УТВЕРЖДЕН
МКЕЮ.00629.ИЗ-ЛУ

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

(«АПК «ЗАСТАВА-ТК», версия 6»)

Руководство администратора

МКЕЮ.00629.ИЗ

2021

СОДЕРЖАНИЕ

1 ВВЕДЕНИЕ 5
1.1 Назначение 5
1.2 Требования к уровню подготовки персонала 5
1.3 Типографские соглашения 5

2 ОБЩИЕ СВЕДЕНИЯ 6
2.1 Технические характеристики 6
2.2 Состав 6
2.2.1 Системный блок 7
2.2.2 Ключевой носитель 8
2.2.3 Программное обеспечение 9

3 УСТАНОВКА И НАСТРОЙКА АПК «ЗАСТАВА-ТК» 11
3.1 Подготовка к работе 11
3.1.1 Сборка и подключение 11
3.1.2 Проверка настроек BIOS 11
3.1.3 Проверка контрольной суммы 14
3.1.4 Настройка сетевых параметров 14
3.1.5 Конфигурирование «ЗАСТАВА-Клиент» 19
3.1.6 Настройка получения политики безопасности 19
3.2 Описание операций 20
3.2.1 Включение 21
3.2.2 Проверка контрольной суммы 21
3.2.3 Настройки датчика вскрытия 22
3.2.4 Режимы работы после срабатывания датчика вскрытия 24
3.2.5 Сброс состояния датчика вскрытия 25
3.2.6 Смена PIN-кода ключевого носителя 26
3.2.7 Просмотр локальных журналов событий 26
3.2.8 Включение режима обработки CRL 28
3.2.9 Автоматический контроль целостности 30
3.2.10 Обновление 30
3.2.11 Выключение 30

4 ГРАФИЧЕСКИЙ ИНТЕРФЕЙС «ЗАСТАВА-КЛИЕНТ» 31
4.1 Запуск графического интерфейса «ЗАСТАВА-Клиент» 31
4.2 Индикация текущего статуса 31
4.3 Ввод пароля токена 32
4.4 Панель управления 32
4.5 Окно «Журнал» 34
4.5.1 Структура окна «Журнал» 35
4.5.2 Фильтрация отображаемых событий 37
4.5.3 Настройка параметров регистрации событий 37
4.5.4 Копирование описания событий 39
4.5.5 Файл регистрации системных событий 39
4.5.6 Очистка журнала и файла регистрации системных событий 39
4.6 Окно «Монитор» 39
4.6.1 Вкладка «Статистика» 40
4.6.2 Вкладка «Список SA» 42
4.6.3 Вкладка «Список Фильтров» 48
4.7 Окно «Сертификаты и ключи» 52
4.7.1 Структура окна «Сертификаты и ключи» 53
4.7.2 Характеристики сертификатов 55

4.7.3 Регистрация и удаление сертификата ... 56
4.7.4 Списки отозванных сертификатов ... 60
4.8 Окно «Управление политиками» ... 62
4.8.1 Структура окна «Управление политиками» ... 62
4.8.2 Типы политик ... 62
4.8.3 Параметры политик «ЗАСТАВА-Клиент» ... 63
4.8.4 Изменение параметров ЛПБ ... 67
4.8.5 Регистрация ЛПБ ... 68
4.8.6 Просмотр ЛПБ ... 69
4.8.7 Активация ЛПБ ... 69
4.9 Окно «Токены» ... 69
4.9.1 Смена PIN-кода токена ... 70
4.9.2 Порядок уничтожения криптографических ключей, утилизации смарт-карт. 71
4.10 Окно «Плагины» ... 72
4.10.1 Просмотр криптобиблиотек и криптоалгоритмов ... 73
4.10.2 Активация криптобиблиотеки ... 73
4.11 Окно «Прочие настройки» ... 73
4.11.1 Вкладка «Журнал» ... 75
4.11.2 Вкладка «IKE» ... 78
4.11.3 Вкладка «GUI» ... 82
4.11.4 Вкладка «Настройки обновления» ... 83
4.12 Окно «Помощь» ... 84

5 ИНТЕРФЕЙС КОМАНДНОЙ СТРОКИ «ЗАСТАВА-КЛИЕНТ» ... 86
5.1 Мониторинг работы «ЗАСТАВА-Клиент» ... 86
5.1.1 Обзор средств мониторинга ... 86
5.2 Утилита vpnmonitor ... 86
5.2.1 Справочная система по работе с утилитой ... 86
5.2.2 Просмотр статистики ... 86
5.2.3 Вывод информации о политике, активированной на «ЗАСТАВА-Клиент» ... 89
5.2.4 Просмотр информации по созданным SA ... 90
5.2.5 Фильтрация фильтров и созданных SA по параметрам ... 90
5.2.6 Просмотр списка фильтров ... 95
5.3 Утилита vpnconfig ... 97
5.3.1 Справочная система по работе с утилитой ... 97
5.3.2 Просмотр информации о «ЗАСТАВА-Клиент» ... 98
5.3.3 Работа с сертификатами и ключами ... 98
5.3.4 Работа с ЛПБ ... 100
5.3.5 Регистрация событий ... 103
5.3.6 Протокол IKE ... 106
5.3.7 Токены ... 110
5.4 Утилита plg_ctl ... 112
5.4.1 Синтаксис ... 112
5.4.2 Вывод информации о криптобиблиотеке или криптоалгоритмах ... 113
5.4.3 Примеры команд в интерфейсе командной строки ... 114
5.5 Утилиты icv_writer и icv_checker ... 114

6 НЕШТАТНЫЕ СИТУАЦИИ ... 116
6.1 Срабатывание датчика вскрытия ... 116
6.2 Некорректная работа АПК «ЗАСТАВА-ТК» после обновления ОС ... 116
6.3 Нарушение целостности образа ... 117
6.4 Автоматическое отключение АПК ... 117

7 ВОЗМОЖНЫЕ НЕИСПРАВНОСТИ И СПОСОБЫ ИХ УСТРАНЕНИЯ ... 118

ПЕРЕЧЕНЬ ПРИНЯТЫХ ТЕРМИНОВ И СОКРАЩЕНИЙ..... 119

ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ..... 120

1 Введение

Настоящий документ предназначен для средства криптографической защиты информации (СКЗИ) МКЕЮ.00629 «Аппаратно-программный комплекс «VPN/FW «ЗАСТАВА-ТК», версия 6» («АПК «ЗАСТАВА-ТК», версия 6») (далее – АПК «ЗАСТАВА-ТК», АПК) и содержит описание составных частей АПК, описание интерфейса программного обеспечения (ПО), процедуры, выполняемые администратором в процессе подготовки АПК к работе, текущие операции, действия при возникновении нештатных ситуаций.

1.1 Назначение

АПК «ЗАСТАВА-ТК» предназначен для защиты корпоративных вычислительных ресурсов на сетевом уровне модели взаимодействия OSI/ISO (стек протоколов TCP/IP) с использованием технологий VPN на основе интернет-протоколов семейства IPSec.

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

АПК является, согласно действующим нормативным правовым актам Российской Федерации, СКЗИ. Использование АПК должно осуществляться в соответствии с документом МКЕЮ.00629.ИЭ «Аппаратно-программный комплекс «VPN/FW «ЗАСТАВА-ТК», версия 6» («АПК «ЗАСТАВА-ТК», версия 6»). Правила пользования.

1.2 Требования к уровню подготовки персонала

Уровень подготовки обслуживающего персонала должен удовлетворять следующим требованиям:

— высшее или среднее техническое образование;

— знание положений настоящего руководства и эксплуатационной документации, входящей в комплект поставки.

В АПК «ЗАСТАВА-ТК» определены роли:

1) Администратор АПК;
2) Пользователь.

Пользователь должен иметь базовые навыки работы с персональным компьютером.

Администратор АПК должен знать основы администрирования локальных сетей.

1.3 Типографские соглашения

Курсив	*Курсив* используется, чтобы выделить названия файлов. Курсив также может использоваться для акцента.
«Кавычки»	Текст, заключенный в кавычки, используется для названий элементов интерфейса.
`Непропорциональный`	Непропорциональный шрифт используется для ссылок на системные папки и каталоги, команд в интерфейсе командной строки.
<Угловые скобки>	Угловые скобки используются в названиях клавиш на клавиатуре компьютера, а также в описаниях параметров.

2 ОБЩИЕ СВЕДЕНИЯ

2.1 Технические характеристики

Технические характеристики АПК «ЗАСТАВА-ТК» приведены в таблице (см. Таблица 1).

Таблица 1 – Технические характеристики АПК

Наименование	Значение
Габаритные размеры (В×Ш×Г)	206×115×265 мм
Масса, не более	1,1 кг
Потребляемая мощность, не более	24 Вт
Возможность установки локального ПО	нет
Процессор	Intel Celeron J1900 Quad-Core
Частота процессора	2,0 ГГц
Объем оперативной памяти	32 Гбайт
Объем жесткого диска	4 Гбайт
Количество подключаемых мониторов	1
Контроль вскрытия корпуса	есть
Встроенный считыватель смарт-карт	есть

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

2.2 Состав

В состав АПК «ЗАСТАВА-ТК» входят следующие компоненты:

- аппаратная платформа x64 ТОНК;
- операционная система (ОС) AltLinux СПТ 7.0, 64-битная версия;
- СКЗИ ЖТЯИ.00088-01 «КриптоПро CSP», версия 4.0 (исполнение 2-Base);
- ПО «ЗАСТАВА-Клиент», версия 6 (далее – «ЗАСТАВА-Клиент»);
- СКЗИ RU.63793390.00009ESMART Token ГОСТ, выполненное на базе микросхемы MIK51SC72Dv6, в составе:
  1) считыватель смарт-карт ESMART Reader ER4006 – считыватель смарт-карт формата ID-1 без корпуса RU.63793390.00007-01;
  2) программный компонент «ESMART Firmware Checker» RU.63793390.00018-01, предназначенный для контроля целостности ПО аппаратного модуля (АМ) и ОС Trust 2.05 микросхемы MIK51SC72Dv6;
  3) программный компонент «ESMART PKCS11» RU.63793390.00001-01 – ПО для ОС, обеспечивающий прикладной программный интерфейс СКЗИ (исполнения 1, 2, 3);

– смарт-карта формата ID-1 RU.63793390.00004-01, которая содержит компоненты: микросхема ДВУК.431295.011-001[1], ПО АМ, состоящее из загрузчика и функциональной части[2].

2.2.1 Системный блок

В качестве системного блока АПК используется аппаратная платформа x64 ТОНК, оборудованная считывателем смарт-карт. Для обеспечения защиты от несанкционированного доступа (НСД) системный блок оборудован датчиком контроля вскрытия корпуса (далее – датчик вскрытия).

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

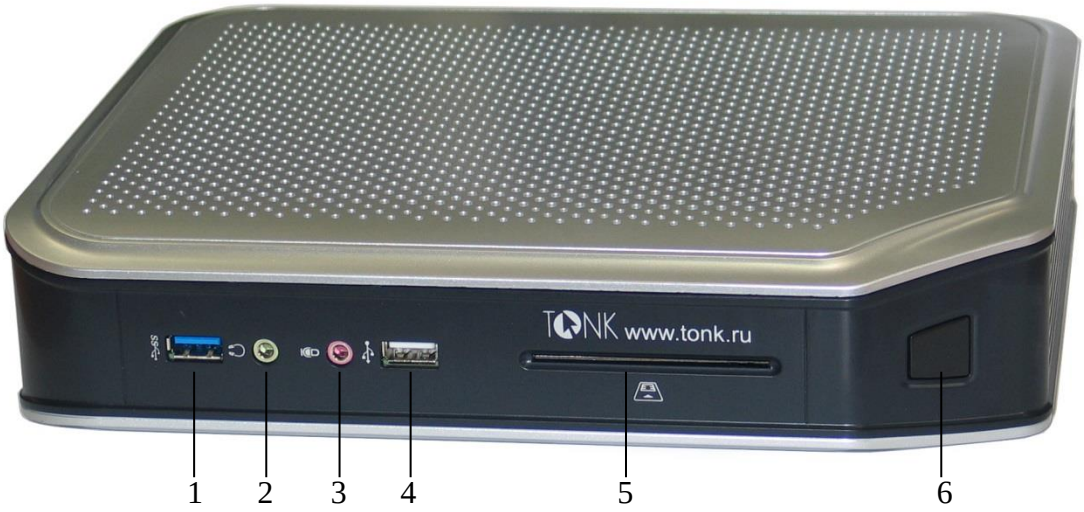

Рисунок 1 – Внешний вид передней панели системного блока

Таблица 2 – Назначение элементов передней панели системного блока

№ указателя	Назначение элемента
1	Порт USB 3.0
2	Гнездо для подключения наушников/колонок
3	Гнездо для подключения микрофона
4	Порт USB 2.0
5	Картоприемник для установки смарт-карты

[1] Изделие «Отечественная микросхема MIK51SC72Dv6 с ОС Trust 2.05, предназначенная для использования в качестве средства криптографической защиты информации».

[2] В соответствии со спецификацией ПО АМ присвоены децимальные номера:
RU.63793390.00003-01 12 01, RU.63793390.00003-01 12 02, RU.63793390.00006-01 12 01, RU.63793390.00006-01 12 02, RU.63793390.00007-01 12 01, RU.63793390.00007-01 12 02, RU.63793390.00008-01 12 01, RU.63793390.00008-01 12 02.
При этом индекс 01 соответствует загрузчику ПО АМ, а индекс 02 – функциональной части ПО АМ.

№ указателя	Назначение элемента
6	Кнопка питания с LED-индикатором. Светится красным цветом, если системный блок подключен к сети питания и выключен. Светится зеленым цветом, если системный блок включен.

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

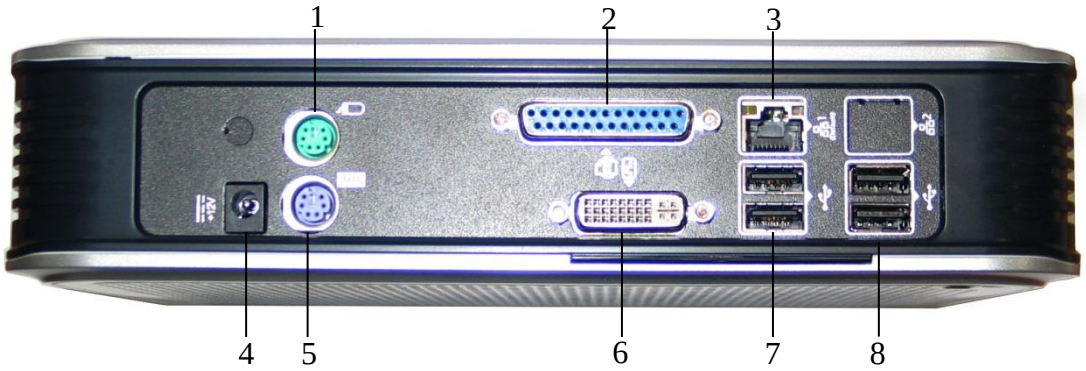

Рисунок 2 – Внешний вид задней панели системного блока

Таблица 3 – Назначение элементов задней панели системного блока

№ указателя	Назначение элемента
1	Порт PS/2 для подключения манипулятора типа «мышь»
2	Порт LPT для подключения принтера
3	LAN (RJ-45)
4	Разъем электропитания
5	Порт PS/2 для подключения клавиатуры
6	Разъем подключения монитора (DVI-I)
7	Порт USB 2.0 (2 шт.)
8	Порт USB 2.0 (2 шт.)

2.2.2 Ключевой носитель

В качестве ключевого носителя в АПК используется электронный идентификатор (смарт-карта) ID-1 RU.63793390.00004-01 из состава СКЗИ ESMART Token ГОСТ.

Использование ключевого носителя обеспечивает двухфакторную аутентификацию пользователя при входе в ОС АПК. Работа возможна только при установленном в АПК ключевом носителе. При извлечении ключевого носителя из картоприемника сеанс работы завершается.

Для защиты от НСД ключевой носитель защищен PIN-кодом длиной от 4 до 8 символов. В ключевом носителе имеется два типа PIN-кода – пользователя и администратора ключевого носителя. Для аутентификации используется PIN-код пользователя.

Внимание! При поставке для всех ключевых носителей задан заводской PIN-код пользователя: 12345678. Перед началом использования ключевого носителя необходимо сменить PIN-код каждого ключевого носителя на личный, как описано в подразделе 3.2.6.

В качестве защиты ключевого носителя от подбора PIN-кода методом перебора используется блокировка после ввода неверного PIN-кода установленное число раз (10 по умолчанию). После блокировки ключевого носителя получить доступ к хранящимся на нем ключам невозможно.

Разблокировать ключевой носитель можно с помощью PIN-кода администратора ключевого носителя. Если превышено количество допустимых попыток неверного ввода PIN-кода администратора ключевого носителя, ключевой носитель не подлежит дальнейшему использованию и должен быть утилизирован.

Обновление открытых и закрытых ключей, используемых в составе АПК, следует производить не реже, чем один раз в 1 (один) год 3 (три) месяца.

Внимание! Использование открытых и закрытых ключей, срок действия которых закончился, ЗАПРЕЩЕНО!

2.2.3 Программное обеспечение

АПК поставляется с полностью установленным и настроенным ПО.

СКЗИ «КриптоПро CSP» обеспечивает реализацию целевых криптографических функций шифрования, контроля целостности данных.

СКЗИ «ESMART Token ГОСТ» обеспечивает реализацию целевой криптографической функции открытого распределения криптографических ключей. СКЗИ «ESMART Token ГОСТ» выполняет следующие функции:

- генерация случайных последовательностей произвольной длины;
- вычисление значения хэш-функции в соответствии с ГОСТ Р 34.11-94, ГОСТ Р 34.11-2012 в 256-битном режиме;
- выработка пар закрытый/открытый ключи электронной подписи (ЭП) в соответствии с ГОСТ Р 34.10-2001, ГОСТ Р 34.10-2012 в 256-битном режиме;
- выработка симметричных ключей шифрования в соответствии с ГОСТ 28147-89;
- хранение в защищенном от НСД виде, в энергонезависимой памяти, закрытого ключа ЭП и симметричных ключей шифрования;
- хранение в защищенном от НСД виде, в энергонезависимой памяти, паролей и другой текстовой информации;
- вычисление и проверка ЭП в соответствии с ГОСТ Р 34.10-2001, ГОСТ Р 34.10-2012;
- шифрование и расшифрование в соответствии с ГОСТ 28147-89;

– выработка ключей по алгоритму VKO ГОСТ Р 34.10-2001 и ГОСТ Р 34.10-2012 в 256-битном режиме.

ПО «ЗАСТАВА-Клиент» предназначен для защиты и фильтрации входящего и исходящего трафика на компьютере пользователя. ПО «ЗАСТАВА-Клиент» обеспечивает контроль и фильтрацию сетевого трафика, а также взаимную криптографическую защиту абонентов при установлении соединения, шифрование и контроль целостности IP-пакетов в корпоративной информационной системе.

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

– защита трафика на сетевом уровне при помощи протоколов IPsec ESP;
– обеспечение двусторонней криптографической аутентификации при установлении соединений с другими хостами защищенной корпоративной сети на базе протоколов IKEv2, контроля целостности данных и конфиденциальности информации путем ее шифрования;
– пакетная фильтрация трафика, основанная на использовании полей заголовков транспортных и сетевых протоколов:
  – на сетевом уровне – через IP v4-адрес и/или поле заголовка IP-протокола;
  – на транспортном уровне – по направлению TCP-соединения и по протоколам сервисов (TCP/UDP-портам);
– расширенная фильтрация пакетов (применение конечных автоматов для большого числа сетевых протоколов);
– осуществление определенной политики взаимодействия (имитозащита и/или шифрование трафика) для каждого защищенного соединения; параметры трафика определяются сетевыми адресами, портами и/или идентификационной информацией конечного отправителя и получателя;
– возможность применения различных степеней защиты трафика;
– сокрытие топологии защищаемой сети (поддержка режима туннелирования трафика);
– возможность использования конфигурируемых туннельных адресов для IPsec-протоколов;
– поддержка работы в режиме «мобильного пользователя» (когда IP-адрес компьютера назначается динамически, т.е. заранее неизвестен);
– поддержка «горячего» резервирования шлюзов безопасности так, что один из этих шлюзов является активным, а остальные шлюзы будут использованы как резервные при выходе из строя основного активного шлюза.

3 Установка и настройка АПК «ЗАСТАВА-ТК»

3.1 Подготовка к работе

АПК «ЗАСТАВА-ТК» поставляется с полностью установленным ПО.

Подготовка АПК к работе включает следующие операции:

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

Внимание! При поставке для всех ключевых носителей заданы одинаковые заводские PIN-коды пользователя: 12345678. Перед началом использования ключевого носителя необходимо сменить PIN-код на личный, как описано в подразделе 3.2.6. Категорически запрещено использовать заводские PIN-коды.

3.1.1 Сборка и подключение

Порядок подключения АПК «ЗАСТАВА-ТК» (см. Рисунок 2, Таблица 3):

1) Подключить к системному блоку монитор, клавиатуру, мышь.
2) Подключить АПК к сети Интернет с помощью сетевого кабеля (поз. 3).
3) Подключить блок питания к разъему электропитания (поз. 4).
4) Подключить монитор и системный блок к сети питания. Убедиться в том, что кнопка питания на корпусе системного блока светится красным цветом.

3.1.2 Проверка настроек BIOS

Для проверки настроек BIOS необходимо:

1) Включить АПК кнопкой питания. Для входа в меню BIOS до начала загрузки ОС нажимать клавишу <F2> до появления запроса на ввод пароля.
2) При появлении запроса на ввод пароля ввести пароль на BIOS. Пароль, установленный производителем: **Tonk123!@#**.
3) После появления на экране меню BIOS проверить и, при необходимости, изменить настройки следующих параметров BIOS:
   – в разделе «Main» (см. Рисунок 3) дата (параметр «System Date») и время (параметр «System time») должны совпадать с текущими;

Рисунок 3 – Раздел «Main»

– в разделе «Security \\ Secure Boot Menu» (см. Рисунок 4) параметр «Secure Boot» должен иметь значение «Disabled»;

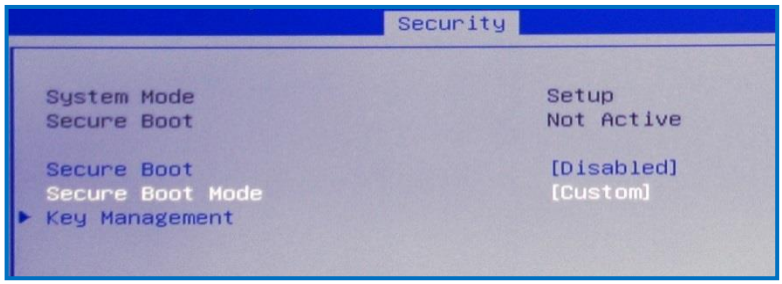

Рисунок 4 – Раздел «Secure Boot Menu»

– в разделе «Advanced \\ ACPI Settings» (см. Рисунок 5) все параметры должны иметь значение «Disabled»;

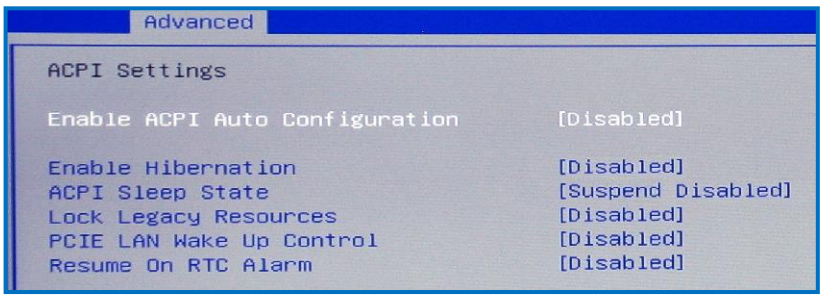

Рисунок 5 – Раздел «ACPI Settings»

– в разделе «Advanced \\ PPM Configuration» (см. Рисунок 6) параметры должны иметь значения:
  – «EIST» – «Disabled»;
  – «CPU C state Report» – «Disabled»;
  – «SOix» – «Disabled»;

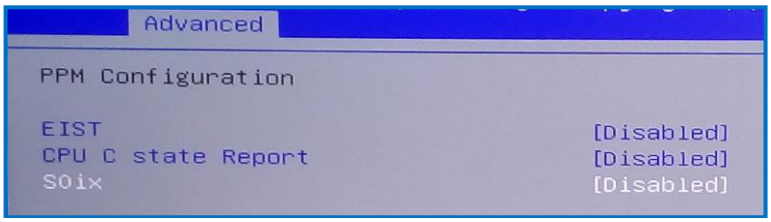

Рисунок 6 – Раздел «PPM Configuration»

– в разделе «Advanced \\ LPSS & SCC Configuration» (см. Рисунок 7) параметр «OS Selection» должен иметь значение «Android»;

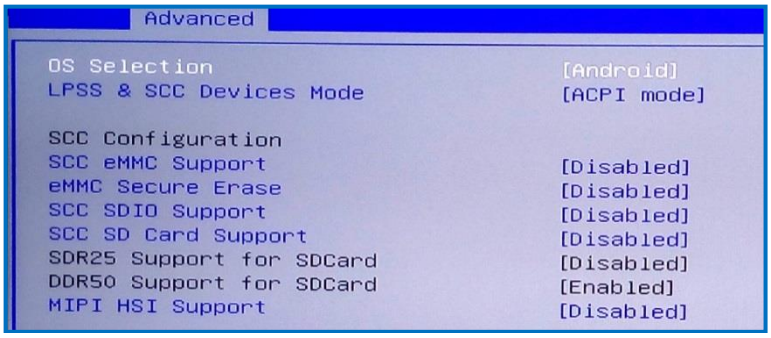

Рисунок 7 – Раздел «LPSS & SCC Configuration»

– в разделе «Advanced \\ System Component» (см. Рисунок 8) параметр «PNP Setting» должен иметь значение «Disabled»;

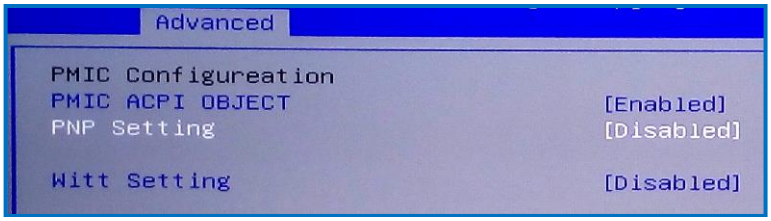

Рисунок 8 – Раздел «System Component»

– в разделе «Advanced \\ Trusted Computing» (см. Рисунок 9) параметр «Security Device Support» должен иметь значение «Disabled»;

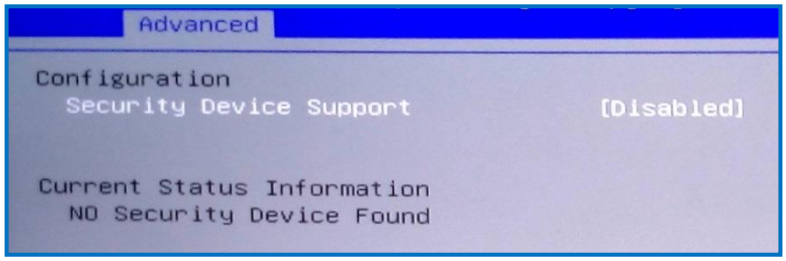

Рисунок 9 – Раздел «Trusted Computing»

– в разделе «Advanced \\ USB Configuration» (см. Рисунок 10) параметры должны иметь значения:
  – «USB Mass Storage Driver Support» – значение «Disabled»;

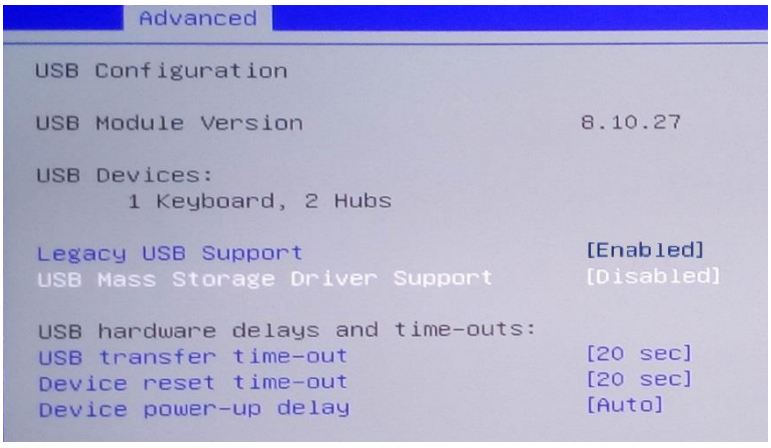

Рисунок 10 – Раздел «USB Configuration»

– в разделе «Boot» (см. Рисунок 11) параметр «Boot Option #1» должен иметь значение «HDD0».

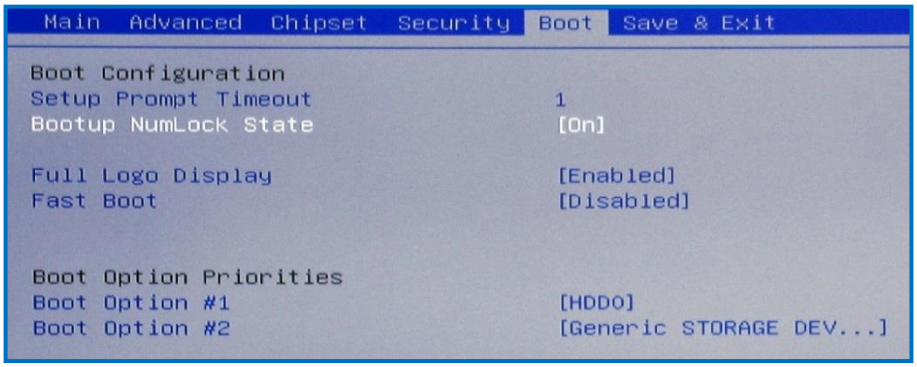

Рисунок 11 – Раздел «Boot»

Примечание – В случае выхода из строя батареи питания CMOS на системной плате АПК осуществляется замена батареи, повторная установка вышеперечисленных параметров BIOS и смена пароля на вход в меню BIOS. Периодичность смены батареи – один раз в пять лет.

4) В случае изменения настроек следует сохранить изменения, выбрав в разделе «Save & Exit» параметр «Save Changes».
5) Выключить АПК «кнопкой питания . После выключения кнопка питания будет подсвечиваться красным цветом.

