УТВЕРЖДЕН

МКЕЮ.00436-01 32 01-ЛУ

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

(«ПК «VPN/FW «ЗАСТАВА», версия 6»)

Компонент

«ЗАСТАВА-Управление», версия 6

Руководство системного программиста

МКЕЮ.00436-01 32 01

Листов 284

Инв.№ подл.	Подп. и дата	Взам. инв. №	Инв.№ дубл.	Подп. и дата
3297				

2016

Содержание

1. Введение 7
1.1. О программе ЗАСТАВА-Управление 7
1.1.1. Назначение 7
1.1.2. Область применения 8
1.1.3. Характеристики 8
1.1.4. Поддерживаемые протоколы и технологии 9
1.2. Об этом документе 11
1.2.1. Как пользоваться этим документом 11
1.2.2. Типографские соглашения 12
2. Подготовка к использованию *ЦУП* 13
2.1. Системные требования 13
2.1.1. *ЦУП-Консоль* 13
2.1.2. *ЦУП-Сервер* 13
2.2. Поддерживаемые версии управляемых *Агентов* 13
2.3. Инсталляция *ЦУП* 14
2.3.1. Подготовка 14
2.3.2. Запуск инсталляции 15
2.3.3. Продолжение инсталляции: создание БД *ЦУП* 17
2.3.4. Продолжение инсталляции: настройка *ЗАСТАВА-Офис* 22
2.3.5. Завершение инсталляции: ввод файла с лицензией 23
2.4. Деинсталляция 23
3. Подготовка к использованию 24
3.1. Программная группа *ЦУП* 24
3.2. Расположение файлов *ЦУП* 24
3.3. Запуск *ЦУП-Консоль* 25
3.3.1. Создание конфигурации источника данных (DSN) для доступа к БД *ЦУП* 25
3.3.2. Ввод информации о расположении *ЦУП-Сервер* и БД *ЦУП* 25
4. Обзор конфигурации *ЦУП* 27
4.1. Введение 27
4.2. Связь между модулями *ЦУП-Консоль*, *ЦУП-Сервер*, БД *ЦУП* и *ЗАСТАВА-Офис ЦУП* 27
4.3. Подготовка к конфигурированию 29
4.4. Регистрация сертификатов 30
4.5. Основные Объекты ГПБ 31
4.6. Другие Объекты ГПБ 32
4.7. Создание ГПБ в *ЦУП-Консоль* 32
4.7.1. Объекты Политики 33
4.7.2. Правила 37
4.7.3. Расписания 45
4.7.4. Серверы 45
4.7.5. Серверы аутентификации 45
4.7.6. Сетевые Сервисы 46
4.7.7. Настройки IKE 47
4.7.8. Действия 48
4.7.9. Определяемая пользователем ЛПБ 50
4.7.10. Домены 50
4.7.11. Использование нескольких *ЦУП* 52
4.8. Работа с ГПБ и Проектами 53
4.9. Построение ЛПБ для *Агентов* 54

4.10. Образец конфигурации *ЦУП* 55
4.11. Использование удаленной *ЦУП-Консоль* 55
5. Обзор *ЦУП-Консоль* **57**
5.1. Главное окно *ЦУП-Консоль* 57
5.1.1. Строка меню 58
5.1.2. Инструментальная линейка 63
5.1.3. Работа с секциями *ЦУП* 64
5.2. Управление Объектами в *ЦУП-Консоль* 64
5.2.1. Контекстные меню 64
5.2.2. Создание Объектов 64
5.2.3. Выбор нескольких Объектов 65
5.2.4. Редактирование Объектов 65
5.2.5. Перемещение Объектов 66
5.2.6. Размещение Объектов Политики 66
5.2.7. Удаление Объектов 66
5.2.8. Поиск информации 67
5.2.9. Фильтрация отображения Правила 68
5.2.10. Сортировка информации 70
5.2.11. Фильтр поиска для Объектов политики 70
5.2.12. Комбинации клавиш для быстрого доступа к командам 71
6. Вложенные окна *ЦУП-Консоль* **74**
6.1. Топология 74
6.2. Карта 75
6.3. Зоны 77
6.4. Секция Объекты Политики 77
6.5. Серверы 78
6.6. Таблица Правил 78
6.7. Пользовательские ЛПБ 79
6.8. NAT правила 80
6.9. IKE CFG правила 80
6.10. Серверные правила 81
6.11. Домены 81
6.12. Центры Сертификации 82
6.13. Действия 83
6.14. Настройки IKE 83
6.15. Сетевые Сервисы 84
6.16. Расписания 84
6.17. Монитор 85
6.18. Журнал и SysLog-журнал 85
6.19. Журнал исполнения 87
6.20. Валидность сертификатов 87
6.21. Дескрипторы агентов 88
6.22. Дескрипторы серверов 89
7. Создание Глобальной Политики Безопасности в *ЦУП-Консоль* **91**
7.1. Объекты Политики 91
7.1.1. Общие задачи 91
7.1.2. Объекты Шлюзов Безопасности 102
7.1.3. Объекты Хостов Безопасности 135
7.1.4. Объекты IP-хост 136
7.1.5. Объекты IP Диапазон 138
7.1.6. Объект Подсеть 139

7.1.7. Объекты Пользователь 140
7.1.8. Объект Группы 146
7.1.9. Объект Политики Internet Zone 148
7.1.10. Объекты Политики Any и Internet 148
7.2. Зоны 149
7.2.1. Создание Объектов Зон 149
7.2.2. Редактирование параметров зоны 150
7.2.3. Удаление зон 150
7.3. Правила 150
7.3.1. Создание Правил 150
7.3.2. Редактирование Правил 152
7.3.3. Удаление Правил 152
7.3.4. Создание иерархии Правил 153
7.3.5. Выключение и включение Правил 154
7.3.6. Скрытие Правил 154
7.3.7. Трассировка Правил 155
7.3.8. Особенности создания Правил, где участвуют Пользователи 155
7.3.9. Фильтрация в окне *Таблица правил* 156
7.3.10. Расписания Правил 156
7.4. Домены 158
7.4.1. Операции с доменами 158
7.4.2. Топология доменов 159
7.4.3. Определение Объектов Политики в домен 160
7.4.4. Учетные записи доменов 162
7.5. Настройки IKE 164
7.5.1. Объект первой фазы 164
7.5.2. Объекты IKE-Предложение 166
7.6. Действия 167
7.6.1. Создание Действий 168
7.6.2. Создание IPsec-Предложения 170
7.6.3. Редактирование Действий и IPsec-Предложений 171
7.6.4. Удаление Объектов действий 171
7.7. Сетевые сервисы 171
7.7.1. Иконки сетевых сервисов 172
7.7.2. Создание сетевых сервисов TCP 172
7.7.3. Создание Объектов сетевых сервисов UDP 173
7.7.4. Создание Объектов сетевых сервисов ICMP 174
7.7.5. Создание групп сетевых сервисов 174
7.7.6. Редактирование сетевых сервисов 174
7.7.7. Процедуры межсетевых экранов 175
7.8. Определяемые пользователем ЛПБ 176
7.8.1. Создание и редактирование Объектов определяемой пользователем ЛПБ 177
7.9. Серверы 177
7.9.1. Общие принципы создания Объектов в окне *Серверы* 179
7.9.2. Серверы-Прогрузчики 180
7.9.3. Прокси-Серверы 186
7.9.4. Прочие Серверы 196
7.10. Объекты УЦ (Certificate Authority) 202
7.10.1. Основные сведения 203
7.10.2. Дополнительные сведения 204
7.11. Мониторинг активации ГПБ 204
7.11.1. Фильтрация в окне *Монитор* 205

7.11.2. Меню *Просмотр* в окне *Монитор* 205
7.11.3. Обновление статуса мониторинга 205
7.12. Просмотр журналов регистрации Log и Syslog 206
7.12.1. Работа с журналами регистрации 206
7.12.2. Фильтрация результатов в журнале регистрации (Log) 207
7.12.3. Фильтрация результатов в журнале Syslog 208
7.12.4. Правила фильтрации в журнале Syslog 209
7.12.5. Мониторинг сообщений в журнале событий 209
7.12.6. Просроченные сертификаты 214
7.13. Дескрипторы Агентов 214
7.13.1. Добавление дескриптора Агента 214
7.13.2. Удаление дескриптора Агента 214
7.13.3. Просмотр дескриптора Агента 215
7.14. Дескрипторы Серверов 215
7.14.1. Добавление дескриптора Сервера 215
7.14.2. Удаление дескриптора Сервера 215
7.14.3. Просмотр дескриптора Сервера 215
8. Работа с Проектами и Глобальными Политиками Безопасности 216
8.1. Работа с проектами 216
8.1.1. Открытие проекта 216
8.1.2. Сохранение проекта 217
8.1.3. Перезагрузка проектов из базы данных 217
8.2. Трансляция ГПБ в ЛПБ 217
8.2.1. Просмотр и редактирование ЛПБ 218
8.3. Экспортирование ЛПБ 220
8.3.1. Экспортирование полных ЛПБ для *Агента* 220
8.4. Активация ЛПБ на *Агентах* 220
8.4.1. *Агенты* 221
8.4.2. Cisco и *Агенты* Microsoft 221
8.4.3. Сценарии Активации 221
8.4.4. Контроль статуса *Агента* 222
9. Другие функции *ЦУП* 224
9.1. Работа с заказными криптоалгоритмами 224
9.2. Использование удаленной *ЦУП-Консоль* 225
9.2.1. Конфигурирование локальной *ЦУП-Консоль* 225
9.2.2. Конфигурирование хоста удаленной *Консоли* 226
9.2.3. Запуск удаленной *Консоли* 228
9.2.4. Настройка других параметров системы 229
10. Работа со средством конфигурирования *ЦУП* 230
10.1. Управление базой данных 230
10.1.1. Создание новой базы данных 230
10.1.2. Удаление базы данных 230
10.1.3. Соединение с базой данных 231
10.2. Управление Лицензией 231
11. Приложение 1. Меры безопасности при использовании *ЦУП* 232
11.1. Краткий обзор проблем безопасности в *ЦУП* 232
11.1.1. Безопасность базы данных *ЦУП* 232
11.1.2. Безопасность Сертификатов и ключей 233
11.1.3. Безопасность управления сетевыми соединениями 233
11.1.4. Защита данных ЛПБ 233
11.2. Рекомендации по Политике Безопасности *ЦУП* 233

11.2.1. Общие замечания 233
11.2.2. Рекомендации для обеспечения безопасности *ЦУП* платформы 234
12. Приложение 2. Настройка сервера обновлений 237
12.1. Создание сервера обновлений 237
12.1.1. Настройка встроенного сервера обновления 237
12.1.2. Настройка автоматического обновления *Агентов* в *ЦУП-Консоль* 241
12.1.3. Настройка обновления на *Агент* 241
13. Приложение 3. Пример конфигурирования *ЦУП* 242
13.1. *ЦУП* и два *ЗАСТАВА-Клиент* 242
13.1.1. Цель 242
13.1.2. Описание сертификатов 242
13.1.3. Подготовка к установке 243
13.1.4. Установка пакета программ *ЦУП* 243
13.1.5. Установка *ЗАСТАВА-Клиент* 245
13.1.6. Конфигурирование *ЗАСТАВА-Офис* 245
13.1.7. Создание ГПБ в *ЦУП-Консоль* 246
13.1.8. Конфигурирование *ЗАСТАВА-Клиент* 251
13.1.9. Активизация ГПБ 253
14. Приложение 4. *ЦУП* файлы инициализации 254
14.1. Файл TPNServer.ini 254
14.1.1. Опции транслятора 254
14.1.2. Опции Cisco IOS 255
14.1.3. Опции Cisco PIX 255
14.1.4. Другие параметры 256
14.1.5. Параметры сервера приложений секция [Appsrv] 257
14.2. Файл distributor.ini 257
14.2.1. Секция [GlobalSettings] 258
14.2.2. Секция [ConfFiles] 258
15. Приложение 5. Сетевые сервисы и Группы сетевых сервисов по умолчанию 259
15.1. Сетевые сервисы 259
15.2. Группы сетевых сервисов 261
16. Приложение 6. Глоссарий Протоколов 262
17. Приложение 7. ICMP-коды 272
18. Приложение 8. Утилит командной строки TPNCLI 274
19. Устранение неисправностей 278
20. Перечень сокращений 280
Перечень ссылочных документов 283
Лист регистрации изменений 284

1. Введение

1.1. О программе ЗАСТАВА-Управление

Этот документ описывает функциональные возможности, особенности конфигурирования и применения одного из компонент ПК «VPN/FW «ЗАСТАВА», версия 6, а именно, МКЕЮ.00434-01 «ЗАСТАВА-Офис», версия 6 (далее - *ЗАСТАВА-Офис* или *Агент*) для системного программиста и персонала, обеспечивающего эксплуатацию *ЗАСТАВА-Управление* (далее - администратор).

1.1.1. Назначение

Компонент МКЕЮ.00436-01 «ЗАСТАВА-Управление», версия 6, входящий в программный комплекс (ПК) МКЕЮ.00433-01 «VPN/FW «ЗАСТАВА», версия 6 (далее - ПК «VPN/FW «ЗАСТАВА»), выполняет функции Центра управления политиками безопасности (далее – *ЦУП*) и представляет собой программу для унифицированного управления сетевой безопасностью в гетерогенных средах. Использование *ЦУП* позволяет централизованно создавать, распределять и активировать политику сетевой безопасности в информационной (информационно-телекоммуникационной) сети, содержащей *Агенты* от различных производителей, в том числе компоненты ПК «VPN/FW «ЗАСТАВА», версия 6: МКЕЮ.00435-01 «ЗАСТАВА-Клиент», версия 6 (далее – *ЗАСТАВА-Клиент*), МКЕЮ.00434-01 «ЗАСТАВА-Офис», версия 6 (далее – *ЗАСТАВА-Офис*) (*ЗАСТАВА-Клиент, ЗАСТАВА-Офис* - обычно употребляется собирательный термин *Агенты*). *ЦУП* обеспечивает централизованный контроль доступа в защищенных сетях путем определения Политики Безопасности для IP-фильтрации (включая конфигурирование межсетевых экранов (МЭ) с контролем состояний протоколов) и для обработки IPsec-трафика на управляемых *Агентах*. Защита сетевых соединений управляется через IPsec-Политики для *Агентов*. *ЦУП* также определяет тип аутентификации пользователей и удаленных хостов в рамках стандартных опций IKE: с использованием цифровых сертификатовили предварительно распределенных ключей.

ЦУП унифицирует управление сетевой безопасностью в «много-вендорных» сетях путем одновременного и целостного конфигурирования, как МЭ, так и шлюзов безопасности (VPN-шлюзов) от таких известных производителей, как, Cisco Systems™ и Microsoft™. Таким образом, *ЦУП* дополняет функции управления сетями, обеспеченные централизованными платформами управления Cisco, и позволяет пользователю определить (и заменить) только те части конфигурации *Агента*, которые имеют отношение к сервисам, управляемым *ЦУП*. Контроль доступа, аутентификация пользователя/узла и шифрование трафика не затрагивают частей конфигурации *Агента*, относящихся к другим сервисам - роутинг, IDS, профилирование

трафика и т.д. Они определяются независимо и согласованно (без конфликтов) вне *ЦУП*, на соответствующих продуктах управления Cisco: Cisco Secure Policy Manager. *ЦУП* создает и централизованно управляет Локальными Политиками Безопасности (ЛПБ) *Агентов* в продуктах *ЗАСТАВА,* встроенных *Агентах* Microsoft XP/2003 IPsec Agent, маршрутизаторах Cisco, МЭ Cisco PIX Firewall в рамках общей корпоративной Глобальной Политики Безопасности (ГПБ). ГПБ и ЛПБ хранятся в базе данных (БД) *ЦУП* и отображаются и управляются через *ЦУП-Консоль.*

1.1.2. Область применения

ЗАСТАВА-Управление применяется для управления *Агентами* в локальных, корпоративных и глобальных сетях, где в качестве протокола сетевого уровня используется протокол IP.

ЗАСТАВА-Управление, версия 6 предназначена для работы на компьютерах со следующими операционными системами (ОС):

- Для серверной части компонента «ЗАСТАВА–Управление»
  - ОС Windows Server 2008 платформа x64, Windows Server 2008 R2, платформа x64, Windows Server 2012, платформа x64; Windows Server 2012 R2, платформа x64.
- Для клиентской части компонента «ЗАСТАВА–Управление»
  - ОС Windows XP SP3, ОС Windows 7, ОС Windows 8, ОС Windows 10 платформа x64;

Компоненты *ЦУП* (*ЦУП-Консоль*, *ЦУП-Сервер, БД ЦУП*) могут быть установлены как на одном компьютере, так и на разных компьютерах. Допускается установка клиентской части компонента «ЗАСТАВА–Управление» на ОС для серверной части компонента «ЗАСТАВА–Управление». В любом случае, для каждого компонента *ЦУП* используемая ОС должна иметь установленную и активированную поддержку сети и стека TCP/IP.

1.1.3. Характеристики

ЦУП позволяет Администратору Безопасности:

- Создавать и редактировать ГПБ;
- Преобразовывать ГПБ в ЛПБ для конкретных *Агентов*;
- Доставлять ЛПБ по защищенному каналу и активировать на *Агент* (по запросу или по команде с *ЦУП*) через протокол распределения политики (Policy Management Protocol - PMP), используя защищенное соединение ISAKMP/IKE SA;

- Отсылать ЛПБ маршрутизаторам и МЭ Cisco и *Агентам* Microsoft IPsec в текстовом формате через зашифрованный туннель;
- Организовывать взаимодействие и, при необходимости, защищать трафик между *Агентами* и внешними системами - серверами регистрации, системами сетевого управления и средствами безопасности третьих производителей на основе протоколов IPsec;
- Использовать специальные носители информации (PKCS#11-совместимые токены) для того, чтобы хранить критическую информацию пользователя;
- Вести файл журнала регистрации и контролировать события системы через этот файл;
- Собирать Syslog-сообщения от управляемых *Агентов*;
- Хранить ГПБ и ЛПБ для *Агентов* (т.е. наборы Объектов Политики и Правила управления их взаимодействиями) в БД *ЦУП*;
- Экспортировать/импортировать Проекты ГПБ из/в XML-файлов;
- Управлять маршрутизаторами Cisco, МЭ Cisco PIX в роли Шлюзов Безопасности;
- Управлять встроенными в ОС Windows *Агентами* Microsoft IPsec Agents в роли Хостов Безопасности и Пользователей;
- Управлять IKE CFG и расширенной аутентификацией на Шлюзах Безопасности;
- Помещать *ЦУП* и управляемые *Агенты* за NAT-устройства; определять Правила NAT, чтобы ЦУП принимал их в расчет при вычислении политик безопасности на уровне *Агентов*. Для некоторых *Агентов* возможно активное управление NAT-конфигурацией (путем включения команд NAT в ЛПБ *Агента*);
- Управлять сервисами Application Proxy (HTTP, FTP и т.д.) в *Агентах*;
- Быстро выполнять начальное конфигурирование *Агентов*, загружая начальные инсталляционные пакеты от *ЦУП* через веб-протокол (HTTP/HTTPS);
- Управлять политикой автоматического обновления для *Агентов*;
- Управление качеством обслуживания (QoS): осуществляется путем модификации поля DiffServ при туннелировании IP-пакетов (поддерживается *Агентами*, начиная с версии 5.0). Данная функциональность полезна для протоколов, чувствительных к задержкам (VoIP и т.п.).

1.1.4. Поддерживаемые протоколы и технологии

В *ЦУП* применяются различные концепции, протоколы технологии, используемые в средах сетевой безопасности, такие как IPsec, IKE, PKI, RADIUS и т.д. Эти концепции,

протоколы и технологии подробно описаны в соответствующих RFC (Request For Comments). Ниже приводится список документов, которые являются отправной точкой для понимания концепций сетевой безопасности:

Общие стандарты группы IPsec

RFC 2401	Security Architecture for the Internet Protocol	http://www.ietf.org/rfc/rfc2401.txt
RFC 2411	IP Security Document Roadmap	http://www.ietf.org/rfc/rfc2411.txt

IPsec: протоколы ESP и AH

RFC 2402	IP Authentication Header (AH)	http://www.ietf.org/rfc/rfc2402.txt
RFC 2406	IP Encapsulating Security Payload (ESP)	http://www.ietf.org/rfc/rfc2406.txt

IPsec: обмен ключами

RFC 2408	Internet Security Association and Key Management Protocol (ISAKMP)	http://www.ietf.org/rfc/rfc2408.txt
RFC 2409	Internet Key Exchange	http://www.ietf.org/rfc/rfc2409.txt
RFC 3173	IP Payload Compression Protocol (IPComp)	http://www.ietf.org/rfc/rfc3173.txt

PKI

RFC 2459	Internet X.509 Public Key Infrastructure Certificate and CRL Profile	http://www.ietf.org/rfc/rfc2459.txt

Другие протоколы

RFC 0792	Internet Control Message Protocol (ICMP)	http://www.ietf.org/rfc/rfc792.txt
RFC 1777	Lightweight Directory Access Protocol (LDAP)	http://www.ietf.org/rfc/rfc1777.txt
RFC 1155	Structure and Identification of Management Information for TCP/IP-based Internets	http://www.ietf.org/rfc/rfc1155.txt
RFC 1157	Simple Network Management Protocol (SNMP)	http://www.ietf.org/rfc/rfc1157.txt
RFC 2138	Remote Authentication Dial-in User Service (RADIUS)	http://www.ietf.org/rfc/rfc2138.txt

Термины и определения

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

1.2. Об этом документе

Этот документ описывает функциональные возможности *ЦУП* версии 6.

1.2.1. Как пользоваться этим документом

В зависимости от того, какую информацию Вы хотите найти в данном документе, можно для начала:

- Научиться устанавливать и настраивать *ЦУП*, для этого перейти к разделу 2 ПОДГОТОВКА К ИСПОЛЬЗОВАНИЮ *ЦУП*.
- Получить общие теоретические и практические сведения о том, как обеспечить Безопасность Вашей сети путем конфигурирования ГПБ в *ЦУП*, включая стратегию вне программирования ГПБ, для этого перейти к разделу 4 ОБЗОР КОНФИГУРАЦИИ *ЦУП*.
- Узнать о структуре главного окна *ЦУП-Консоль* и научиться перемещаться по структуре Объекта, для этого перейти к разделу 5 ОБЗОР *ЦУП-КОНСОЛЬ* .
- Узнать о структуре четырех областей окна в главном окне *ЦУП-Консоль*, для этого перейти к разделу 6 ВЛОЖЕННЫЕ ОКНА *ЦУП-КОНСОЛЬ*.
- Ознакомиться с инструкциями по установке, удалению и управлению Объектами в *ЦУП-Консоль*, чтобы создать ГПБ, для этого перейти к разделу 7 СОЗДАНИЕ ГЛОБАЛЬНОЙ ПОЛИТИКИ БЕЗОПАСНОСТИ В ЦУП.
- Узнать определения и структуры Проектов и ГПБ, в том виде, в котором они используются в *ЦУП*, а также принципы работы с ними, для этого перейти к разделу 8 РАБОТА С ПРОЕКТАМИ И ГЛОБАЛЬНЫМИ ПОЛИТИКАМИ БЕЗОПАСНОСТИ.
- Ознакомиться с инструкциями по работе с криптоалгоритмами и конфигурированию *ЦУП-Консоль*, для этого перейти к разделу 9 ДРУГИЕ ФУНКЦИИ *ЦУП*.
- Ознакомиться с инструкциями по пользованию Утилиты Конфигурирования *ЦУП* (SecureManage Configuration Tool) и научиться управлять лицензией *ЦУП* и БД *ЦУП*, с которыми *ЦУП* будет работать, для этого перейти к разделу 10 РАБОТА СО СРЕДСТВОМ КОНФИГУРИРОВАНИЯ *ЦУП*.
- Рассмотреть пошаговый пример конфигурирования *ЦУП* для работы с *ЗАСТАВА-Клиент*, для этого перейти к приложению (см. Приложение 2. Настройка сервера обновлений).

1.2.2. Типографские соглашения

В данном документе используются следующие типографские соглашения:

Полужирный шрифт	Полужирный шрифт используется для выделения названий меню, вкладок, кнопок, полей, Объектов и строк контекстного меню, а также для визуального выделения.
Курсив	Курсив используется для выделения названий программ, программных окон, всплывающих окон, строк меню, параметров Объекта и атрибутов, а также для указания данных, которые нужно ввести в поле, а также для визуального выделения.
«Кавычки»	Кавычки используются для указания строки из списка в данном поле (т. е. строку из предопределенного списка в окне).
МАЛЕНЬКИЕ ПРОПИСНЫЕ	Маленькие прописные буквы используются в названиях документов (стандартов, монографий, бумаг, технической документации, документации пользователя для программного обеспечения, систем интерактивной справки и т. д.) и разделов документов.
`Непропорциональный шрифт`	Непропорциональный шрифт используется в ссылках на папки системы и директории, меню *Start*, названиях файлов и путей и командах DOS/shell.
<угловые скобки>	В угловые скобки заключают названия клавиш на клавиатуре.

2. Подготовка к использованию *ЦУП*

2.1. Системные требования

Программно-аппаратное обеспечение компьютера, на котором устанавливается *ЗАСТАВА-Управление*, должно отвечать следующим *минимальным* требованиям.

2.1.1. *ЦУП-Консоль*

Программно-аппаратное обеспечение компьютера, на котором устанавливается *ЦУП-Консоль ЗАСТАВА-Управление*, должно отвечать следующим *минимальным* требованиям (может устанавливаться на отдельном компьютере или вместе с другими компонентами *ЦУП*):

- 64-разрядный процессор 1400 МГц или выше;
- оперативная память – не менее 512 Мбайт;
- ОС Windows XP SP3, ОС Windows 7, ОС Windows 8 платформа x64;
- поддержка сети (TCP/IP) должна быть установлена и активирована;
- разрешающая способность дисплея – не менее 1024x768 (рекомендуется 1280x1024 и более).

2.1.2. *ЦУП-Сервер*

Программно-аппаратное обеспечение компьютера, на котором устанавливается *ЦУП-Сервер ЗАСТАВА-Управление*, должно отвечать следующим *минимальным* требованиям (может устанавливаться на отдельном компьютере или вместе с другими компонентами *ЦУП*):

- 64-разрядный процессор1400 МГц или выше;
- оперативная память – не менее 512 Мбайт;
- ОС Windows Server 2008 платформа x64, Windows Server 2008 R2, платформа x64, Windows Server 2012, платформа x64; Windows Server 2012 R2, платформа x64;
- поддержка сети (TCP/IP) должна быть установлена и активирована.

Допускается установка клиентской части компонента «ЗАСТАВА–Управление» на ОС для серверной части компонента «ЗАСТАВА–Управление».

2.2. Поддерживаемые версии управляемых *Агентов*

ЦУП может управлять удалёнными маршрутизаторами, МЭ, шлюзами безопасности и VPN-клиентами различных производителей. Ниже приведен список версии устройств/программ, которые были полностью проверены на совместимость с *ЦУП ЗАСТАВА-Управление*:

- маршрутизаторы Cisco IOS routers с версией IOS 12.3;
- МЭ Cisco PIX Firewalls версий 6.3;
- *Агенты* Microsoft IPsec Agent, встроенные в ОС Microsoft Windows XP, 2003;
- *Агенты* (*ЗАСТАВА-Клиент, ЗАСТАВА-Офис*) версий 5.2 и выше.

Примечание. Другие типы и версии устройств/программ могут также корректно работать с *ЦУП*, однако, это не гарантируется, поэтому рекомендуется предварительно провести полномасштабное тестирование в лабораторных условиях.

2.3. Инсталляция *ЦУП*

2.3.1. Подготовка

ЦУП поставляется вместе с *ЗАСТАВА-Офис* (который защищает компьютер *ЦУП* и распределяет политики безопасности (ЛПБ) *Агентам*), MS SQL Server 2008 R2 Express Edition и набором компонентов для поддержки Java-приложений.

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

МКЕЮ.00433-01 программный комплекс защиты корпоративных вычислительных ресурсов на сетевом уровне с использованием технологий VPN и распределенного межсетевого экранирования на основе интернет-протоколов семейства IPsec/IKE «VPN/FW «ЗАСТАВА», версия 6» «VPN/FW «ЗАСТАВА», версия 6 и его компоненты в варианте VPN (СКЗИ + МЭ), обладающие криптографическим функционалом, являются, согласно действующим нормативным правовым актам Российской Федерации, средством криптографической защиты информации (СКЗИ). Использование *ПК «VPN/FW «ЗАСТАВА», версия 6* и его компонентов как СКЗИ должно осуществляться в соответствии с документом МКЕЮ.00433-01 90 01 «Программный комплекс защиты корпоративных вычислительных ресурсов на сетевом уровне с использованием технологий VPN и распределенного межсетевого экранирования на основе интернет-протоколов семейства IPsec/IKE «VPN/FW «ЗАСТАВА», версия 6» («ПК «VPN/FW «ЗАСТАВА», версия 6»). Правила пользования».

В состав ПК в варианте VPN (СКЗИ + МЭ) входит СКЗИ «КриптоПро CSP», производства ООО «КРИПТО-ПРО» (г. Москва). В зависимости от комплектации и

исполнения в состав «ПК «VPN/FW «ЗАСТАВА», версия 6» могут входить следующие СКЗИ:

- ЖТЯИ.00050-03 «КриптоПро CSP», версия 3.6.1[1], исполнение 1 или исполнения 2;
- ЖТЯИ.00083-01 «КриптоПро CSP», версия 3.9 , исполнение 1 или исполнение 2;
- ЖТЯИ.00087-01 «КриптоПро CSP», версия 4.0КС1;
- ЖТЯИ.00088-01 «КриптоПро CSP», версия 4.0КС2.

	Чтобы инсталлировать и деинсталлировать *ЦУП*, Вы должны иметь привилегии *администратора* ОС.
	Длина пароля администратора ОС должна быть не меньше шести буквенно-цифровых символов
	Вы должны отключить все антивирусное программное обеспечение (ПО) до начала установки *ЦУП*. Не забудьте активировать антивирусное ПО, как только установка *ЦУП* будет завершена!
	БД MS SQL Server 2008 R2 Express Edition используется только для тестовых проектов, а также для проектов, с числом объектов безопасности менее 100, в остальных случаях рекомендуется использовать внешнюю БД Microsoft SQL Server 2008 или Postgre SQL версии 9.x.
	Если в качестве Сервера базы данных *ЦУП* Вы будете использовать *уже существующий* MS SQL Server или Postgre SQL, то перед инсталляцией *ЦУП* надо убедиться в том, что Вы знаете логин и пароль администратора SQL-сервера и что он должным образом сконфигурирован.
	СКЗИ «КриптоПро CSP» версии 3.6.1, «КриптоПро CSP» версии 3.9, «КриптоПро CSP» версии 4.0 должно быть установлено с поддержкой уровня ядра для этого при установке приложения необходимо выбрать тип установки Custom и установить модуль Kernel mode CSP.

2.3.2. Запуск инсталляции

Запуск инсталляции должен производиться следующим образом:

1) Вставить диск с дистрибутивом в привод CD-ROM и запустить файл `ZASTAVA.exe`. Начнется процесс инсталляции.
2) Подтвердить Ваше принятие лицензионного соглашения, нажав соответствующий переключатель, и нажать кнопку **Далее**.
3) Выбрать папку, куда будет установлено приложение.
4) Выбрать модули *ЦУП*, которые будут установлены (по умолчанию устанавливаются все модули) (см. Рисунок 1).

[1] При условии соблюдения ограничений документа ИЗВЕЩЕНИЕ ОБ ИЗМЕНЕНИЯХ ЖТЯИ.00050-02.1-2015

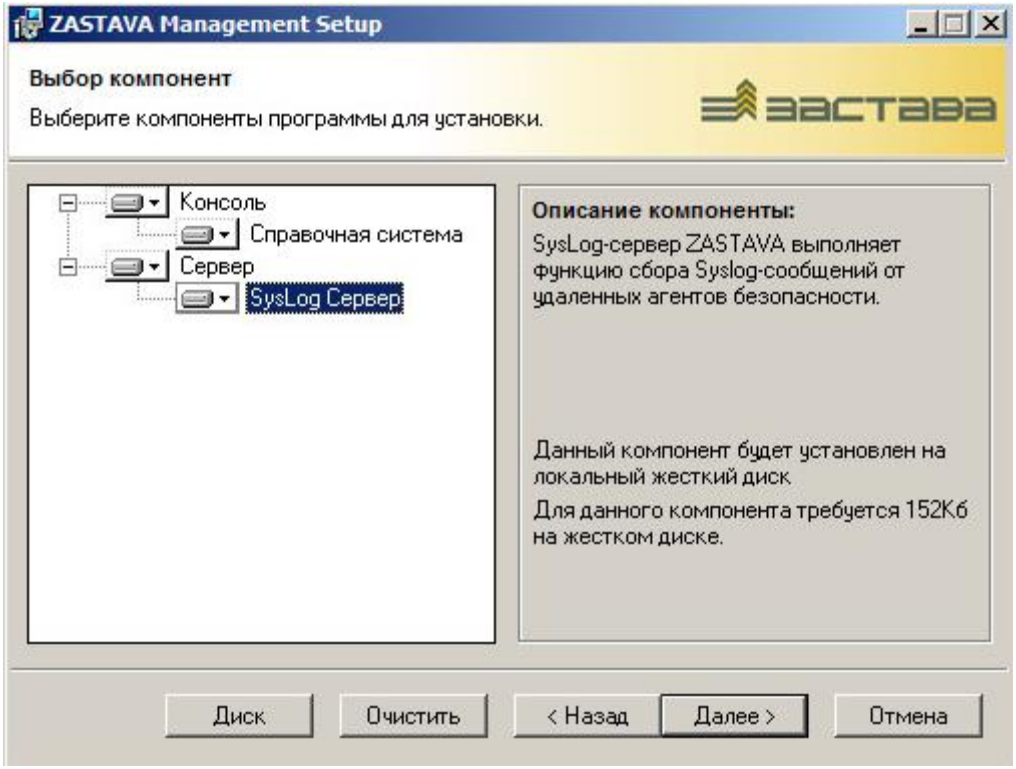

Рисунок 1 – Выбор устанавливаемых компонентов *ЦУП*

5) Если на Вашем компьютере не установлен сервер баз данных MS SQL, то появится окно с предложением установки Microsoft SQL Server 2008 R2 Express Edition. При необходимости – снять отметку с соответствующего пункта.

6) Ознакомиться со списком дополнительного ПО, необходимого для работы *ЦУП*. Обратите внимание, что, если такое ПО не установлено на Вашем компьютере, оно будет установлено автоматически, как часть инсталляции *ЦУП*. Нажать кнопку **Далее**.

7) После этого запустится процесс инсталляции необходимых продуктов. На все вопросы, которые могут появиться при инсталляции дополнительных продуктов, можно ответить по умолчанию.

8) В процессе установки MS SQL Server 2008 R2 на этапе конфигурирования пароля для аутентификации под учетной записью администратора (см. Рисунок 2) необходимо сгенерировать пароль, отвечающий следующим требованиям:

- не содержит всю или часть имени учетной записи пользователя;
- длиной более восьми знаков;
- содержит символы, по крайней мере, трёх следующих категорий:
  - заглавные буквы английского алфавита (от A до Z);
  - строчные буквы английского алфавита (от a до z);

– основные 10 цифр (0-9);
– небуквенные символы (например: !, #, %).

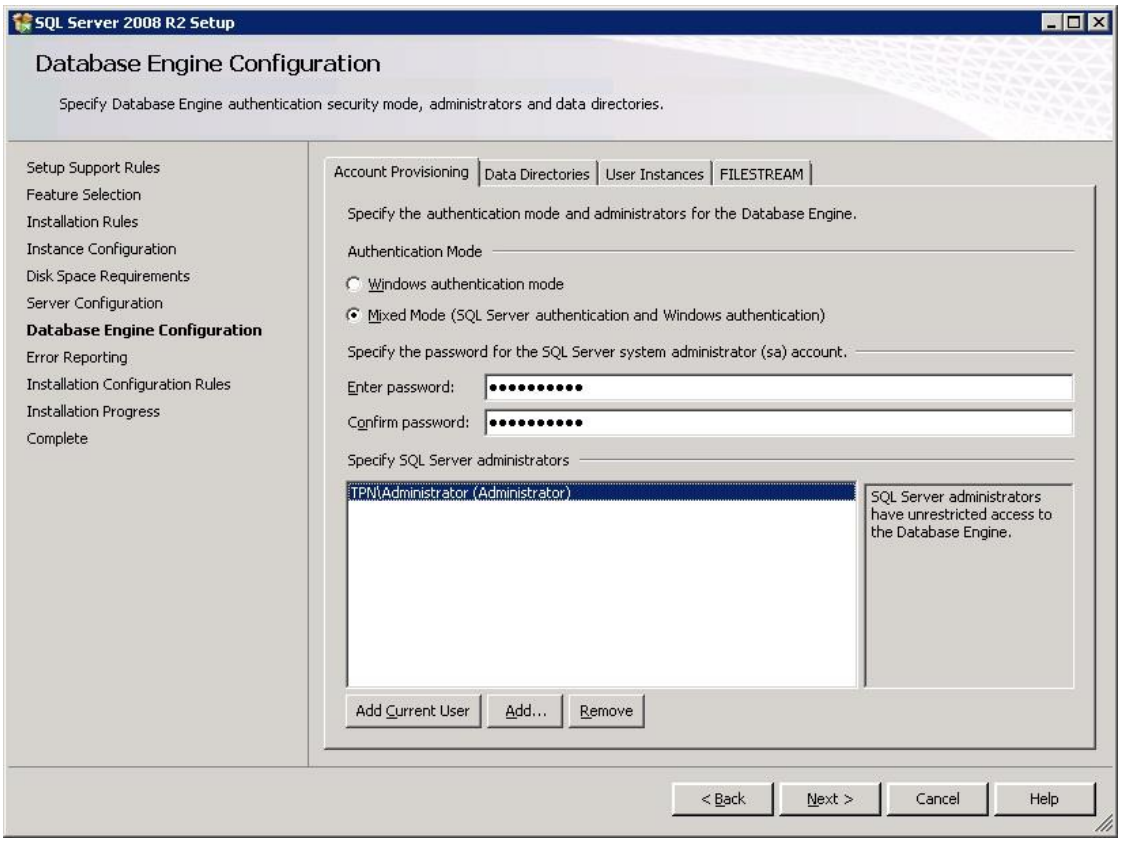

Рисунок 2 – Окно конфигурирования пароля учетной записи администратора БД

2.3.3. Продолжение инсталляции: создание БД *ЦУП*

2.3.3.1. Настройка MS SQL Server 2008 R2 Express Edition

Перед созданием БД *ЦУП* необходимо настроить MS SQL Server 2008 R2 Express Edition:

1) В меню *Пуск* выбрать **SQL Server Configuration Manager** (см. Рисунок 3).

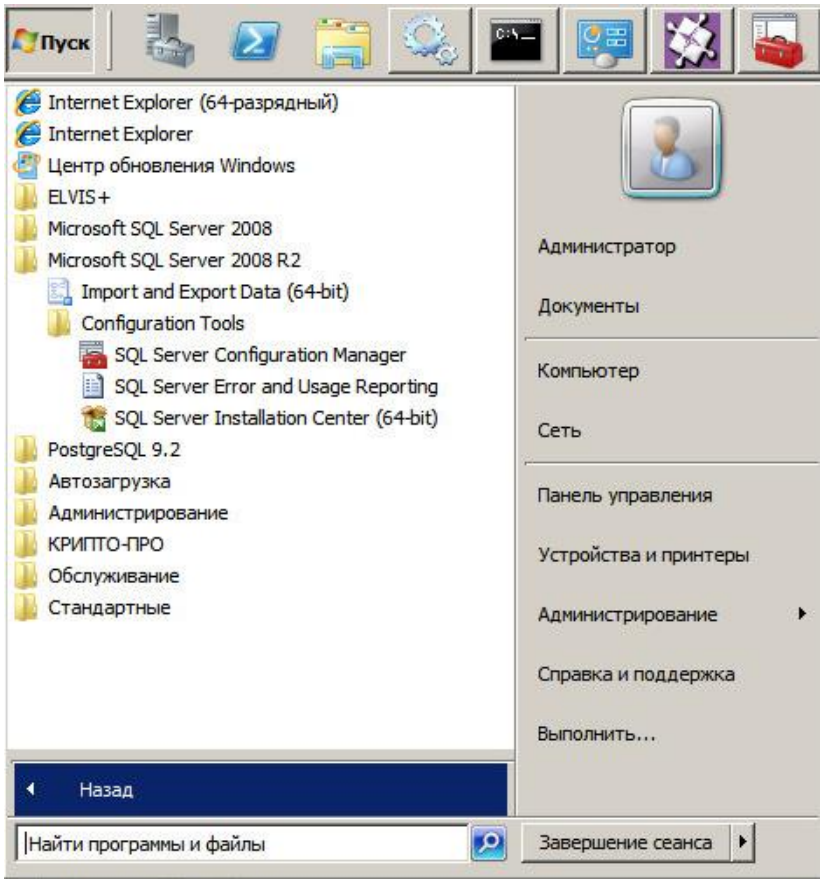

Рисунок 3 – Запуск SQL Server Configuration Manager

2) Раскрыть список *SQL Server Network Configuration*, выбрать **Protocols for SQLEXPRESS**, затем – **TCP/IP** (см. Рисунок 4).

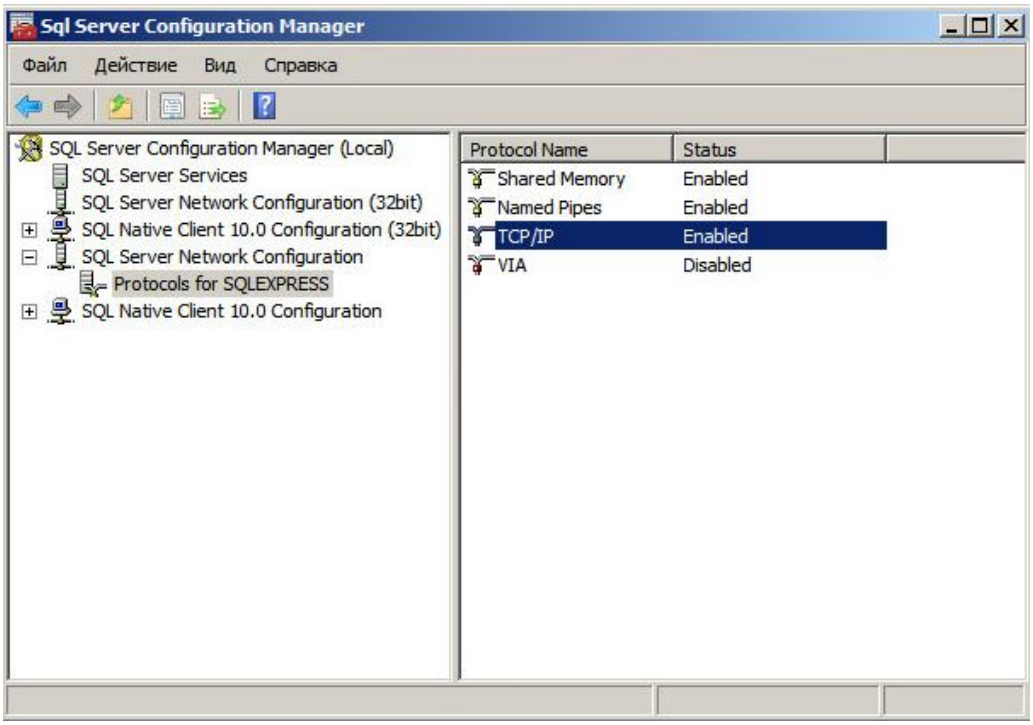

Рисунок 4 – Настройка TCP/IP при конфигурации MS SQL Server 2008 R2 Express Edition

3) Выбрать вкладку IP Addresses и в разделе IPALL в поле TCP Port задать значение 1433. Значение в поле TCP Dynamic Ports удалить (см. Рисунок 5).

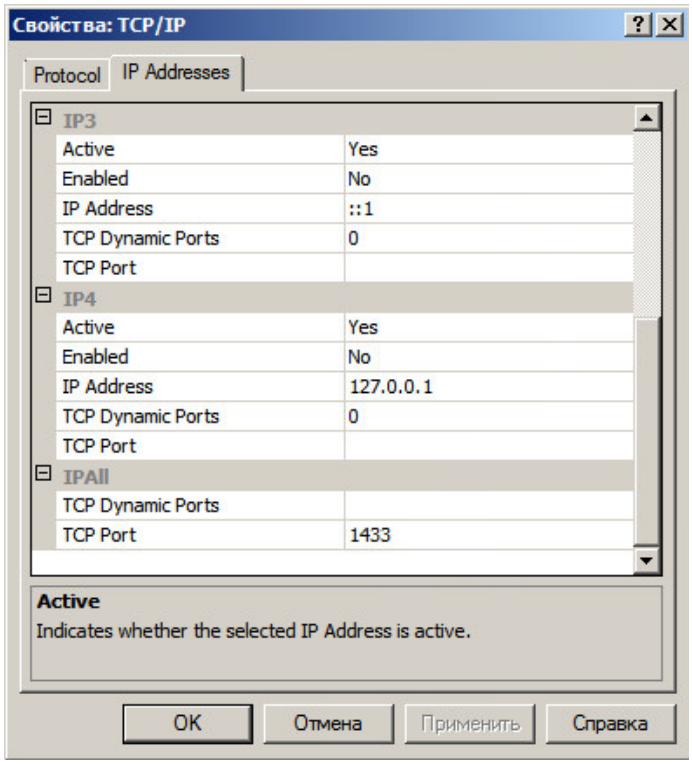

Рисунок 5 - Настройка TCP/IP при конфигурации MS SQL Server 2008 R2 Express Edition

2.3.3.2. Создание БД *ЦУП* MS SQL Server 2008 R2

Как только процесс установки необходимых продуктов завершится, будет автоматически запущена утилита конфигурирования *ЦУП* в режиме Мастера:

1) Появится окно с вопросом о выборе - создавать новую БД *ЦУП* или настроить соединение с существующей. В большинстве случаев необходимо создавать новую БД (см. Рисунок 6);

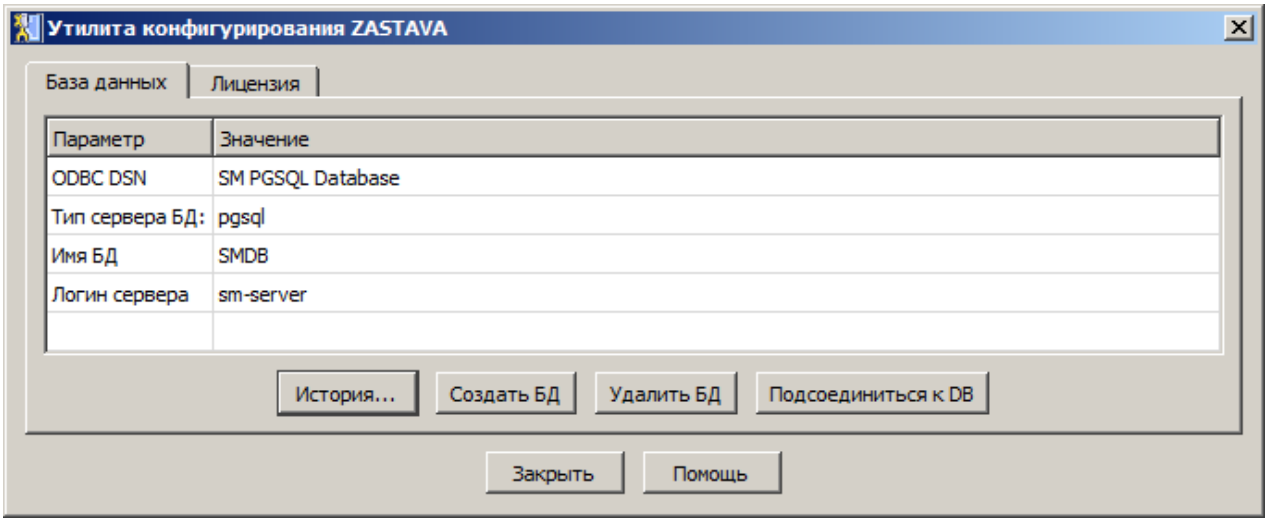

Рисунок 6 – Создание БД

2) В появившемся окне необходимо выбрать сервер БД и нажать кнопку **Далее** (см. Рисунок 7);

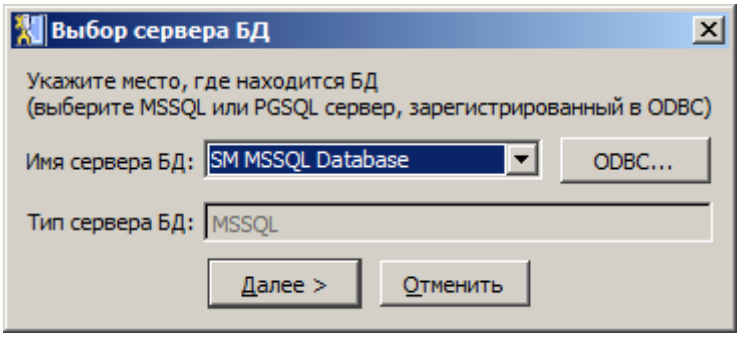

Рисунок 7 – Выбор сервера БД

Использовать существующую БД *ЦУП* можно только в том случае, если она была создана *этой же версией* продукта.

При попытке подключения к БД, неподходящей версии, инсталлятор предложит выбрать другую БД, создать новую БД или отменить инсталляцию.

Подробнее о подключении к существующей БД *ЦУП* см. подраздел 10.1.

При необходимости настройки сервера БД нужно выбрать его из списка и нажать кнопку **ODBC..**, в открывшемся окне произвести необходимые настройки.

3) Ввести логин и пароль администратора сервера БД, которые были заданы на этапе установки MS SQL 2008 (см. Рисунок 8). Нажать кнопку **ОК** (данная информация будет проверена на следующем этапе, при попытке создания БД).

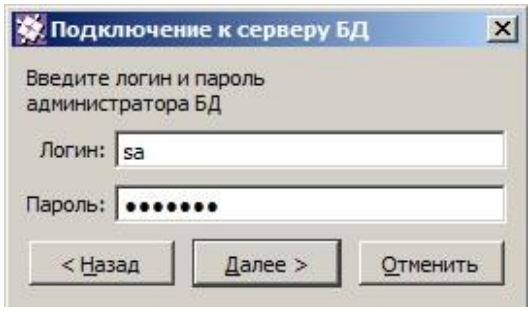

Рисунок 8 – Ввод логина и пароля администратора БД

4) Задать информацию для создания двух учетных записей – одной для *ЦУП-Сервер*, второй – для *ЦУП-Консоль* (см. Рисунок 9).

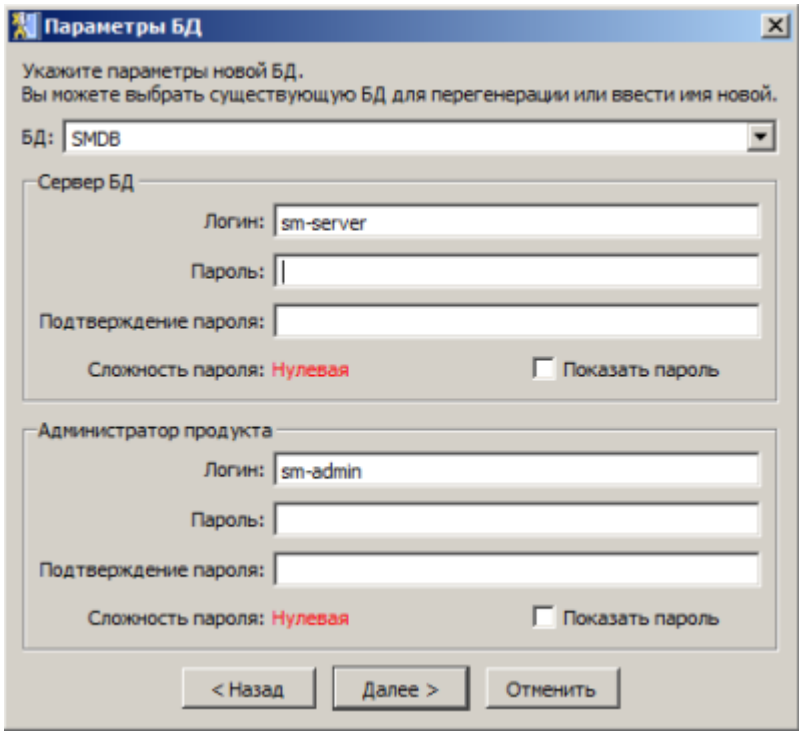

Рисунок 9 – Ввод параметров БД

2.3.3.3. Создание БД *ЦУП* Postgre SQL

Запустить утилиту конфигурирования *ЦУП* в режиме Мастера.

