПБ допускает обработку СОС (параметр CRL processing, установлен в значение «ENABLE» или «ENABLE_SOFT»), возможны следующие ситуации:

— [Сертификат содержит поле «Точки распространения СОС» (CRL Distribution Point)]. Сначала ПАК «ЗАСТАВА-Клиент» будет искать требуемый СОС среди зарегистрированных. Если требуемый СОС найден, сертификат будет проверен по этому СОС. Если нет требуемого СОС среди зарегистрированных, ПАК «ЗАСТАВА-Клиент» сделает попытку получить его с LDAP-сервера, указанного в СОС. Если требуемый СОС недоступен, соединение с партнером, приславшим этот сертификат, не будет устанавливаться;

— [Сертификат не содержит поле «Точки распространения СОС», но соответствующий СОС зарегистрирован в ПАК «ЗАСТАВА-Клиент»]. Если этот СОС действителен, то сертификат будет проверен по этому СОС. Если у СОС истек срок действия, ПАК «ЗАСТАВА-Клиент» сделает попытку получить СОС с LDAP-сервера, указанного в ЛПБ. Если требуемый СОС недоступен, соединение с партнером, приславшим этот сертификат, не будет устанавливаться;

— [Сертификат не содержит поле «Точки распространения СОС» и соответствующий СОС не зарегистрирован в ПАК «ЗАСТАВА-Клиент»]. ПАК «ЗАСТАВА-Клиент» не проверяет аннулирован ли сертификат. Если сертификат подтверждается допустимым сертификатом УЦ и может быть проверен по цепочке доверия, соединение с партнером, приславшим этот сертификат, будет устанавливаться.

Когда устанавливается защищенное соединение (SA), ПАК «ЗАСТАВА-Клиент» будет автоматически выполнять действия, описанные выше.

4.7.7.2. Проверка сертификата

Проверить сертификат, зарегистрированный в ПАК «ЗАСТАВА-Клиент», можно, отображая его цепочку доверия (т.е. список УЦ, подтверждающих подлинность сертификата). Данную цепочку можно просмотреть в окне «Сертификаты и Ключи», выбрав на соответствующей вкладке требуемый для проверки сертификат и нажав на нем дважды правой клавишей мыши. В верхней части окна «Параметры сертификата» будет показана Иерархия сертификата.

Удостоверьтесь в том, что дата, время и настройки часового пояса правильно установлены на используемом СВТ. Неправильная установка данных параметров может привести к тому, что сертификаты или СОС будут отмечены как недействительные.

Если активная ЛПБ допускает обработку СОС (параметр CRL processing установлен в значение «ENABLE» или «ENABLE_SOFT»), ПАК «ЗАСТАВА-Клиент» будет пытаться удостовериться в том, что сертификат не аннулирован. Для получения дополнительной информации см. п. 4.7.7.1.

4.8. Окно «Управление политиками»

Окно «Управление политиками» предназначено для редактирования списка ЛПБ и установки опций ЛПБ (см. Рисунок 26). Для получения информации о ЛПБ см. п. 4.8.3. Для получения информации об особенностях создания ЛПБ см. п. 4.8.5.

ЛПБ является текстовым файлом, описывающим правила, которые определяют, как ПАК «ЗАСТАВА-Клиент» связывается с другими объектами в защищённой среде. В результате ЛПБ может быть установлена, активирована и просмотрена.

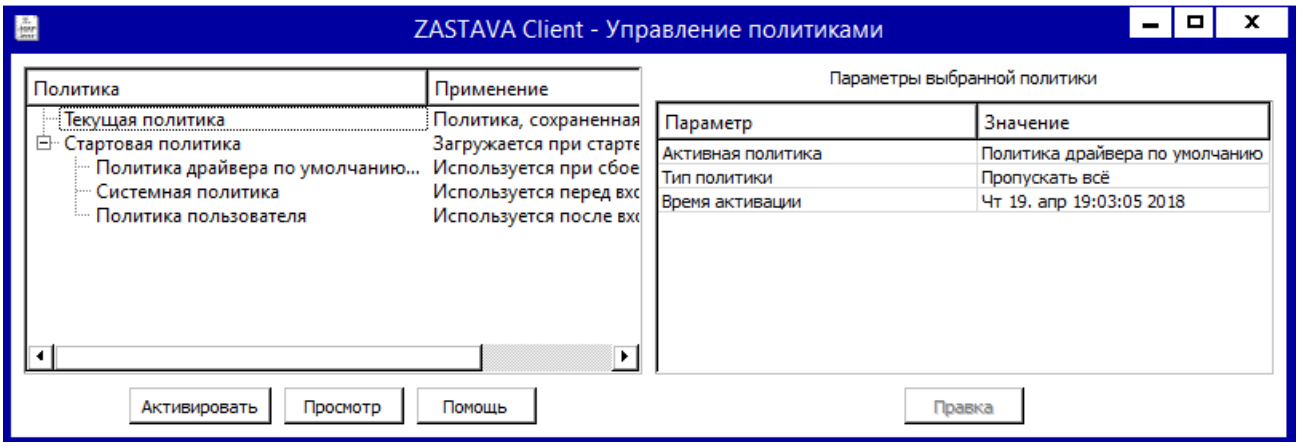


Рисунок 26 – Окно «Управление политиками»

4.8.1. Структура окна «Управление политиками»

Окно «Управление политиками» состоит двух областей:

— левая область с деревом политик;

— правая область с параметрами выбранной политики.

В графе «Политика» содержит дерево существующих политик. При выделении политики в дереве политик в области «Параметры выбранной политики» будут отображаться параметры политики. Графа «Политика» содержит также кнопки «Активировать», «Просмотр» и «Помощь».

4.8.2. Типы политик

В графе «Политика» существуют следующие типы политик:

— текущая – политика, сохраняемая в драйвере ПАК «ЗАСТАВА-Клиент»;

— стартовая – политика, загружаемая при старте ОС. Виды стартовой политики:

а) политика драйвера по умолчанию (DDP) – политика, загружаемая при сбое;

б) системная – политика, используемая перед входом и после выхода пользователя;

в) политика пользователя – политика, используемая после входа пользователя в ОС.

4.8.3. Параметры политик ПАК «ЗАСТАВА-Клиент»

4.8.3.1. Системная ЛПБ

Системная политика может быть получена из файла, с сервера или быть равной политике драйвера по умолчанию.

Для изменения параметров системной политики необходимо в окне «Управление политиками» выполнить шаги представленные на рисунке (см. Рисунок 27).

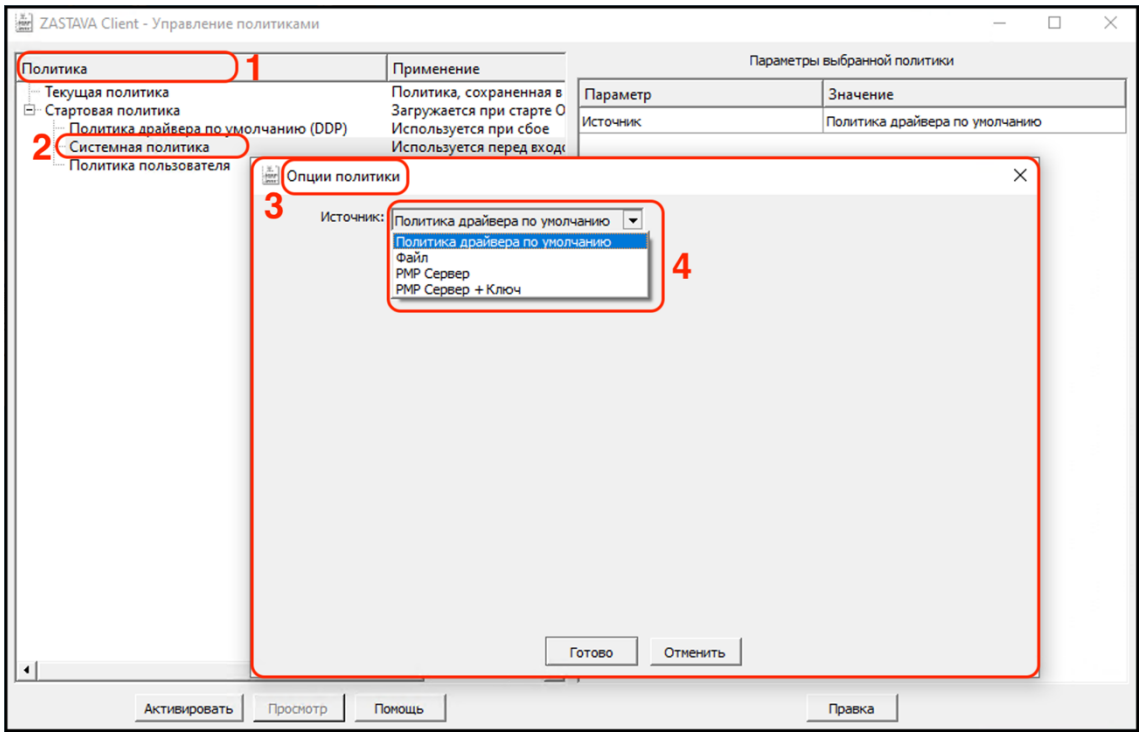


Рисунок 27 – Настройка параметров системной политики

Для настройки параметров системной политики требуется перейти в графу «Политика» (цифра 1). Выбрать в дереве и нажать дважды левой клавишей мыши на строку «Системная политика» (цифра 2). В открывшемся окне настроек «Опции политики» (цифра 3) открыть выпадающий список вариантов настроек (цифра 3).

Для настройки системной политики необходимо выбрать тип метода активации:

1) «Политика драйвера по умолчанию» и определить параметры данного метода как представленно на рисунке (см. Рисунок 28).

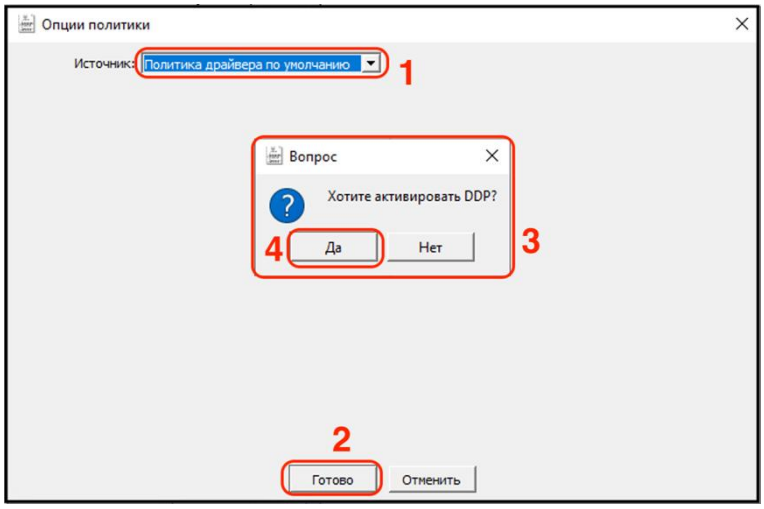


Рисунок 28 – Тип метода активации «Политика драйвера по умолчанию»

Выбрать метод «Политика драйвера по умолчанию» (цифра 1) нажать кнопку «Готово» (цифра 2). В открывшемся окне «Вопрос» (цифра 3) нажать кнопку «Да» (цифра 4);

2) «Файл» и определить параметры данного метода как представленно на рисунке (см. Рисунок 29).