3.1.3 Проверка контрольной суммы

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

3.1.4 Настройка сетевых параметров

По умолчанию для АПК «ЗАСТАВА-ТК» настроено автоматическое получение IP-адреса от DHCP-сервера. Если в вашей сети используется автоматическое получение IP-адреса, никаких дополнительных настроек производить не нужно. Достаточно проверить, что сетевое соединение установлено. Для этого надо подвести курсор мыши к значку сетевых соединений в трее, появившееся всплывающее сообщение должно содержать фразу «Проводное соединение <название сети> установлено».

Настройка сетевых параметров выполняется, если для АПК требуется задать статический адрес. Настройка сетевых параметров включает настройку IP-адреса и, при необходимости, настройку таблицы маршрутизации.

Для настройки сетевых параметров необходимо:

1) Включить АПК как описано в подразделе 3.2.1.
2) Нажать правой клавишей мыши на значок сетевых соединений в трее.
3) В появившемся меню выбрать команду «Изменить соединения». Появится окно «Сетевые соединения» (см. Рисунок 12).

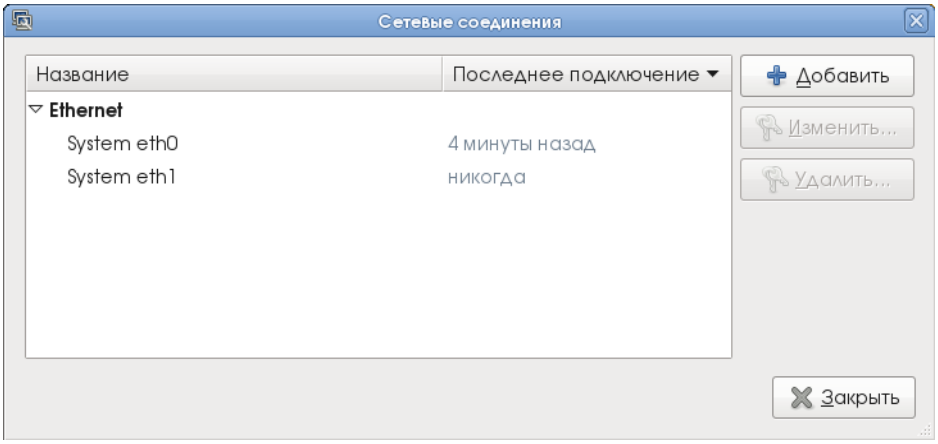

Рисунок 12 – Окно «Сетевые соединения»

4) Нажать кнопку «Добавить». Появится диалог выбора типа соединения (см. Рисунок 13).

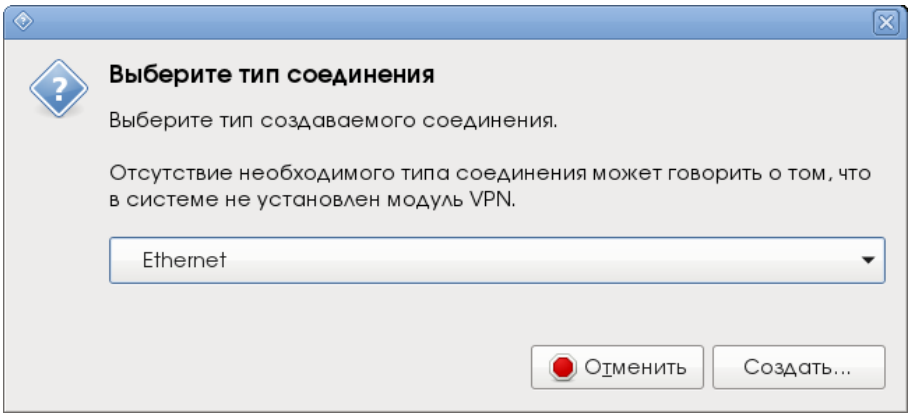

Рисунок 13 – Выбор типа сетевого соединения

5) Оставить тип соединения «Ethernet» и нажать кнопку «Создать». Откроется окно создания соединения (см. Рисунок 14).

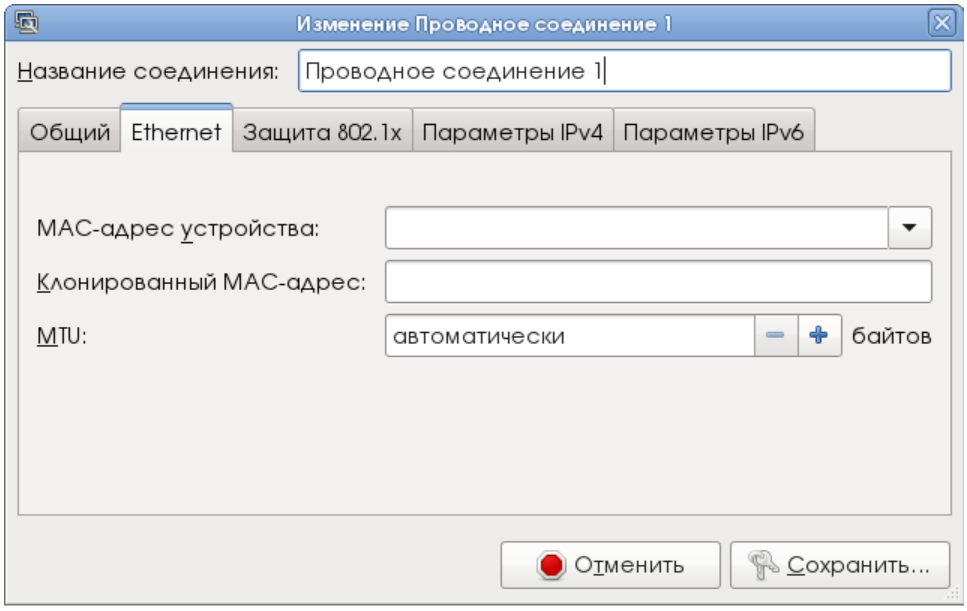

Рисунок 14 – Окно создания сетевого соединения

6) В поле «Название соединения» ввести имя создаваемого соединения.
7) На вкладке «Ethernet» из раскрывающегося списка выбрать «MAC-адрес устройства» (в данном случае в списке будет только одно значение). Остальные поля оставить без изменений (см. Рисунок 15).

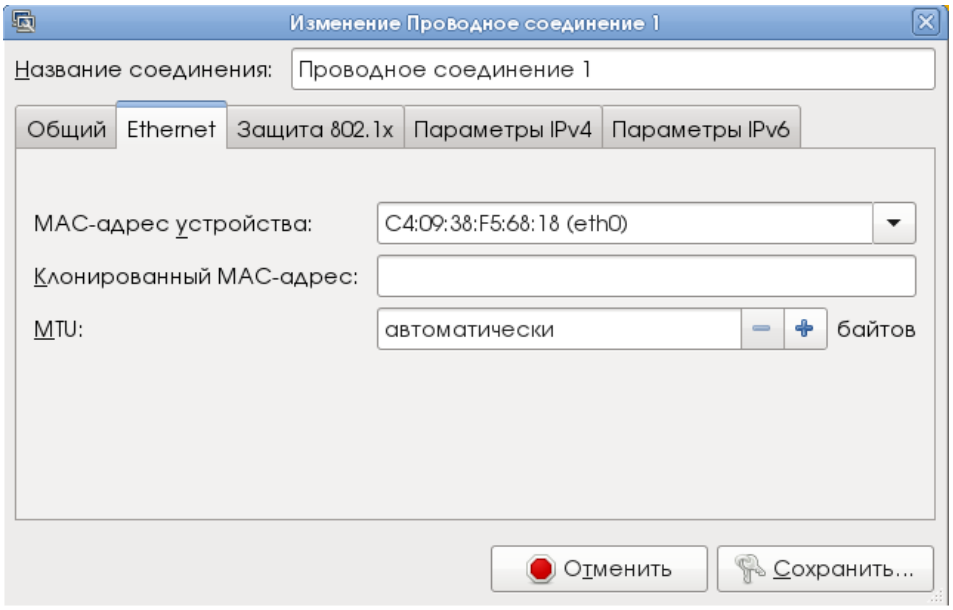

Рисунок 15 – Окно создания сетевого соединения с заполненными полями вкладки «Ethernet»

8) На вкладке «Параметры IPv4» выполнить следующие настройки (см. Рисунок 16):
   – в поле «Способ настройки» выбрать значение «Вручную»;
   – нажать кнопку «Добавить» и задать адрес сетевого интерфейса АПК с маской сети, а также адрес шлюза;
   – при необходимости задать адрес DNS-сервера;

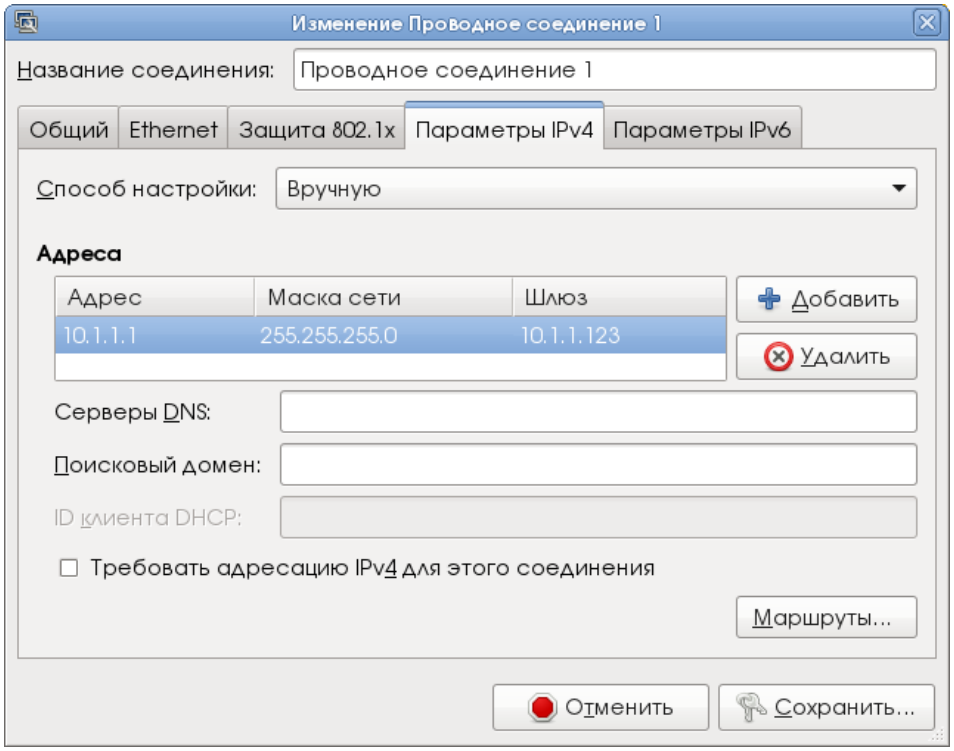

Рисунок 16 – Окно создания сетевого соединения. Вкладка «Парметры IPv4»

– при необходимости заполнить таблицу маршрутизации, для этого надо:

a) нажать кнопку «Маршруты»;

b) в открывшемся окне (см. Рисунок 17) нажать кнопку «Добавить» и ввести данные;

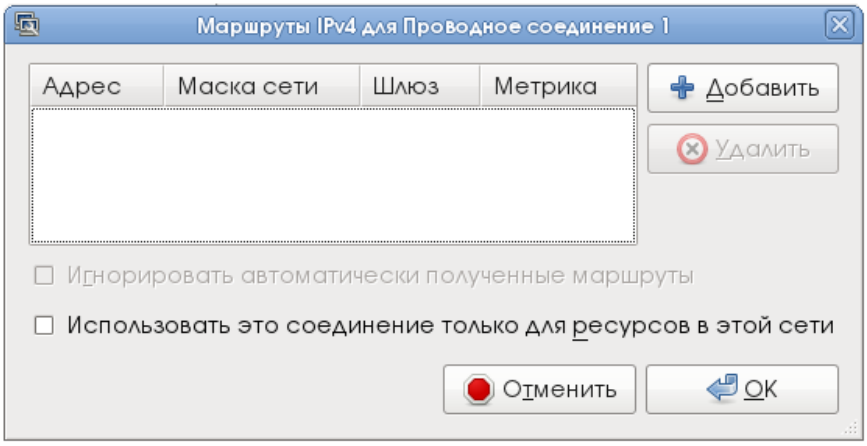

Рисунок 17 – Окно добавления маршрута

c) нажать кнопку «ОК», в результате маршрут будет добавлен, окно закроется.

9) Нажать кнопку «Сохранить» в окне создания сетевого соединения.

10) В появившемся окне «Аутентификация» (см. Рисунок 18) ввести PIN-код пользователя ключевого носителя администратора, затем нажать кнопку «Аутентификация».

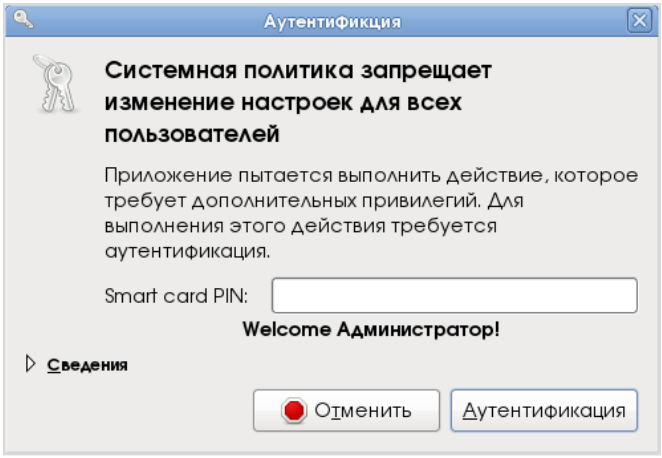

Рисунок 18 – Ввод PIN-кода

11) В окне «Сетевые соединения» появится строка с вновь созданным соединением (см. Рисунок 19). Нажать кнопку «Закрыть».

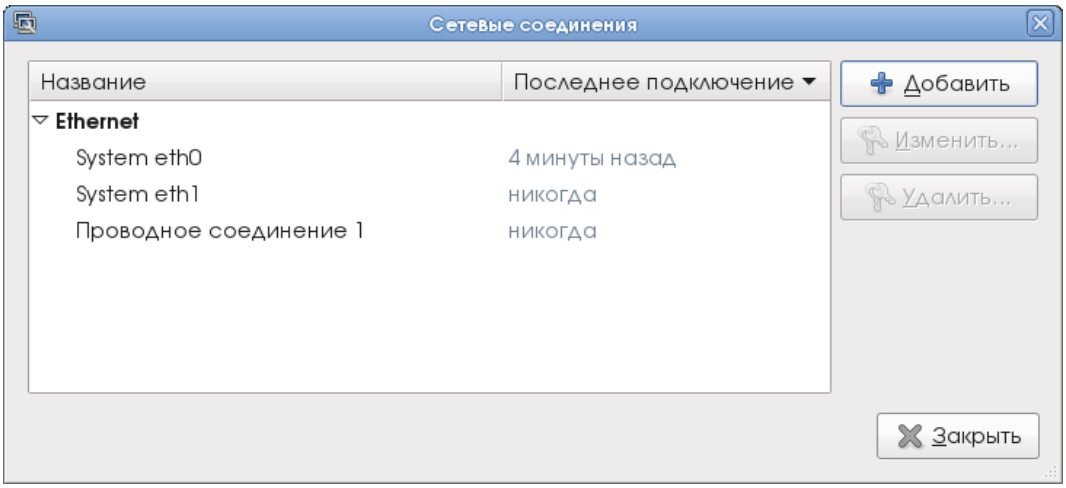

Рисунок 19 – Окно «Сетевые соединения». Добавлено вновь созданное соединение

12) Нажать на значок сетевых соединений в трее. В открывшемся меню вновь созданное соединение будет в списке доступных соединений (см. Рисунок 20). Для подключения необходимо нажать на название соединения. После подключения в трее появится всплывающее сообщение «Соединение установлено».

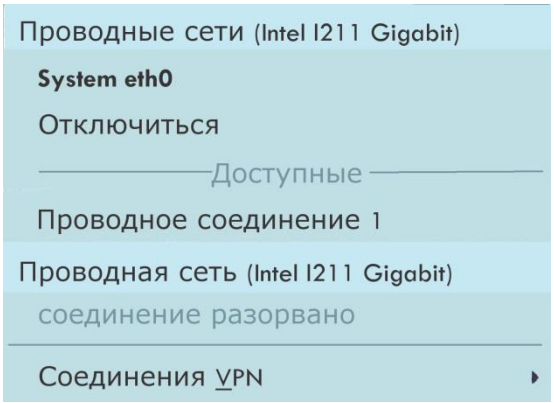

Рисунок 20 – Список соединений

3.1.5 Конфигурирование «ЗАСТАВА-Клиент»

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

Кроме того, «ЗАСТАВА-Клиент» может быть сконфигурирован в соответствии с потребностями пользователя с помощью графического интерфейса, как описано в разделе 4, или с помощью командной строки, как описано в разделе 5.

Настройка интерфейса «ЗАСТАВА-Клиент» может выполняться только администратором АПК. Остальным пользователям изменение настроек запрещено.

3.1.6 Настройка получения политики безопасности

При поставке в АПК в качестве текущей ЛПБ установлена политика, сохраненная в драйвере по умолчанию. При этом значок «ЗАСТАВА-Клиент» в трее – синего цвета . Необходимо установить в качестве текущей ЛПБ политику пользователя.

Политика пользователя создается в ЦУП и загружается на АПК по сети.

Настройка получения политики пользователя производится с помощью «ЗАСТАВА-Клиент».

Для настройки параметров получения пользовательской политики безопасности необходимо:

1) Открыть Панель управления «ЗАСТАВА-Клиент», нажав правой кнопкой мыши на значок в системном трее и выбрав пункт «Панель управления».
2) Открыть окно «Управление политиками», нажав кнопку «Политика» (см. Рисунок 21).

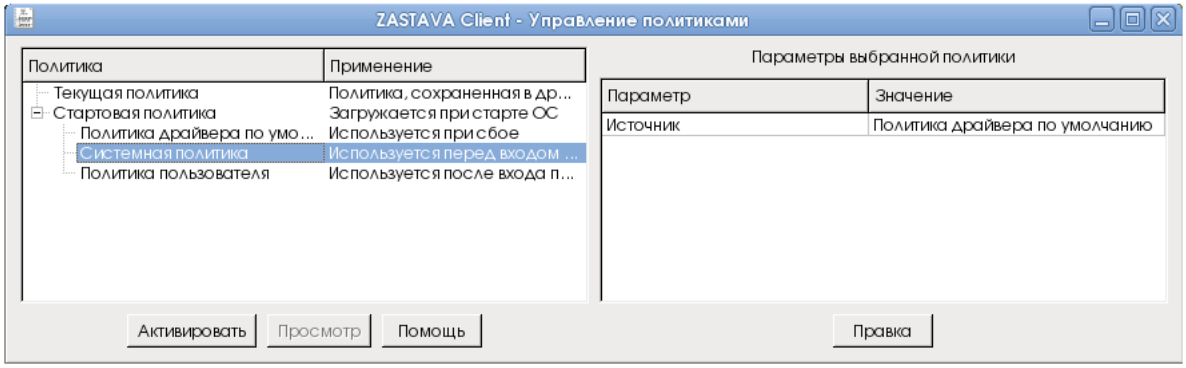

Рисунок 21 – Окно управления политиками

3) В открывшемся окне выбрать пункт «Политика пользователя» и нажать клавишу <Enter>. Откроется окно «Опции политики» (см. Рисунок 22).

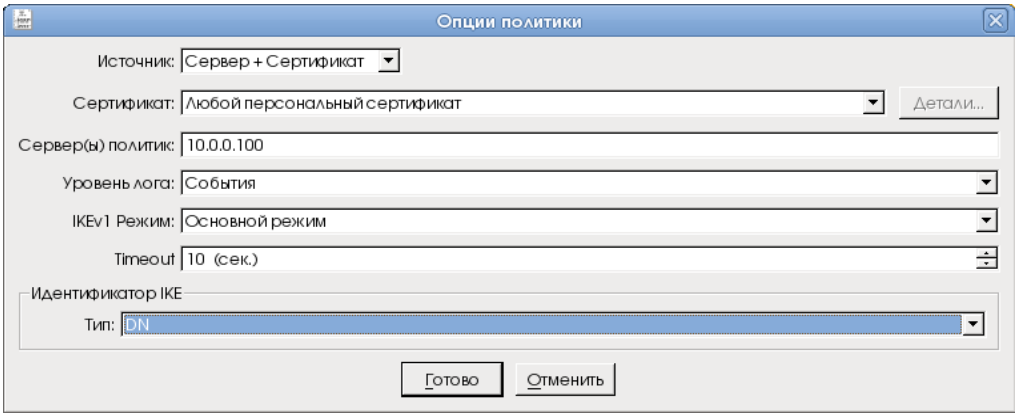

Рисунок 22 – Окно «Опции политики». Настройка политики пользователя

4) В окне «Опции политики» выполнить следующие настройки:
   - в поле «Источник» выбрать «Сервер + Сертификат» для загрузки ЛПБ с сервера ЦУП и установки SA IPsec с помощью сертификата;
   - в поле «Сервер(ы) политик» указать 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»;
     - «IKEv1 Режим» – «Основной режим»;
     - «Timeout» – 10 (сек).
5) Нажать кнопку «Готово». В появившемся запросе на активацию измененной политики выбрать «Да» (см. Рисунок 23).

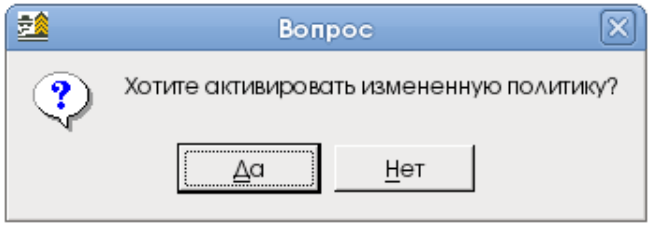

Рисунок 23 – Запрос на активацию политики

В результате будет загружена и активирована пользовательская политика. При успешной загрузке значок программы в трее изменит свой цвет на зеленый – .

3.2 Описание операций

Основные операции, выполняемые в АПК «ЗАСТАВА-ТК»:

– включение (см. подраздел 3.2.1);
– просмотр локальных журналов событий (см. подраздел 3.2.7);
– проверка контрольной суммы ОС (см. подраздел 3.2.2);
– настройка датчика вскрытия: изменение режима работы после срабатывания датчика вскрытия, смена пароля администратора и пароля на вход в меню BIOS (см. подраздел 3.2.3);
– смена PIN-кода ключевого носителя (см. подраздел 3.2.6);
– включение режима обработки CRL (см. подраздел 3.2.8);
– автоматический контроль целостности (см. подраздел 3.2.9);
– обновление (см. подраздел 3.2.10);
– выключение (см. подраздел 3.2.11).

3.2.1 Включение

Внимание! При эксплуатации АПК в круглосуточном режиме требуется обязательное извлечение ключевого носителя и перезагрузка АПК не реже, чем каждые 24 часа.

Для включения АПК необходимо:

1) Вставить ключевой носитель администратора АПК до упора в картоприемник на передней панели системного блока. При вставленном ключевом носителе на считываете смарт-карт будет светиться светодиод желтым цветом.
2) Включить АПК нажатием кнопки питания, после включения кнопка питания должна светиться зеленым цветом. Дождаться загрузки ОС.
3) В появившемся запросе ввести PIN-код пользователя ключевого носителя администратора АПК и нажать кнопку «Войти». Будет выполнен вход в систему.

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

3.2.2 Проверка контрольной суммы

Проверка контрольной суммы образа ОС производится администратором АПК в следующих случаях:

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

Результаты проверки заносятся в формуляр АПК.

Процедура проверки контрольной суммы:

1) Включить АПК, нажав кнопку питания, дождаться появления меню выбора вариантов загрузки «ARM-ZAGS load menu».

2) Выбрать пункт меню «Check control sum» и нажать клавишу <Enter>.
3) На экране появится сообщение о проверке контрольной суммы образа ОС. Дождаться окончания проверки.
4) По окончании проверки на экране появится сообщение с вычисленной контрольной суммой. Сверить вычисленную контрольную сумму с записанной в формуляре.
5) Выключить АПК, нажав кнопку питания.

3.2.3 Настройки датчика вскрытия

Меню датчика вскрытия позволяет выполнять следующие операции:

– менять пароль администратора (см. п. 3.2.3.2.1);
– менять пароль BIOS (см. п. 3.2.3.2.2);
– задавать режим работы АПК после срабатывания датчика вскрытия (см. п. 3.2.4);
– сбрасывать датчик вскрытия в состояние «корпус не вскрыт» (см. п. 3.2.5).

3.2.3.1 Меню датчика вскрытия

Для входа в меню датчика вскрытия следует при включении компьютера, но до начала загрузки ОС, нажимать клавишу <Ctrl> до появления меню датчика вскрытия (см. Рисунок 24).

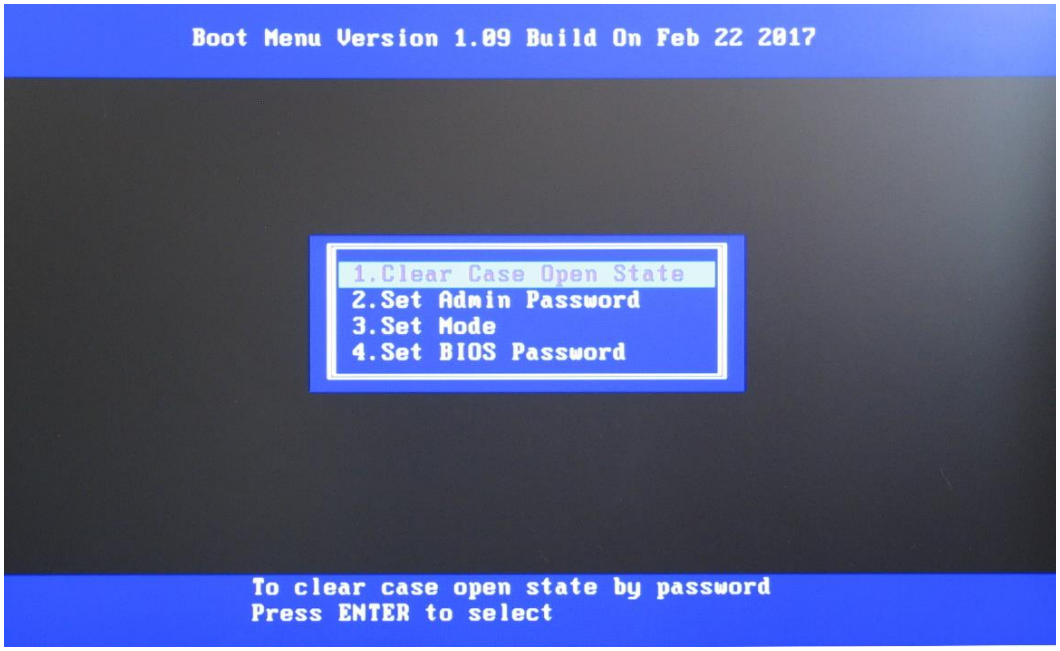

Рисунок 24 – Меню датчика вскрытия

Меню датчика вскрытия содержит следующие пункты:

– Clear Case Open State – сброс состояния датчика вскрытия;
– Set Admin Password – установка пароля администратора контроля вскрытия;
– Set Mode – выбор режима работы АПК после срабатывания датчика вскрытия:
  – Soft – возможна загрузка ОС без сброса состояния датчика вскрытия. При этом в BIOS остается информация о времени вскрытия;
  – Hard – без сброса состояния датчика загрузка ОС невозможна;
– Set BIOS Password – установка пароля на BIOS.

3.2.3.2 Установка пароля

Из меню датчика вскрытия можно изменить как пароль администратора безопасности, так и пароль от BIOS.

3.2.3.2.1 Установка пароля администратора

Для установки пароля администратора необходимо:

1) В меню датчика вскрытия выделить строку «Set Admin Password» и нажать клавишу <Enter>. Появится предложение ввода текущего пароля администратора: «Input previous administrator password».
2) Ввести пароль администратора и нажать клавишу <Enter>. Появится предложение ввода нового пароля администратора: «Input new administrator password».
3) Ввести новый пароль и нажать клавишу <Enter>.

Внимание! Для обеспечения требуемого уровня защиты от НСД пароль должен состоять из случайного набора не менее восьми буквенно-цифровых символов. В составе пароля нельзя использовать: повторяющиеся комбинации; повторяющиеся символы, а также символы, расположенные на клавиатуре в закономерном порядке; данные, связанные с личностью пользователя (дата рождения, имя и т.д.).

4) Повторить ввод нового пароля и нажать клавишу <Enter>. В результате пароль будет изменен, появится сообщение об успешном изменении пароля и выключении АПК: «Modify administrator password success, please power off manually!».
5) Выключить АПК, нажав кнопку питания.

3.2.3.2.2 Установка пароля на BIOS

Для установки пароля на BIOS необходимо:

1) В меню датчика вскрытия выделить строку «Set BIOS Password» и нажать клавишу <Enter>. Появится предложение ввода пароля администратора: «Input administrator password».
2) Ввести пароль администратора и нажать клавишу <Enter>. Появится предложение ввода нового пароля на BIOS: «Input new BIOS password».
3) Ввести новый пароль на BIOS и нажать клавишу <Enter>.

Внимание! Для обеспечения требуемого уровня защиты пароль должен состоять из случайного набора не менее восьми буквенно-цифровых символов. В составе пароля нельзя использовать: повторяющиеся комбинации; повторяющиеся символы, а также символы, расположенные на клавиатуре в закономерном порядке; данные, связанные с личностью пользователя (дата рождения, имя и т.д.).

4) Повторить ввод нового пароля и нажать клавишу <Enter>. В результате пароль будет изменен, появится сообщение об успешном изменении пароля и выключении АПК: «Modify bios password success, please power off manually!».

5) Выключить АПК, нажав кнопку питания.

3.2.4 Режимы работы после срабатывания датчика вскрытия

После срабатывания датчика вскрытия возможны два режима работы АПК:

– Soft – в случае срабатывания датчика вскрытия возможна загрузка ОС и дальнейшая штатная работа. При этом сброс состояния датчика вскрытия не производится, т.о. каждый раз при включении/перезагрузке АПК будет срабатывать сигнализация датчика вскрытия. В режиме Soft сброс состояния датчика вскрытия возможно произвести впоследствии в любой удобный момент;

  Режим Soft рекомендуется выбирать при физической удаленности администратора АПК от места установки АПК.