1) Появится окно с вопросом о выборе - создавать новую БД ЦУП или настроить соединение с существующей. В большинстве случаев необходимо создавать новую БД;

Использовать существующую БД *ЦУП* можно только в том случае, если она была создана *этой же версией* продукта.

При необходимости настройки сервера БД нужно выбрать его из списка и нажать кнопку **ODBC..**, в открывшемся окне произвести необходимые настройки.

Подробнее о подключении к существующей БД *ЦУП* см. подраздел 10.1.

2) В появившемся окне выбрать сервер БД и нажать кнопку далее (см. Рисунок 10);

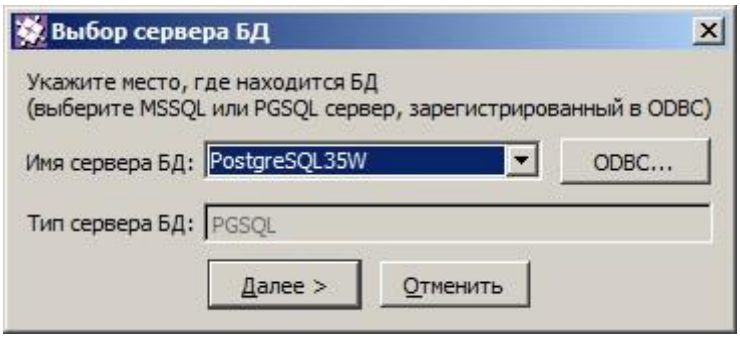

Рисунок 10 – Выбор сервера базы данных

3) Ввести логин и пароль администратора БД;

4) Задать информацию для создания двух учетных записей – одной для *ЦУП-Сервер*, второй – для *ЦУП-Консоль* (см. Рисунок 11).

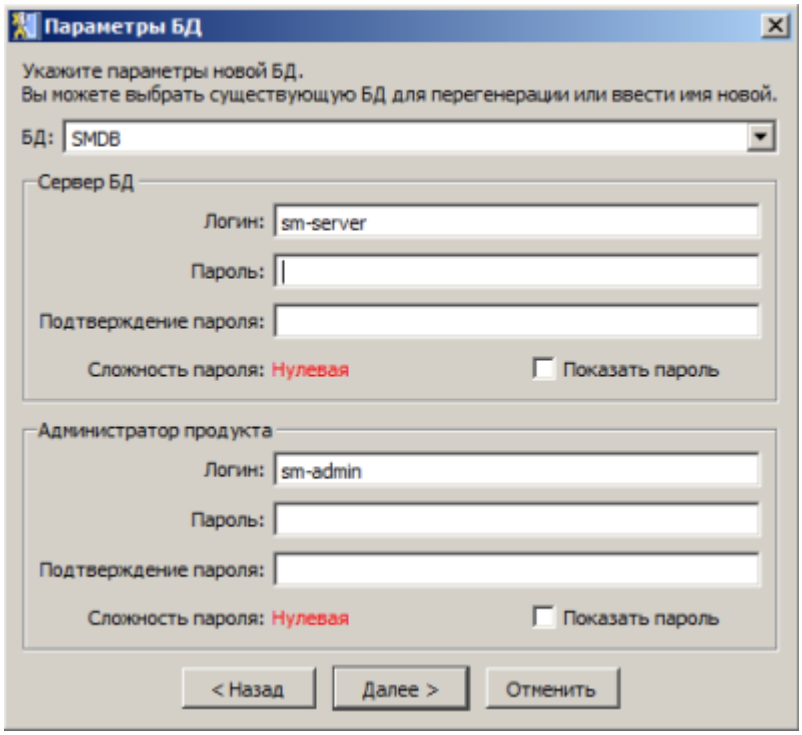

Рисунок 11 – Ввод параметров БД

2.3.4. Продолжение инсталляции: настройка *ЗАСТАВА-Офис*

На данном этапе Вам будет предложено сконфигурировать *ЗАСТАВА-Офис*, который был установлен вместе с *ЦУП*. Этот процесс включает в себя указание идентификатора локального сертификата, который будет использоваться в *ЦУП* (данное действие имеет смысл в том случае, если в *ЗАСТАВА-Офис* импортировано более одного локального сертификата).

Если у Вас в Хранилище сертификатов уже есть установленные сертификаты, то необходимо выбрать соответствующий для доступа к серверу политик (см. Рисунок 12), если установленных сертификатов нет, то список будет пустым. Добавить сертификаты можно будет позже вручную.

	Без конфигурирования *ЗАСТАВА-Офис* активация ГПБ в *ЦУП* будет невозможна.
	Более подробную информацию о конфигурировании *ЗАСТАВА-Офис*, о назначении сертификатов и о том, откуда их взять, можно прочитать в документе МКЕЮ.00434-01 32 01 «Программный комплекс защиты корпоративных вычислительных ресурсов на сетевом уровне с использованием технологий VPN и распределенного межсетевого экранирования на основе интернет-протоколов семейства IPsec/IKE «VPN/FW «ЗАСТАВА», версия 6» («ПК «VPN/FW «ЗАСТАВА», версия 6»). Компонент «ЗАСТАВА-Офис», версия 6. Руководство системного программиста».

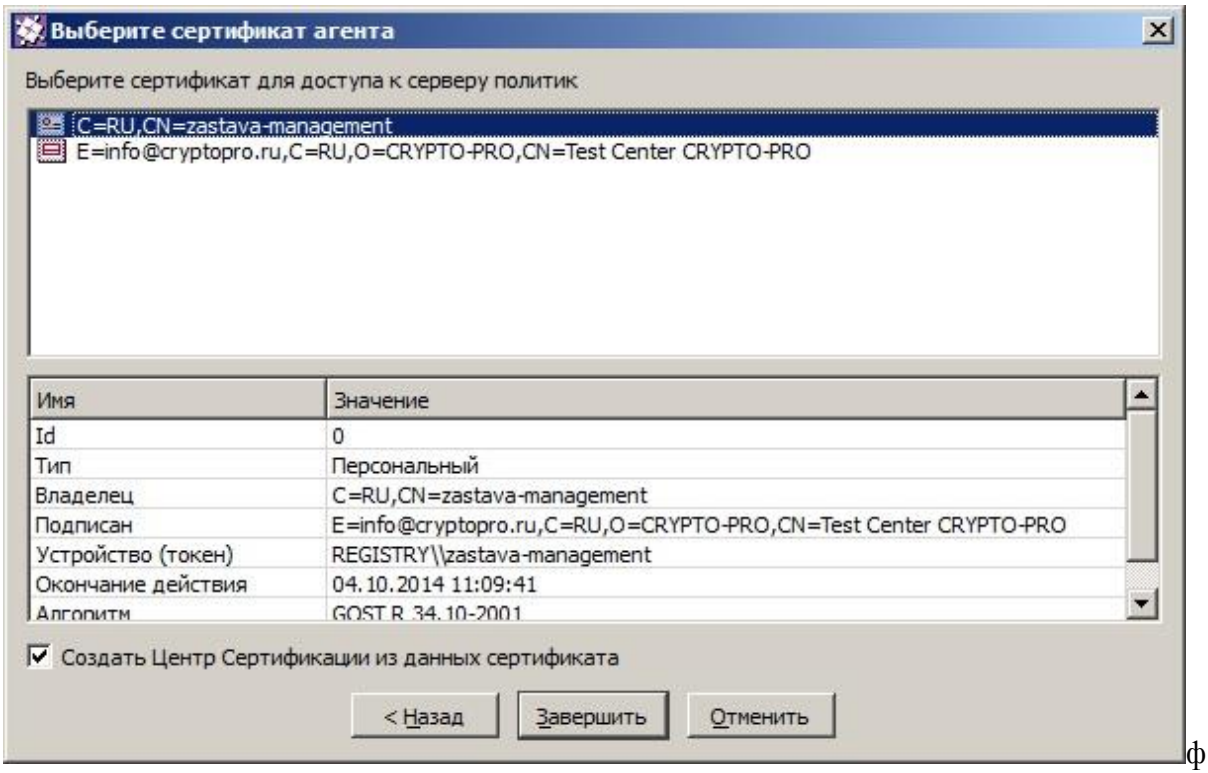

Рисунок 12 – Выбор сертификата *Агента*

2.3.5. Завершение инсталляции: ввод файла с лицензией

Импорт лицензии должен проводиться следующим образом:

1) После успешного создания БД *ЦУП* появится соответствующее информационное окно. Нажать кнопку **ОК**.
2) В окне *Лицензия* можно при помощи соответствующей кнопки **Загрузить** файл с лицензионной информацией. Лицензионные файлы выдаются фирмой-поставщиком. Для получения файла Вам может потребоваться идентификатор из поля ID хоста. Более подробную информацию можно найти в подразделе 10.2.
3) Нажать кнопку **Закрыть.**

2.4. Деинсталляция

Для удаления *ЗАСТАВА-Управление* Вашей системы надо закрыть все программные окна *ЗАСТАВА-Управление* и затем произвести деинсталляцию *ЗАСТАВА-Управление* (*ЦУП, ZASTAVAOffice,*), используя **Add/Remove Programs** в Панели Управления ОС Windows или запустив мастера установки *ЗАСТАВА-Управление*, который предложит Вам удалить уже установленную версию. Все компоненты *ЗАСТАВА-Управление* будут полностью удалены, как только компьютер будет перезагружен.

В некоторых случаях после деинсталляции в основной директории *ЗАСТАВА-Управление* могут остаться файлы, созданные пользователем в процессе работы (лог-файлы, сертификаты и т.п.). При необходимости, удалить эти файлы вручную.

3. Подготовка к использованию

3.1. Программная группа *ЦУП*

После успешной инсталляции создается программная группа ZASTAVA Management, содержащая программные модули (см. Рисунок 13).

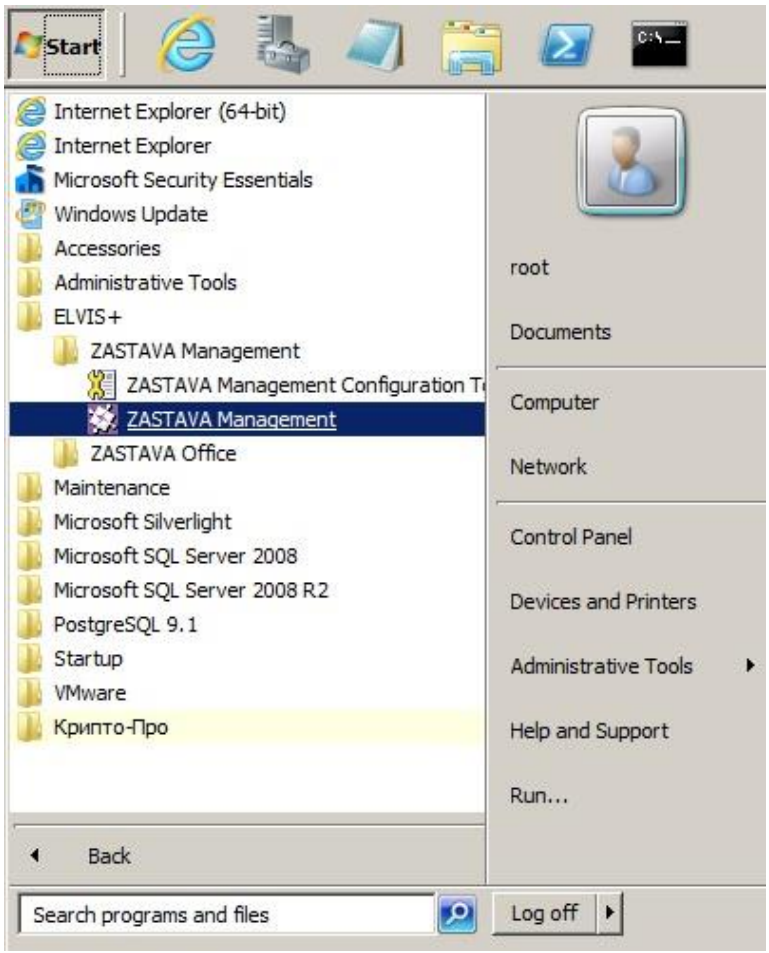

Рисунок 13 - Запуск ZASTAVA Management

ZASTAVA Management (*ЦУП-Консоль*) – основной программный модуль, предназначенный для создания и редактирования ГПБ.

SecureManage Configuration Tool (*Утилита конфигурирования ЦУП*) – модуль для конфигурирования БД *ЦУП* (влияет на *ЦУП-Сервер* и другие модули *ЦУП*).

3.2. Расположение файлов *ЦУП*

Основные файлы *ЦУП* (исполняемые модули, журнал протокола и проч.) располагаются в т.н. главной директории *ЦУП*: `C:\Programs Files\ELVIS+\ZASTAVA Management`.

3.3. Запуск *ЦУП-Консоль*

Запустить *ЦУП-Консоль* из меню *Start* (`Start\Programs\ELVIS+\ZASTAVA Management`) или двойным нажатием левой кнопкой мыши на соответствующую иконку на рабочем столе. Появится окно входа в *Консоль*. Убедиться в том, что в поле логина указано верное имя пользователя, соответствующее учетной записи администратора *ЦУП-Консоль* (см. п. 2.3.3), ввести пароль для данной учетной записи и нажать кнопку **ОК**. После этого должно появиться главное окно *ЦУП-Консоль*.

Если Вы установили «удаленную» *ЦУП-Консоль* (т.е. отдельно от *ЦУП-Сервер*) под ОС Windows, то *при первом запуске* необходимо ввести логин и пароль администратора, а также адрес и порт для подключения к серверу.

3.3.1. Создание конфигурации источника данных (DSN) для доступа к БД *ЦУП*

Источник данных для доступа к БД *ЦУП* должен создаваться следующим образом:

1) Открыть *Утилита конфигурирования ZASTAVA* и Нажать кнопку **Создать БД**. В открывшемся окне *Выбор сервра БД* нажать кнопку **ODBC**. В открывшемся окне *Управление серверами БД (ODBC)* нажать кнопку **Добавить**.

2) В поле **Имя** ввести произвольное имя конфигурации источника данных, например, «ZastavaDSN». В поле **Сервер** ввести имя или IP-адрес MS SQL-сервера, на котором установлена БД *ЦУП* (БД должна быть создана заранее, в процессе конфигурирования *ЦУП-Сервер*, подробнее см. п. 2.3.3).

3) В поле **Драйвер** выбрать драйвер для доступа к MS SQL Server ("SQL Server").

4) В поле **Имя Пользователя** указать имя пользователя (по умолчанию - "**sm-server**"), а в поле **Пароль** – пароль для этого пользователя (данные параметры были заданы при создании БД *ЦУП* – подробнее см. п. 2.3.3).

5) В поле **Порт** задать соответствующий значение для связи с сервером БД. Нажать кнопку **Готово**.

3.3.2. Ввод информации о расположении *ЦУП-Сервер* и БД *ЦУП*

После создания DSN-конфигурации Вы должны вернуться в окно входа в *Выбор сервера БД* и выполнтиь следующее:

1) В поле **Имя пользователя** указать имя пользователя для доступа к БД *ЦУП* (например, "sa").

2) В поле **Пароль** указать соответствующий пароль. Нажать кнопку **Далее**.

3) В открывшемся окне *Параметры БД* в поле **БД** указать имя БД ("SMDB").

4) В поле **Сервер БД** задать и подтвердить пароль для учетной записи **sm-server**.

5) В поле **Администратор продукта** задать и подтвердить пароль для учетной записи **sm-admin**. Нажать нопку **Далее**.

6) В открывшемся окне можно выбрать сертификат **ЦУП**. Нажать кнопку **Завершить**.

При последующих запусках *ЦУП-Консоль* необходимо будет вводить только пароль, все остальные параметры будут заполнены автоматически.

4. Обзор конфигурации *ЦУП*

4.1. Введение

Рекомендуется прочитать данный раздел перед тем, как Вы начнете создавать Вашу ГПБ в *ЦУП-Консоль*, и использовать его как руководство при планировании процесса конфигурирования. В данном разделе описывается последовательность действий при создании ГПБ в *ЦУП-Консоль*, а также представлена информация по конфигурации и стратегии, не включенные в последующие секции. При создании *ЦУП* преследовалась цель предоставить Администратору Безопасности максимальные удобства при вводе параметров ГПБ. Файл с описанием и набором параметров ГПБ называется Проектом. Существует лишь незначительное количество ограничений в последовательности создания Проекта и ввода информации о ГПБ в *ЦУП*. Проект и информацию ГПБ нужно вводить в логической последовательности, т.е. в соответствии с тем, как управляется структура компонентов Среды Безопасности и как осуществляется корпоративная Политика Безопасности. Таким образом, пользователю предоставлена большая свобода выбора способа ввода этой информации.

Тем не менее, Вам следует придерживаться некоторых основных принципов при вводе ГПБ в *ЦУП*. Это упростит процесс создания ГПБ для Вашей Среды Безопасности и снизит количество ошибок. В данном разделе, кроме основных принципов, содержатся более подробное описание некоторых аспектов *ЦУП* и принципы сетевой безопасности ПК «VPN/FW «ЗАСТАВА».

4.2. Связь между модулями *ЦУП-Консоль*, *ЦУП-Сервер*, БД *ЦУП* и *ЗАСТАВА-Офис ЦУП*

БД *ЦУП* используется для хранения всей информации о текущем ГПБ-Проекте. Физически *БД ЦУП* представляет собой набор таблиц, создаваемых в реляционной системе управления базами данных (СУБД), которая может располагаться либо на одном хосте с *ЦУП-Сервер*, либо на отдельном хосте. В настоящее время для ОС Windows поддерживаются следующие СУБД:

— MS SQL Server 2008 R2 Express Edition - простой процессор БД с минимальным набором инструментов управления. Он включен в пакет инсталляции *ЦУП*.

— Microsoft SQL Server 2008 - процессор БД с современным набором инструментов управления. Он не включен в пакет инсталляции *ЦУП* и должен быть приобретен и установлен отдельно (до инсталляции *ЦУП*).

— Postgre SQL версии 9.x - это объектно-реляционная СУБД. Она не включена в пакет инсталляции *ЦУП* и должна быть приобретена и установлена отдельно (до инсталляции *ЦУП*).

Модуль *ЦУП-Консоль* - визуальный центр системы управления безопасностью, позволяющий администратору *ЦУП* выполнять следующие основные функции:

1) Создавать и редактировать ГПБ.
2) Отдавать команду *ЦУП-Сервер* на трансляцию ГПБ в набор ЛПБ для каждого из управляемых *Агентов*.
3) Отдавать команду *ЦУП-Сервер* на активацию ГПБ (т.е. на доставку и прогрузку ЛПБ для каждого из управляемых *Агентов*).
4) Отслеживать состояние защищённой сети (текущий статус управляемых *Агентов*, происходящие на них события и т.п.).

Модуль *ЦУП-Сервер* – это набор сервисов (т.е. процессов без графического интерфейса), выполняющих базовые функции ПК «VPN/FW «ЗАСТАВА» (трансляцию и активацию ГПБ, мониторинг, взаимодействие с *ЦУП-Консоль* и т.п.).

Ниже приводится список основных сервисов, которые входят в состав модуля *ЦУП-Сервер:*

- **SecureManage Server** – транслирует ГПБ в набор ЛПБ, регистрирует события, и т.д.
- **SecureManage Distributor** - распределяет оттранслированные ЛПБ управляемым *Агентам*.
- **SecureManage Syslog Server** - собирает Syslog-сообщения от удалённых *Агентов*.
- **SecureManage Application Server** – обрабатывает запросы от *ЦУП-Консоль*, принимает запросы HTTP/HTTPS от *Агентов* и позволяет им загружать начальные пакеты конфигурации.

Для безопасной передачи ЛПБ на управляемые *Агенты, ЦУП* должен быть частью защищенной сети (виртуальная частная сеть (ВЧС)). Для этого используется стандартный *Агент ЗАСТАВА-Офис* (т.н. *ЗАСТАВА-Офис ЦУП*), который устанавливается на одном компьютере с *ЦУП-Сервером* и защищает все исходящие/входящие соединения. Этот *ЗАСТАВА-Офис* с точки зрения ГПБ представляет собой обычный Шлюз Безопасности, который имеет собственную ЛПБ. Для изучения инструкций по использованию *ЗАСТАВА-Офис* надо обратиться к документу МКЕЮ.00434-01 32 01 «Программный комплекс защиты корпоративных вычислительных ресурсов на сетевом уровне с использованием технологий VPN и распределенного межсетевого экранирования на основе интернет-протоколов семейства

IPsec/IKE «VPN/FW «ЗАСТАВА», версия 6» («ПК «VPN/FW «ЗАСТАВА», версия 6»). Компонент «ЗАСТАВА-Офис», версия 6. Руководство системного программиста».

При необходимости, хост с *ЦУП-Консоль* также может быть защищен путём установки *ЗАСТАВА-Клиент*. Данная защита обязательна при использовании *ЦУП-Консоль* в удалённом режиме (т.е. когда трафик управления между *ЦУП-Консоль* и *ЦУП-Сервер* и/или БД *ЦУП* проходит через потенциально опасные сети).

4.3. Подготовка к конфигурированию

Перед конфигурированием *ЦУП* Администратор Безопасности должен сделать следующее:

— Собрать информацию о всех компонентах (Объектах Политики) защищенной системы, которыми будет управлять *ЦУП*:
  - Местоположение и тип всех Объектов Политики.
  - IP-адреса всех Объектов Политики (кроме объектов типа Пользователь). Для всех Объектов с несколькими IP-адресами (например, для Шлюзов Безопасности), должны быть известны все IP-адреса Объекта, а также фактические логические имена всех сетевых интерфейсов.

— Для каждого управляемого *Агента* издать и зарегистрировать в данном *Агенте* цифровой сертификат, который необходим для установления защищенных IPsec-соединений. Если вместо сертификатов используются предварительно распределенные ключи, то необходимо создать и запомнить секретные значения и логические идентификаторы этих ключей. Более подробные сведения о сертификатах и ключах приведены в документе: МКЕЮ.00434-01 32 01 «Программный комплекс защиты корпоративных вычислительных ресурсов на сетевом уровне с использованием технологий VPN и распределенного межсетевого экранирования на основе интернет-протоколов семейства IPsec/IKE «VPN/FW «ЗАСТАВА», версия 6» («ПК «VPN/FW «ЗАСТАВА», версия 6»). Компонент «ЗАСТАВА-Офис», версия 6. Руководство системного программиста», а также в одноименных документах по другим *Агентам*.

— Подготовить аутентификационную информацию для *ЦУП*:
  - Файл с основным сертификатом Удостоверяющего центра (УЦ), а также файлы с локальным сертификатом *ЦУП* и соответствующим закрытым ключом.
  - Для всех управляемых Объектов Политики должна быть известна информация об используемых сертификатах: поле **Владелец** или **Альтернативное имя владельца**, **Алгоритм цифровой подписи**. Если вместо сертификатов

используются предварительно распределенные ключи, то должны быть известны их логические идентификаторы.

В данном руководстве предполагается, что все персональные сертификаты (т.е. локальный сертификат *ЦУП* и сертификаты всех управляемых Объектов Политики) выпущены одним сертификатом УЦ (корневой сертификат УЦ). Однако *ЦУП* поддерживает и конфигурации, где управляемые Объекты Политики используют разные сертификаты УЦ. В этом случае, для корректной работы *ЦУП* все подобные сертификаты должны быть зарегистрированы как «Доверяемые» в *ЗАСТАВА-Офис ЦУП*.

Существует возможность импортировать фактические файлы сертификатов в *ЦУП-Консоль* для всех управляемых *Агентов*. В этом случае вся информация о сертификате будет извлечена автоматически. Подробнее см. п. 7.1.1.1.

4.4. Регистрация сертификатов

Подробности выполнения описанных ниже операций с *ЗАСТАВА-Офис* можно посмотреть в документе МКЕЮ.00434-01 32 01 «Программный комплекс защиты корпоративных вычислительных ресурсов на сетевом уровне с использованием технологий VPN и распределенного межсетевого экранирования на основе интернет-протоколов семейства IPsec/IKE «VPN/FW «ЗАСТАВА», версия 6» («ПК «VPN/FW «ЗАСТАВА», версия 6»). Компонент «ЗАСТАВА-Офис», версия 6. Руководство системного программиста».

Регистрация сертификата выполняется следующим образом:

1) Запустить графический интерфейс *ЗАСТАВА-Офис* и импортировать корневой сертификат УЦ. Этот сертификат необходимо импортировать с флагом **Доверяемый**.
2) Импортировать локальный сертификат (и соответствующий закрытый ключ) в *ЗАСТАВА-Офис*.
3) Проверить и, при необходимости, изменить настройки политик безопасности по умолчанию в *ЗАСТАВА-Офис* (окно *Управление политиками*, закладка *Политика*).
4) Запустить *ЦУП-Консоль* и зарегистрировать идентификатор локального сертификата *ЗАСТАВА-Офис* в Объекте Политики, представляющем *ЦУП-Сервер*.

Для дескриптора *Агента* версии 6.1 зарегистрировать сертификат можно путем экспорта в *Агента* сгенерированного *из ЦУП* сертификата. Для того чтобы создать ключевую пару необходимо нажать кнопку **Генерировать** и заполнить все поля в окне *Генерировать ключевую пару*. Отправить созданный запрос в УЦ (в зависимости от требований УЦ используйте электронную почту, веб-браузер или другие средства). После получения сертификата из УЦ импортировать его в *объект политики*, для этого необходимо в контекстном меню окна *Центры сертификации* выбрать пункт **Заменить подписанным и**

отправить. После этого откроется окно *Импорт сертификатов* в этом окне необходимо посмотреть и проверить параметры сертификата (в случае необходимости изменить их), после чего нажать кнопку **Готово**. Сертификат будет добавлен в ГПБ и отправлен *Агенту*. Для того чтобы ключевая информация была экспортирована и сохранена правильно, в *Графическом интерфейсе Агент* на закладке *Токены* надо поставить наивысший приоритет тому токену, который соответствует криптоалгоритму ключевой информации. Алгоритм создания ключевой пары для *Агента* из *ЦУП* показан на рисунке (см. *Рисунок 14*).

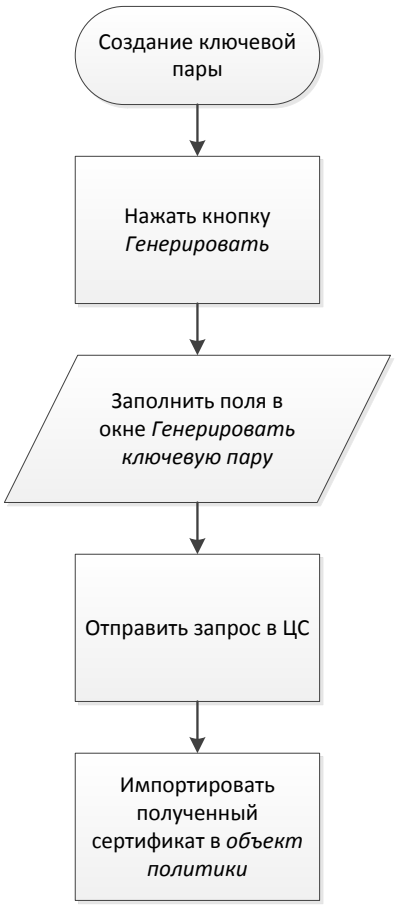

Рисунок 14 – Алгоритм создания ключевой пары

4.5. Основные Объекты ГПБ

Для создания самой простой ГПБ необходимо определить лишь два типа компонентов:

- Объекты Политики (в том числе Зоны);
- Правила.

Объекты Политики создают модель сетевой топологии, представляющую как физические Объекты (хосты, шлюзы), так и логические Объекты (группы, диапазоны адресов и т.д.).

Правила определяют, как Объекты Политики могут обмениваться информацией в защищенной системе. Создание Правил Безопасности - наиболее важный шаг при работе с

ЦУП, поскольку Правила являются основой ГПБ - все привязано к Правилам в той или иной степени.

4.6. Другие Объекты ГПБ

К другим Объектам ГПБ относятся:

- Серверы;
- Сетевые Сервисы;
- Настройки IKE;
- Действия;
- ЛПБ, определяемые пользователем;
- Домены.

Серверы представляют собой особые виды хостов (не обязательно защищенных), к которым будет разрешен доступ различным участникам защищенной системы.

Сетевые Сервисы используются для уточнения Правил: если в Правиле указан Сетевой Сервис, то это Правило будет действовать только для соответствующего типа трафика.

Настройки IKE определяют параметры протокола IKE (Internet Key Exchange), которые будут использоваться в процессе установления первичного защищенного соединения (IKE/ISAKMP SA).

Действия указываются в Правилах и определяют метод обработки трафика: пропускать, сбрасывать или зашифровывать/расшифровывать.

Пользовательские (*Определяемые пользователем) ЛПБ* позволяют Администратору Безопасности составлять типовые, не изменяющиеся фрагменты ЛПБ и вставлять их в произвольное место итоговой ЛПБ, которая генерируется при трансляции ГПБ.

Домены позволяют реализовать модель разграничения прав доступа к консоли ПО *ЗАСТАВА-Управление* по принципу авторизации.

4.7. Создание ГПБ в *ЦУП-Консоль*

В этом подразделе представлен только план процесса создания ГПБ. Подробнее о навигации и использовании *ЦУП-Консоли* описано в разделах 5 - 7 и в Приложение 2. Настройка сервера обновлений, в котором представлен пример пошаговой конфигурации.

В процессе конфигурирования ГПБ настоятельно рекомендуется либо делать заметки, либо выполнять действия по плану.

4.7.1. Объекты Политики

Первым шагом к созданию ГПБ является создание в *ЦУП-Консоль* Объектов Политики. Каждый хост или маршрутизатор, который является частью Безопасной Среды (Security Community) или будет взаимодействовать с ней извне, должен быть представлен как Объект Политики. Например, если Вы хотите включить внешний FTP-сервер в ГПБ, его необходимо описать в *ЦУП* как Объект IP-Хост.

Наиболее типичными Объектами Политики являются следующие объекты: Хосты Безопасности, Шлюзы Безопасности, IP-Хосты, Диапазоны IP-адресов, Подсети и Пользователи. Объекты Политики с собственной системой шифрования (Шлюзы Безопасности, Хосты Безопасности, Пользователи) могут управляться либо из данного экземпляра *ЦУП* (т.н. Управляемые Объекты Политики), либо каким-то другим способом, например, из других *ЦУП* (т.н. Неуправляемые Объекты Политики).

ЦУП должен быть представлен в ГПБ как Шлюз Безопасности с типом *Агента ЗАСТАВА-Офис* (обычно данный объект создается автоматически после конфигурирования БД *ЦУП*).

4.7.1.1. Шлюзы Безопасности

Конфигурировать Шлюзы Безопасности сложнее, чем другие виды Объектов Политики в *ЦУП*, и они являются контрольными точками в защите Вашей Безопасной Среды. Перед созданием Объекта Шлюза Безопасности, который выполняет IPsec-обработку (т.е. не является просто маршрутизатором или МЭ), необходимо знать следующее:

- какие подсети будет защищать Шлюз Безопасности;
- IP-адреса и логические имена всех интерфейсов Шлюза Безопасности;
- какие сертификаты будут использованы для аутентификации Шлюза Безопасности.

Шлюз Безопасности обычно имеет как минимум два интерфейса. В процессе создания Объекта Вам нужно будет указать вид *Агента*, который представляет данный Шлюз Безопасности (*ЗАСТАВА-Офис*, маршрутизатор Cisco или МЭ Cisco PIX Firewall, Шлюз Microsoft IPsec Agent, Неуправляемый Шлюз Безопасности).

4.7.1.2. Группы

Объекты Политики можно также организовать в группы. Если один и тот же набор Правил будет применяться к нескольким Объектам Политики (например, если все компьютеры в одном отделе будут использовать один и тот же набор Правил обработки трафика), то все эти Объекты Политики можно объединить в Группу. Сама по себе Группа считается Объектом Политики, поскольку один набор Правил применяется ко всем членам группы, тем не менее, это лишь совокупность других Объектов Политики. Полезность объединения Объектов

Политики в Группы становится очевидной, когда возникает необходимость создать Правила Безопасности между Объектами Политики или применить данное Правило ко всей Группе, а не к каждому Объекту Политики в отдельности. Создавайте Группы при любой возможности, это поможет Вам снизить количество используемых Правил.

Перед тем, как применить какое-либо Правило к Группе, надо убедиться в том, что его можно применить ко всем ее членам. Например, если некоторые члены Группы являются Хостами Безопасности, а другие представляют собой незащищенные IP-Хосты, Правило, использующее шифрование, нельзя применить к данной Группе.

4.7.1.3. Пользователи

Пользователь - это *Агент* без фиксированного IP-адреса, но со своей собственной системой шифрования, которая может в Безопасной Среде соединяться с узлом, находящимся вне этой Среды. Это портативные компьютеры или компьютеры сети, к которой сервер DHCP не присваивает постоянные IP-адреса. Примером Пользователя является *ЗАСТАВА-Клиент* на портативном компьютере.

Способность определять мобильных *Агентов* как Пользователей - значительное преимущество Безопасной Среды, основанной на *Агентах* и управляемой *ЦУП*. Пользователь может безопасно соединяться с корпоративной сетью, независимо от того, где он вышел в сеть Интернет. До тех пор, пока мобильный пользователь может соединяться с сетью Интернет, его/ее доступ к корпоративной сети его/ее компании его/ее надежен и безопасен. Более того, переговоры между *ЗАСТАВА-Клиент* и *ЦУП* происходят автоматически, ни мобильному пользователю, ни Администратору Безопасности не нужно ни вмешиваться, ни менять конфигурацию.

4.7.1.4. Зоны

Зона – это пространство IP-адресов за Шлюзом Безопасности, которое состоит из группы связанных хостов, защищенных тем же самым Шлюзом. Хотя **Зона** может показаться похожей на **Подсеть** и **IP-Диапазоны**, существуют значительные различия. **Подсети** и **IP-Диапазоны** – определенные наборы IP-адресов, которые применяют к определенным существующим Объектам Политики (компьютерам) с IP-адресами, в то время как **Зона** – это только *пространство* IP-адресов, к которому могут принадлежать Объекты Политики за Шлюзом Безопасности. (**Подсети** и **IP-Диапазоны** не обязательно должны находиться за Шлюзом Безопасности.) **Зоны** - единственный источник информации для *ЦУП* о том, какие хосты каким Шлюзом защищены.

	Внутренний интерфейс **Шлюза Безопасности** должен быть включен в **Зону**. Если присутствует вложенный **Шлюз**, то его внешний интерфейс тоже должен быть включен в **Зону**.
	IP-адрес может находиться только в одной **Зоне.**

4.7.1.5. Процесс создания *Агентов* Политики

Задача: Создать *Агентов* Политики, представляющих все виды *Агентов*, которые можно включить в ГПБ, управляемую *ЦУП.*

Логическая схема: Создать Объекты один за другим. Создать Группу и объединить в нее некоторые Объекты Политики.

Для создания *Агента* Политики нужно выполнить следующие действия:

1) Создать Объект Хост Безопасности:

- Используйте **Править -> Добавить -> Хост Безопасности.**
- Выбрать производителя *Агента* и его версию.
- Ввести уникальное **Имя** для присвоения Объекту Хоста Безопасности.
- Ввести **Адрес *Агента* Объекта**, этот IP-адрес будет использоваться для того, чтобы поддерживать связь с этим Объектом.
- Выбрать домен, в который будет входить данный Объект.
- В закладке *Топология* ввести параметры интерфейса(ов) Хоста Безопасности.
- В закладке *Местоположение* ввести параметры местоположения Хоста Безопасности.
- Ввести параметры сертификата, который будет идентифицировать этот Хост Безопасности или импортировать соответствующий сертификат.
- Если Вы хотите изменить параметры надо обратиться к п. 7.1.3.

2) Создать Объект Шлюз Безопасности, выполняя ту же последовательность действий, что и для Объекта Хост Безопасности. Кроме того:

- Убедиться в том, что Вы ввели точные имена логических сетевых интерфейсов.
- Если Объект Шлюза Безопасности будет представлять *Агента* Cisco, нет необходимости указывать SNMP-сообщения, но нужно подробно указать SSH или опции Telnet-соединения во вложенной закладке *Параметры соединения* закладки *Управление*.
- Если Вы хотите изменить параметры надо обратиться к п. 7.1.2.

3) Создать Объект *Пользователь*:

- Использовать **Править -> Добавить -> Пользователь**, где они доступны.
- Ввести уникальное **Имя** для присвоения Объекту *Пользователь*.

- Выбрать версию и набор свойств *Агента*, которые будет представлять Объект *Пользователь*.
- Во вложенной закладке *Сертификаты закладки ВЧС* входят параметры сертификатов, которые идентифицируют этот Объект или импортируют файл сертификата.
- Если Вы хотите изменить параметры надо обратиться к п. 7.1.7.

4) Создать Объект *IP Хоста*:

- Используйте **Править -> Добавить -> IP Хост**.
- Ввести уникальное **Имя** для присвоения Объекту *IP Хоста*.
- При необходимости можно ввести текстовое описание Объекта.
- В закладке *Топология* ввести параметры интерфейса(ов) *IP Хоста*.
- Если Вы хотите изменить параметры надо обратиться к п. 7.1.4.

5) Создать Объект **Подсеть**:

- Используйте команду **Править -> Добавить -> Подсеть**, где она доступна.
- Ввести уникальное имя для присвоения Объекту **Подсеть**.
- Ввести основной **IP-адрес** и сетевую **Маску** для **Подсети**.
- Если Вы хотите изменить параметры надо обратиться к п. 7.1.6.

6) Создать Объект **IP Диапазона**:

- Используйте команды **Править** −> **Добавить** −> **IP Диапазон**, где они доступны.
- Ввести уникальное имя для присвоения Объекту **IP Диапазон**.
- Добавить список адресов IP-диапазона или один адрес, выбрав формат, в котором Вы хотите ввести данные, затем ввести нужные данные. При необходимости, повторить.
- Если Вы хотите изменить параметры надо обратиться к п. 7.1.5.

7) Создать Объект **Группы** и присвоить Группе несколько Объектов Политики:

- Используйте команды **Править** -> **Добавить -> Группы**
- Ввести уникальное **Имя** для присвоения Объекту **Группа**.
- Выбрать Объект (ты) Политики в закладке *Доступные элементы*, которые Вы хотите включить в эту Группу, и перенести их в список **Члены группы**.

8) Создать объект **Зона**:

- Навести курсор на секцию *Топология*, использовать **Править->Добавить->Зона** или Добавить **Зону** из контекстного меню в *Топологии.*
- Ввести уникальное **Имя** для присвоения Объекту **Зона**.
- Ввести диапазон(ы) **IP-адресов**, который будет определять **Зону**.
- Если Вы хотите изменить параметры надо обратиться к п. 7.2.2.

4.7.2. Правила

Правила Безопасности – это основные правила для функционирования *ЦУП*. Правила используются для того, чтобы систематизировать информацию (Объекты Политики и Действия) в согласованную и целостную ГПБ. Правила определяют, как различные компоненты Безопасной Среды могут обмениваться информацией, т.е. какие соединения допускаются, а какие нет.

Создать Правила Безопасности между всеми Объектами Политики, которым нужно безопасно передавать информацию в Безопасной Среде. В большинстве контекстов сетевой Безопасности, это довольно сложная задача, поскольку для каждого взаимодействия, требующего шифрованный доступ, нужно создавать отдельные Правила. В *ЦУП* при подходе, ориентированном на Объект и на Группу, этот процесс гораздо проще, потому что маловероятно, что каждому участнику Вашей Безопасной Среды понадобится уникальный уровень доступа к безопасным коммуникациям. *ЦУП* позволяет группировать Объекты с одинаковым уровнем доступа и применять одно правило ко всей группе, если эта группа определена как Группа или Подсеть.

Пример:

В Отделе продаж есть 100 компьютеров, которым нужно обмениваться информацией так же, как 100 компьютерам в Отделе маркетинга. На всех 200 компьютерах установлены *Агенты*, и они идентифицированы уникальными сертификатами. Можно определить эту коммуникацию одним правилом (компьютеры каждого отдела были собраны в отдельные Группы). Одно это правило может управлять любым количеством Объектов и сервисов, при условии, что Группы создаются раньше, чем правила. С *ЦУП* некоторые Объекты могут быть дополнительно защищены *ЗАСТАВА-Офис,* а некоторые нет. Некоторые из них могут менять местоположение, а некоторые нет. С точки зрения Правил, ничто из вышеперечисленного не играет роли, надо создать одно правило, и *ЦУП* определит Политики для Объектов. Неуправляемые (UNMANAGED) Объекты тоже участвуют в правилах. Существует два вида коммуникаций с неуправляемыми Объектами:

коммуникация с IP-Хостами;

– коммуникация с неуправляемыми Объектами, идентифицированными особыми мандатными (см. пояснения выше об управлении с использованием мандатов).

Правила обрабатываются в соответствии с их положением в уровне иерархии. То есть, если правило имеет вложенные правила, вложенные правила обрабатываются раньше основного правила. Исключением являются: правила "**Any-Any**", которые всегда обрабатываются последними; правила "**Any-agent**" и/или **Правила**, в состав которых входят Пользователи, обрабатываются предпоследними (см. п. 4.7.2.3). *ЦУП* выполняет эти операции автоматически.

4.7.2.1. Правила для беспроводных сетей

ЦУП позволяет создавать Правила, чтобы обеспечить защиту трафика и строгую аутентификацию для Пользователей в беспроводных (WiFi) сетях. Эти Правила определяют *Политику, основанную на расположении*, где Пользователю разрешен доступ к защищаемым конфиденциальным ресурсам на основании его расположения в определенном адресном пространстве, представленном в виде *Подсети* или *IP Диапазона*. Есть несколько причин для создания этих Правил, чтобы защитить сегмент беспроводной сети с IKE/IPsec:

- Wired Equivalent Privacy (WEP) протокол потенциально уязвим;
- Как только сегмент проводной сети защищен ВЧС, можно построить виртуальные сети, основанные на IPsec в одной физической WiFi-сети;
- Аутентифицированные пользователи, находящиеся внутри сети, могут безопасно обмениваться информацией за ее границами.

Расположение определяется при создании Правила, в частности, когда определяются источники(и) и приемник(и), которыми управляет Правило. Расположения появляются в полях **Источник** и **Приемник Таблицы ГПБ**. Пользователь и Группы могут определяться как особые Объекты Политики в пределах расположения - т.е. такие Объекты Политики могут определять правила **Источников** или **Приемников** вместе с IP-адресами, составляющими Расположение. Любые члены Группы, которые не являются Пользователями, будут игнорироваться, когда применяется правило, основанное на расположении. Политики, основанные на расположении, могут применять действия **PASS**, **DROP** и шифрования и использоваться в любой комбинации Сетевых Сервисов. В этом смысле Политики, основанные на расположении, не отличаются от «обычных» Политик.

4.7.2.2. Описание WIFI сценария с использованием Политики, основанной на расположении POLICY

Типичный сценарий сети с WiFi-сегментом показан на рисунке (см. Рисунок 15).

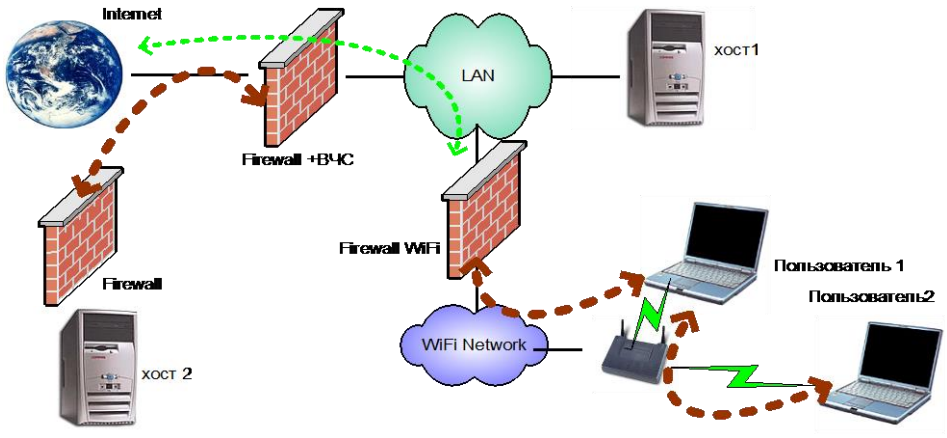

Рисунок 15 – Сеть с WiFi-сегментом

Для того чтобы правильно выполнить беспроводной сегмент данного образца сети надо придерживаться следующих руководящих принципов:

1) *Пользователь1* и *Пользователь2*, ради удобства, должны быть членами Группы (при условии, что они имеют одинаковый уровень доступа к защищаемым конфиденциальным ресурсов). Назовем эту Группу **Wireless Group**.
2) Создать **Подсеть** или **Объект** IP Диапазона с адресным пространством WiFi-сети. Назовем этот **Объект Wireless Подсеть.**
3) Чтобы *Пользователь1* и *Пользователь2* взаимодействовали друг с другом через защищенный протокол внутри WiFi-сети надо создать Правило с параметрами (см. Таблица 1).

Таблица 1 – Параметры Правила для взаимодействия внутри WiFi-сети

Параметр	**Описание**
Источник	Wireless Group @location: Wireless Subnet
Приемник	Wireless Group @location: Wireless Подсеть
Действие	Любое действие, которое использует шифрование

4) Чтобы два этих Пользователя имели безопасный доступ в сеть Интернет надо создать Правило со следующими параметрами (см. Таблица 2). На Шлюзе Firewall+ВЧС шифруется трафик.

Таблица 2 - Параметры Правила для безопасного доступа в сеть Интернет

Параметр	**Описание**
Источник	Wireless Group @location: Wireless Subnet
Приемник	Internet
Действие	Любое действие, которое использует шифрование

5) Чтобы два этих Пользователя имели нешифрованный доступ (открытый трафик) в/из Хост1, находясь внутри WiFi-сети (см. Таблица 3), и защищенный доступ (зашифрованный трафик) в/из хоста из сети Интернет (см. Таблица 4), надо создать два Правила.

Таблица 3 – Параметры Правила для доступа по открытому (нешифрованному) каналу связи относительно Хост1, находясь внутри WiFi-сети

Параметр	**Описание**
Источник	Wireless Group @location: Wireless Subnet

Приемник	Хост1
Действие	Pass

Таблица 4 - Параметры Правила для защищенного доступа по шифрованному каналу связи относительно Хост1 из сети Интернет

Параметр	**Описание**
Источник	Wireless Group
Приемник	Хост1
Действие	Любое действие, которое использует шифрование

6) Чтобы два этих Пользователя имели шифрованный доступ к Хост2, как внутри WiFi-сети (см. Таблица 5), так и из сети Интернет (см. Таблица 6), надо создать два Правила.

Таблица 5 - Параметры Правила для шифрованного доступа относительно Хост2 внутри WiFi-сети

Параметр	**Описание**
Источник	Wireless Group @location: Wireless Subnet
Приемник	Хост2
Действие	Любое действие, которое применяет шифрование

Таблица 6 - Параметры Правила для шифрованного доступа относительно Хост2 из сети Интернет

Параметр	**Описание**
Источник	Wireless Group
Приемник	Хост2
Действие	Любое действие, которое применяет шифрование

7) Чтобы два этих (и любой другой) Пользователя имели защищенный доступ к Хост2, находясь в адресном пространстве LAN IP (см. Таблица 7), надо создать следующее Правило.

Таблица 7 - Параметры Правила для защищенного доступа к Хост2, находясь в адресном пространстве LAN IP

Параметр	**Описание**
Источник	LAN

Параметр	Описание
Приемник	Хост2
Действие	Любое действие, которое применяет шифрование

Чтобы любой Пользователь, который может соединиться с Вашей беспроводной точкой доступа, мог участвовать в безопасных коммуникациях, следует определить правило, чей **Источник** будет Any Объект @location: Wireless Subnet. Однако следует учитывать, что это сделает Вашу сеть доступной (или, точнее сказать, любой сегмент Вашей сети определяется в **Приемнике** Правила) для всех, находящихся в пределах радиуса действия Вашей точки доступа. Такие функциональные возможности, тем не менее, могут быть полезны, при условии, что Объект(ы) **Цель** выбран с особой тщательностью. Например, можно указать, что каждому клиенту или дистрибьютору, который приходит в Ваш офис и у которого есть портативный компьютер с беспроводной картой, разрешен доступ к специальному серверу или просто доступ к сети Интернет без риска для безопасности остальной сети.

4.7.2.3. Опции ANY и INTERNET Объекты

Кроме возможности использовать набор Объектов Политики, доступными являются еще две опции: **Any** и **Internet Объект**ы. Эти Объекты появляются в диалоговом окне выбор Объекта Политики вместе с другими Объектами Политики. Выбор одного из этих Объектов или обоих в качестве **Источника** или **Приемника** Правила представляет большие удобства при создании Правил. Если **Internet Объект** используется как **Источник** или **Цель** (Приемник) Правила ГПБ, и уже существующий *Агент* выбран для другого, это значит, что Правило будет управлять коммуникациями между указанным *Агентом* и *любым возможным узлом коммуникаций, расположенным в Интернет-зоне* (независимо от того, определен он в ГПБ или нет). Такие Правила **Internet**-*Агента* будут применяться после обработки всех Правил agent-agent.

Ели **Any Объект** используется, как **Источник** и **Приемник** правила ГПБ и существующий *Агент* выбран для другого, это значит, что Правило будет управлять коммуникациями между указанным *Агентом* и *любым другим объектом из сети Интернет (включая объекты, описанные в ГПБ), который попытается обменяться с ним информацией и еще не включен в Правило этим Агентом.* Если **Any Объект** используется и как **Источник**, и как **Приемник (Цель)** Правила, это правило будет управлять всеми коммуникациями между *любыми двумя Агентами*, если эту коммуникацию не регулирует другое Правило. Такие **Any-Any** Правила всегда будут применяться в последнюю очередь, после обработки всех остальных Правил Безопасности. Подобным образом, все Правила **Any**-*Агента* будут применяться предпоследними, после всех остальных правил, за исключением Правила **Any-Any,** если

таковое имеется. Опцию **Any** можно использовать для создания неполных правил или шаблонов.

4.7.2.4. Правила и вложенные Правила

Важным аспектом создания правил является возможность создать иерархическое дерево этих Правил, которые отвечали бы требованиям Вашей Безопасной Среды. Можно создать «основные» Правила, которые будут применяться ко многим *Агентам*, а затем специальные Правила для «особых случаев» или исключений из основных Правил. «Родительские» Правила по своей сути более глобальны, в отличие от «дочерних» Правил, которые более специфичны.