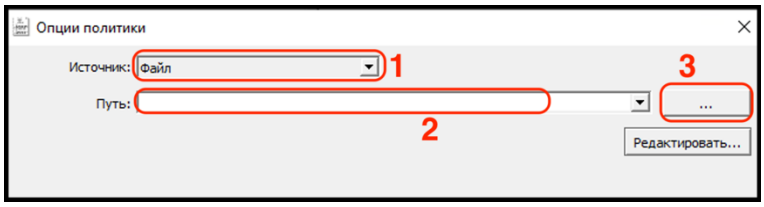


Рисунок 29 – Тип метода активации «Файл»

Выбрать метод «Файл» (цифра 1), в открывшемся поле «Путь» (цифра 2) указать путь к файлу с политикой или выбрать необходимый файл, нажав кнопку «…» (цифра 3);

⚠	Политика безопасности не должна задаваться из файла! Политика безопасности должна быть прогружена строго с сервера ПО «ЗАСТАВА-Управление».
⚠	С помощью кнопки «Редактировать» при выборе метода активации из файла можно произвести изменение файла политики в окне «Редактор».

3) «PMP Сервер» для установки SA и определить параметры данного метода, выполнив шаги настроек как представленно на рисунке (см. Рисунок 30).

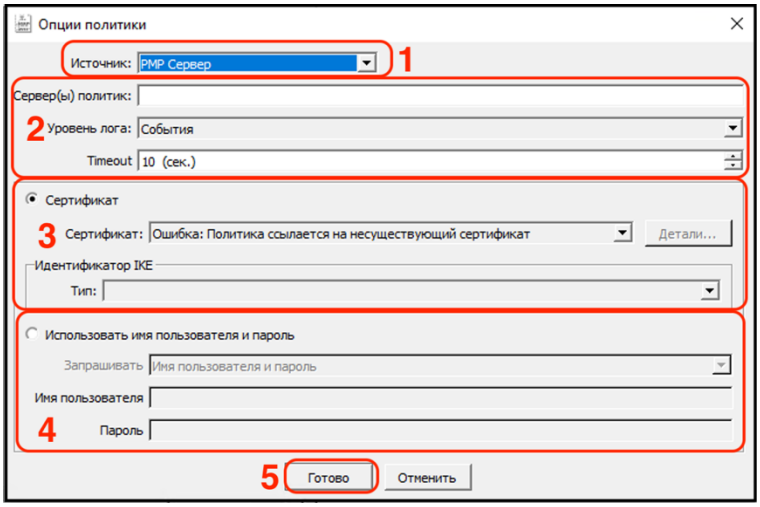


Рисунок 30 – Тип метода активации «PMP Сервер»

а) Выбрать метод «PMP Сервер» (цифра 1), в открывшемся блоке выполнить следующие настройки (цифра 2):

— 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;

— для журналирования сообщений при передаче ЛПБ с сервера политики необходимо выбрать уровень подробности регистрации событий в поле «Уровень лога»;

— отметить время, через которое необходимо обращаться к серверу за ЛПБ, в поле «Timeout»;

б) В блоке настроек «Сертификат» (цифра 3) выбрать:

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

— в поле «Идентификатор IKE» выбрать тип IKE идентификатора для прогрузки политики, согласованного с ПО «ЗАСТАВА-Управление». Идентификатор IKE бывает нескольких видов: DN, DNS, E-mail, IP. DN – использование данных о субъекте импортированного сертификата. Для использования альтернативного имени субъекта (которое указывается в сертификате) необходимо выбирать оставшиеся три типа идентификатора IKE – DNS, E-mail, IP;

в) В блоке настроек «Использовать имя пользователя и пароль (цифра 3) при необходимости вввести в соответствующие поля требуемые данные;

г) Нажать кнопку «Готово». Сохранение опций политики требует введения пароля администратора;

д) Для активации политики надо нажать в появившемся после сохранения параметров политики информационном окне кнопку «Да». Если активировать политику не требуется, нажать кнопку «Нет».

4) «PMP Сервер+Ключ» и определить параметры данного метода как представленно на рисунке (см. Рисунок 31).

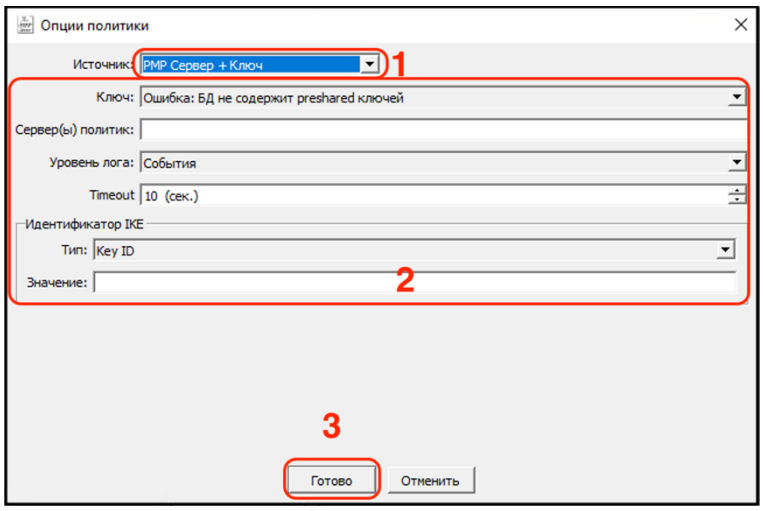


Рисунок 31 – Тип метода активации «PMP Сервер+Ключ»

а) Выбрать метод «PMP Сервер+Ключ» (цифра 1), в открывшемся блоке выполнить следующие настройки (цифра 2):

— выбрать ключ;

— 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;

— для журналирования сообщений при передаче ЛПБ с сервера политики необходимо выбрать уровень подробности регистрации событий в поле «Уровень лога»;

— отметить время, через которое необходимо обращаться к серверу политики за ЛПБ, в поле «Timeout»;

б) В блоке настроек «Сертификат» (цифра 3) выбрать:

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

— в поле «Идентификатор IKE» выбрать тип IKE идентификатора для прогрузки политики, согласованного с ПО «ЗАСТАВА-Управление». Идентификатор IKE бывает нескольких видов: DN, DNS, E-mail, IP. DN – использование данных о субъекте импортированного сертификата. Для использования альтернативного имени субъекта (которое указывается в сертификате), необходимо выбирать оставшиеся три типа идентификатора IKE – DNS, E-mail, IP;

в) Нажать кнопку «Готово». Сохранение опций политики требует введения пароля администратора;

г) Для активации политики нажать в появившемся после сохранения параметров политики информационном окне кнопку «Да». Если активировать политику не требуется, нажать кнопку «Нет».

4.8.3.2. Политика пользователя

Политика пользователя – это 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 графе «Политика» нажать дважды левой клавишей мыши и выбрать необходимые параметры в окне «Опции политик» (см. Рисунок 32).

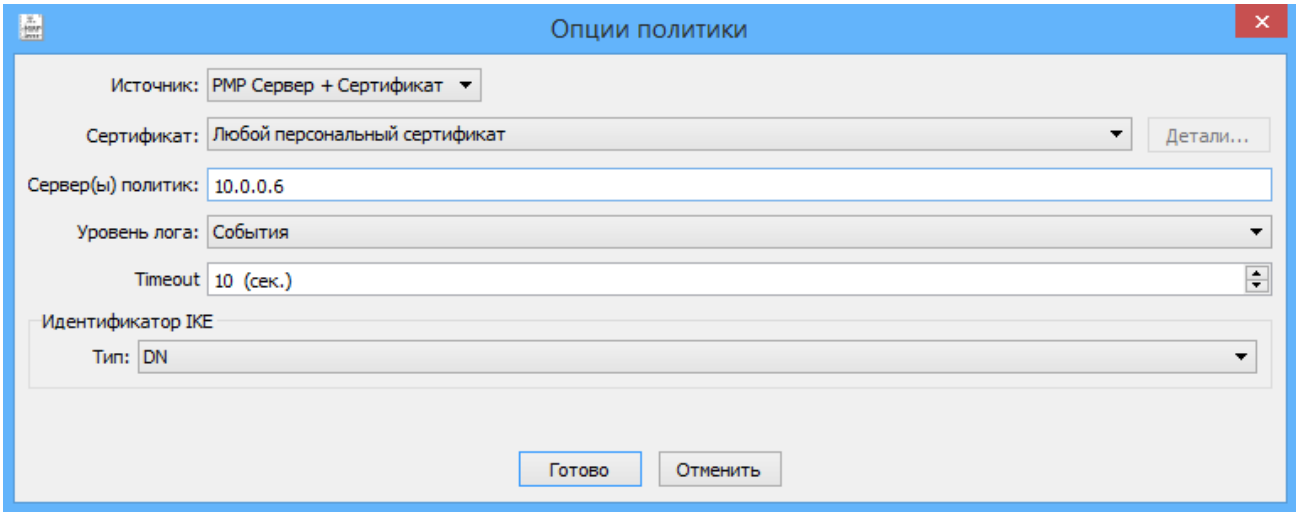


Рисунок 32 – Настройка параметров политики пользователя

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 33). Сохранение опций политики требует введения пароля администратора;

⚠	Политика безопасности не должна задаваться из файла! Политика безопасности должна быть прогружена строго с сервера ПО «ЗАСТАВА-Управление».

— при выборе метода прогрузки «Отсутствует», в случае ошибки при прогрузке пользовательской политики будет прогружаться системная политика;

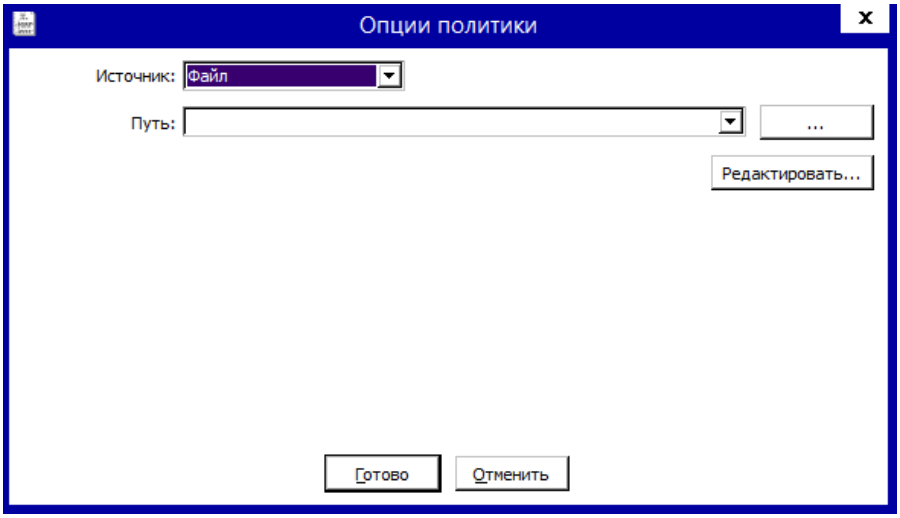


Рисунок 33 – Настройки политики пользователя при прогрузке политики из файла

— 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 32). Для настройки прогрузки пользовательской политики с сервера необходимо:

а) выбрать зарегистрированный сертификат из выпадающего списка поля «Сертификат». В данном случае должен быть выбран «Любой персональный 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.