– Hard – при выборе данного режима, после срабатывания датчика вскрытия загрузка ОС и работа с АПК невозможны без сброса состояния датчика вскрытия.

3.2.4.1 Режим Soft

В режиме Soft возможна загрузка ОС и дальнейшая работа с АПК. Если датчик вскрытия зафиксировал вскрытие корпуса, то при включении компьютера раздастся звуковой сигнал и на экране появится сообщение «A case open event has occurred. Do you want to continue entering system ?(y/n)».

Следует нажать клавишу <y> для загрузки ОС АПК и продолжения работы в штатном режиме.

При нажатии клавиши <n> произойдет перезагрузка АПК и снова появится сообщение о вскрытии корпуса.

Сообщение о вскрытии корпуса будет появляться каждый раз при перезагрузке/включении АПК до сброса состояния датчика вскрытия (см. п. 3.2.5).

3.2.4.2 Режим Hard

Режим Hard предполагает невозможность загрузки ОС после срабатывания датчика вскрытия корпуса. Если датчик вскрытия зафиксировал вскрытие корпуса, то при включении компьютера раздастся звуковой сигнал и на экране появится сообщение «A case open event has occurred. Press “Enter” key to restart».

Для продолжения работы следует сбросить датчик вскрытия с исходное состояние (см. п. 3.2.5).

3.2.4.3 Переключение между режимами Soft и Hard

При поставке установлен режим Soft. Для изменения режима работы АПК после срабатывания датчика вскрытия, необходимо:

1) В меню датчика вскрытия выделить строку «Set Mode» и нажать клавишу <Enter>. Появится предложение ввода пароля администратора: «Input administrator password».

2) Ввести пароль администратора и нажать клавишу <Enter>. На экране появится запрос на изменение режима с указанием текущего режима работы.
3) Нажать клавишу <y> для изменения режима. На экране появится сообщение об успешном изменении режима работы (см. Рисунок 25).

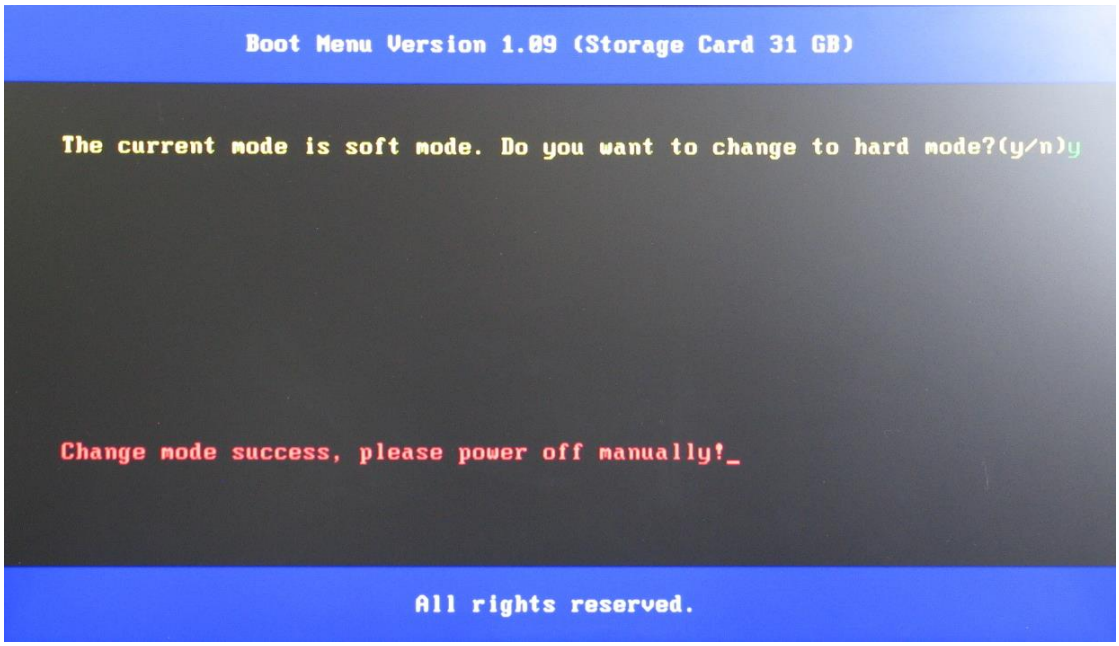

Рисунок 25 – Вид экрана после изменения режима на Hard

4) Выключить АПК, нажав кнопку питания.

3.2.5 Сброс состояния датчика вскрытия

Для сброса датчика вскрытия в состояние «корпус не вскрыт» необходимо:

1) Зайти в меню датчика вскрытия. Для этого при включении АПК до начала загрузки ОС нажимать клавишу <Ctrl> до появления меню датчика вскрытия.
2) В меню датчика вскрытия выделить пункт «Clear Case Open State» (см. Рисунок 26) и нажать клавишу <Enter>.

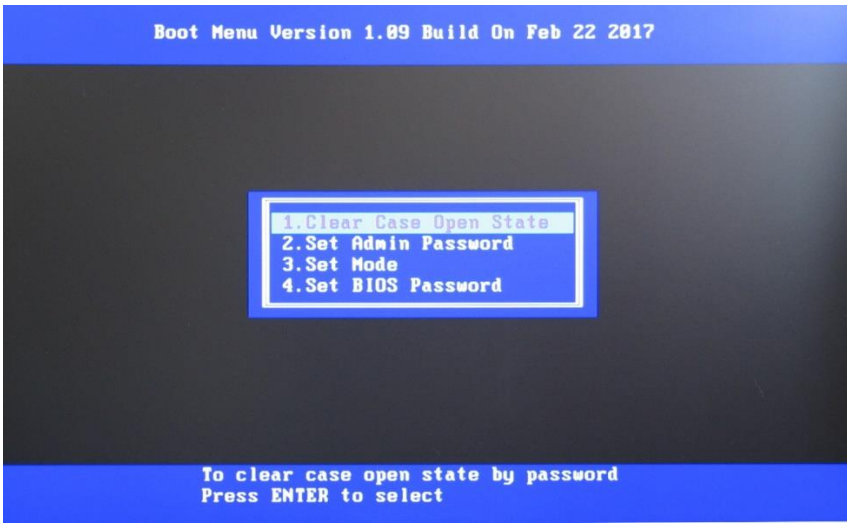

Рисунок 26 – Меню датчика вскрытия, выделен пункт «Clear Case Open State»

3) На экране ввода пароля ввести пароль администратора и нажать клавишу <Enter>. Датчик вскрытия будет сброшен в состояние «корпус не вскрыт».

4) Выключить питание АПК, нажав кнопку питания.

3.2.6 Смена PIN-кода ключевого носителя

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

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

Процедура смены PIN-кода ключевого носителя приведена в п. 4.9.1.

3.2.7 Просмотр локальных журналов событий

Просмотр локальных журналов событий осуществляется администратором для выявления причин неисправности АПК. Администратору доступны следующие журналы:

– журнал СКЗИ (см. п. 3.2.7.1);
– журнал событий (см. п. 3.2.7.2).

3.2.7.1 Просмотр журнала СКЗИ

Для просмотра журнала СКЗИ необходимо:

1) Открыть Панель управления «ЗАСТАВА-Клиент», нажав правой кнопкой мыши на значок  в системном трее и выбрав пункт «Панель управления».

2) Открыть журнал нажатием кнопки  «Журнал» на Панели управления (см. Рисунок 27).

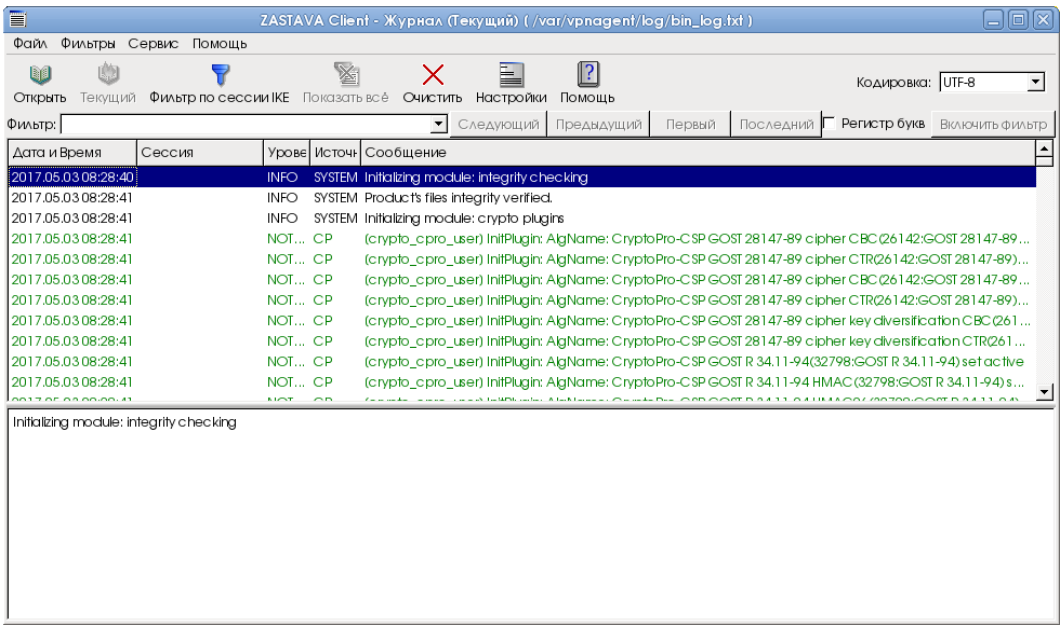

Рисунок 27 – Журнал

В журнале возможна фильтрация отображаемых событий по одному из предустановленных фильтров, либо по произвольно заданному тексту. Подробное описание работы с журналом приведено в подразделе 4.5

3.2.7.2 Просмотр журнала событий

Журнал событий ОС Linux хранится в директории `/var/log/auth/all`.

Открыть журнал событий для просмотра можно, например, с помощью команды: `Less`, для этого необходимо:

1) Открыть терминал, нажав на значке  в меню приложений (см. Рисунок 28).

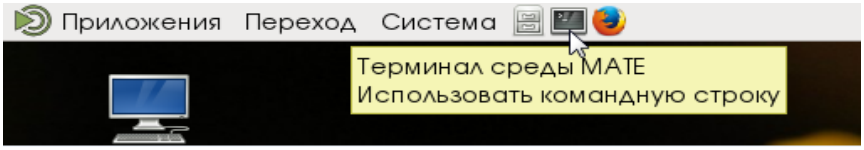

Рисунок 28 – Запуск терминала

2) Открыть журнал (см. Рисунок 29) с помощью команды: `less /var/log/auth/all`

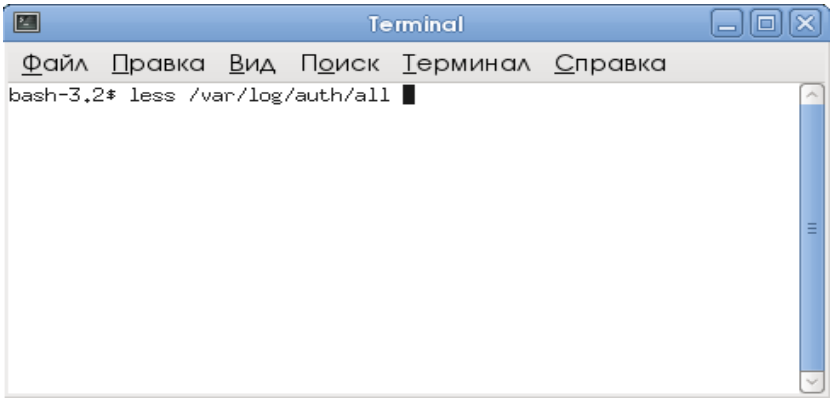

Рисунок 29 – Терминал

Журнал будет открыт в терминале (см. Рисунок 30).

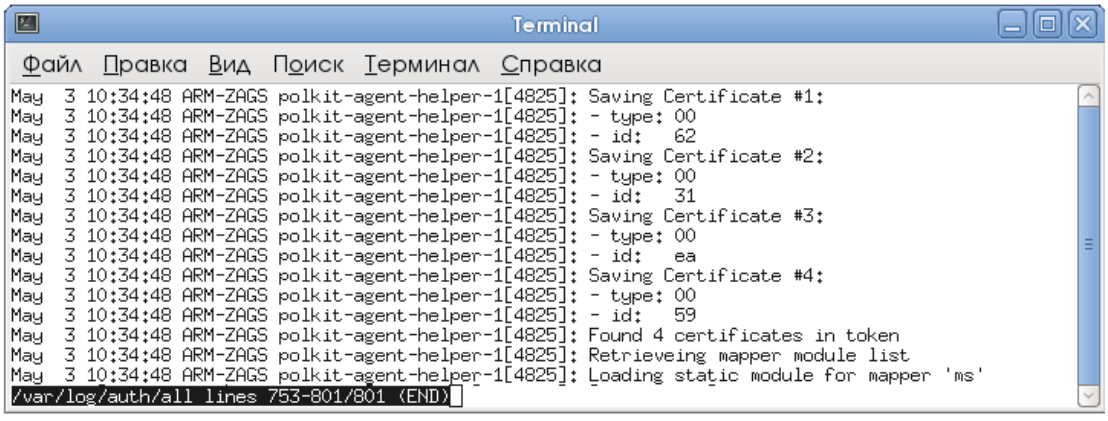

Рисунок 30 – Просмотр журнала событий

3) Выполнить поиск по журналу. Основные команды `Less`:

– `h` — вызов справки;
– `q` — выход;
– `SPACE` — на экран вперёд;

– ← , → — горизонтальная прокрутка;
– ↓ , ↑ — вертикальная прокрутка;
– `F` — просмотр растущего файла;
– `<N>g` — перейти на строку N (по умолчанию: 1);
– `<N>%` — перейти на позицию N% (к примеру, 50 %);
– `/pattern` — поиск по шаблону вперёд;
– `?pattern` — поиск по шаблону назад;
– `n` — следующее совпадение;
– `N` — предыдущее совпадение.

3.2.8 Включение режима обработки CRL

Для включения обработки CRL необходимо:

1) Включить АПК (либо выполнить перезагрузку).
2) В меню загрузчика выбрать пункт «Enable CRL processing for login OS» (см. Рисунок 31).

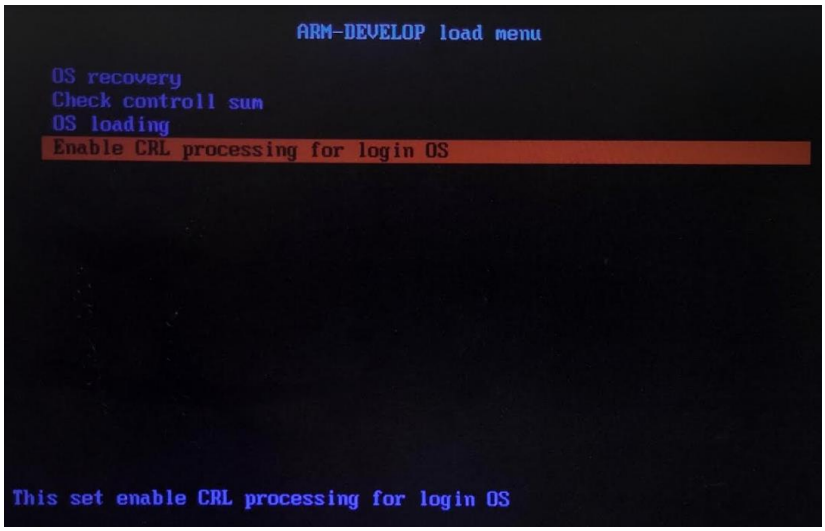

Рисунок 31 – Пункт меню загрузчика «Enable CRL processing for login OS»

3) На экране АПК отобразится поле для введения пароля. Ввести пароль, заданный Изготовителем (Поставщиком) (см. Рисунок 32).

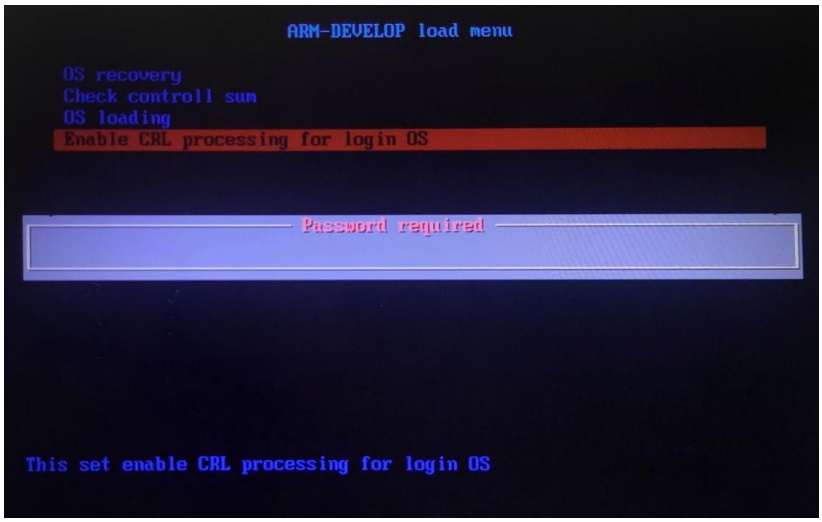

Рисунок 32 – Окно ввода пароля на включение обработки CRL

4) Дождаться появления окна ввода IP-адреса сервера, с которого будет получен CRL.
5) Ввести IP-адрес сервера, с которого будет получен CRL (см. Рисунок 33). Нажать клавишу <Enter>.

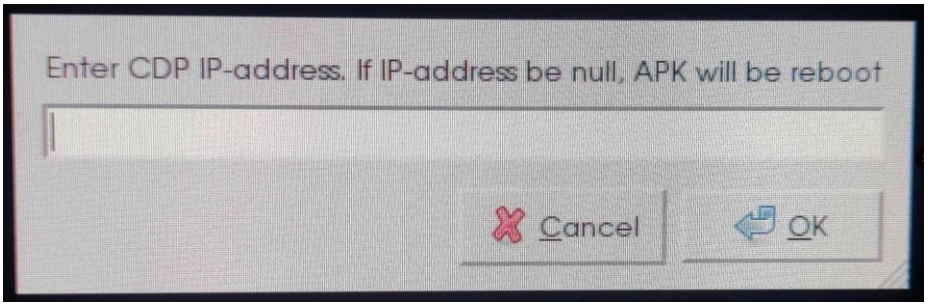

Рисунок 33 – Окно ввода IP-адреса сервера, с которого будет загружен CRL

6) На экране АПК отобразится сообщение с предупреждением о перезагрузке АПК. (см. Рисунок 34).

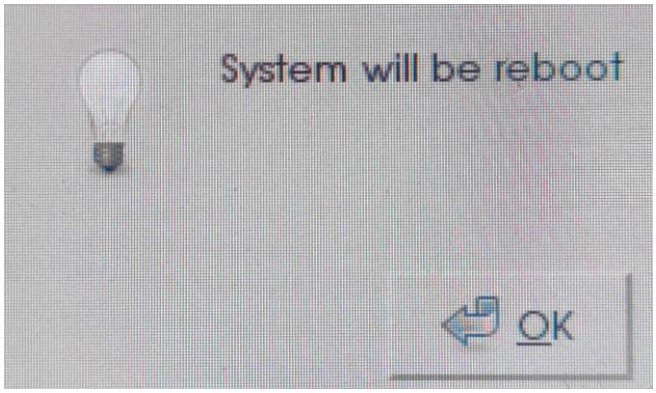

Рисунок 34 – Окно предупреждения о необходимости перезагрузки

7) Нажать кнопку «ОК». АПК перезагрузится.

После включения обработки CRL системная политика «ЗАСТАВА-Клиент» автоматически меняется с «Default Driver Policy» (DDP) на политику загружаемую «из файла». Файл политики расположен по адресу /root/SYSTEM_LSP.txt. В политику автоматически добавляются фильтры на пропуск трафика TCP для взаимодействия с сервером, с которого загружается CRL. Пример политики изображен на рисунке (см. Рисунок 35).

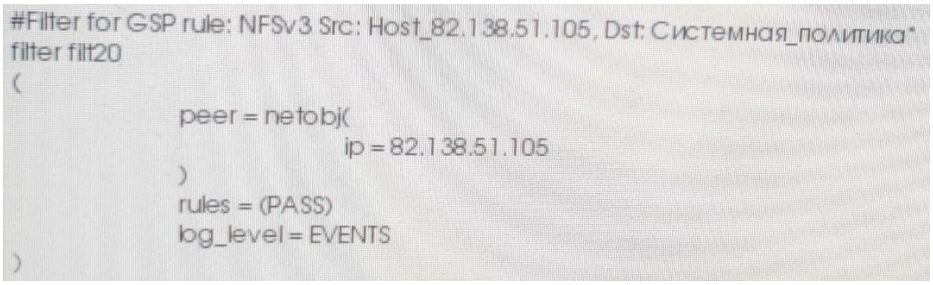

Рисунок 35 – Пример системной политики

Для отключения режима обработки CRL необходимо выполнить операцию «Возврат к эталону» (см. подраздел 6.2).

3.2.9 Автоматический контроль целостности

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

По умолчанию контроль целостности запускается один раз в три часа.

В случае положительного результата прохождения контроля целостности в системный журнал journalctl, записывается событие «Динамический контроль СКЗИ пройден УСПЕШНО».

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

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

В случае нарушения целостности АПК выключается.

3.2.10 Обновление

Обновление ОС производится в автоматическом режиме. Обновление осуществляется в соответствии с требованиями документа МКЕЮ.00629.ИЭ «Аппаратно-программный комплекс «VPN/FW «ЗАСТАВА-ТК», версия 6» (АПК «ЗАСТАВА-ТК», версия 6). Правила пользования.

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

3.2.11 Выключение

Для выключения АПК необходимо:

1) Завершить работу всех программ, запущенных на АПК;
2) Выключить питание одним из способов:
   – В меню приложений выбрать команду «Система» → «Выключение» (см. Рисунок 36).
   – Нажать кнопку питания .

   Дождаться завершения работы ОС и выключения АПК. При выключенном АПК кнопка питания подсвечивается красным цветом.

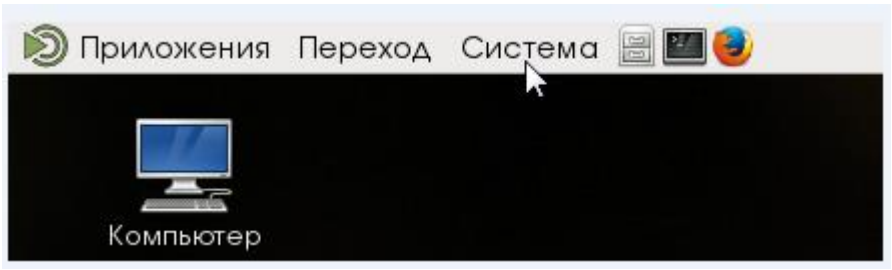

Рисунок 36 – Меню приложений

4 Графический интерфейс «ЗАСТАВА-Клиент»

4.1 Запуск графического интерфейса «ЗАСТАВА-Клиент»

Системные модули «ЗАСТАВА-Клиент» запускаются автоматически при загрузке ОС и работают постоянно в фоновом режиме. При работе «ЗАСТАВА-Клиент» в системном трее присутствует значок программы – .

При необходимости, открыть графический интерфейс «ЗАСТАВА-Клиент» можно одним из способов:

- дважды нажать на значок в системном трее;
- нажать правой клавишей мыши на значок в системном трее и в появившемся контекстном меню (см. Рисунок 37) выбрать требуемый пункт. Из контекстного меню можно открыть Панель управления или одно из окон «ЗАСТАВА-Клиент»;
- выполнить команду: `/opt/ZASTAVAclient/bin/vpnagent`.

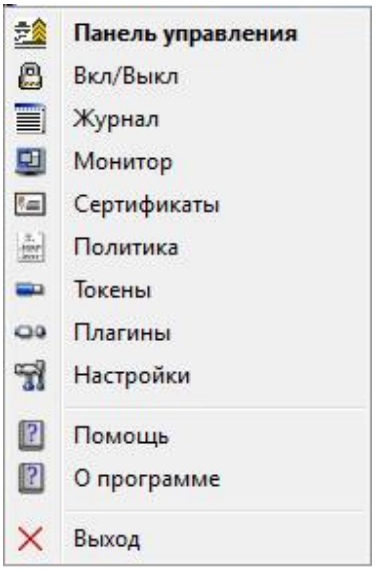

Рисунок 37 – Контекстное меню значка «ЗАСТАВА-Клиент» в системном трее

4.2 Индикация текущего статуса

Текущий статус локальной политики безопасности (ЛПБ) «ЗАСТАВА-Клиент» отображается цветом значка в трее, кроме того, текущий статус можно просмотреть в нижней части Панели управления «ЗАСТАВА-Клиент» (см. подраздел 4.1).

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

Статусы «ЗАСТАВА-Клиент» представляются разными графическими символами (см. Таблица 4).

Таблица 4 – Перечень графических символов статусов ЛПБ

Статус «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; предыдущая политика будет восстановлена	(жёлтый)
Активирована «Политика драйвера по умолчанию»	(синий)
Системная служба «ЗАСТАВА-Клиент» `vpndmn` не запущена	(серый)
При загрузке политики «ЗАСТАВА-Клиент» с Центром управления политиками безопасности (далее - ЦУП) (сервер доступен)	(темно зеленый с ярко зеленой рамкой)
При загрузке политики «ЗАСТАВА-Клиент» с ЦУП (сервер недоступен)	(желтый с красной рамкой)

4.3 Ввод пароля токена

Ввод пароля ключевого носителя (токена) требуется тогда, когда «ЗАСТАВА-Клиент» начинает инициировать создание защищенного соединения с сервером ЦУП. В процессе создания соединения при обращении к персональному сертификату будет запрошен пароль (PIN-код токена) ключевого носителя (см. Рисунок 38).

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

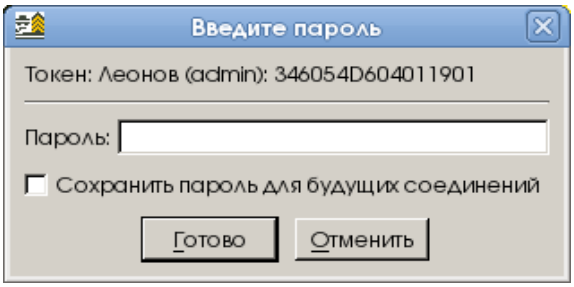

Рисунок 38 – Ввод пароля токена при создании защищенного соединения

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

4.4 Панель управления

Панель управления «ЗАСТАВА-Клиент» (см. Рисунок 39) содержит кнопки, при помощи которых можно выполнить необходимую операцию или открыть дополнительное окно.

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

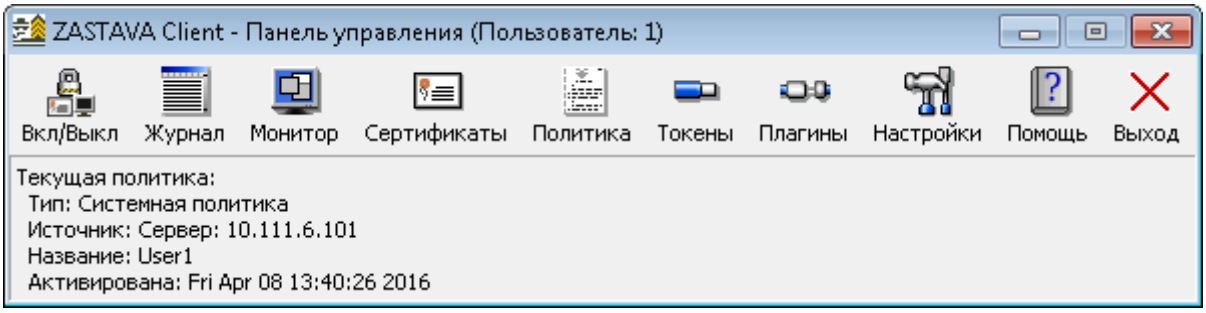

Рисунок 39 – Панель управления

Описание кнопок Панели управления приведено в таблице (см. Таблица 5).

Таблица 5 – Кнопки Панели управления

Кнопка	Описание
Вкл/Выкл	Переключение между пользовательской и системной политикой безопасности: «Вкл» – прогружается пользовательская политика; «Выкл» – удаляются все созданные «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 компьютером.
Сертификаты	Открывает окно «Сертификаты и Ключи», предназначенное для регистрации в «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 «ЗАСТАВА-Клиент». Изменять настройки может только администратор АПК. Остальным пользователям изменение настроек запрещено.
Помощь	Отображает меню, содержащее следующие команды: Помощь – вызывает справочную систему «ЗАСТАВА-Клиент»; О ZASTAVA Client – отображает окно с информацией о программе. Подробно см. подраздел 4.12.
Выход	Закрывает графический интерфейс «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 40) открывается нажатием кнопки «Журнал» на Панели управления. В журнале отображается содержимое файла регистрации событий «ЗАСТАВА-Клиент».

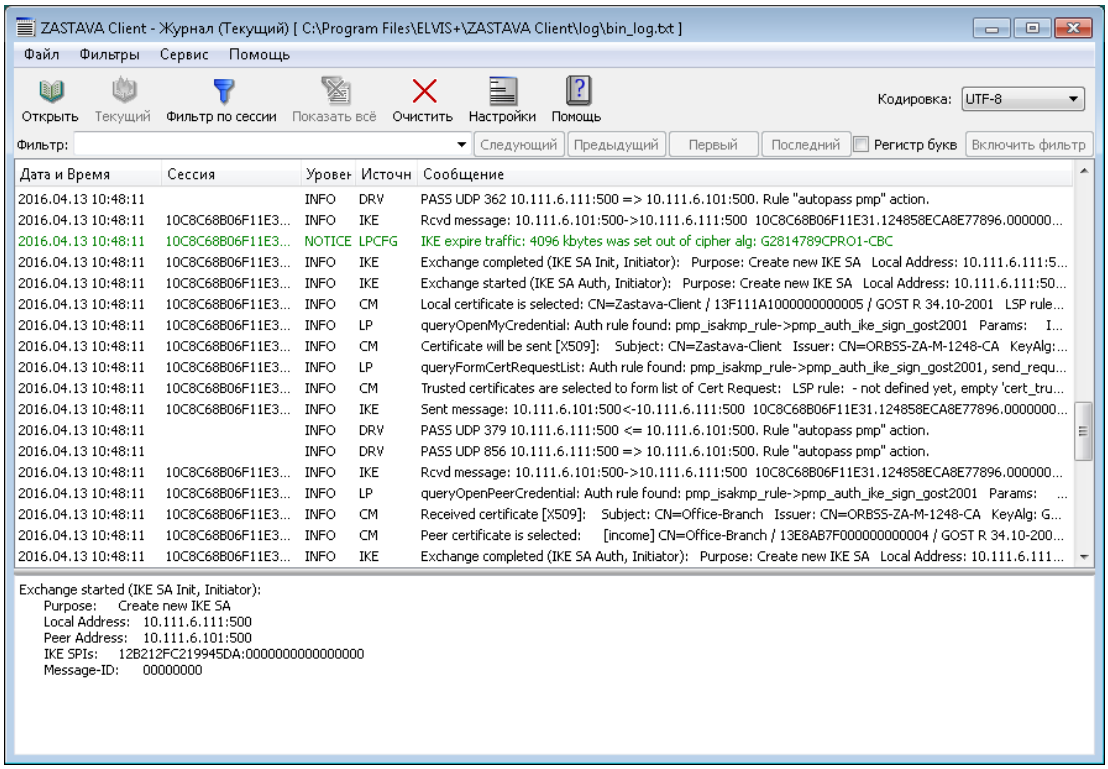

Рисунок 40 – Окно с зарегистрированными событиями

В верхней части окна расположена панель управления.