Пример:

У Вас есть 100 *ЗАСТАВА-Клиент,* объединенных в одну *Группу* в одном отделе, и 100 *ЗАСТАВА-Клиент* объединенных во вторую *Группу* в другом отделе компании. Сотрудникам этих отделов, за небольшим исключением, нужно определенным образом обмениваться информацией. Таким образом, Вы будете применять одинаковые правила обработки трафика почти ко всем 100 *Клиент* в первой *Группе* и почти ко всем *ЗАСТАВА-Клиент* во второй *Группе,* за небольшим исключением. Определить правила основного дерева для каждой индивидуальной *ЗАСТАВА-Клиент – ЗАСТАВА-Клиент* коммуникации, поскольку эти исключения более сложные, и они загромождают основное дерево этими особыми случаями. Поэтому лучше использовать «дочерние» Правила (вложенные Правила): создать между двумя *Группами* одно основное Правило, а затем «дочерние»; эти вложенные Правила будут представлять исключения из основного Правила. Такие родительские/дочерние отношения между Правилами можно сформулировать так: «Все 100 *ЗАСТАВА-Клиент* в первой *Группе* будут обмениваться информацией со всеми 100 *ЗАСТАВА-Клиент* во второй *Группе,* кроме *ЗАСТАВА-Клиент* номер 86 в *Группе 1*, который будет по-другому обмениваться информацией с *ЗАСТАВА-Клиент* номер 47 в *Группе 2*.»

Так же, как и Правила в основном дереве, вложенные правила можно применять в любой последовательности на данном иерархическом уровне.
Исключением являются Правила "**Any-Any"**, которые всегда обрабатываются в последнюю очередь, а также Правила "**Any**-*Агент*" и/или правила, касающиеся Пользователей, которые обрабатываются предпоследними. *Родительское Правило* применяется только после применения всех «дочерних» Правил.

4.7.2.5. Регистрация события

Уровень регистрации события можно установить отдельно для каждого правила в ГПБ. У каждого Правила есть параметр *Уровень лога* (*Log Level),* в котором указан уровень информации о событиях системы, публикующийся в журнале событий. По умолчанию *Уровень лога* установлен в значение **Нет**, т.е. сбор информации о событиях в системе, относящихся к

выбранному Правилу, не ведется. Вы можете изменить *Уровень лога* на другое доступное значение, чтобы уровень регистрации событий соответствовал требуемому.

Процесс создания Правил

Задача: Создать Правила между Объектами Политики, как сгруппированными, так и не сгруппированными, чтобы сконфигурировать безопасные взаимодействия между этими Объектами.

Логическая схема: Перейти к секции *Таблица Правил*. Создать Правило, указав два Объекта, между которыми будет использоваться Правило. Можно указать Сетевой Сервис, который будет использовать это Правило и **Действие**, которое оно будет применять. Можно указать уровень регистрации для этого Правила (т.е. уровень событий, которые будут регистрировать Объекты, когда применяется Правило). Также доступен выбор Маршрута для Правила, указывающий шлюзы, через которые будет доступна реализация Правила и Расписание, обозначающее время действия Правила. Создать вложенные Правила («дочерние»), чтобы использовать их как исключения к основному Правилу.

Шаги:

1) Для создания используйте **Править** -> **Добавить** -> **Правило** или **Правило** из контекстного меню в *Таблице Правил*. Ввести уникальное имя для Правила.
2) Указать, является ли создаваемое Правило, вложенным Правилом к уже существующему в *Таблице Правил*. Выбрать Родительское Правило из выпадающего списка поля **Родительская связь**. Вложенное Правило появится под основным Правилом в *Таблице Правил*.
3) Выбрать **Действие**, которое данное Правило будет применять между этими двумя Объектами Политики.
4) Выбрать нужный уровень регистрации событий.

Выбрать Объект Политики и указать его как инициатора безопасного соединения (**Источник**). Если Объект **Источник** является Пользователем, т.е. находится внутри определенного сегмента сети (как WiFi-сегмент), выбрать **Подсеть** или **IP Диапазон**, которые будут представлять этот сегмент.

5) Выбрать *Объект Политики*, который будет обмениваться информацией с Объектом Политики, который указан в шаге 2); это будет Объект **Цель**. Если Объект **Цель** является Пользователем, т.е. находится внутри определенного сегмента сети (как WiFi-сегмент), выбрать расположения Подсеть или IP Диапазон, которые будут представлять этот сегмент.
6) Выбрать Маршрут, определив *Агентов*, через которые Правило будет следовать.
7) Выбрать любые Сетевые Сервисы, которые будет использовать данное Правило.
8) Выбрать **Расписание для Правила**.

4.7.2.6. Указания по реализации

Перед активацией ГПБ, созданной в *ЦУП,* надо распределить исходные ЛПБ каждому *Агенту*. В большинстве случаев, данная ЛПБ не допустит безопасную коммуникацию, кроме как с *ЦУП;* т.е. будет проводиться Политика **Drop.** Следует принять во внимание некоторые последствия такой ситуации.

Если, по недосмотру, Вы не указали в *ЦУП* Правило Безопасности для данного *Агента,* которое позволяет этому *Агенту* участвовать в Безопасной Среде, то этот *Агент* не сможет обмениваться информацией с другим узлом в Безопасной Среде, пока не будет добавлено Правило, перенесена и активирована ГПБ, и пока *Агент* не загрузит ЛПБ из *ЦУП*. Сюда войдут все приложения, включая электронную почту и доступ к сетевым принтерам. Это может произойти в процессе дистрибуции или активации исходной ЛПБ или при обновлении ГПБ/ЛПБ (в результате добавления новых узлов в Среде Безопасности и т.д.).

Это может вызвать негативные последствия в Вашей организации, если пользователи, которым нужен постоянный доступ к сетевым ресурсам, временно не могут его получить. Тогда можно создать временную «мягкую» Политику, которая допускает все сетевые соединения при запуске ЛПБ. Для этого создать дополнительное Правило (или несколько дополнительных Правил, в зависимости от ситуации) в *ЦУП-Консоль* и указать, что для данного узла или группы узлов весь сетевой трафик должен быть пропущен. После того как ГПБ успешно развернута и установлена на любом узле с «мягкой» Политикой **Pass**, удалить правило, перенести и активировать измененную ГПБ. Таким образом, пользователи, у которых есть доступ к различным сетевым ресурсам, не заметят изменения, а оно, в свою очередь, позволит Вам использовать безопасное решение так плавно, как это возможно. См. примеры ниже.

Пример 1:

Хост Безопасности, в приведенном выше примере конфигурации, принадлежит пользователю, которому нужен постоянный доступ к сетевым ресурсам, и не может быть отрезан от этих ресурсов ни по какой причине. Можно создать Правило или Правила, чтобы дополнительно защитить сетевой доступ данного пользователя или пользователей. Создать Правило между *Агентом*, которого Вы хотите «защитить» и сетью (или сетевым узлом), с которым у этого *Агента* должна быть непрерывная коммуникация; выбрать для *Действия* **Pass.** После того, как ЛПБ *загружена в Агент* и активирована, удалить Правило.

Пример 2:

У Вас очень большая ГПБ (и, возможно, сеть, которая эксплуатируется 24 часа/7 дней) и Вы не уверены, какие Объекты Политики были созданы для всех узлов. В этом случае можно создать общее Правило, чтобы защитить доступ к сети для всех пользователей. Создать

Правило **Any-Any,** выбрав **Any** для **Источника** и **Приемника**, выбрать *Действие* **Pass**. После того, как ЛПБ *загружена во все Агенты* и успешно активирована, удалить Правило и заново перенести и активировать ГПБ. Пока действует это Правило, весь трафик в и вне сети будет незащищен, включая доступ для Пользователей, не указанных в ГПБ. Если Вы создадите такой вид Правила, удалить его, как только отпадет необходимость, и принимайте особые меры предосторожности, пока действует данное Правило.

Этой процедурой можно воспользоваться, только чтобы избежать критических ошибок и/или для удобства определенных Пользователей. В большинстве случаев, нет необходимости в принятии такого решения.

4.7.3. Расписания

Расписания позволяют указывать определенный интервал времени для действия Правил. Например, если есть необходимость использовать в рабочее время один набор Правил, а в ночное - другой.

Расписанию может быть задана дата активации и завершения, ограничение действия по времени суток и дням недели.

4.7.4. Серверы

Закладка *Серверы* позволяет создавать и редактировать вспомогательные Объекты (серверы), которые не являются в чистом виде Объектами Политики Безопасности, но, тем не менее, выполняют разнообразные важные функции, необходимые для работы защищенной сети. В дальнейшем будем называть такие вспомогательные объекты Серверами.

Большинство Серверов располагаются на реальных хостах в сетевой топологии (например, серверы управления, серверы-прогрузчики и т.п.). Для удобства пользователя многие Серверы создаются автоматически при создании БД *ЦУП* - обычно это приложения (системные сервисы), которые входят в состав *ЦУП* и взаимодействуют с внешними хостами.

Подробная информация о типах Серверов и методах работы с ними приведена в подразделе 7.9.

4.7.5. Серверы аутентификации

Закладка *Серверы аутентификации* позволяет создавать и редактировать вспомогательные Объекты (серверы аутентификации), которые не являются в чистом виде Объектами Политики Безопасности, но, тем не менее, выполняют разнообразные важные функции, необходимые для работы защищенной сети.

Серверы аутентификации - виртуальные сущности (объекты Certification Authority (CA), представляющие собой сертификаты УЦ), которые напрямую не связаны с хостами в сети.

Для удобства пользователя многие Серверы аутентификации создаются автоматически при создании БД *ЦУП* - обычно это приложения (системные сервисы), которые входят в состав *ЦУП* и взаимодействуют с внешними хостами.

Подробная информация о типах Серверов и методах работы с ними приведена в подразделе 7.9.

4.7.6. Сетевые Сервисы

Сетевые Сервисы позволяют определять сетевые протоколы для использования в данном Правиле (около 100 объектов Сетевого Сервиса присутствуют в *ЦУП-Консоль* по умолчанию). Некоторые из этих объектов представляют отдельные сервисы, а некоторые группы таких сервисов. В большинстве случаев это только вопрос выбора Сетевого Сервиса (ов), которые Вы хотите использовать. Если Вам нужно создать новый Объект Сетевой Сервис, то это просто: если Вы знаете номера портов сервисов, которые Вы хотите добавить, можете сразу ввести их.

4.7.6.1. Процесс создания сетевых сервисов

Задача: Создать Объект Сетевой Сервис и Объект **Группа** Сетевых Сервисов.

Логическая схема: Выбрать вкладку *Сетевые Сервисы (*меню *Окно)*. Из контекстного меню выбрать **Добавить сетевой сервис**, указать протоколы, которые будет представлять этот Объект. Затем указать порт, который будет использован. Указать всю информацию, необходимую для отдельного Сетевого Сервиса. Затем создать Группу Сетевых Сервисов и добавить к ней Сетевые Сервисы.

Шаги:

Создать Объект Сетевой Сервис:

1) В закладке *Сетевые Сервисы* выбрать в контекстном меню параметр **Создать** в появившемся окне *Добавить Сетевой Сервис* выбрать вид Сетевого Сервиса из вложенного меню поля **Тип.**
2) В окне *Добавить Сетевой Сервис* ввести уникальное **Имя** для Сетевого Сервиса.
3) Ввести номер Порта(ов).
4) Ввести номер Порта источника, если нужно.
5) Указать другие параметры, такие как опции TCP-соединения или процедуры межсетевого экранирования (МСЭ) FW-процедура.

Создать Группу Сетевых Сервисов:

1) В окне просмотра *Сетевые Сервисы* используйте из контекстного меню *Добавить Сетевой Сервис*, в выпадающем меню *Тип* выбрать **Группа**.
2) В окне *Добавить Сетевой Сервис* - ввести уникальное **Имя** для присвоения Группе Сервисов.

3) Перенести *Сетевые Сервисы* из списка *Доступные Сетевые Сервисы* в список *Выбранные Сетевые Сервисы*.

4.7.6.2. Процедуры межсетевого экрана

МЭ обеспечивают Безопасность внутренних систем и сетей, применяя процедуры, которые фильтруют входящий и исходящий трафик.

Объекты **Процедура МСЭ (FW-процедура)** представляют собой Правила расширенного пакета фильтрации, применяемые в *Агентах* Безопасности. Главным преимуществом Процедуры **МСЭ** над обычными пакетами фильтрации – это то, что они отслеживают состояние сетевого соединения и пропускают только те пакеты, которые соответствуют текущему состоянию соединения. Для некоторых протоколов (например, FTP) номера портов для вторичных соединений присваиваются динамически. В таких случаях нельзя использовать обычные пакеты фильтрации, можно использовать только Процедуры **МСЭ**. Процедуры **МСЭ** специфицированы внутри Сетевых Сервисов, которые затем связываются с Правилами.

Около пятнадцати Процедур **МСЭ** присутствуют в *ЦУП-Консоль* по умолчанию. Процедуры **МСЭ** (FW процедура) для разных видов *Агентов* описаны в файлах описания *Агентов* в подкаталоге `\ads` директории *ЦУП*. Любые заказные Процедуры **МСЭ** должны быть добавлены к соответствующему файлу описания, до того как будут использованы в *ЦУП*.

4.7.7. Настройки IKE

Настройки IKE - набор параметров протокола IKE (Internet Key Exchange), которые предлагаются партнеру при переговорах в процессе установления защищенного соединения ISAKMP Security Association (первая фаза протокола IKE). Есть два вида настроек IKE: общие параметры для первой фазы IKE и специальные предложения для создания ISAKMP Security Associations. Приоритет IKE-Предложений соответствует порядку, в котором они указаны в дереве - сверху вниз. Настройки IKE создаются и редактируются во вкладке Настройки IKE (меню *Окно*), для этого нужно выбрать методы аутентификации и алгоритмы шифрования из выпадающего списка, а затем указать некоторые параметры, касающиеся времени существования защищенного соединения. Два IKE-Предложения первой фазы присутствуют в *ЦУП* по умолчанию.

Если в Вашей Безопасной Среде есть члены, которые будут использовать другие методы аутентификации и шифрования, то можно создать дополнительный набор IKE-опций, для этого просто создать новые объекты IKE-Предложения.

4.7.7.1. Процесс изменения параметров аутентификации

Чтобы изменить какой-либо параметр аутентификации необходимо открыть окно IKE-установки, выбрать одно из IKE-Предложений, которое Вы хотите редактировать, и изменить нужный параметр. Если другие узлы Безопасной Среды используют сертификаты с разными алгоритмами цифровой подписи, тогда Вам нужно создать (командой **Добавить IKE-предложение** из контекстного меню) IKE-Предложения для каждого варианта - например, один объект IKE-Предложения использует подпись RSA для аутентификации, а другой - подпись DSA.

Также, если разные узлы будут использовать разные алгоритмы шифрования, хеш-алгоритмы или **Oakley группы**, Вам нужно создать отдельные IKE-Предложения для каждого возможного варианта.

	IKE-Предложения «предлагаются» в соответствии с их положением в структуре (сверху вниз). Таким образом, самые приоритетные (желаемые) IKE-Предложения должны находиться выше всех остальных в структуре. Можно воспользоваться полем **Приоритет** из контекстного меню *Изменить*, чтобы расположить объекты IKE-Предложения в нужном порядке.
	Если в ГПБ используются Предвариетльно Распределенные Ключи (Preshared Keys) необходимо убедиться в том, что в списке присутствует соответствующее IKE-Предложение с типом аутентификации "Preshared Key
	Убедиться в том, что параметры IKE-Предложения Объекта PMP Distribution Service (соответствуют параметрам, применяемым к *Агентам.* В противном случае Вы не сможете активировать ГПБ. Убедиться в том, что параметры, которые Вы выбрали, поддерживаются криптоплагинами *Агентов.*

4.7.8. Действия

Действие определяет, как обрабатывается трафик между узлами, указанными в Правиле Безопасности. Возможны три вида Действия:

- Пропустить (**PASS**) трафик в том виде, в котором он есть (т.е. незащищенная коммуникация между источником и приемником);
- Не пропускать (**Drop**) весь трафик;
- Зашифровать и пропустить трафик (encrypt and Pass traffic).

Простые Действия **PASS** и **DROP** представлены по умолчанию при создании Правил, таким образом, нас интересуют только Действия, которые шифруют трафик перед тем, как пропустить его.

Определенные Объекты не могут участвовать в Правилах, которые используют действие "encrypt and Pass traffic"(«зашифровать и пропустить трафик»), поскольку по определению они не содержат механизмов, чтобы устанавливать защищенное соединение с другими Объектами Политики. Данные Объекты могут участвовать только в обычных (нешифрованных) действиях **PASS** или **DROP**:

- Объекты Подсеть, IP-Хост и IP-Диапазон, которые не защищены Шлюзом Безопасности;
- Объекты Шлюз Безопасности и Хост Безопасности, у которых в поле **Включить IKE/IPsec-обработку** нет отметок.

При создании **Действий** важно знать, какие алгоритмы будут использоваться всеми Объектами в ГПБ для AH-аутентификации, ESP-шифрования и ESP-аутентификации, IPComp-сжатия. Создать несколько **Действий**, если разные узлы Безопасной Среды будут использовать разные алгоритмы то необходимо создать разные действия для каждого требуемого варианта. (Вы также должны создать разные Правила – при создании Правила надо проследить, что **Действие**, применяемое Правилом, соответствует параметрам, используемым для аутентификации/шифрования для всех Объектов Политики, к которым будет применено это Правило).

4.7.8.1. Процесс создания Действий

Задача: Создать Действие «зашифровать и пропустить». (*Заметьте:* три таких Действия присутствуют автоматически. Можно для практики создать одно из них заново, чтобы Вы могли впоследствии создавать дополнительные Действия).

Логическая схема: Перейти к окну *Действия Создать Действие*, которое включает в себя IPsec с выбранным уровнем шифрования.

Шаги:

1) Открыть меню *Править*, выбрать **Добавить – Действие**:

- Ввести уникальное **Имя** для Действия.
- Выбрать, использовать ли IPsec в режиме туннелирования или будет использован транспортный режим.
- Если Вы используете режим туннелирования, указать нужное значение в поле **Бит** 'Don't fragment'(Don't fragment bit).
- Выбрать, использовать ли тот же Сетевой Сервис (Использовать сервис для IPsec SA), что использует Правило ГПБ при переговорах в IPsec защищенном соединении.
- Выбрать, использовать ли усиленную защищенность (Использовать усиленную защищенность).
- Поля **IKE_CFG** и **XAUTH** действия используются при прокладывании трасс Правил. Если установлены значения (**Вкл**) или (**Выкл**) то будут выбираться трассы

через Шлюзы Безопасности где соответственно включены или выключены протоколы IKE_CFG и XAUTH. При значении полей - **АВТО** трассировщик не анализирует наличие или отсутствие протоколов IKE_CFG и XAUTH на шлюзах, через которые проходит трасса Правила.

– При туннелировании IP-пакетов выбрать, использовать ли QoS management, изменяя DiffServ параметр.

7) Используйте вкладку *Предложение*, чтобы установить опции AH и ESP в окне:

– Выбрать, использовать ли ESP. При использовании протокола необходимо отметить флажок **Включить ESP** и выбрать алгоритмы шифрования и аутентификации из выпадающего меню.

– Выбрать, использовать ли AH. При использовании протокола необходимо отметить флажок **Включить АН**, если используется AH и выбрать алгоритм аутентификации из выпадающего списка.

– Выбрать, использовать ли IPComp-протокол. При использовании протокола необходимо отметить флажок **Включить IPComp** и выбрать алгоритм сжатия из выпадающего списка.

– Требуется указать параметры времени существования защищенного соединения. Заметьте, что нулевое значение предполагает «неограниченное».

4.7.9. Определяемая пользователем ЛПБ

Определяемая пользователем ЛПБ (пользовательская ЛПБ) - это часть Локальной Политики Безопасности (фрагмент ЛПБ) в текстовом формате. Обычно этот фрагмент содержит установки устройства, которые не управляются непосредственно *ЦУП,* например, таблица маршрутизации для устройства Cisco. Заказные ЛПБ можно создавать для любых видов Объектов Политики, кроме Объекта IP Хост или неуправляемого Объекта (потому что невозможно доставить ЛПБ этим Объектам). Можно написать фрагмент ЛПБ с помощью встроенного редактора или импортировать его из файла. В области *Структура ЛПБ* закладки *Управление->ЛПБ* окна *Свойства Объекта Политики* можно указать иерархию Заданных ЛПБ, относящихся к ЛПБ, которая генерируется автоматически, после перемещения этих ЛПБ вверх или вниз списка. Окончательная ЛПБ будет собрана из этих частей в указанном порядке, сверху вниз.

4.7.10. Домены

В *ЗАСТАВА-Управление* предусмотрена доменная модель. Эта модель реализует разграничение прав доступа к консоли *ЗАСТАВА-Управление* по принципу авторизации.

Домен представляет собой Объект, позволяющий описать:

– имя домена;

– связь с родительским доменом;

– текущую учетную запись пользователя и ее права;

– топологию, входящую в домен;

– учетные записи, действующие в домене;

– объекты политики;

– правила;

– зоны;

– расписания.

Домены образуют дерево, корневой домен называется Глобальным. Каждый домен связан с набором учетных записей. При подсоединении к консоли управления пользователь указывает имя учетной записи и ее пароль. В случае успешного ввода, учетная запись, под которой входил пользователь, становится текущей. Домен, который связан с текущей учетной записью, также становится текущим доменом.

4.7.10.1. Права учетных записей

Каждая учетная запись имеет права. При авторизации эти права распространяются на текущий домен и все домены, следующие вниз по иерархии. Права, которыми может обладать учетная запись: *активация, запись и управление учетными записями*.

Активация – право активировать ГПБ на хостах, относящихся к текущему домену. Правом на глобальную активацию и активацию обновленных *Агентов* имеет право только Глобальная учетная запись. Правом на трансляцию также обладает только Глобальная учетная запись.

Запись – право удалять, создавать и модифицировать объекты, относящиеся к текущему домену, за исключением самих доменов, учетных записей, а также диапазонов IP-адресов из числа задающих топологию самого домена.

Управление учетными записями – право удалять, создавать и модифицировать следующие объекты, относящиеся к текущему домену: сами домены, их подчинение другим доменам, учетные записи доменов, их имена, пароли, права, а также ограничения на адреса в домене. Право на управление учетными записями автоматически дает права *Активации* и *Записи*.

Глобальной учетной записью называется учетная запись, относящаяся к Глобальному домену и имеющая право управления учетными записями. Всегда должна быть хотя бы одна Глобальная учетная запись. В случае, если ее нет в БД сервера на момент запуска, сервер не

запускается. В случае, если ее нет в импортируемой БД, она создается (копируется имя и пароль текущей Глобальной учетной записи).

Право управления учетными записями имеет ряд исключений:

- для Глобального домена не допускается удаление, переименование, создание еще одного Глобального домена, введение ограничений на топологию, подчинение Глобального домена другим доменам;
- для текущего домена не допускается удаление, переименование и переподчинение другому домену;
- для текущей учетной записи не допускается удаление (как следствие - нельзя удалить последнюю Глобальную учетную запись), не допускается снятие с самой себя прав (как следствие – нельзя сделать последнюю Глобальную учетную запись неглобальной).

Для текущей учетной записи всегда допускается изменение ее пароля, а также возможность переименования при наличии права управления учетными записями.

Домены могут иметь ограничения по топологии. Внесение изменений в эти ограничения требует наличие права управления учетными записями. Помимо этого требуется, чтобы ограничения для подчиненных доменов были не ниже ограничений домена выше по иерархии.

Для каждого доменного пользователя можно сохранить свой список фильтров и индикаторов для работы с Журналом регистрации событий и журналом Syslog-сообщений.

4.7.11. Использование нескольких *ЦУП*

Можно применить несколько экземпляров *ЦУП* как часть всеобщей системы Безопасности. В данной установке *ЦУП* все *Агенты* во всеобщей Безопасной Среде должны определяться как Объекты Политики. Есть два варианта реализации сложных *ЦУП.*

Воспользоваться первым сценарием, если количество и местоположение Ваших *Агентов* делают неудобным наличие только одного установленного экземпляра или Вам будет удобнее, если некоторыми Объектами Политики будет управлять конкретный экземпляр *ЦУП,* а не иной другой. Сконфигурируйте Безопасную Среду так, чтобы каждый *Агент* получал свою ЛПБ от определенного экземпляра *ЦУП*. Только *Агенты*, которыми управляет каждая локальная установка *ЦУП,* должны определяться как управляемые Объекты в этом локальном *ЦУП*. Все *Агенты*, которые получают ЛПБ из другого экземпляра *ЦУП*, должны определяться

как неуправляемые Объекты в этом локальном *ЦУП*. В этом случае ЛПБ, БД и ГПБ будут разные на разных экземплярах *ЦУП*.

Воспользоваться вторым сценарием, если Вы хотите, чтобы *Агенты* в Безопасной Среде имели опцию загрузки ЛПБ из нескольких разных установок *ЦУП*. В этом случае определить всех *Агентов* как управляемые Объекты в каждой локальной установке *ЦУП*. При попытке загрузить ЛПБ *Агент* попробует загрузить ее с *ЦУП-Сервер*, который расположен в списке первым; если первый *ЦУП* недоступен, он попробует следующий в списке и т.д. В этом случае ЛПБ, БД и ГПБ будут одинаковые на каждом экземпляре *ЦУП*; все установки ниже первого по списку в основном действуют как «резервные устройства» для исходного *ЦУП*. Эта «иерархия» представлена в ЛПБ *Агентов*; в исходной ЛПБ *Агента* (т.е. перед тем, как будет загружена ЛПБ из *ЦУП*). Эта иерархия должна быть указана на токене или в файле, используемом для исходной ЛПБ. В этом случае рекомендуется сконфигурировать механизм SQL Database Replication, чтобы синхронизировать БД *ЦУП* более низкого уровня с БД исходного *ЦУП*.

Основная идея заключается в том, что *Агенты* могут загружать ЛПБ только с установки *ЦУП,* в которой этот *Агент* определяется как управляемый Объект. Если Вы используете несколько экземпляров *ЦУП,* главным образом, чтобы предоставить *Агентам* в Вашей Безопасной Среде несколько местоположений, с которых они смогут загружать свои ЛПБ, воспользуйтесь сценарием 2.

Если Вы используете несколько экземпляров *ЦУП,* чтобы управлять различными сетями, которые не объединены полностью друг с другом (принадлежат разным компаниям и т.д.), воспользуйтесь сценарием 1.

Например:

- Вы хотите, чтобы в каждом экземпляре *ЦУП* были описания всех *Агентов* в каждой сети, но чтобы нельзя было просмотреть ЛПБ *Агентов* в других сетях;
- Вы хотите, чтобы в каждом экземпляре *ЦУП* были описания всех *Агентов* каждой сети, но чтобы нельзя было просмотреть ГПБ в других экземплярах *ЦУП*.

4.8. Работа с ГПБ и Проектами

Различные вложенные окна и меню *ЦУП-Консоль* обеспечивают функции для работы, как с отдельной ГПБ, так и с «проектом» (ГПБ плюс Объекты Политики. *ГПБ* – это набор Правил, которые работают с набором Объектов Политики, в то время как *Проект* – это сумма Правил и Объектов Политики).

Проекты можно импортировать и экспортировать из *ЦУП*. Чтобы иметь несколько ГПБ, которые отличаются в некотором отношении (не только Правилами), Вы должны использовать разные Проекты. Импорт/экспорт XML-структур Проекта сохранит или восстановит все Объекты во всех окнах *ЦУП-Консоль*. Команды **Открыть** и **Сохранить** меню *Проект* загружают или сохраняют всю БД SQL Сервера *ЦУП* в/из файловой системы.

4.9. Построение ЛПБ для *Агентов*

ЛПБ для любого управляемого Защищённого *Агента* можно построить по-разному. Есть три основных метода построения ЛПБ *Агента*:

- Если ничего не добавлять и не изменять в ЛПБ по умолчанию, то ЛПБ будет вычислена автоматически для Защищённого *Агента* из ГПБ.
- Если ЛПБ для данного Защищённого *Агента* нужно больше информации, чем получено в результате автоматического вычисления ЛПБ, то фрагменты ЛПБ будут добавлены к началу или концу «автоматически созданной» ЛПБ. Это выполняется посредством создания Объектов, определяемых пользователем ЛПБ, и в импорте этих фрагментов из ЛПБ в ЛПБ Объекта. Местоположение этих фрагментов ЛПБ в окончательной ЛПБ зависит от позиции Объекта(ов), определяемой пользователем ЛПБ в закладке *Управление->ЛПБ* окна *Изменить Объект Политики*. Определяемые пользователем ЛПБ, помещенные над атрибутом **Автоматически созданная ЛПБ** будут добавлены в порядке сверху вниз, к началу «автоматически созданной» ЛПБ (см. Рисунок 16). Подобным образом, определяемые пользователем ЛПБ, помещенные под атрибутом, будут добавлены в порядке снизу вверх, к концу «автоматически созданной» ЛПБ.

Если Вы хотите определить одну, неизменную ЛПБ для отдельного Защищённого *Агента* (на которую не будут влиять изменения в ГПБ), надо сделать отметку в окне *Не транслировать ЛПБ* в закладке *Управление->ЛПБ* окна *Изменить Объект Политики*. Если отметка стоит, то ЛПБ *Агента* не будет обновляться, независимо от того, сколько изменений происходило с ГПБ, и сколько раз она была преобразована в ЛПБ. Активная ЛПБ будет применяться к *Агенту*, пока Вы не уберете отметку из соответствующего поля, пока снова не преобразуете и не активируете ГПБ.

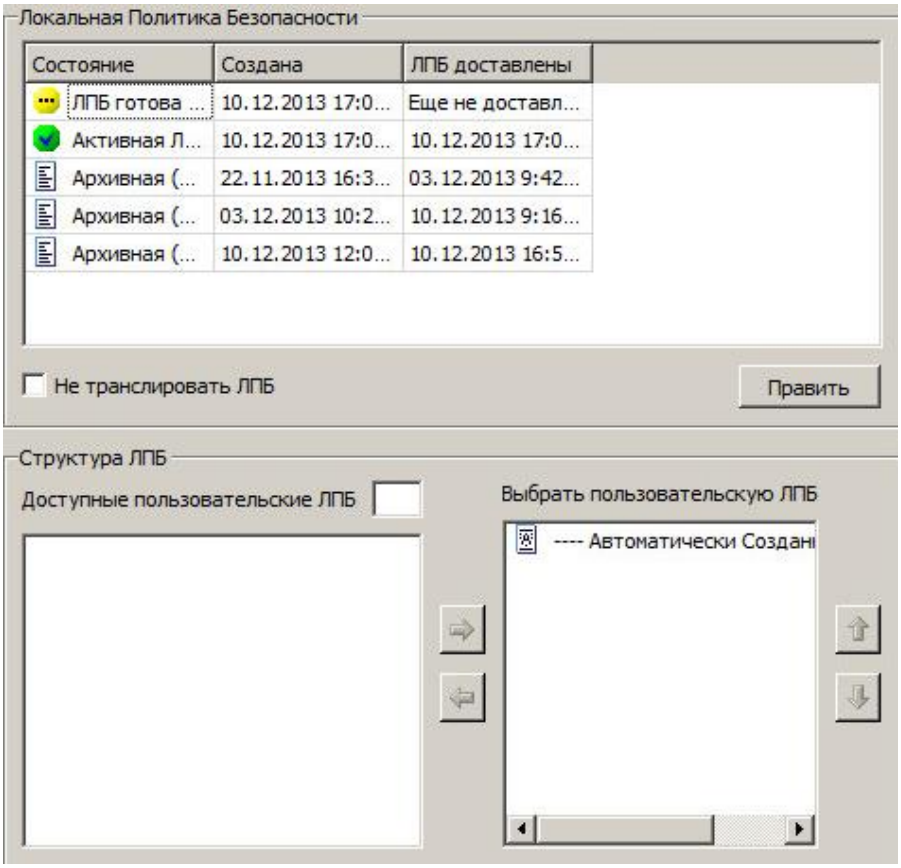

Рисунок 16 – Структура ЛПБ

ЛПБ должна быть сначала сгенерирована или импортирована для этого Объекта Политики!

4.10. Образец конфигурации *ЦУП*

Пошаговый пример конфигурирования ГПБ, ее преобразования в ЛПБ и активирование ЛПБ *Агентов* для базовой Среды Безопасности (*ЦУП* и два *ЗАСТАВА-Клиент*) см. Приложение 3. Пример конфигурирования *ЦУП*.

4.11. Использование удаленной *ЦУП-Консоль*

Если Вашему Администратору Безопасности нужен непрерывный, круглосуточный доступ к управлению центральной Политикой Безопасности из любой точки, можно сконфигурировать экземпляр *ЦУП-Консоль*, чтобы работать на расстоянии, например на портативном компьютере. Конфигурирование удаленной *ЦУП-Консоль* (см. раздел 5) предоставляет Администраторам Безопасности максимальные возможности в управлении корпоративной Политикой Безопасности. Например, один экземпляр *ЦУП-Консоль* можно установить и активировать на специализированной рабочей станции управления Политикой Безопасности, и можно управлять корпоративной ГПБ из этой точки в рабочие часы. Другой экземпляр *ЦУП-Консоль* можно установить на портативном компьютере Администратора

Безопасности, которым Администратор Безопасности будет пользоваться, если его нет в офисе. Все, что требуется от Администратора Безопасности, это выйти из «локальной» (находящегося в офисе) *ЦУП-Консоль* и затем зайти на удаленную *ЦУП-Консоль*. ГПБ можно безопасно управлять через сеть Интернет, используя туннелирующую технологию ВЧС, так как удаленная *ЦУП-Консоль* соединяется с БД, расположенной в корпоративном офисе через *ЗАСТАВА-Офис,* который защищает БД, и, таким образом, все административные функции, которые обычно осуществляются в офисе, можно выполнять удаленно. Инструкции по конфигурированию и удаленному использованию *ЦУП-Консоль* см. в подразделе 9.2.

5. Обзор *ЦУП-Консоль*

ГПБ создается и затем транслируется в ЛПБ в главном окне *ЦУП-Консоль*. Затем ЛПБ активируются на *Агентах* (*ЗАСТАВА-Клиент, ЗАСТАВА-Офис, Агенты* Microsoft IPsec, Cisco маршрутизаторы и PIX Firewalls), что включает отправку ЛПБ отдельному *Агенту*, группе выбранных *Агентов* или всем устройствам в Безопасной Среде и активацию ЛПБ. При обновлении ГПБ Администратор Безопасности может послать Политику обновления в виде новых ЛПБ всем *Агентам*. Если какая-то часть ЛПБ данного *Агента* больше не действительна в соответствии с обновленной ГПБ изменения будут сделаны автоматически и сразу. Можно сделать это, выбрав **Транслировать** из меню *Проект*, и после трансляции новая ГПБ будет активирована, если выбрать **Активировать** из меню *Проект*.

5.1. Главное окно *ЦУП-Консоль*

Главное окно состоит из строки меню, инструментальной линейки и окон просмотра. Для настройки отображения окон с параметрами необходимо воспользоваться параметрами меню *Окно*, в котором надо выбрать необходимые для отображения окна. Окно просмотра – это набор из субокон (секций главного окна), каждое из которых отображает разную информацию в разных вкладках.

1) *Топология* представляет топологию защищённой сети предприятия. Все Объекты Политики с известными IP-адресами, созданные в *ЦУП*, будут отображаться в графическом представлении *Топологии*. Объекты в *Графе топологии* соединены линиями, которые связывают Объекты друг с другом. Эти линии генерируются автоматически, на основе данных, которые содержатся в свойствах Объектов.
2) *Объекты политики* состоит из вкладок *Сетевые объекты*, *Пользователи*, *Группы*, каждая из которых представляет собой список соответствующих Объектов.
3) *Таблица Правил* отображает все Правила ГПБ в виде таблицы. *Таблица Правил* также позволяет определять иерархию Правил («вложенные Правила») и легко просматривать эту структуру. *Таблица Правил* отображает основные параметры Правил ГПБ: Объект(ы) Политики источника, Объект(ы) Политики Цели (Приемника), Сетевые Сервисы, Действие, уровень регистрации Правил ГПБ и Домен. *Таблица Правил* отображает все созданные Правила ГПБ и позволяет создавать, переключаться между уже созданными Правилами ГПБ, переименовывать и удалять их.

Можно изменить размеры каждой из областей относительно остальных, используя ползунковый регулятор.

5.1.1. Строка меню

Строка меню едина для всех секций и содержит следующие меню: *Проект, Править, Просмотр*, *Окно* и *Помощь*, которые включают в себя описанные ниже опции:

5.1.1.1. Меню *Проект*

Меню *Проект* содержит команды (см. Рисунок 17), описание команд представлено в таблице (см. Таблица 8).

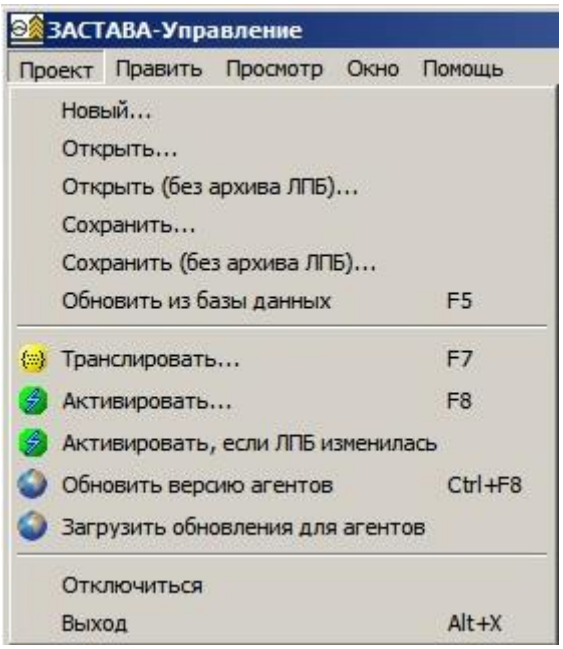

Рисунок 17 – Меню *Проект*

Таблица 8 – Описание команд меню *Проект*

Команда	Характеристика
Новый	Создание нового проекта
Открыть	Импорт Проекта из файла XML или GSP
Открыть (без архива ЛПБ)	Импорт Проекта без архивных ЛПБ
Сохранить	Экспорт данного Проекта в файл GSP
Сохранить (без архива ЛПБ)	Экспорт данного Проекта без ЛПБ
Обновить из БД F5	Обновление текущего проекта ГПБ из БД
Транслировать F7	Транслировать текущую ГПБ в ЛПБ для всех управляемых *Агентов*
Активировать F8	Активация ГПБ для всех Объектов Политики
Активировать, если ЛПБ изменилась	Активация ГПБ только для тех Объектов Политики, у которых ЛПБ в результате трансляции изменилась. Объекты, у которых оттранслированная ЛПБ совпадает с последней прогруженной, активироваться не будут. Данный механизм позволяет существенно снизить время активации ГПБ.
Обновить версию *Агентов*	Загрузка и установка обновлений *Агентами* с сервера обновлений
Загрузить обновления для *Агентов*	Загрузка *Агентами* обновлений с сервера обновлений

Команда	Характеристика
Выход Alt+X	Закрыть *ЦУП-Консоль*
Отключиться / Подключиться	Войти/ выйти из под авторизованной учетной записи пользователя

5.1.1.2. Меню *Править*

Меню *Править* содержит команды (см. Рисунок 18), описание команд представлено в таблице (см. Таблица 9).

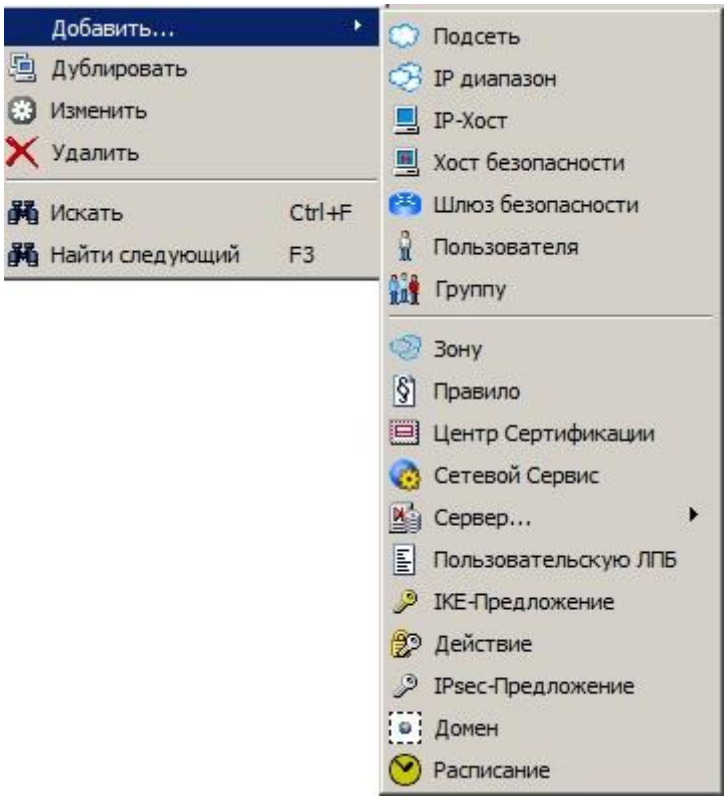

Рисунок 18 – Меню *Править*

Таблица 9 – Описание команд меню *Править*

Команда	Характеристика
Добавить->Подсеть	Добавить новый Объект - Подсеть
Добавить->IP Диапазон	Добавить новый Объект - IP-Диапазон
Добавить->IP Хост	Добавить новый Объект - IP Хост
Добавить->Хост Безопасности	Добавить новый Объект - Хост Безопасности
Добавить->Шлюз Безопасности	Добавить новый Объект - Шлюз Безопасности
Добавить->Пользователя	Добавить новый Объект - Пользователь
Добавить->Группу	Добавить новый Объект - Группа
Добавить->Зону	Добавить новый Объект - Зона
Добавить->Правило	Добавить новое Правило
Добавить->Центр Сертификации	Добавить УЦ
Добавить->Сетевой сервис	Добавить Сетевой сервис
Добавить->Сервер	Добавить Сервер из списка серверов
Добавить->Пользовательскую ЛПБ	Добавить Пользовательскую ЛПБ

Команда	Характеристика
Добавить->IKE-Предложение	Добавить IKE-Предложение
Добавить->Действие	Добавить Действие
Добавить->IPsec-Предложение	Добавить IPsec-Предложение
Добавить -> Домен	Добавить Домен
Добавить -> Расписание	Добавить Расписание
Дублировать	Начать процесс создания нового Объекта Политики на основании характеристик выбранного Объекта Политики
Изменить	Изменить свойства выбранного Объекта
Удалить Del	Удалить выбранный Объект (ы)
Искать Ctrl+F	Открыть окно поиска
Найти следующий F3	Найти следующий объект поиска

5.1.1.3. Меню *Просмотр*

Меню *Просмотр* содержит команды (см. Рисунок 19), описание команд представлено в таблице (см. Таблица 10). Для того что включить слежения за статусом или другой параметр меню *Просмотр*, надо поставить маркер, в виде галочки, напротив нужного пункта.

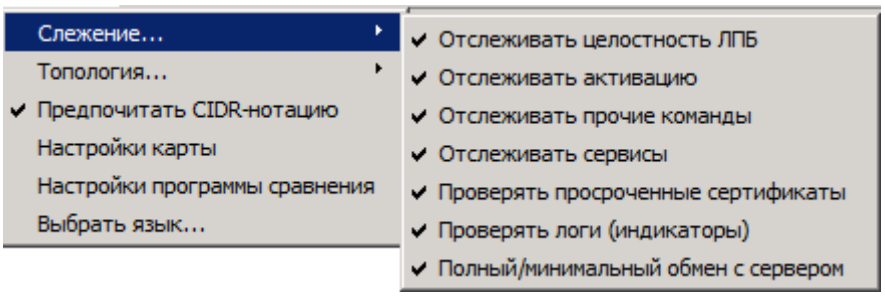

Рисунок 19 – Меню *Просмотр*

Таблица 10 – Описание команд меню *Просмотр*

Команда	Характеристика
Слежение -> Отслеживать целостность ЛПБ	Отобразить статус мониторинга целостности ЛПБ
Слежение -> Отслеживать активацию	Отобразить статус мониторинга активации ЛПБ
Слежение -> Отслеживать прочие команды	Отобразить статус мониторинга обновления версий *Агентов*, статус загрузки списка сертификатов, статус генерации ключевой пары и т.д.
Слежение -> Отслеживать сервисы	Показывать в правом нижнем углу *ЦУП-Консоли* состояние сервисов. Зеленый цвет означает работающий сервис, красный – не работающий
Слежение -> Проверять просроченные сертификаты	Отобразить список просроченных сертификатов

Команда	Характеристика
Слежение -> Проверять логи (индикаторы)	Отобразить список индикаторов
Слежение -> Полный/минимальный обмен с сервером	Оставить только два активных для выбора пункта в параметре Слежение: Отслеживать сервисы и Проверять просроченные сертификаты**.**
Автоматическая расстановка топологии	Запуск процесса автоматической расстановки Объектов в окне *Топология*
Экспорт расположения	Экспорт расположения Объектов в файл
Предпочитать CIDR-нотацию	Включить/Отключить без классовую адресацию
Настройки Карты	Вызов меню настроек *Карты*
Настройки программы сравнения	Вызов окна настройки программы сравнения ЛПБ
Выбрать язык	Выбор языка интерфейса

5.1.1.4. Меню *Окно*

Меню *Окно* содержит команды (см. Рисунок 20) для вывода в консоль новых окон с параметрами.

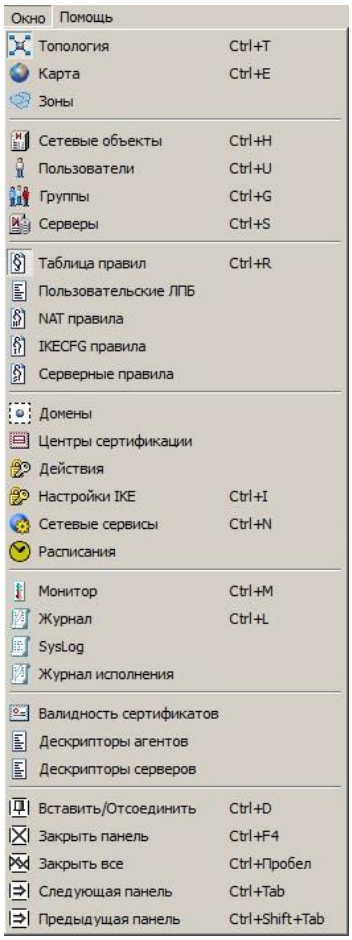

Рисунок 20 – Меню *Окно*

Описание характеристик команд меню *Окно* представлено в таблице (см. Таблица 11).

Таблица 11 – Команды меню *Окно*

Команда	Характеристика

Команда	Характеристика
Топология	Открыть окно просмотра топологии сети
Карта	Открыть окно просмотра *Карты*
Зоны	Открыть окно просмотра *Зон*
Сетевые Объекты	Просмотр окна списка *Сетевых объектов*
Пользователи	Просмотр окна списка *Пользователей*
Группы	Просмотр окна списка *Групп*
Серверы	Сконфигурировать инфраструктуру сервисов, установленных на Объектах Политики
Таблица правил	Просмотр окна Таблицы правил
Пользовательские ЛПБ	Работа с определяемыми пользователями ЛПБ
NAT правила	Работа с NAT-правилами
IKE CFG правила	Работа с IKECFG-правилами
Серверные правила	Работа с серверными правилами
Домены	Открыть окно просмотра существующих Доменов
Центры сертификации	Открыть окно просмотра существующих УЦ
Действия	Открыть окно просмотра существующих Действий
Настройки IKE	Открыть окно просмотра существующих настроек IKE
Сетевые Сервисы	Сконфигурировать фильтры протокола, используемые в Правилах ГПБ
Расписания	Открыть окно просмотра существующих Расписаний
Монитор	Открыть окно Монитор прогрузки ЛПБ. Контролировать активацию ГПБ и загрузку ЛПБ в *Агенты*
Журнал	Открыть окно просмотра Журнала регистрации событий
Syslog	Открыть окно просмотра журнала Syslog-сообщений
Журнал исполнения	Просмотр изменений в проекте, которые были автоматически сделаны при импорте или изменении дескриптора *Агента*
Валидность сертификатов	Просмотр сертификатов с истёкшим / истекающим сроком действия. *ЦУП-Консоль* автоматически отслеживает сертификаты с истёкшим сроком действия. В случае обнаружения таких сертификатов в строке статуса основного окна *ЦУП-Консоль* появляется мигающая иконка  . Нажатие на этой иконке открывает окно со списком сертификатов с истёкшим/ истекающим сроком действия
Дескрипторы Агента	Работа с набором дескрипторов Агентов
Дескрипторы Серверов	Работа с набором дескрипторов Серверов
Вставить/Отсоединить Ctrl+D	Вставить или отсоединить выбранное окно
Закрыть панель Ctrl+F4	Закрыть выбранную панель
Закрыть все Ctrl+Пробел	Скрыть все
Следующая панель Ctrl+Tab	Переход к следующей панели
Предыдущая панель Ctrl+Shift+Tab	Переход к предыдущей панели

5.1.1.5. Меню *Помощь*

Меню *Помощь* содержит команды (см. Рисунок 21), описание команд представлено в таблице (см. Таблица 12).

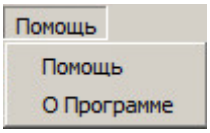

Рисунок 21 – Меню *Помощь*

Таблица 12 – Описание команд меню *Помощь*

Команда	Характеристика
Помощь	Вызов файла справки
О Программе	Открыть окно *О программе «ЗАСТАВА-Управление»* с информацией о ПК «VPN/FW «ЗАСТАВА»

5.1.2. Инструментальная линейка

В главном окне *ЦУП ЗАСТАВА-Управление* существует инструментальная линейка с дублированием функций меню *Править* (см. Таблица 13).

Таблица 13 – Описание доступных кнопок инструментальной панели *Графа топологии*

Кнопка	Характеристика	Кнопка	Характеристика
	Добавить подсеть		Добавить Сервер
	Добавить IP Диапазон		Добавить Пользовательскую ЛПБ
	Добавить IP Хост		Добавить IKE-Предложение
	Добавить хост безопасности		Добавить Действие или Предложение
	Добавить шлюз безопасности		Искать
	Добавить Пользователя		Дублировать
	Добавить Группу		Изменить
	Добавить Зону		Удалить
	Добавить Правило		Монитор
	Добавить ЦС		Журнал регистрации
	Добавить Сетевой сервис		Журнал регистрации Syslog

5.1.3. Работа с секциями *ЦУП*

Чтобы активировать одну из секций окна (окно второго уровня) и работать в ней, надо нажать на ней левой кнопкой мыши в любом месте этой секции.

Любую из секций окна можно выделить в отдельное окно, для этого необходимо выбрать секцию, которую Вы хотите выделить в отдельное окно, и нажать соответствующую команду меню *Окно*. При помощи меню *Окно* также можно переключаться между панелями, содержащими секции, и скрывать панели в случае необходимости.

5.2. Управление Объектами в *ЦУП-Консоль*

5.2.1. Контекстные меню

Можно управлять Объектами во вложенных окнах *ЦУП* через контекстные меню, которые отображаются при нажатии правой кнопкой мыши на Объекте или одном из его атрибутов. Опции, отображенные в контекстном меню – единственно доступные опции в данном контексте.

С помощью контекстного меню окна Объекты политики можно редактировать Тип *Агента*, для этого необходимо зайти в контекстное меню *Агента* и выбрать пункт *Изменить тип агента* и выбрать новые параметры дескриптора *Агента*. Доступно изменение Типа *Агента* для группы Объектов для этого необходимо выделить несколько объектов, выбрать пункт контекстного меню *Изменить тип агента* и выполнить в открывшемся окне необходимые изменения.

С помощью контекстного меню для типа дескриптора *Агента* версии 6.1 можно выполнить следующие действия:

- Сгенерировать ключевую пару на основе уже зарегистрированного у объекта сертификата;
- Скопировать содержимое сертификата или запроса на ключевую пару в буфер обмена;
- Скопировать содержимое сертификата или запроса на ключевую пару в файл;
- Заменить неподписанный сертификат подписанным в УЦ;
- Удалить созданный ранее запрос на регистрацию ключей;
- Загрузить сертификат и список сертификатов с *Агента*;
- Добавить полученный сертификат из *Агента* в ГПБ.