б) ввести адрес сервера в строке «Сервер(ы) политик» и указать порт, с которого будет получена политика. Если порт не указан, то берется значение по умолчанию (500). В качестве адреса сервера политик можно использовать DNS.

Если серверов несколько, IP-адреса указываются через запятую, номер порта указывается через двоеточие;

в) для журналирования сообщений при передаче ЛПБ с сервера политики необходимо выбрать уровень подробности регистрации событий в поле «Уровень лога»;

г) отметить время, через которое необходимо обращаться к серверу политики за ЛПБ, в поле «Time out»;

д) в секции «Идентификатор IKE» выбрать тип IKE идентификатора для прогрузки политики, согласованного с ПО «ЗАСТАВА-Управление»;

2) нажать кнопку «Готово». Сохранение опций политики требует введения пароля администратора;

3) для активации политики нажать кнопку «Да» в появившемся после сохранения параметров политики информационном окне. В случае, если активация политики не требуется, нажать кнопку «Нет».

4.8.3.3. Политика драйвера по умолчанию

В ПАК «ЗАСТАВА-Клиент» имеется 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 графе «Политика» окна «Управление политиками» нажать дважды левой клавишей мыши и выбрать необходимые параметры в окне «Опции политик» (см. Рисунок 34). Доступные значения для «Политики драйвера по умолчанию»:

- «Сбрасывать все» (DROP ALL);
- «Сбрасывать все, кроме DHCP» (DROP ALL EXCEPT DHCP);
- «Пропускать все» (PASS ALL).

Для сохранения выбранных настроек надо нажать кнопку «Готово».

Из соображений безопасности рекомендуется устанавливать «Политика драйвера по умолчанию» в значение «Сбрасывать все». Необходимо учесть, что в этом случае сеть не будет доступна, если СВТ не присвоен статический IP-адрес. Если СВТ получает IP-адрес по DHCP, то нужно 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 СВТ IP-адреса).

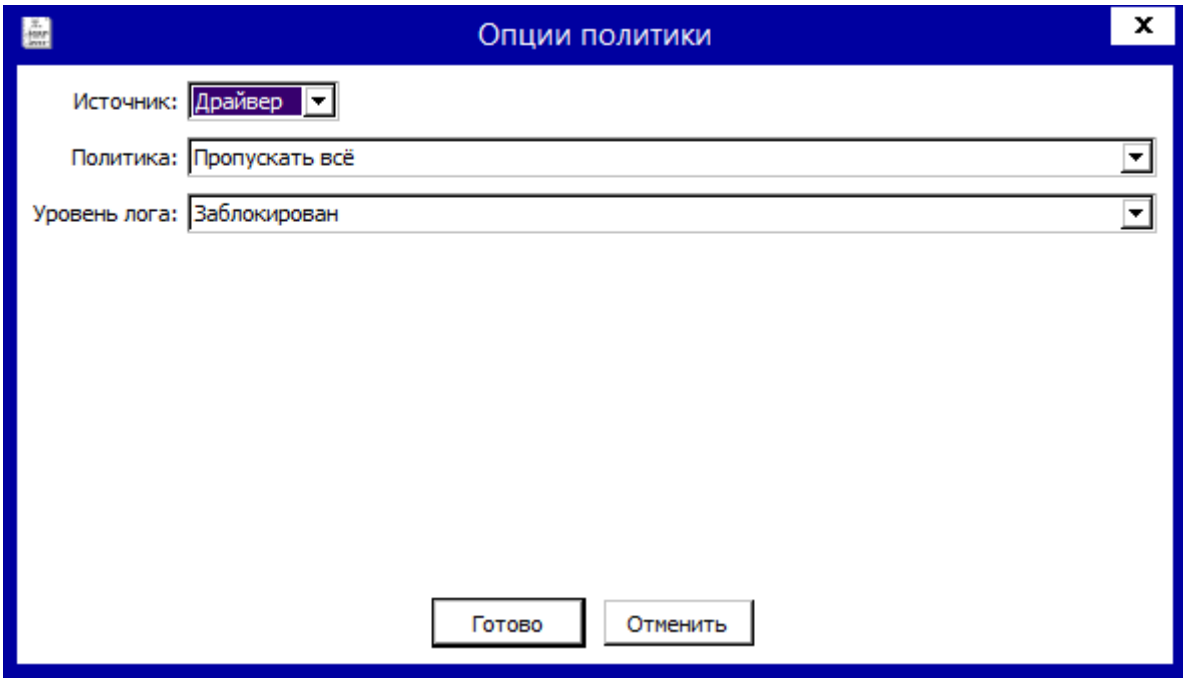


Рисунок 34 – Настройка параметров «Политика драйвера по умолчанию»

4.8.4. Изменение параметров ЛПБ

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

Для изменения доступны параметры следующих политик:

— Политика Драйвера по умолчанию (DDP);

— Системная политика;

— Политика пользователя.

Параметры «Системной политики» и «Политики Драйвера по умолчанию» можно также изменить, нажав правой клавишей мыши по выбранной в дереве политике и выбрав из выпадающего меню параметр «Правка». В появившемся окне «Опции политик» изменить необходимые параметры. Сохранение измененных параметров требует ввода пароля администратора.

4.8.5. Регистрация ЛПБ

ЛПБ создается в ПО «ЗАСТАВА-Управление» и сохраняется как текстовый файл, который затем регистрируется в ПАК «ЗАСТАВА-Клиент».

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

1) нажать кнопку «Правка»;
2) выбрать один из способов добавления ЛПБ: из поля «Источник» в окне «Опции политики» выбрать «Загрузить из файла»;

ЛПБ не рекомендуется загружать из файла! ЛПБ должна быть прогружена с сервера ПО «ЗАСТАВА-Управление».

Для загрузки ЛПБ из файла необходимо указать файл ЛПБ в текстовом формате или ввести вручную путь к файлу.

Далее необходимо выполнить следующие действия:

3) выбрать один из параметров:
   - «Сервер+Сертификат» – для загрузки ЛПБ с сервера и установки IPsec SA с помощью сертификата;
   - «Сервер+Ключ» – для загрузки ЛПБ с сервера и установки IPsec SA с помощью предварительно распределенного ключа, только для системной ЛПБ;
4) выбрать из выпадающего списка зарегистрированный сертификат или предварительно распределенный ключ в соответствии с выбранным методом прогрузки с сервера;
5) ввести IP-адрес или имя сервера в строке «Сервер(ы) политик» и порт, с которого будет получена политика. Если порт не будет указан, то берется значение по умолчанию (500). Если серверов несколько, IP-адреса указываются через запятую. Номер порта указывается через двоеточие;
6) отметить время, через которое необходимо обращаться к серверу ЛПБ, в поле «Time out»;
7) выбрать тип идентификатора в секции «Идентификатор IKE» для прогрузки политики, который должен быть согласован с ПО «ЗАСТАВА-Управление»;
8) нажать кнопку «Сохранить»;
9) для активации зарегистрированной политики после сохранения параметров нажать кнопку «Да». В случае, если активация политики не требуется, нажать кнопку «Нет».

4.8.6. Просмотр ЛПБ

В поле с деревом политик окна «Управление политиками» можно посмотреть текущую ЛПБ, для этого необходимо выбрать из дерева политик строку «Текущая политика» и нажать кнопку «Просмотр» в окне «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, выбрав в меню «Файл» команду «Сохранить» и определив путь для сохранения.

4.8.7. Активация ЛПБ

Для активации ЛПБ (т.е. для загрузки в драйвер ПАК «ЗАСТАВА-Клиент») необходимо выделить нужную политику в дереве политик окна «Управление политиками» ПАК «ЗАСТАВА-Клиент» и нажать кнопку «Активировать», ввести логин и пароль администратора. ЛПБ загрузится

в драйвер, и правила, определённые в ЛПБ, вступят в действие. Если активация прошла успешно, IP-трафик будет обрабатываться в соответствии с правилами, описанными в ЛПБ.

4.9. Окно «Токены»

Смена ПИН-кода пользователя ключевого носителя производится перед началом использования ключевого носителя, в дальнейшем смену ПИН-кода требуется производить не реже, чем один раз в шесть месяцев. Смена ПИН-кода производится с помощью ПАК «ЗАСТАВА-Клиент».

Администратор обязан хранить ПИН-код доступа к своим ключевым носителям в тайне и не имеет права сообщать ПИН-код никому.

ПАК «ЗАСТАВА-Клиент» позволяет использовать токены как среду транспортировки важной информации (сертификатов, закрытых ключей). Окно «Токены» (см. Рисунок 35) содержит список всех зарегистрированных модулей токенов.

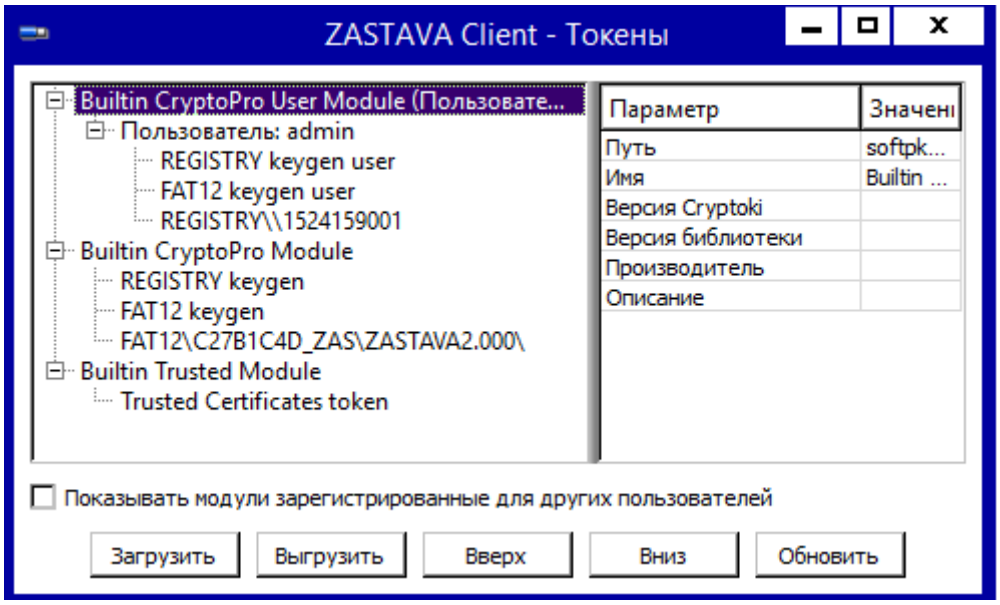


Рисунок 35 – Окно «Токены»

4.9.1. Смена ПИН-кода токена

ПИН-код может быть изменен только на активном токене (соединение с токеном должно быть открыто).