Основную часть окна занимает таблица с описанием системных событий. Уровень детализации настраивается пользователем (подробнее см. п. 4.5.3).

Системные события в таблице разбиты по следующим параметрам:

- дата и время – время регистрации события;
- сессия – шестнадцатеричное выражение, составленное из: cookie Initiator; cookie Responder; Messenger ID. Причем любое из двух первых выражений служит идентификатором IKE-сессии;
- уровень – значимость события (INFO, WARNING, ERROR и т.д.);
- источник – программный модуль, в котором произошло событие;
- сообщение – текстовое представление произошедшего системного события.

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

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

4.5.1 Структура окна «Журнал»

4.5.1.1 Строка меню окна «Журнала»

Строка меню содержит следующие меню: «Файл», «Фильтры», «Сервис», «Помощь». Команды меню представлены в таблице (см. Таблица 6).

Таблица 6 – 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 общей справочной системы «ЗАСТАВА-Клиент».

4.5.1.2 Панель инструментов окна «Журнал»

Описание элементов Панели инструментов окна «Журнал» приведено в таблице (см. Таблица 7).

Таблица 7 – Описание кнопок панели инструментов окна «Журнал»

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

4.5.1.3 Контекстное меню окна «Журнал»

Команды контекстного меню окна «Журнал» и их описание приведены в таблице (см. Таблица 8).

Таблица 8 – 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»).

Команда	Характеристика
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 Фильтрация отображаемых событий

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

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

Чтобы отфильтровать события по произвольно заданному тексту надо 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 надо нажать правой клавишей мыши на нужной ячейке и в появившемся контекстном меню выбрать команду «Копировать в поле фильтра».

4.5.3 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 41) производится настройка параметров регистрации событий. Содержание вкладки полностью дублирует вкладку «Журнал» окна «Прочие настройки» и настраивается аналогичным образом (см. п. 4.11.1).

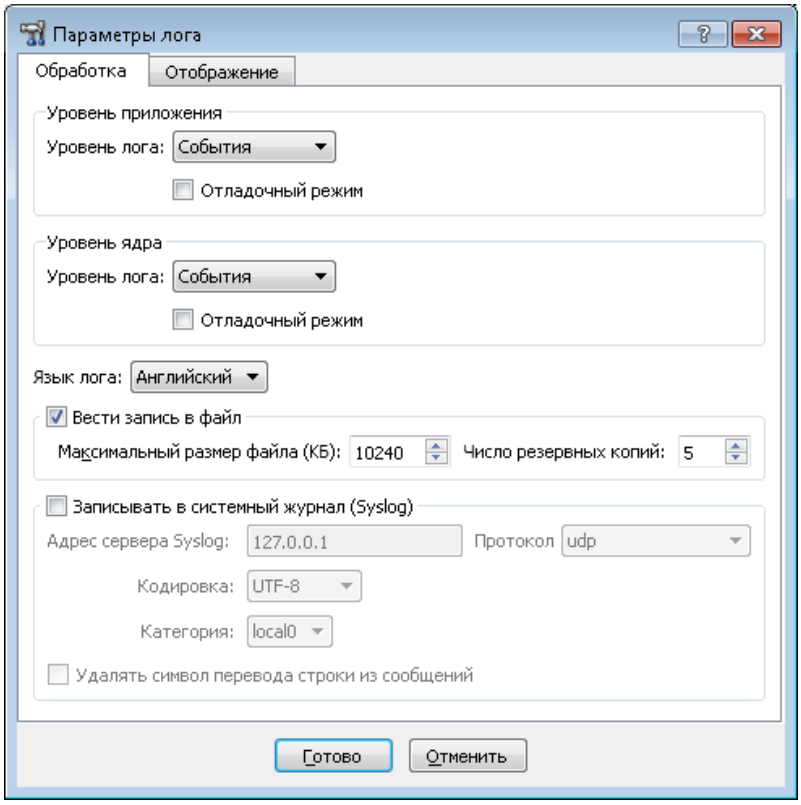

Рисунок 41 – Окно настройки параметров регистрации событий

Параметры представления журнала настраиваются на вкладке «Отображение» (см. Рисунок 42).

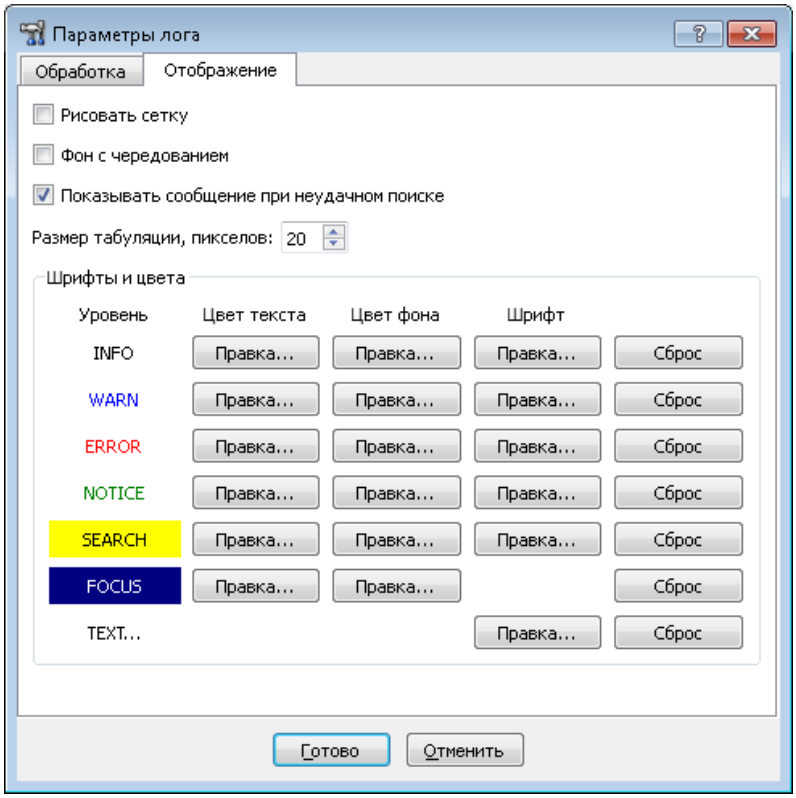

Рисунок 42 – Настройка параметров представления журнала

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

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

Для отмены настроек следует нажать кнопку «Отменить».

4.5.4 Копирование описания событий

Для копирования информации необходимо:

1) Выделить одну или несколько строк в журнале. Выделение нескольких строк производится 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 скопирована в выбранное приложение.

4.5.5 Файл регистрации системных событий

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

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

4.5.6 Очистка журнала и файла регистрации системных событий

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

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

4.6 Окно «Монитор»

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

Кроме того, окно «Монитор» позволяет провести фильтрацию защищённых соединений, просмотреть статистику по пакетам, список выделенных адресов ike-cfg, а также

параметры шлюзов прикладного уровня. Окно содержит несколько вкладок, как показано на рисунке (см. Рисунок 43).

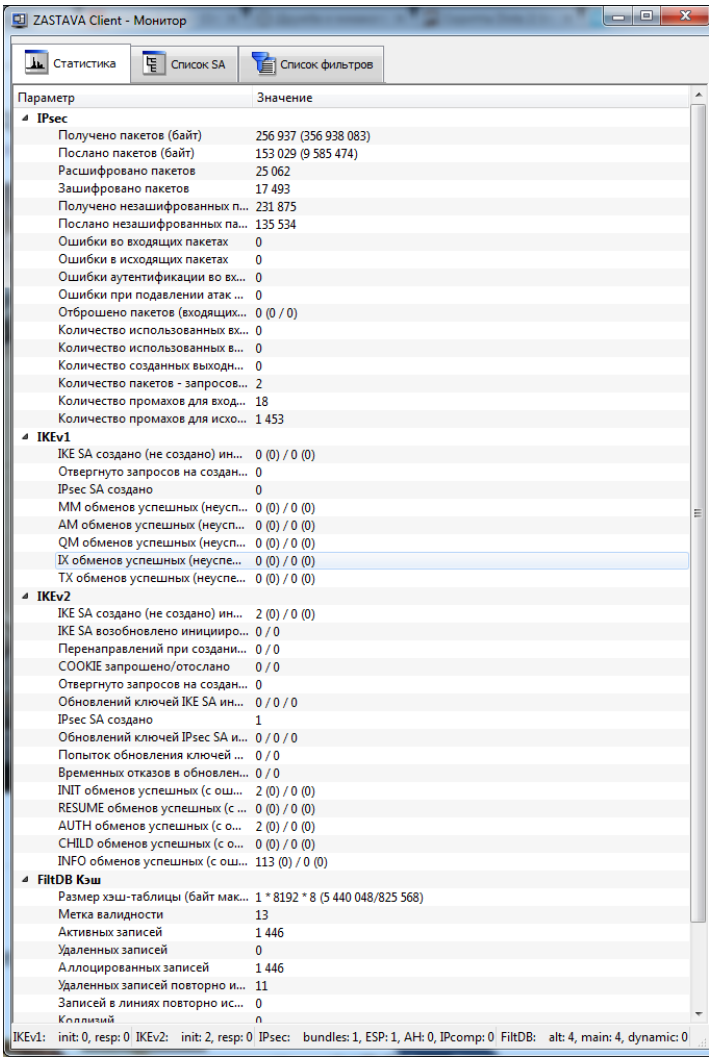

Рисунок 43 – Окно «Монитор», вкладка «Статистика»

4.6.1 Вкладка «Статистика»

На вкладке «Статистика» (см. Рисунок 43) можно получить статистическую информацию по всем пакетам, прошедшим через драйвер «ЗАСТАВА-Клиент» (например, по протоколу IPsec) (см. Таблица 9).

Таблица 9 – 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

Параметр	Описание
Ошибки аутентификации во входящих пакетах	Количество ошибок аутентификации во входящих пакетах
Ошибки при подавлении атак воспроизведения во входящих пакетах	Количество ошибок при подавлении атак воспроизведения во входящих пакетах
Отброшено пакетов (входящих/исходящих)	Количество отброшенных пакетов или фрагментов
Количество использованных входных фрагментов	Количество IP-фрагментов, использованных при реассемблировании входного пакета
Количество использованных выходных фрагментов	Количество IP-фрагментов, использованных при реассемблировании выходного пакета
Количество созданных выходных фрагментов	Количество IP-фрагментов, созданных при фрагментации выходного пакета
Количество пакетов – запросов на понижение MTU	Количество пакетов – запросов на понижение MTU
Количество промахов для входящих пакетов при поиске фильтра в хэш-таблице	Количество промахов для входящих пакетов при поиске фильтра в хэш-таблице
Количество промахов для исходящих пакетов при поиске фильтра в хэш-таблице	Количество промахов для исходящих пакетов при поиске фильтра в хэш-таблице
IKEv2	
IKE SA создано (не создано) инициированных/отвеченных	Количество созданных (не созданных) инициированных/ отвеченных IKE SA в формате x(x)/x(x)
IKE SA возобновлено инициированных/отвеченных	Количество возобновленных IKE SA инициированных/отвеченных
Перенаправлений при создании IKE SA получено/послано	Количество перенаправлений IKE SA получено/послано
COOKIE запрошено/отослано	Количество запрошенных/отправленных токенов COOKIE
Отвергнуто запросов на создание IKE SA	Количество отвергнутых запросов на создание IKE SA
Обновлений ключей IKE SA инициированных/отвеченных/ коллизий	Количество обновлений ключей IKE SA инициированных/ отвеченных/коллизий в формате x/x/x
IPsec SA создано	Количество созданных IPsec SA
Обновлений ключей IPsec SA инициированных/отвеченных/ коллизий	Количество обновлений ключей IPsec SA инициированных/ полученных/коллизий в формате x/x/x
Попыток обновления ключей несуществующей IPsec SA данным хостом/партнером	Количество попыток обновления ключей несуществующей IPsec SA данным хостом/партнером
Временных отказов в обновлении ключей данным хостом/партнером	Количество временных отказов в обновлении ключей данным хостом/партнером
INIT обменов успешных (с ошибками или неуспешных) инициировано/отвечено	Количество обменов INIT_IKE_SA успешных (с ошибками или неуспешных) инициировано/отвечено в формате x(x)/x(x)
RESUME обменов успешных (с ошибками или неуспешных) инициировано/отвечено	Количество обменов RESUME_IKE_SA успешных (с ошибками или неуспешных) инициировано/отвечено в формате x(x)/x(x)

Параметр	Описание
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 содержит древовидную структуру (см. Рисунок 44) активных защищённых соединений, установленных с данным компьютером, а также создающихся защищённых соединений. В правой части окна содержится детальная информацию о выбранном в левой части окна активном соединении.

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

Таблица в левой части окна содержит следующую информацию о защищенных соединениях (IPSec SAs) (см. Таблица 10).

Таблица 10 – Информация об активных защищенных соединениях

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

Параметр	Характеристика
Время создания	Время создания соединения

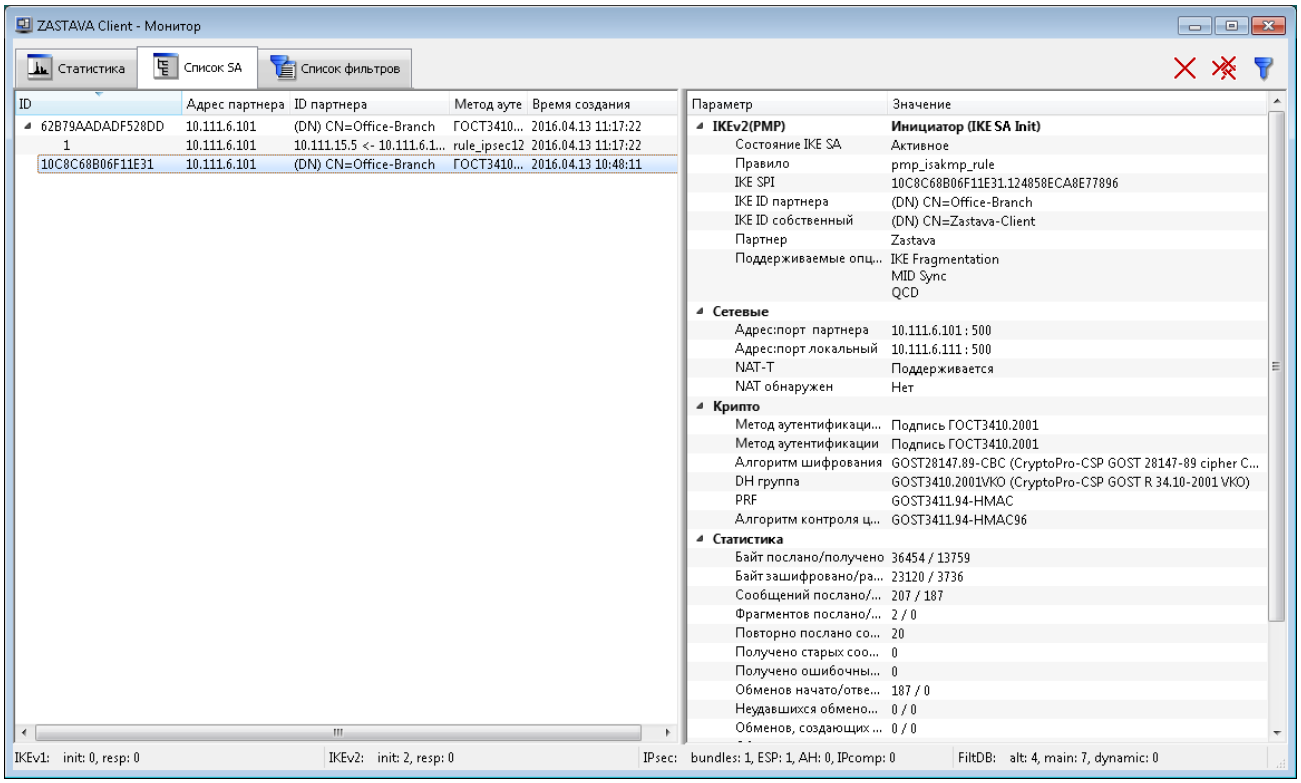

Рисунок 44 – Окно «Монитор», вкладка «Список SA»

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 45).

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

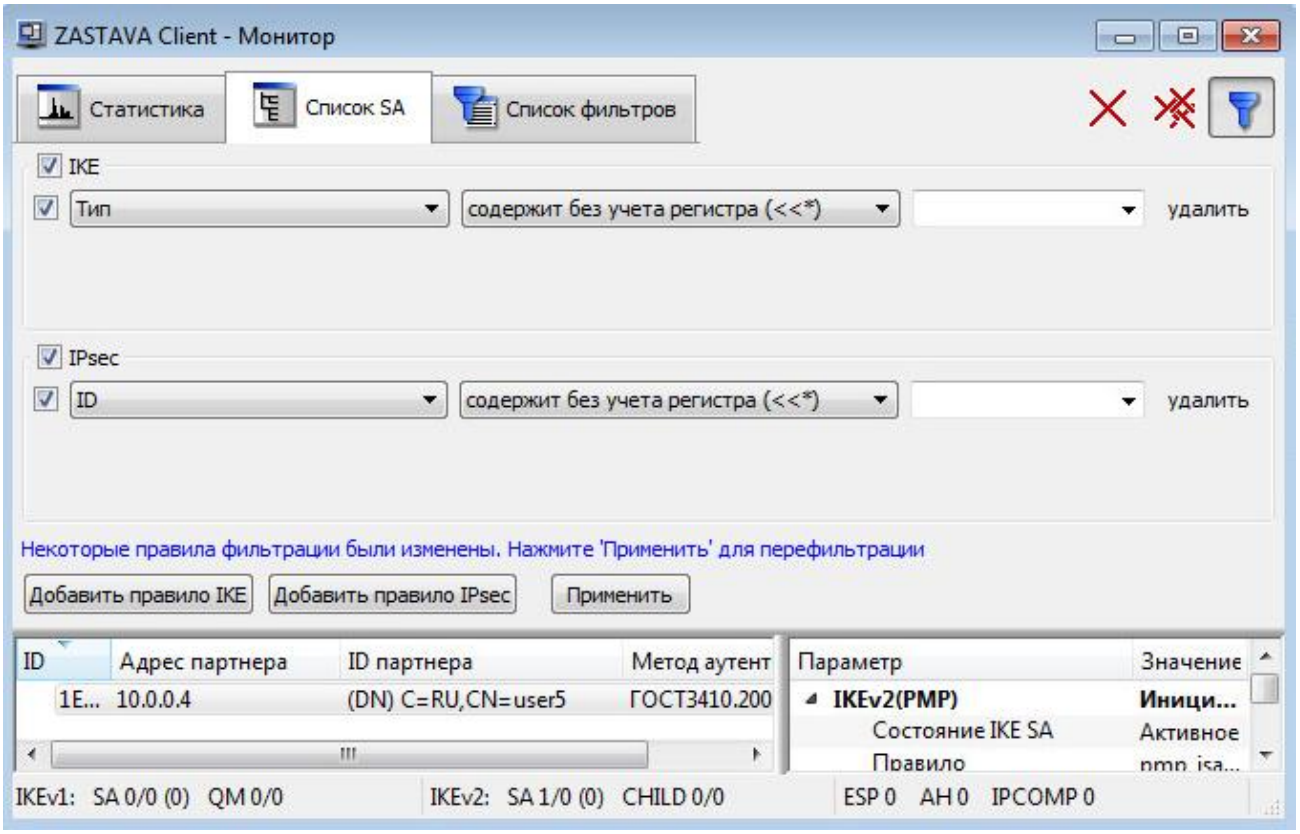

Рисунок 45 – Окно «Монитор», активный «Фильтр»

Параметры фильтрации протокола IKE приведены в таблице (см. Таблица 11).

Таблица 11 – Параметры фильтрации протокола IKE

Параметр	Характеристика
Тип	Тип создания SA
Режим	Режим создания SA
Роль	Роль локальной машины при создании SA
Состояние IKE SA	Состояние IKE SA
EAP ID собственный	Свой EAP ID
IKE ID собственный	IKE ID данного компьютера
EAP ID партнера	EAP ID, присланный партнером
IKE ID партнера	IKE ID партнера
ID партнера	ID партнера (IKE ID или EAP ID в зависимости от метода аутентификации)
Правило	Имя правила
Алгоритм шифрования	Алгоритм шифрования
Хэш-функция	Алгоритм хэширования
DH группа	DH-группа
Алгоритм контроля целостности	Алгоритм контроля целостности
PRF	Псевдослучайная функция
Локальный адрес	IP-адрес данного компьютера, использованный при создании защищенного соединения
Локальный порт	UDP-порт на данном компьютере, использованный при создании защищенного соединения

Параметр	Характеристика
Адрес партнера	IP компьютера, с которым создано защищенное соединение
Порт партнера	UDP-порт компьютера, с которым создано защищенное соединение
Перенаправлен с адреса	IP компьютера, с которого произошло перенаправление на данный
Метод аутентификации партнера	Метод аутентификации партнера
Метод аутентификации	Метод идентификации данного компьютера
IKE SPI	IKEv2 SPI
Уровень лога	Уровень подробности регистрации событий
Поддерживаемые опции	Список поддерживаемых опций

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

Таблица 12 – Параметры фильтрации протокола IPsec SA

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

Тип	Характеристика
(ESP) Преобразование	(ESP) Алгоритм шифрования
(ESP) Аутентификация	(ESP) Алгоритм имитозащиты
(ESP) Исходный адрес партнера	(ESP) Исходный адрес партнера
(ESP) Исходный адрес локальный	(ESP) Исходный адрес данного компьютера
(ESP) Декапсулировано пакетов	(ESP) Декапсулировано пакетов
(ESP) Декапсулировано байт	(ESP) Декапсулировано байт
(ESP) Ошибки дешифрации (пакетов)	(ESP) Ошибки дешифрации (пакетов)
(ESP) Ошибки аутентификации (пакетов)	(ESP) Ошибки аутентификации (пакетов)
(ESP) Ошибки атак воспроизведения (пакетов)	(ESP) Ошибки атак воспроизведения (пакетов)
(ESP) Ошибки ограничения трафика (пакетов)	(ESP) Ошибки ограничения трафика (пакетов)
(ESP) Прочие ошибки декапсуляции (пакетов)	(ESP) Прочие ошибки декапсуляции (пакетов)
(ESP) Инкапсулировано пакетов	(ESP) Инкапсулировано пакетов
(ESP) Инкапсулировано байт	(ESP) Инкапсулировано байт
(ESP) Ошибки шифрации (пакетов)	(ESP) ошибки шифрации (пакетов)
(IPcomp) Правило	(IPcomp) Правило
(IPcomp) CPI in	Значение CPI для входящей SA (IPcomp)
(IPcomp) CPI out	Значение CPI для исходящей SA (IPcomp)
(IPcomp) Rekey CPI in	Значение CPI для входящей SA, ключи которой были обновлены (IPcomp)
(IPcomp) Уровень лога	(IPcomp) Уровень подробности регистрации событий
(IPcomp) PMTU	(IPcomp) значение MTU, которое установлено на промежуточном шлюзе
(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 13).

Таблица 13 – 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	

Команда	Характеристика
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 IP-порт	
равен	значение поля (порт) равно эталону
не равен	значение поля не равно эталону
в диапазоне	значение поля входит в диапазон, заданный эталоном, в качестве эталона можно указать просто порт (8080) или диапазон (0..65535)
не в диапазоне	значение поля не входит в диапазон, заданный эталоном
Операции для фильтрации по полю уровень лога	
равен	значение поля равно эталону (возможные значения: disabled, events, details, verbose)
не равен	значение поля не равно эталону
больше чем	значение поля больше эталона (disabled < events < details < verbose)
меньше чем	значение поля меньше эталона
больше или равен	значение поля больше или равно эталону
меньше или равен	значение поля меньше или равно эталону
Операции для фильтрации по IPsec-соединению по полю протокол	
равен	значение поля равно эталону (возможные значения: esp, pcp)
не равен	значение поля не равно эталону
Операции для фильтрации по IPsec-соединению по полю mode	
равен	значение поля равно эталону (возможные значения: tunnel, transport)
не равен	значение поля не равно эталону
Операции для фильтрации по IP-протоколу	
равен	значение поля (протокол) равно эталону
не равен	значение поля не равно эталону

Команда	Характеристика
в диапазоне	значение поля входит в диапазон, заданный эталоном, в качестве эталона можно указать просто протокол (6) или диапазон (0..255)
не в диапазоне	значение поля не входит в диапазон, заданный эталоном
Операции для фильтрации по диапазону IP-адресов	
содержит	значение поля (IP-диапазон) содержит IP-адрес, заданный эталоном
не содержит	значение поля (IP-диапазон) не содержит IP-адрес, заданный эталоном
в диапазоне	значение поля (IP-диапазон) входит в другой IP-диапазон, заданный эталоном
не в диапазоне	значение поля (IP-диапазон) не входит в другой IP-диапазон, заданный эталоном
равен	значение поля (IP-диапазон) совпадает с IP-диапазоном, заданный эталоном
не равен	значение поля (IP-диапазон) не совпадает с IP-диапазоном, заданный эталоном

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

На вкладке «Список SA» существует контекстное меню с командами (см. Таблица 14).

Таблица 14 – 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 46).

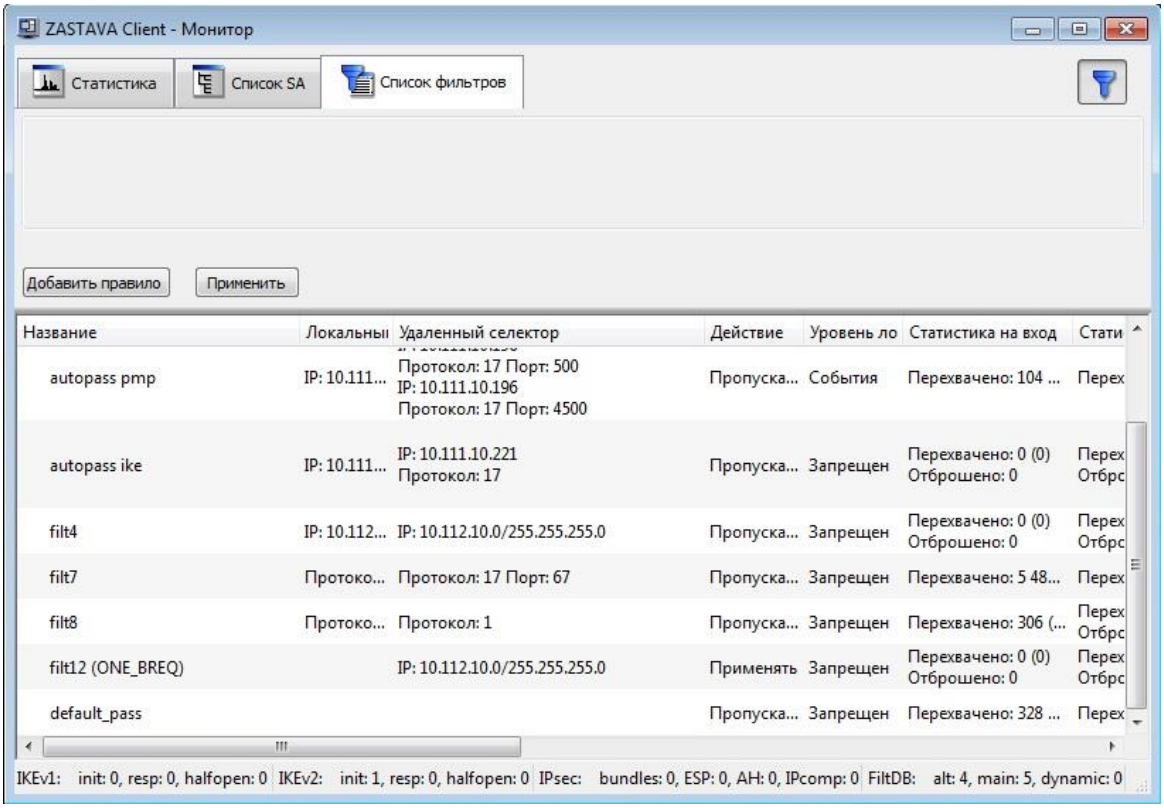

Рисунок 46 – Окно «Монитор», вкладка «Список фильтров»

Основную часть вкладки занимает список фильтров, который включает в себя статистику по параметрам фильтрации (см. Таблица 15).

Таблица 15 – Параметры фильтров

Параметр	Характеристика
Название	Параметр фильтрации по полю «Название»
Локальный селектор	Адрес, протокол и порт локального селектора
Удаленный селектор	Адрес, протокол и порт удаленного селектора
Действие	Действие для фильтрации
Уровень лога	Уровень подробности регистрации событий
Статистика на вход	Статистика входящих пакетов
Статистика на выход	Статистика исходящих пакетов
Входящих пакетов в секунду	Статистика входящих пакетов в секунду
Входящих байт в секунду	Статистика входящих байт в секунду
Исходящих пакетов в секунду	Статистика исходящих пакетов в секунду
Исходящих байтов в секунду	Статистика исходящих байт в секунду
Входящих промахов в кэше	Статистика промахов после проверки входящих пакетов на соответствие с фильтрами в кэше
Исходящих промахов в кэше	Статистика промахов после проверки исходящих пакетов на соответствие с фильтрами в кэше
Входящих промахов в кэше в секунду	Статистика промахов после проверки входящих пакетов в секунду на соответствие с фильтрами в кэше

Параметр	Характеристика
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 16).