5.2.2. Создание Объектов

Все Объекты в *ЦУП-Консоль* создаются одинаково. Когда курсор установлен на соответствующем месте в одном из четырех окон (подробнее см. раздел 6), используйте

нажатие правой кнопки мыши для вызова контекстного меню и выбора соответствующего Объекта. Также создание возможно через меню *Править* (Править -> Добавить -> выбрать Объект).

Вы должны ввести уникальное имя для каждого Объекта данного вида в *ЦУП*. Это необходимо для того, чтобы не возникло никаких конфликтов в БД *ЦУП*. Кроме того, никогда не используйте в любом имени Объекта пробелы, символ тильды (~) или любые другие коды ASCII со значениями больше 128.

5.2.2.1. Дублирование Объектов

Можно облегчить и ускорить процесс создания Объектов Политики в секциях *Топология* и *Объекты Политики,* путём простого «дублирования» существующего Объекта. Это можно сделать, выбрав существующий Объект Политики и использовать команду **Дублировать** из главного или контекстного меню. При дублировании существующего Объекта, открывается окно *Дублировать* для создания нового Объекта; из дублированного Объекта все установки параметров, кроме тех, которые уникальны для каждого Объекта, копируются во всех закладках окна.

Например, установки интерфейса дублированного Объекта, IKE-сертификат и данные, подтверждающие подлинность, заранее согласованного ключа, не будут скопированы в новый Объект, потому что эти параметры должны иметь уникальные значения для каждого Объекта Политики. Заметьте, **Any** и **Internet** Объекты не могут быть дублированы.

5.2.3. Выбор нескольких Объектов

Можно выделить ряд смежных Объектов, помещая Объекты (в *Топологии*) в буксируемый и растягивающийся прямоугольник или, удерживая клавишу <Shift>, нажав на каждый Объект, свойства которого Вы хотите редактировать (во всех вложенных окнах).

После выделения Объектов, можно выбрать вид преобразований из строки меню или из контекстного меню. Заметьте, если команда контекстного меню недоступна для всех выделенных Объектов, она будет недоступна для группы выделенных Объектов.

5.2.4. Редактирование Объектов

Можно редактировать атрибуты Объекта, выделив Объект в окне программы и нажав клавишу <Enter>, двойным нажатием на Объекте левой клавишей мыши, а также выбрав команду **Изменить** из контекстного или главного меню.

5.2.4.1. Одновременное редактирование нескольких Объектов

Свойства нескольких Объектов Политики можно редактировать одновременно. Надо выделить ряд смежных Объектов, помещая Объекты (в секции *Топология*) в буксируемый, растягивающийся прямоугольник, или, удерживая клавишу <Shift>, выделить Объекты, свойства которых Вы хотите редактировать (во всех вложенных окнах). В меню *Править*

нужно выбрать команду **Изменить,** появится список свойств отдельного Объекта Политики, эти свойства можно редактировать для всей Группы. Заметьте, доступны будут только те свойства, которые имеют значение для всех выделенных Объектов.

Изменить значение нужного параметра в появившемся диалоговом окне. Данное значение параметра будет изменено для всех выделенных Объектов.

5.2.5. Перемещение Объектов

Чтобы переместить Объекты Политики в секции *Топология* необходимо выбрать Объект(ы) и переместить его(их) в нужное место.

5.2.6. Размещение Объектов Политики

5.2.6.1. Автоматическая расстановка топологии

В *ЗАСТАВА-Управление* реализована функция автоматической расстановки Топологии, для вызова последней необходимо воспользоваться меню *Просмотр*. Автоматическая расстановка Топологии приведет расположение объектов к максимально симметричному виду, например, если несколько Объектов Политики принадлежат Зоне, Объекты Политики будут распределяться по кругу вокруг Объекта Зона.

5.2.6.2. Размещение Объектов вручную

Чтобы разместить Объекты Политики вручную в *Графе топологии* надо выделить их и переместить в другое место.

5.2.7. Удаление Объектов

Выделенные Объекты можно удалить с помощью команды **Delete**. Несколько Объектов Политики, включая узлы концентраторов, соединители можно удалять одной командой. Надо выделить ряд смежных Объектов, помещая их в растягивающийся буксируемый прямоугольник (во вложенном окне *Топология*), или, удерживая клавишу <Shift>, выделить Объекты, которые Вы хотите удалить. Затем используйте команду **Delete**. Заметьте, **Any**, **Internet** и **Internet Zone** Объекты нельзя удалить. Объекты Политики, удаленные во вложенных окнах секций *Топология* или *Объекты политики* будут автоматически удалены из других секций, тем не менее, в *Таблице Правил* Объекты Политики – это только «ссылки для быстрого вызова» Объектов, и они не будут отображаться только в тех вложенных окнах, в которых они «удалены». Удаление члена Группы – это лишь удаление Объекта Политики из Группы, а не самого Объекта.

При удалении объектов, которые участвуют в IKECFG-правилах, выводится предупреждения о том, что объект участвует в IKECFG-правилах. Если удалить объект, который является единственным участником правила, то удалится все IKECFG-правило. Если в IKECFG-правиле объект политики не является единственным участником, то этот объект удалится из IKECFG-правила.

5.2.8. Поиск информации

Чтобы быстро найти информацию в *ЦУП* надо использовать команды **Найти** и **Найти следующий.** Эти команды позволяют осуществлять поиск всей информации во вложенном окне или более узкий поиск по типу информации, которую Вы ищете. Сначала выбрать вложенное окно, в котором Вы хотите осуществить поиск. Поиск производится только в выделенном вложенном окне. Затем нажать клавиши <Ctrl>+<F>.

5.2.8.1. Использование окна поиска

Окно поиска позволяет найти требуемые Объекты ГПБ (см. Рисунок 22).

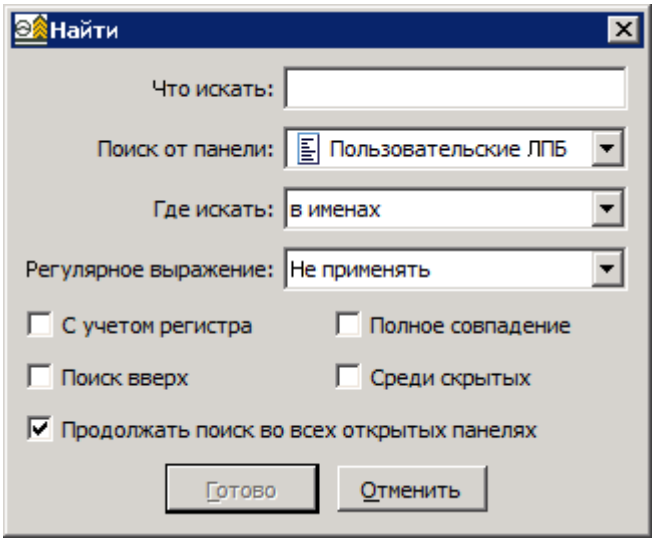

Рисунок 22 – Окно поиска

Поиск требуемых Объектов выполняется следующим образом:

1) Ввести информацию (буквенно-цифровую строку), которую Вы ищете, в поле **Что искать**. Это может быть целый параметр или любая его часть.
2) Выбрать панель, в которой будет производиться поиск. Для этого надо использовать выпадающее меню *Поиск в панели*.
3) Выбрать область поиска. Выбор области поиска зависит от выбранной панели. Ограничить дальнейший поиск, для этого надо указать, использовать ли для поиска полное совпадение или поиск вверх по списку.
4) Чтобы поиск проходил с учетом регистра клавиатуры или только по целой строке, надо сделать отметку в соответствующем окне.
5) Чтобы искать, используя регулярные выражения, надо сделать отметку в этом окне.
6) Чтобы искать во всех открытых панелях, надо сделать отметку в соответствующем окне.

7) Чтобы поиск осуществлялся среди скрытых объектов, надо сделать сделать отметку в соответствующем окне.

Поиск следующего вхождения: Нажать клавишу <F3>, чтобы найти следующее вхождение данных, которые Вы ищете.

5.2.9. Фильтрация отображения Правила

ЦУП позволяет Вам отображать только выбранные Правила ГПБ. Для этого необходимо выбрать интересующие Правила последовательным нажатием мыши с зажатыми клавишами <Ctrl> или <Shift>, затем, используя команду **Скрыть остальные** контекстного меню, скрыть ненужные для отображения Правила (см. Рисунок 23).

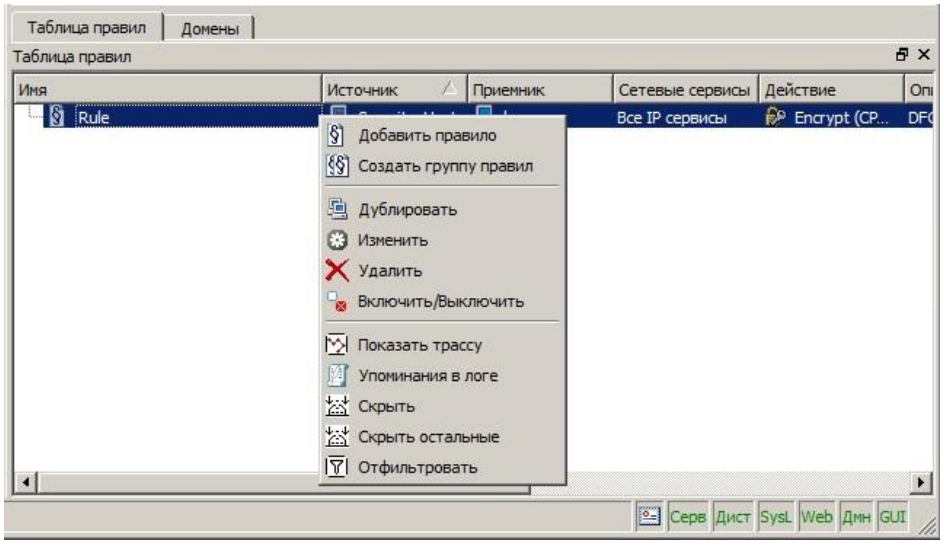

Рисунок 23 – Контекстное меню окна *Таблица правил*

Фильтрация Правил настраивается с помощью окна *Отфильтровать* (см. Рисунок 24). Для запуска этого окна, необходимо выбрать пункт контекстного меню *Отфильтровать* окна *Таблица правил*.

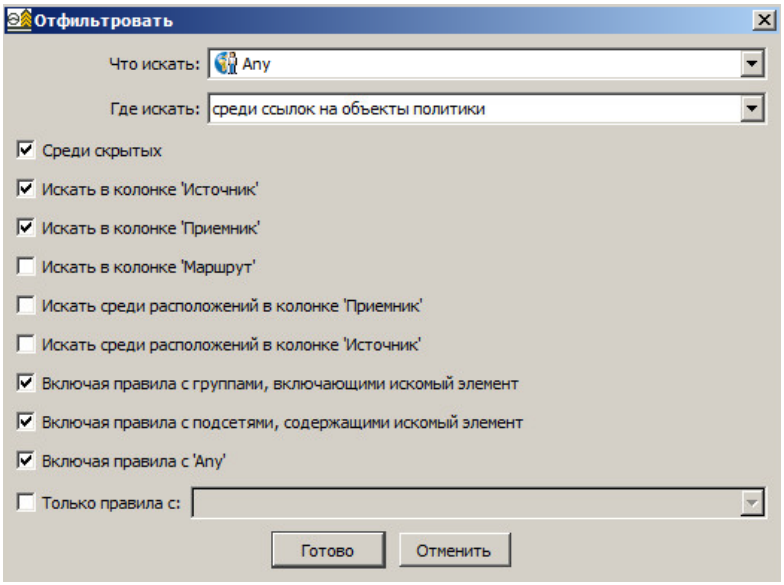

Рисунок 24 – Фильтрация отображения Правил

Поиск требуемых Правил выполняется следующим образом:

1) В **Где искать** выбрать, по каким полям будет производиться поиск Правил: **ID в БД**, **Имя**, **Описание**, **Действие**, **Объект политики**, **Расписание**, **Сетевой сервис**.
2) Ввести информацию (буквенно-цифровую строку), которую Вы ищете в поле **Что искать.**

Поиск следующего вхождения: Нажать клавишу <F3>, чтобы найти следующее вхождение данных, которые Вы ищете.

Чтобы вернуть скрытые Правила в список отображаемых необходимо использовать команду **Раскрыть** контекстного меню на вкладке скрытых Правил (см. Рисунок 25).

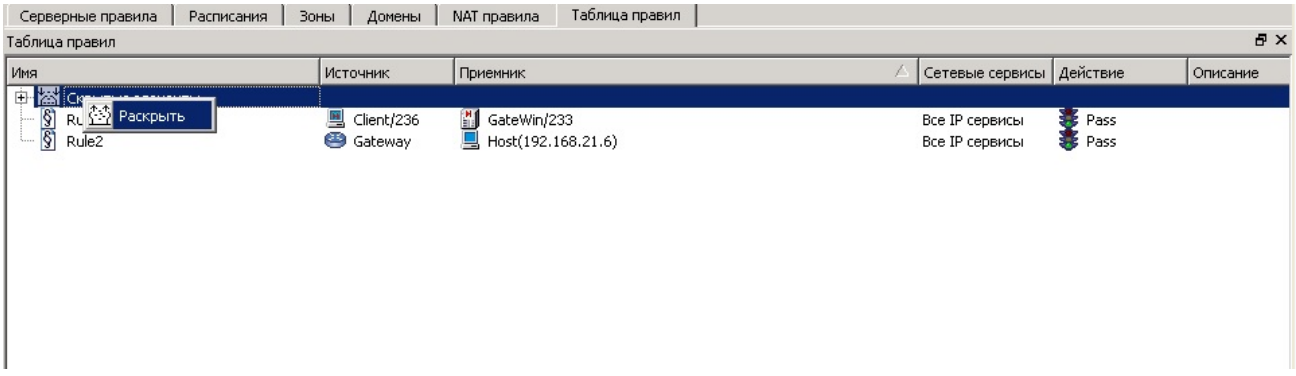

Рисунок 25 – Фильтрация отображения Правил

Другая доступная опция контекстного меню *Таблицы Правил* – команда **Скрыть** (см. Рисунок 23). Действие этой команды противоположно действию команды **Скрыть остальные** – она скрывает выбранные Правила во вкладку *Скрытые*.

Чтобы вернуть скрытые Правила в список отображаемых необходимо использовать команду **Раскрыть** контекстного меню на вкладке *Скрытых Правил*.

5.2.10. Сортировка информации

В секции *Таблица Правил* и в секциях *Объектов политики (Сетевые объекты, Пользователи и Группы)* можно сортировать информацию в столбцах таблицы. Чтобы отсортировать Объекты в определенном столбце надо нажать на заголовок столбца. Первое нажатие сортирует в возрастающем порядке (0-9, A-Z), следующее нажатие отсортирует в убывающем порядке (Z-A, 9-0).

Процедура сортировки происходит по следующим Правилам:

– Сортируется текст данной клетки таблицы;

– Если клетка содержит несколько Объектов, то имена этих Объектов будут добавлены в строку в том порядке, в котором они находятся в клетке и эта строка будет использована для сортировки.

– Вложенные Правила, также можно сортировать, но только в рамках Родительского Правила.

5.2.11. Фильтр поиска для Объектов политики

В секции *Объекты политики (Сетевые объекты, Пользователи и Группы)* можно настроить фильтр поиска Правил, связанных с конкретным *Объектом*. Контекстное меню секции *Объекты политики* показано на рисунке (см. Рисунок 26).

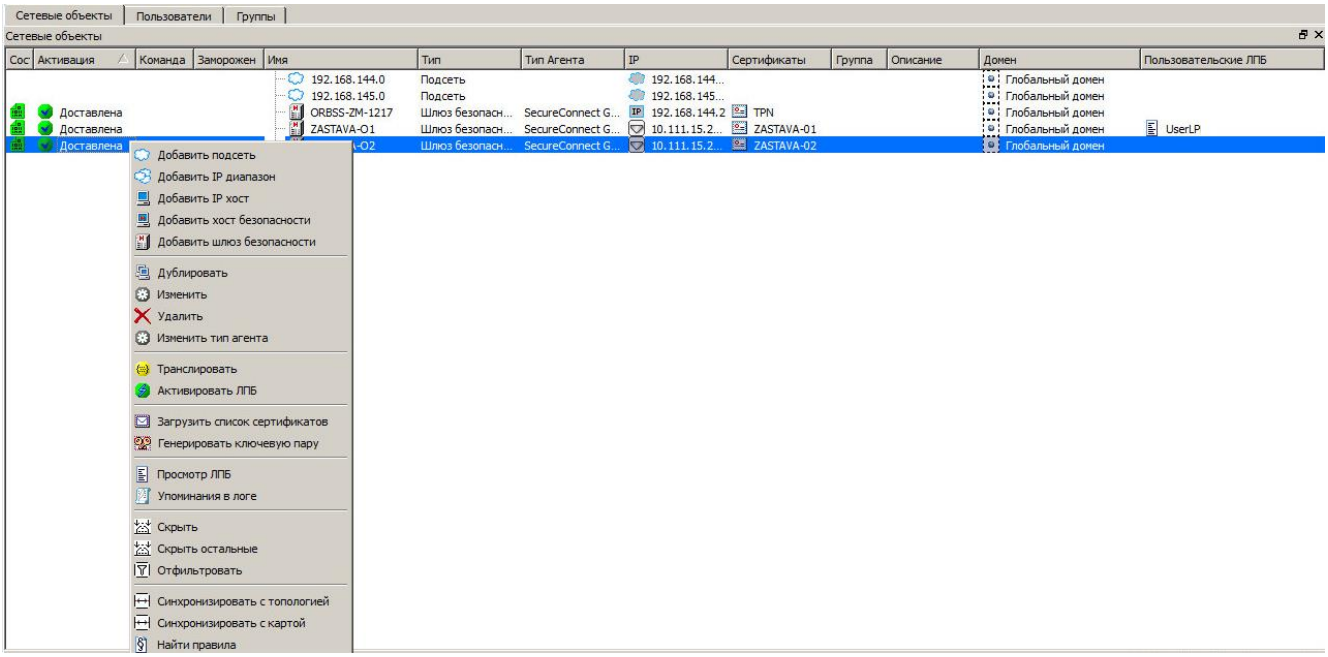

Рисунок 26 – Контекстное меню окна *Объекты*

Фильтрация Правил настраивается с помощью окна *Найти и отфильтровать* (см. Рисунок 27). Для запуска этого окна, необходимо выбрать пункт контекстного меню *Найти правила* секции *Объекты политики*.

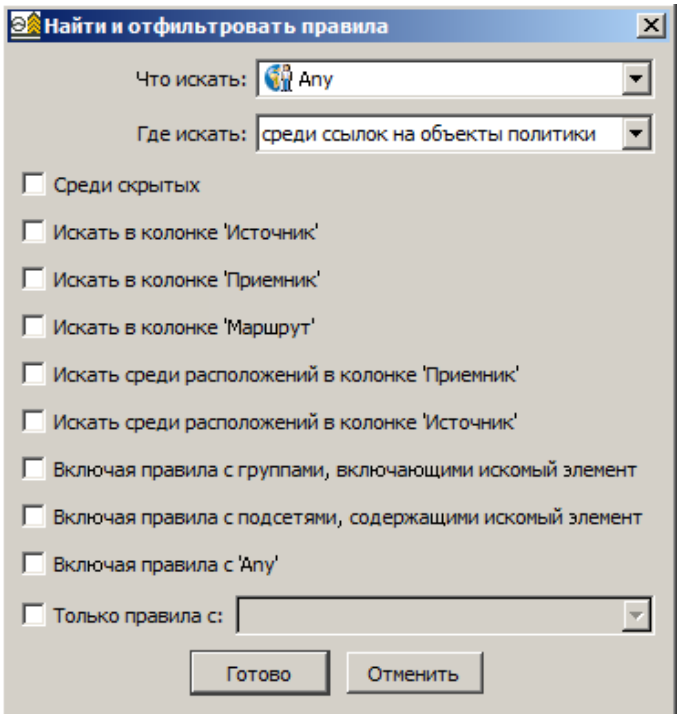

Рисунок 27 – Фильтрация отображения Правил

Поиск требуемых Правил выполняется следующим образом:

1) В **Где искать** выбрать, по каким полям будет производиться поиск: **ID в БД**, **Имя**, **Описание**, **Действие**, **Объект политики**, **Расписание**, **Сетевой сервис**.
2) Ввести информацию (буквенно-цифровую строку), которую Вы ищете в поле **Что искать**.

5.2.12. Комбинации клавиш для быстрого доступа к командам

Для удобства работы с *ЗАСТАВА-Управление* некоторые команды главного и контекстного меню дублируются специальными комбинациями клавиш на клавиатуре. Набор доступных команд зависит от того, в какой секции Вы работаете, и какой объект выбран. Ниже приведен полный список сокращённых клавиатурных команд.

5.2.12.1. Сокращённые клавиатурные команды для всех секций графического интерфейса *ЦУП-Консоли*

При помощи сокращенных клавиатурных команд в секциях графического интерфейса *ЦУП-Консоли* можно выполнять действия по перезагрузке Проекта, транслирования ГПБ и др. (см. Таблица 14).

Таблица 14 – Сокращенные клавиатурные команды в секциях графического интерфейса *ЦУП-Консоли*

Обозначение	Команда
F7	Транслировать ГПБ
F8	Активировать ГПБ для всех Объектов Политики

Alt+F4	Закрыть *ЦУП*
Ctrl+F8	Обновить версию *Агентов*

5.2.12.2. Сокращённые клавиатурные команды для вызова необходимых окон

В таблице (см. Таблица 15) представлен список сокращенных клавиатурных команд для быстрого вызова необходимых окон (эти команды дублируют соответствующие пункты меню *Окно*).

Таблица 15 – Сокращенные клавиатурные команды для вызова необходимых окон

Обозначение	Команда
Ctrl+T	Вызов окна *Топология*
Ctrl+E	Вызов окна *Карта*
Ctrl+M	Вызов окна *Монитор*
Ctrl+L	Вызов окна *Журнал*
Ctrl+H	Вызов окна *Сетевые Объекты*
Ctrl+U	Вызов окна *Пользователи*
Ctrl+G	Вызов окна *Группа*
Ctrl+R	Вызов окна *Таблица Правил*
Ctrl+N	Вызов окна *Сетевые Сервисы*
Ctrl+S	Вызов окна *Серверы*
Ctrl+I	Вызов окна *Настройки IKE*
Команды управления окнами	
Ctrl+D	Вставить/Отсоединить
Ctrl+F4	Закрыть Панель
Ctrl+Пробел	Закрыть Все
Ctrl+Tab	Следующая панель
Ctrl+Shift+Tab	Предыдущая панель

5.2.12.3. Общие сокращённые клавиатурные команды

При помощи общих сокращённых клавиатурных команд можно копировать, вырезать, вставлять текст и т.д. (см. Таблица 16).

Таблица 16 – Общие сокращённые клавиатурные команды

Обозначение	Команда
Ctrl+C	Скопировать выбранный элемент в буфер обмена
Ctrl+X	Удалить выбранный элемент и поместить его в буфер обмена
Ctrl+V	Вставить содержимое буфера обмена
Ctrl+A	Выбрать все объекты в активном окне
Delete	Удалить выбранный объект

Обозначение	Команда
Enter	Отобразить свойства выбранного Объекта Политики
Ctrl+F	Найти строку текста

6. Вложенные окна *ЦУП-Консоль*

6.1. Топология

Секция *Топология* предназначена для представления топологии Вашей сети в как можно более понятном, графическом виде (см. Рисунок 28). В данной секции можно создавать, редактировать и удалять Объекты Политики.

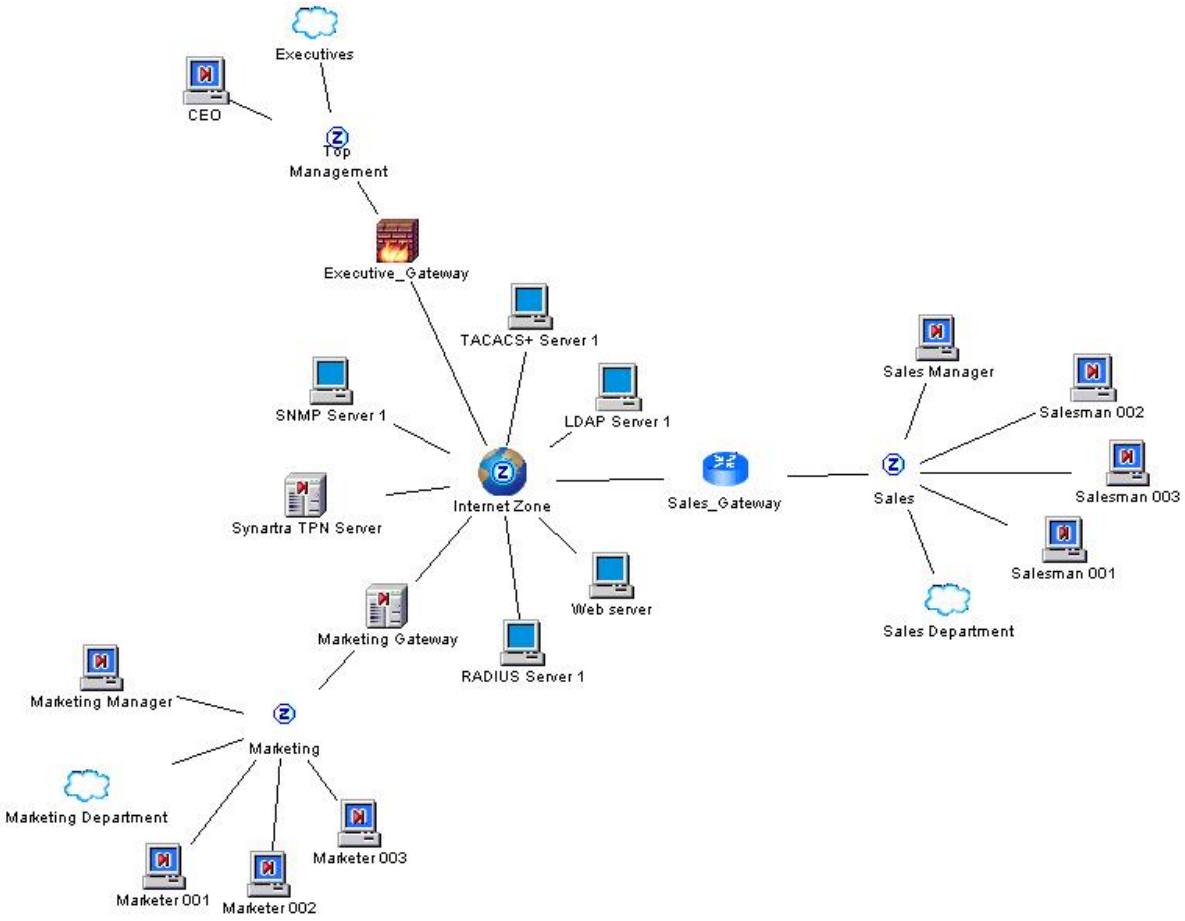

Рисунок 28 – Отображение Графа Топологии

Все Объекты Политики, созданные в данном Проекте, (за исключением Пользователей и Групп), будут отображаться в этой секции. При создании Проекта в *Графе топологии* будут присутствовать только «технологический» объект **Internet Zone** и Шлюз Безопасности, представляющий *ЦУП-Сервер*.

Объекты в *Графе топологии* соединяются друг с другом автоматически на основании связей между адресными пространствами сетевых объектов и Объектов **Зона**. Соединения строятся на основании принадлежности Объекта к защищенному периметру, т.е. **Зоне.**

Все Объекты Политики, включая Объекты **Подсеть** и **IP-диапазон** (за исключением Подсетей, не привязанных к Зонам), чьи IP-адреса являются частью адресного пространства

Зоны, будут автоматически соединяться с этой Зоной линией связи. В противном случае они будут автоматически соединяться с Объектом **Internet Zone**.

Если у Объекта **Шлюз Безопасности** несколько интерфейсов, то он может соединяться с несколькими Зонами одновременно. Объекты **Хост Безопасности** всегда должны принадлежать только одной Зоне. Если у Объекта сети несколько интерфейсов, чьи IP-адреса все принадлежат одной Зоне, связь будет всё равно представлена на дисплее одной линией.

В окне *Топологии* доступна своя инструментальная линейка (см. Таблица 17).

Таблица 17 – Описание доступных кнопок инструментальной панели Т*опологии*

Кнопка	Характеристика	Кнопка	Характеристика
	Уместить в окно		Повернуть вправо
	Уменьшить масштаб		Повернуть влево
	Увеличить масштаб		Размер иконок
	Показать имена Объектов в Окне топологии		Показать надписи для связей в Окне топологии
	Ограничить количество отображаемых в Окне топологии узлов		

6.2. Карта

Окно *Карта* позволяет видеть расположение Объектов Политики на карте Земного Шара (см. Рисунок 29).

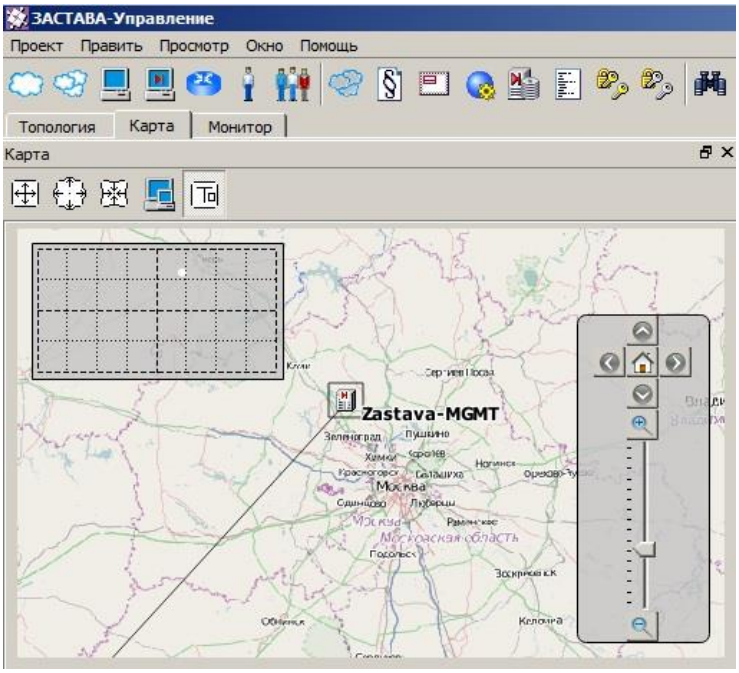

Рисунок 29 – Окно *Карта*

Окно масштабируется ползунком, расположенным в правой части секции, здесь же предусмотрены клавиши движения вправо/влево и вверх/вниз для перемещения по *Карте*. Также для этого доступен манипулятор мышь с зафиксированной левой кнопкой.

В окне *Карта* доступна своя инструментальная линейка (см. Таблица 18).

Таблица 18 – Описание доступных кнопок инструментальной панели окна *Карта*

Кнопка	Характеристика	Кнопка	Характеристика
	Уместить в окно		Увеличить масштаб
	Уменьшить масштаб		Размер иконок
	Показать имена		

Контекстное меню окна *Карты* позволяет добавлять Объекты Политики (см. Рисунок 30).

Для того, чтобы Объект Политики отображался на карте, необходимо указать его географические координаты во вкладке *Местоположение* свойств Объекта. Координаты можно ввести вручную или присвоить их Объекту, выбрав кнопку **Указать координаты** и перемещая появившийся флажок с помощью мыши. В этом окне также возможно масштабирование через ползунковые регуляторы.

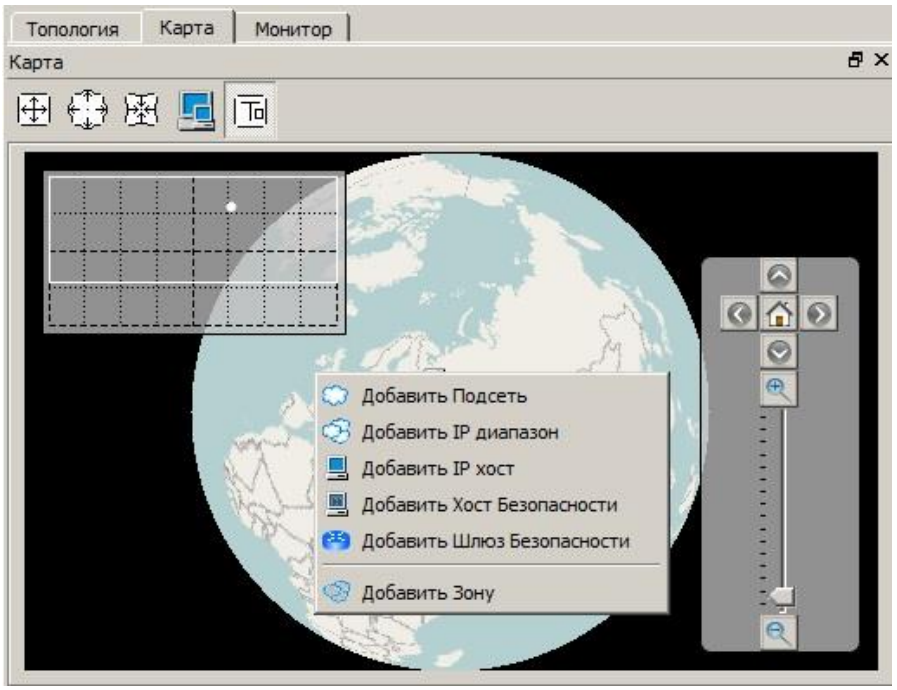

Рисунок 30 – Контекстное меню окна *Карта*

6.3. Зоны

Окно *Зоны* отображает Зоны (пространства IP-адресов, защищенных Шлюзом Безопасности) в виде таблицы. В таблице показана информация о каждой Зоне: Имя, Тип, Описание, IP-адреса, Шлюзы, Области, Хосты и Домен.

Контекстное меню окна *Зоны* позволяет добавлять/удалять Зону (см. Рисунок 31).

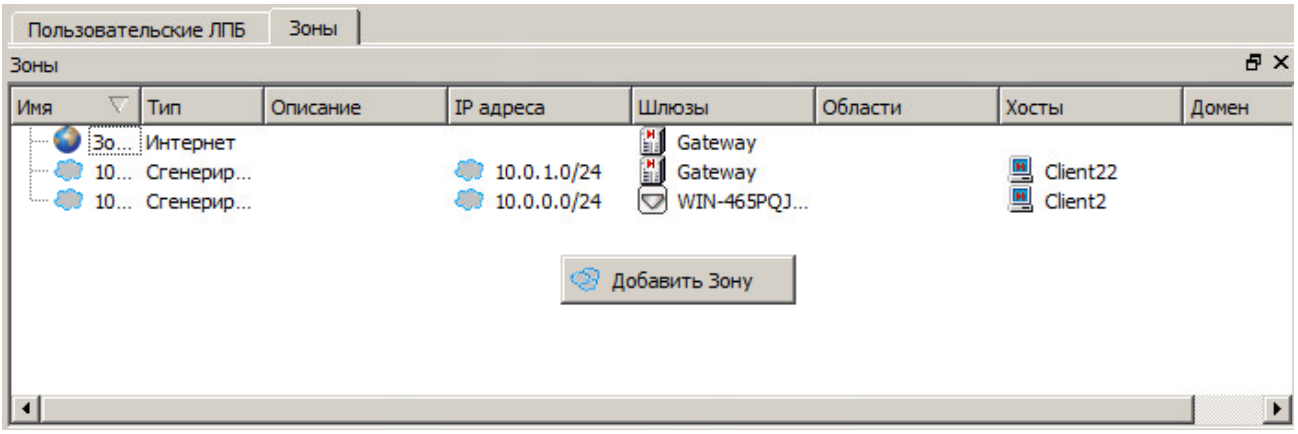

Рисунок 31 – Окно *Зоны*

6.4. Секция Объекты Политики

Секция *Объекты Политики* предназначена для тех случаев, когда просмотр Объектов Политики в виде таблицы удобнее. Так, например, когда Вам нужно просмотреть *Таблицу объектов*, отсортированные по типу, версии *Агента*, IKE-идентификаторам, членству в Группе и т.д. Более того, секция *Объекты политики* – единственная секция, в которой отображаются Объекты Пользователь и Группа. Все Объекты Политики могут создаваться, редактироваться и удаляться в секции *Объекты Политики*. Исключением являются Объекты Зона, которые формально не являются Объектами Политики, поскольку не могут участвовать в Правилах; Объекты Зона отображаются только в секции *Топология*.

Секция *Объектов Политики* представлена окном и вкладками, которые можно добавить или удалить по желанию. При переключении между вкладками происходит отображение соответствующей информации в окне *Секции Политики* (см. Рисунок 32).

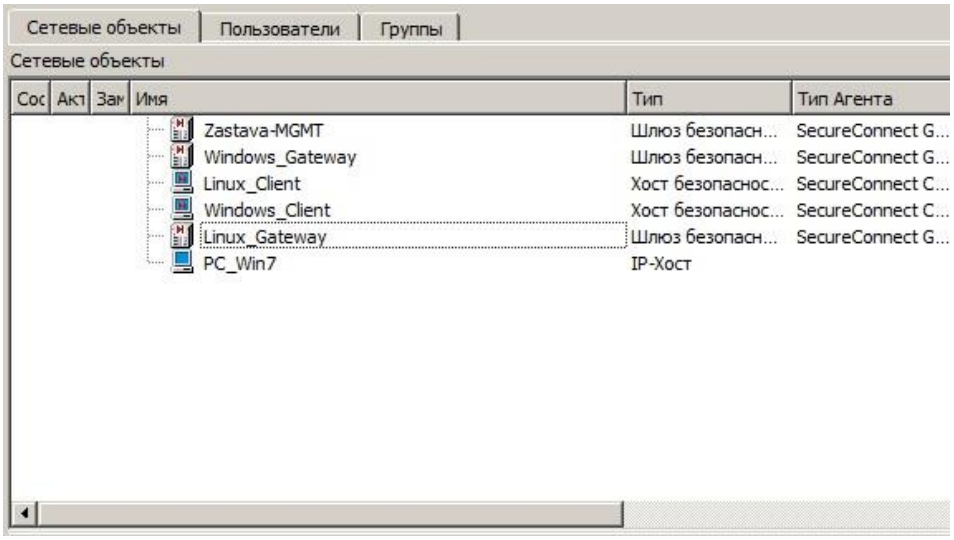

Рисунок 32 – Секция *Объекты Политики*

6.5. Серверы

Окно *Серверы* содержит список Серверов в виде таблицы с указанием следующей информации: Имя, Тип, Владелец (Объект Политики, который выполняет функции Сервера), IP-адрес и Опции (см. Рисунок 33). По каждому из параметров возможна сортировка списка.

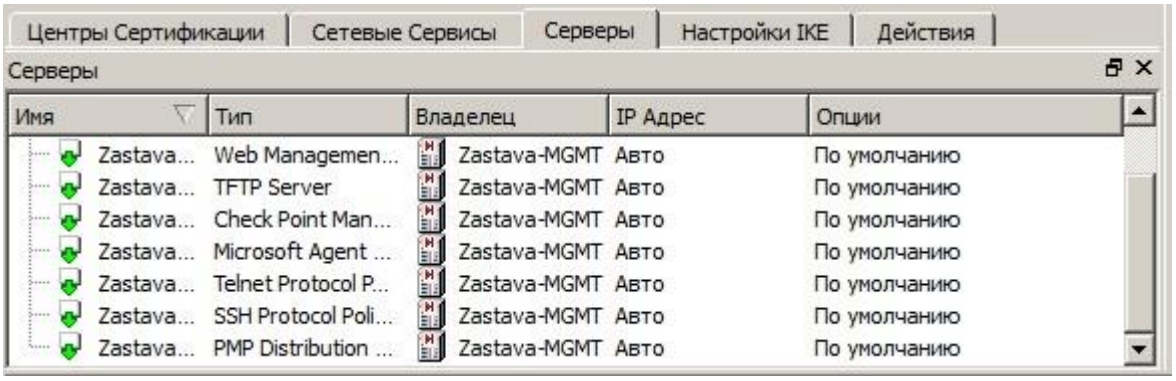

Рисунок 33 – Окно *Серверы*

6.6. Таблица Правил

Таблица Правил отображает все Правила в ГПБ в форме таблицы (см. Рисунок 34). В таблице показана информация о каждом Правиле в ГПБ: его **Имя**, Объект(ы): **Источник**, **Приемник**, любые используемые **Сетевые Сервисы**, **Действие**, которое будет применяться, **Описание**, **Маршрут**, **Расписание**, уровень регистрации Правила (**Уровень лога**) и его **Домен**. Этот просмотр особенно удобен, если Вы используете иерархию Правил, поскольку вложенные Правила будут отображаться сразу под родительскими Правилами. В этой секции можно создавать, редактировать и удалять Правила, а также работать с иерархической структурой Правил.

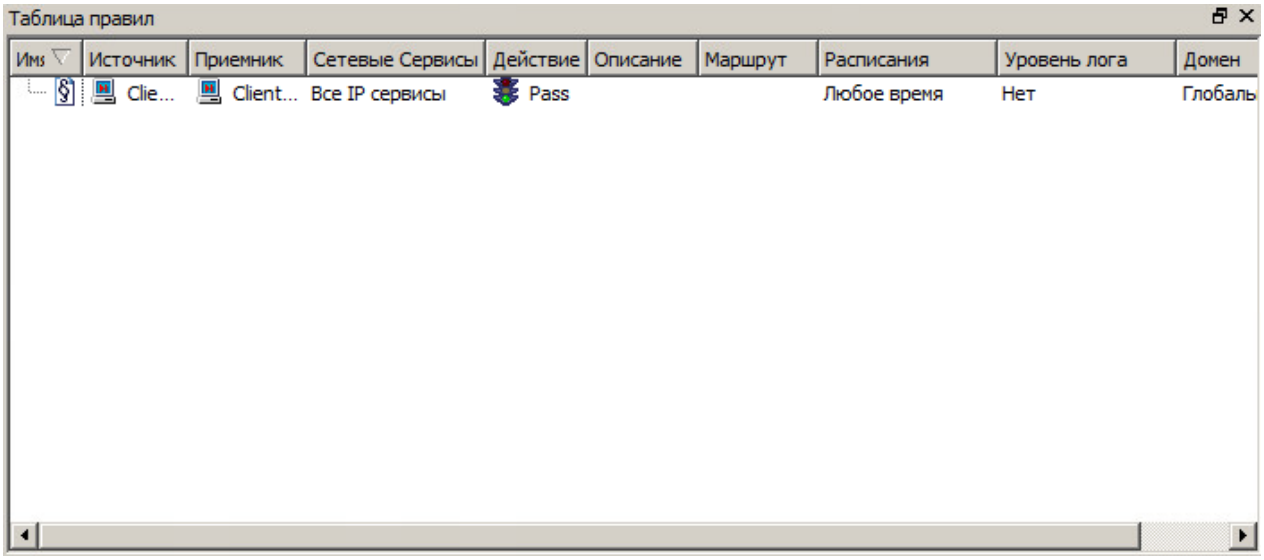

Рисунок 34 – Окно просмотра *Таблицы Правил*

Контекстное меню окна *Таблицы Правил* позволяет создавать Новое Правило или Группу Правил и настроить фильтрацию правил (см. Рисунок 35).

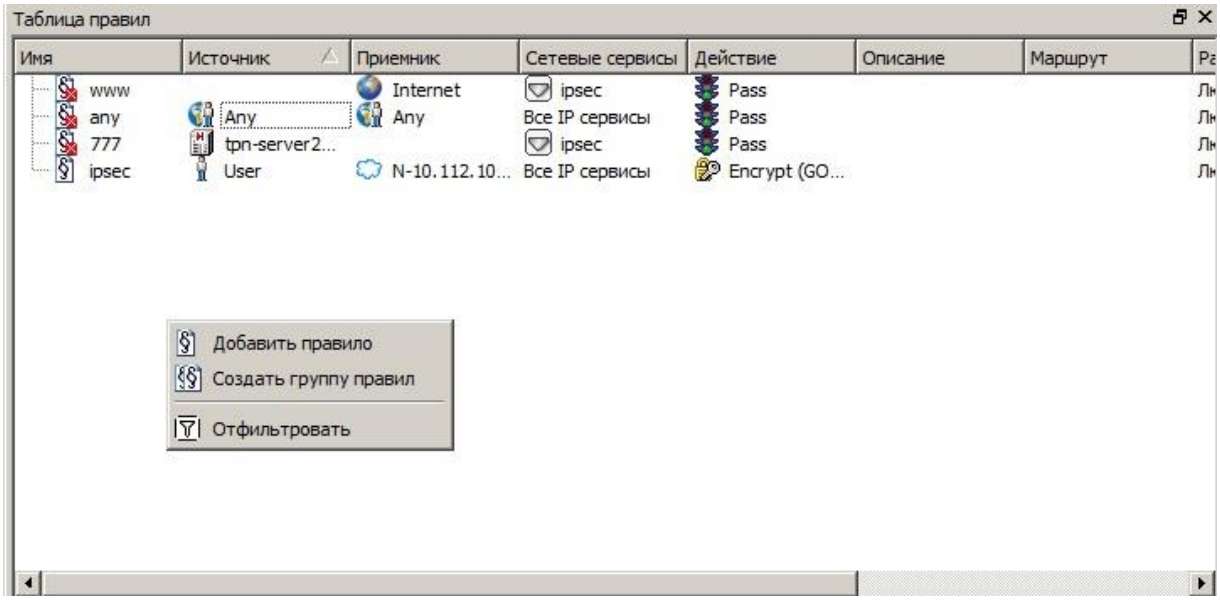

Рисунок 35 – Контекстное меню окна *Таблица Правил*

6.7. Пользовательские ЛПБ

Окно *Пользовательские ЛПБ* отображает список определяемых Пользователем ЛПБ – часть ЛПБ в текстовом формате (см. Рисунок 36).

Контекстное меню окна *Пользовательские ЛПБ* позволяет добавлять новую Пользовательскую ЛПБ.

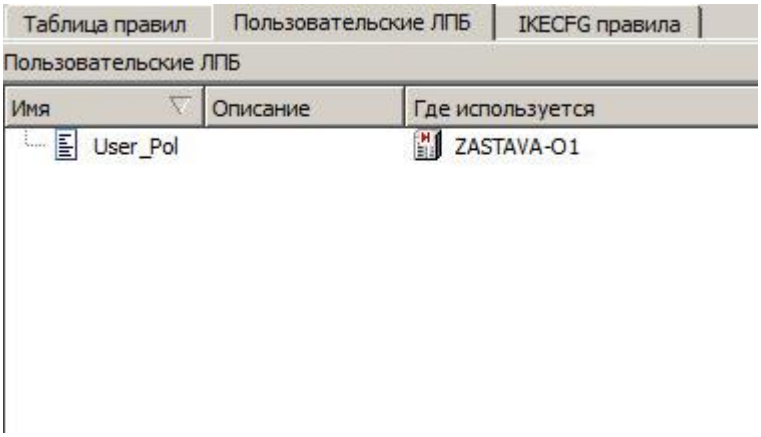

Рисунок 36 – Окно *Пользовательские ЛПБ*

6.8. NAT правила

Окно *NAT правила* отображает список NAT Правил созданных в закладке *NAT Правила* в *Объектов Политики* (см. Рисунок 37). Окно NAT Правила отображает все NAT Правила в ГПБ в форме таблицы. В таблице показана информация о каждом Правиле NAT в ГПБ: **Устройство**, на котором создано правило, **Тип NAT** - динамический или статический, **Источник исходного пакета**, **Приемник исходного пакета**, **Исходный сетевой Сервис**, **Источник преобразованного пакета**, **Приемник преобразованного пакета, Преобразованный сетевой Сервис, интерфейс**.

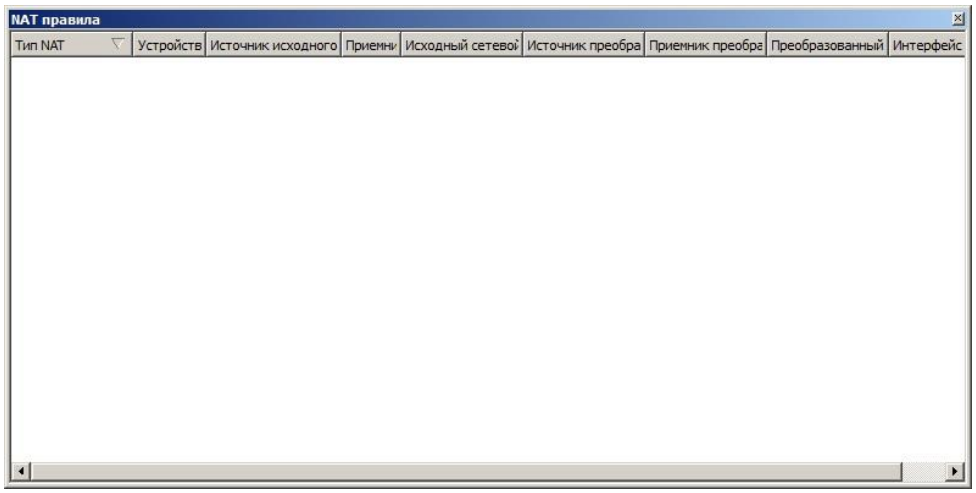

Рисунок 37 – Окно *NAT правила*

6.9. IKE CFG правила

Окно *IKE CFG правила* отображает список **IKE CFG правил**, созданных в закладке *IKE CFG Объектов Политики* (см. Рисунок 38). Окно *IKE CFG правила* отображает все **IKE CFG правила** в ГПБ в форме таблицы. В таблице показана информация о каждом **IKE CFG**

правиле в ГПБ: Ресурс IP-адресов, Устройство, на котором создано правило, Объект политики, Broadcast маска, DNS-серверы.

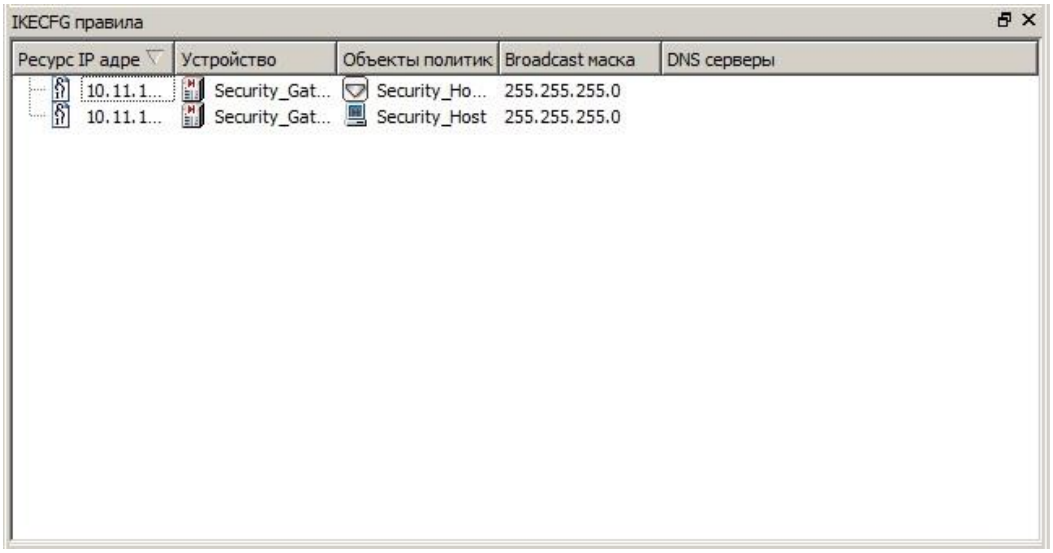

Рисунок 38 – Окно *IKE CFG правила*

6.10. Серверные правила

Во многих местах графического интерфейса *ЦУП-Консоли* используется универсальный элемент управления, предназначенный для привязки к редактируемому Объекту серверов различного типа (Серверы прогрузки, серверы аутентификации и т.п.).

Окно *Серверные правила* отображает все **Серверные правила** в ГПБ в форме таблицы (см. Рисунок 39). В таблице показана информация о каждом **Серверном правиле** в ГПБ: Применение, Источник, Приемник, Владелец сервера, Сервис, Действие, Уровень лога.