Для смены ПИН-кода необходимо:

1) открыть панель управления, нажав правой клавишей мыши на значок в системной информационной панели и выбрав пункт «Панель управления» (см. Рисунок 36);

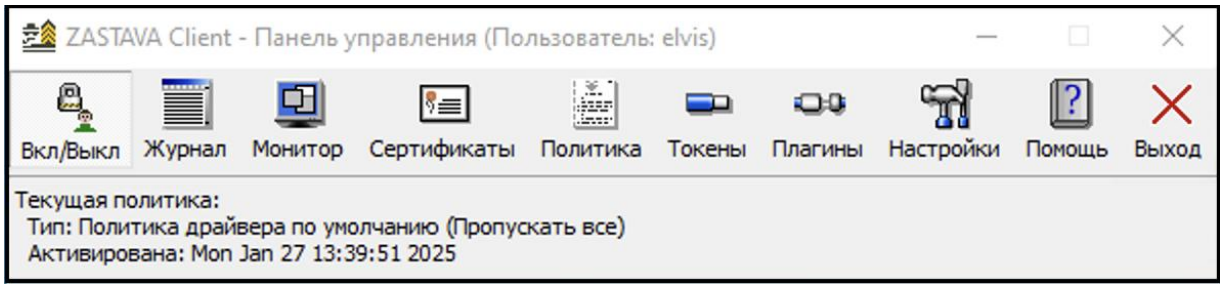


Рисунок 36 – Панель управления ПАК «ЗАСТАВА-Клиент»

2) открыть окно «Токены» нажатием кнопки  «Токены» на панели управления;

3) в окне «Токены» (см. Рисунок 37) выбрать из списка в левой части окна название своего ключевого носителя, затем нажать кнопку «Сменить ПИН-код»;

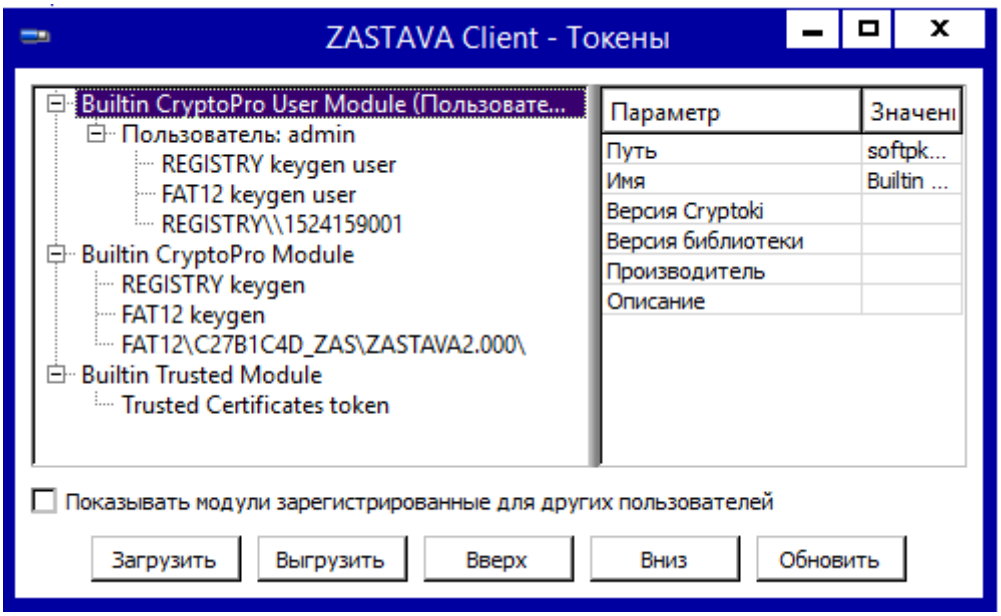


Рисунок 37 – Окно «Токены»

4) в открывшемся окне «Сменить ПИН-код» установить переключатель «Тип» в положение «ПИН-код пользователя» (см. Рисунок 38);

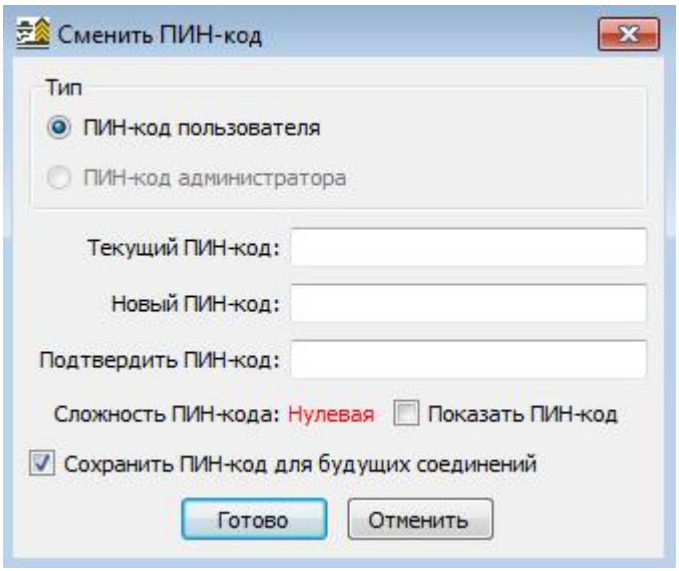


Рисунок 38 – Окно смены ПИН-кода ключевого носителя

5) ввести текущий ПИН-код ключевого носителя в поле «Текущий ПИН-код». Ввести новый ПИН-код в поля «Новый ПИН-код» и «Подтвердить ПИН-код». При смене ПИН-кода необходимо руководствоваться следующими правилами:

— длина ПИН-кода должна быть не менее семи символов;

— в числе символов обязательно должны присутствовать буквы в верхнем и нижнем регистрах, цифры и специальные символы (@, #, $, &, *, % и т.п.);

— ПИН-код не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии и т.д.), а также общепринятые сокращения («USER», «ADMIN» и т.д.);

— при смене ПИН-кода новое значение должно отличаться от предыдущего не менее, чем на четыре символа;

6) при необходимости установить флажок «Сохранить ПИН-код для будущих соединений». В этом случае при установлении нового защищенного соединения в течение одного сеанса работы не нужно будет заново вводить ПИН-код;

7) нажать кнопку «Готово». ПИН-код ключевого носителя будет изменен.

4.10. Окно «Плагины»

Модуль управления криптобиблиотек (модуль криптоплагинов) – встроенный программный модуль, предназначенный для подключения криптобиблиотек. 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.

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).

4.10.1. 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, раскроется, как показано на рисунке (см. Рисунок 39).

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

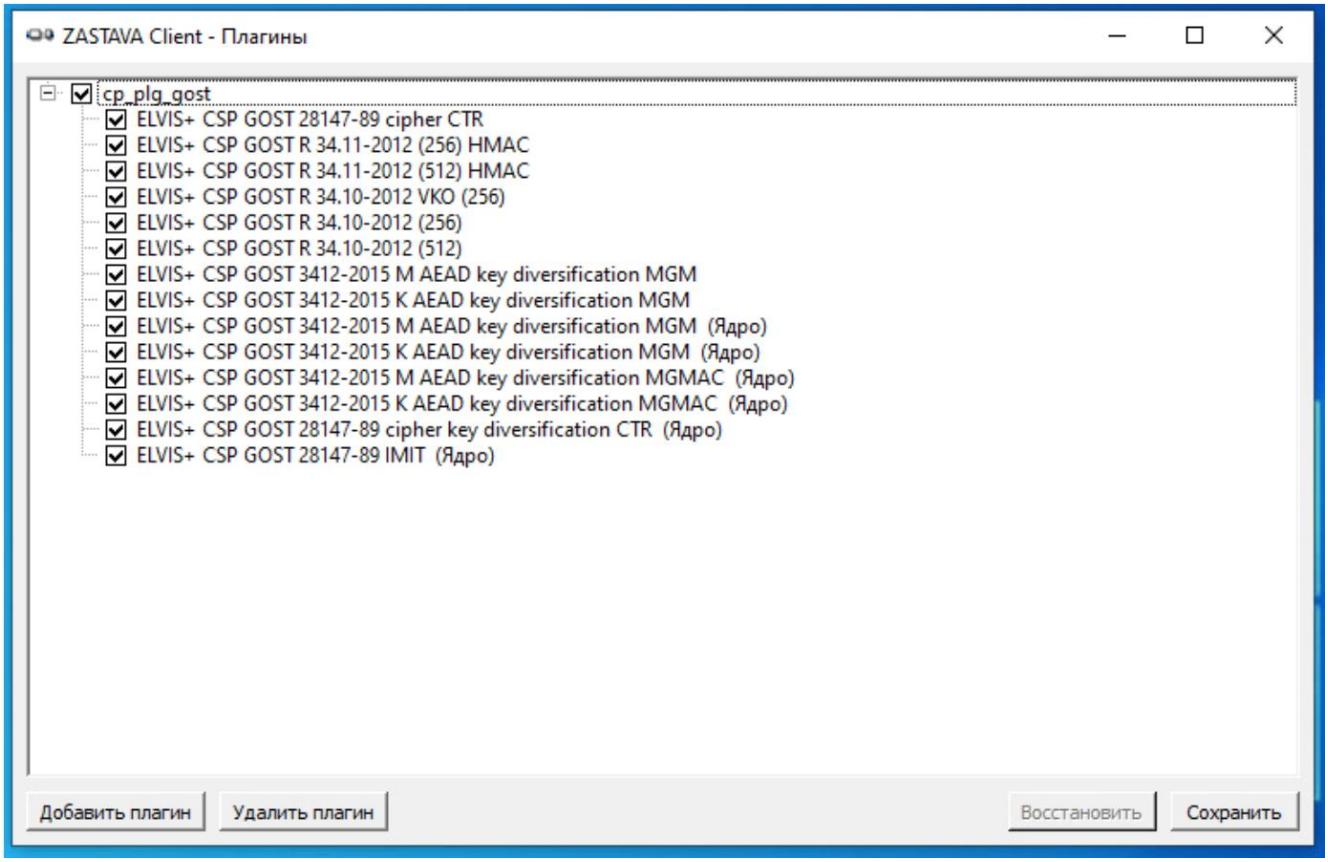


Рисунок 39 – Окно модуля криптоплагинов

4.10.2. Активация криптобиблиотеки

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

1) для активации криптоалгоритма необходимо найти его в списке и нажать кнопку «Восстановить»;
2) 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.