Таблица 16 – Команды контекстного меню вкладки «Список фильтров»

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

4.6.3.2 Фильтрация

Для задания правил фильтрации следует:

1) Открыть панель фильтров кнопкой  .
2) Нажать кнопку «Добавить правило», появится строка задания правила фильтрации (см. Рисунок 47).
3) Задать правило фильтрации:
   а) Выбрать из первого списка параметр фильтрации (см. Таблица 17).
   б) Выбрать из второго списка условие фильтрации.
   в) В третьем поле задать или выбрать из списка значение, по которому будет производиться сравнение.


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


Чтобы отключить применение фильтра следует снять флажок слева от фильтра.

4) При необходимости, добавить еще одно или несколько правил фильтрации, нажав кнопку «Добавить правило».
5) После задания всех требуемых правил фильтрации надо нажать кнопку «Применить», в результате в таблице будут отображаться только фильтры, соответствующие заданным правилам.

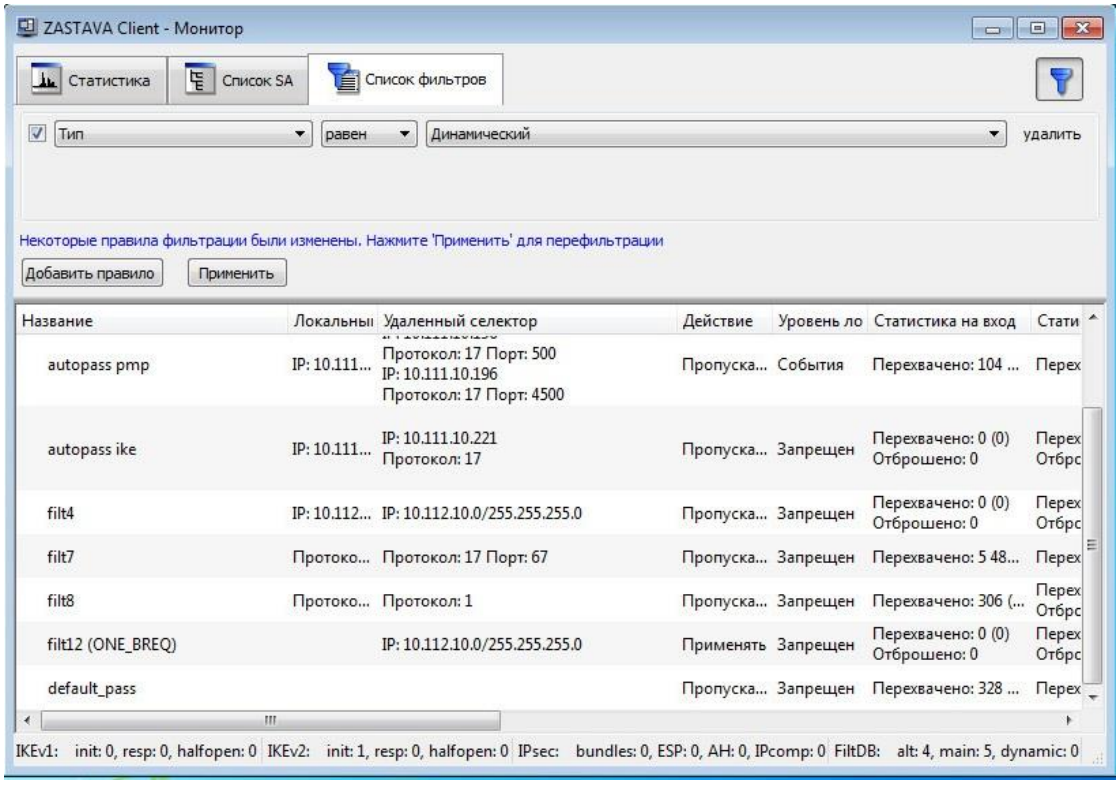

Рисунок 47 – Окно «Монитор», вкладка «Список фильтров». Открыта панель фильтрации

Таблица 17 – 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»
Исходящих байт отброшено	Фильтрация поля «Исходящих байт отброшено»
Входящих промахов в кэше	Фильтрация поля «Входящих промахов в кэше»

Параметр	Характеристика
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, СОС регистрируются в «ЗАСТАВА-Клиент» через окно «Сертификаты и Ключи». Вызвать это окно можно, нажав кнопку «Сертификаты» на Панели управления.

«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 «ЗАСТАВА-Клиент» с целью проверки подлинности всех сертификатов, присылаемых партнерами по связи в процессе установления защищенных соединений (см. «сертификаты партнёров»).
- **Персональный сертификат** – сертификат, используемый данным пользователем «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 протоколов IKEv2.
- **Прочие сертификаты** – сертификаты, используемые данным «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 «ЗАСТАВА-Клиент». Отличительной особенностью является то, что это CA-сертификаты промежуточных УЦ, выданные промежуточным сертифицирующим органом (CA – certification authority).

«ЗАСТАВА-Клиент» поддерживает СОС. Для получения более полной информации надо обратиться к п. 4.7.4.

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 48).

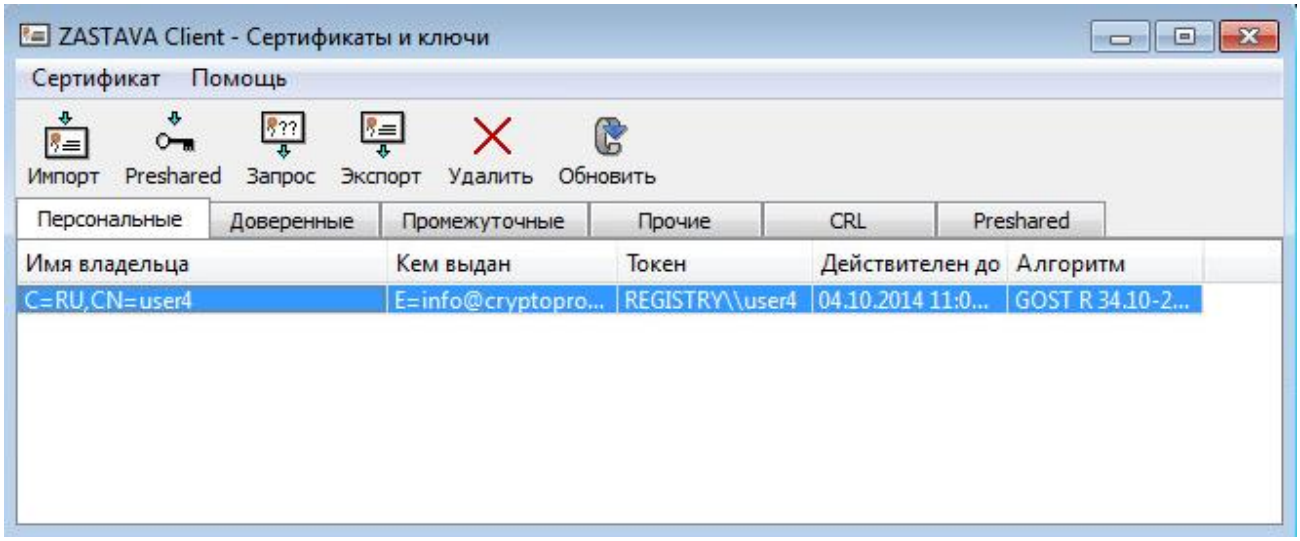

Рисунок 48 – Окно «Сертификаты и Ключи»

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 18).

Таблица 18 – 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 (не используется в АПК информация по данной вкладке приведена для справки)

4.7.1.2 Строка меню

Строка меню содержит следующие меню: «Сертификаты», «Помощь». Команды меню представлены в таблице (см. Таблица 19).

Таблица 19 – Команды меню

Команда	Действие

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 (функция не используется в АПК).
Генерация запроса сертификата	Запускает мастер Генерации запроса сертификата (функция не используется в АПК).
Экспорт сертификата	Запускает мастер Экспорта сертификатов, который помогает экспортировать любой сертификат.
Обновить	Обновляет список сертификатов, зарегистрированных в базе данных (БД). Если окно «Сертификаты и ключи» открыто, когда активизирована ЛПБ, то сертификаты, полученные в течение IKE-обмена, не обновляются автоматически. СОС, полученные автоматически от сервера LDAP, также не показываются. Нажатие кнопки «Обновить» гарантирует то, что Вы видите наиболее свежую информацию о БД.
Помощь	
Работа с сертификатами и ключами	Открывает раздел справки «Работа с сертификатами и ключами».
Помощь	Вызов общей справочной системы «ЗАСТАВА-Клиент».

4.7.1.3 Панель инструментов окна «Сертификаты и ключи»

Описание кнопок панели инструментов приведено в таблице (см. Таблица 20). Функции этих кнопок соответствуют функциям пунктов меню (см. п. 4.7.1.2).

Таблица 20 – Кнопки панели инструментов окна «Сертификаты и ключи»

Кнопка	Действие
 Импорт	Запускает мастер импорта сертификатов
 Preshared	Запускает мастер импорта предварительно распределенных ключей (функция не используется в АПК)
 Запрос	Запускает мастер Генерации запроса сертификата (функция не используется в АПК)
 Экспорт	Запускает мастер Экспорта сертификатов
 Удалить	Удаляет выбранный сертификат
 Обновить	Обновляет список сертификатов, зарегистрированных в БД

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 кнопкой мыши или воспользоваться клавишей <Enter>.

Характеристики сертификата приведены в таблице (см. Таблица 21).

Таблица 21 – Характеристики сертификата

Параметр	Характеристика
Version	Версия сертификата
Серийный номер	Серийный номер сертификата
Issuer	Кем выдан сертификат
Subject	Содержит отличительное имя субъекта, то есть владельца закрытого ключа, соответствующего открытому ключу данного сертификата. Субъектом сертификата может выступать УЦ, Регистрационный Центр (РЦ) или конечный субъект
Sign Algorithm	Алгоритм цифровой подписи сертификата
Key Algorithm	Тип открытого ключа (алгоритм цифровой подписи и длина)
Public Key	Значение открытого ключа
Действителен с	Начальная дата действия сертификата
Действителен до	Конечная дата действия сертификата
Authority Key Identifier	Идентификатор ключа издателя, помогает определить правильный ключ для верификации подписи на сертификате
Subject Key Identifier	Идентификатор ключа субъекта, используется для того, чтобы различать ключи подписи в сертификатах одного и того же владельца
Key Usage	Назначение ключа
Ext. Key Usage	Расширенное назначение ключа
CRL Distribution Points	Точки распространения COC, 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 COC; <Issuer Value> – имя организации, выпустившей COC
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 Состав списка отозванных сертификатов

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

Таблица 22 – Информация о COC

Параметр	Характеристика

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

4.7.3 Регистрация и удаление сертификата

4.7.3.1 Регистрация сертификата

В «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 «ЗАСТАВА-Клиент» необходимо сделать следующее:

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

2) В появившемся окне выбрать необходимый для установки сертификат и нажать кнопку «Открыть» (см. Рисунок 49).

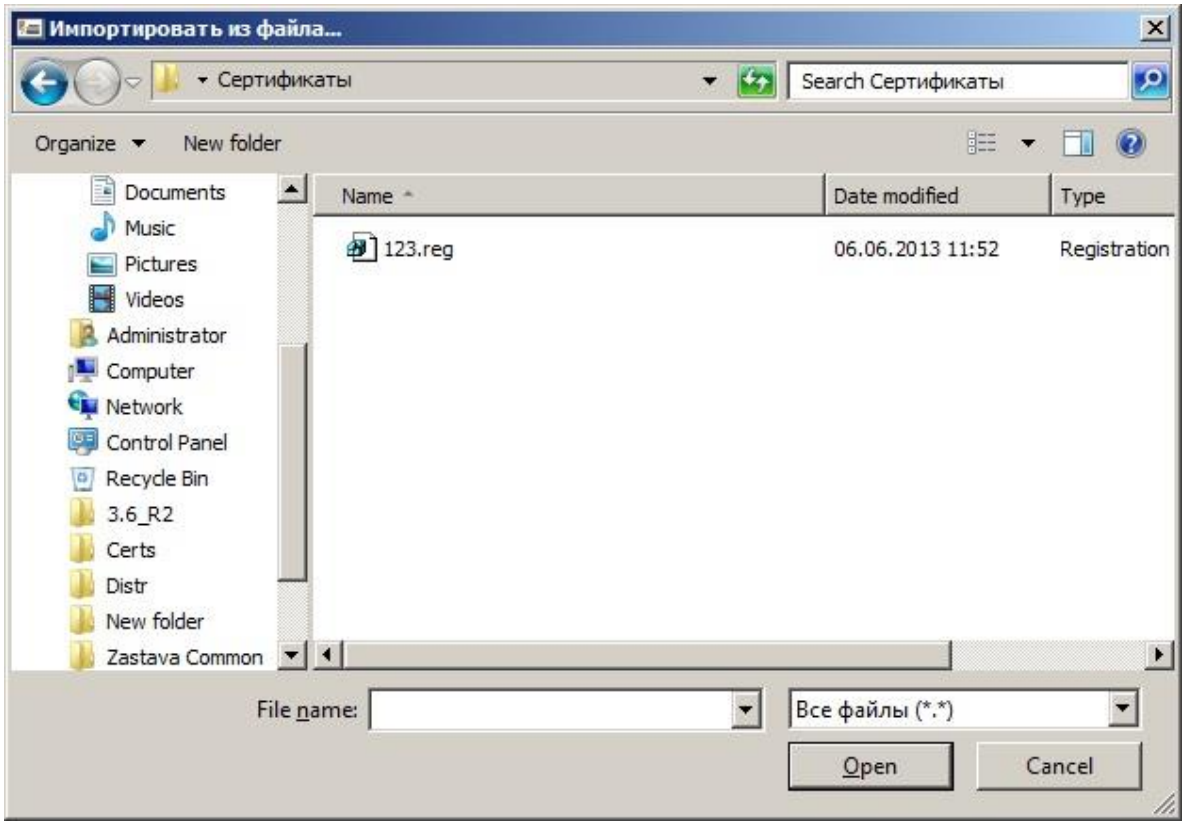

Рисунок 49 – Выбор импортированного объекта

3) Режим импорта будет выбран автоматически, в соответствии с типом сертификата. Нажать кнопку «Далее» (см. Рисунок 50).

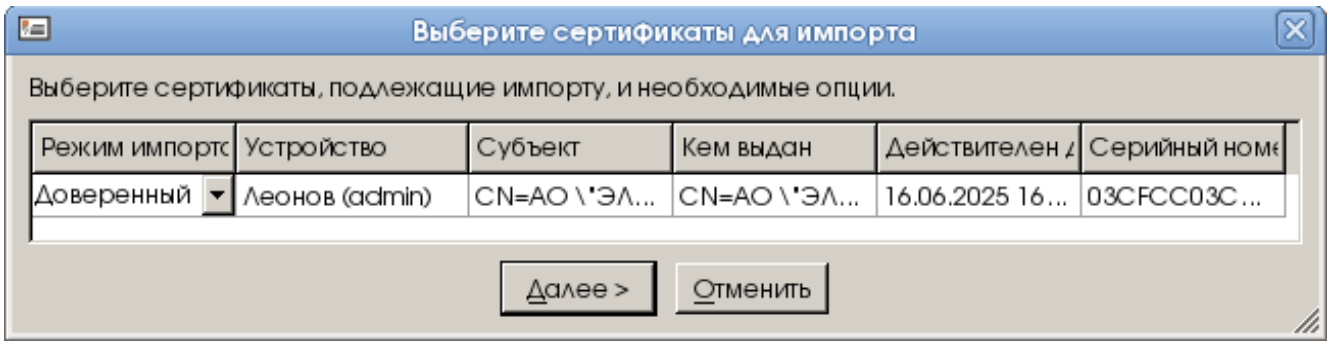

Рисунок 50 – Выбор режима импорта сертификата

4) При успешном импортировании появится индикатор (см. Рисунок 51). Теперь Мастер сертификатов показывает импортированный сертификат, нажать кнопку «Готово».

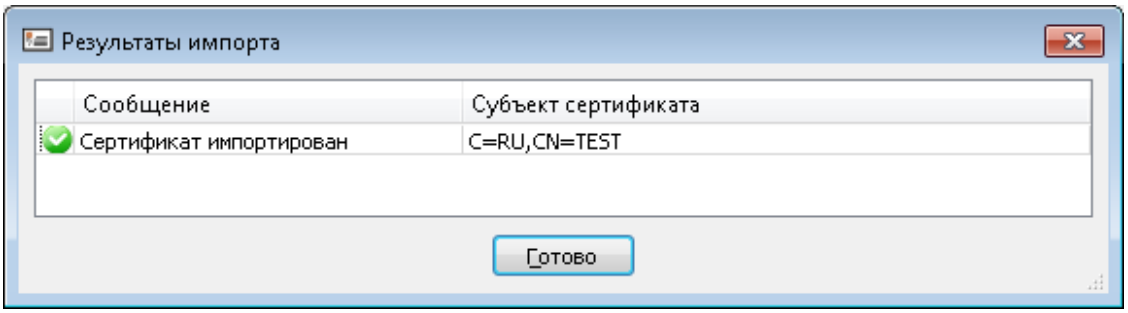

Рисунок 51 – Окно результата импортирования сертификата

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

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

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

   – При регистрации сертификата УЦ, нужно в поле «Режим импорта» (см. Рисунок 52) назначить этому сертификату соответствующий статус – «Доверенный». После чего нажать кнопку «Далее».

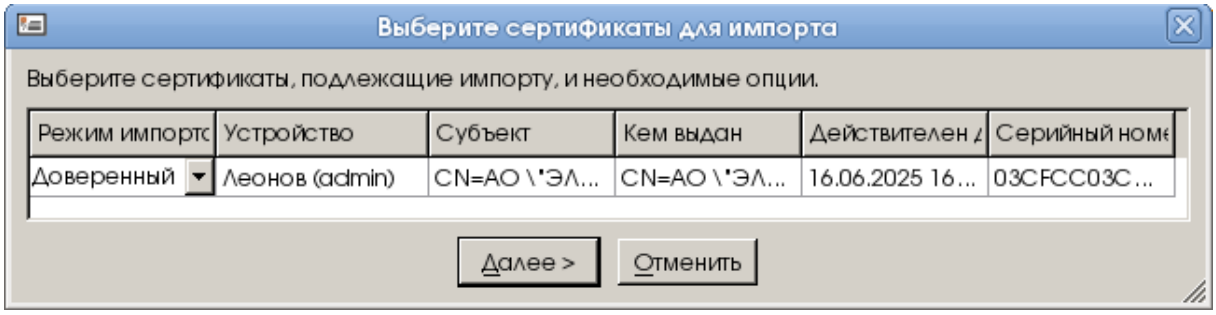

Рисунок 52 – Выбор режима импорта сертификата для регистрации Доверенного сертификата

– Необходимо ввести PIN-код токена (см. Рисунок 53), в котором будет содержаться сертификат. После ввода PIN-кода нужно нажать кнопку «Готово».

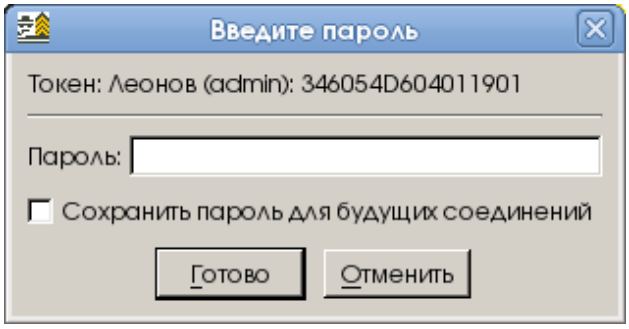

Рисунок 53 – Ввод пароля токена

	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 «ЗАСТАВА-Клиент» свяжитесь с администратором УЦ, чтобы сравнить сигнатуру (fingerprint) оригинального сертификата УЦ с сигнатурой полученного сертификата, которая отображается в полях «Fingerprint» в таблице сертификатов «ЗАСТАВА-Клиент». Если сигнатуры не совпадают, немедленно удалите сертификат из «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 отображает объекты сертификата, содержащиеся на токене. Все эти сертификаты имеют статус «Доверяемый». Вы можете сохранять сертификат УЦ как «Доверяемый». Сертификаты партнёров по связи, импортированные из токенов, будут всегда проверяться по цепочке доверия.

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

4.7.3.2 Удаление сертификата

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

Если срок действия сертификата, находящегося в «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).

4.7.3.2.1 Формат строки уникального имени (DN)

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

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

где: `attrN=attrN_value`;

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

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

Например, строка DN может выглядеть следующим образом:

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

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

Таблица 23 – Типы атрибутов

Типы атрибутов	Наименование	Расшифровка
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 «Субьект»)		

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

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

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

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

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

Возможно также добавление произвольных атрибутов в строку DN, используя «точечно-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 ВЧС-Агенты третьих производителей распознают сертификаты удаленных партнеров по связи, только если атрибуты DN расположены в определенном порядке. После получения сертификата от УЦ надо убедиться в том, что «ЗАСТАВА-Клиент» способен корректно взаимодействовать со всеми видами Агентов, необходимыми для работы.

В «ЗАСТАВА-Клиент» атрибуты DN-сертификатов расположены в том же порядке, в котором они указаны в сертификате. Во многих аналогичных изделиях третьих производителей используется реверсивное отображение атрибутов DN.

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

4.7.4 Списки отозванных сертификатов

COC – это список сертификатов, которые в настоящее время не имеют силы и не должны использоваться для формирования защищенных соединений (SA) в течение сеанса безопасного соединения.

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

В большинстве случаев «ЗАСТАВА-Клиент» автоматически проверяет сертификаты по COC. Всякий раз, когда сертификат получен от партнёра по связи по протоколу IKE, «ЗАСТАВА-Клиент» сначала попытается найти необходимый COC. При отсутствии COC в «ЗАСТАВА-Клиент» (или если срок действия COC закончился) «ЗАСТАВА-Клиент» соединится с LDAP «ЗАСТАВА-Клиент», чтобы получить обновленный COC. Если сертификат партнёра по связи или соответствующий сертификат УЦ указан в COC, или требуемый COC не доступен – связь с партнером не будет установлена. Если в текущей ЛПБ обработка COC выключена, сертификаты не будут проверяться по COC. Для получения информации о проверке сертификатов по COC см. п. 4.7.4.2.

4.7.4.1 Обработка COC

При проверке валидности сертификата «ЗАСТАВА-Клиент» путем просмотра COC (CRL) удостоверяется то, что сертификат не аннулирован. COC может быть импортирован в

«ЗАСТАВА-Клиент» вручную или автоматически (из внешнего «ЗАСТАВА-Клиент», используя протокол LDAP).

Включение обработки СОС осуществляется выбором соответствующего режима в настройках «ЗАСТАВА-Клиент» (см. п. 4.11.2). Описание режимов обработки СОС приведено в таблице (см. Таблица 24):

Таблица 24 – Режимы работы обработки CRL

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

4.7.4.2 Проверка сертификата

Проверить сертификат, зарегистрированный в «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 (левой) кнопкой мыши. В верхней части окна «Параметры сертификата» будет показана Иерархия сертификата.

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

4.8 Окно «Управление политиками»

Окно «Управление политиками» предназначено для редактирования списка ЛПБ и установки опций ЛПБ (см. Рисунок 54). Для получения информации об 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 «ЗАСТАВА-Клиент» связывается с другими объектами в защищённой среде.

ЛПБ может быть установлена, активирована и просмотрена.

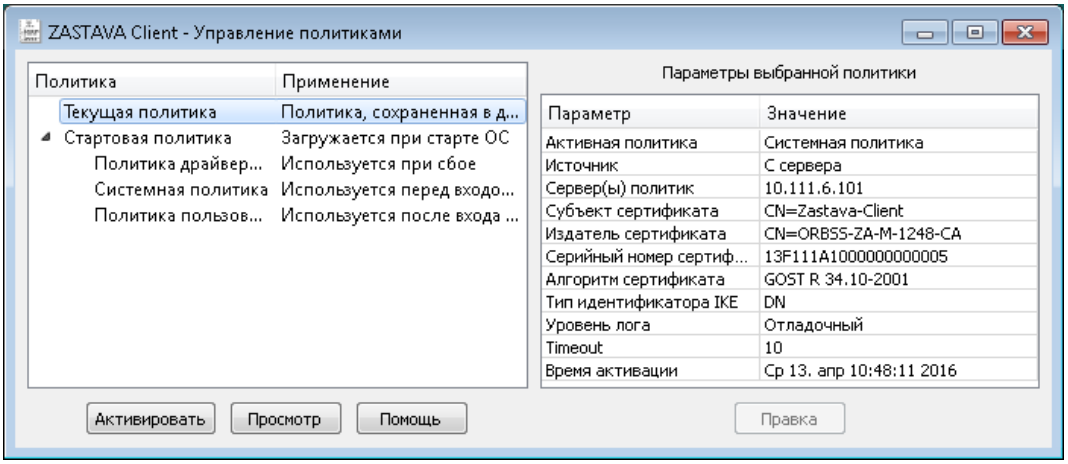

Рисунок 54 – Окно «Управление политиками»

4.8.1 Структура окна «Управление политиками»

Окно «Управление политиками» состоит двух разделов:

– раздел с деревом политик;

– раздел с параметрами выбранной политики.

Поле «Политика» содержит дерево существующих политик. При выделении политики в дереве политик в поле «Параметры выбранной политики» отображаются параметры политики. Поле «Политика» содержит также кнопки «Активировать», «Просмотр» и «Помощь».

4.8.2 Типы политик

В поле «Политика» существуют следующие типы политик:

– Текущая – политика, сохраняемая в драйвере «ЗАСТАВА-Клиент».

– Стартовая – политика, загружаемая при старте ОС:

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

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

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

4.8.3 Параметры политик «ЗАСТАВА-Клиент»

4.8.3.1 Системная ЛПБ

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

Для изменения параметров системной политики необходимо на системной политике в поле «Политика» нажать дважды левой кнопкой мыши и выбрать необходимые параметры в окне «Опции политик» (см. Рисунок 55).

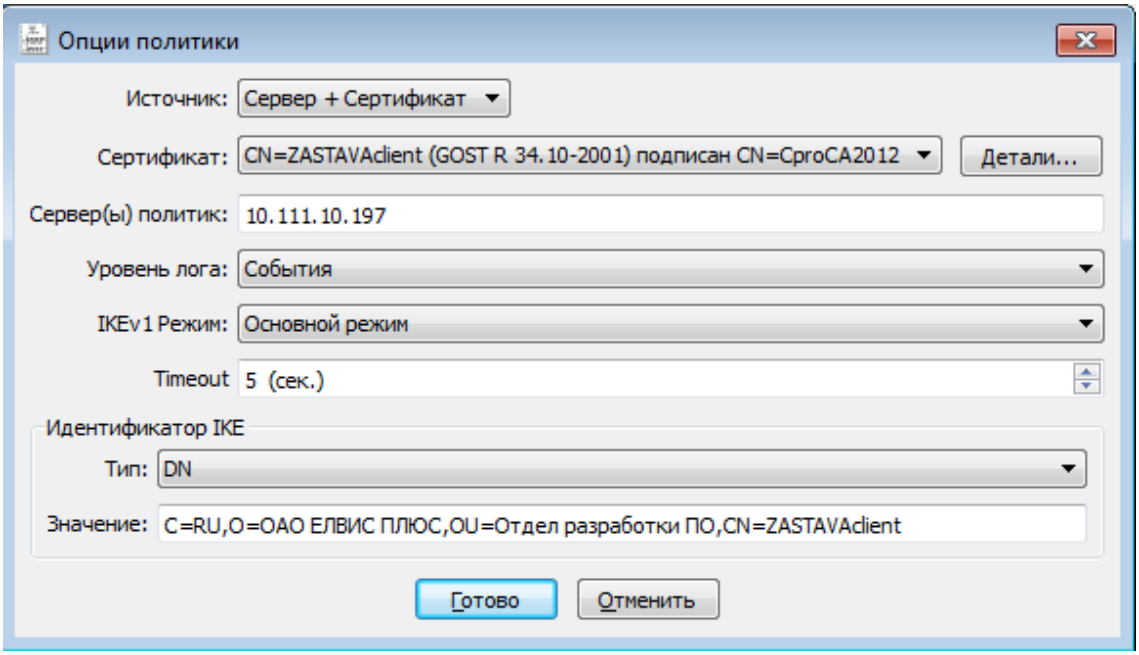

Рисунок 55 – Настройка параметров системной политики

Для настройки системной политики необходимо:

1) Выбрать тип метода активации из поля «Источник» и определить параметры данного метода:

– При выборе метода прогрузки из файла необходимо в поле «Путь» указать путь к файлу с политикой или выбрать необходимый файл, нажав кнопку «…».

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

– При выборе метода прогрузки с сервера необходимо в поле «Источник» выбрать из раскрывающегося списка необходимый параметр для установки SA. Раскрывающийся список содержит следующие значения: «Сервер+Сертификат», «Сервер+Ключ». Для настройки прогрузки политики с сервера необходимо:

а) Выбрать из выпадающего списка поля «Сертификат» или «Ключ» зарегистрированный сертификат или Preshared Key.

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

б) Чтобы настроить получение ЛПБ с сервера политики необходимо ввести в поле «Сервер(ы) политик» IP-адрес(а) сервера и порт, с которого будет получена политика, если не указать порт, то берется значение по умолчанию (500). Если серверов несколько, IP-адреса указываются через запятую. Номер порта указывается через двоеточие.

в) Для журналирования сообщений при передаче ЛПБ с сервера политики необходимо выбрать уровень подробности регистрации событий в поле «Уровень лога», подробнее об уровне регистрации событий см. п. 4.11.1.1.

г) Выбрать режим установления соединения IKE.

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

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

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

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

4.8.3.2 Политика пользователя

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

Для изменения параметров пользовательской политики необходимо на политике пользователя в поле «Политика» надо нажать дважды левой кнопкой мыши и выбрать необходимые параметры в окне «Опции политик» (см. Рисунок 56).