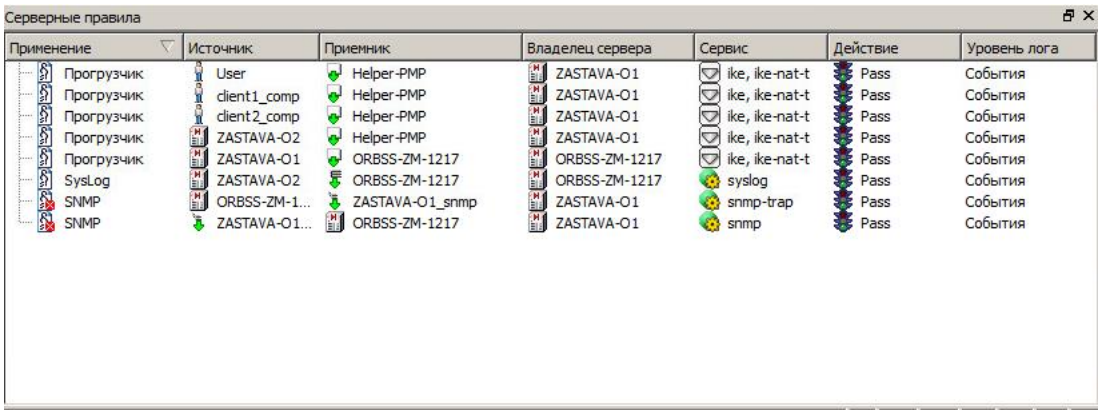

Рисунок 39 – Окно *Серверные правила*

6.11. Домены

Окно *Домены* отображает существующие Домены в виде таблицы со следующей информацией: Имя Домена, Права доступа текущей учетной записи, IP-адреса, Учетные записи, Объекты Политик, Правила, Зоны и Расписания (см. Рисунок 40).

Данное окно всегда содержит Глобальный Домен, который доступен с момента начала использования *ЦУП-Консоли*, этот Домен невозможно удалить.

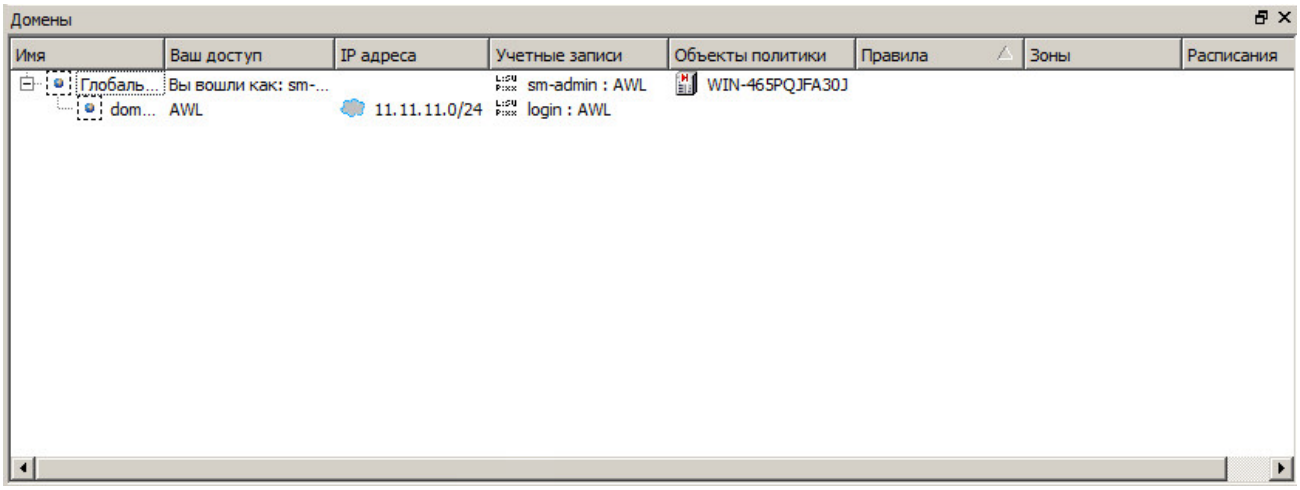

Рисунок 40 – Окно *Домены*

6.12. Центры Сертификации

Окно *Центры Сертификации* содержит описания Удостоверяющего Центра (УЦ), которые издают сертификаты (см. Рисунок 41). По сути, описание УЦ представляет собой описание сертификата УЦ (CA certificate), принадлежащего данному УЦ.

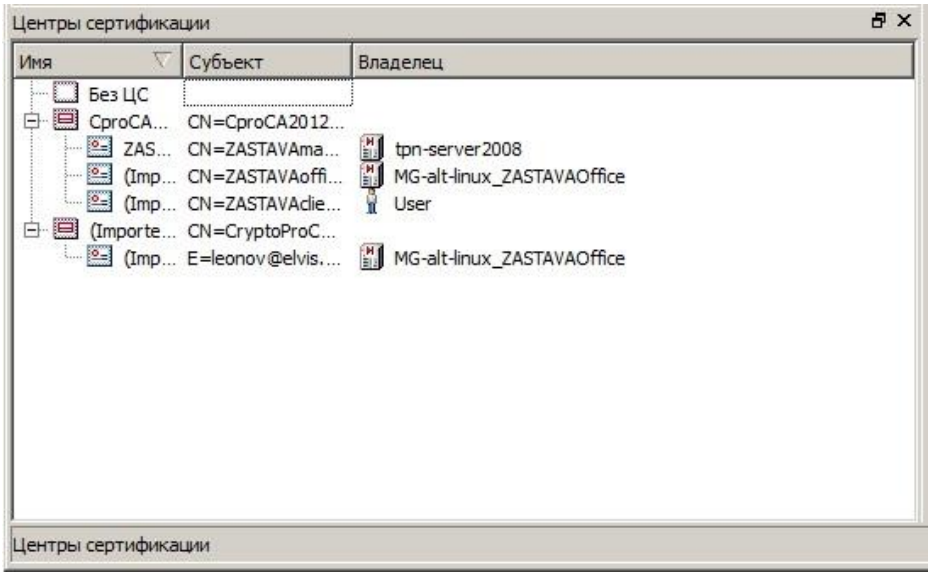

Рисунок 41 – Окно *Центры Сертификации*

Вводить эту информацию обязательно только в некоторых случаях, например, некоторые *Агенты* (в частности, маршрутизаторы Cisco IOS версий 12.2 и выше) требуют наличия в конфигурации информации о сертификате УЦ, которым подписан сертификат партнера по взаимодействию.

Контекстное меню окна *Центры Сертификации* позволяет добавлять новый УЦ, импортировать и экспортировать СА сертификаты, фильтровать и искать необходимую информацию в окне с помощью опций окна *Отфильтровать*. Для дублирования/изменения/изменения владельца и удаления УЦ нужно воспользоваться контекстным меню.

6.13. Действия

Окно *Действия* отображает список Действий в виде таблицы с указанием следующей информации: Имя/Приоритет, АН-аутентификация, ESP-шифрование, ESP-аутентификация и протокол IPComp (см. Рисунок 42). По каждому из параметров возможна сортировка списка.

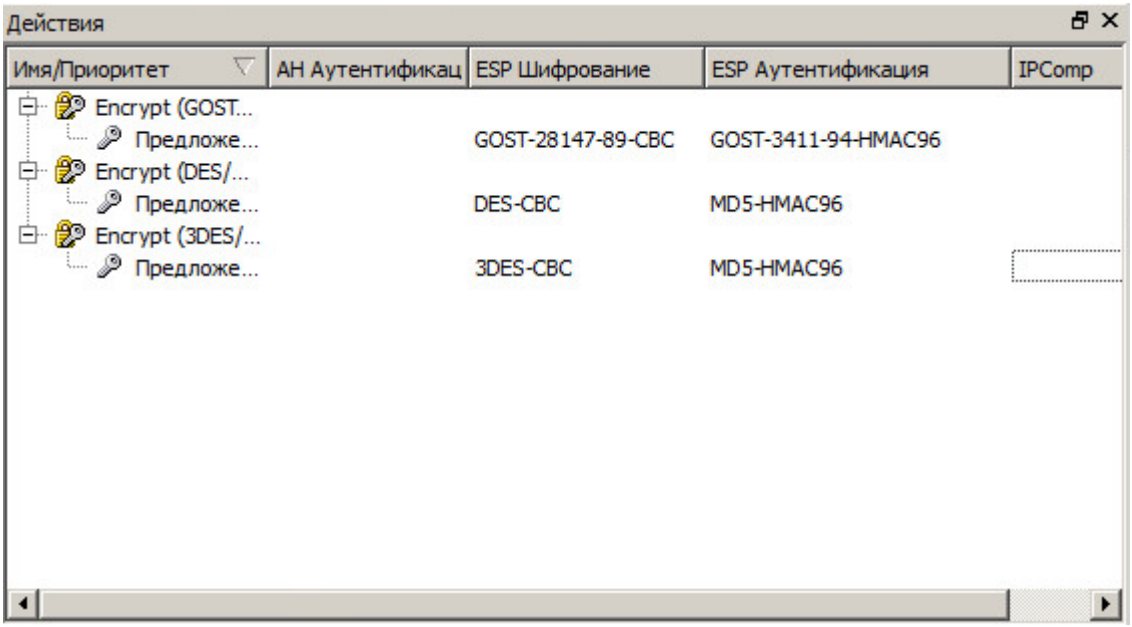

Рисунок 42 – Окно *Действия*

6.14. Настройки IKE

Окно *Настройки IKE* отображает список IKE-предложений в виде таблицы с указанием следующей информации: Имя/Приоритет, Аутентификация, Алгоритм Шифрования, Алгоритм хеширования и Oakley-группу (см. Рисунок 43). По каждому из параметров возможна сортировка списка.

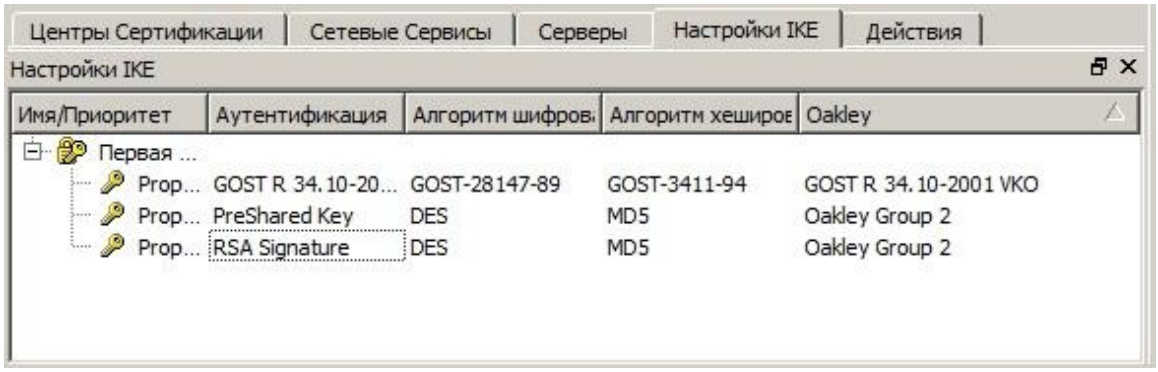

Рисунок 43 – Окно *Настройки IKE*

6.15. Сетевые Сервисы

Окно *Сетевые Сервисы* содержит список последних с указанием их Имени, Типа, Протокола, TCP/UDP-порта и ICMP-типа (см. Рисунок 44). По каждому из параметров возможна сортировка списка.

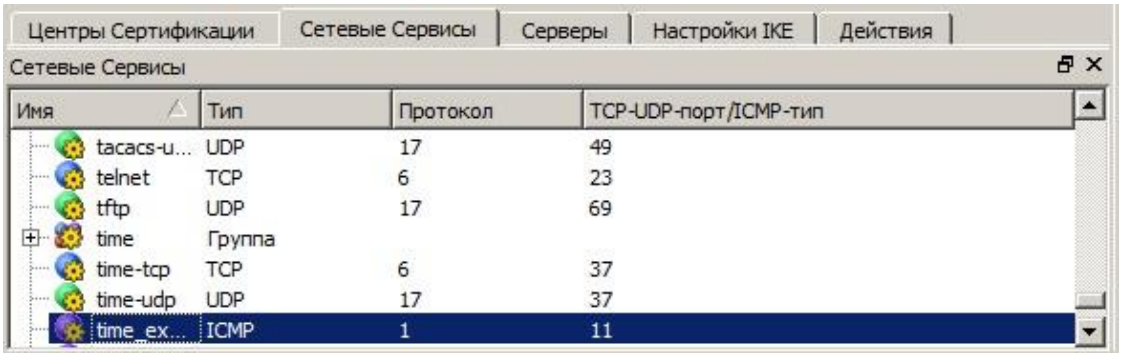

Рисунок 44 – Окно *Сетевые Сервисы*

6.16. Расписания

Окно *Расписания* отображает Расписания Правил в виде таблицы со следующей информацией: Имя, дата активации/завершения, часы действия, дни недели действия и Домен (см. Рисунок 45).

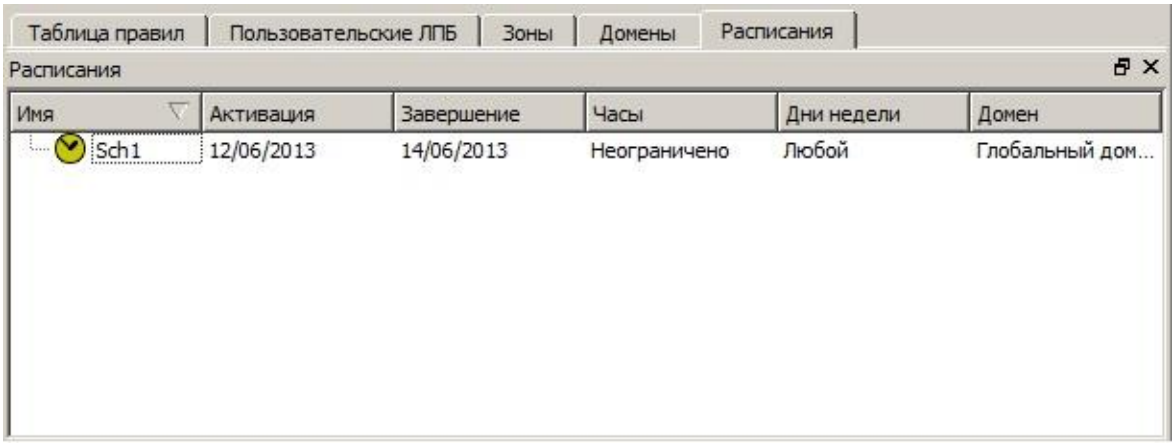

Рисунок 45 – Окно *Расписания*

6.17. Монитор

В окне *Монитор* отображены результаты активации ГПБ, окно остается пустым до начала активации ГПБ (см. Рисунок 46).

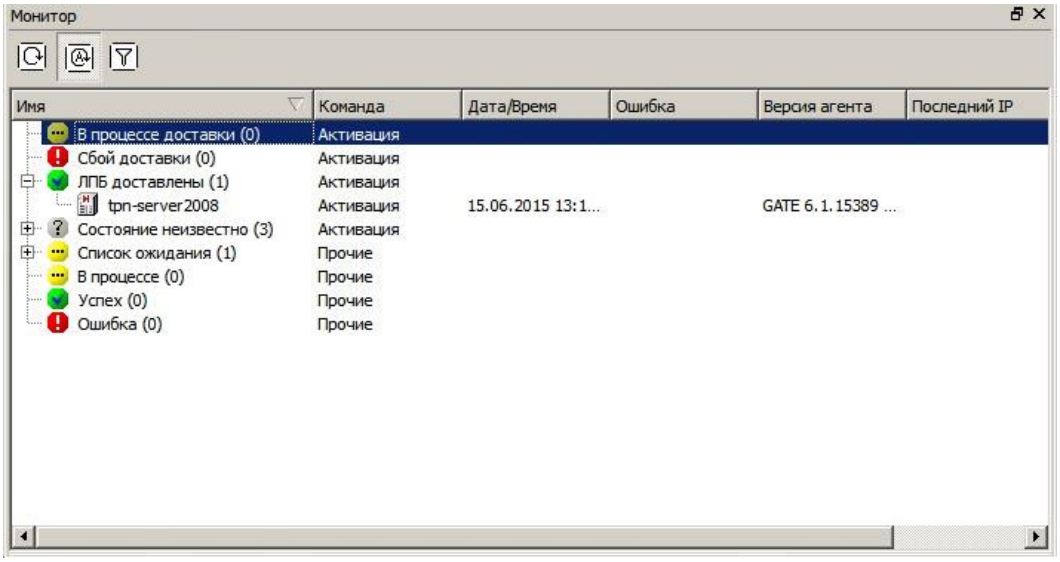

Рисунок 46 – Окно *Монитор*

В окне *Монитор* доступна своя инструментальная линейка (см. Таблица 19).

Таблица 19 – Инструментальная линейка окна *Монитор*

Кнопка	Характеристика	Кнопка	Характеристика
	Обновить статус мониторинга		Фильтровать объекты для мониторинга
	Обновлять монитор каждые 5 сек.		

6.18. Журнал и SysLog-журнал

Окно *Журнал* используется для просмотра зарегистрированный ошибок, предупреждений, событий и информационных сообщений, собранных в процессе работы с *ЦУП* (см. Рисунок 47).

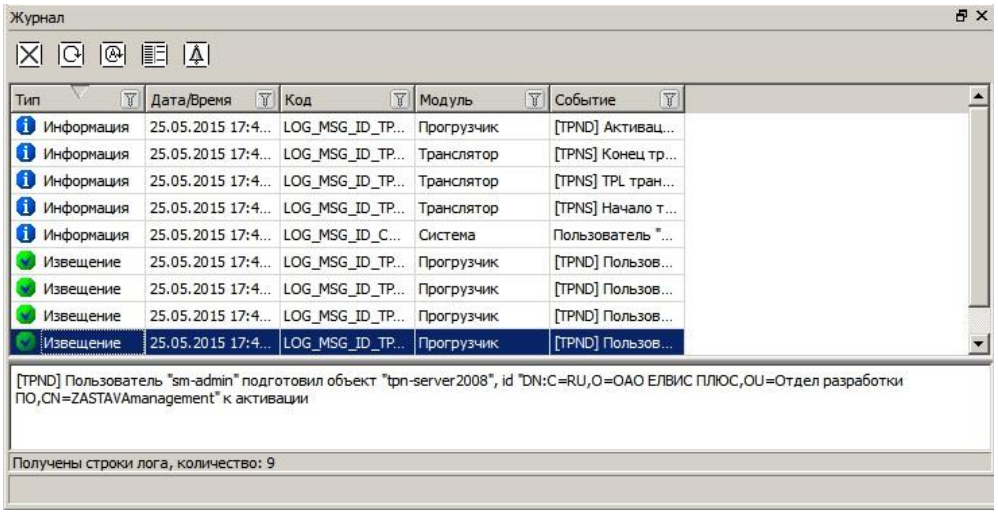

Рисунок 47 – Окно *Журнал*

Окно *Журнал* содержит инструментальную линейку, по средствам которой, можно настроить параметры логирования сообщений (см. Таблица 20).

Таблица 20 – Инструментальная линейка окна *Журнал*

Кнопка	Характеристика	Кнопка	Характеристика
	Обновить лог		Показать только отфильтрованные сообщения
	Автоматическое обновление журнала каждые 10 сек.		Установить уровни лога…
	Индикаторы		Очистить лог

Окно SysLog-журнала используется для просмотра собранных SysLog-событий (см. Рисунок 48).

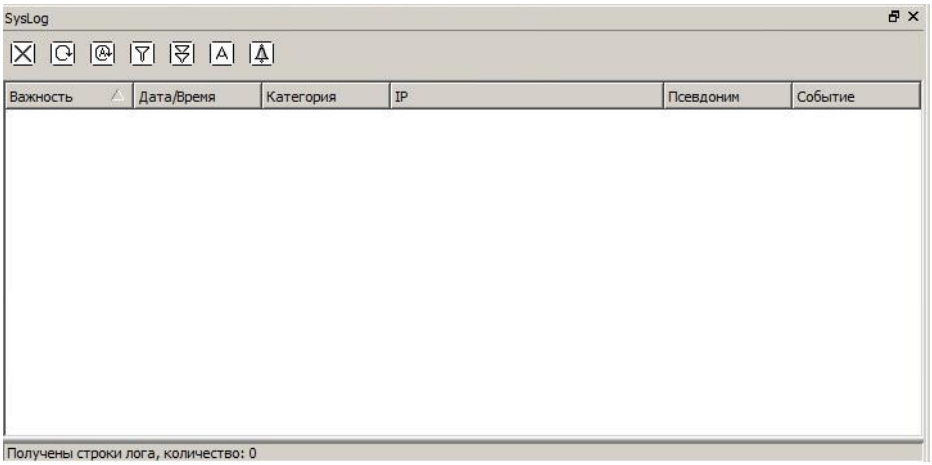

Рисунок 48 – Окно *Syslog*

Окно *Syslog* содержит инструментальную линейку, по средствам которой, можно настроить параметры логирования *Syslog* сообщений (см. Таблица 21).

Таблица 21 – Инструментальная линейка окна *Syslog*

Кнопка	Характеристика	Кнопка	Характеристика
	Обновить лог		Показать только отфильтрованные сообщения
	Автоматическое обновление журнала каждые 10 сек.		Фильтры Syslog-сервера
	Индикаторы		Задать псевдоним
	Очистить лог		

6.19. Журнал исполнения

Окно *Журнал Исполнения* используется для просмотра внесённых изменений после импорта изменений в проект. *Журнал Исполнения* можно сохранить или открыть уже существующий, также доступна навигация по журналу с помощью меню *Вид* (см. Рисунок 49).

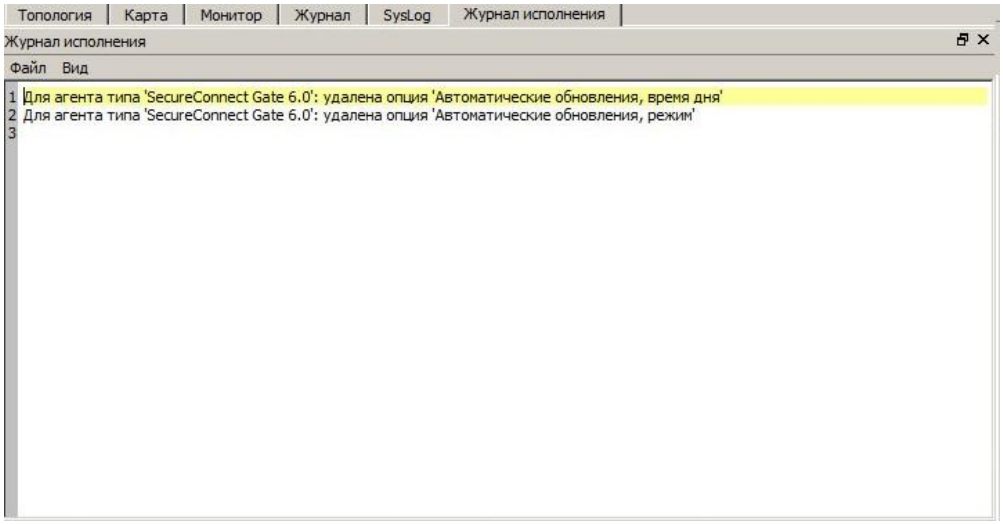

Рисунок 49 – Окно *Журнал исполнения*

6.20. Валидность сертификатов

Окно *Валидность сертификатов* используется для того, чтобы отслеживать сертификаты с истёкшим сроком действия (см. Рисунок 50). Открыть это окно, используя команду **Валидность сертификатов** из меню *Окно*. Окно содержит список просроченных сертификатов, представленных в форме таблицы, с возможностью фильтрации по сроку истечения сертификата. Для фильтрации по сроку истечения сертификата необходимо отметить одно из полей в поле **Сертификаты**.

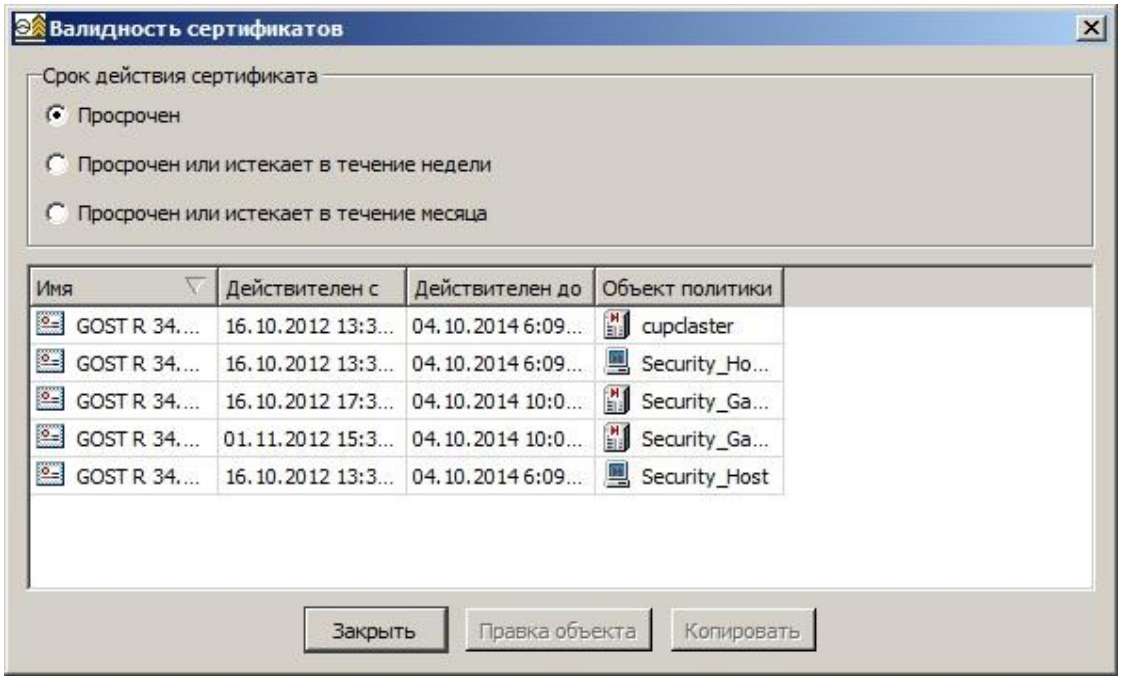

Рисунок 50 – Окно *Валидность сертификатов*

ЦУП-Консоль автоматически отслеживает сертификаты с истёкшим сроком действия. В случае обнаружения таких сертификатов в строке статуса основного окна *ЦУП-Консоль* появляется мигающая иконка . Нажатие на эту иконку открывает окно со списком сертификатов с истёкшим / истекающим сроком действия. Иконка мигает до тех пор, пока окно *Валидность сертификатов* не было открыто.

6.21. Дескрипторы агентов

Окно *Дескрипторы Агентов* (см. Рисунок 51) используется для управления XML-файлами, которые содержат описания параметров для каждого типа Агента, производителя *Агента*, версии *Агента* (главной и второстепенной) и набор свойств. Эти XML-файлы переопределены в *ЦУП* и расположены в поддиректории `<ads>` инсталляционной директории *ЦУП* (см. подраздел 3.2).

Окно состоит из двух секций: в первой выводится список Агентов с указанием Производителя, Версии и Минорной версии, во второй выводится сам дескриптор. Содержание таблицы может сортироваться в возрастающем или убывающем порядке, нажимая на любом из заголовков колонки. Содержание таблицы сортируется согласно выбранной колонке.

Преобразовать устаревшие дескрипторы в поддерживаемые можно добавлением строки вида «SecureConnect Mobile Client,5.2,-,-,User->SecureConnect Mobile Client,5.3,-,-,User» с описанием замены в файл agent_replacements.txt в главной директории. После описания замены надо перезапустить GUI/CLI и повторить попытку импорта конфигурации.

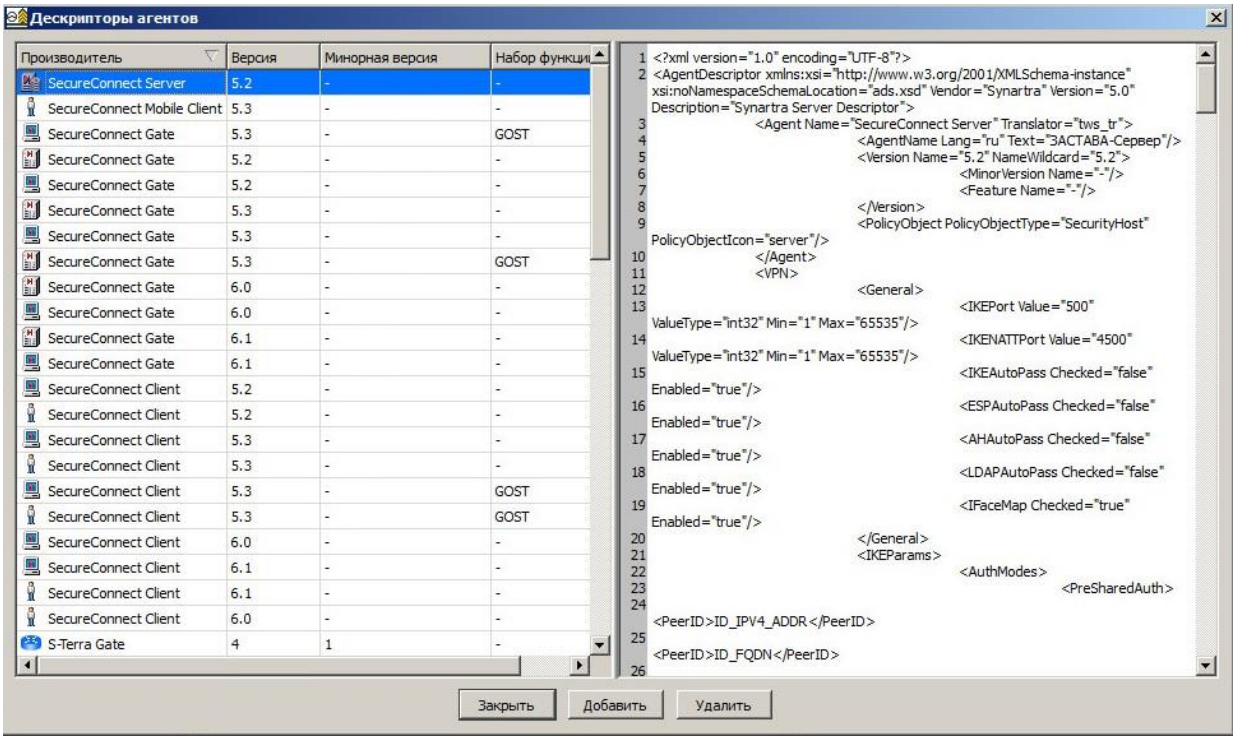

Рисунок 51 – Окно *Дескрипторы агентов*

6.22. Дескрипторы серверов

Окно *Дескрипторы серверов* (см. Рисунок 52) используется для управления XML-файлами, которые содержат описания параметров для каждого Имени Сервера, класса **Сервера**, версии *Объекта* (главной и второстепенной) и набор свойств. Эти XML-файлы переопределены в *ЦУП* и расположены в поддиректории `<ads>` инсталляционной директории *ЦУП* (см. подраздел 3.2).

Окно состоит из двух секций: в первой выводится список Серверов с указанием Имени и класса, во второй выводится сам дескриптор. Содержание таблицы может сортироваться в возрастающем или убывающем порядке, нажимая на любом из заголовков колонки. Содержание таблицы сортируется согласно выбранной колонке.

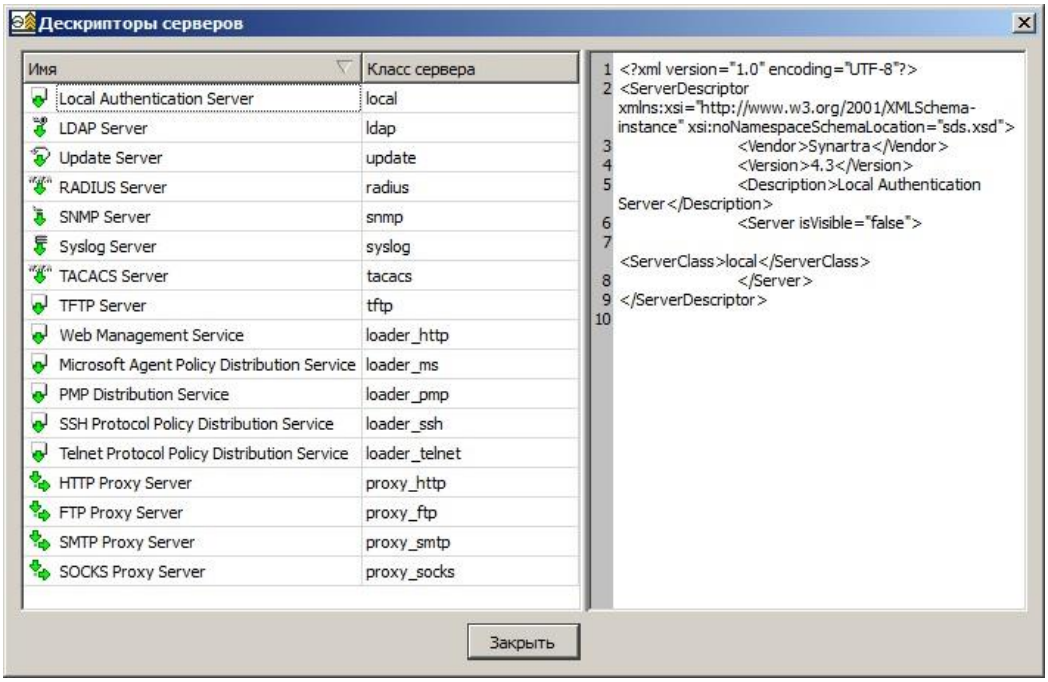

Рисунок 52 – Окно *Дескрипторы серверов*

7. Создание Глобальной Политики Безопасности в *ЦУП-Консоль*

В окне просмотра в виде уникальных значков отображаются Объекты Политики, Правила, сетевые сервисы, (доступные) действия, а также вспомогательные узлы. Управление ими производится в четырех окнах просмотра Политики.

В этой части описываются все типы Объектов, их назначение, параметры и характеристики; инструкции по созданию, редактированию, удалению и управлению этими Объектами, а также способы изменения их параметров и характеристик.

7.1. Объекты Политики

Объекты политики представляют собой различные виды защитных устройств в Среде Безопасности (см. Таблица 22). Управление этими устройствами осуществляется с помощью ЛПБ, используя *ЦУП*. Часть устройств может получать ЛПБ из другого источника или вообще не использовать ЛПБ. Взаимодействие между Объектами политики определяется Правилами.

Таблица 22 – Описание Объектов Политики

Тип Объекта	Описание
Шлюз Безопасности	Сетевой Шлюз (в том числе *ЗАСТАВА-Офис ЦУП*), на котором установлен *ЗАСТАВА–Офис* (или маршрутизатор Cisco, Cisco PIX Firewall или Microsoft IPsec *Агент*); это также может быть обычный Шлюз без криптографической системы, например МЭ, устройство NAT или просто маршрутизатор
Хост Безопасности	Сетевой узел, имеющий постоянный IP-адрес, на котором установлен *ЗАСТАВА-Клиент* или Microsoft IPsec *Агент*
Пользователь	Сетевой узел, не имеющий постоянного IP-адреса, на котором установлен *ЗАСТАВА-Клиент* или IPsec *Агент*
IP хост	Сетевой узел без криптографической системы, не управляемый *ЦУП* (может быть защищен с помощью Шлюза Безопасности)
Диапазон IP-адресов	Несколько IP-адресов, которые могут либо подчиняться Правилам, либо защищаться Шлюзом Безопасности
Подсеть	Несколько IP-адресов, которые могут либо подчиняться Правилам, либо защищаться Шлюзом Безопасности (определенные в форме адресов/ сетевых масок).
Группа	Несколько Объектов политики, зарегистрированных в *ЦУП*

7.1.1. Общие задачи

7.1.1.1. Форма для работы с сертификатами

Для работы с Сертификатами необходимо зайти в свойства *Объекта Политики*, для которого требуется сертификат, в разделе *ВЧС* выбрать *Сертификаты* и нажать кнопку **Добавить** (см. Пример 1).

Если у Вас есть файл с выпущенным для данного Объекта сертификатом (и, возможно, с секретным ключом), то необходимо нажать кнопку **Импортировать** и следовать инструкциям, указанным в диалогах. Сертификат и (при наличии) закрытый ключ будут импортированы в БД *ЦУП* (см. Пример 2).

Для типа дескрипторов *Агент* версии 6.1 и выше можно генерировать в *ЦУП* сертификаты и экспортировать их в *Агент* и *ГПБ* (см. Пример 3).

Для типа дескрипторов *Агент* версии 6.1 и выше можно импортировать в *ЦУП* сертификаты зарегистрированные в *Агент* (см. Пример 4).

Если файла с сертификатом нет, то необходимо нажать кнопку **Добавить** и заполнить нужные поля формы вручную (см. Пример 1). Поля формы представляют собой параметры, необходимые для создания сертификата (см. Рисунок 53 и Таблица 23).

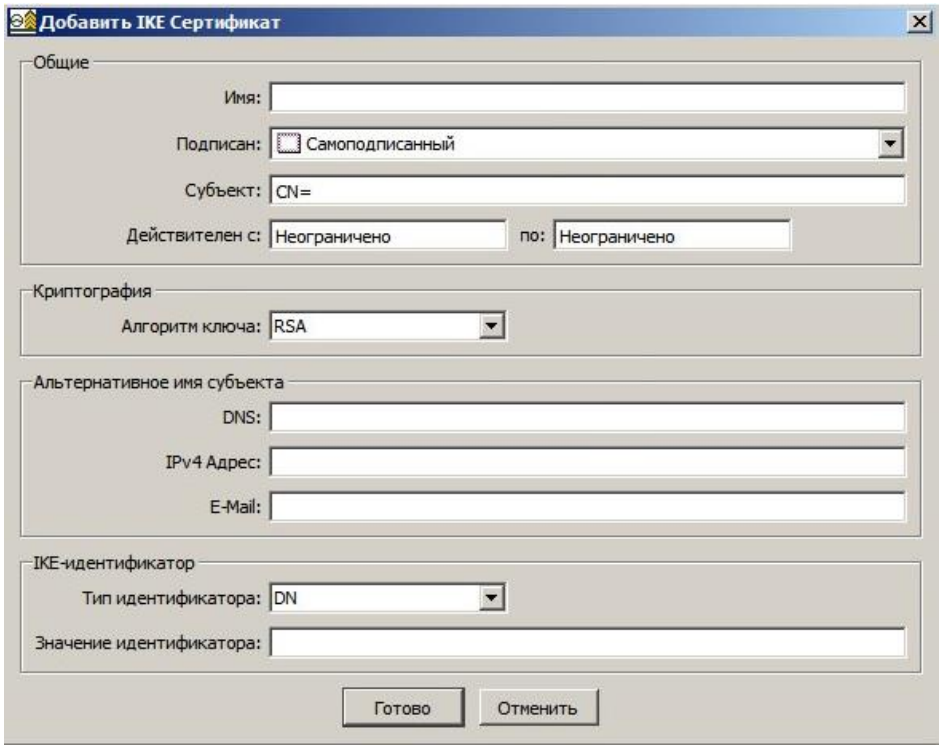

Рисунок 53 – Окно для добавления сертификата

Таблица 23 – Описание параметров, используемых при добавлении сертификата

Параметр	**Значение**
Имя	DN сертификата
Подписан	Сертификат УЦ, которым подписан данный сертификат.
Субъект	Поле **Владелец сертификата**, содержащее информацию о владельце сертификата в формате Distinguished Name (DN) (например, CN=Alice, OU=Management, O=MyCompany).
Действителен с	Начало срока действия сертификата
по	Окончание срока действия сертификата

Параметр	Значение
Альтернативное Имя Владельца	Поле **Альтернативное Имя Владельца сертификата**, содержащее дополнительную информацию о владельце сертификата: – DNS - DNS-имя хоста (например, alice.mycompany.com); – IPv4 address - IP-адрес хоста (например, 192.168.0.1); – E-mail - адрес электронной почты владельца (например, alice@mycompany.com).
Алгоритм ключа	Тип открытого ключа, содержащегося в сертификате
Тип идентификатора	Какую именно информацию о владельце использовать для идентификации данного сертификата при установлении IKE/IPsec-соединений. Возможные варианты: DN (т.е. Subject), DNS, IPv4 или E-mail. Примечание. Некоторые типы *VPN-Агентов* (например, Cisco) работают не со всеми типами IKE Identity. В этом случае список доступных значений при задании данного параметра будет ограничен.
Значение идентификатора	Собственно, значение IKE Identity. Данное поле заполняется автоматически - в зависимости от параметра Identity type и параметров с информацией о владельце сертификата.

7.1.1.1.1. Пример 1

Информация о сертификате введена вручную (сам сертификат в БД *ЦУП* не импортирован) (см. Рисунок 54).

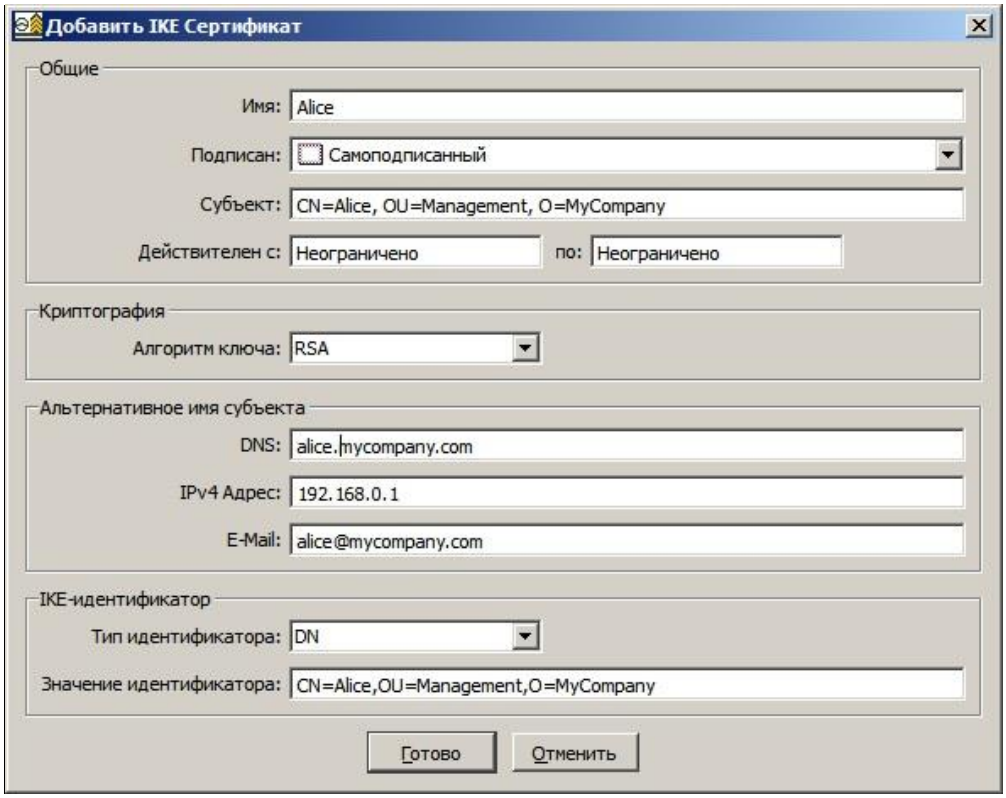

Рисунок 54 – Определение информации идентичности: Пример 1

7.1.1.1.2. Пример 2

Сертификат (без закрытого ключа) импортирован в БД *ЦУП* при помощи кнопки **Импортировать**. Все основные параметры формы заполнены автоматически на основании информации из сертификата (см. Рисунок 55).

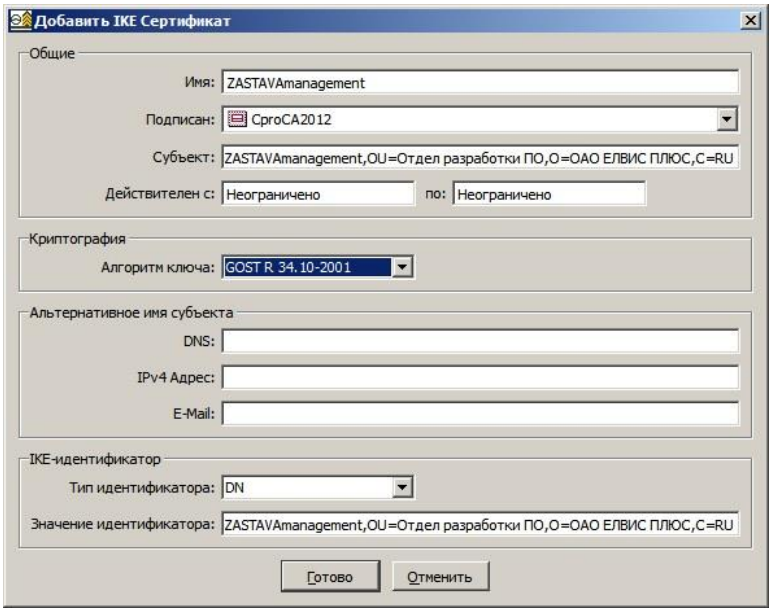

Рисунок 55 – Определение информации идентичности: Пример 2

7.1.1.1.3. Пример 3

Для типа дескрипторов *Агент* версии 6.1 существует возможность генерации сертификатов.

Для того чтобы сгенерировать сертификат и добавить его в политику необходимо нажать кнопку **Генерировать** на закладке *Сертификаты* параметров *Объекта политики* и заполнить все поля в окне *Генерировать ключевую пару*. После генерации сертификат будет отображаться на закладке *Сертификаты* параметров *Объекта политики* с статусом **Подписать это!**. Сертификат необходимо экспортировать в буфер обмена или в файл с помощью команды в контекстного меню Объекта в окне *Объектов политики.* Отправить созданный запрос в УЦ (в зависимости от требований УЦ используйте электронную почту, веб-браузер или другие средства). После получения сертификата из УЦ импортировать его в *Объект политики*, для этого необходимо в контекстном меню окна *Центры сертификации* выбрать пункт **Заменить подписанным**. После этого в окне *Импорт сертификатов* необходимо посмотреть и проверить параметры сертификата (в случае необходимости изменить их) и нажать кнопку **Готово** (см. Рисунок 56). Сертификат будет добавлен в ГПБ и отправлен *Агенту*.

При несоответствии параметров сертификата в контейнере и параметров в запросе на генерирование ключевой пары в *ЦУП* возникнет предупреждение в момент экспорта запроса в буфер обмена или в файл.

Для того чтобы ключевая информация была экспортирована и сохранена правильно, в *Графическом интерфейсе Агент* на закладке *Токены* надо поставить наивысший приоритет тому токену, который соответствует криптоалгоритму ключевой информации.

Для удаления запроса на генерацию ключевой пары, необходимо выбрать пункт контекстного меню *Удалить запросы для сертификатов или ключей.*

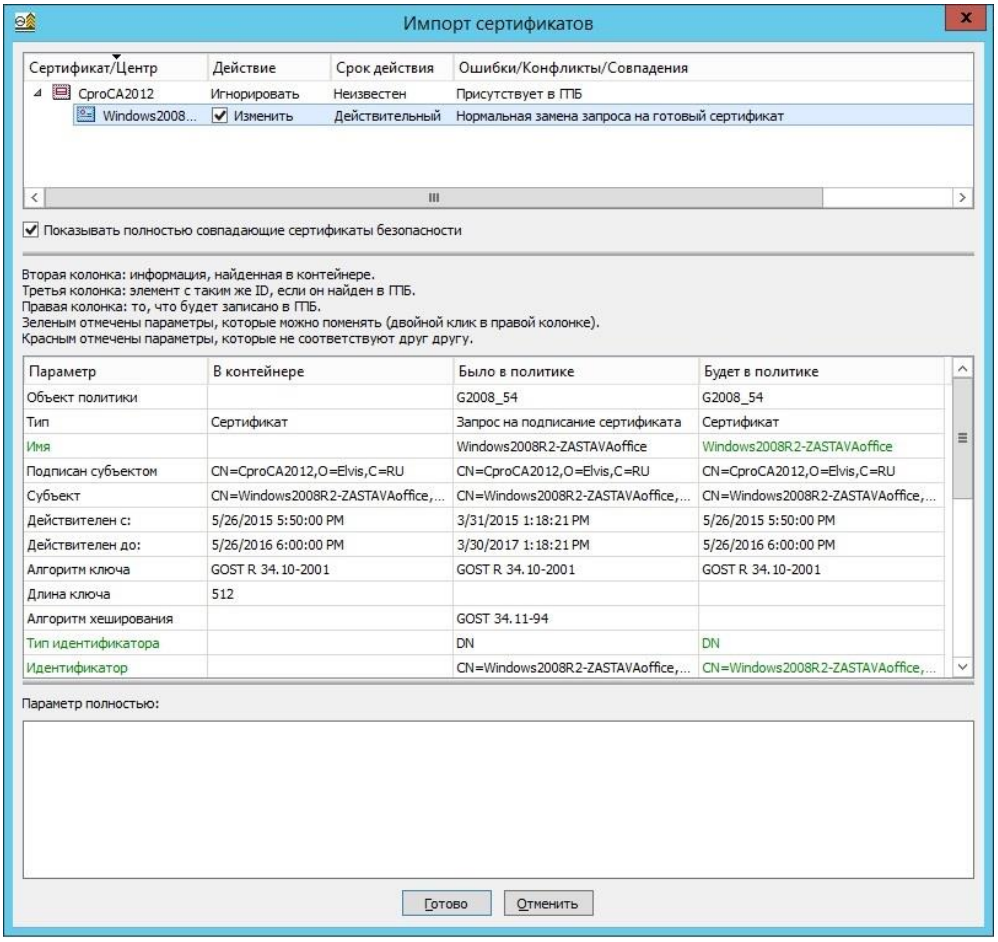

Рисунок 56 – Импорт сертификатов

7.1.1.1.4. Пример 4

Для дескриптора *Агента* версии 6.1 и выше можно загрузить список сертификатов из *Агента*, для этого в контекстном меню *Объекта политики* надо выбрать пункт **Получить список сертификатов.** После успешной загрузки сертификатов в контекстном меню *Объекта политики* выбрать пункт **Добавить загруженные сертификаты в политику** и в окне *Импорт сертификата* нажать кнопку **Готово**.

7.1.1.2. Привязка удаленных серверов и создание Технологических Правил

Во многих местах графического интерфейса *ЦУП-Консоли* используется универсальный элемент управления, предназначенный для привязки к редактируемому Объекту серверов различного типа (Серверы прогрузки, серверы аутентификации и т.п.).

Ниже описываются общие принципы работы данного механизма на примере закладки *Параметры соединения* в свойствах *Агента ЗАСТАВА-Офис* (поле **Удаленный сервер**). При помощи кнопок **Добавить** и **Удалить** добавляются и удаляются Серверы, с которыми будет

взаимодействовать редактируемый Объект (см. Рисунок 57). В данном примере к Объекту привязан PMPv2-сервер **Zastava-MGMT** (одноименный с Объектом Политики), работающий на хосте с *ЦУП* и отвечающий за доставку конфигураций на *Агенты* по протоколу PMPv2 (Policy Management Protocol).