5. ИНТЕРФЕЙС КОМАНДНОЙ СТРОКИ ПАК «ЗАСТАВА-КЛИЕНТ»

5.1. Мониторинг работы ПАК «ЗАСТАВА-Клиент»

5.1.1. Обзор средств мониторинга

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

- журналы регистрации событий (bin_log.txt, vpndmn_init.log);
- утилиты конфигурирования и мониторинга активности.

5.1.1.1. Файл регистрации системных событий

Записи о регистрируемых системных событиях хранятся в директории «/var/vpnagent/log/ (например, bin_log.txt и vpndmn_init.log)» для ОС Astra Linux Special Edition 1.7.

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 СВТ. Кроме того, утилита vpnmonitor позволяет просмотреть статистику по пакетам.

Для вызова утилиты ОС Astra Linux Special Edition 1.7 необходимо использовать полный путь «/opt/ZASTAVAclient/bin/vpnmonitor», либо добавить короткую ссылку (alias) на директорию «aliasvpnmonitor="/opt/ZASTAVAclient/bin/vpnmonitor"».

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. Параметры команды «vpnmonitor –s» представлены в таблице (см. Таблица 27):

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

Таблица 27 – Параметры команды «vpnmonitor –s»

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

Список параметров выводимой статистики представлен в таблице (см. Таблица 28).

Таблица 28 – Печень параметров статистики

Параметр	Описание
IPsec	
Packets (bytes) recieved	Количество пакетов, полученное с момента запуска ПАК «ЗАСТАВА-Клиент»
Packets (bytes) sent	Количество пакетов, посланное с момента запуска ПАК «ЗАСТАВА-Клиент»
Decapsulated packets	Количество расшифрованных пакетов
Encapsulated packets	Количество зашифрованных пакетов
Packets recieved unsecure	Количество полученных ПАК «ЗАСТАВА-Клиент» 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 восстановлении фрагментированных входных IP-пакетов
Output frags consumed	Количество IP-фрагментов, использованных при восстановлении фрагментированных выходных IP-пакетов
Output frags created	Количество IP-фрагментов, созданных при фрагментации выходного пакета
Decrease MTU requests	Количество пакетов – запросов на понижение MTU
Outgoing packets reinjected as input	Количество исходящих пакетов, преобразованных во входящие
Incoming packets not found in hash table	Количество промахов для входящих пакетов при поиске фильтра в хэш-таблице
Outgoing packets not found in hash table	Количество промахов для исходящих пакетов при поиске фильтра в хэш-таблице
IKEv2	
IKE SAs created (failed) initiated/responded	Количество созданных (не созданных) инициированных/отвеченных IKE SA в формате x(x)/x(x)
Resumed IKE SA initiated/responded	Количество возобновленных IKE SA инициированных/отвеченных
IKE SA redirections received/sent	Количество перенаправлений IKE SA получено/послано
COOKIE requested/sent	Количество запрошенных/отправленных токенов COOKIE
Denied IKE SA requests	Количество отвергнутых запросов на создание IKE SA
IKE SA rekeys initiated/responded/collisions	Количество обновлений ключей IKE SA инициированных/отвеченных/коллизий в формате x/x/x
IPsec SA bundless created	Количество созданных IPsec SA
IPsec SA rekeys initiated/responded/collisions	Количество обновлений ключей IPsec SA инициированных/полученных/коллизий в формате x/x/x
Attempts to rekey non-existend IPsec SA by this host/by peer	Количество попыток обновления ключей несуществующей IPsec SA данным хостом/партнером по связи

Параметр	Описание
Temporary rekey failures on this host/on peer	Количество временных отказов в обновлении ключей данным хостом/партнером по связи
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)
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
Outgoing packets reinjected    |0
as input                       |
```

```
Incoming packets not found i~|72 662
n hash table                 |
Outgoing packets not found i~|337
n hash table                 |

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 ПАК «ЗАСТАВА-Клиент»

Для просмотра информации об активированной на ПАК «ЗАСТАВА-Клиент» политике 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
```

5.2.4. Просмотр информации по созданным SA

Для просмотра активных защищённых соединений, установленных с данным СВТ, а также создающихся защищённых соединений, необходимо выполнить команду:

```
vpnmonitor –i
```

Пример вывода команды «vpnmonitor -i» представлен ниже:

```
E00834D4AD1962CF.C46F13CE092AB899  10.111.6.152  (DN)  C=RU,CN=user2
GOST3410.2001-Sig/Gost3410.2001-Sig
IKE states count 1
IPsec states count 0
```

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:

1) /opt/ZASTAVAclient/bin/vpnmonitor -i -view details

Bad value for option: -view, for argument #1: details

-view <line|list|count|json|xml|csv>

— line – print general info in one line, values delimited by tab symbol;
— list – print full info in multiline in format '<field name>: <field value>';
— count – print only items count;
— json – print full info in JSON format;
— xml – print full info in XML format;

2) «-view line | table | list| details» (по умолчанию используется -view table -show all). Описание значений параметра «view»:

— «view line» – показывать информацию по стейту в виде строк;
— «view table» – показывать основную информацию по стейту (IP, ID) в виде таблицы;
— «view list» – показывать всю информацию по стейту в формате параметр-значение;
— «view details» – показывать всю информацию по стейту в таблице формата параметр: значение;
— «view count» – показывать текущую информацию.

3) «-show all | ike | ipsec | ipsectree». Описание значений параметра «show»:

— «show all» - показывать все стейты;
— «show ike» – показывать только IKE стейты;
— «show ipsec» – показывать только IPsec стейты;
— «show ipsectree» – показывать IKE и SA стейты.

Для фильтрации защищенных соединений необходимо определить тип SA, по которому будет произведена фильтрация:

— 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 29 и Таблица 30),

— «operation» – операция для произведения сравнения по выбранному полю с эталоном (см. Таблица 31),

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

Таблица 29 – Параметры фильтрации протокола IKE

Параметр	Характеристика
type	Тип создания SA
mode	Режим создания SA
role	Роль локального СВТ при создании SA
state	Состояние IKE SA
eapid_local	Свой EAP ID
ikeid_local	IKE ID данного СВТ
eapid_remote	EAP ID, присланный партнером по связи
ikeid_remote	IKE ID партнера по связи
id_remote	ID партнера по связи (IKE ID или EAP ID в зависимости от метода аутентификации)
rule_name	Имя правила
algcipher	Алгоритм шифрования
alghash	Алгоритм хэширования
dhgroup	DH-группа
algintegrity	Алгоритм контроля целостности
algprf	Псевдослучайная функция
local_ip	IP-адрес данного СВТ, использованный при создании защищенного соединения
local_port	UDP-порт на данном СВТ, использованный при создании защищенного соединения
peer_ip	IP-адрес СВТ, с которым создано защищенное соединение
peer_port	UDP-порт СВТ, с которым создано защищенное соединение
redirect_ip	IP-адрес СВТ, с которого произошло перенаправление на данное СВТ
peer_auth_method	Метод аутентификации партнера по связи
auth_method	Метод идентификации данного СВТ
spi	IKEv2 SPI
log_level	Уровень регистрации событий
features	Список поддерживаемых опций

Таблица 30 – Параметры фильтрации протокола IPsec

Тип	Характеристика
idstr	Идентификационный номер
ike_saref_str	Ссылка на IKE SA
ike_id_remote	IKE SA ID СВТ, с которым создано защищенное соединение
mode	Режим создания SA
role	Роль при создании SA
peer_id	ID СВТ партнёра по связи
local_id	ID данного СВТ
peer_ip	IP-адрес СВТ, с которым создано защищенное подключение
peer_port	UDP-порт СВТ, с которым создано защищенное подключение
local_ip	IP-адрес данного СВТ, использованный при создании защищенного соединения
local_port	UDP-порт на данном СВТ, использованный при создании защищенного соединения

Тип	Характеристика
ike_cfg_server	IKE CFG адрес, выданный ПАК «ЗАСТАВА-Клиент»
dhgroup	DH группа
filter	**Фильтр**
rule	Название применяемого правила
ah_proto	(AH) Правило
ah_spi_in	Значение SPI для входящей SA (AH)
ah_spi_out	Значение SPI для исходящей SA (AH)
ah_rekey_spi	Значение SPI для входящей SA, ключи которой были обновлены
ah_log_level	(AH) Уровень регистрации событий
ah_pmtu	(AH) Значение MTU, которое установлено на промежуточном агенте
ah_status	(AH) Состояние
ah_auth	(AH) Алгоритм имитозащиты
ah_pkts_decap	(AH) Декапсулировано пакетов
ah_bytes_decap	(AH) Декапсулировано байт
ah_pkts_decap_ce	(AH) Ошибки дешифрации (пакетов)
ah_pkts_decap_ae	(AH) Ошибки аутентификации (пакетов)
ah_pkts_decap_re	(AH) Ошибки атак воспроизведения (пакетов)
ah_pkts_decap_tl	(AH) Ошибки ограничения трафика (пакетов)
ah_pkts_decap_oe	(AH) Прочие ошибки декапсуляции (пакетов)
ah_pkts_encap	(AH) Инкапсулировано пакетов
ah_bytes_encap	(AH) Инкапсулировано байт
ah_pkts_encap_ce	(AH) Ошибки шифрации (пакетов)
esp_proto	(ESP) Правило
esp_spi_in	Значение SPI для входящей SA (ESP)
esp_spi_out	Значение SPI для исходящей SA (ESP)
esp_rekey_spi	Значение SPI для входящей SA, ключи которой были обновлены (ESP)
esp_log_level	(ESP) Уровень регистрации событий
esp_pmtu	(ESP) Значение MTU, которое установлено на промежуточном агенте
esp_status	**Состояние**
esp_transform	(ESP) Алгоритм шифрования
esp_auth	(ESP) Алгоритм имитозащиты
esp_orig_peer_ip	(ESP) Исходный адрес партнера по связи
esp_orig_local_ip	(ESP) Исходный адрес данного СВТ
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 агенте
ipcomp_status	(IPcomp) Состояние
ipcomp_compression	(IPcomp) Алгоритм сжатия

Таблица 31 – Описание типов операций фильтрации

Команда	Характеристика
Операции для фильтрации по типу обмена	

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

В некоторых командных оболочках запрещено использование некоторых символов (например, в bash '(', ')', '*', кавычки и т.д.), поэтому перед этими символами нужно ставить знак экранирования '\' 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 -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)
```

Для удаления всех IKE стейтов используется команда:

```
vpnmonitor -i -clearikesa [delpmp]
```

5.2.6. 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 34).

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. Таблица 32);
- «– orderby <field>» – сортировка по заданному полю (см. Таблица 33);
- «– 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 32 – 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_str	Параметр фильтрации по времени жизни
comment	Параметр фильтрации по полю «Комментарий»
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

Параметр	Характеристика
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 33 – 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
```

Отображаемые параметры информации о действующих фильтрах описаны в таблице (см.Таблица 34).

Таблица 34 – 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>
```

где <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 ПАК «ЗАСТАВА-Клиент».