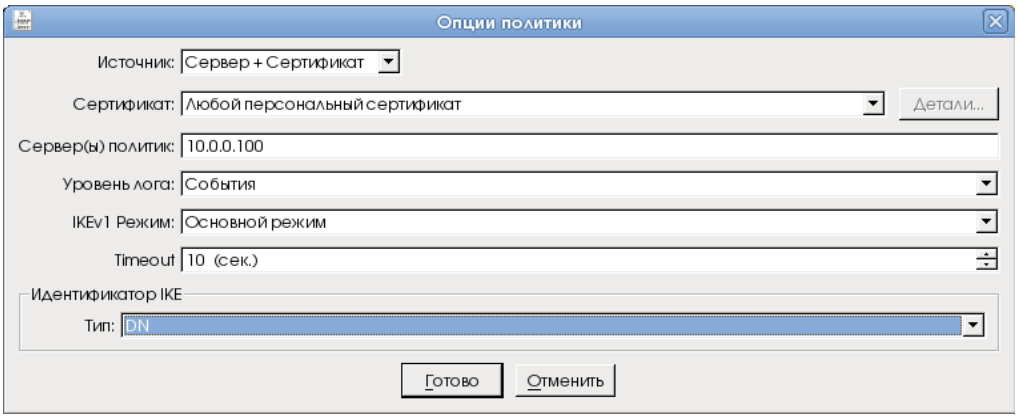

Рисунок 56 – Настройка параметров политики пользователя

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 57). Сохранение опций политики требует введения пароля администратора.

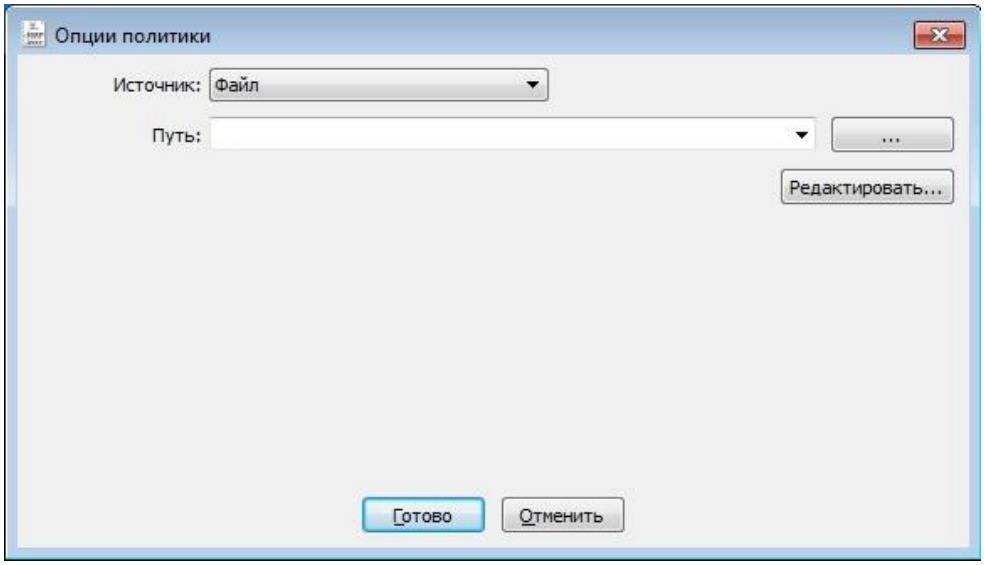

Рисунок 57 – Настройки политики пользователя при прогрузке политики из файла

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

– 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 58). Для настройки прогрузки пользовательской политики с сервера необходимо:

а) Выбрать из выпадающего списка поля «Сертификат» зарегистрированный 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.

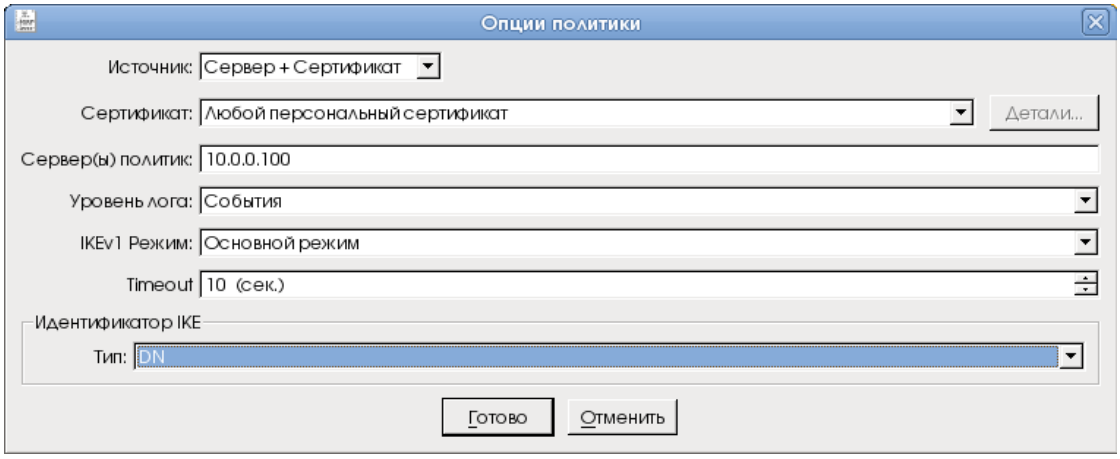

Рисунок 58 – Настройки политики пользователя при выборе метода прогрузки с сервера

б) Ввести адрес сервера в строке «Сервер(ы) политик» и указать порт, с которого будет получена политика, если не указать порт, то берется значение по умолчанию (500). В качестве адреса сервера политик можно использовать DNS. Если серверов несколько, IP-адреса указываются через запятую. Номер порта указывается через двоеточие.

в) Для журналирования сообщений при передаче ЛПБ с сервера политики необходимо выбрать уровень подробности регистрации событий в поле «Уровень лога», подробнее об уровне регистрации событий см. п. 4.11.1.1.

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

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

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

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

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

4.8.3.3 Политика драйвера по умолчанию

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

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

Для изменения параметров «Политика драйвера по умолчанию» необходимо в поле «Политика» окна «Управление политиками» нажать дважды левой кнопкой мыши и выбрать необходимые параметры в окне «Опции политик» (см. Рисунок 59). «Политика драйвера по умолчанию» может быть установлена, либо в «Сбрасывать все» (DROP ALL), либо в «Сбрасывать все, кроме DHCP» (DROP ALL EXCEPT DHCP), либо в «Пропускать все» (PASS ALL). После выбора необходимых настроек нажать кнопку «Сохранить» для сохранения настроек в «ЗАСТАВА-Клиент».

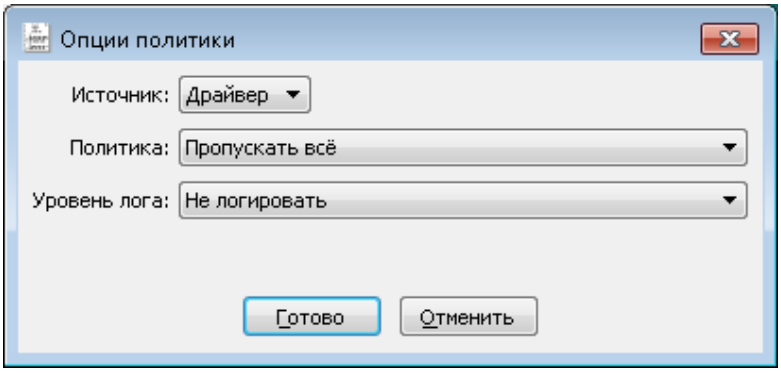

Рисунок 59 – Настройка параметров «Политика драйвера по умолчанию»

Из соображений безопасности рекомендуется устанавливать «Политика драйвера по умолчанию» в значение «Сбрасывать все». Следует учесть, что в этом случае сеть не будет доступна, если компьютеру не присвоен статический IP-адрес. Если компьютер получает IP-адрес по DHCP, то следует выбрать опцию «Сбрасывать все, кроме DHCP». В этом случае сеть будет недоступна до момента активации рабочей ЛПБ (исключение составляет только трафик DHCP, необходимый для назначения компьютеру IP-адреса).

4.8.4 Изменение параметров ЛПБ

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

Для изменения доступны параметры следующих политик:

- политика драйвера по умолчанию (DDP) – политика, загружаемая при сбое;
- системная политика – политика, используемая перед входом пользователя в ОС;
- политика пользователя – политика, используемая после входа пользователя в ОС.

Параметры «Системной политики» и «Политики Драйвера по умолчанию» можно также изменить, выделив в дереве политик требуемую политику и нажав один раз правую кнопку мыши, из выпадающего меню выбрать 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 ЦУП и сохраняется как текстовый файл, который затем регистрируется в «ЗАСТАВА-Клиент».

ЛПБ может быть зарегистрирована в окне «Управление политиками». ЛПБ может находиться в файловой системе. При активации указанной политики «ЗАСТАВА-Клиент» обратится к заданному источнику и скопирует политику в драйвер «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» окна «Опции политик»:

- Загрузить из файла (данная функция не используется в АПК).

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

- Загрузить с сервера ЦУП.

Для загрузки ЛПБ с сервера необходимо выполнить следующие действия:

а) Выбрать один из параметров:
   - «Сервер+Сертификат» – для загрузки ЛПБ с сервера и установки IPsec SA с помощью сертификата;
   - «Сервер+Ключ» – для загрузки ЛПБ с сервера и установки IPsec SA с помощью предварительно распределенного ключа, только для системной ЛПБ (данная функция не используется в АПК).

б) Выбрать из выпадающего списка зарегистрированный сертификат или предварительно распределенный ключ, в соответствии с выбранным методом прогрузки с сервера.

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

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

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

е) Выбрать тип идентификатора в секции «Идентификатор IKE» для прогрузки политики, который должен быть согласован с ЦУП.

3) Нажать кнопку «Сохранить».

4) Ответить на вопрос об активации политики. Для активации зарегистрированной политики после сохранения параметров надо нажать кнопку «Да».

4.8.6 Просмотр ЛПБ

В поле с деревом политик окна «Управление политиками» можно произвести просмотр текущей ЛПБ, для этого необходимо выбрать из дерева политик строку «Текущая политика» и нажать кнопку «Просмотр» окна «Управление политиками». В появившемся окне «Редактор» можно просмотреть код политики, произвести изменения или поиск необходимых параметров, выполнить переход на определенную строку политики, воспользовавшись для этого меню «Вид» окна «Редактор» и, при необходимости, сохранить данную политику, 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 «ЗАСТАВА-Клиент») необходимо выделить нужную политику в дереве политик окна «Управление политиками» «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»

«ЗАСТАВА-Клиент» позволяет использовать токены как среду транспортировки важной информации (сертификатов, закрытых ключей). Окно «Токены» (см. Рисунок 60) содержит список всех зарегистрированных модулей токенов. В АПК в качестве токена используется смарт-карта.

АПК поставляется уже с зарегистрированными токенами. Для пользователя АПК доступна только смена PIN-кода пользователя токена.

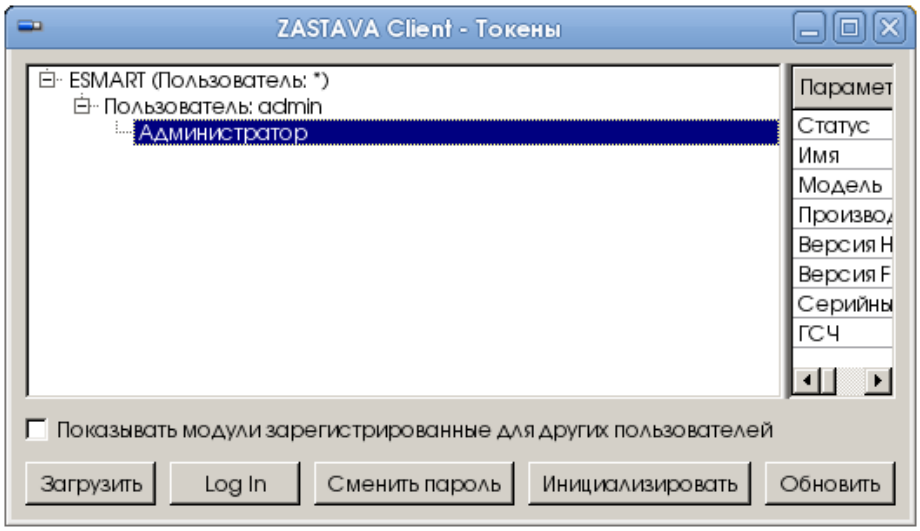

Рисунок 60 – Окно «Токены»

4.9.1 Смена PIN-кода токена

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

Для смены PIN-кода необходимо:

1) Открыть Панель управления, нажав правой кнопкой мыши на значок в системном трее и выбрав пункт «Панель управления» (см. Рисунок 61).

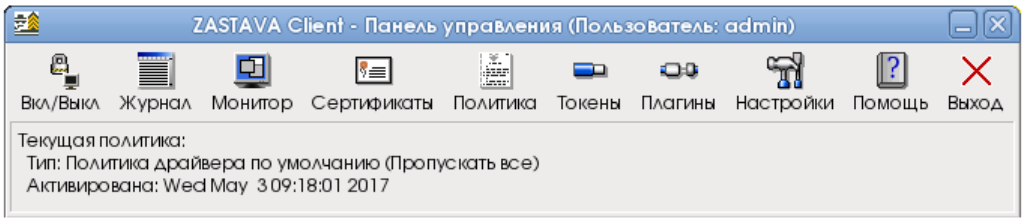

Рисунок 61 – Панель управления «ЗАСТАВА-Клиент»

2) Открыть окно «Токены» нажатием кнопки «Токены» на Панели управления.

3) В окне «Токены» (см. Рисунок 62) выбрать из списка в левой части окна название своего ключевого носителя, затем нажать кнопку «Сменить пароль».

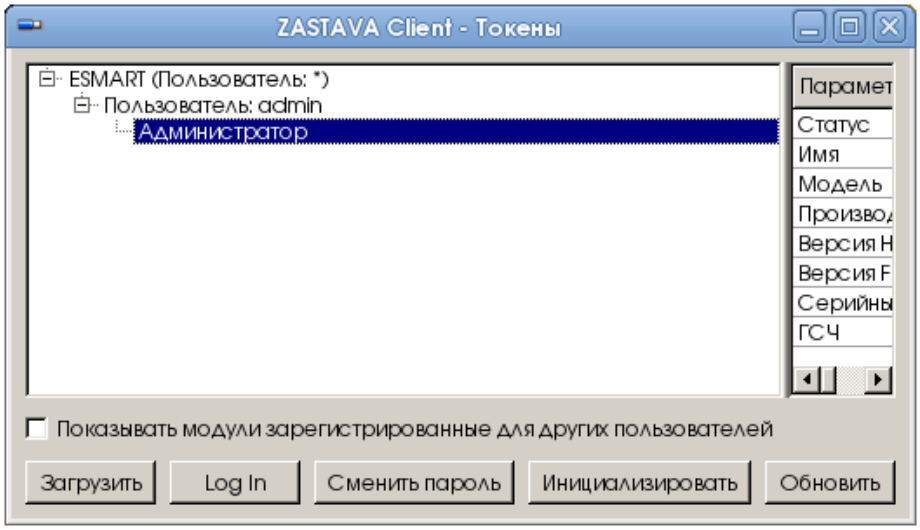

Рисунок 62 – Окно «Токены»

4) В открывшемся окне «Сменить пароль» установить переключатель «Тип пароля» в положение «Пароль пользователя» (см. Рисунок 63).

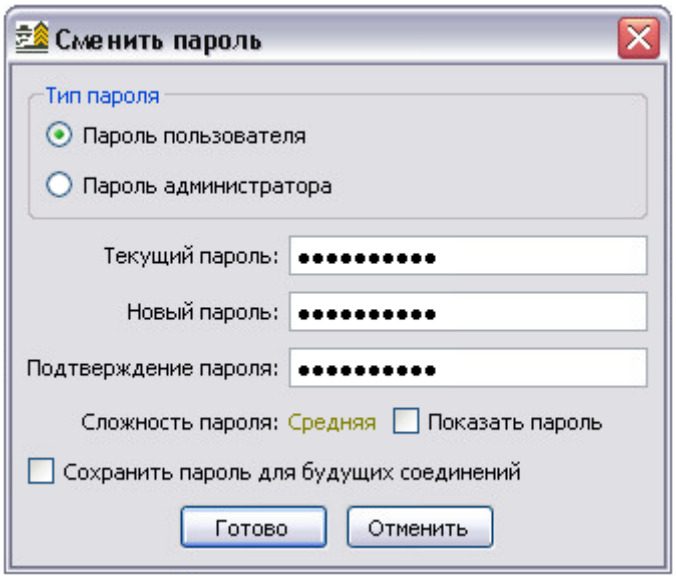

Рисунок 63 – Окно смены PIN-кода ключевого носителя

5) Ввести текущий PIN-код ключевого носителя в поле «Текущий пароль». Ввести новый PIN-код в поля «Новый пароль» и «Подтверждение пароля».

   При смене PIN-кода необходимо руководствоваться следующими правилами:

   – длина PIN-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.);
   – PIN-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 PIN-кода новое значение должно отличаться от предыдущего не менее, чем на четыре символа.

6) При необходимости, установить флажок «Сохранить пароль для будущих соединений». В этом случае при установлении нового защищенного соединения в течение одного сеанса работы не нужно будет заново вводить PIN-код.
7) Нажать кнопку «Готово». PIN-код ключевого носителя будет изменен.

4.9.2 Порядок уничтожения криптографических ключей, утилизации смарт-карт

Уничтожение (стирание) криптоключей, содержащихся на смарт-карте, может производиться либо путем форматирования смарт-карты - стирания (разрушения) криптоключей без повреждения смарт-карты (для обеспечения возможности её многократного использования), либо путём физического уничтожения смарт-карты.

Форматирование смарт-карты производится Администратором АПК. Для этого необходимо:

1) открыть окно «Токены»;

2) в окне «Токены» выбрать из списка в левой части окна название необходимого ключевого носителя, затем нажать кнопку «Инициализировать»;

3) в окне «Инициализация токена» (см. Рисунок 64) следует ввести PIN-код администратора и установить и подтвердить новый PIN-код заводского состояния «12345678».

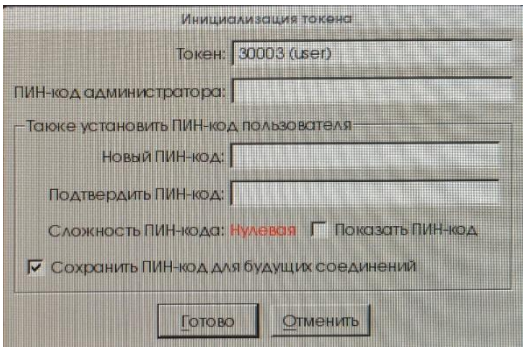

Рисунок 64 – Окно Инициализация токена

После инициализации токена все данные, включая криптографические ключи, со смарт-карты будут удалены.

В случае если при обращении к смарт-карте в целях уничтожения (стирания) криптоключей Администратора безопасности превышено количество допустимых попыток неверного ввода PIN-кода (10 попыток по умолчанию), смарт-карта не подлежит дальнейшему использованию и должна быть утилизирована.

Утилизация выполняется путем нанесения неустранимого физического повреждения, исключающего возможность повторного её использования и восстановления ключевой информации. Рекомендуемые способы утилизации смарт-карты – разрезание карты ножницами по середине микросхемы.

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. В состав АПК входит набор штатных криптобиблиотек (см. Таблица 25).

Таблица 25 – Состав криптобиблиотек

Наименование	Описание
`crypto_cpro_user`	Криптоалгоритмы ГОСТ для шифрования

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 65).

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

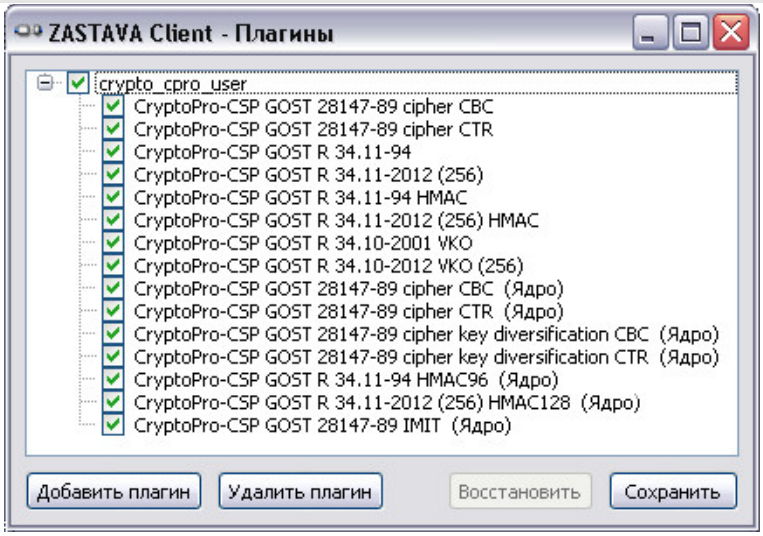

Рисунок 65 – Окно модуля криптоплагинов

4.10.2 Активация криптобиблиотеки

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

1) Чтобы активировать криптоалгоритм надо 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.

4.11 Окно «Прочие настройки»

Все параметры, которые определяют работу «ЗАСТАВА-Клиент», можно разделить на две группы:

– локальные установки;
– параметры в ЛПБ.

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

Чтобы получить доступ к окну «Прочие настройки» необходимо на Панели управления нажать кнопку «Настройки» (см. Рисунок 66).

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


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


Некоторые изменения, например, активация ЛПБ, не могут быть отменены.

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

Таблица 26 – Параметры окна «Прочие настройки»

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

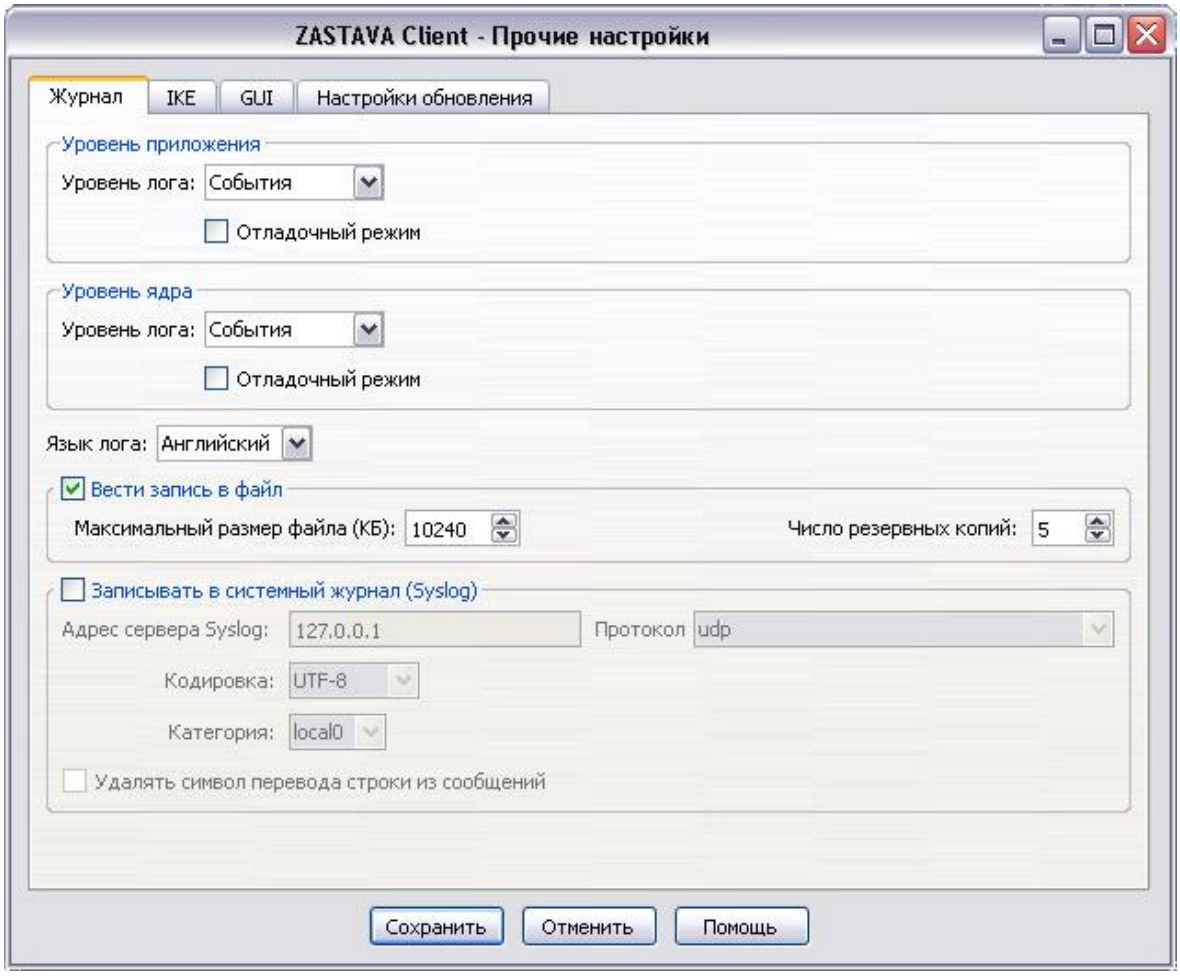

Рисунок 66 – Окно «Прочие настройки» с отображением вкладки «Журнал»

4.11.1 Вкладка «Журнал»

Регистрация событий позволяет сохранять хронологию системных событий, происходящих в «ЗАСТАВА-Клиент». Настройку системы регистрации событий можно произвести во вкладке «Журнал» окна «Прочие настройки», для выбора вкладки «Журнал» необходимо на Панели управления нажать кнопку «Настройки» и в появившемся окне выбрать вкладку «Журнал» (см. Рисунок 67).

На вкладке «Журнал» окна «Прочие настройки» можно изменить язык регистрации системных событий, для этого необходимо выбрать нужное значение в поле «Язык лога» и нажать кнопку «Сохранить» для сохранения изменений.

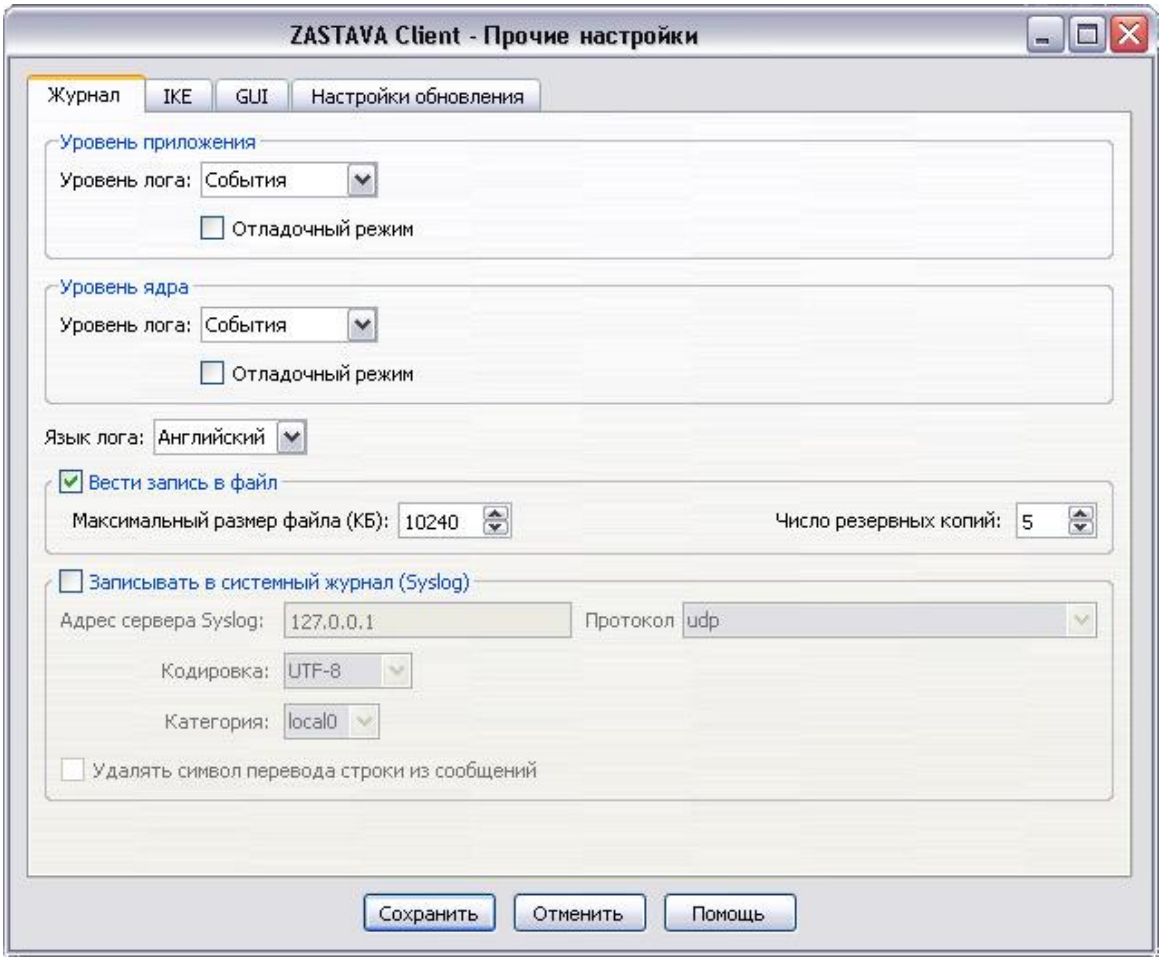

Рисунок 67 – Вкладка «Журнал» окна «Прочие настройки»

4.11.1.1 Уровень регистрации событий

Задать уровень регистрации событий можно для двух уровней: уровень приложения и уровень ядра (см. Рисунок 67). На уровне приложения генерируются сообщения от службы (процессы и т.д.), на Уровне ядра – сообщения от драйвера. Сообщения уровня ядра в журнале помечаются как «DRV».

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

Если установлен флажок «Отладочный режим» (см. Рисунок 67) уровни регистрации событий, заданные в политике, будут игнорироваться.

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

Таблица 27 – Значения для уровня регистрации событий

Уровень регистрации событий	Параметры
Заблокирован	События не будут регистрироваться
События	Будет регистрироваться минимальное количество информации об операциях, а также все сообщения об ошибках.

Уровень регистрации событий	Параметры
Подробный	Будет регистрироваться полная информация об операциях (для поиска неисправностей).
Отладочный	Все события будут зарегистрированы; уровень используется, в основном, для отладки.

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

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

Настройки системы регистрации событий (название архивных файлов журнала, их количество, максимальный размер файла журнала, настройки Syslog) хранятся в секции `/LOG` файла localsettings.ini, который располагается в секции /var/vpnagent/. Некоторые из этих параметров могут также настраиваться через графический интерфейс «ЗАСТАВА-Клиент», см. вкладку «Журнал» окна «Прочие настройки».

4.11.1.2 Параметры файла регистрации событий

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

Сам журнал может просматриваться по нажатию кнопки «Журнал» на Панели управления (см. подраздел 4.5).