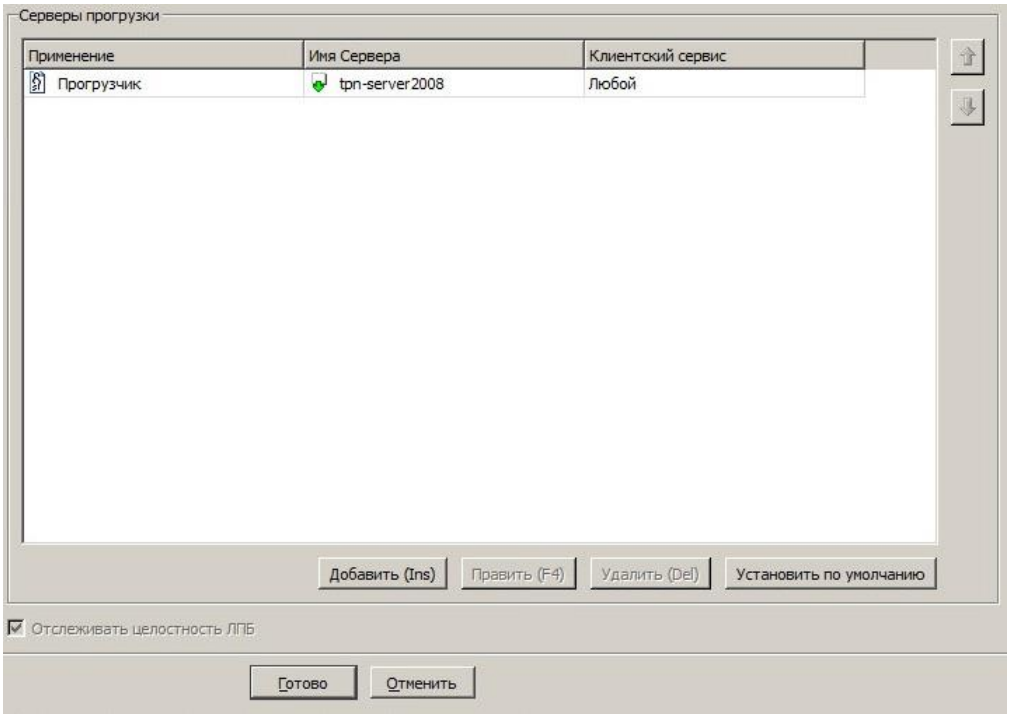

Рисунок 57 – Привязка удаленных серверов и создание Технологических Правил в закладке *Параметры соединения* в свойствах объекта

В контекстном меню окна *Серверы прогрузки* выбрать действие **Включить/Выключить** (см. Рисунок 58) отвечает за создание **Технологического Правила**. Если правило включено, то при трансляции ГПБ для всех Объектов Политики, через которые проходит трасса между сервером и *Агентом*, будут автоматически созданы фильтры для пропускания трафика заданного типа (тип трафика определяется Объектом **Сетевой Сервис** в колонке **Клиентский сервис**). Если правило выключено, то соответствующие фильтры будут созданы только в ЛПБ данного *Агента* и данного сервера, т.е. придется принимать специальные меры для пропускания этого трафика через промежуточные маршрутизаторы.

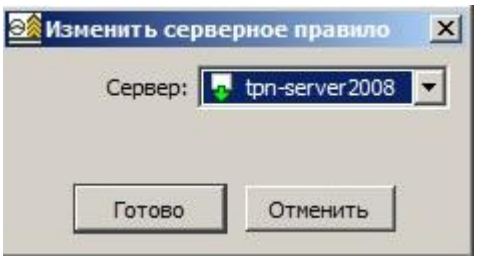

Рисунок 58 – Окно изменения Серверного правила

Приоритет фильтров (т.е. порядок их появления в ЛПБ) можно изменять при помощи кнопок со стрелками справа от таблицы.

Таким образом, при помощи подобной привязки сервера к редактируемому Объекту решаются сразу две задачи:

1) В конфигурацию Объекта будут вставлены команды, обеспечивающие взаимодействие Объекта с данным сервером (в нашем случае будут разрешены управляющие воздействия со стороны "Zastava-MGMT").

2) В конфигурации самого Объекта, привязанного сервера и, при **включенном** состоянии - в конфигурациях промежуточных маршрутизаторов, будут созданы фильтры для пропускания соответствующего трафика (в нашем случае - трафик для работы протокола IKE по порту UDP 500 и протокола IKE-NAT-Traversal по порту UDP 4500).

7.1.1.3. Создание и редактирование NAT-Правил (для Шлюзов Безопасности)

ЦУП поддерживает работу с сетями, где используется трансляция сетевых адресов (Network Address Translation, NAT) различных видов:

- статическая трансляция адресов (static NAT, dynamic NAT);
- динамическая трансляция адресов (NAPT).

Обычно NAT конфигурируется на пограничных устройствах, отделяющих локальные сети от сети Интернет – это может быть как небольшое специализированное аппаратное устройство, так и полноценный VPN-шлюз/МЭ. В обоих случаях для описания данного устройства (*Агента*) в *ЦУП* необходимо создать объект Шлюз Безопасности.

Для некоторых типов *Агентов* возможно *активное управление* NAT-конфигурацией (путем включения команд NAT в ЛПБ *Агента*), для остальных *Агентов ЦУП* просто учитывает информацию о NAT-преобразованиях на данном объекте, чтобы отслеживать возможные изменения IP-адресов при прохождении трафика через сеть (это делается специальным алгоритмом трассировки, на этапе трансляции ГПБ).

Правила NAT создаются на закладке *NAT Правила* в *Свойствах объекта Шлюз Безопасности.* Для того чтобы ввести информацию о Правилах NAT для данного объекта надо поставить отметку в поле **Включить NAT** (см. Рисунок 59). Отметка в поле **Разрешить управление NAT** определяет, будет ли транслироваться FW-процедура в Политику, т.е. выполняется ли преобразование NAT непосредственно *Агентом*. Если отметка снята, то в

Политику транслируется фильтр с учетом преобразованных адресов, но само преобразование выполняется не *Агентом*. Затем создать одно или несколько NAT-Правил.

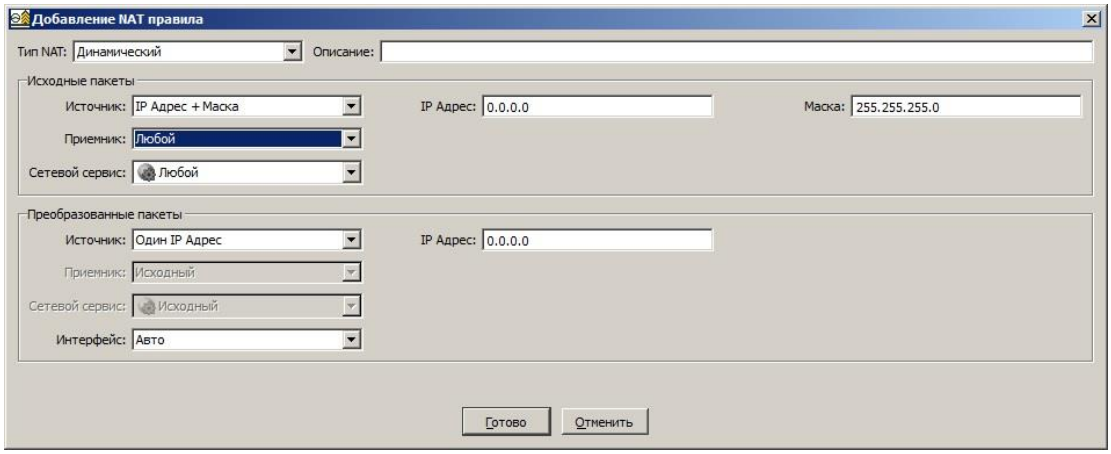

Рисунок 59 – Пример создания NAT-Правила

Добавление NAT-Правила происходит следующим образом:

1) Нажать кнопку **Добавить**.
2) Из выпадающего списка выбрать тип NAT, который будет применяться данным Правилом.
3) Можно ввести текстовое описание данного NAT-Правила в строке *Описание*.
4) Ввести описание «приватного» (видимого внутри локальной сети) IP-адреса(ов) для поля **IP Адрес** в исходном IP-пакете (в терминологии Cisco: "inside local"):
   – В строке *Источник* в поле **Исходные пакеты**, выбрать формат, в котором будут указаны IP-адреса. При выборе в качестве источника существующего объекта из выпадающего списка, правило будет привязано к адресу Объекта Политики.
   – Ввести всю информацию, необходимую для выбранного формата.
5) Ввести описание «публичного» (видимого снаружи, в глобальной сети) IP-адреса(ов) для поля **IP Address** в преобразованном IP-пакете (в терминологии Cisco: "inside global"):
   – В строке *Источник* в поле **Преобразованные пакеты**, выбрать формат, в котором будут указываться IP-адреса. Если адрес в глобальной сети совпадает с адресом внутри локальной сети, выбрать значение **Исходный** (трансляция адреса для данного поля IP-пакета производиться не будет).
   – Ввести всю информацию, необходимую для выбранного формата.

6) Если необходимо, ввести описание IP-адреса(ов) для поля **IP Address** в исходном IP-пакете (в терминологии Cisco: "outside local"):
   - В строке *Приемник* в поле **Исходные пакеты**, выбрать формат, в котором Вы будете указывать IP-адреса.
   - Ввести всю информацию, необходимую для выбранного формата.
7) Если необходимо, ввести описание IP-адреса(ов) для поля **IP Address** в оттранслированном IP-пакете (в терминологии Cisco: "outside global"):
   - В строке *Приемник* в поле **Преобразованные пакеты**, выбрать формат, в котором Вы будете указывать IP-адреса. Если адрес транслировать не нужно, выбрать значение **Исходный.**
   - Ввести всю информацию для IP-адресов, необходимую для выбранного формата.
8) Если Вы хотите, чтобы данное NAT-Правило применялось только к некоторым типам трафика, то в поле **Исходные пакеты** в строке *Сетевой сервис* надо указать нужный Сетевой Сервис. При этом надо убедиться в том, что в поле **Преобразованные пакеты** строка *Сетевой сервис* имеет значение **Исходный**, либо выбрать в качестве значения конкретный Сетевой Сервис – в последнем случае будет включена *трансляция сетевых сервисов* (например, таким образом можно транслировать HTTP-трафик с порта TCP:80 на порт TCP:8080 и т.п.). Список доступных для выбора Сетевых Сервисов редактируется в соответствующем окне *ЦУП*.
9) Если Вы хотите определить интерфейс, через который будет осуществляться трансляция, необходимо выбрать этот интерфейс в поле **Интерфейс** поля **Преобразованные пакеты**.
10) Нажать кнопку **OK**. В таблице появится новое NAT-Правило.

Если в **Исходном пакете** значение **Приемника**, **Источника** или **Сервиса** выбран в значение любой, то значение этого параметра преобразованного пакета будет иметь значение исходный.

Если преобразуется **Источник**, то значение параметра **Приемник** будет равно значению **Исходный** и наоборот, преобразовывать оба параметра нельзя.

В качестве **Приемника** и **Источника** могут быть выбраны существующие объекты.

Пример:

Шлюз Безопасности выполняет NAT (точнее – NAPT) для группы IP-хостов, находящихся за этим Шлюзом, с адресами 192.168.0.1...192.168.0.10. В сети Интернет эти «приватные» адреса будут преобразованы в единый «глобальный» адрес 1.1.1.1. Трансляция адресов должна производиться для любых видов трафика (сетевых сервисов).

В этом случае, NAT-Правило для данного Шлюза Безопасности должно быть создано со следующими параметрами:

- Тип NAT: **Динамический;**
- Исходные пакеты **Источник**: (**Диапазон IP-адресов**) 192.168.0.1 192.168.0.10;
- Исходные пакеты **Приемник: Любой**;
- Исходные пакеты **Сетевой сервис**: **Любой**;
- Преобразованные пакеты **Источник**: (**IP-адрес**) 1.1.1.1;
- Преобразованные пакеты **Приемник: Исходный**;
- Преобразованный пакет **Сетевой сервис**: **Исходный**;
- Преобразованный пакет **Интерфейс**: **Авто**.

7.1.1.4. Автоматическое обновление *Агентов*

Агенты поддерживают процедуру автоматического обновления, которая позволяет скачивать и устанавливать новые версии продукта. Конфигурирование автоматического обновления может выполняться как через локальные настройки *Агента*, так и централизованно – через *ЗАСТАВА-Управление*, когда настройки указываются в ЛПБ *Агента*.

При включении режима автоматического обновления *Агент* будет периодически связываться с указанным сервером, содержащим обновления (данный сервер может располагаться в локальной сети или в сети Интернет). Если на сервере выложена свежая версия продукта, то будет запущен процесс обновления (скачивание файла обновления, деинсталляция текущей версии и инсталляция новой, с сохранением всей информации о настройках, сертификатах и т.п.).

В зависимости от настроек в ЛПБ *Агента*, процессы скачивания и инсталляции обновлений могут выполняться либо полностью автоматически, либо по команде пользователя. Кроме того, поддерживается инсталляция обновлений по расписанию.

Обращение к серверу обновлений производится по открытому протоколу HTTP. При необходимости защиты данного соединения можно воспользоваться штатными средствами продуктов *ПК «VPN/FW «ЗАСТАВА»*(создать в *ЦУП* правило для защищенного соединения между данным *Агентом* и сервером обновления).

Для настройки автоматических обновления объекта с *Агентом* через *ЦУП* открыть свойства данного объекта и выбрать закладку *Автоматическое обновление* (см. Рисунок 60).

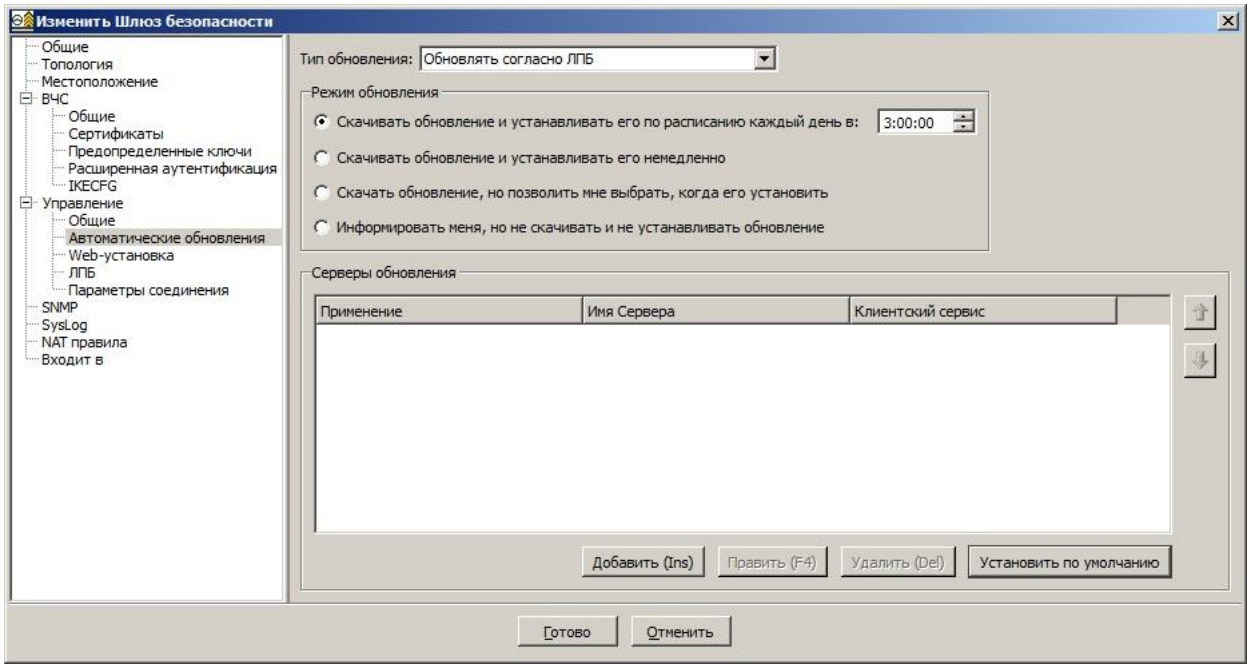

Рисунок 60 - Конфигурирование автоматического обновления

Для конфигурирования автоматического обновления необходимо отметить нужные параметры в закладке *Автоматические обновления* (см. Таблица 24).

Таблица 24 – Описание элементов интерфейса

Элемент	Описание
Выпадающий список **Тип Обновления**	Включение в ЛПБ Объекта (*Агент*) информации о настройках процедуры обновлениях.
Режим обновления	Режим скачивания и инсталляции обновлений (четыре варианта).
Группа элементов **Серверы обновления**	Стандартные элементы управления для настройки технологических правил (см. п. 7.1.1.2 и п. 7.9.4.7).

	Для централизованного управления настройками автообновлений (через *ЦУП*) необходимо на самом *Агенте* включить режим **Local Security Policy** (в окне *Настройки –> Настройки Обновления*). В противном случае информация о настройках обновлений в ЛПБ будет игнорироваться *Агентом*.
	Более подробное описание процедуры создания и настройки сервера обновлений для процедуры автообновления представлено в приложении (см. Приложение 2. Настройка сервера обновлений).
	Для автоматического обновления *Агентов* на ОС Windows XP необходимо выполнить дополнительные настройки опций защиты системных файлов на компьютере с установленным *Агентом*: поставить маркер в поле System Properties ->Driver Signing Options ()-> Ignore - Install the software anyway and don't ask for my approval.

7.1.2. Объекты Шлюзов Безопасности

Агенты типа «Шлюзы Безопасности» защищают данный сегмент сети. Весь входящий и исходящий трафик должен сначала пройти через Шлюз, который обеспечивает Безопасность трафика с помощью Политики Безопасности, установленной администратором Безопасности. Шлюз обрабатывает трафик в соответствии с ГПБ и принимает решение пропустить его или блокировать, (или же пропустить трафик, приняв меры Безопасности) согласно с выбранной Политикой. У Шлюза Безопасности должно быть, по меньшей мере, два интерфейса. Примерами Шлюзов Безопасности могут служить *ЗАСТАВА-Офис*, маршрутизаторы Cisco, Cisco PIX Firewalls.

7.1.2.1. Создание Объектов Шлюзов Безопасности

Этот пункт содержит инструкцию по созданию Объектов Шлюзов Безопасности для нескольких различных типов *Агентов* Шлюзов. Поскольку создание и планирование конфигурации Шлюзов Безопасности является одним из самых важных и комплексных аспектов программирования *ЦУП*, создание Объектов Шлюзов Безопасности будет детально рассмотрено ниже.

Дальнейшие сведения о параметрах Шлюзов Безопасности можно найти в п. 7.1.2.7.

7.1.2.2. *ЗАСТАВА-Офис*

Установить курсор в секции *Топология* или выбрать вкладку *Сетевые Объекты* в секции *Объекты политики*, используя контекстную команду **Добавить->Шлюз Безопасности**. Откроется окно *Выбор Дескриптора Агента* (см. Рисунок 61).

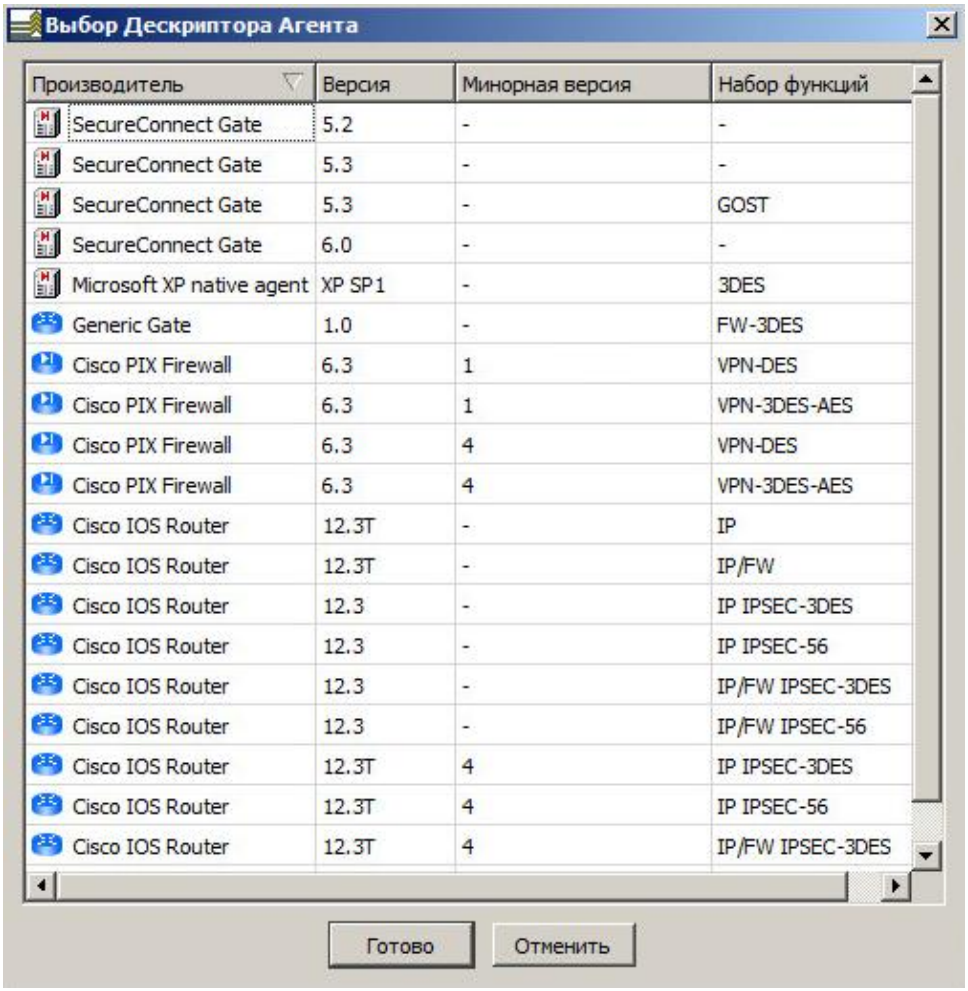

Рисунок 61 – Шлюз Безопасности, выбор дескриптора *Агента*

Шаг 1: Общие характеристики

Указать общие характеристики Объекта следующим образом:

1) Указать производителя и версию *Агента*, которого будет представлять этот Шлюз Безопасности в окне *Выбор Дескриптора Агента*.

2) На закладке *Общее* ввести **Имя** объекта Шлюза Безопасности.

3) В строке *Адрес Агента* набрать IP-адрес Шлюза, который будет представлять этот Объект. Именно на этот адрес *ЦУП* будет отправлять ЛПБ для данного Объекта.

4) Выбрать домен, в который будет входить данный объект Шлюз Безопасности. Если создаваемый Шлюз Безопасности является кластером, то отметить флаг **Этот объект – кластер**.

Шаг 2: Топология

Выбрать закладку *Топология*, чтобы ввести информацию об интерфейсах Шлюза Безопасности.

Указать параметры топологии Объекта следующим образом:

1) Нажать кнопку **Добавить** и ввести логическое имя и IP-адрес первого интерфейса Шлюза Безопасности. Таким же образом указать данные для всех интерфейсов. Можно указывать несколько IP-адресов для одного интерфейса, для этого надо «создать» интерфейс с тем же логическим именем.

2) Если IP-адрес данного интерфейса находится в пределах Зоны, эта Зона отобразится в колонке **Зона** таблицы *Интерфейсы*, иначе там появится значение **Auto** и **Зона** будет создана автоматически. При добавлении IP-интерфейса, находящегося в зоне **Internet**, необходимо выбрать нужный параметр **Зона Интернет** из списка **Привязка к зоне:**, эта Зона отобразится в колонке **Зона** таблицы *Интерфейсы*.

3) Если данный Шлюз Безопасности будет использоваться только как конечная точка для IPsec-туннелей, надо убрать отметку в поле **Включить перенаправление незащищенного трафика**, установленную по умолчанию.

Шаг 3: Местоположение

Перейти на закладку *Местоположение*, чтобы настроить опции **Местоположение** следующим образом:

1) В поле **Координаты** необходимо указать географические координаты Шлюза Безопасности. Координаты можно ввести вручную или присвоить их Шлюзу Безопасности, выбрав кнопку **Указать координаты**.

2) Если известен адрес Шлюза Безопасности его можно найти с помощью поля **Найти**.

3) После определения местоположения необходимо нажать кнопку **Готово.**

Если координаты не указаны, то поле **Координаты** имеет значение «-».

Шаг 4: Виртуальная частная сеть

В закладке *ВЧС* настроить опции ВЧС:

1) Перейти на вложенную закладку *Общее*.

– Если Вы не хотите чтобы Шлюз использовал протоколы IKE и IPsec, надо убрать отметку в поле **Включить IKE/IPsec обработку**, которая установлена по умолчанию. В п. 7.1.2.7 можно найти пример, когда требуется отмена этой функции. В поле **IKE порт** можно изменить порт, который будет использоваться

Шлюзом. В поле **IKE-NAT-T** можно изменить порт, используемый Шлюзом для работы протокола IKE-NAT-Traversal.

– Установить **IP-адрес** Шлюза, который будет использоваться как туннельный. Если туннельный адрес является действительным IP-адресом Шлюза, выбрать из списка один из зарегистрированных IP-адресов интерфейса, или оставить установленное по умолчанию значение **Авто**.

– Отметить типы трафика, которые будут пропускаться Шлюзом без проверки явных Правил ЛПБ в списке *Пропуск трафика*.

2) Перейти на вложенную закладку *Сертификаты* и зарегистрировать сертификаты, если Ваш Шлюз Безопасности будет использовать сертификаты (см. Рисунок 62).

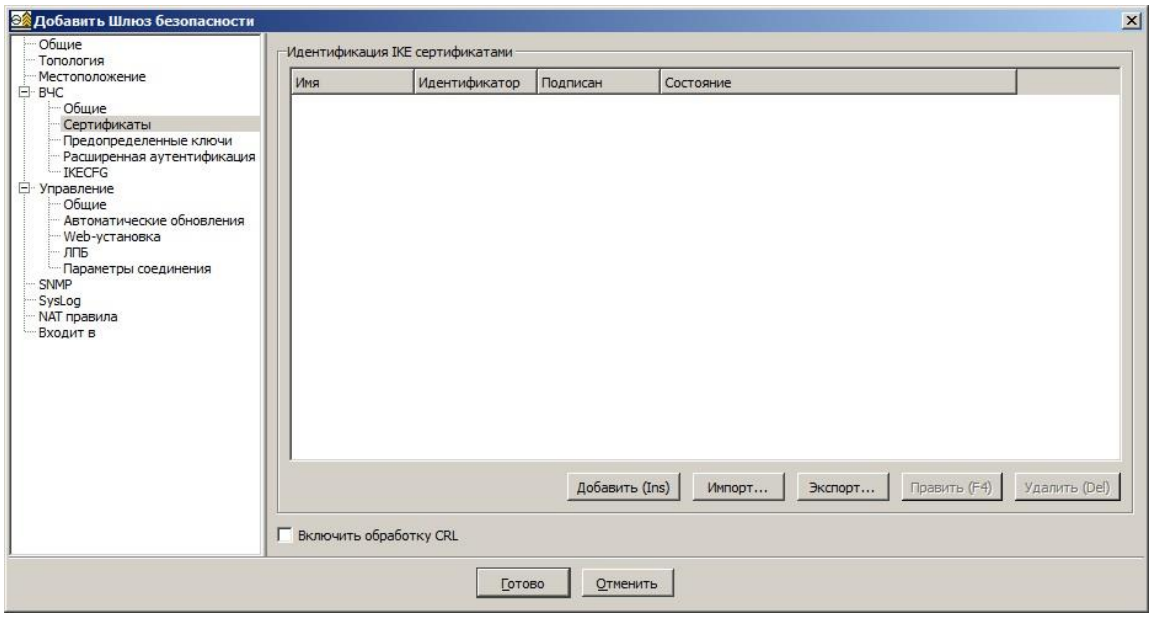

Рисунок 62 – Шлюз Безопасности, закладка *ВЧС*, вложенная закладка *Сертификаты*

Зарегистрировать сертификаты можно следующим образом:

– Чтобы зарегистрировать сертификат надо нажать кнопку **Добавить** и ввести необходимую информацию о сертификате Шлюза Безопасности. Эти данные должны полностью соответствовать данным фактического сертификата; и этот сертификат должен быть зарегистрирован в *ЗАСТАВА-Офис*, который представляет данный Шлюз (подробнее о способах регистрации сертификатов см. п. 7.1.1.1).

– Если *ЗАСТАВА-Офис*, представляемый данным Шлюзом Безопасности будет использовать список отозванных сертификатов (СОС) чтобы подтверждать сертификаты пользователей, поставить отметку в поле **Обработка СОС**.

– Выбрать один или несколько *LDAP серверов* для того, чтобы скачать сертификаты и СОС, которые будет использовать *ЗАСТАВА-Офис.*

3) Если Шлюз Безопасности будет использовать предварительно распределенные ключи, то следует зарегистрировать предварительно распределенные ключи на закладке *Предопределенные ключи*. Это можно сделать следующим образом:

– Перейти на закладку *Предопрелделенные ключи*, нажать кнопку **Добавить** и ввести необходимую информацию о предварительно распределенном ключе (он должен быть зарегистрирован в действующем *ЗАСТАВА-Офис*, который представляет данный Объект Шлюза Безопасности). Выполнить действия, чтобы ввести данные о дополнительных предварительно распределенных ключах, используемых Шлюзом Безопасности.

– Ввести **Имя ключа**. Это имя должно соответствовать имени предварительно распределенного ключа в *ЗАСТАВА-Офис*, который представляет данный Шлюз Безопасности.

– Поставить отметку в поле **Управляемый** (если *Агенты* поддерживают управление значением предварительно распределенных ключей).

– Из выпадающего списка *Партнер* выбрать партнера по связи совместно, с которым данный Объект Политики будет использовать этот ключ.

– Выбрать способ идентификации локального ключа из первого списка *Тип ID ключа*. Таким образом, партнер по связи сможет убедиться в том, что данный ключ является Правильным. По умолчанию для идентификации педваритнльно распределенного ключа будет использован первичный IP-адрес *ЗАСТАВА-Офис*. В этом случае не требуется предоставлять дополнительных сведений. Локальный ключ также может быть идентифицирован с помощью другого IP-адреса, сервиса DNS, ключа ID или шестнадцатеричного идентификатора ключа. В таком случае выбрать тип идентификации ключа из выпадающего списка и ввести значение идентификатора в строке *Значение ID ключа*.

– Выбрать способ идентификации ключа сетевого узла из второго списка *Тип ID ключа*. Это позволит *ЗАСТАВА-Офис* убедиться в том, что данный ключ является Правильным. По умолчанию для идентификации предварительно распределенного ключа будет использован первичный IP-адрес. В этом случае не требуется предоставлять дополнительных сведений. Ключ сетевого узла также может быть идентифицирован с помощью другого IP-адреса, сервиса DNS, ключа

ID или шестнадцатеричного ключа ID. В этом случае выбрать тип идентификации ключа из списка и ввести значение идентификатора в строке *Значение ID ключа.*

4) Перейти на вложенную закладку *Расширенная аутентификация*. Протокол XAUTH используется для расширенной аутентификации при установлении соединения ВЧС с использованием протокола IKE. Таким образом, для опознания удаленного пользователя, Шлюзы будут обращаться на внешний центр аутентификации для получения дополнительных мандатов. Если данный Шлюз Безопасности опознаёт удаленных пользователей/Хосты Безопасности через внешние серверы аутентификации с использованием протокола XAUTH, можно указать это в конфигурации *ЦУП*:

   – Поставить отметку в поле **Включить расширенную аутентификацию EAP/XAUTH**.
   – Выбрать Объекты Безопасности, которые должны быть аутентифицированы с помощью внешнего сервера в списке *Доступные объекты* и переместить их в список *Выбранные объекты*.
   – Добавить внешние серверы аутентификации, к которым будет обращаться Шлюз Безопасности для получения дополнительных мандатов. Объекты серверов TACACS+ и/или RADIUS должны быть заранее созданы в окне *Серверы* (подробнее см. в п. 7.1.1.2).
   – По умолчанию *ЦУП* будет автоматически выбирать интерфейс Шлюза Безопасности, который использует XAUTH, с помощью алгоритма трассировки топологии. Если Вы хотите вручную выбрать интерфейс Шлюза, который будет использовать XAUTH, надо выбрать нужный интерфейс из выпадающего списка.

5) Выбрать вложенную закладку *IKE CFG*. Протокол IKE CFG используется для того, чтобы загружать IP-адрес и другие данные сетевой конфигурации на удаленный клиент ВЧС, как часть предварительного согласования по протоколу IKE. Это помогает избежать маршрутизации ответных пакетов удаленному клиенту ВЧС с локального сервера; также это используется для того, чтобы выделять трафик, поступающий от аутентифицированных удаленных пользователей и затем применять к нему фильтрацию МЭ, используя локальный пул IP-адресов вместо общих Интернет-адресов. Если данный Шлюз Безопасности требует конфигурирования удаленных Хостов Безопасности/ пользователей через IKE CFG, присваивая им IP-адреса в пространстве IP-адресов, расположенном за Шлюзом,

можно отразить это в конфигурации *ЦУП*, создавая Правила IKE CFG, для этого необходимо:

- Выбрать закладку IKE CFG;
- Нажать кнопку **Добавить** и создать Правила IKE CFG:
- Выбрать Объекты Политики, к которым будет применяться протокол IKE CFG из списка *Доступные объекты* и переместить их в список *Выбранные объекты*.
- Указать **Ресурс IP-адресов**, находящийся за Шлюзом Безопасности, из которого будут браться адреса для удаленных Хостов Безопасности / Пользователей.
- Из выпадающего списка выбрать метод, которым будет вводиться **Ресурс IP-адресов** (IP Диапазон, IP Адрес + Маска или DHCP). При выборе метода получения ресурса через DHCP в качестве идентификатора клиента будет направлен адрес, выбранный DHCP-сервером, который первым ответит на запрос (DHCP REQUEST), отправленный со шлюза. При обмене информацией с DHCP-сервера, с которым работает шлюз, запрашиваются следующие параметры: IP-адрес, subnet mask и broadcast addr, DNS.
- В предлагаемое поле ввести подходящие значения для области IP-адресов.
- Указать **Broadcast-маску** и адрес **DNS-сервера** в поле **Дополнительные параметры**.

Шаг 5: Управление *Агентами*

Выбрать закладку *Управление*. Эта закладка предназначена для установки Политики драйвера, которая будет использована по умолчанию, настройки уровней регистрации событий для *ЗАСТАВА-Офис*, а также для управления его ЛПБ и установки соединений.

1) Выбрать вложенную закладку *Общее*:

- Установить Политику, которую будет использовать Шлюз Безопасности по умолчанию в поле **Политика по умолчанию**. Эта Политика (**Пропустить всех** или **Запретить всех**) будет применяться при взаимодействии с теми узлами сети, для которых ЛПБ *ЦУП* не предусматривает точных Правил.
- Если Вы хотите, чтобы Шлюз Безопасности автоматически пропускал широковещательный трафик Broadcast, трафик с групповыми адресами Multicast и/или ICMP-трафик, надо поставить соответствующие флажки (**Пропуск Broadcast, Пропуск Multicast** или **Пропуск ICMP**).
- Установить уровни регистрации событий Шлюза Безопасности Уровни Лога для различных типов событий. Эта настройка аннулирует любые настройки уровней

регистрации, сделанные в самом *ЦУП*. Для того чтобы использовать настройки уровней регистрации *ЗАСТАВА-Офис* надо выбрать в выпадающем списке значение **По умолчанию**.

2) Выбрать вложенную закладку *Автоматические обновления:*

– Определить необходимую информацию об Автоматическом обновлении для Шлюза Безопасности как указано в п. 7.1.1.4.

3) Выбрать закладку *Web-установка* свойств объекта:

– Отметить флажок **Разрешить доступ по WEB**, для получения начального конфигурационного пакета;
– В поле **Имя пользователя** надо задать произвольный логин для доступа Пользователя к *ЦУП*;
– В поле **Пароль** при помощи кнопки **Изменить** надо задать пароль.

4) Выбрать вложенную закладку *ЛПБ*.

Блоки **Локальная Политика Безопасности** и **Структура ЛПБ** будут доступны только после трансляции ГПБ и создания ЛПБ для данного Шлюза Безопасности. Если Вы не хотите, чтобы в следующий раз при трансляции ГПБ для этого Шлюза Безопасности была создана ЛПБ (например, если Вы вручную внесли изменения в текущую ЛПБ Шлюза Безопасности, и хотите сохранить установки), надо поставить отметку в поле **Не транслировать ЛПБ**. Таким образом, трансляция ЛПБ будет отменена для этого Шлюза до тех пор, пока не будет убрана отметка.

5) Выбрать закладку *Параметры соединения*:

– Выбрать *Метод загрузки ЛПБ*. Если Вы хотите для передачи начальной ЛПБ использовать метод автоматизированной передачи ЛПБ надо выбрать метод прогрузки политики PMPv2. Передача ЛПБ с помощью метода прогрузки «direct access» используется для *Агента*, на котором установлен *ЦУП*.
– Убедиться в том, что PMP Server (т.е. *ЦУП*) находится в списке *Удалённых серверов* (подробнее см. п. 7.1.1.2).

Шаг 6: Настройка SNMP

Нажать на закладке *SNMP* и поставить отметку в поле **Включить SNMP**, если Вы хотите установить SNMP-мониторинг для данного Шлюза Безопасности. Затем установить настройки SNMP следующим образом (В п. 7.1.2.7 можно найти полный список SNMP-сообщений):

1) По умолчанию порт SNMP клиента установлен на **3454**, а значение среды SNMP – на **public**. При необходимости эти значения могут быть изменены в соответствующих полях.

Для аутентификации сообщений SNMP использует имена сообщества (*community names*). Имя сообщества можно считать паролем, совместно используемым SNMP-серверами и SNMP-*Агентами*. Все SNMP-сообщения должны содержать имя сообщества. Сообщения, содержащие имя сообщества, которое не установлено на хосте, не будут приняты.

2) Если Вы хотите, чтобы Шлюз всегда пропускал SNMP-трафик без предварительной проверки Правил ЛПБ, надо поставить отметку в поле **Включить правило**.

Несмотря на то, что существует опция автоматического пропуска “SNMP autopass”, рекомендуется создать Правило для пропуска SNMP-трафика, поступающего со Шлюза Безопасности на SNMP-сервер – т.к. это безопаснее.

3) Выбрать один или несколько SNMP-серверов, на которые *ЗАСТАВА-Офис* будет отправлять SNMP-сообщения. Обратите внимание, что в списке появятся только те серверы, которые были предварительно зарегистрированы в окне *Серверы* (подробнее см. п. 7.1.1.2).

4) Выбрать SNMP-сообщения, которые данный *ЗАСТАВА-Офис* будет посылать на SNMP-серверы, перемещая их из списка *Доступные* в список *Выбранные*.

Шаг 7: Принадлежность к группе

На закладке *Входит в* показано, к каким Группам принадлежит данный Шлюз Безопасности. Можно добавить Шлюз в существующую Группу или удалить его из нее. На закладке содержатся два списка: в первом (**Доступные группы**) показан полный перечень Групп, зарегистрированных в папке *Группы* в секции *Объекты политики;* (за исключением тех Групп, в которых в данный момент состоит Шлюз Безопасности); во втором (**Выбранные группы)** перечислены Группы, в которых в данный момент состоит Шлюз Безопасности

Чтобы изменить состав Группы и добавить в Группу созданный Шлюз Безопасности необходимо переместить нужную Группу из списка *Доступные группы* в список *Выбранные группы*, используя кнопки со стрелками.

Шаг 8: SysLog

Для сбора сообщений по протоколу SysLog от *Шлюза Безопасности* необходимо добавить SysLog-сервер, для этого нужно нажать кнопку **Добавить** в вкладке *Syslog* и выбрать сервер из списка.

Появятся только те серверы, которые были заранее зарегистрированы в окне *Серверы*. Единственным исключением является Syslog-сервер (представленный сервисом **TPNSyslog**), который автоматически создается на хосте *ЦУП* при установке *ЦУП*, и, таким образом, всегда находится в списке (подробнее см. п. 7.1.1.2).

Шаг 9: NAT Правила

Если для данного объекта необходимо учесть/сконфигурировать трансляцию сетевых адресов (NAT, Network Address Translation) надо обратиться к п. 7.1.1.3.

Шаг 10: Завершение создания Шлюза

Нажать кнопку **Готово** Шлюз Безопасности будет добавлен в *Граф топологии* и папку *Сетевые Объекты* в секции *Объекты политики*.

7.1.2.3. *ЗАСТАВА-Офис* в кластерном исполнении

ЗАСТАВА-Офис может быть установлен и сконфигурирован для работы в режиме высокой надёжности (High Availability) на кластерной информационной системе. Для описания процесса установки *ЗАСТАВА-Офис* в режиме высокой надёжности надо обратиться к документу МКЕЮ.00434-01 32 01 Компонент «ЗАСТАВА-Офис», версия 6. «Руководство системного программиста».

Для прогрузки кластера необходимо выполнить следующие действия:

— создать объект *Хост безопасности* (Сервер) или *Шлюз безопасности* (см. п. 7.1.2.2) с типом дескриптора *Агент* версии 6.0;
— на вкладке *Общее* поставить галочку **Кластер** и выбрать количество узлов;
— в конфигурации топологии задать под одним именем адреса всех узлов кластера и непосредственно кластерный адрес(а);
— на вкладке *ВЧС/общее* в качестве туннельного адреса задать кластерный адрес;
— зарегистрировать локальные сертификаты каждого узла на вкладке *ВЧС/сертификаты*;
— соответственно в *Агентах* на узлах кластера зарегистрировать эти сертификаты в качестве локальных и дать имена интерфейсам;
— создать правило, оттранслировать и проактивировать конфигурацию.

Для дескриптора *Агента* версии 6.1 и выше доступна загрузка сертификатов для каждого узла кластера. Для этого необходимо воспользоваться контекстным меню *Объекта политики*: Выбрать пункт **Загрузить список сертификатов,** в окне *Выберите узел кластера* маркером выбрать номер узла кластера и нажать кнопку **Готово**. После загрузки сертификатов необходимо выполнить пункт **Добавить полученные сертификаты в политику**. В появившемся окне *Импорт сертификатов* проверить полученные из *Агента* сертификаты и нажать кнопку **Готово.**

Для дескриптора *Агента* версии 6.1 и выше доступно обновление и загрузка обновлений для каждого узла кластера. Для этого необходимо воспользоваться контекстным меню *Объекта политики*.

При обновлении кластера с версией дескриптора *Агента* выше 6.1 существует возможность обновить отдельно каждый узел кластера, для этого после выбора необходимого действия с помощью команд контекстного меню *Агент* **Загрузить обновления для агента** или **Обновить версию агента** в появившемся окне *Выберите узел кластера* с помощью маркера надо выбрать номер узла кластера. Если оставить маркер в значении «0», то действие будет выполнено для всех узлов кластера.

При импорте ГПБ, в которой не были заданы номера узлов кластера для локальных сертификатов на вкладке *ВЧС/сертификаты*, это произойдет автоматически по следующему алгоритму:

1) У сертификатов с ненулевым номером узла, но на НЕ кластерах, номер узла сбрасывается в 0.

2) У сертификатов с нулевым номером узла (или номером узла больше размера кластера) на кластерах номер узла выбирается следующим образом: первый номер, для которого еще нет сертификата, такие сертификаты рассматриваются в алфавитном порядке по полю sn.

3) Если свободных номеров нет, то номер узла не меняется.

Во всех трех случаях генерируются предупреждения:

- при старте TPNServer и загрузке БД, в которой есть такие сертификаты, предупреждения пишутся в vdb_server.log.
- при импорте xml, в которой есть такие сертификаты, предупреждения также будут показаны в логе исполнения.

После этого можно прогружать *Агенты* с *ЦУП* по протоколу PMPv2.

7.1.2.4. Маршрутизаторы Cisco и МЭ PIX Firewalls

Установить курсор в секции *Топология* или выбрать вкладку *Сетевые Объекты* в секции *Объекты политики*, выполнить команду **Добавить->Шлюз Безопасности**. Откроется окно *Выбор Дескриптора Агента*.

Шаг 1: Общие характеристики

На закладке *Общее* нужно сделать следующее:

1) Указать производителя и версию *Агента*, которого будет представлять этот Шлюз Безопасности в окне *Выбор Дескриптора Агента*.

Имя Объекта Шлюза Безопасности, представляющего устройство Cisco должно начинаться с буквы и содержать только латинские буквы, цифры, дефис, точку и символы подчеркивания. После создания этих Объектов *ЦУП* проверит их имена и, если Вы использовали неприемлемый символ, выведет сообщение об ошибке.

2) На закладке *Общее* ввести **Имя** объекта Шлюза Безопасности.

3) В строке *Адрес Агента* набрать IP-адрес Шлюза, который будет представлять этот Объект. Именно на этот адрес *ЦУП* будет отправлять ЛПБ для данного Объекта.

4) Можно ввести текстовое описание Объекта в строке *Описание.*

Шаг 2: Топология

Перейти на закладку *Топология*, чтобы ввести данные об интерфейсах Шлюза Безопасности (если эта информация не была восстановлена через SNMP, как отмечено выше). На закладке *Топология* нужно сделать следующее:

1) Нажать кнопку **Добавить** и ввести **Логическое имя** и **IP-адрес** первого интерфейса Шлюза Безопасности. Повторить эту операцию для всех интерфейсов Шлюза Безопасности. Для одного интерфейса можно указать несколько адресов; для этого надо создать дополнительные интерфейсы с тем же логическим именем. Если IP-адрес данного интерфейса находится в пределах Зоны, эта Зона отобразится в колонке *Зона* таблицы интерфейса, иначе там появится значение **Auto**, и **Зона** будет создана автоматически. При добавлении IP-интерфейса, находящегося в зоне **Internet**, необходимо выбрать **Зона Интернет** из выпадающего списка.

Для Cisco PIX Firewall необходимо указать уровень защиты интерфейса. Для этого после имени интерфейса напечатайте несколько пробелов, а затем ввести число от 0 до 99. *ЦУП* предусматривает два зарезервированных имени для интерфейсов: inside (внутреннее), уровень защиты которого равен 100 и outside (внешнее), уровень защиты которого равен 0. В том случае, когда для интерфейса используется резервное имя, можно опустить параметр уровня защиты.

При автоматической привязке интерфейс привязывается к оптимальной зоне. Если интерфейс целиком попадает в одну или несколько постоянных зон, то оптимальной считается наименьшая из них, иначе оптимальной считается временно созданная auto-зона. Если оптимальная зона меняется (например, из-за того, что удаляются, создаются или меняются определенные зоны), такой интерфейс автоматически переприязывается к другой подходящей зоне.

При жесткой привязке интерфейс привязывается к произвольной, определенной пользователем зоне или Internet-зоне. При изменениях топологии переприязка не происходит.

2) Если Шлюз Безопасности будет использоваться только как конечный пункт IPsec-туннелей надо отменить установленную по умолчанию отметку в поле **Включить перенаправление незащищенного трафика**.

Шаг 3: Местоположение

Перейти на закладку *Местоположение*, чтобы настроить опции *Местоположение* следующим образом:

1) В поле **Координаты** необходимо указать географические координаты Шлюза Безопасности. Координаты можно ввести вручную или присвоить их Шлюзу Безопасности, выбрав кнопку **Указать координаты**.
2) Если известен адрес Шлюза Безопасности, его можно найти с помощью поля **Найти**.
3) После определения местоположения необходимо нажать кнопку **Готово.**

Если координаты не указаны, то поле **Координаты** имеет значение «-».

Шаг 4: Виртуальная частная сеть

Перейти на закладку *ВЧС*, чтобы установить опции ВЧС.

1) Выбрать вложенную закладку *Общее*.
2) Если Вы не хотите, чтобы Шлюз Безопасности использовал протоколы IKE или IPsec, надо отменить отметку в поле **Включить IKE/IPsec** (установленную по умолчанию). В п. 7.1.2.7 можно найти пример, когда может понадобиться отменить эту установку. В поле **IKE port** можно изменить порт, который Шлюз будет использовать для IKE-трафика. В поле **IKE-NAT-T** можно изменить порт, используемый Шлюзом для работы протокола IKE-NAT-Traversal.
3) Выбрать виды трафика, которые будут автоматически пропускаться Шлюзом без предварительной проверки явных Правил ЛПБ, для этого надо поставить отметки в соответствующих полях в **Автопропуск трафика**.
4) Выбрать вложенную закладку *Сертификаты*, чтобы зарегистрировать сертификаты. Это делается следующим образом:
   - Нажать кнопку **Добавить** и ввести необходимую информацию о сертификате Шлюза Безопасности. Эта информация должна точно совпадать с информацией действительного сертификата; этот сертификат должен быть зарегистрирован на действительном устройстве Cisco, которое представляет данный Объект Шлюза Безопасности (подробнее о способах добавления сертификатов см. п. 7.1.1.1).

- Выбрать УЦ, выдавший сертификат, из выпадающего списка (обратите внимание, что эта информация обязательно для Cisco IOS версий 12.2 и выше). В списке содержатся названия всех УЦ, зарегистрированных в окне *Серверы*.
- Если устройство Cisco будет использовать СОС для подтверждения сертификатов предполагаемых партнеров по связи, надо поставить отметку в поле **Обработка СОС**.
- Добавить один или несколько LDAP-серверов, которые будет использовать устройство Cisco для того, чтобы загрузить сертификаты и СОС, используя соответствующую команду **Добавить**. Обратите внимание, что в списке появятся только те LDAP-серверы, которые были заранее зарегистрированы в окне *Серверы* (подробнее см. п. 7.1.1.1).

5) Если Шлюзы Безопасности будут использовать пердварительно распределенные ключи, в этом случае необходимо выбрать вложенную закладку *Предопределенные ключи*, чтобы зарегистрировать предварительно распределенные ключи. Это можно сделать следующим образом:

   Нажать кнопку **Добавить** в поле **IKE Preshared Key Identities** и ввести необходимую информацию о предварительно распределенном ключе. Данный предварительно распределенный ключ должен быть зарегистрирован на фактическом устройстве Cisco, которое представляет данный Шлюз Безопасности, если значение этого предварительно распределенный ключа не управляется *ЦУП*. Ввести информацию обо всех предварительно распределенных ключах, используемых Шлюзом Безопасности, для этого необходимо выполнить следующее:

   - Ввести имя данного ключа.
   - Поставить отметку в поле **Шестнадцатеричная строка**, если Вы хотите ввести значение ключа в шестнадцатеричном формате.
   - Поставить отметку в поле **Управляемый**, если *ЦУП* управляет значением данного ключа.
   - Ввести значение ключа. Если Вы поставили отметку в поле **Шестнадцатеричная строка**, в поле **Значение ключа** надо ввести шестнадцатеричную последовательность с четным количеством знаков. Иначе, надо ввести значение в буквенно-цифровом формате.
   - Из выпадающего списка *Партнер* выбрать узел сети, совместно с которым данный Объект Политики использует этот ключ.

– Из первого выпадающего списка *Тип ID ключа* выбрать способ идентификации локального ключа. Это позволит узлу сети убедиться в том, что ключ является Правильным. По умолчанию, для идентификации предопределенного ключа будет использован первичный IP-адрес устройства Cisco. В этом случае не требуется вводить дополнительных данных. Локальный ключ может также быть идентифицирован с помощью другого IP-адреса, сервиса DNS, ID ключа или шестнадцатеричного ID ключа. В таком случае надо выбрать тип идентификации из выпадающего списка и ввести значение идентификатора в поле **Значение ID ключа.**

6) Выбрать способ идентификации ключа сетевого узла из второго выпадающего списка *Тип ID ключа*. Таким образом, устройство Cisco сможет убедиться в том, что данный ключ является Правильным. По умолчанию, для идентификации предопределенного ключа будет использоваться первичный IP-адрес сетевого узла. В данном случае не требуется указывать дополнительных данных. Ключ сетевого узла может также быть идентифицирован с помощью другого IP-адреса, сервиса DNS, ID ключа или шестнадцатеричного ID ключа. В таком случае выбрать тип ID ключа из выпадающего списка и ввести значение этого идентификатора в поле **Значение ID ключа**.Протокол XAUTH используется для более полной аутентификации при установлении VPN соединения с использованием протокола IKE. Таким образом, Шлюзы могут аутентифицировать удаленных пользователей, обратившись к внешнему серверу аутентификации для получения дополнительных мандатов. Если данный Шлюз Безопасности проводит аутентификацию удаленных пользователей/ Хостов Безопасности через внешний сервер аутентификации с помощью протокола XAUTH, можно отразить это в настройках *ЦУП*. Выбрать вложенную закладку *Расширенная аутентификация* (если она доступна), и сделать следующее:

– Поставить отметку в поле **Включить XAUTH**.