Для вызова утилиты в ОС Astra Linux Special Edition 1.7 необходимо использовать полный путь /opt/ZASTAVAclient/bin/vpnconfig, либо добавить короткую ссылку (alias) на директорию:

```
alias vpnconfig="/opt/ZASTAVAclient/bin/vpnconfig".
```

Операции с утилитой vpnconfig доступны только администратору ПАК «ЗАСТАВА-Клиент».

При штатной работе ПАК «ЗАСТАВА-Клиент» изменения локальных установок обычно не требуется и управление ПАК «ЗАСТАВА-Клиент» производится централизованно при помощи ПО «ЗАСТАВА-Управление» (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 выполнить команду:

```
vpnconfig –h.
```

Справка о конкретной команде:

```
vpnconfig -help <команда>.
```

Справка о конкретной команде и типе объектов:

```
vpnconfig -help <команда> <тип объекта>.
```

Также существует возможность получить подробную справку с примерами и описанием команд, для этого надо выполнить команду:

```
vpnconfig –h all.
```

5.3.2. Просмотр информации о ПАК «ЗАСТАВА-Клиент»

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

```
vpnconfig –ver.
```

Пример вывода команды «vpnconfig –ver»:

```
Product name: ZASTAVA Client
Vendor name: AO ELVIS-PLUS
Product build: 6.80.22727.23807
Product release: 6.80
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 и СОС регистрируются в ПАК «ЗАСТАВА-Клиент». Описание видов сертификатов и их параметров приведено в подразделе 4.7.

ПАК «ЗАСТАВА-Клиент» поддерживает СОС. Более полная информация приведена в п. 4.7.7.

5.3.3.1. Свойства сертификата и его проверка

Для просмотра всех свойств сертификата необходимо узнать id сертификата, для этого выполнить команду:

```
vpnconfig –list cert
```

Затем выполнить команду, указав id требуемого сертификата:

```
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 по связи.

Описание всех свойств сертификата представлено в таблице (см. Таблица 35).

Таблица 35 – Свойства сертификата

Свойство	Описание
Version	Версия сертификата
Серийный номер	Серийный номер сертификата

Свойство	Описание
Issuer	Кем выдан сертификат
Subject	Содержит отличительное имя субъекта, то есть владельца закрытого ключа, соответствующего открытому ключу данного сертификата. Субъектом сертификата может выступать УЦ, РЦ или конечный субъект
Sign Algorithm	Алгоритм цифровой подписи сертификата
Key Algorithm	Тип открытого ключа (алгоритм цифровой подписи и длина)
Public Key	Значение открытого ключа
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 сертификата

В ПАК «ЗАСТАВА-Клиент» можно регистрировать два типа X.509 сертификатов: 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 ПАК «ЗАСТАВА-Клиент», необходимо произвести следующие действия:

1) выполнить команду:

```
vpnconfig –list token
```

далее в появившемся списке найти токен «Trusted Certificates token» и запомнить его ID;

2) выполнить команду:

```
vpnconfig –add cert <file> password <password> pin <pin> ca token
<token_id>
```

где:

— «<password>» – пароль доступа к закрытому ключу;

— «<pin>» – пароль доступа к токену;

— «<token_id>» - ID для «Trusted Certificates token»;

3) в случае ввода корректного ПИН-кода и пароля появится сообщение, сигнализирующее об успешной регистрации сертификата:

```
Certificate is imported
```

4) после этого выполнить команду:

```
vpnconfig –login token <token_id> <pin> save
```

где:

— «<pin>» – пароль доступа к токену;

— «<token_id>» - ID для Trusted Certificates token.

Если сертификат УЦ был получен через незащищённый канал (например, по электронной почте), и необходимо сохранить его как «Доверенный», требуется проверить подлинность этого сертификата вручную. Непосредственно после регистрации его в ПАК «ЗАСТАВА-Клиент» требуется связаться с уполномоченным представителем УЦ, чтобы сравнить сигнатуру (fingerprint) оригинального сертификата УЦ с сигнатурой полученного сертификата УЦ, которая отображается в полях «Fingerprint» в таблице сертификатов ПАК «ЗАСТАВА-Клиент». Если сигнатуры не совпадают требуется немедленно удалить сертификат из ПАК «ЗАСТАВА-Клиент».

Зарегистрировать персональный сертификат можно двумя способами: импортировать из транспортного контейнера PKCS#12, либо создать ключевую пару и сформировать запрос на персональный сертификат.

Чтобы зарегистрировать новый персональный сертификат в ПАК «ЗАСТАВА-Клиент» путем импорта из транспортного контейнера, 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 ПИН-код токена в появившемся окне. После ввода ПИН-кода нажать кнопку «Готово»;

3) поставить флажок в поле «Save password for future requests», если требуется сохранить пароль токена для будущих соединений;

4) в случае ввода корректного ПИН-кода появится сообщение, сигнализирующее об успешной регистрации сертификата:

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

5) с помощью СКЗИ можно скопировать в реестр или на носитель содержимое контейнера, включающего закрытый ключ и сертификат;

6) ПАК «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.

Способ добавления сертификата путём создания запроса в ПАК «ЗАСТАВА-Клиент»:

```
/opt/ZASTAVAclient/bin/vpnconfig -add request
```

```
Format:
  vpnconfig -add request <token_id> <key_algorithm> <key_length>
<hash_algorithm> <subject> [ip=<ip-address>] [dns=<dns>] [email=<e-
mail>] [upn=<upn>] [eku=ipsec|sclogin] [noexport] [cms [signer=<dn>]]
    - add certificate request.
    <token_id> - id of token.
    <key_algorithm>, <key_length>, <hash_algorithm> - key algorithm,
key length
      and hash algorithm. Use command (vpnconfig -list token) to see
tokens, what
      key algorithms allowed for selected token and what key lengths
and hash
      algorithms allowed for selected key algorithm.
    <subject> - formatted string:
      C=Country Code, ST=State, L=Locality, O=Organisation,
      OU=Organisational Unit, T=Title, CN=Common Name
      Do not forget use quotes if subject contains spaces.
    <ip-address>, <dns>, <e-mail>, <upn> - optional subject
alternative name strings.
    eku - optional extended key usage type: 'IKE/IPsec' or 'Smart Card
Login'.
    noexport - flag to mark private key as non-exportable.
    cms - generate signed request in CMS format.
    signer - subject of the certificate used to sign request,
             if not specified, value from local settings will be used.
  Example:
  vpnconfig -add request 0 RSA 512 MD5 "C=Russia,O=Elvis\+"
ip=87.240.134.23 noexport
```

В результате запроса создаётся ключевая пара на указанном токене и выдаётся запрос на сертификат, на основании которого нужно выпустить персональный сертификат на УЦ и затем импортировать этот сертификат командой:

```
 add cert
```

В результате выполнения команды будет выведено сообщение:

```
[root@mp-c9f2-cli ~]# /opt/ZASTAVAclient/bin/vpnconfig -add request 3
"GOST R 34.10-2012 256" 512 "GOST 34.11-2012 256" "C=RU,CN=test_cert"
eku=ipsec
-----BEGIN CERTIFICATE REQUEST-----
<- содержимое запроса ->
-----END CERTIFICATE REQUEST-----
```

5.3.3.3. Экспорт сертификата

Для того чтобы выполнить процедуру экспорта сертификата, необходимо выполнить команду:

```
vpnconfig -export cert <id> <file> [key] [der] [base64] [pkcs7]
[pkcs12] [path] [password <password>]
```

5.3.3.4. Удаление сертификата

Для удаления сертификата из ПАК «ЗАСТАВА-Клиент» необходимо узнать его id. Для этого нужно воспользоваться командой «vpnconfig –list cert».

После этого необходимо выполнить команду:

```
vpnconfig –remove cert <id>
```

Если срок действия сертификата, находящегося в ПАК «ЗАСТАВА-Клиент», закончился, данный сертификат будет автоматически удалён из ПАК «ЗАСТАВА-Клиент» после проверки. Однако это не относится к локальным сертификатам (с закрытыми ключами). Поэтому необходимо удостовериться в корректности настроек даты, времени и настроек часового пояса на используемом СВТ.

5.3.3.5. Регистрация предварительно распределенного ключа

Чтобы зарегистрировать предварительно распределенный ключ в ПАК «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 значения 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, 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.

Если все введенные данные корректны, появятся следующие сообщения:

```
Password OK.
Preshared key imported
```

5.3.3.6. 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
```

5.3.3.7. Удаление предварительно распределенного ключа

Для удаления предварительно распределенного ключа из ПАК «ЗАСТАВА-Клиент» необходимо выполнить команду:

```
vpnconfig -remove cert <id>
```

В случае успешного удаления предварительно распределенного ключа будет выведено сообщение: «Preshared key was deleted».

5.3.3.8. Список отозванных сертификатов

COC – это список сертификатов, которые с данного момента времени не имеют силы и не должны использоваться для формирования защищенных соединений (SA) в течение сеанса безопасного соединения. Подробное описание COC представлено в п. 4.7.7.

Для того чтобы просмотреть зарегистрированный COC, необходимо выполнить команду:

```
vpnconfig -list cert crl
```

5.3.3.9. Импортирование COC вручную

ПАК «ЗАСТАВА-Клиент» поддерживает возмодность импорта COC вручную. Процесс импорта идентичен процессу регистрации сертификата. Чтобы зарегистрировать COC в ПАК «ЗАСТАВА-Клиент», необходимо выполнить команду:

```
vpnconfig –add cert <file>.
```

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

COC не может быть удален из ПАК «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, необходимо обновить COC 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 ПАК «ЗАСТАВА-Клиент»

5.3.4.2.1. Системная ЛПБ

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

Для изменения параметров системной политики необходимо воспользоваться утилитой «vpnconfig».

Для настройки системной политики необходимо 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 по PMP необходимо выполнить команду:

```
vpnconfig -set lsp system pmp <cert_id> <id_type> <server_ip> <log level> <timeout>
```

где:

<any> - значение для использования любого зарегистрированного локального сертификата для установления соединения;

<cert_id> - ID выбранного сертификата;

<id_type> - тип идентификатора для прогрузки политики, который должен быть согласован с ПО «ЗАСТАВА-Управление»;

<server_ip> или <server_name> - IP-адрес или имя сервера ЛПБ соответственно. После регистрации ЛПБ ПАК «ЗАСТАВА-Клиент» будет обращаться к заданному источнику всякий раз, когда политика активируется;

<log level> - уровень журналирования;

<timeout> - временной промежуток между обращениями к серверу ЛПБ;

— при выборе метода прогрузки «отсутствует» необходимо выполнить команду:

```
vpnconfig -set lsp system none
```

тогда в случае ошибки при прогрузке пользовательской политики будет прогружаться DDP.

	Использовать метод прогрузки политики из файла запрещено!
	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 пользователя – это политика, используемая после входа пользователя в ОС. Политика пользователя может быть получена из файла или от сервера ЛПБ.

Для изменения параметров пользовательской политики необходимо воспользоваться утилитой «vpnconfig»:

— при выборе метода прогрузки из файла выполнить команду:

```
vpnconfig -set lsp user file <path>
```

где: «path» – путь к файлу конфигурации;

— при выборе метода прогрузки с сервера выполнить команду:

```
vpnconfig -set lsp user pmp any|<cert_id> <id_type> <server_ip> [<log level>]
```

где:

<any> - значение для использования любого зарегистрированного локального сертификата для установления соединения;

<cert_id> - ID выбранного сертификата;

<id_type> - тип идентификатора для прогрузки политики, который должен быть согласован с ПО «ЗАСТАВА-Управление»;

<server_ip> или <server_name> - IP-адрес или имя сервера ЛПБ соответственно. После регистрации ЛПБ ПАК «ЗАСТАВА-Клиент» будет обращаться к заданному источнику всякий раз, когда политика активируется;

<log level> - уровень журналирования;

<timeout> - временной промежуток между обращениями к серверу ЛПБ.

	Использовать метод прогрузки политики из файла запрещено!
	Для настройки параметров политики и ее активации можно воспользоваться 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 ПАК «ЗАСТАВА-Клиент» имеется 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 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`). Необходимо учесть, что в этом случае сеть не будет доступна, если СВТ не присвоен статический IP-адрес. Если СВТ получает IP-адрес по DHCP, то нужно 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 СВТ IP-адреса).

Если на СВТ с ПАК «ЗАСТАВА-Клиент» настроена удаленная аутентификация при входе пользователя в систему (например, аутентификация посредством домен-контроллера), то для ее правильной работы для «Политики драйвера по умолчанию» должно быть установлено значение «Пропускать все».

5.3.4.2.4. Изменение сертификата для соединения с сервером

Для изменения сертификата, с помощью которого будет устанавливаться соединение с сервером политики, нужно выполнить команду:

```
vpnconfig -set lsp system|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.

5.3.4.2.5. Уровень регистрации событий

Для журналирования сообщений при передаче ЛПБ от сервера политики необходимо установить уровень регистрации событий, выполнив команду:

```
vpnconfig -set lsp system|user loglevel <log level>
```

где: «<log level>» – уровень регистрации событий при передаче ЛПБ от сервера политики.

5.3.4.2.6. IKE идентификатор

Чтобы настроить получение ЛПБ от 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 от сервера политики, необходимо указать IP-адрес(а) сервера, с которого будет получена политика, выполнив команду:

```
vpnconfig -set lsp system|user server <server_ip>
```

После регистрации ЛПБ ПАК «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 ПАК «ЗАСТАВА-Клиент») 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|user|ddp
```

ЛПБ загрузится в драйвер ПАК «ЗАСТАВА-Клиент», 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

Для чтения информации журнала событий может использоваться утилита «vpnconfig» в следующем формате: vpnconfig -view log [nocase] [<filter>], где [nocase] – фильтрация без учета регистра, <filter> может быть:

- «session <IKE session>» - фильтр по сессии IKE;
- «exchange <IKE exchange>» - фильтр по обмену IKE;
- «level <level>» - фильтр по уровню (INFO, WARN, ERROR, NOTICE);
- «source <source>» - фильтр по источнику;
- «text <text>» - фильтр по полному тексту в любой колонке;
- «sub <text>» - фильтр по подстроке в любой колонке;
- «last <count>» - показать count последних строк.

Файлы регистрации событий располагаются в директории «/var/vpnagent/log/» (например, «bin_log.txt и vpndmn_init.log».

5.3.6. Токены

5.3.6.1. 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
```

5.3.6.2. Просмотр зарегистрированных токенов

Для просмотра всех зарегистрированных токенов необходимо выполнить команду:

```
vpnconfig –list token
```

Вывод результата выполнения данной команды будет содержать информацию о каждом токене. Пример вывода:

```
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
    RNG: Not supported
```

5.3.6.3. 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 название в системе (см. п. 5.3.6.2);
- «<pin>» – ПИН-код токена;
- «[save]» – необязательный параметр, если его не установить, то ПАК «ЗАСТАВА-Клиент» будет запрашивать ПИН-код при каждом обращении к токену.

Для того чтобы закончить сеанс работы с токеном, необходимо выполнить команду:

```
vpnconfig –logout token <token_id>
```

5.3.6.4. Смена ПИН-кода токена

Для смены ПИН-кода токена необходимо выполнить команду:

```
vpnconfig -password token <token_id> <pin> [save]
```

где:

- «<token_id>» – идентификатор токена или его название в системе;
- «<pin>» – новый ПИН-код токена;
- «[save]» – необязательный параметр, который отвечает за сохранение ПИН-кода для дальнейших обращений к токену.

ПИН-код может быть изменен только на активном токене (соединение с токеном должно быть открыто).

5.3.7. 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 параметров обновления или их редактирования выполнить команду и задать <id> необходимого параметра и его значение:

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

где:

— « <id>» – идентификатор параметра обновлений;

— «<value>» – значение выбранного параметра.

Параметры обновления приведены в таблице (см. Таблица 36).

Таблица 36 – Параметры обновления

Номер параметра	Параметр	Расшифровка
0	Download path	Путь к папке с обновлениями
1	Update URI	Адрес ресурса, к которому ПАК «ЗАСТАВА-Клиент» будет обращаться при проверке обновлений
2	Always verify downloaded files	Включение/отключение проверки хэш-сумм при загрузке обновлений: true – проверять; 0 – не проверять (не рекомендуется)

Для просмотра статуса обновлений ПАК «ЗАСТАВА-Клиент» необходимо выполнить команду:

```
vpnconfig –update status
```

Для проверки наличия новых обновлений на сервере обновлений ПАК «ЗАСТАВА-Клиент» необходимо выполнить команду:

```
vpnconfig –update check
```

5.4. Утилита plg_ctl

Модуль управления криптобиблиотеками (криптоплагинами) – встроенный программный модуль, предназначенный для подключения криптобиблиотек, используемых в ПАК «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 ПАК «ЗАСТАВА-Клиент» как отдельный модуль (плагин). По умолчанию в состав ПАК «ЗАСТАВА-Клиент» входит набор штатных криптобиблиотек.

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 быть указано в кавычках.

Следующий общий синтаксис используется при запуске утилиты «plg_ctl»:

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

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

5.4.2. Действия

Перечень поддерживаемых утилитой «plg_ctl» действия представлен в таблице (см. Таблица 37).

Таблица 37 – 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

5.4.3. Опции

Перечень поддерживаемых утилитой «plg_ctl» опций представлен в таблице (см. Таблица 38).

Таблица 38 – 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`
`-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

5.4.4. 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 будет использован путь к файлу криптобиблиотеки, указанный в файле конфигурации.

Пример:

```
plg_ctl –i c:\temp\test_plg.cfg –b c:\work\bin\test_plg.dll
```

5.4.5. Удаление криптобиблиотеки

Для удаления криптобиблиотеки необходимо указать следующую команду:

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

5.4.6. Вывод информации о криптобиблиотеке или криптоалгоритмах

Для вывода информации о криптобиблиотеки или криптоалгоритмах необходимо указать следующую команду: :

```
«plg_ctl –p» <имя криптобиблиотеки> [-a <имя криптоалгоритма>]
```

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, см. п. 5.4.7.

Пример вывода информации обо всех зарегистрированных криптоалгоритмах уровня приложения:

```
plg_ctl –p * -a * -u
```

5.4.7. Примеры команд в интерфейсе командной строки

Примеры команд в интерфейсе командной строки приведены в таблице (см. Таблица 39).

Таблица 39 – Примеры команд в интерфейсе командной строки

Команда	Выполняемое действие
plg_ctl –p	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. Утилита icv_checker

Проверить КС можно, запустив в утилиту «icv_checker».

Для получения справки по работе утилиты в ОС Astra Linux Special Edition 1.7 необходимо выполнить команду без параметров:

```
/opt/ZASTAVAclient/bin/icv_checker
```

Для удобства далее по тексту вызов утилиты сокращен до ее названия. Используется следующий синтаксис:

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

Формат файла с КС должен быть следующий:

```
filename1(full path)=<hash value (64 chars)>
...
filenameN(full path)=<hash value (64 chars)>
```

Утилита возвращает следующие коды:

— 0 – OK;

— 1 – неправильный параметр запуска;

— –1 – некорректная КС в файле;

— –2 – иные ошибки.

Для проверки целостности ПО необходимо выполнить команду:

```
icv_checker filelist.hash
```

где: «filelist.hash» - файл с текущим значением КС.

Для проверки целостности файла «filelist.hash» необходимо выполнить команду:

```
icv_checker filelist_hash.hash
```

где: «filelist_hash.hash» - файл с текущим значением КС для файла «filelist.hash».

Пример выполнения утилиты «icv_checker»:

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

6. ДОСТУП В СЕТЬ ИНТЕРНЕТ ЧЕРЕЗ ПРОКСИ-СЕРВЕР

При использовании веб-браузера Internet Explorer версии 11 и выше при доступе через системные настройки прокси-сервера (в настройках веб-браузера) на прокси-сервер, владельцем которого является Агент с предустановленным ПО «ЗАСТАВА-Офис», при вводе логина и пароля необходимо деактивировать функцию «Запомнить учётные данные» (соответствующий флажок должен быть снят).

В случае, если функция «Запомнить учётные данные» не была деактирована (соответствующий флажок должен не был снят), то после работы удалить сохранённые учётные данные можно, выполнив шаги:

— в программе эмулятора терминала выполнить команду:

```
cmdkey /list
```

— найти свой логин и скопировать значение графы «Конечный файл» вида «"LegacyGeneric:target=10.111.10.69"»;

— выполнить консольную команду:

```
cmdkey /delete:<"Конечный файл">
```

В противном случае веб-браузер будет автоматически использовать единожды введённые и сохранённые учётные данные до тех пор, пока они не будут изменены или удалены из глобальной политики безопасности (ГПБ).

7. ВОЗМОЖНЫЕ НЕИСПРАВНОСТИ И СПОСОБЫ ИХ УСТРАНЕНИЯ

Возможные неисправности и способы их устранения приведены в таблице (см. Таблица 40).

Таблица 40 – Возможные неисправности и способы их устранения

Описание неисправности	Способы устранения
Ключевой носитель заблокирован после превышения числа попыток ввода ПИН-кода	Разблокировать ключевой носитель, используя ПИН-код администратора
Ключевой носитель заблокирован после превышения числа попыток ввода ПИН-кода администратора	Ключевой носитель не подлежит дальнейшему использованию и должен быть утилизирован

Возможные режимы работы ПАК «ЗАСТАВА-Клиент» сигнализирующие о неисправности, и действия администратора приведены в таблице (см. Таблица 41).