Параметры SYSTEM, LP, LDAP, CM управляются как из «ЗАСТАВА-Клиент», так и централизовано из ЦУП, при условии, что уровень регистрации событий данных модулей в ЦУП установлен в значение DEFAULT.

4.11.1.3 Параметры журнала Syslog

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

Таблица 28 – Настройка параметров записи в системный журнал

Настройки	Параметры
Адрес сервера Syslog	Задаёт значение адреса syslog-сервера

Настройки	Параметры
Протокол	Протокол, в соответствии с которым будет происходить передача данных
Категория	Оно из предопределённых значений от local0 до local7. Позволяет идентифицировать сообщения от «ЗАСТАВА-Клиент» в общем журнале
Кодировка	Кодировка, в которой будут формироваться сообщения для системного журнала
Удалять символ перевода строки из сообщений	Параметр для склеивания строчек в многострочном сообщении

4.11.2 Вкладка «IKE»

«ЗАСТАВА-Клиент» позволяет настроить параметры протокола IKE, для этого необходимо воспользоваться вкладкой «IKE» окна «Прочие настройки» (см. Рисунок 68).

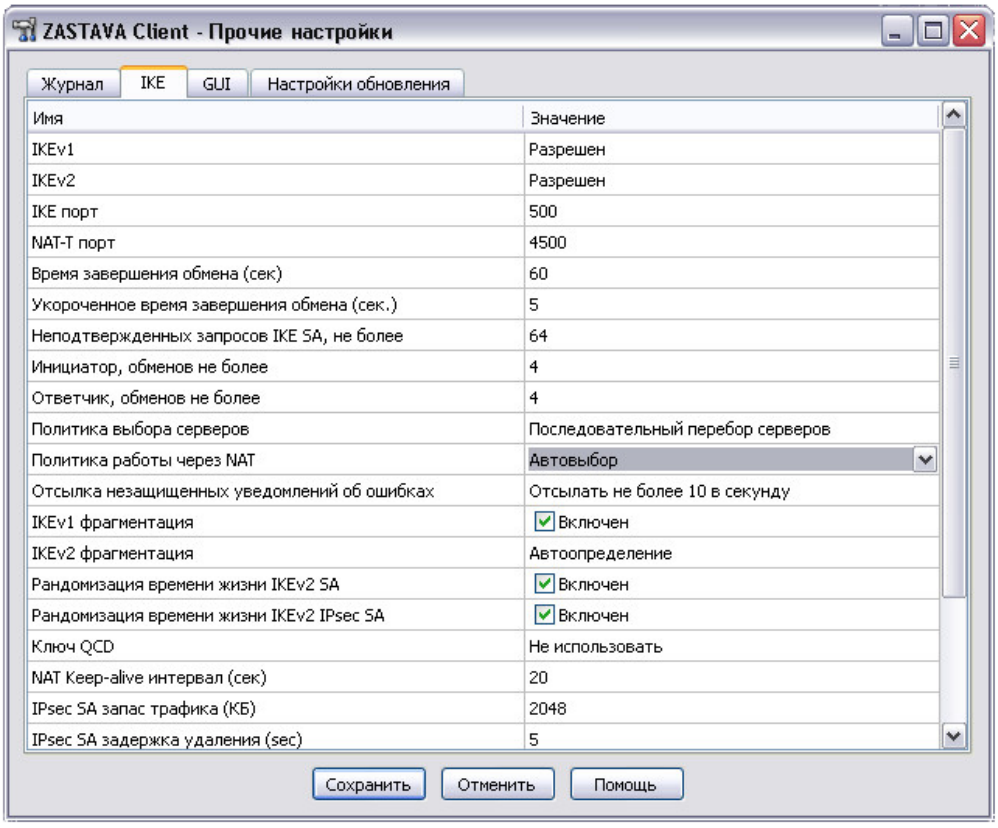

Рисунок 68 – Окно «Прочие настройки» вкладки «IKE»

4.11.2.1 Изменение параметров

Все параметры на вкладках изменяются одинаково, одним из приведенных способов, в зависимости от типа поля:

- выбрать из списка;
- двойное нажатие левой клавишей мыши на поле со значением параметра, ввести новое значение с клавиатуры. Недопустимые символы не отображаются в поле;
- установить/снять флажок.

Чтобы сохранить изменения необходимо нажать кнопку «Сохранить».

4.11.2.2 Параметры протокола IKE

Протокол IKE является протоколом управления ключами. IKE подтверждает подлинность IPsec-партнёров и организует вторичные IPsec-соединения. Параметры IKE приведены в таблице (см. Таблица 29).

Таблица 29 – Параметры IKE

Параметр	Расшифровка
IKEv1	Управление режимом работы IKEv1 (по умолчанию – Разрешен) Режимы: — Разрешен; — Только ответчик; — Запрещен.
IKEv2	Управление режимом работы IKEv2 (по умолчанию - Разрешен) Режимы: — Разрешен; — Только ответчик; — Запрещен.
IKE порт	Номер порта для IKE-соединения (1–65535, по умолчанию 500)
NAT-T порт	Порт для работы алгоритма NAT-Traversal. Трафик IKE будет переключен на этот порт, когда при установлении соединения между партнерами обнаруживается присутствие NAT-устройств. (1–65535, по умолчанию 4500)
Время завершения обмена (сек)	Максимальное время для создания защищенного соединения (SA). (5–600, по умолчанию 60)
Укороченное время для завершения обмена (сек)	Укороченное время для завершения обмена (3-60, по умолчанию 5)
Неподтвержденных запросов IKE SA, не более	Максимальное количество стейтов IKE в процессе создания SA, в которых нет подтверждения IP-адреса партнера (0–256, по умолчанию 64). Если количество запросов от неподтвержденных IP-адресов превышает этот параметр, то для IKEv2 любой новый запрос также игнорируется, но при этом запускается процедура подтверждения IP-адреса. Эта процедура заключается в отправке инициатору специального значения – COOKIE, которое тот должен вернуть. Стейт при этом не создается. Если запрос посылался с несуществующего IP-адреса, то COOKIE инициатором получено не будет и, соответственно, не будет возвращено. Если же адрес был реальный, то инициатор повторно посылает запрос, включая в него COOKIE. Такие запросы считаются ответчиком подтвержденными и минуют проверку на превышение описываемого параметра
Ответчик, обменов не более	Максимальное количество параллельных обменов, которые данный хост готов принимать в качестве ответчика в рамках одной IKE SA (1–16, по умолчанию – 4). Для IKEv2 этот же параметр (но заданный у партнера) будет определять максимальное количество параллельных обменов, которые могут быть инициированы данным хостом в рамках одной IKE SA
Политика выбора	Политика выбора серверов (по умолчанию – Последовательный

Параметр	Расшифровка
серверов	перебор серверов) Режимы: — Соединяться только с первым сервером из списка; — Последовательный перебор серверов; — Перебор серверов в 2 потока; — Перебор серверов в 4 потока; — Перебор серверов в 8 потоков.
Политика работы через NAT	Политика выбора метода работы через NAT (по умолчанию – Автовыбор)
Отсылка незащищенных уведомлений об ошибках	Частота отправки незащищенных сообщений об ошибках (по умолчанию – Отсылать не более 10 раз в секунду). Возможные значения: не отсылать, Отсылать не более 1 сек, Отсылать не более 10 сек, Отсылать не более 100 сек, Всегда отсылать
IKE v2 фрагментация	Управление режимом фрагментации (IKEv2) (по умолчанию – Автоопределение) Значения: — Не использовать; — Автоматический; — Всегда фрагментировать.
Рандомизация времени жизни IKE v2 IPsec SA	Рандомизация времени жизни IPsec SA (по умолчанию включена)
Рандомизация времени жизни IKE v2 SA	Рандомизация времени жизни IKE SA (IKEv2) (по умолчанию включена)
Ключ QCD	Ключ для выработки токена для метода Quick Crash Detection (генерируется автоматически или может быть отключен, по умолчанию «Не использовать»). На всех узлах кластера значение ключа должно быть одинаковое, сгенерированное на одном узле значение необходимо применить для всех узлов кластера. Для выключения необходимо указать значение «не использовать». Отключение параметра не рекомендуется, но возможно в тестовых и отладочных целях или в случае проблем со сторонними агентами
NAT Keep - alive интервал (сек)	Интервал в секундах для отправки UDP пакета для поддержания трансляции на NAT устройстве (1-60, по умолчанию 20)
IPsec SA запас трафика (КБ)	Запас трафика IPsec, по достижении которого запускается процесс обновления ключей (0-16384, по умолчанию 2048)
IPsec SA задержка удаления (сек)	Задержка до удаления IPsec (по умолчанию 5)
Инициировать IPsec SA при перезагрузке ЛПБ	При включенном режиме на каждое IPSec правило в политике создается IKE и IPsec SA при перегрузке политики
IPSec SA размер окна для подавления атак воспроизведения	IPSec размер окна для подавления атак воспроизведения (по умолчанию 64). Возможные значения: 32, 64, 128,264, 512, отключено
Инициировать IPsec SAs при загрузке ЛПБ	Управление режимом инициации IPsec SAs при загрузке ЛПБ (по умолчанию выключен)

Параметр	Расшифровка
IKE-CFG конфигурирование DNS серверов	Параметр, регулирующий режимы обработки IKE-CFG. При установлении SA, на интерфейсе, через который оно установлено, прописывается DNS-сервер в зависимости от настроек: — Выключено – используется системный DNS. DNS, указанный в политике, не используется; — Включено – используется DNS, указанный в политике, системный DNS не используется; — Включено, применять до системных (используется по умолчанию) – используется DNS, указанный в политике, и он применяется в первую очередь; — Включено, применять после системных – DNS, указанный в политике, используется после неудачной попытки использования системного DNS. После разрыва SA соответствующая запись о DNS-сервере удаляется
Обработка CRL	Параметр, регулирующий режимы обработки СОС Режимы: — Выключена (используется по умолчанию); — Включена, отзывать если CRL недоступен; — Включена, не отзывать если CRL недоступен.

Некоторые дополнительные параметры протокола IKE хранятся в ЛПБ, создаваемой для «ЗАСТАВА-Клиент» в ЦУП.

4.11.2.3 Политика работы через NAT

Управление политикой выбора метода работы через NAT осуществляется из локальных настроек «ЗАСТАВА-Клиент» на вкладке «IKE», параметр «Политика работы через NAT». Политика может быть такой, как представленная в таблице (см. Таблица 30).

Таблица 30 – Управление политикой выбора метода работы через NAT

Параметр	Расшифровка
Не использовать	«ЗАСТАВА-Клиент» не предлагает (будучи инициатором) и не воспринимает (будучи респондентом) ни один из методов UDP-инкапсуляции. То есть, инкапсуляции не будет даже при наличии NAT.
Стандарт	Этот режим устанавливается по умолчанию после установки «ЗАСТАВА-Клиент». Будучи инициатором, предлагаются все варианты UDP-инкапсуляции, кроме метода Huttunen, будучи респондентом приоритетным считается метод Стандарт.
Все методы	Использовать все методы. Будучи инициатором, предлагаются все варианты UDP-инкапсуляции, будучи респондентом приоритетным считается метод Стандарт.
Huttunen	Этот метод делает вариант Huttunen более приоритетным. Будучи инициатором, «ЗАСТАВА-Клиент» предлагает только его. Будучи респондером, «ЗАСТАВА-Клиент» считает метод Huttunen более приоритетным (но не единственно возможным).
Автовыбор	Этот режим устанавливается по умолчанию после установки «ЗАСТАВА-Клиент». Режим характеризуется тем, что, будучи инициатором, в Main Mode «ЗАСТАВА-Клиент» пытается сам выбрать подходящий метод UDP-инкапсуляции.
Стандарт (Принудительно)	Стандартный режим с принудительной инкапсуляцией. Полностью аналогичен режиму Стандарт, за тем исключением, что инкапсуляция используется всегда, независимо от наличия или отсутствия NAT-а между

Параметр	Расшифровка
	партнерами.
Все методы (принудительно)	Режим Все методы с принудительной инкапсуляцией. Полностью аналогичен режиму Все методы, за тем исключением, что инкапсуляция используется всегда, независимо от наличия или отсутствия NAT-а между партнерами.
Huttunen (Принудительно)	Режим Huttunen с принудительной инкапсуляцией. Полностью аналогичен режиму Huttunen, за тем исключением, что инкапсуляция используется всегда, независимо от наличия или отсутствия NAT-а между партнерами
Автовыбор (Принудительно)	Автоопределение с принудительной инкапсуляцией. Режим полностью аналогичен режиму Автовыбор, за тем исключением, что инкапсуляция используется всегда, независимо от наличия или отсутствия NAT-а между партнерами.

4.11.3 Вкладка «GUI»

Вкладка «GUI» окна «Прочие настройки» позволяет настроить представление графического интерфейса «ЗАСТАВА-Клиент» (см. Рисунок 69).

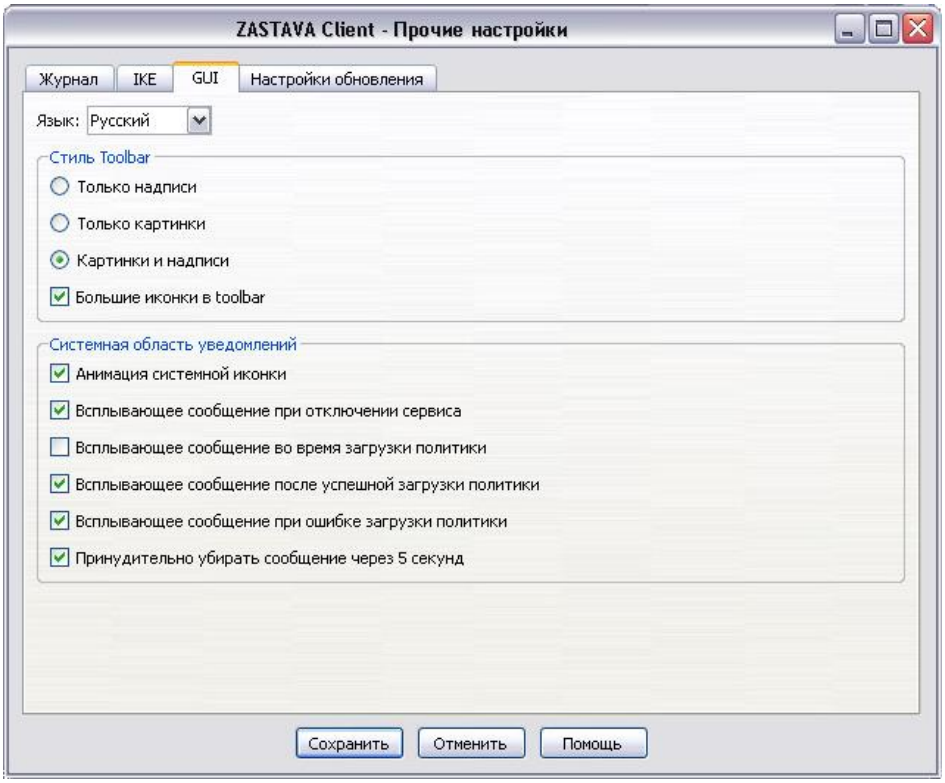

Рисунок 69 – Вкладка «GUI» окна «Прочие настройки»

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

Также можно изменить представление иконок на Панели управления «ЗАСТАВА-Клиент», для этого необходимо поставить флажок в поле «Большие иконки в toolbar».

Язык GUI также можно поменять на этой вкладке.

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

Параметры вкладки «GUI» представлены в таблице (см. Таблица 31).

Таблица 31 – Параметры вкладки «GUI»

Параметр	Описание
Только картинки	Отображает/скрывает Панель управления в виде иконок и в представлении всех окон «ЗАСТАВА-Клиент».
Только надписи	Отображает/скрывает имена кнопок на Панели управления и в представлении всех окон «ЗАСТАВА-Клиент».
Картинки и надписи	Отображает/скрывает имена кнопок на Панели управления и в представлении всех окон «ЗАСТАВА-Клиент».
Большие значки в toolbar	Изменяет размер иконок на Панели управления и в представлении всех окон «ЗАСТАВА-Клиент».
Язык	Изменяет язык интерфейса (пункты «Русский», «English») представления GUI «ЗАСТАВА-Клиент».
Анимация системной иконки	Отображает/скрывает анимацию системного значка на панели инструментов рабочего стола.
Всплывающие сообщения при отключении сервиса	Включает трансляцию всплывающих сообщений при отключении сервиса
Всплывающие сообщения во время загрузки политики	Включает трансляцию всплывающих сообщений во время загрузки политики
Всплывающие сообщения после успешной загрузки политики	Включает трансляцию всплывающих сообщений после успешной загрузки политики
Всплывающие сообщения при ошибке загрузки политики	Включает трансляцию всплывающих сообщений при ошибке загрузки политики
Принудительно убрать сообщения через 5 секунд	Закрывает тултипы через 5 секунд, даже если пользователь не двигает мышью (по умолчанию используется – включен)

4.11.4 Вкладка «Настройки обновления»

Вкладка «Настройки обновления» окна «Прочие настройки» предназначена для локального конфигурирования автоматических обновлений.

В АПК используется централизованное обновление по команде с сервера. Ручные настройки обновления не функционируют. Описание вкладки «Настройки обновления» приведено для справки.

4.11.4.1 Описание элементов интерфейса

Общий вид вкладки «Настройки обновления» приведен на рисунке (см. Рисунок 70). Описание элементов интерфейса вкладки «Настройки обновления» приведено в таблице (см. Таблица 32).

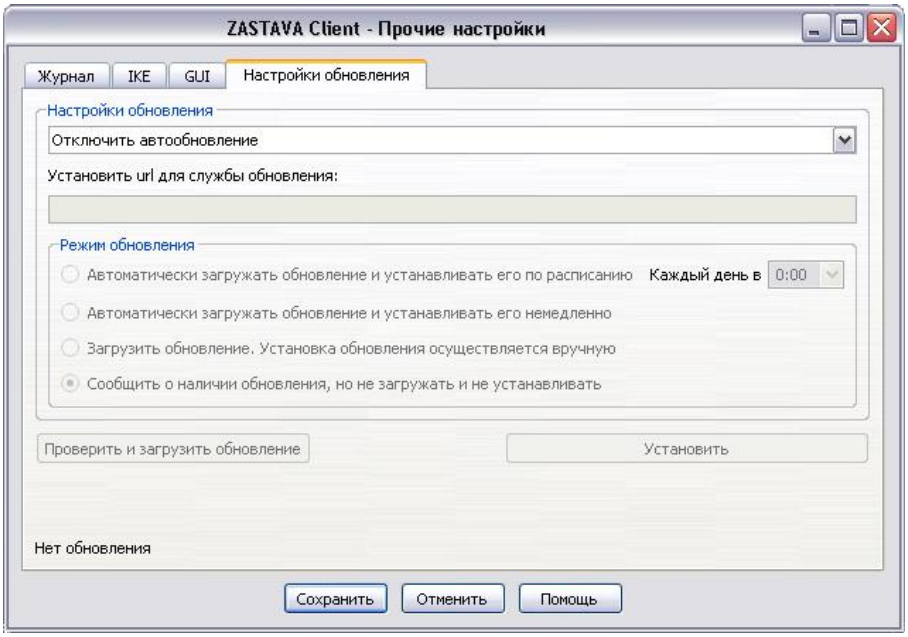

Рисунок 70 – Вкладка «Настройки обновления» окна «Прочие настройки»

Таблица 32 – Описание элементов интерфейса вкладки «Настройки обновления»

Элемент	Описание
Выпадающий список	Метод конфигурирования обновлений. Доступные значения: – Отключить автообновление – автоматические обновления отключены. – ЛПБ – конфигурирование обновлений выполняется централизованно, через ЦУП (параметры будут считываться из ЛПБ). – Ручные установки – конфигурирование обновлений проводится вручную.
Установить url для службы обновления	(Учитывается только в методе конфигурирования Ручные установки) Адрес ресурса, к которому будет обращаться «ЗАСТАВА-Клиент» при проверке обновлений.
Режим обновления	(Учитывается только в методе конфигурирования Ручные установки) Режим скачивания и инсталляции обновлений (четыре варианта).
Кнопка «Проверить и загрузить обновление»	При нажатии кнопки проверяется соединение с указанным сервером и наличие свежей версии «ЗАСТАВА-Клиент». В случае успеха будет выведено соответствующее сообщение и можно будет запустить скачивание обновления.
Кнопка «Установить»	Инсталлировать скачанное обновление.

4.12 Окно «Помощь»

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

Навигационная область справочной системы отображается в левой части окна справки (см. Рисунок 71).

Для просмотра справки по определенным интересующим настройкам необходимо нажать ссылку на необходимый раздел для его просмотра. При выборе раздела из списка этот раздел будет отображен в правой части окна.

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

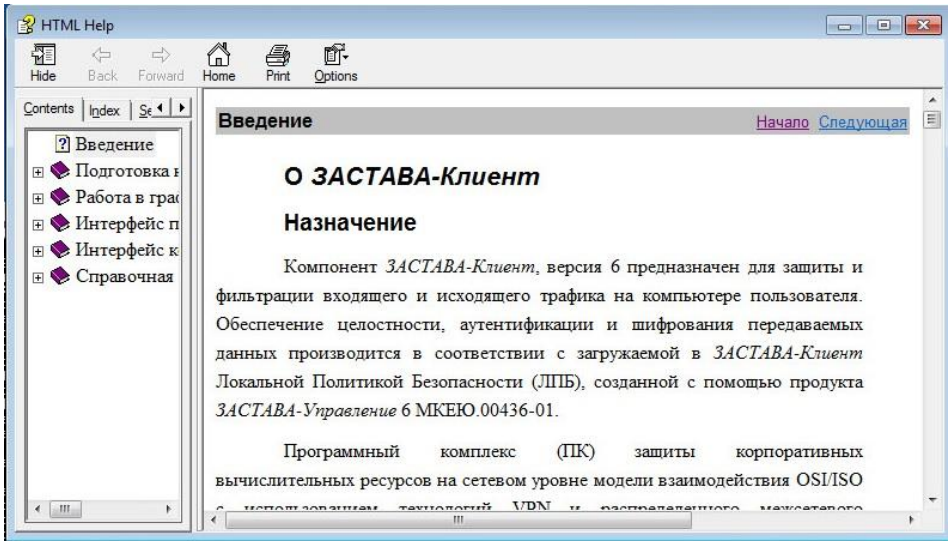

Рисунок 71 – Окно справочной системы «ЗАСТАВА-Клиент»

5 Интерфейс командной строки «ЗАСТАВА-Клиент»

Интерфейс командной строки позволяет администратору автоматизировать процесс конфигурирования «ЗАСТАВА-Клиент». Интерфейс командной строки может также использоваться, если по некоторым причинам вам более удобно работать с консольными приложениями, чем в оконной среде.

5.1 Мониторинг работы «ЗАСТАВА-Клиент»

5.1.1 Обзор средств мониторинга

Для возможности осуществления мониторинга работы «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`).

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

5.1.1.2 Очистка файла регистрации системных событий

Очистка содержимого файла регистрации системных событий происходит автоматически по достижении им максимально допустимого размера. Подробно о настройке параметров регистрации системных событий и управлении файлами регистрации см. п. 5.3.5. Это событие будет зарегистрировано и размещено в начале файла журнала.

5.2 Утилита vpnmonitor

Утилита vpnmonitor предоставляет возможность обзора активных в настоящее время защищенных соединений, установленных с данным компьютером. Кроме того, утилита vpnmonitor позволяет просмотреть статистику по пакетам.

5.2.1 Справочная система по работе с утилитой

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

5.2.2 Просмотр статистики

Для вывода статистики выполнить команду (см. Таблица 33):

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

Таблица 33 – Параметры команды `vpnmonitor -s`

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

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

Таблица 34 – Печень параметров статистики

Параметр	Описание
IPsec	
Packets (bytes) recieved	Количество пакетов, полученное с момента запуска «ЗАСТАВА-Клиент»
Packets (bytes) sent	Количество пакетов, посланное с момента запуска «ЗАСТАВА-Клиент»
Decapsulated packets	Количество расшифрованных пакетов
Encapsulated packets	Количество зашифрованных пакетов
Packets recieved unsecure	Количество полученных «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 реассемблировании входного пакета
Output frags consumed	Количество IP-фрагментов, использованных при реассемблировании выходного пакета
Output frags created	Количество IP-фрагментов, созданных при фрагментации выходного пакета
Decrease MTU requests	Количество пакетов – запросов на понижение MTU
Incoming packets not found in hash table	Количество промахов для входящих пакетов при поиске фильтра в хэш-таблице
Outgoing packets not found in hash table	Количество промахов для исходящих пакетов при поиске фильтра в хэш-таблице
IKEv2	
IKE SAs created (failed) initiated/responded	Количество созданных (не созданных) инициированных/отвеченных IKE SA в формате x(x)/x(x)

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

Параметр	Описание
Full lines	Количество заполненных линий
Empty lines	Количество пустых линий
Other lines	Количество остальных линий
Average length of non-empty lines	Средняя длина непустых линий

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

```
param                          |value
-------------------------------|-----------------------------
IPsec                          |
Packets (bytes) recieved       |979 847 (159 993 099)
Packets (bytes) sent           |87 331 (18 829 527)
Decapsulated packets           |4
Encapsulated packets           |4
Packets recieved unsecure      |979 843
Packets sent unsecure          |87 327
Incoming errors                |0
Outgoing errors                |0
Incoming auth errors           |0
Incoming anti-replay errors    |0
Dropped packets (in/out)       |0 (0 / 0)
Input frags consumed           |0
Output frags consumed          |0
Output frags created           |0
Decrease MTU requests          |0
Incoming packets not found i~|72 662
n hash table                   |
Outgoing packets not found i~|337
n hash table                   |

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

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

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

Для просмотра информации об активированной на «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 компьютером, 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:

- `-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.
- `-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 35 и Таблица 36), `operation` – операция для произведения сравнения по выбранному полю с эталоном (см. Таблица 37), `etalon` – эталонное значение выбранного поля, по которому будет произведено сравнение в соответствии с выбранной операцией.

Таблица 35 – Параметры фильтрации протокола IKE

Параметр	Характеристика
type	Тип создания SA
mode	Режим создания SA
role	Роль локальной машины при создании SA
state	Состояние IKE SA
eapid_local	Свой EAP ID
ikeid_local	IKE ID данного компьютера
eapid_remote	EAP ID, присланный партнером
ikeid_remote	IKE ID партнера
id_remote	ID партнера (IKE ID или EAP ID в зависимости от метода аутентификации)
rule_name	Имя правила
algcipher	Алгоритм шифрования

Параметр	Характеристика
alghash	Алгоритм хэширования
dhgroup	DH-группа
algintegrity	Алгоритм контроля целостности
algprf	Псевдослучайная функция
local_ip	IP-адрес данного компьютера, использованный при создании защищенного соединения
local_port	UDP-порт на данном компьютере, использованный при создании защищенного соединения
peer_ip	IP компьютера, с которым создано защищенное соединение
peer_port	UDP-порт компьютера, с которым создано защищенное соединение
redirect_ip	IP компьютера, с которого произошло перенаправление на данный
peer_auth_method	Метод аутентификации партнера
auth_method	Метод идентификации данного компьютера
spi	IKEv2 SPI
log_level	Уровень регистрации событий
features	Список поддерживаемых опций

Таблица 36 – Параметры фильтрации протокола IPsec

Тип	Характеристика
idstr	Идентификационный номер
ike_saref_str	Ссылка на IKE SA
ike_id_remote	IKE SA ID компьютера, с которым создано защищенное соединение
mode	Режим создания SA
role	Роль при создании SA
peer_id	ID компьютера партнёра
local_id	ID данного компьютера
peer_ip	IP-адрес компьютера, с которым создано защищенное подключение
peer_port	UDP-порт компьютера, с которым создано защищенное подключение
local_ip	IP-адрес данного компьютера, использованный при создании защищенного соединения
local_port	UDP-порт на данном компьютере, использованный при создании защищенного соединения
ike_cfg_server	IKE CFG адрес, выданный клиенту
dhgroup	DH группа
filter	Фильтр
rule	Название применяемого правила
esp_proto	(ESP) Правило

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

Таблица 37 – Описание типов операций фильтрации

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

Команда	Характеристика
not_icontain	поле не содержит подстроку (эталон), игнорируя регистр букв
contain	поле содержит подстроку (эталон), учитывая регистр букв
not_contain	поле не содержит подстроку (эталон), учитывая регистр букв
iequal	поле равняется эталону, игнорируя регистр букв
not_iequa	поле не равняется эталону, игнорируя регистр букв
equal	поле равняется эталону, учитывая регистр букв
not_equal	поле не равняется эталону, учитывая регистр букв
Операции для фильтрации по полю IP-адрес	
inrange	значение поля (IP-адрес) входит в диапазон заданный эталоном, в качестве эталона можно указать просто IP-адрес (10.1.1.1) или диапазон (10.1.1.1…10.1.1.255) или подсеть (10.1.1.0/24 или 10.1.1.0/255.255.255.0)
not_inrange	значение поля (IP-адрес) не входит в диапазон
equal	значение поля (IP-адрес) равно эталону (IP-адрес)
not_equal	значение поля (IP-адрес) не равно эталону (IP-адресу)
Операции для фильтрации по полю IP-порт	
equal	значение поля (порт) равно эталону
not_equal	значение поля не равно эталону
inrange	значение поля входит в диапазон заданный эталоном, в качестве эталона можно указать просто порт (8080) или диапазон (0…65535)
not_inrange	значение поля не входит в диапазон заданный эталоном
Операции для фильтрации по полю уровень лога	
equal	значение поля равно эталону (возможные значения: disabled, events, details, verbose)
not_equal	значение поля не равно эталону
gt	значение поля больше эталона (disabled < events < details < verbose)
lt	значение поля меньше эталона
gteq	значение поля больше или равно эталону
lteq	значение поля меньше или равно эталону
Операции для фильтрации по IPsec-соединению по полю mode	
equal	значение поля равно эталону (возможные значения: tunnel, transport)
not_equal	значение поля не равно эталону

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

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

Существует возможность поиска стейта по его ID:

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

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

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

Пример:

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

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 40).

Для просмотра определенного фильтра можно воспользоваться командами:

```
vpnmonitor -f [-view <table|line|list|details|count>] [-filter
<…>] [-delay <num>] [-orderby <field> [up] [-tail <num>] [-cmd
<delete>]
```

где: – `view <table|line|list|details|count>` – показывать информацию:

- `table` – в виде таблицы;
- `line` – в виде строк;
- `list` – в формате параметр – значение, для каждого фильтра;
- `details` – в таблице формата параметр – значение, для каждого фильтра;
- `count` – показывать количество фильтров;
- `filter` – фильтрация в соответствии с заданным правилом (см. Таблица 38);
- `orderby <field>` - сортировка по заданному полю (см. Таблица 39);
- `delay <num>` - вывод команды с задержкой в заданное количество секунд;
- `tail <num>` - вывод послендих <num> строк;
- `cmd <delete>` - удалить отфильтрованные значения (только для динамических фильтров).

Таблица 38 – Параметры фильтрации протокола

Параметр	Характеристика
type	Параметр фильтрации по полю «Тип»
name	Параметр фильтрации по полю «Название»
action	Параметр фильтрации по полю «Действие»
log_level	Параметр фильтрации по полю «Уровень лога»
flags_ttl_str	Параметр фильтрации по времени жизни
comment	Параметр фильтрации по полю «Комментарий»
if-names	Параметр фильтрации по полю «Интерфейс»
srcsel_as_str	Параметр фильтрации по полю «Локальный селектор»
srcsel_ip	Фильтрация поля «Локальный селектор» по IP-адресу
srcsel_port	Фильтрация поля «Локальный селектор» по порту
dstsel_as_str	Параметр фильтрации по полю «Удаленный селектор»
dstsel_ip	Фильтрация поля «Удаленный селектор» по IP-адресу

Параметр	Характеристика
dstsel_port	Фильтрация поля «Удаленный селектор» по порту
pkt_in	Параметр фильтрации по полю «Входящие пакеты»
pkt_out	Параметр фильтрации по полю «Исходящие пакеты»
bytes_in	Параметр фильтрации по полю «Входящих байт»
bytes_out	Параметр фильтрации по полю «Исходящих байт»
drop_in	Параметр фильтрации по полю «Входящих байт отброшено»
drop_out	Параметр фильтрации по полю «Исходящих байт отброшено»
miss_in	Параметр фильтрации по полю «Входящих промахов в кэше»
miss_out	Параметр фильтрации по полю «Исходящих промахов в кэше»
fh_count	Параметр фильтрации по полю «Записей в кэше»
fwprocs	Параметр фильтрации по полю «Фаервольные процедуры»

Таблица 39 – Описание типов операций фильтрации

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

Пример:

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

Таблица 40 – Отображаемые параметры информации о действующих фильтрах

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

Пример вывода команды `vpnmonitor -f` представлен ниже:

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

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

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

5.3 Утилита vpnconfig

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

Операции с утилитой `vpnconfig` доступны только администратору АПК.

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

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

Некоторые изменения, например, активация ЛПБ, не могут быть отменены.

5.3.1 Справочная система по работе с утилитой

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

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

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

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

5.3.2 Просмотр информации о «ЗАСТАВА-Клиент»

Для получения информации о «ЗАСТАВА-Клиент» необходимо воспользоваться командой: `vpnconfig –ver`.

Пример вывода команды `vpnconfig –ver`:

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

5.3.3 Работа с сертификатами и ключами

Цифровые сертификаты и предварительно распределенные ключи необходимы, чтобы проверять подлинность партнеров по взаимодействию, сертификаты (включая сертификаты УЦ), предварительно распределенные ключи, СОС регистрируются в «ЗАСТАВА-Клиент». Описание видов сертификатов и их параметров приведено в подразделе 4.7.

«ЗАСТАВА-Клиент» поддерживает СОС. Для получения более полной информации обращайтесь к п. 4.7.4.

5.3.3.1 Свойства сертификата и его проверка

Для просмотра всех свойств сертификата необходимо узнать id сертификата, для этого надо выполнить команду: `vpnconfig –list cert`. Затем выполнить команду: `vpnconfig –view cert <id>`.

Будет выведена полная информация о свойствах сертификата, а также выведена его *цепочка доверия*, т.е. список УЦ, подтверждающих подлинность сертификата. Обычно нет необходимости проверять сертификат вручную, поскольку после получения сертификата от партнёра по связи через протокол IKE, сертификат всегда проверяется автоматически. Однако, ручная проверка сертификата полезна, когда возникают проблемы при создании защищенного соединения с данным партнёром связи.

Описание всех свойств сертификата представлено в таблице (см. Таблица 41).

Таблица 41 – Свойства сертификата

Свойство	Описание
Version	Версия сертификата
Серийный номер	Серийный номер сертификата
Issuer	Кем выдан сертификат
Subject	Содержит отличительное имя субъекта, то есть владельца закрытого ключа, соответствующего открытому ключу данного сертификата. Субъектом сертификата может выступать УЦ, РЦ или конечный субъект.
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

Свойство	Описание
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 Списки Отозванных Сертификатов

СОС – это список сертификатов, которые с данного момента времени не имеют силы и не должны использоваться для формирования защищенных соединений (SA) в течение сеанса безопасного соединения. Подробное описание СОС представлено в п. 4.7.4.

Для того чтобы просмотреть зарегистрированный СОС необходимо выполнить команду: `vpnconfig -list cert crl`.

5.3.3.2.1 Импортирование СОС вручную

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

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

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

5.3.4 Работа с ЛПБ

Для просмотра доступных политик необходимо выполнить команду: `vpnconfig -list lsp`. Вывод результата выполнения данной команды будет содержать список ЛПБ и их параметры, а также состояние ЛПБ.

5.3.4.1 Установка списка ЛПБ

ЛПБ может быть удалена, изменена и активирована. Во время активации ЛПБ необходимо ввести логин и пароль администратора.

5.3.4.2 Настройка параметров политик «ЗАСТАВА-Клиент»

5.3.4.2.1 Системная ЛПБ

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

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

Для настройки системной политики необходимо:

1) Выбрать тип метода активации из поля «Источник» и определить параметры данного метода:
   - При выборе метода прогрузки из файла необходимо выполнить команду: `vpnconfig -set lsp system file <path>`, где: `path` – путь к файлу конфигурации.
   - При выборе метода прогрузки с сервера необходимо выполнить команду: `vpnconfig -set lsp system pmp <cert_id> <id_type> <server_ip> <log level> [<timeout>]`. Указать `cert_id`, для просмотра `id` сертификата можно воспользоваться командой: `vpnconfig -list cert personal`, либо указать значение `any` при использовании для соединения любого зарегистрированного локального сертификата. Указать `<id_type>` тип идентификатора для прогрузки политики, который должен быть согласован с ЦУП. Указать `<server_ip>|<server_name>` адрес сервера прогрузки|имя компьютера, после регистрации ЛПБ «ЗАСТАВА-Клиент» будет обращаться к заданному источнику всякий раз, когда политика активируется. Указать уровень журналирования событий `<log level>`. Указать временной промежуток между обращениями к серверу `<timeout>`.
   - При выборе метода прогрузки «отсутствует» необходимо выполнить команду: `vpnconfig -set lsp system none`, тогда в случае ошибки при прогрузке пользовательской политики, будет прогружаться DDP.

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

5.3.4.2.2 Политика пользователя

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

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

Для настройки политики пользователя необходимо:

– При выборе метода прогрузки из файла 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>]`. Указать `cert_id`, для просмотра `id` сертификата можно воспользоваться командой: `vpnconfig -list cert personal`, либо указать значение `any` при использовании для соединения любого зарегистрированного локального сертификата. Указать `<id_type>` тип идентификатора для прогрузки политики, который должен быть согласован с ЦУП. Указать `<server_ip>|<server_name>` адрес сервера прогрузки|имя компьютера, после регистрации ЛПБ «ЗАСТАВА-Клиент» будет обращаться к заданному источнику всякий раз, когда политика активируется. Указать уровень журналирования событий `<log level>`. Указать временной промежуток между обращениями к серверу `<timeout>`.

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

5.3.4.2.3 Политика драйвера по умолчанию

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

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

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

Для настройки параметров политики и ее активации можно воспользоваться одной командой: `vpnconfig -login admin <admin login> <admin password> -activate lsp ddp [pass|drop|dropall]`.

Из соображений безопасности рекомендуется устанавливать «Политика драйвера по умолчанию» в значение «Сбрасывать все» (`dropall`). Следует учесть, что в этом случае сеть не будет доступна, если компьютеру не присвоен статический IP-адрес. Если компьютер получает IP-адрес по DHCP, то следует выбрать опцию «Сбрасывать все, кроме DHCP» (`drop`). В этом случае сеть будет недоступна до момента активации рабочей ЛПБ (исключение составляет только трафик DHCP, необходимый для назначения компьютеру IP-адреса).

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

5.3.4.2.4 Изменение сертификата 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 с сервера политики необходимо установить уровень регистрации событий, для этого нужно выполнить команду `vpnconfig -set lsp system|user loglevel <log level>`, где: `<log level>` – уровень регистрации событий при передаче ЛПБ с сервера политики.

5.3.4.2.6 IKE идентификатор

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

5.3.4.2.7 Серверы политик

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

После регистрации ЛПБ «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 «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`. ЛПБ загрузится в драйвер «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

Конфигурирование регистрации событий происходит с помощью команды: `vpnconfig -set log`, параметры команды представлены числами от 0 до 15 (см. Таблица 42).

Таблица 42 – Параметры команды `vpnconfig –set log`

Числовой параметр	**Описание**	**Расшифровка**
0	Log Level	Уровень регистрации событий
1	Log Level kernel	Уровень регистрации событий уровня ядра
2	File log	Включение или отключение параметра записи системных событий в файл
3	Max Log Size	Установка максимального размера файла записи системных событий
4	Backup Depth	Установка количества создаваемых резервных копий файла записи системных событий
5	Syslog	Включение или отключение параметра записи системных событий на syslog-сервер
6	Destination	Задание адреса удаленного syslog-сервера
7	Protocol	Протокол
8	Put msg len when use tcp	Выводить сообщение при использовании протокола tcp
9	Encoding from	Выбор алгоритма кодировки для открытия журнала событий
10	Encoding to	Выбор алгоритма кодирования сообщений записи системных событий
11	Facility	Настойка уровня протоколирования Syslog
12	Language	Установка языка журналирования
13	Broadcast messages to terminals from vpndmn	Широковещательные сообщения терминалам от службы «ЗАСТАВА-Клиент»
14	Verbose mode for application level	Установить отладочный уровень регистрации событий для уровня приложения
15	Verbose mode for kernel level	Установить отладочный уровень регистрации событий для уровня драйвера
16	Syslog Singleline	Удалять символы новой линии из сообщений

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

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

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

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

Параметры уровня регистрации могут также указываться в ЛПБ, созданной в ЦУП для «ЗАСТАВА-Клиент». В этом случае установки из ЛПБ будут иметь преимущество перед локальными установками. Вы можете посмотреть текущий реальный уровень регистрации событий, выполнив команду: `vpnconfig -list log`, в выводе этой команды будет содержаться вся информация о настройках системы регистрации событий «ЗАСТАВА-Клиент».

Настройки системы регистрации событий (название архивных файлов журнала, их количество, максимальный размер файла журнала, настройки Syslog) хранятся в секции `LOG` файла localsettings.ini, который располагается в основной директории «ЗАСТАВА-Клиент».

5.3.5.1 Файл регистрации событий

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

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

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

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

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

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

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

5.3.5.2 Параметры журнала Syslog

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

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

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

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

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

5.3.5.3 Удалённая регистрация событий

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

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

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

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

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

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

5.3.6 Протокол IKE

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

- Для просмотра настроек протокола надо выполнить команду: `vpnconfig -list ike`.
- Для изменения настроек протокола надо выполнить команду: `vpnconfig -set ike <id-parameter> <value>`.
- Для установки параметра в значение по умолчанию необходимо выполнить команду: `vpnconfig -reset <ike> <id-parameter>`.

5.3.6.1 Параметры протокола IKE

Протокол IKE является протоколом управления ключами. IKE подтверждает подлинность IPsec-партнёров и организует вторичные IPsec-соединения. Параметры протокола IKE приведены в таблице (см. Таблица 43).

Таблица 43 – Параметры протокола IKE

Идентификатор параметра	Параметр	Расшифровка
0	IKEv1	Управление режимом работы IKEv1. Возможные значения: – Disabled – Enabled (используется по умолчанию) – Responder only
1	IKEv2	Управление режимом работы IKEv2 Возможные значения: – Disabled – Enabled (используется по умолчанию) – Responder only
2	IKE port	Номер порта для IKE-соединения (1-65535, по умолчанию 500)
3	NAT-T port	Порт для работы алгоритма NAT-Traversal. Трафик IKE будет переключен на этот порт, когда при установлении соединения между партнерами обнаруживается присутствие NAT-устройств. Значение по умолчанию: (1-65535, по умолчанию 4500)
4	Time to complete exchange (sec)	Максимальное время для создания защищенного соединения (SA). (5-600, по умолчанию 60)
5	Shortened time to complete exchange (sec)	Укороченное время для завершения обмена (3-60, по умолчанию 5)
6	Max half-open states	Максимальное количество стейтов IKE в процессе создания SA, в которых нет подтверждения IP-адреса партнера (0-256, по умолчанию 64) Если количество запросов от неподтвержденных IP-адресов превышает этот параметр, то для IKEv2 любой новый запрос также игнорируется, но при этом запускается процедура подтверждения IP-адреса. Эта процедура заключается в отправке инициатору

Идентификатор параметра	Параметр	Расшифровка
		специального значения – COOKIE, которое тот должен вернуть. Стейт при этом не создается. Если запрос посылался с несуществующего IP-адреса, то COOKIE инициатором получено не будет и, соответственно, не будет возвращено. Если же адрес был реальный, то инициатор повторно посылает запрос, включая в него COOKIE. Такие запросы считаются ответчиком подтвержденными и минуют проверку на превышение описываемого параметра
7	Initiate no more exchanges	Максимальное количество параллельных обменов (1–16, по умолчанию – 4), которые могут быть инициированы в рамках одной IKE SA. Если система посылает больше запросов, то они будут ожидать завершения какого-либо из активных обменов. Данный параметр актуален только для IKEv1.
8	Respond to no more exchanges	Максимальное количество параллельных обменов, которые данный хост готов принимать в качестве ответчика в рамках одной IKE SA (1–16, по умолчанию – 4). Для IKEv2 этот же параметр (но заданный у партнера) будет определять максимальное количество параллельных обменов, которые могут быть инициированы данным хостом в рамках одной IKE SA.
9	Servers selecting policy	Политика выбора серверов (по умолчанию – Try servers sequencially)
10	NAT traversal policy	Политика выбора метода работы через NAT (по умолчанию - Автовыбор)
11	Sending unprotected error notifications	Частота отправки незащищенных сообщений об ошибках (по умолчанию – Limit rate to 10 per second)
12	IKE v1 fragmentation	Включение/отключение режима фрагментации (IKEv1) (по умолчанию включен)
13	IKE v2 fragmentation	Управление режимом фрагментации (IKEv2) (по умолчанию – Auto)
14	IKEv2 SA lifetime jitter	Рандомизация времени жизни IKE SA (IKEv2) (по умолчанию включена)
15	IKEv2 IPsec SA lifetime jitter	Рандомизация времени жизни IKE IPsec SA (IKEv2) (по умолчанию включена)
16	QCD Secret	Ключ для выработки токена для метода Quick Crash Detection (по умолчанию отключен). На всех узлах кластера значение ключа должно быть одинаковое, сгенерированное на одном узле значение необходимо применить для всех узлов кластера. Для выключения необходимо указать значение «не использовать». Отключение параметра не рекомендуется, но возможно в тестовых и отладочных целях или в случае проблем со сторонними агентами.
17	NAT Keep alive interval (sec)	Интервал в секундах для отправки UDP пакета для поддержания трансляции на NAT устройстве (1-60, по умолчанию 20)
18	IPsec SA provision traffic	Запас трафика IPsec, по достижении которого запускается процесс обновления ключей (0-16384, по умолчанию

Идентификатор параметра	Параметр	Расшифровка
	(KB)	2048)
19	IPsec SA removal delay (sec)	Задержка до удаления IPsec (по умолчанию – 5)
20	IPsec SA anti-replay window	IPSec размер окна для подавления атак воспроизведения (по умолчанию 64). Возможные значения: 32, 64, 128,264, 512, отключено.
21	Initiate Persistent IPsec SAs on LSP reload	При включенном режиме на каждое IPSec правило в политике создается ike и ipsec sa при перегрузке политики (по умолчанию – false)
22	IKE-CFG configure DNS servers	Параметр, регулирующий режимы обработки IKE-CFG. При установлении SA, на интерфейсе, через который оно установлено, прописывается DNS-сервер в зависимости от настроек: — Выключено – используется системный DNS. DNS, указанный в политике, не используется; — Включено – используется DNS, указанный в политике, системный DNS не используется; — Включено, применять до системных (используется по умолчанию) – используется DNS, указанный в политике, и он применяется в первую очередь; — Включено, применять после системных – DNS, указанный в политике, используется после неудачной попытки использования системного DNS. После разрыва SA соответствующая запись о DNS-сервере удаляется.
23	CRL processing	Параметр, регулирующий режимы обработки СОС. Возможные значения: — Disabled (Выключена) (используется по умолчанию); — Enabled, revoke also if COC not available (Включена, отзывать, если СОС недоступен); — Enabled, don't revoke if CRL not available (Включена, не отзывать, если СОС недоступен).

Некоторые дополнительные параметры протокола IKE хранятся в ЛПБ, создаваемой для «ЗАСТАВА-Клиент» в ЦУП.

5.3.6.1.1 Политика выбора метода работы через NAT

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

Таблица 44 – Варианты политики выбора метода работы через NAT

Числовое значение	Политика
0 (Запретить)	«ЗАСТАВА-Клиент» не предлагает (будучи инициатором) и не воспринимает (будучи респондентом) ни один из методов UDP-инкапсуляции. То есть, инкапсуляции не будет даже при наличии NAT.
1 (Стандарт)	Будучи инициатором, предлагаются все варианты UDP-инкапсуляции, кроме метода Huttunen, будучи респондентом приоритетным считается метод Стандарт.

Числовое значение	Политика
2 (Все методы)	Использовать все методы. Будучи инициатором, предлагаются все варианты UDP-инкапсуляции, будучи респондентом приоритетным считается метод Стандарт.
3 (Huttunen)	Этот метод делает вариант Huttunen более приоритетным. Будучи инициатором, «ЗАСТАВА-Клиент» предлагает только его. Будучи респондером метод Huttunen считается более приоритетным (но не единственно возможным).
4 (Автовыбор)	Этот режим устанавливается по умолчанию после установки «ЗАСТАВА-Клиент». Режим характеризуется тем, что, будучи инициатором, в Main Mode «ЗАСТАВА-Клиент» пытается сам выбрать подходящий метод UDP-инкапсуляции.
129 (Стандарт (Принудительно))	Стандартный режим с принудительной инкапсуляцией. Полностью аналогичен режиму Стандарт, за тем исключением, что инкапсуляция используется всегда, независимо от наличия или отсутствия NAT-а между партнерами.
130 (Все методы (Принудительно))	Режим Все методы с принудительной инкапсуляцией. Полностью аналогичен режиму Все методы, за тем исключением, что инкапсуляция используется всегда, независимо от наличия или отсутствия NAT-а между партнерами.
131 (Huttunen (Принудительно))	Режим Huttunen с принудительной инкапсуляцией. Полностью аналогичен режиму Huttunen, за тем исключением, что инкапсуляция используется всегда, независимо от наличия или отсутствия NAT-а между партнерами
132 (Автовыбор (Принудительно))	Автоопределение с принудительной инкапсуляцией. Режим полностью аналогичен режиму Автовыбор, за тем исключением, что инкапсуляция используется всегда, независимо от наличия или отсутствия NAT-а между партнерами.

5.3.6.1.2 Описание режимов обработки СОС

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

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

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

Таблица 45 – Режимы работы обработки CRL

Числовое значение	**Режим работы обработки** СОС
0	Disabled. Обработка СОС выключена. Поиск и проверка СОС не производятся ни для какого сертификата
1	Enabled, revoke also if CRL not available. Обработка СОС включена, при этом, если СОС не доступен, сертификат будет считаться отозванным. Обработка осуществляется следующим образом: Если в сертификате нет поля CDP (CRL Distribution Points – Точки распространения

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

5.3.7 Токены

5.3.7.1 Просмотр модулей токенов

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

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

5.3.7.2 Просмотр зарегистрированных токенов

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

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

Token
  Id: 6
  Label: Trusted Certificates token
  Model: Trusted Token
  Manufacturer: ELVIS-PLUS
  Serial Number: 29092009
  Hardware Version: 2.0
  Firmware Version: 2.0
  Logged In: Yes
  Trusted: Yes
  Login required: Yes
```

5.3.7.3 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. 5.3.7.2);

`<pin>` – PIN-код токена;

`[save]` – необязательный параметр, если его не установить, то «ЗАСТАВА-Клиент» будет запрашивать PIN-код при каждом обращении к токену.

Для того чтобы закончить сеанс работы с токеном необходимо выполнить команду `vpnconfig –logout token <token_id>`.

5.3.7.4 Смена PIN-кода токена

Для смены PIN-кода токена следует выполнить команду: `vpnconfig -password token <token_id> <pin> [save]`,

где: `<token_id>` – идентификатор токена или его название в системе;

`<pin>` – новый PIN-код токена;

`[save]` – необязательный параметр, который отвечает за сохранение PIN-кода для дальнейших обращений к токену.

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

5.4 Утилита plg_ctl

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

Следующий общий синтаксис используется при запуске утилиты `plg_ctl`:

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

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

5.4.1.1 Действия

Утилита `plg_ctl` поддерживает следующие действия, представленные в таблице (см. Таблица 46).

Таблица 46 – Действия, поддерживаемые утилитой `plg_ctl`

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

5.4.1.2 Опции

Утилита `plg_ctl` поддерживает следующие опции, представленные в таблице (см. Таблица 47).

Таблица 47 – Опции, поддерживаемые утилитой `plg_ctl`

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

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

```
-a <имя_криптоалгоритма> -u
```

5.4.2 Вывод информации о криптобиблиотеке или криптоалгоритмах

Для вывода информации о криптобиблиотеки или криптоалгоритмах необходимо указать следующее:

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

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

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

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

5.4.3 Примеры команд в интерфейсе командной строки

Примеры команд в интерфейсе командной строки приведены в таблице (см. Таблица 48).

Таблица 48 – Примеры команд в интерфейсе командной строки

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

5.5 Утилиты icv_writer и icv_checker

Утилита `icv_writer` предназначена для вычисления контрольной суммы.

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

Следующий синтаксис используется для запуска утилит `icv_writer`:

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

или

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

Утилита возвращает следующие коды:

0 – OK.

1 – неправильный параметр запуска

–1 – иные ошибки

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

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

Проверить контрольные суммы можно, запустив в утилиту `icv_checker`.

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

Используется следующий синтаксис:

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

Формат файла с контрольными суммами должен быть следующий:

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

утилита возвращает следующие коды:

0 – OK.

1 – Неправильный параметр запуска

–1 – некорректная контрольная сумма в файле

–2 – иные ошибки

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

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

Пример выполнения утилиты `icv_checker`:

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

6 НЕШТАТНЫЕ СИТУАЦИИ

6.1 Срабатывание датчика вскрытия

Датчик вскрытия срабатывает в случае физического вскрытия корпуса системного блока АПК «ЗАСТАВА-ТК». После фиксирования датчиком факта вскрытия корпуса, каждый раз при включении/перезагрузке АПК будет раздаваться звуковой сигнал.

Для отключения сигнализации необходимо сбросить датчик вскрытия в состояние «корпус не вскрыт» как описано в п. 3.2.5.

В зависимости от установленного режима датчика вскрытия возможны два варианта работы после срабатывания датчика вскрытия:

– «мягкий» режим (Soft) – при включении АПК на экране появится сообщение о факте вскрытия корпуса, пользователю будет предложено загрузить ОС и продолжить работу. Данное сообщение будет появляться каждый раз при включении до тех пор, пока датчик вскрытия не будет сброшен в состояние «корпус не вскрыт»;

– «жесткий» режим (Hard) – до сброса состояния датчика вскрытия дальнейшая работа невозможна. При включении АПК появится сообщение о факте вскрытия корпуса и будет предложено перезагрузить АПК. При перезагрузке следует войти в меню датчика вскрытия и сбросить датчик вскрытия в состояние «корпус не вскрыт».

6.2 Некорректная работа АПК «ЗАСТАВА-ТК» после обновления ОС

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

Для возврата к эталону необходимо предварительно запросить у Изготовителя (Поставщика) пароль доступа к эталону.

Возврат к эталону выполняется следующим образом:

1) Включить АПК, нажав кнопку питания , дождаться появления меню выбора вариантов загрузки «ARM-ZAGS load menu».
2) Выбрать пункт меню «ZAGS-OS recovery» и нажать клавишу <Enter>.
3) В появившемся окне «Password required» ввести полученный у производителя пароль доступа к эталону. Нажать клавишу <Enter>.
4) На экране появится сообщение о проверке контрольной суммы заводского образа ОС. Дождаться окончания проверки.

5) По окончании проверки в случае совпадения контрольных сумм будет загружена эталонная ОС, АПК перезагрузится.

   При несовпадении контрольных сумм на экран будет выведено соответствующее сообщение. В этом случае необходимо обратиться к Изготовителю (Поставщику).

6.3 Нарушение целостности образа

В случае нарушения целостности образа необходимо:

- назначить ответственного за расследование инцидента. Всю ключевую информацию считать скомпрометированной;
- в случае если действия, которые привели к инциденту, не являются угрозой безопасности (например, нарушение образа для обновления при передаче по каналам данных), необходимо выполнить возврат в эталон (см. подраздел 6.2) и выпустить новую ключевую информацию для VPN;
- в случае если действия, которые привели к инциденту, являются угрозой безопасности, то необходимо отправить АПК Изготовителю (Поставщику) на восстановление.

6.4 Автоматическое отключение АПК

Автоматическое отключение АПК происходит в следующих случаях:

- В случае неуспешного прохождения автоматического контроля целостности (см. подраздел 3.2.9). В случае автоматического отключения необходимо включить АПК заново (см. подраздел 3.2.1). Если после включение обнаружится нарушение целостности образа АПК необходимо выполнить действия, описанные в подразделе 6.3.
- В случае неуспешного прохождения контроля целостности ПО СКЗИ «ESMART Token ГОСТ», который запускается в фоновом режиме при каждом старте ОС АПК.

7 ВОЗМОЖНЫЕ НЕИСПРАВНОСТИ И СПОСОБЫ ИХ УСТРАНЕНИЯ

Возможные неисправности и способы их устранения приведены в таблице (см. Таблица 49).

Таблица 49 – Возможные неисправности и способы их устранения

Описание неисправности	Способы устранения
Отсутствие доступа пользователя к удаленному рабочему столу	Последовательно выполнить приведенные ниже действия до устранения неисправности: 1) проверить и, при необходимости, изменить настройки получения политики безопасности (см. п. 3.1.6); 2) проверить и, при необходимости, скорректировать настройки сетевых параметров (см. подраздел 3.1.4); 3) проверить контрольную сумму ОС (см. подраздел 3.2.2); 4) проверить и, при необходимости, изменить настройки BIOS (см. подраздел 3.1.2); 5) просмотреть журналы СКЗИ и журнал событий ОС на предмет выявления неполадок (см. подраздел 3.2.7); 6) обратиться к производителю.
Сбой настроек BIOS	Проверить и, при необходимости, изменить настройки BIOS (см. подраздел 3.1.2).
Ключевой носитель заблокирован после превышения числа попыток ввода PIN-кода	Разблокировать ключевой носитель, используя PIN-код администратора (см. Руководство администратора на электронный идентификатор (смарт-карту) ID-1 RU.63793390.00004-01 из состава СКЗИ ESMART Token ГОСТ).
Ключевой носитель заблокирован после превышения числа попыток ввода PIN-кода администратора	Ключевой носитель не подлежит дальнейшему использованию и должен быть утилизирован.

Перечень принятых терминов и сокращений

BIOS – Basic input/output system – Базовая система ввода-вывода
CA – Certification Authority – см. УЦ
CRL – Certificate Revocation List – см. СОС
CSP – Cryptographic Service Provider – Криптопровайдер
DH – Diffie-Hellman – протокол Диффи-Хеллмана
DHCP – Dynamic Host Configuration Protocol — протокол динамической настройки узла
DN – Distinguished Name – Уникальное имя
DNS – Domain Name System – система доменных имен для именования хостов в глобальных сетях
ESP – Encapsulated Security Payload – протокол из группы IPsecGMT – время по Гринвичу
GUI – (Graphical User Interface) графический интерфейс пользователя
IKE – Internet Key Exchange – протокол обмена ключевой информацией; используется совместно с протоколами IPsec для организации первичного защищенного канала ISAKMP SA
IP – Internet Protocol – Протокол сетевого уровня, являющийся базовым протоколом IP-сетей
IPsec – IP security – Группа протоколов для установления защищенных соединений в IP-сетях
LDAP – Lightweight Directory Access Protocol группа стандартных протоколов для доступа к каталогам ("Directories")
LSP – Local Security Policy – см. ЛПБ
MTU – Maximum Transmission Unit – Максимальный размер полезного блока данных одного пакета, который может быть передан протоколом без фрагментации
NAT – Network Address Translation – Трансляция сетевых адресов
PIN – Personal identification number – Персональный идентификационный код
PRF – Pseudo-random function – Псевдослучайная функция
SA – Security Association – Защищенное соединение (в контексте протоколов IPsec и IKE)
TCP – Сетевой протокол транспортного уровня (с гарантированной доставкой) в IP-сетях
UDP – Сетевой протокол транспортного уровня (без гарантированной доставки) в IP-сетях
URI – Uniform Resource Identifier – Унифицированный идентификатор ресурса
USB – Universal serial bus – Универсальная последовательная шина
VPN – Virtual Private Network – Виртуальная частная сеть
АМ – Аппаратный модуль
АПК – Аппаратно-программный комплекс
БД – База данных
ВЧС – Виртуальная частная сеть
ГОСТ – Государственный стандарт
ЗРС – Запрос регистрации сертификата
ЛПБ – Локальная политика безопасности
НСД – Несанкционированный доступ
ОС – Операционная система
ПО – Программное обеспечение
РЦ – Регистрационный центр
СКЗИ – Средство криптографической защиты информации
СОС – Список отозванных сертификатов
УЦ – Удостоверяющий центр
ЦУП – Центр управления политиками безопасности
ЭП – Электронная подпись

Лист регистрации изменений

Изм.	Номера листов (страниц)				Всего листов (страниц) в докум.	№ докум-мента	Входящий № сопроводит. документа и дата	Подп.	Дата
	измененных	замененных	новых	аннулиро-ванных					