Только для PIX Firewall.
Если Вы хотите, чтобы сервер XAUTH предоставлял удаленным пользователям информацию об авторизации в виде списков доступа, надо поставить отметку в поле *Внешняя аутентификация*.

– Выбрать Объекты Политики, которые должны быть идентифицированы с помощью внешнего сервера в списке *Доступные объекты* и переместить их в список *Выбранные объекты*.

- Выбрать внешние Серверы аутентификации, которые Шлюз Безопасности будет проверять на наличие дополнительных мандатов в списке *Серверы аутентификации* (Для этого Вы должны были заранее создать Объекты серверов TACACS+ и/или RADIUS в окне *Серверы*). Подробнее см. п. 7.1.1.2.
- По умолчанию, *ЦУП* будет автоматически выбирать тот интерфейс Шлюза Безопасности, который будет использоваться для XAUTH с помощью алгоритма трассировки топологии. Если Вы хотите вручную установить интерфейс, который будет использоваться для XAUTH, надо выбрать нужный интерфейс из выпадающего списка.
- Протокол **IKE CFG** используется для того, чтобы загружать IP-адрес и другие данные сетевой конфигурации на удаленный *ВЧС-Клиент*, как часть процесса предварительного согласования IKE. В первую очередь это используется для того, чтобы избежать маршрутизации ответных пакетов с локального сервера удаленному *ВЧС-Клиенту*. Также это позволяет выделять трафик, исходящий от идентифицированных удаленных пользователей, и затем применить к нему фильтрацию МЭ, используя локальный пул IP-адресов, вместо общих адресов глобальной сети. Если данный Шлюз Безопасности требует конфигурирования удаленных Хостов Безопасности/пользователей через IKE CFG, присваивая им IP-адреса в пространстве IP-адресов, расположенном за Шлюзом, можно отразить это в конфигурации *ЦУП*, создавая Правила IKE CFG. Создание правила IKE CFG происходит следующим образом:
- Перейти на закладку **IKECFG**;
- Нажать кнопку **Добавить** и создать Правила IKE CFG:
- Выбрать Объекты Политики, к которым будет применяться протокол IKE CFG из списка *Доступные объекты* и переместить их в список *Выбранные объекты*.
- Указать **Ресурс IP-адресов**, находящийся за Шлюзом Безопасности, из которого будут браться адреса для удаленных Хостов Безопасности / Пользователей. Из выпадающего списка выбрать метод, которым будет вводиться **Ресурс IP-адресов** (IP Диапазон, IP Адрес + Маска или DHCP). При выборе метода получения ресурса через DHCP в качестве идентификатора клиента будет направлен адрес, выбранный DHCP-сервером, который первым ответит на запрос (DHCP REQUEST), отправленный со шлюза. При обмене информацией с DHCP-сервера, с которым работает шлюз, запрашиваются следующие параметры: IP-адрес, subnet mask и broadcast addr, DNS.

- В предлагаемое поле ввести подходящие значения для области IP-адресов.
- Указать **Broadcast-маску** и адрес **DNS-сервера** в поле **Дополнительные параметры**.

Шаг 5: Управление *Агентом*

1) Выбрать вложенную закладку *Управление*. Эта закладка предназначена для установки Политики драйвера, которая будет использована по умолчанию, уровней регистрации для *ЗАСТАВА-Офис*, а также для управления его ЛПБ.

2) Выбрать вложенную закладку *Общее*:

   - Установить Политику, которую будет использовать Шлюз Безопасности по умолчанию. Эта Политика **Пропустить всех** или **Запретить всех** будет применяться при взаимодействии с теми узлами сети, для которых ЛПБ устройства Cisco не предусматривает точных Правил.
   - Если Вы хотите, чтобы Шлюз Безопасности автоматически и/или через ICMP-трафик делал установки, надо сделать соответствующие отметки.
   - Установить уровни регистрации событий Шлюза Безопасности для консоли Cisco.

3) Выбрать вложенную закладку *ЛПБ*:

   - Блоки *Локальная Политика Безопасности* и *Структура ЛПБ* будут доступны только после трансляции ГПБ и создания ЛПБ для данного Шлюза Безопасности. Если Вы не хотите, чтобы в следующий раз при трансляции ГПБ для этого Шлюза Безопасности была создана ЛПБ (например, если Вы вручную внесли изменения в текущую ЛПБ Шлюза Безопасности, и хотите сохранить установки), надо поставить отметку в поле **Не транслировать ЛПБ.** Таким образом, трансляция ЛПБ будет отменена для этого Шлюза до тех пор, пока не будет убрана отметка.

4) Выбрать вложенную закладку *Параметры соединения*. Эти параметры управляют процессом коммуникации между сервисом *ЦУП* и маршрутизатором Cisco/МЭ PIX Firewall во время активации ГПБ.

   Указать параметры соединения Объекта следующим образом:

   - Выбрать режим коммуникации, который будет использован между устройством Cisco и *ЦУП*: SSH версии 1 или telnet.
   - Ввести **Имя** пользователя, чтобы *ЦУП* мог получить доступ к устройству Cisco.

– Ввести пользователя (SSH/telnet) и пароли, чтобы *ЦУП* мог получить доступ к устройству Cisco.

Если Вы хотите сохранять данные о том, были ли внесены изменения в ЛПБ пользователя с момента последней активации, надо поставить отметку в поле **Отслеживание целостности ЛПБ.** В поле **Удаленные Серверы** определяют сервер (*ЦУП* случай), который распределит ЛПБ этим Шлюзам Безопасности. Подробнее см. п. 7.1.1.2.

Шаг 6: Настройка SNMP

1) Выбрать закладку *SNMP* и поставить отметку в поле **Включить SNMP**, если Вы хотите установить текущий контроль SNMP для данного Шлюза Безопасности. Затем установить настройки SNMP, полный список сообщений SNMP можно найти в п. 7.1.2.7.

2) По умолчанию, порт SNMP-Клиента **Порт клиента** установлен на **161**, а значение SNMP-сообщества **Группа** по умолчанию – на **public**.

Для аутентификации сообщений SNMP использует имена сообщества (community name). Имя сообщества можно считать кодом доступа, который совместно используется SNMP-серверами и *Агентами* SNMP. Все сообщения SNMP должны содержать имя сообщества. Если сообщение содержит имя сообщества, которое не настроено на хосте, оно будет отклонено.

3) Выбрать один или несколько SNMP-серверов в **SNMP-серверы**, на которые данный Шлюз Безопасности будет посылать SNMP-сообщения.

В списке *Доступные* появятся только те серверы, которые были ранее зарегистрированы в окне *Серверы* (подробнее см. в подразделе 7.9).

Шаг 7: Настройка журнала регистрации Syslog Distributor

Системный журнал позволяет *Агентам* посылать регистрационные данные на удаленный сервер в стандартизованном формате. Для того чтобы установить отправку данных журнала регистрации с данного устройства Cisco надо в контекстном меню выбрать параметр **Включить** и сделать следующее:

1) Установить уровень регистрации для отправки отчетов о событиях системного журнала регистрации. Все сообщения системного журнала регистрации с уровнем регистрации ниже установленного не будут отправляться на Syslog-сервер.
2) Выбрать один или несколько Syslog-серверов, на которые данный Шлюз будет отправлять сообщения журнала регистрации.
3) При необходимости настроить отображение логирования в окне Syslog.

Шаг 8: Принадлежность к группе

На закладке *Входит в* показано, к каким группам принадлежит данный Шлюз Безопасности. Можно добавить Шлюз в существующую группу или удалить его из нее. На закладке содержатся два списка: в первом *Доступные группы* показан полный перечень Групп, зарегистрированных в папке *Группы* в секции *Объекты Политики* (за исключением тех Групп, в которых в данный момент состоит Шлюз Безопасности); во втором *Выбранные группы* перечислены Группы, к которым в данный момент принадлежит Шлюз Безопасности.

Чтобы изменить состав Группы и добавить в Группу созданный Шлюз Безопасности необходимо переместить нужную Группу из списка *Доступные группы* в список *Выбранные группы*, используя кнопки со стрелками.

Шаг 9: Правила NAT

Если для данного объекта необходимо учесть/сконфигурировать трансляцию сетевых адресов (NAT, Network Address Translation) надо обратиться к п. 7.1.1.3.

Шаг 10: Завершение создания Шлюза

Нажать кнопку **OK**. Шлюз Безопасности будет добавлен в Топологию ВЧС и папку *Сетевые Объекты* в секции *Объекты Политики*.

7.1.2.5. Шлюзы Безопасности Microsoft IPsec *Агент*

Агенты IPsec, входящие в ОС Windows XP и 2003, также можно определить, как Шлюзы Безопасности. Установить курсор на секцию *Топология ВЧС* или выбрать папку *Сетевые объекты* в секции *Объекты политики*, используя команду **Добавить->Шлюз Безопасности**.

Шаг 1: Общие характеристики

1) Указать производителя и версию *Агента*, которого будет представлять этот Шлюз Безопасности в окне *Выбор Дескриптора Агента*.
2) На закладке *Общее* ввести **Имя** объекта Шлюза Безопасности.
3) В строке *Адрес Агента* набрать IP-адрес Шлюза, который будет представлять этот Объект. Именно на этот адрес *ЦУП* будет отправлять ЛПБ для данного Объекта.
4) Если Вы хотите создать неуправляемый Шлюз Безопасности, надо убрать отметку в поле **Управляемый.**
5) При необходимости можно также ввести текстовое описание Объекта.

Шаг 2: Топология

Перейти на закладку *Топология*, чтобы ввести информацию об интерфейсах Шлюза Безопасности (если эта информация не была восстановлена через SNMP, как отмечено выше):

- Нажать кнопку **Добавить** и ввести логическое имя и IP-адрес первого интерфейса Шлюза Безопасности. Таким же образом ввести данные всех интерфейсов Шлюза Безопасности. Для одного интерфейса можно указывать несколько IP-адресов, для этого необходимо создать дополнительные интерфейсы с тем же логическим именем.
- Если IP-адрес данного интерфейса попадает в пределы какой-либо Зоны, эта Зона отобразится в колонке *Зона* таблицы *Интерфейсы*, иначе там появится значение **Auto** и **Зона** будет создана автоматически. При добавлении IP-интерфейса, находящегося в зоне **Internet**, необходимо в поле **Привязка к зоне:** выбрать параметр **Зона Интернет**, эта зона отобразится в колонке *Зона* таблицы *Интерфейсы*.
- Если данный Шлюз Безопасности будет использоваться только в качестве конечной точки для туннелей IPsec, надо убрать отметку в поле **Включить перенаправление незащищенного трафика** (она установлена по умолчанию).

При автоматической привязке интерфейс привязывается к оптимальной зоне. Если интерфейс целиком попадает в одну или несколько постоянных зон, то оптимальной считается наименьшая из них, иначе оптимальной считается временно созданная auto-зона. Если оптимальная зона меняется (например, из-за того, что удаляются, создаются или меняются определенные зоны), такой интерфейс автоматически перепривязывается к другой подходящей зоне.

При жесткой привязке интерфейс привязывается к произвольной, определенной пользователем зоне или Internet-зоне. При изменениях топологии перепривязка не происходит.

Шаг 3: Местоположение

Перейти на закладку *Местоположение*, чтобы настроить опции *Местоположение* следующим образом:

1) В поле **Координаты** необходимо указать географические координаты Шлюза Безопасности. Координаты можно ввести вручную или присвоить их Шлюзу Безопасности, выбрав кнопку **Указать координаты**.
2) Если известен адрес Шлюза Безопасности его можно найти с помощью поля **Найти**.
3) После определения местоположения необходимо нажать кнопку **Готово.**

Если координаты не указаны, то поле **Координаты** имеет значение «-».

Шаг 4: Виртуальная частная сеть

Перейти на закладку *ВЧС***,** чтобы настроить опции ВЧС.

1) Выбрать вложенную закладку *Общее*.

– Если Вы не хотите, чтобы Шлюз Безопасности использовал IKE или IPsec, надо убрать отметку в поле **Включить IKE/IPsec обработку** (она установлена по умолчанию). В п. 7.1.2.7 можно найти пример того, когда может потребоваться отмена этой опции. Можно изменить порт, который будет использоваться шлюзом для IKE-трафика в поле **IKE порт**. В поле **IKE-NAT-T** можно изменить порт, используемый шлюзом для работы протокола IKE-NAT-Traversal.

– Установить IP-адрес, который будет использоваться для туннелирования. Если адрес туннеля является фактическим IP-адресом, из выпадающего списка выбрать один из зарегистрированных IP-адресов интерфейсов или оставить значение **Авто**, установленное по умолчанию.

2) Перейти на закладку *Сертификаты*, чтобы зарегистрировать сертификаты. Это делается следующим образом:

– Нажать кнопку **Добавить** в поле **Идентификатор IKE сертификата** и ввести необходимые данные о сертификате Шлюза Безопасности. Эти данные должны в точности соответствовать данным настоящего сертификата; этот сертификат будет зарегистрирован в фактическом *Агенте* Microsoft IPsec, которого будет представлять данный Объект. Следуйте инструкциям, описанным в п. 7.1.1.1, чтобы ввести информацию обо всех дополнительных сертификатах данного Шлюза Безопасности. Другие способы добавления сертификатов см. в п. 7.1.1.1.

– Выбрать **LDAP сервер**, который будет использоваться с Microsoft IPsec *Агентом*, чтобы загрузить сертификаты. Обратите внимание, что LDAP-серверы, возможно, были уже зарегистрированы в окне *Серверы*. См. подробнее п. 7.1.1.2.

– Если Ваш Шлюз Безопасности будет использовать предвариетльно распределенные ключи, то надо перейти на вложенную закладку *Предопределенные ключи*, чтобы зарегистрировать предвариетльно распределенные ключи. Это делается следующим образом:

  – Нажать кнопку **Добавить** в поле **Identities согласованного ключа для IKE** и ввести необходимую информацию о предопределенном ключе. Этот предварительно распределенный ключ должен быть заранее зарегистрирован в фактическом *Агенте* Microsoft IPsec, которого представляет данный Объект.

Следуйте инструкциям, описанным ниже, чтобы ввести информацию обо всех дополнительных сертификатах данного Шлюза Безопасности.

- Ввести имя для данного ключа.
- Поставить отметку в поле **Шестнадцатеричная строка**, если Вы хотите ввести значение ключа в шестнадцатеричном формате.
- Поставить отметку в поле **Управляемый**, если значение данного предварительно распределенного ключа не управляется *ЦУП*.
- Ввести значение ключа. Если Вы поставили отметку в поле **Шестнадцатеричная строка** надо ввести в поле **Значение ключа** шестнадцатеричную строку с четным количеством символов. В противном случае надо ввести буквенно-цифровое значение ключа.
- Из выпадающего списка *Партнер* выбрать партнера по связи, совместно с которым данный Объект Политики будет использовать этот ключ.
- Из первого выпадающего списка *Тип ID ключа* выбрать способ идентификации локального ключа. Это позволит партнеру по связи удостовериться в том, что данный ключ является Правильным. По умолчанию, для идентификации предопределенного ключа будет использоваться первичный IP-адрес устройства ВЧС. В этом случае не требуется указывать дополнительной информации. Локальный ключ также может быть идентифицирован с помощью другого IP-адреса, DNS, ID-ключа или шестнадцатеричного ID-ключа. В этом случае выбрать тип идентификации ключа из выпадающего списка и ввести значение выбранного идентификатора в поле **Значение ID ключа.**

Из второго выпадающего списка *Тип ID ключа* выбрать способ идентификации ключа партнера по связи. Это позволит устройству ВЧС удостовериться в том, что данный ключ является Правильным. По умолчанию, для идентификации предвариетльно распределенного ключа будет использован первичный IP-адрес партнера по связи. В этом случае нет необходимости указывать дополнительную информацию. Ключ партнера по связи может также быть идентифицирован при помощи другого IP-адреса, DNS, ID-ключа или шестнадцатеричного ID-ключа. В таком случае выбрать из выпадающего списка способ идентификации ключа и ввести значение выбранного идентификатора в поле **Значение ID ключа**.

Шаг 5: Управление *Агентами*

Перейти на вложенную закладку *Управление*, чтобы установить Политику драйвера для *Агента* Microsoft IPsec, которая будет использоваться по умолчанию, а также для управления ЛПБ и настройки опций соединений.

Указать параметры для управления *Агентом* следующим образом:

1) Выбрать вложенную закладку *Общее*, чтобы установить Политику, которую будет использовать данный Шлюз Безопасности по умолчанию. Эта Политика

(**Пропустить всех** или **Запретить всех**) будет использоваться для тех партнеров по связи, для которых ЛПБ *Агента* Microsoft IPsec не предусматривает точных Правил. Если Вы хотите, чтобы Шлюз Безопасности автоматически пропускал широковещательный трафик **Пропуск broadcast**, трафик с групповыми адресами **Пропуск multicast** и/или трафик **Пропуск ICMP**, надо пометить соответствующие флажки (**Пропуск Broadcast, Пропуск Multicast** или **Пропуск ICMP**).

2) Выбрать вложенную закладку *ЛПБ*. Внимание: блоки *Локальная Политика Безопасности* и *Структура ЛПБ* будут доступны только после трансляции ГПБ и создания ЛПБ для данного Шлюза Безопасности. Если Вы не хотите, чтобы ЛПБ для данного Шлюза Безопасности создавалась в следующий раз, при трансляции ГПБ (например, если Вы вручную внесли изменения в текущую ЛПБ и хотите сохранить эти настройки, надо поставить отметку в поле **Не транслировать ЛПБ**). Трансляция ЛПБ для данного Шлюза будет прекращена до тех пор, пока не будет убрана эта отметка.

3) Перейти на вложенную закладку *Параметры соединения.*

4) Выбрать **Метод загрузки ЛПБ** на данный *Агент* Microsoft IPsec.

5) Если Вы хотите сохранить данные о том, были ли внесены изменения в ЛПБ Шлюза Безопасности с момента последней активации, надо поставить отметку в поле **Отслеживание целостности ЛПБ**. В меню *Просмотр* сразу же после трансляции ГПБ и активации ЛПБ **Проверить целостность** напротив Объекта пользователя появится иконка статуса целостности ЛПБ. Подробнее см. в п. 8.4.4 и в п. 7.1.1.2.

Шаг 6: Настройка SNMP

Перейти на вложенную закладку *SNMP* и поставить отметку в поле **Включить SNMP,** если Вы хотите разрешить SNMP-мониторинг для данного Шлюза Безопасности. Затем установить настройки SNMP. Это делается следующим образом (полный список сообщений SNMP можно найти в п. 7.1.2.7):

1) По умолчанию, порт SNMP-Клиент установлен на **161**, а значение **Группы SNMP** установлено на **public**. При необходимости эти значения можно изменить в соответствующих полях.

Для аутентификации сообщений SNMP использует *имена сообщества*. Имя сообщества можно считать кодом, совместно используемым SNMP-серверами и SNMP-*Агентами*. Все сообщения SNMP должны содержать имя сообщества. Если сообщение содержит имя сообщества, не установленное на хосте, оно будет блокировано.

2) Выбрать один или несколько SNMP-серверов, на которые данный *Агент* Microsoft IPsec будет отправлять сообщения SNMP в **SNMP-Серверы**.

Появятся только те SNMP-серверы, которые были заранее зарегистрированы в окне *Серверы* (подробнее см. п. 7.1.1.2).

Шаг 7: Принадлежность к группе

На закладке *Входит в* показано, к каким Группам принадлежит данный Шлюз Безопасности. Можно добавить Шлюз в существующую Группу или удалить его из нее. На закладке содержатся два списка: в первом - *Доступные группы* - показан полный перечень Групп, зарегистрированных в папке *Группы* в секции *Объекты политики;* (за исключением тех Групп, в которых в данный момент состоит Шлюз Безопасности); во втором списке - *Выбранные группы* - перечислены Группы, в которых в данный момент состоит Шлюз Безопасности.

Для того чтобы изменить состав Группы надо переместить Шлюз Безопасности из одного списка в другой, используя кнопки со стрелками.

Шаг 8: Завершение создания Шлюза

Нажать кнопку **OK.** Новый **Шлюз Безопасности** будет добавлен в *Топология ВЧС* и папку *Сетевые Объекты* секции *Объекты политики*.

7.1.2.6. Типовые (Неуправляемые) Шлюзы Безопасности

Установить курсор на секцию *Топология ВЧС* или выбрать папку *Сетевые Объекты* в секции *Объекты политики*, используя команду **Добавить->Шлюз Безопасности**.

Шаг 1: Общие характеристики

На закладке *Общее* нужно сделать следующее:

1) В строке *Адрес Агента* набрать IP-адрес Шлюза, который будет представлять этот Объект. Именно на этот адрес *ЦУП* будет отправлять ЛПБ для данного Объекта.

2) Указать производителя и версию *Агента*, которого будет представлять этот Шлюз Безопасности в окне *Выбор Дескриптора Агента*. На закладке *Общее* ввести Имя Объекта Шлюза Безопасности.

3) В строке *Адрес Агента* набрать IP-адрес Шлюза, который будет представлять этот Объект. Именно на этот адрес *ЦУП* будет отправлять ЛПБ для данного Объекта. При необходимости в соответствующее поле можно ввести текстовое описание данного Объекта.

Шаг 2: Топология

На закладке *Топология* нужно сделать следующее:

1) Выбрать вложенную закладку *Топология*, чтобы ввести информацию об интерфейсах Шлюза Безопасности.

2) Нажать кнопку **Добавить** и ввести логическое имя и IP-адрес первого интерфейса Шлюза Безопасности. Таким же образом ввести данные обо всех интерфейсах Шлюза Безопасности. Для одного интерфейса можно указывать несколько IP-адресов, просто создать дополнительные интерфейсы с тем же логическим адресом. Если IP-адрес данного интерфейса попадает в пределы какой-либо Зоны, эта Зона отобразится в колонке **Зона** таблицы *Интерфейсы*, иначе там появится значение **Auto** и **Зона** будет создана автоматически. При добавлении IP-интерфейса, находящегося в зоне Internet, необходимо выбрать нужный параметр **Зона Интернет** из списка **Привязка к зоне:**, эта зона отобразится в колонке **Зона** таблицы *Интерфейсы*.

3) Если данный Шлюз Безопасности будет использоваться только в качестве конечной точки для туннелей IPsec, надо убрать отметку в поле **Включить перенаправление незащищенного трафика** (она установлена по умолчанию).

При автоматической привязке интерфейс привязывается к оптимальной зоне. Если интерфейс целиком попадает в одну или несколько постоянных зон, то оптимальной считается наименьшая из них, иначе оптимальной считается временно созданная auto-зона. Если оптимальная зона меняется (например, из-за того, что удаляются, создаются или меняются определенные зоны), такой интерфейс автоматически перепривязывается к другой подходящей зоне.

При жесткой привязке интерфейс привязывается к произвольной, определенной пользователем зоне или Internet-зоне. При изменениях топологии перепривязка не происходит.

Шаг 3: Местоположение

Перейти на закладку *Местоположение*, чтобы настроить опции *Местоположение* следующим образом:

1) В поле **Координаты** необходимо указать географические координаты Шлюза Безопасности. Координаты можно ввести вручную или присвоить их Шлюзу Безопасности, выбрав кнопку **Указать координаты**.

2) Если известен адрес Шлюза Безопасности его можно найти с помощью поля **Найти**.

3) После определения местоположения необходимо нажать кнопку **Готово.**

Если координаты не указаны, то поле **Координаты** имеет значение «-».

Шаг 4: Виртуальная частная сеть

Перейти на закладку *ВЧС,* чтобы настроить опции ВЧС следующим образом:

1) Выбрать вложенную закладку *Общее*. Если Вы не хотите, чтобы Шлюз Безопасности использовал IKE или IPsec, надо убрать отметку в поле **Включить IKE/IPsec обработку** (она установлена по умолчанию). В п. 7.1.2.7 можно найти пример того, когда может потребоваться отмена данной функции. В поле **IKE порт** можно изменить порт, который Шлюз Безопасности будет использовать для IKE-трафика. В поле **IKE-NAT-T** можно изменить порт, используемый шлюзом для работы протокола IKE-NAT-Traversal.

2) Перейти на закладку *Сертификаты*, чтобы зарегистрировать сертификаты.

   – Нажать кнопку **Добавить** в поле **Идентификатор IKE сертификата** и ввести все необходимые данные сертификата Шлюза Безопасности. Эти данные должны в точности соответствовать данным фактического сертификата; этот сертификат должен быть зарегистрирован на фактическом продукте ВЧС, который представляет данный Объект Безопасности. Подробнее о способах добавления сертификатов см. п. 7.1.1.1.

3) Перейти на закладку *Предопределенные ключи*, чтобы зарегистрировать предварительно распределенные ключи. Для этого надо нажать кнопку **Добавить** поле **Идентификатор согласованного ключа для IKE** и ввести всю необходимую информацию о предварительно распределенном ключе. Этот предварительно распределенный ключ должен быть зарегистрирован на фактическом устройстве ВЧС, которое представляет данный Шлюз Безопасности. Для того чтобы ввести информацию о любых дополнительных предварительно распределенных ключах необходимо сделать следующее:

– Ввести имя для данного ключа.

- Поставить отметку в поле **Шестнадцатеричная строка**, если Вы хотите ввести значение ключа в шестнадцатеричном формате.
- Если *ЦУП* не управляет данным предварительно распределенным ключом надо поставить отметку в поле **Неуправляемый.**
- Ввести значение ключа. Если Вы поставили отметку в поле **Шестнадцатеричная строка** надо ввести шестнадцатеричную строку имени с четным количеством символов в поле **Значение ключа.** В противном случае надо ввести буквенно-цифровое значение ключа.
- Из выпадающего списка *Партнер* выбрать партнеров по связи, совместно с которыми данный Шлюз Безопасности будет использовать этот ключ.
- Из первого выпадающего списка *Тип ID ключа* выбрать способ идентификации локального ключа. Это позволит партнеру по связи удостовериться в том, что данный ключ является Правильным. По умолчанию, для идентификации предварительно распределенного ключа будет использоваться первичный IP-адрес устройства ВЧС. В этом случае не требуется указывать дополнительной информации. Локальный ключ также может быть идентифицирован с помощью другого IP-адреса, DNS, ID-ключа или шестнадцатеричного ID-ключа. В этом случае надо выбрать тип идентификации ключа из выпадающего списка и ввести значение выбранного идентификатора в поле **Значение ID ключа.**
- Из второго выпадающего списка *Тип ID ключа* выбрать способ идентификации ключа партнера по связи. Это позволит устройству ВЧС удостовериться в том, что данный ключ является Правильным. По умолчанию для идентификации предопределенного ключа будет использован первичный IP-адрес партнера по связи. В этом случае нет необходимости указывать дополнительную информацию. Ключ партнера по связи может также быть идентифицирован при помощи другого IP-адреса, DNS, ID-ключа или шестнадцатеричного ID-ключа. В таком случае надо выбрать из выпадающего списка способ идентификации ключа и ввести значение выбранного идентификатора в поле **Значение ID ключа.**

4) Протокол XAUTH используется для более полной аутентификации при установлении ВЧС связи с использованием протокола IKE. Таким образом, Шлюзы могут аутентифицировать удаленных пользователей, обратившись к внешнему серверу аутентификации для получения дополнительных мандатов. Если данный Шлюз Безопасности проводит аутентификацию удаленных пользователей/ Хостов

Безопасности через внешний сервер аутентификации можно отразить это в настройках *ЦУП*. Выбрать вложенную закладку *Расширенная аутентификация.*

5) Для добавления XAUTH-правил выполнить следующие действия:

- Выбрать в списке *Доступные объекты* Объекты Политики, аутентификация которых будет осуществляться через внешний сервер, и переместить их в список *Выбранные объекты*.
- В списке *Серверы аутентификации* выбрать один или несколько серверов аутентификации, которые будут проверяться Шлюзом Безопасности на наличие дополнительных мандатов (Подходящие Объекты серверов TACACS+ и/или RADIUS должны быть заранее созданы в окне *Серверы*). Подробнее см. п. 7.1.1.2.
- По умолчанию, *ЦУП* автоматически выберет тот интерфейс Шлюза Безопасности, который будет использоваться для XAUTH, используя алгоритм трассировки топологии. Если Вы хотите вручную выбрать интерфейс Шлюза Безопасности, который будет использоваться для XAUTH, надо убрать отметку в поле **Выбрать интерфейс для XAUTH** и выбрать необходимый интерфейс из выпадающего списка.

6) Протокол IKE CFG используется для того, чтобы загружать IP-адрес и другие данные сетевой конфигурации на удаленный клиент ВЧС, как часть процесса предварительного согласования в IKE. В первую очередь это используется для того, чтобы избежать маршрутизации ответных пакетов с локального сервера удаленному клиенту ВЧС. Также это позволяет выделять трафик, исходящий от идентифицированных удаленных пользователей и затем применить к нему фильтрацию МЭ, используя локальный пул IP-адресов, вместо общих адресов глобальной сети. Если данный Шлюз Безопасности конфигурирует Хосты Безопасности / Пользователей через IKE CFG, назначая им IP-адреса из пула IP-адресов, расположенного за Шлюзом, можно создать любое количество Правил IKE CFG в *ЦУП*. Выбрать вложенную закладку *IKE CFG*. Создать правила IKE CFG следующим образом:

   - Перейти на закладку **IKECFG**;
   - Нажать кнопку **Добавить** и создать Правила IKE CFG:
   - Выбрать Объекты Политики, к которым будет применяться протокол IKE CFG из списка *Доступные объекты* и переместить их в список *Выбранные объекты*.

– Указать **Ресурс IP-адресов**, находящийся за Шлюзом Безопасности, из которого будут браться адреса для удаленных Хостов Безопасности / Пользователей. Из выпадающего списка выбрать метод, которым будет вводиться **Ресурс IP-адресов** (IP Диапазон, IP Адрес + Маска или DHCP). При выборе метода получения ресурса через DHCP в качестве идентификатора клиента будет направлен адрес, выбранный DHCP-сервером, который первым ответит на запрос (DHCP REQUEST), отправленный со шлюза. При обмене информацией с DHCP-сервера, с которым работает шлюз, запрашиваются следующие параметры: IP-адрес, subnet mask и broadcast addr, DNS.
– В предлагаемое поле ввести подходящие значения для области IP-адресов.
– Указать **Broadcast-маску** и адрес **DNS-сервера** в поле **Дополнительные параметры**.

Шаг 5: Настройка SNMP

Перейти на закладку *SNMP* и поставить отметку в поле **Включить SNMP**, если Вы хотите разрешить использование SNMP-мониторинга для данного Шлюза Безопасности. Установить параметры SNMP (полный список SNMP-сообщений можно найти в п. 7.1.2.7):

1) По умолчанию, порт клиента SNMP установлен на **161**, а значение среды SNMP – на **public**. При необходимости эти значения можно изменить в соответствующих полях.

Для аутентификации сообщений SNMP использует *имена сообщества (community names)*. Имя сообщества можно считать кодом, совместно используемым SNMP-серверами и SNMP-*Агентами*. Все SNMP-сообщения должны содержать имя сообщества. Если сообщение содержит имя сообщества, которое не установлено на хосте, оно будет блокировано.

2) Выбрать один или несколько SNMP-серверов в *SNMP Серверы*, на которые Шлюз будет отправлять SNMP-сообщения, для этого переместить их из списка *Доступные* в список *Выбранные*.

В списке появятся только те SNMP-Серверы, которые были заранее зарегистрированы в окне *Серверы* (подробнее см. в п. 7.1.1.2).

Шаг 6: Настройка журнала регистрации Syslog

Системный журнал позволяет *Агентам* посылать регистрационные данные на удаленный сервер в стандартизованном формате. Для того чтобы установить отправку данных журнала регистрации с данного Шлюза, надо добавить Syslog-сервер, нажав кнопку **Добавить** в

вкладке Syslog и в списке выбрать один или несколько Syslog-серверов из выпадающего списка, на которые данный Шлюз будет отправлять сообщения Syslog.

Внимание! В списке появятся только те Syslog-серверы, которые были заранее зарегистрированы в окне *Серверы*. Единственным исключением является Syslog-сервер (представленный сервисом **TPNSyslog**), который автоматически создается на хосте *ЦУП* при установке *ЦУП*, и, таким образом, всегда находится в списке.

Если Вы импортировали Проект из ранней версии *ЦУП*, Syslog-сервер не будет автоматически создан на хосте *ЦУП*. В этом случае Вам придется вручную создать Syslog-сервер на хосте *ЦУП* (подробнее см. подраздел 7.9).

Шаг 7: Принадлежность к группе

На закладке *Входит в* показано, к каким Группам принадлежит данный Шлюз Безопасности. Можно добавить Шлюз в существующую Группу или **удалить** его из нее. На закладке содержатся два списка: в первом списке *Доступные группы* показан полный перечень Групп, зарегистрированных в папке *Группы* в секции *Объекты политики* (за исключением тех Групп, в которых в данный момент состоит Шлюз Безопасности); во втором *Выбранные группы* перечислены Группы, в которых в данный момент состоит Шлюз Безопасности.

Для того чтобы изменить состав Группы надо переместить Шлюз Безопасности из одной Группы в другую, используя кнопки со стрелками.

Шаг 8: Правила NAT

Если для данного объекта необходимо учесть/сконфигурировать трансляцию сетевых адресов (NAT, Network Address Translation) надо обратиться к п. 7.1.1.3.

Шаг 9: Завершение создание Шлюза

Нажать кнопку **OK.** Новый **Шлюз Безопасности** будет добавлен в графическое отображение *Графа топологии* и папку *Сетевые Объекты* секции *Объекты политики*.

7.1.2.7. Редактирование параметров Шлюза Безопасности

Для того чтобы отредактировать Объект Шлюза Безопасности надо выбрать его в секции *Топология ВЧС* или *Объекты политики*, используя команду **Изменить**. Появившееся окно *Свойства* идентично окну *Добавить объект Шлюз безопасности*.

7.1.2.7.1. Автопропуск трафика (закладки Управление и ВЧС)

Автоматический пропуск - указывают, можно ли определенные типы трафика пропускать автоматически. Когда autopasses назначен для данного типа трафика, то трафик

пропускается без проверки. Автоматический пропуск трафика может быть выбран для следующих типов трафика:

LDAP
SNMP
ICMP
ISAKMP
AH
ESP
Broadcast (IP-адреса 255.255.255.255)
Multicast (IP-адреса 224.0.0.0.239.255.255.255)

Автопропуск трафика для ISAKMP, AH, ESP и LDAP устанавливается во вложенной закладке *Общее* на закладке *ВЧС*.

Автопропуск трафика для Broadcast, multicast и ICMP устанавливается на закладке *Управление*. По умолчанию автопропуск трафика устанавливается для ICMP.

Autopasses обладает некоторыми свойствами, которые не очевидны. Например, когда определен автоматический пропуск для ICMP, то только 3, 4, 11 и 12 типы будут пропускаться. Если Вы не уверены как работают данные функции, необходимо выполнить следующие действия:
- Убедиться в том, что в соответствующем поле для **протокола** установлена отметка автоматического пропуска;
- Оттранслировать ГПБ;
- Проверить, что ГПБ понятна для Шлюза Безопасности и в неё внесены изменения.

7.1.2.7.2. Сообщения SNMP

Сообщения SNMP используются *Агентами* для передачи информации SNMP-серверу о произошедших важных событиях с *Агентом* в защищаемой среде. Можно выбирать, какие сообщения данный *Агент* будет посылать серверу, указав их в закладке *SNMP* в окне *Свойства.* Для изменения статуса SNMP-сообщения надо выделить его в списке и использовать кнопки со стрелками <вправо> и <влево> для его перемещения в списке. Ниже приведён список сообщений (см. Таблица 25) (Отметим, что не все *Агенты* их используют).

Таблица 25 - Сообщения SNMP для передачи информации SNMP-серверу

Сообщения	Значение
IKE_NEG_FAILURE	Неудачная попытка создания ISAKMP защищенного соединения. Два участника переговоров в IKE-сессии не договорились, какой протокол использовать для переговоров
IKE_INVALID_COOKIE	Получены ошибочные *идентификаторы сессии (cookie)* и использование их для проверки, что другие участники IKE доступны и аутентифицированы невозможно
IPSEC_NEG_FAILURE	Неудачная попытка создания IPsec защищенного соединения. Параметры AH/ESP не согласованы
IPSEC_AUTH_FAILURE	Получен не аутентифицированный IPsec или SKIP-пакет

Сообщения	Значение
IPSEC_REPLAY_FAILURE	Получен пакет с ошибочным последовательным номером. Наиболее вероятно, что некоторые пакеты были повторно получены
IPSEC_POLICY_FAILURE	Получен пакет с нарушением Политики. Партнер не найден в БД
IPSEC_INVALID_SPI	Получен пакет с неизвестным SPI
LOCAL_PARAMS_CHANGING	Изменены локальные параметры
LSP_SETTING	Установлена ЛПБ
LSP_LOADED	Успешно загружена ЛПБ
USER_LOGIN_OK	Пользователь успешно вошёл в систему
USER_LOGIN_ERROR	Ошибка при входе пользователя
USER_LOGOFF	Пользователь успешно вышел из системы
IPSEC_SA_CREATED	Успешно создано новое IPsec-соединение
IPSEC_SA_DELETED	IPsec-соединение удалено
ADMIN_LOGIN_OK	Администратор успешно вошёл в систему
ADMIN_LOGIN_ERROR	Ошибка при входе администратора
ADMIN_LOGOFF	Администратор успешно вышел из системы
VPNSVC_LOADED	Успешно загружены системные сервисы
VPNSVC_INLOADED	Системные сервисы не загружены

Только *Агенты* используют сообщения от *ЦУП*.

7.1.2.7.3. Отмена использования IKE/IPsec

На вложенной закладке *Общее вкладки ВЧС* есть поле **Включить IKE/IPsec обработку** (по умолчанию в нем стоит отметка). Данный параметр показывает, может ли *Агент* обрабатывать IPsec-трафик. Таким образом, если *Агент* не может использовать эту функцию, или если Вы хотите использовать *Агент* для другой цели, надо убрать отметку в этом поле. Первый вариант довольно прост, что касается второго, его можно описать следующим образом: Допустим, у Вас есть Подсеть, защищенная с помощью двух Шлюзов Безопасности Cisco PIX Firewall (**PIX1** и **PIX2)**, при этом оба они могут обрабатывать IPsec-трафик. Однако Вам необходимо сделать так, чтобы весь IPsec-трафик обрабатывался только **PIX1**. В таком случае надо убрать отметку в поле **Включить IKE/IPsec обработку** для Объекта Политики **PIX2**. Во время трансляции ГПБ, алгоритм трассировки *ЦУП* поймет, что все IPsec Правила, которые распространяются на Подсеть, должны проходить только через **PIX1**, в то время как все остальные (не относящиеся к IPsec) Правила, распространяющиеся на Подсеть, могут проходить через оба Шлюза. (ЛПБ **PIX1** содержит, как Правила МЭ, так и IPsec-Правила, в то время как ЛПБ **PIX2** содержит только Правила МЭ).

7.1.2.7.4. Настройка ЛПБ (закладка *Управление*)

Конфигурирование настроек ЛПБ производится на вложенной закладке *ЛПБ* на закладке *Управление* для применяемых *Агентов*.

7.1.2.7.5. Блок Локальная Политика Безопасности

Блок *Локальная Политика Безопасности* содержит автоматически созданный список всех ЛПБ, приготовленных для данного Шлюза Безопасности, в нем указан текущий **Статус** ЛПБ, когда **Создана** ЛПБ, когда **Активирована** и любые пояснения, связанные с ЛПБ. Выбрать ЛПБ и нажать кнопку **Править** для выбора, просмотра или редактирования. Откроется окно текстового редактора, которое предоставляет ЛПБ для непосредственного редактирования.

Если для данного Объекта Политики стоит отметка в поле **Не транслировать ЛПБ**, то при трансляции ГПБ на данный *Агент* не будет создаваться ЛПБ (эта функция полезна в том случае, если Вам необходимо редактировать основную часть ЛПБ).

7.1.2.7.6. Блок Структура ЛПБ

Фрагменты ЛПБ в текстовом формате могут быть добавлены в начало и/или конец ЛПБ *Агента*, оттранслированной из ГПБ. Эти фрагменты, известные как определяемые пользователем ЛПБ (Custom LSP), могут быть созданы вручную или импортированы из файла. (О том, как создавать Определяемые пользователем ЛПБ, см. п. 4.7.9).

Блок *Структура ЛПБ* содержит атрибут *Автоматически Созданная ЛПБ*. Этот атрибут действует, как место для размещения (**placeholder**) - он указывает на местонахождение ЛПБ, оттранслированной из ГПБ в общей ЛПБ. То есть, если определяемая пользователем ЛПБ (фрагмент ЛПБ) помещен *над* атрибутом *Автоматически Созданная ЛПБ*, данный фрагмент ЛПБ будет помещен *перед* ЛПБ, образованной от ГПБ в общей ЛПБ Шлюза Безопасности. Аналогично фрагмент определяемой пользователем ЛПБ, находящийся в иерархии ниже атрибута *Автоматически Созданная ЛПБ,* будет помещен *после* ЛПБ, образованной из ГПБ.

Для того чтобы добавить или удалить определяемую пользователем ЛПБ из ЛПБ Шлюза Безопасности надо нажать кнопку **Править.** Список *Список пользовательских ЛПБ* (всех зарегистрированных на данный момент определяемых пользователем ЛПБ) отобразится в верхнем левом углу окна *Редактировать структуру ЛПБ*, а *Структура ЛПБ* - в верхнем правом углу. Переместить определяемые пользователем ЛПБ между списками *Список пользовательских ЛПБ* и *Структура ЛПБ*, используя кнопки со стрелками <вправо> и <влево>.

Чтобы изменить порядок, в котором пользовательские ЛПБ будут исполняться в ЛПБ Шлюза Безопасности, надо выбрать ЛПБ в *Списке пользовательских ЛПБ* и переместить с помощью кнопок со стрелками «вверх» и «вниз».

7.1.3. Объекты Хостов Безопасности

Хосты Безопасности являются *Агентами*, которые могут устанавливать защищённые соединения с сетевыми узлами в среде Безопасности с фиксированного IP-адреса. Хосты Безопасности могут быть управляемыми, в этом случае их ЛПБ создается *ЦУП*, или неуправляемыми. Примерами Хостов Безопасности могут служить *ЗАСТАВА-Клиент* и *Агенты* Microsoft IPsec.

7.1.3.1. Создание Объектов Хостов Безопасности

Чтобы создать Хост Безопасности надо использовать команду **Добавить−>Хост Безопасности**, далее следовать инструкциям по созданию Объекта Шлюза Безопасности. Дескрипторы *Агента* включают описания *ЗАСТАВА-Клиент, Агентов* IPsec ОС Microsoft Windows XP/2003, типового клиента.

7.1.3.2. *ЗАСТАВА-Клиент*

Для того чтобы создать *управляемый* Объект Хоста Безопасности, который будет представлять *ЗАСТАВА-Клиент,* надо следовать инструкции по созданию Объекта Шлюза Безопасности, представляющего *ЗАСТАВА-Офис* (подробнее см. п. 7.1.2.1). Пропустить шаги, описанные для вложенной закладки *IKE CFG*, находящейся на закладке *ВЧС* и закладки *Правила NAT*, т.к. их нет для Хостов Безопасности.

Другим важным различием является наличие вложенной закладки *Расширенная аутентификация* на закладке *ВЧС* в меню Объекта Хоста Безопасности, представляющего *ЗАСТАВА-Клиент.* Протокол XAUTH используется для более полной аутентификации пользователя при установлении соединения ВЧС с использованием протокола IKE. Таким образом, Шлюзы могут аутентифицировать удаленных пользователей, обращаясь к внешним серверам аутентификации для получения дополнительных мандатов. Если мандаты данного Хоста Безопасности будут храниться на внешнем сервере аутентификации, надо показать это в настройках *ЦУП.*

Для аутентификации пользователя *Агента*, который представляет данный Хост Безопасности, внешний сервер аутентификации RADIUS или TACACS+ будет запрашивать у пользователя имя и пароль. Перейти на вложенную закладку *Расширенная аутентификация* и ввести имя пользователя и пароль, по которым данный сервер аутентификации будет опознавать данный Хост Безопасности.

7.1.3.3. *Агенты* Microsoft IPsec

Чтобы создать управляемый или неуправляемый Объект Хоста Безопасности, который будет представлять *Агента* Microsoft IPsec, надо следовать инструкциям по созданию Объектов Шлюзов Безопасности, представляющих *Агентов* Microsoft IPsec (см. п. 7.1.2.1). Пропустить шаги, описанные в закладке *Правила NAT*, т.к. ее нет в меню *Хост Безопасности*.

7.1.3.4. Неуправляемый Хост Безопасности

Чтобы создать неуправляемый Объект Хоста Безопасности надо следовать инструкциям по созданию типового неуправляемого Объекта Шлюза Безопасности (см. п. 7.1.2.1). Пропустить разделы, касающиеся вложенной закладки *IKE CFG*, находящейся на закладке *ВЧС* и закладки *Правила NAT*, т.к. их нет в меню *Хостов Безопасности*.

7.1.3.5. Редактирование параметров Хостов Безопасности

Чтобы отредактировать Объект Хоста Безопасности надо выбрать его в секции *Топология ВЧС* или *Объекты политики* и выбрать параметр **Изменить**. Открывшееся окно *Изменить объект Хост Безопасности* идентично окну *Добавить объект Хост Безопасности*. Атрибуты и параметры Объектов Хостов Безопасности те же, что и у Шлюзов Безопасности, представляющих *Агентов* той же версии. За исключением того, что в меню *Хостов Безопасности* представляющих *ЗАСТАВА-Клиент* нет вкладок *Правила NAT* и *IKE CFG* и закладка *Расширенная аутентификация* представляет закладку с настройками *XAUTH Client*, а для *Хостов Безопасности*, представляющих *ЗАСТАВА-Офис*, закладка *Расширенная аутентификация* представляет закладку с настройками *XAUTH Server*. Полное описание см. в п. 7.1.3.2.

7.1.4. Объекты IP-хост

IP-хост – это Объекты, у которых есть фиксированный IP-адрес, но нет собственной криптографической системы, и которые не управляются *ЦУП*. Объекты IP-хостов обычно представляют незащищенные компьютеры и те компьютеры, которые защищены Объектом Шлюза Безопасности (во втором случае IP-адрес IP-хоста должен находиться в зоне, защищенной данным Шлюзом Безопасности, а этот Шлюз должен быть установлен как **Защитный Шлюз** для данного IP-хоста).

7.1.4.1. Создание Объектов IP-хост

Использовать команду **Добавить->IP хост**. Откроется окно *Добавить _IP Хост* на закладке *Общее*.

На закладке *Общее* сделать следующее:

1) Ввести уникальное имя для данного Объекта IP-хоста.

2) При необходимости можно ввести текстовое описание Объекта.

3) Выбрать домен, в который будет входить данный IP-Хост.

4) Перейти на закладку *Местоположение*. в поле **Координаты** необходимо указать географические координаты IP-Хоста. Координаты можно ввести вручную или присвоить их IP-Хосту, перемещая маркер по карте и нажав кнопку **Указать координаты**. Если известен адрес IP-Хоста его можно найти с помощью поля **Найти**. После определения местоположения необходимо нажать кнопку **Готово**.

5) Перейти на закладку *Топология*. Нажать кнопку **Добавить** и ввести **Логическое имя** и **IP-адрес** первого интерфейса IP-хоста. Таким же образом надо ввести данные всех интерфейсов данного IP-хоста. Для одного интерфейса можно указывать несколько IP-адресов, для этого нужно создать дополнительные интерфейсы с тем же логическим именем. Если IP-адрес данного интерфейса попадает в пределы какой-либо Зоны, эта Зона отобразится в колонке *Зона* таблицы *Интерфейсы*, иначе там появится значение **Auto** и **Зона** будет создана автоматически. При добавлении IP-интерфейса, находящегося в зоне Internet, необходимо выбрать нужный параметр **Зона Интернет** из списка *Привязка к зоне:*, эта зона отобразится в колонке *Зона* таблицы *Интерфейсы*.

6) Перейти на закладку *Входит в*. Здесь можно добавить IP-хост к уже существующей Группе. Для этого выбрать имя Группы в списке *Доступные группы* и нажать на кнопку со стрелкой <направо>, чтобы переместить IP-хост в *Выбранную группу*. Чтобы убрать IP-хост из Группы надо выбрать название Группы в списке *Выбранные группы* и нажать кнопку со стрелкой <влево>, чтобы переместить ее в *Доступные группы*.

7) Нажать кнопку **OK** и IP-хост будет добавлен в графическое представление *Графа топологии* и в папку *Сетевые Объекты* в секции *Объекты политики*.

7.1.4.2. Редактирование параметров IP-хост

Чтобы отредактировать Объект IP-хост необходимо два раза нажать на него левой кнопкой мыши или один раз клавишей <Enter>, предварительно выбрав его изображение в секции *Топология*. Открывшееся окно *Изменить IP Хост* идентично окну *Добавить IP Хост*.

7.1.5. Объекты IP Диапазон

IP Диапазон – это тип Группы, который представляет один или несколько диапазонов IP-адресов. Объект IP Диапазон может принимать участие в Политике Безопасности так, что одинаковые Правила будут применяться ко всем членам Среды Безопасности, чьи IP-адреса находятся в данном диапазоне адресов (IP Диапазон). Диапазоны адресов IP могут использоваться для того, чтобы устанавливать одинаковые Правила по обработке трафика для большого числа Объектов Политики, чьи IP-адреса заданы непрерывными или дискретными значениями.

Для ввода данных об IP-адресах можно использовать три различных формата: **first address:last address** (первый адрес: последний адрес), **subnet:mask** (Подсеть: маска), или единственный IP-адрес (в отличие от Объектов подсети, которые представляют только один диапазон IP-адресов, вводимый в формате subnet:mask).

7.1.5.1. Создание Объектов IP Диапазона

Использовать команду **Добавить->IP Диапазон**. Откроется окно *Добавить IP Диапазон*, на закладке *Общее*.

На закладке *Общее* сделать следующее:

1) Ввести уникальное имя для данного Объекта IP Диапазон.
2) Выбрать домен, в который будет входить данный IP Диапазон. Выбрать вкладку *Топология,* указать формат, в котором будут вводиться данные IP-адресов.
3) В открывшихся полях ввести данные IP-адресов для данного диапазона IP-адресов.
4) При необходимости в соответствующее поле можно ввести текстовое описание данного Объекта.
5) Перейти на закладку *Местоположение* в поле **Координаты** указать географические координаты Объекта IP Диапазон. Координаты можно ввести вручную или присвоить их Объекту IP Диапазон, перемещая маркер по карте и нажав кнопку **Указать координаты**. Если известен фактический адрес Объекта IP Диапазон его можно найти с помощью поля **Найти.**
6) После определения местоположения необходимо нажать кнопку **Готово.**
7) Перейти на закладку *Входит в*. Здесь можно добавить данный диапазон IP-адресов к уже существующей Группе. Для этого необходимо выбрать название Группы в списке *Доступные группы* и нажать на кнопку со стрелкой <вправо>, чтобы

переместить ее в список *Выбранные группы*. Чтобы удалить диапазон IP-адресов из Группы надо выбрать название Группы в списке *Выбранные группы* и нажать кнопку со стрелкой <влево>, чтобы переместить ее в *Доступные группы*.

8) Нажать кнопку **OK** и новый Объект IP Диапазон добавится к графическому представлению *Графа топологии* и в папке *Сетевые Объекты* секции *Объекты политики*.

7.1.5.2. Редактирование параметров Объекта IP Диапазон

Для редактирования Объекта IP-Диапазон необходимо два раза нажать на него левой кнопкой мыши или клавишей <Enter>, предварительно выбрав его изображение в секции *Топология*. Открывшееся окно *Изменить IP Диапазон* идентично окну *Добавить IP Диапазон*.