Таблица 41 – Возможные режимы работы ПАК «ЗАСТАВА-Клиент» и действия администратора

Описание режима	Действия администратора
Статус ПАК «ЗАСТАВА-Клиент»: ошибка активации; предыдущая политика не будет восстановлена. Прогружена любая другая политика, например, «Политика драйвера по умолчанию» (красный цвет значка в системной информационной панели)	Для предотвращения нарушения политики безопасности, необходимо настроить политику драйвера по умолчанию в значение «Сбрасывать всё, кроме DHCP». Затем для установления причины ошибки активации проверить сетевую доступность ПО «ЗАСТАВА-Управление» и правильность настройки политики. Убедиться в том, что персональный сертификат в ПАК «ЗАСТАВА-Клиент» совпадает с сертификатом, загруженным в ПО «ЗАСТАВА-Управление», и что доверенный сертификат в ПАК «ЗАСТАВА-Клиент» установлен. Убедиться в действительности сертификатов. Убедиться в подключении ключевого контейнера. Сеанс с ключевым контейнером должен быть открыт
Статус ПАК «ЗАСТАВА-Клиент»: ошибка активации; предыдущая политика будет восстановлена (жёлтый цвет значка в системной информационной панели)	
Статус ПАК «ЗАСТАВА-Клиент»: системная служба ПАК «ЗАСТАВА-Клиент» `vpndmn` не запущена (серый цвет значка в системной информационной панели)	Вручную запустить системную службу ПАК «ЗАСТАВА-Клиент» `vpndmn`
Статус ПАК «ЗАСТАВА-Клиент»: при загрузке политики ПАК «ЗАСТАВА-Клиент» с ПО «ЗАСТАВА-Управление» (сервер недоступен, цвет значка в системной информационной панели – желтый с красной рамкой)	Проверить сетевую доступность ПО «ЗАСТАВА-Управление» и правильность настройки политики

Характерные ошибки при работе с ПАК «ЗАСТАВА-Клиент» и рекомендации по их устранению приведены в таблице (см. Таблица 42).

Таблица 42 – Характерные ошибки при работе с ПАК «ЗАСТАВА-Клиент» и рекомендации по их устранению

Тип ошибки	Описание ошибки	Рекомендации по устранению
Неправильное использование утилиты командной строки ПАК «ЗАСТАВА-Клиент»	Синтаксическая ошибка (Syntax error): – при вводе неверных/несуществующих параметров и ключей при использовании утилиты vpnconfig.exe; – при вводе неверных/несуществующих параметров и ключей при использовании утилиты vpnmonitor.exe; – при вводе неверных/несуществующих параметров и ключей при использовании утилиты plg_ctl.exe; – при вводе неверных/несуществующих параметров и ключей при использовании утилиты icv_checker.exe	Воспользоваться: – предлагаемым списком команд и ключей утилиты, который выводится при ошибке. Описание команд приведено в подразделе 5.3; – предлагаемым списком команд и ключей утилиты, который выводится при ошибке. Описание команд приведено в подразделе 5.2; – предлагаемым списком команд и ключей утилиты, который выводится при ошибке. Описание команд приведено в подразделе 5.4; – командой вызова справочной информации `icv_checker.exe -h`. Описание команд утилиты приведено в подразделе 5.5
Ошибки при работе с графическим интерфейсом ПАК «ЗАСТАВА-Клиент»	Ошибка доступа: – не отображаются параметры настроек на вкладке «Политика»; – не отображаются импортированные сертификаты на вкладке «Сертификаты»; – не отображается журнал на вкладке «Журнал»; – при обращении к вкладке «Токены» появляется сообщение «Не удалось загрузить параметры токенов»	Необходимо запустить службу vpndmn
Ошибки при настройке политики безопасности в ПАК «ЗАСТАВА-Клиент»	IKE Connection timeout: возникает при указании в настройках получения политики безопасности неверного IP-адреса сервера политик	Необходимо узнать корректный IP-адрес сервера политик и также указать его в настройках политики безопасности ПАК «ЗАСТАВА-Клиент». Если это не помогло, необходимо убедиться в сетевой доступности ПО «ЗАСТАВА-Управление»
	IKE Peer reported error: возникает при указании в политике безопасности сертификата, не совпадающего с сертификатом, указанном в ПО «ЗАСТАВА-Управление»	Необходимо указать в настройках политики безопасности ПАК «ЗАСТАВА-Клиент» сертификат, указанный в ГПБ ПО «ЗАСТАВА-Управление»
	IKE Error: возникает при отсутствии доверенного сертификата УЦ на вкладке «Сертификаты» ПАК «ЗАСТАВА-Клиент», либо при указании неверного доверенного сертификата УЦ	Необходимо импортировать корректный доверенный сертификат УЦ на вкладке «Сертификаты» ПАК «ЗАСТАВА-Клиент»
	Не удалось загрузить политику. Отсутствует персональный сертификат: возникает при отсутствии персонального сертификата на вкладке «Сертификаты» ПАК «ЗАСТАВА-Клиент». При этом в опциях политики безопасности отображается ошибка, что политика ссылается на несуществующий сертификат	Если на вкладке «Сертификаты» ПАК «ЗАСТАВА-Клиент» скопированный контейнер отображается как «Key Pair without Certificate», импортировать персональный сертификат этого контейнера закрытого ключа на этой же вкладке

Тип ошибки	Описание ошибки	Рекомендации по устранению
	Local certificate not found or not valid: возникает, если у сертификата, указанного в политике безопасности ПАК «ЗАСТАВА-Клиент», истек срок действия	Необходимо перевыпустить сертификат и контейнер закрытого ключа. Далее необходимо указать новый сертификат в ГПБ ПО «ЗАСТАВА-Управление» и импортировать контейнер закрытого ключа в ОС. В политике безопасности ПАК «ЗАСТАВА-Клиент» указать использование нового сертификата для подключения к серверу управления

ПЕРЕЧЕНЬ СОКРАЩЕНИЙ

CRL (от англ. Certificate Revocation List) – список отозванных сертификатов

ESP (от англ. Encapsulated Security Payload) - протокол из группы IPsecGMT – время по Гринвичу

IKE (от англ. Internet Key Exchange) - протокол обмена ключевой информацией

IP (от англ. Internet Protocol) – протокол сетевого уровня, являющийся базовым протоколом IP-сетей

IPsec (от англ. IP security) - группа протоколов для установления защищенных соединений в IP-сетях

MTU (от англ. Maximum Transmission Unit) - максимальный размер полезного блока данных одного пакета, который может быть передан протоколом без фрагментации

SA (от англ. Security Association) - защищенное соединение (в контексте протоколов IPsec и IKE)

VPN (от англ. Virtual Private Network) – виртуальная частная сеть

АПМДЗ – аппаратно-программный модуль доверенной загрузки

ГПБ – глобальная политика безопасности

КС – контрольная сумма

ЛПБ – локальная политика безопасности

ОС – операционная система

ПО – программное обеспечение

РЦ – регистрационный центр

СВТ – средство вычислительной техники

СЗИ – средство защиты информации

СКЗИ – средство криптографической защиты информации

СОС – список отозванных сертификатов

УЦ – удостоверяющий центр

ПРИЛОЖЕНИЕ 1

ПОДДЕРЖИВАЕМЫЕ ИЗДЕЛИЯ ЛИНЕЙКИ «ЗАСТАВА»

ПАК «ЗАСТАВА-Клиент» поддерживает работу с программными изделиями линейки «ЗАСТАВА-Управление»:

- МКЕЮ.00570-01 Программный комплекс «ЗАСТАВА-Управление «VPN/FW «ЗАСТАВА», версия 6;
- МКЕЮ.00631-01 Программный комплекс «VPN/FW «ЗАСТАВА-Управление», версия 6 КС3»;
- МКЕЮ.00669-01 Программное обеспечение «ЗАСТАВА-Управление», версия 8 КС1»;
- МКЕЮ.00690-01 Программно-аппаратный комплекс «ЗАСТАВА-Управление», версия 8 КС3».

ПАК «ЗАСТАВА-Клиент» поддерживает работу с программными изделиями линейки «ЗАСТАВА-Офис»:

- МКЕЮ.00627-01 Программный комплекс защиты корпоративных вычислительных ресурсов на сетевом уровне с использованием технологий VPN и распределённого межсетевого экранирования на основе интернет-протоколов семейства IPsec / IKE «VPN/FW «ЗАСТАВА-Офис», версия 6 КС1» (исполнения: ZO6-L32-VF-01, ZO6-L64-VF-01);
- МКЕЮ.00628-01 Программный комплекс защиты корпоративных вычислительных ресурсов на сетевом уровне с использованием технологий VPN и распределённого межсетевого экранирования на основе интернет-протоколов семейства IPsec / IKE «VPN/FW «ЗАСТАВА-Офис», версия 6 КС3» (исполнение ZO6-L64-FV-03);
- МКЕЮ.00599 Программно-аппаратный комплекс "VPN/FW "ЗАСТАВА-Офис", версия 6 КС3 (исполнение ZO6-EL64-FV-03);
- МКЕЮ.00651-01 Программный комплекс «VPN/FW «ЗАСТАВА-Офис», версия 8 КС1»;
- МКЕЮ.00652-01 Программно-аппаратный комплекс «VPN/FW «ЗАСТАВА-Офис», версия 8 КС3».

ПАК «ЗАСТАВА-Клиент» поддерживает работу с аппаратно-программными комплексами линейки «ЗАСТАВА»:

- МКЕЮ.00557 Аппаратно-программный комплекс «VPN/FW «ЗАСТАВА-150»;
- МКЕЮ.00630 Аппаратно-программный комплекс «VPN/FW «ЗАСТАВА-150», версия 6;

- МКЕЮ.00664 Аппаратно-программный комплекс «VPN/FW ЗАСТАВА-150» (исполнение ZO8-APK-150);
- МКЕЮ.00581 Аппаратно-программный комплекс «VPN/FW ЗАСТАВА-1500»;
- МКЕЮ.00653 Аппаратно-программный комплекс «VPN/FW ЗАСТАВА-1500» (исполнение ZO8-APK-1500);
- МКЕЮ.00661 Аппаратно-программный комплекс «VPN/FW ЗАСТАВА-1500» (исполнение ZO8-APK-1500-A);
- МКЕЮ.00582 Аппаратно-программный комплекс «VPN/FW ЗАСТАВА-6000»;
- МКЕЮ.00654 Аппаратно-программный комплекс «VPN/FW ЗАСТАВА-6000» (исполнение ZO8-APK-6000);
- МКЕЮ.00660 Аппаратно-программный комплекс «VPN/FW ЗАСТАВА-6000» (исполнение ZO8-APK-6000-A);
- МКЕЮ.00666 Аппаратно-программный комплекс «VPN/FW ЗАСТАВА-10000» (исполнение ZO8-APK-10000-A);
- МКЕЮ.00667 Аппаратно-программный комплекс «VPN/FW ЗАСТАВА-10000».

ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ

Изм.	Номера листов (страниц)				Всего листов (страниц) в документе	Номер документа	Входящий номер сопрово-дительного документа и дата	Подпись	Дата
	Измененных	Замененных	Новых	Аннулированных					