7.1.6. Объект Подсеть

Подсеть является одним из видов группы, представленной в виде диапазона IP-адресов, определяемого установленным базовым IP-адресом и маской подсети. Подсеть может принимать участие в *Политике Безопасности* так, что одни и те же Правила будут в одинаковом порядке применяться ко всем членам *Среды Безопасности*, чьи IP-адреса попадают в диапазон данной подсети. Подсеть может использоваться для того, чтобы применять одинаковые Правила по обработке трафика к большому количеству Объектов Политики, IP-адреса которых задаются последовательно, и этот набор IP-адресов представляет собой диапазон IP-адресов, ограниченный введенной последовательностью.

7.1.6.1. Создание Объектов подсети

Использовать команду **Добавить->Подсеть.** Откроется окно *Добавить Подсеть* с закладкой *Общее*.

На закладке *Общее* сделать следующее:

1) Ввести уникальное **Имя** для данного Объекта подсети.

2) Выбрать домен, в который будет входить данный IP Диапазон.

3) Выбрать вкладку *Топология,* ввести базовый **IP-адрес** для данной подсети.

4) Ввести **Маску** подсети.

5) При необходимости в соответствующее поле можно ввести текстовое **Описание** данного Объекта.

6) Перейти на закладку *Местоположение* в поле **Координаты** указать географические координаты **Подсети**. Координаты можно ввести вручную или присвоить их

Подсети, перемещая маркер по карте и нажав кнопку **Указать координаты**. Если известен адрес **Подсети** его можно найти с помощью поля **Найти.** Если координаты не указаны, то поле **Координаты** имеет значение «-».

7) После определения местоположения необходимо нажать кнопку **Готово.**

8) Перейти на закладку *Входит в*. Здесь можно добавить данную *Подсеть* к уже существующей Группе. Для этого необходимо выбрать название Группы в списке *Доступные группы* и нажать на кнопку со стрелкой <вправо>, чтобы переместить ее в список *Выбранные группы*. Чтобы удалить *Подсеть* из Группы надо выбрать название Группы в списке *Выбранные группы* и нажать на кнопку со стрелкой <влево>, чтобы переместить ее в *Доступные группы*.

9) Нажать кнопку **OK** и новый Объект подсети появится в графическом представлении *Графа топологии* и в папке *Сетевые Объекты* секции *Объекты политики*.

7.1.6.2. Редактирование параметров подсети

Чтобы отредактировать Объект Подсеть необходимо два раза нажать на него левой кнопкой мыши или один раз клавишей <Enter>, предварительно выбрав его изображение в секции *Топология*. Открывшееся окно *Свойства* идентично окну *Добавить Подсеть*.

7.1.7. Объекты Пользователь

Пользователь (User) – это *Агент* без фиксированного IP-адреса, однако имеющий свою собственную криптографическую систему, которая может создавать защищенное соединение с узлом сети в Среде Безопасности, находясь при этом вне данной среды. Обычно, это портативные компьютеры или компьютеры в сети, чей DHCP-сервер не назначает постоянных IP-адресов. Примерами Пользователей могут служить *ЗАСТАВА-Клиент, Агент* Microsoft IPsec или типовой клиент на мобильном компьютере.

7.1.7.1. Создание Объектов Пользователь

Опции (закладки), которые будут доступны в окне *Добавить Пользователя,* зависят от того, какой тип *Агента* Вы выберете. О создании Объектов, представляющих каждый из типов *Агентов*, излагается в п. 7.1.2.1. Материал, изложенный в данном пункте, предполагает, что Вы уже знакомы с понятиями вышеуказанного раздела, поэтому ниже внимание будет сосредоточено на опциях, которые доступны только для определенных типов *Агентов.*

Выбрать в секции *Объекты политики* папку *Пользователи*, использовать команду **Добавить Пользователя**. Откроется окно *Выбор Дескриптора Агента*.

Шаг 1: Общие характеристики

1) В окне *Выбор Дескриптора Агента* выбрать номер версии ПО клиента, который использует этот Пользователь, и нажать кнопку **Готово.**

2) Ввести уникальное Имя для данного Объекта Пользователя.

3) Выбрать домен, в который будет входить данный объект Пользователь.

4) Вы вернетесь в окно *Добавить Пользователя*. Теперь в этом окне доступны пять закладок. Эти закладки будут разными, в зависимости от выбранного ПО клиента.

5) Чтобы создать Неуправляемого Пользователя надо убрать отметку в поле **Управляемый.**

Типовые клиенты (Generic Clients) не могут быть управляемыми Пользователями.

6) При желании можно ввести текстовое **Описание** Объекта.

Шаг 2: Местоположение

Перейти на закладку *Местоположение,* чтобы настроить опции *Местоположение* следующим образом:

1) В поле **Координаты** необходимо указать географические координаты Шлюза Безопасности. Координаты можно ввести вручную или присвоить их Шлюзу Безопасности, выбрав кнопку **Указать координаты.**

2) Если известен адрес Шлюза Безопасности его можно найти с помощью поля **Найти.**

3) После определения местоположения необходимо нажать кнопку **Готово.**

Если координаты не указаны, то поле **Координаты** имеет значение «-».

Шаг 3: Виртуальная частная сеть

Перейти на закладку *ВЧС,* чтобы настроить опции ВЧС.

1) Выбрать вложенную закладку *Общее*:

   – В поле **IKE Port** можно изменить порт, который будет использоваться Пользователем для IKE-трафика.
   – Только для *ЗАСТАВА-Клиент:* Выбрать типы трафика, которые будут автоматически пропускаться Пользователем, без предварительной проверки Правил ЛПБ, для этого поставить отметки в соответствующих полях.

2) Перейти на вложенную закладку *Сертификаты*:

   – Чтобы зарегистрировать сертификат надо нажать кнопку **Добавить** в окне *Добавить IKE сертификат* и ввести все необходимые данные о сертификате Пользователя. Эти данные должны в точности соответствовать данным фактического сертификата; этот сертификат должен быть зарегистрирован на фактическом клиенте, которого представляет данный объект Пользователя. Подробнее о способах добавления сертификатов см. п. 7.1.1.1.
   – Только для *ЗАСТАВА-Клиент:* Если *ЗАСТАВА-Клиент*, представляемый данным Объектом Пользователя, будет использовать СОС, чтобы устанавливать подлинность сертификатов возможных партнеров по связи, поставить отметку в поле **Обработка СОС.**
   – При необходимости - выбрать один или несколько LDAP-серверов, которые будут использоваться данным Пользователем для скачивания сертификатов и СОС. Для этого надо переместить их из списка *Доступные* в список *Выбранные*. Внимание: В списке *Доступные* появятся только те LDAP-серверы, которые были заранее зарегистрированы в окне *Серве*ры (подробнее см. п. 7.1.1.2 и подраздел 7.9).

3) Перейти на вложенную закладку *Предопределенные ключи:*

   – Чтобы зарегистрировать предварительно распределенный ключ надо нажать кнопку **Добавить** и ввести всю необходимую информацию о предварительно распределенном ключе. Этот ключ должен быть зарегистрирован на фактическом клиенте, которого представляет данный Объект Пользователя. Ввести имя для этого ключа **Имя ключа**. Это имя должно быть тем же, что и имя Объекта фактического предварительно распределенного ключа, который использует данный Пользователь.
   – Если Пользователь использует *ЗАСТАВА-Клиент* не надо ставить отметку в поле **Управляемый** (*Агенты* не поддерживают управление значением предварительно распределенных ключей).
   – Из выпадающего списка *Партнер* выбрать партнеров по связи, совместно с которыми текущие Объекты Политики будут использовать этот предварительно распределенный ключ.
   – Из первого выпадающего списка *Тип ID ключа* выбрать способ идентификации локального ключа. Это позволит партнеру по связи удостовериться в том, что данный ключ является Правильным. По умолчанию, для идентификации

предварительно распределенного ключа будет использоваться первичный IP-адрес устройства ВЧС. В этом случае не требуется указывать дополнительной информации. Локальный ключ также может быть идентифицирован с помощью другого IP-адреса, DNS, ID-ключа или шестнадцатеричного ID-ключа. В этом случае выбрать тип идентификации ключа из выпадающего списка и ввести значение выбранного идентификатора в поле **Значение ключа.**

- Из второго выпадающего списка *Тип ID ключа* выбрать способ идентификации ключа партнера по связи. Это позволит устройству ВЧС удостовериться в том, что данный ключ является Правильным. По умолчанию для идентификации предопределенного ключа будет использован первичный IP-адрес партнера по связи. В этом случае нет необходимости указывать дополнительную информацию. Ключ партнера по связи может также быть идентифицирован при помощи другого IP-адреса, DNS, ID-ключа или шестнадцатеричного ID-ключа. В таком случае выбрать из выпадающего списка способ идентификации ключа и ввести значение выбранного идентификатора в поле **Значение ключа**.

4) (Только для *ЗАСТАВА-Клиент* и типовых клиентов). Перейти на закладку *Расширенная аутентификация* и ввести имя и пароль, по которым сервер аутентификации будет распознавать этот хост. Протокол XAUTH используется для расширенной аутентификации Пользователей, при установлении соединения VPN с использованием протокола IKE. Таким образом, Шлюзы могут аутентифицировать удаленных Пользователей, запрашивая дополнительные мандаты на внешнем сервере аутентификации. Если мандаты данного Пользователя будут храниться на внешнем сервере аутентификации можно отразить это в настройках *ЦУП*. Когда Шлюзу потребуется аутентифицировать пользователя (оператора) *Агента*, представляемого данным Пользователем, внешний сервер аутентификации RADIUS или TACACS+ запросит ввод имени и пароля.

Шаг 4: Управление *Агентами* (Только для *ЗАСТАВА-Клиент* и *Агентов* Microsoft)

Перейти на закладку *Управление*. На этой закладке устанавливается Политика, которую будет использовать драйвер по умолчанию и уровни регистрации событий для *ЗАСТАВА-Клиент* и *Агентов* Microsoft IPsec, а также для управления их локальными Политиками Безопасности.

1) Перейти на закладку *Общее*:

- Установить Политику, которую будет использовать Пользователь по умолчанию. Эта Политика (**Пропустить всех** или **Запретить всех**) будет применяться к тем партнерам по связи, для которых ЛПБ Пользователя не предусматривает точных Правил.
- Если Вы хотите, чтобы Пользователь автоматически пропускал широковещательные сообщения, предназначенные, как для всех компьютеров сети, так и для определенной группы компьютеров, и/или ICMP-трафик, надо поставить отметки в соответствующих полях.
  - Если вы хотите настроить параметры протокола DHCP, надо поставить отметку в соответствующем поле Пропуск DHCP.

2) Перейти на вложенную закладку *ЛПБ*:

   - Блоки *Локальная Политика Безопасности* и *Структура ЛПБ* будут не пустыми и доступными только после трансляции ГПБ и создания ЛПБ для данного Пользователя. Если Вы не хотите, чтобы ЛПБ была создана для данного Пользователя в следующий раз при трансляции ГПБ (например, если Вы вручную внесли изменения в текущую ЛПБ и хотите сохранить настройки), надо поставить отметку в поле **Не транслировать ЛПБ**. До тех пор, пока не будет убрана эта отметка, трансляция ЛПБ для данного Пользователя производиться не будет.

3) Выбрать вложенную закладку *Параметры соединений* (Только для *Агентов* Microsoft):

   - Выбрать **Метод загрузки**, который будет использоваться *Агентом* Microsoft IPsec при обращении к *ЦУП* для получения ЛПБ.
   - Если Вы хотите сохранять данные о том, были ли внесены изменения в ЛПБ Пользователя с момента последней активации, надо поставить отметку в поле **Отслеживание целостности ЛПБ**.
   - Выбрать **Получить параметры объекта**.
   - Сразу же после трансляции ГПБ и активации ЛПБ напротив Объекта Пользователя появится иконка статуса целостности ЛПБ. Подробнее см. в п. 8.4.4 и п. 7.1.1.2.

Шаг 5: Настройка SNMP

Если Вы хотите установить SNMP-контроль для данного Пользователя надо перейти на закладку *SNMP* и поставить отметку в поле **Включить SNMP**. Затем изменить настройки SNMP следующим образом:

1) По умолчанию порт SNMP-клиента установлен на **3454** (*ЗАСТАВА-Клиент*) или на **161** (Microsoft и типовые клиенты), а значение SNMP-сообщества по умолчанию установлено на **public**. При необходимости, значение последнего можно изменить в соответствующем поле.

Для аутентификации сообщений SNMP использует имена сообщества. Имя сообщества можно считать паролем, совместно используемым SNMP-серверами и SNMP-*Агентами*. Все сообщения SNMP должны содержать имя сообщества. Если сообщение содержит имя сообщества, неустановленное на хосте, оно не будет принято.

2) Поставить отметку в поле **Включить правило**, если Вы хотите, чтобы Пользователь всегда пропускал SNMP-трафик без предварительной проверки Правил ЛПБ.

3) Выбрать один или несколько серверов SNMP, на которые данный клиент будет посылать SNMP-сообщения.

   Внимание: В списке появятся только те серверы, которые были предварительно зарегистрированы в окне *Серверы* (подробнее см. в подразделе 7.9).

4) Переместить из списка *Доступные* в список *Выбранные* те SNMP-сообщения, которые данный клиент будет посылать на SNMP-серверы (полный список SNMP-сообщений можно найти в п. 7.1.2.7).

Шаг 6: Принадлежность к Группе

На закладке *Входит в* показано, к каким Группам принадлежит данный Пользователь, можно добавить Пользователя в существующую Группу или удалить его из нее. На закладке содержатся два списка: в первом *Доступные группы* показан полный перечень Групп, зарегистрированных в папке *Группы* в секции *Объекты политики;* (за исключением тех Групп, в которых в данный момент состоит Пользователь); во втором списке *Выбранные группы* перечислены Группы, в которых в данный момент состоит Пользователь.

Для того чтобы изменить состав Группы надо переместить Пользователя из одного списка в другой, используя кнопки со стрелками.

Нажать кнопку **OK**, и новый Пользователь будет добавлен в папку *Пользователи* и секцию *Объекты политики*.

7.1.7.2. Редактирование параметров Пользователя

Чтобы отредактировать Объект Пользователя надо выбрать его в секции *Объекты политики*, используя *Свойства*. Открывшееся окно *Свойства* идентично окну *Добавить объект Пользователь.*

7.1.8. Объект Группы

Объект Группы – это просто Группа определенных Объектов Политики, к которой могут применяться одинаковые Правила. В Группу можно объединить несколько Объектов Политики различных типов, при этом она не требует никаких других характеристик. Перед тем, как создавать Правило, которое будет применяться ко всем членам Группы, надо убедиться в том, что это Правило можно применять к каждому члену Группы. Подробнее см. раздел 4.

Любой Объект Политики может входить сразу в несколько Групп.

7.1.8.1. Создание Объекта Группы

Создание Объекта Группы происходит следующим образом:

1) Выбрать в секции *Объекты политики* папку *Группы*, используя команду **Добавить**–> **Группу**. Откроется окно *Добавить Группу*.
2) Ввести уникальное имя для данного Объекта Группы.
3) Выбрать домен, в который будет входить данный Объект Группа.
4) При необходимости можно ввести текстовое описание Объекта.
5) При необходимости можно ввести местоположение Объекта Группа в закладке *Местоположение.*
6) Перейти на закладку *Члены групп*. Переместить Объекты Политики, которые будут входить в Группу из списка *Доступные объекты* в список *Члены групп*.
7) Перейти на закладку *Входит в*. На этой закладке показано, к каким еще Группам принадлежит данная Группа. Можно добавить данную Группу в другую существующую Группу. На этой закладке отображаются два списка: в первом *Доступные группы* находится полный перечень Групп, зарегистрированных в папке *Группы* в секции *Объекты политики;* во втором списке *Выбранные группы* перечислены все Группы, в которые в данный момент входит данная Группа. Чтобы изменить состав Групп надо переместить Группу из одного списка в другой, использую кнопки со стрелками.

8) Нажать кнопку **OK**, новая Группа будет добавлена в папку *Группы* в секции *Объекты политики*.

7.1.8.2. Редактирование параметров Группы

Чтобы отредактировать Объект Группы надо выбрать папку *Группы* в секции *Объекты политики* и выбрать в таблице Группу, которую Вы хотите отредактировать, и выбрать настройку *Свойства*. Открывшееся окно *Свойства* идентично окну *Добавить объект Группа*.

7.1.8.3. Создание вложенных Групп в иерархической структуре

Можно создавать иерархии Групп, где одна группа может полностью находиться внутри другой. Дочерняя Группа размещается под родительской Группой. Чтобы вложить одну Группу в другую необходимо выполнить следующее:

1) Создать Группу (*Group*) и поместить в нее нужные Объекты Политики.
2) Создать вторую Группу (*Group*2) и поместить в нее нужные Объекты Политики.
3) Чтобы вложить *Group2* в *Group* нужно:
   - Выбрать папку *Группы*.
   - Выбрать в таблице *Group*, используя *Свойства.*
   - Выбрать *Group2* в таблице **в Члены группы** окна *Свойства группы*. Переместить *Group_2* из списка *Доступные объекты* в список *Члены группы* и нажать кнопку **OK**.

Теперь *Group_2* дважды представлена в дереве *Группы*: «фактический» Объект *Group_2* на первом уровне иерархии и ссылка на Объект *Group_2*, который входит в состав *Group_1* (см. Рисунок 63).

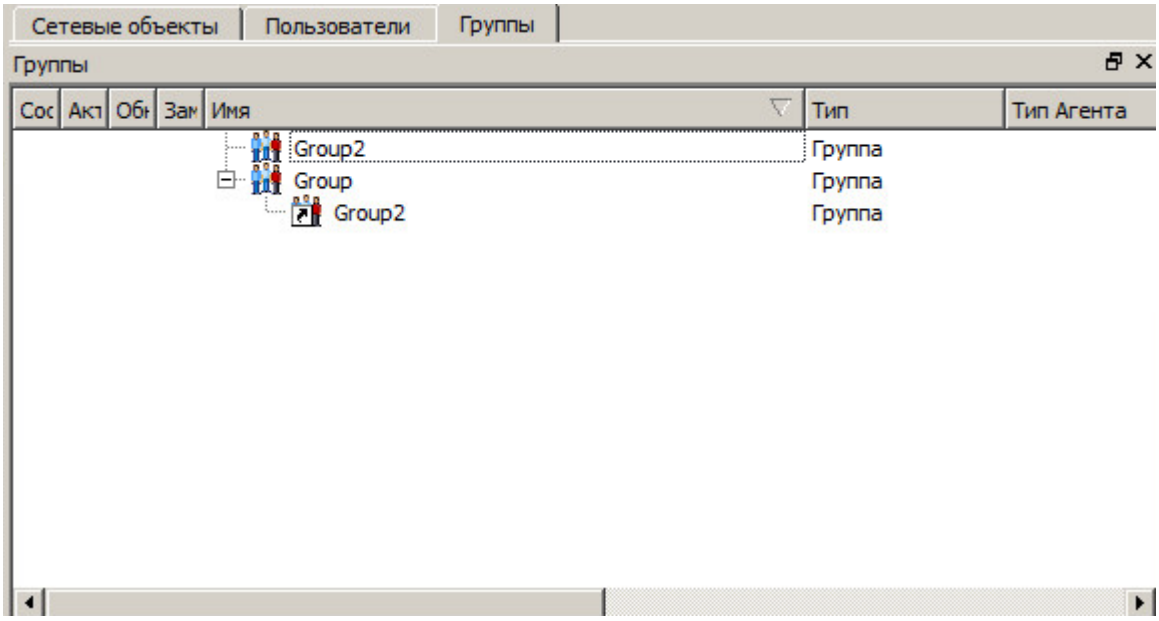

Рисунок 63 – Вложенные группы

7.1.9. Объект Политики Internet Zone

В *Графе топологии* присутствует Объект Политики **Internet Zone**. Он определяет все пространство, находящееся вне Зон, установленных в ГПБ. Если интерфейс Объекта Политики не попал ни в одну из Зон, установленных в данный момент в ГПБ, он будет связан с **Internet Zone**. Этот Объект всегда появляется в *Графе топологии* и его нельзя удалить.

7.1.10. Объекты Политики Any и Internet

Объекты **Internet** всегда появляются в *Графе ГПБ* и они не могут быть удалены. Объекты **Any** и **Internet** могут быть использованы в качестве источников или цели Правила ГПБ. Однако если эти объекты используются в качестве источника или Цели, ни один другой Объект Политики не может быть использован для данного источника или Цели.

Когда в качестве источника или Цели Правила ГПБ используется Объект **Any**, он представляет любой возможный хост, вне зависимости от того, входит ли он в ГПБ или нет. Таким образом, Правило ГПБ, установленное, например, для хоста Безопасности и Объекта **Any** будет определять порядок взаимодействия между Объектом хоста Безопасности и всеми возможными партнерами.

В том случае, когда в качестве источника или Цели Правила ГПБ используется Объект **Internet**, он представляет каждый из возможных партнеров по связи, находящихся в Зоне Internet Zone (вне зависимости от того, определены они в ГПБ или нет).

Объекты **Any** и **Internet** не могут входить в Группы**.**


Правила, содержащие Объект **Any** всегда транслируются после всех остальных Правил.

7.2. Зоны

Зона используется для определения группы связанных сетевых устройств, которые защищены одним и тем же Шлюзом Безопасности. Точнее, зона – это пространство IP-адресов, защищаемое Шлюзом Безопасности. *ЦУП* использует зоны для того, чтобы проводить трассировку топологии во время трансляции ГПБ, а также, чтобы определять, какие диапазоны IP-адресов защищены каждым Шлюзом Безопасности. Только благодаря зонам *ЦУП* может определить, какие устройства защищены и каким Шлюзом Безопасности!

Объекты зон могут быть созданы только в *Топологии*, однако они не считаются Объектами Политики. Определяются зоны в любой Политике Безопасности, которая включает в себя Шлюзы Безопасности. Входящий трафик для любого из *Агентов* зоны должен проходить через Шлюз Безопасности, который защищает данную зону. Кроме того, несколько зон могут находиться внутри друг друга, однако диапазоны IP-адресов любых двух зон не должны перекрывать друг друга.

7.2.1. Создание Объектов Зон

Объект Зона может создаваться автоматически при создании объекта Шлюз Безопасности, исходя из значений его IP-адресов и их масок и состояния флага **Internet**, выбранного при создании топологии Шлюза. Если флаг **Internet** установлен, то данный интерфейс автоматически входит в зону **Internet**, если флаг **Internet** на интерфейсе Шлюза не установлен, то данный интерфейс автоматически подключается к уже существующей зоне, если адрес и маска соответствуют ее параметрам. Если такой зоны еще нет, то она появится в топологии после создания Шлюза.

Для создания Объекта Зона, после установки *ЗАСТАВА-Управление* надо использовать команду **Добавить Зону.** Откроется окно *Добавить Зону*:

1) Ввести уникальное **Имя** для данной зоны.
2) Перейти во вкладку *Топология*, нажать кнопку **Добавить.**
3) В предлагаемые поля ввести данные об **IP-адресах** для данной зоны.
4) Повторить действия, описанные в пунктах 2) - 3), чтобы добавить следующие IP-адреса в данную зону. В соответствующее поле можно ввести текстовое описание Объекта.

Нажать кнопку **OK**, и в секции *Топология ВЧС* появится новый *Объект зоны*. Все ранее созданные Объекты Политики, чьи IP-адреса попадают в данную зону, будут автоматически отключены от автоматической зоны и подключены к *Объекту зоны,* который Вы только что создали.

Убедиться в том, что IP-адреса, указанные для данной зоны, не включены ни в одну другую зону. Также удостовериться в том, что, если часть диапазона адресов Подсети или диапазона IP-адресов входит в зону, то и все пространство адресов данной Подсети и диапазона IP-адресов тоже находится в этой зоне.

7.2.2. Редактирование параметров зоны

Чтобы отредактировать Объект Зоны надо выбрать его в секции *Топология* , используя опцию **Изменить**. Открывшееся окно *Свойства* идентично окну *Добавить Зону*. Можно удалить защищенный IP-адрес из Зоны или добавить в нее новый, а также отредактировать диапазон IP-адресов, использую кнопки **Добавить, Править** и **Удалить**.

7.2.3. Удаление зон

Выбрать Объект Зоны, используя команду **Удалить** (в главном/контекстном меню) или кнопку на Панели инструментов. После того, как Объект Зоны будет удален, все Объекты Политики, которые были к нему подключены, будут подключены к Объекту **Internet Zone**.

7.3. Правила

Объекты Правил представляют Правила обработки трафика. Правила обработки трафика создаются в соответствии с Политикой Безопасности компании и являются важнейшим элементом ГПБ. При преобразовании ГПБ в ЛПБ, эти глобальные Правила обработки трафика трансформируются в локальные Правила для каждого *Агента*. Обычно, необходимо определить Объекты Политики, IKE-предлагаемые наборы параметров (proposals) и действия до создания Правил. Подробнее см. раздел 4.

7.3.1. Создание Правил

Можно создать новое Правило следующим способом:

– Используйте Править->Добавить-> Правило или команду из контекстного меню *Добавить Правило* в *Секции Правил*. Откроется окно *Добавить Правило*.

В окне *Добавить Правило* указать информацию, необходимую для создания Правила:

– Выбрать Родительское Правило, если такое имеется.
– Ввести уникальное **Имя** для данного Правила.

- Выбрать **Домен**, которому принадлежит Правило.
- Из выпадающего списка выбрать *Действия*, которые будет применять данное Правило.
- Выставить уровень протоколирования (Уровень лога) для Правила (см. Таблица 26).

Таблица 26 – Описание уровней регистрации событий

Параметр	Описание
Нет	События не будут регистрироваться
События	Будут регистрироваться сообщения об ошибках, а также минимум информации об операциях
Детальный	Будет сообщаться полная информация об операциях, с целью поиска неисправностей
Подробный	Будут регистрироваться все события; в основном используется для отладки

- Отметить флаг **Включить Правило**.
- Выбрать один или несколько источников Правила и указать его как инициатора безопасного соединения (Источник). Для этого надо выбрать вложенную вкладку *Объекты* во вкладке *Источники,* переместить Объекты Политики из списка *Доступные объекты* в список *Выбранные объекты*.
- Если в дальнейшем Вы хотите идентифицировать источники для Правила по расположению Объектов (например, если источники находятся в сегменте сети WiFi) надо нажать кнопку **Показать Расположения** и переместить местоположения из списка *Доступные объекты* в список *Выбранные объекты*. При создании Правил с участием Пользователей, см. также п. 7.3.8.
- Выбрать **Цель Правила**. Для этого выбрать вложенную вкладку *Объекты вкладки Приемники* переместить Объекты Политики из списка *Доступные объекты* в список *Выбранные объекты*.
- Если в дальнейшем Вы хотите идентифицировать Цели правила по расположению Объектов (например, если Цели находятся в сегменте сети WiFi) надо нажать кнопку **Показать Расположения** и переместить список от *Доступные Расположения* в список *Выбранные Расположения*.
- Выбрать **Маршрут Правила**.
- Выбрать Сетевые сервисы, которые будут использовать данное Правило (если необходимо). Для этого надо выбрать вкладку *Сетевые Сервисы* и переместить сетевые сервисы из списка *Доступные Сервисы* в список *Выбранные Сервисы*.
- Выбрать **Расписание для Правила**.

Новое Правило будет добавлено в *Таблицу Правил*.

Уровень регистрации **Подробный** создает огромное количество сообщений; эту настройку следует использовать с особой осторожностью.

Изначально Правила могут создаваться с пустыми полями **Источник** и **Цель** (Приемник). Однако при трансляции такие Правила станут причиной ошибок.

Если Вы установили протокол TCP в качестве сетевых сервисов, можно указать, кто может инициировать TCP-соединения, выбрав значение "refuse incoming TCP connections". Таким образом, обозначения **Источник** и **Цель** важны при использовании Правилом Объекта сетевых сервисов, который содержит асимметричные процедуры МЭ или TCP-сервиса, с установленной отметкой в поле **Refuse incoming TCP connections**.

7.3.2. Редактирование Правил

Отредактировать Правило можно одним из следующих способов:

– В *Таблице Правил* выбрать строку, содержащую данное Правило, используя команду **Изменить**.

– Дважды нажать левой кнопкой мыши на соответствующем пункте в *Таблице Правил*.

Открывшееся окно *Изменить Правило* идентично окну *Добавить Правило*. Отредактировать параметры Правила способом, описанным выше.

7.3.2.1. Одновременное редактирование нескольких Правил

Можно одновременно редактировать параметры для нескольких Правил. С помощью клавиш <Shift> или <Ctrl> и мыши выбрать в *Таблице Правил* все Правила, чьи параметры Вы хотите отредактировать. Используйте команду **Изменить** контекстного меню. Появится подменю, содержащее список индивидуальных параметров Правил, которые можно применить к Группе.

Изменить в диалоговом окне значение нужного параметра. Значение этого параметра будет изменено для всех выбранных Правил.

7.3.2.2. Сортировка Объектов Политики при создании Правила

В *Таблице Правил* можно отсортировать Объекты Политики во вкладке *Источник* или *Приемник*, или сетевой сервис во вкладке *Сетевые Сервисы* по имени и типу, для этого нужно воспользоваться контекстным меню.

7.3.3. Удаление Правил

Выбрать строку, содержащую нужное Правило в *Таблице Правил*, и использовать команду **Удалить** (главное/контекстное меню или Панель инструментов).

Можно одной командой удалить сразу несколько Правил. Надо выделить Правила, которые Вы хотите удалить, с помощью мыши и удерживая клавишу <Ctrl> или <Shift>. Выполнить команду **Удалить**.

7.3.4. Создание иерархии Правил

После того как Вы создали Правило, можно вложить данное Правило в другое Правило, т.е. сделать его вложенным Правилом (исключением или дополнением) главного Правила. Это делается только для того, чтобы перемещать *Объект Правила* среди различных уровней иерархии Правил, а не для изменения порядка применения Правил, находящихся на одном уровне (последнее невозможно в любом случае). Можно сделать следующее:

- Повысить значимость вложенного Правила на один или более уровней вверх по иерархии (например, сделать «дочернюю» значимость Правила «родительской» или включить Правило в Родительское Правило).
- Понизить значимость Правила можно, переместив его на несколько уровней вниз по иерархии (например, сделать Родительское Правило «дочерним» Правилом другого Родительского Правила).

Функция перемещения Объектов Правил по иерархии может оказаться полезной в том случае, например, если один из отделов отделения Вашей компании был переведен в другое отделение. Правила, управляющие соединениями отдела можно переместить из головного Правила «старого» отдела в «новый» с помощью одной команды. То же применимо к работнику, которого переводят из одного отдела в другой или из одного места в другое. Даже если Вы по ошибке поместите Правило не туда, его легко можно будет перенести.

Правила и вложенные Правила на данном уровне иерархии могут применяться в любом порядке. Единственным исключением здесь являются Правила **"Any↔Any" (Любой-Любой**), которые всегда применяются последними, и Правила **"Any↔agent" (Любой-*Агент***) и/или Правила, включающие Пользователей, применяются в предпоследнюю очередь. Родительское Правило применяется только после всех «дочерних» Правил.

7.3.4.1. Перемещение Правила на более низкий уровень иерархии

Чтобы сделать Правило «дочерним» Правилом, надо открыть окно *Изменить Правило* и в выпадающем меню *Родитель* выбрать соответствующее Родительское Правило.

7.3.4.2. Перемещение Правила на более высокий уровень иерархии

Чтобы переместить Правило на корневой уровень, надо открыть окно *Изменить Правило* и в выпадающем меню *Родитель* выбрать пункт **Нет родительского правила**. Чтобы

переместить Правило на один уровень вверх надо выбрать для него Родительское Правило уровнем выше.

7.3.5. Выключение и включение Правил

При необходимости Правила можно выключать и включать. Способность к выключению и включению отдельных Правил является одним из основных аспектов процесса создания и тестирования ГПБ. Также это может пригодиться для введения временных изменений в рабочую Среду Безопасности. Выключенное Правило не будет транслироваться, и, таким образом, выключение Правил может использоваться для определения неисправностей.

Чтобы выключить Правило, надо выбрать его в *Таблице Правил* и использовать в контекстном меню команду **Выключить**. В *Таблице Правил* появится соответствующая пиктограмма  .

Чтобы включить Правило, надо выбрать его и использовать в главном или контекстном меню команду **Включить**. На иконке включенного Правила исчезнет красный круг с белым знаком **X**.

Можно выключать и включать группы Правил с помощью одной команды. Надо выделить Правила, которые Вы хотите выключить или включить с помощью мыши, удерживая клавишу <Ctrl> или <Shift>. Затем используйте в контекстном меню команду **Выключить** или **Включить**.

Если Вы заблокируете Родительское Правило, вместе с ним будут заблокированы все его «дочерние» Правила (если они есть).

7.3.6. Скрытие Правил

Можно скрыть одно Правило или Группу Правил при отображении. Для этого надо выбрать нужное Правило или Группу Правил в *Таблице Правил*. Затем использовать команду **Скрыть** в контекстном меню.

Чтобы показать скрытые Правила надо использовать в контекстном меню команду **Раскрыть.** Все скрытые Правила тут же появятся, независимо от того, сколько раз была использована команда **Скрыть**.

Для удобства скрытия нескольких правил можно воспользоваться командой **Скрыть остальные**, для этого надо выделить одно или несколько правил, которые скрывать не надо, и выбрать в контекстном меню команду **Скрыть остальные.**

7.3.7. Трассировка Правил

Поскольку схемы Объектов в *Графе топологии* могут быть довольно сложными, *ЦУП* позволяет напрямую наблюдать в *Топологии* путь трафика для конкретного Правила, выбранного в *Таблице Правил или в Серверные Правила*.

Для трассировки Правила выбрать его в *Таблице Правил или в Серверные Правила* и использовать в контекстном меню команду **Показать трассу**. Линии, которые представляют поток данных между Объектами Политики, указанными в Правиле, будут отображаться в виде цветных линий. Правила окраски следующие:

1) Правило с действием PASS отображается зеленым цветом.
2) Правило с действием DROP отображается красным цветом.
3) Правило с действием Encrypt отображается синим цветом.
4) Правило с действием NAT+PASS или IKECFG+PASS отображается коричневым цветом.
5) Правило с действием NAT+IPSEC или IKECFG+IPSEC отображается фиолетовым цветом.

7.3.8. Особенности создания Правил, где участвуют Пользователи

Создание Правил, где участвуют Пользователи, происходит следующим образом:

1) Поскольку для объекта Пользователь его расположение в топологии сети неизвестно, существует ряд особенностей при создании Правил вида **Пользователь->Ресурс**, где: Ресурс – произвольный Объект Политики (например, Подсеть). При трансляции подобных Правил подразумевается, что Пользователь располагается только в Зоне Internet (т.е. трассы будут строиться только из Зоны Internet к Ресурсу). Поэтому, если Пользователь может находиться еще и в других местах (Подсетях, Диапазонах), которые находятся не в Зоне Internet, необходимо *явно* прописать эти места в поле **Расположения** (Locations) в данном Правиле.

2) В ситуации, когда *ЦУП* находится за NAT и Пользователь оказался в одной зоне с *ЦУП* (изнутри NAT), то правило прогрузки Пользователя может не сработать, поскольку в конфигурации Пользователя будет указан внешний NAT-адрес *ЦУП* (при условии, что нет других Правил с Пользователями из зоны *ЦУП*). В таком случае необходимо создать явное правило вида «Пользователь*@ЗонаЦУП -> ЦУП*, Pass», т.е. указать транслятору на то, что Пользователи могут появляться в Зоне *ЦУП*.

7.3.9. Фильтрация в окне *Таблица правил*

При большом количестве правил поиск нужного правила становится затруднительным. Для отфильтрования необходимой информации служит строка ввода *Что искать*. Действие фильтра распространяется на таблицу *Таблица правил*, если она отвечена в поле *Поиск в панели*. Фильтрация осуществляется по полям **ID в БД**, **Имя**, **Описание, Действие**, **Объект политики**, **Расписание, Сетевой сервис** таблицы. Фильтр применяется после нажатия кнопки **Готово**.

7.3.10. Расписания Правил

Для просмотра окна Расписаний нужно выбрать пункт **Расписания** в меню *Окно* (см. Рисунок 64).

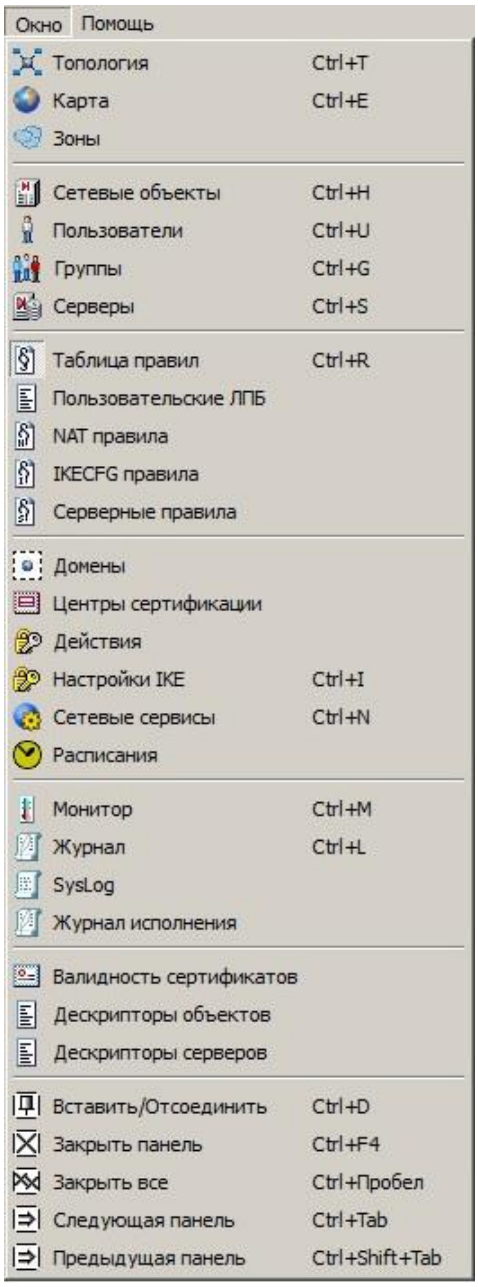

Рисунок 64 - Вызов окна Расписаний Правил

Добавить новое Расписание можно с помощью контекстной команды **Создать Расписание** или соответствующей командой в меню *Править*.

Окно просмотра содержит следующую информацию о Расписании: Имя, Дату активации, Дату завершения, Часы действия, Дни недели, в течение которых Правило активно и Домен, которому принадлежит Расписание (см. Рисунок 65).

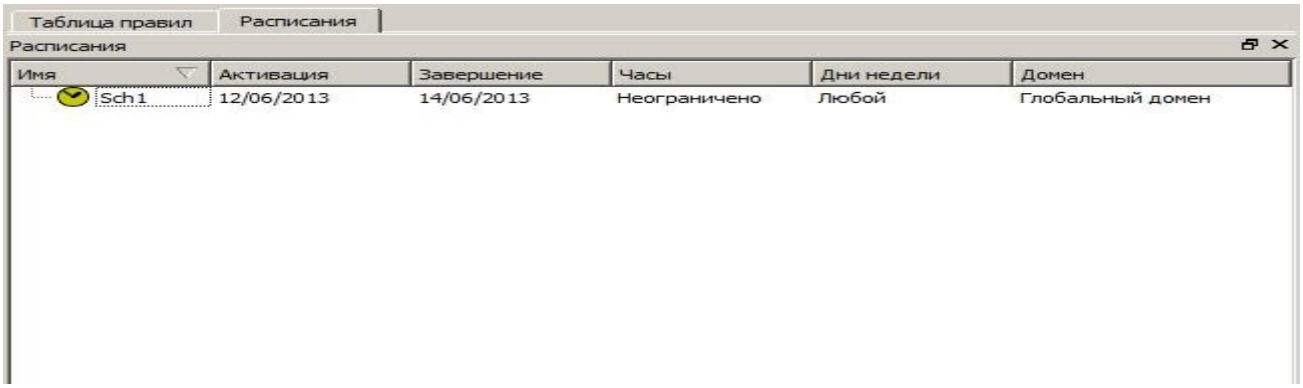

Рисунок 65 – Окно просмотра Расписаний

При создании или изменении нового/существующего Расписания необходимо указать параметры этого Расписания (см. Рисунок 66).

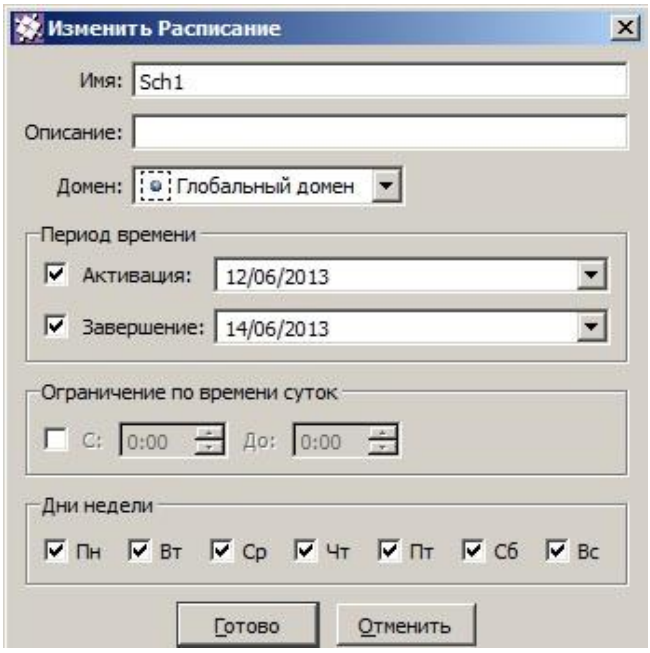

Рисунок 66 – Параметры Расписания

Для создания Расписания необходимо:

- Задать уникальное Имя;
- При необходимости ввести текстовое Описание;
- Выбрать Домен, которому будет принадлежать Расписание;

– Указать дату активации и завершения Правил, входящих в данное Расписание (при необходимости);
– Указать период времени суток, в течение которого будут выполняться Правила, входящие в данное Расписание (при необходимости);
– Указать дни недели, в течение которых будут выполняться Правила, входящие в данное Расписание (при необходимости).

7.4. Домены

7.4.1. Операции с доменами

По умолчанию в ГПБ создается домен с именем **Глобальный домен**. Удалить **Глобальный домен** невозможно. Для добавления домена нужно воспользоваться контекстным меню вкладки *Домены* рабочей области, выбрав пункт **Добавить домен** или выбрав пункт **Добавить домен** из меню *Править*.

Для дублирования/изменения/удаления домена нужно воспользоваться контекстным меню Объекта домен вкладки *Домены* рабочей области, выбрав пункт **Дублировать/Изменить/Удалить** (см. Рисунок 67) или при помощи команд инструментальной линейки.

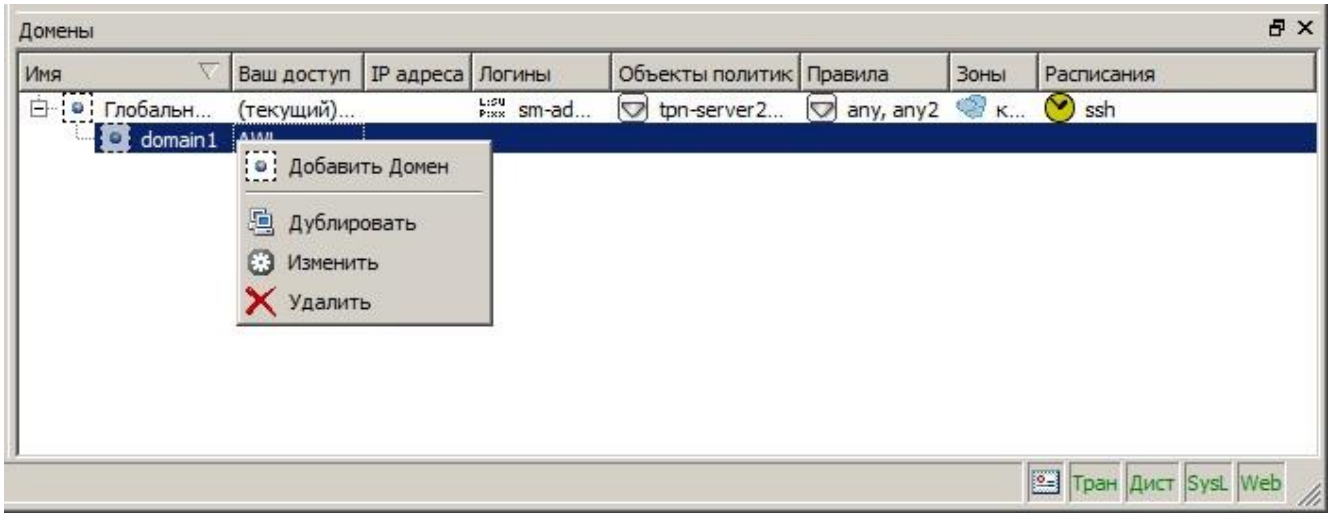

Рисунок 67 – Дублирование/Изменение/Удаление домена

Невозможно удалить Домен, которому принадлежат Объекты Политики.

Для отображения/скрытия вкладки *Домены* необходимо выбрать пункт **Домены** в меню *Окно*.

Существует иерархия доменов. Связь создаваемого домена с родительским задается при помощи выпадающего списка *Родитель* вкладки *Общие* диалогового окна *Добавить Домен/Изменить Домен* (см. Рисунок 68).

Существует возможность обновления дескрипторов *Агент* версии 6.1 и выше в домене и загрузки обновлений в *Агент*, для этого необходимо воспользоваться контекстным меню *Домена,* выбрать в нем пункт **Обновить версию агентов в домене** или **Загрузить обновления для Агентов в домене.**

Существует возможность загрузки сертификатов для дескрипторов *Агент* версии 6.1 и выше в домене, для этого необходимо воспользоваться контекстным меню *Домена* и выбрать в нем пункт **Загрузить список сертификатов** после загрузки сертификатов добавить сертификаты в политику выбрав пункт контекстного меню **Добавить полученные сертификаты в политику**. В открывшемся окне *Импорт сертификатов* проверить полученные сертификаты и нажать кнопку **Готово**. Для удаления загруженных сертификатов необходимо выбрать пункт контекстного меню **Удалить запросы для сертификатов или ключей.**

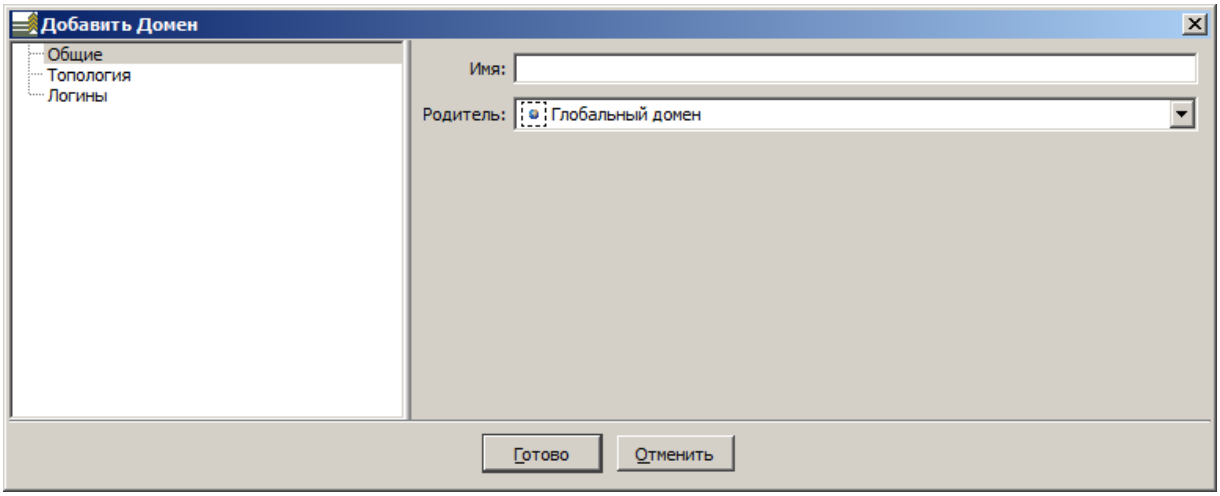

Рисунок 68 – Связь с Родительским доменом

7.4.2. Топология доменов

Для описания принадлежности сетевых объектов домену необходимо в топологии домена описать IP-диапазоны, из которых выделены IP-адреса сетевым объектам. Если у сетевых объектов отсутствую IP-адреса, то их принадлежность домену можно описать при условии, что в топологии домена отсутствует описание IP-диапазонов. Список IP-диапазонов домена задается на вкладке *Топология* диалоговых окон *Добавить Домен* или *Изменить Домен* (см. Рисунок 69).

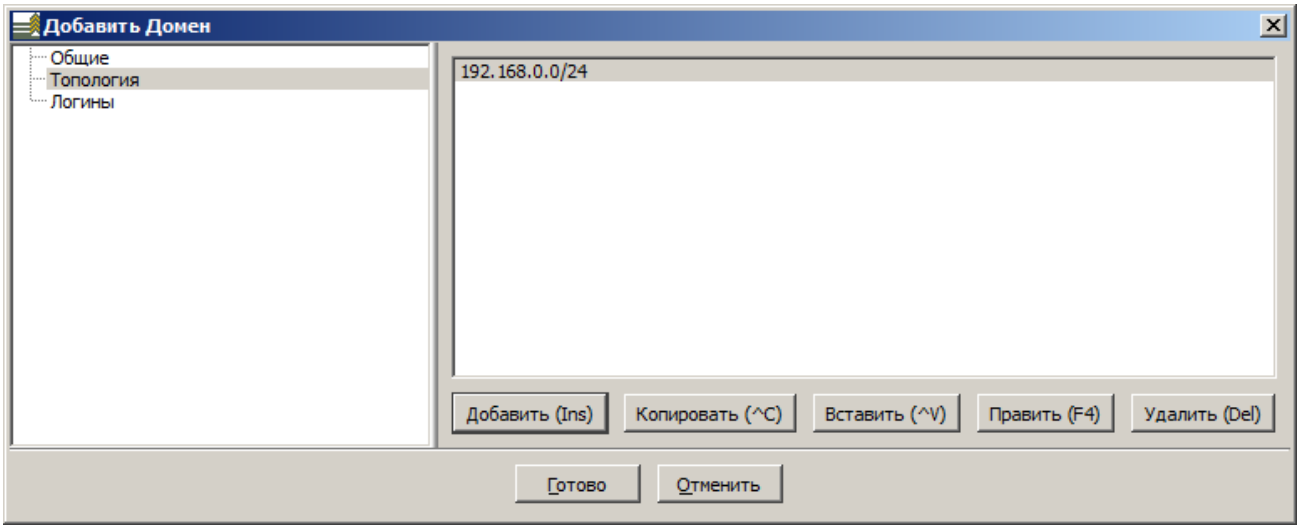

Рисунок 69 – Топология домена

Для добавления IP-диапазона в топологию создаваемого/существующего домена нужно на вкладке *Топология* диалогового окна *Добавить Домен* нажать кнопку **Добавить** или клавишу <Insert>. Далее появится диалоговое окно *Добавление IP диапазона*, в поле **Тип элемента** которого можно указать один из трех типов элементов:

- IP-Адрес + Маска (выбирается по умолчанию) – для указания IP-адреса Подсети с маской Подсети (IP-адрес подсети может быть указан только в десятичной системе исчисления, маска Подсети может быть указана как в слэш-нотации, так и в десятичной системе исчисления);
- Один IP-Адрес – для указания одного IP-адреса (IP-адрес может быть указан только в десятичной системе исчисления);
- IP-Диапазон – для указания IP-Диапазона, заключенного между первым и последним IP-адресами (IP-адреса могут быть указаны только в десятичной системе счисления).

7.4.3. Определение Объектов Политики в домен

Доменная модель позволяет описать принадлежность домену следующих Объектов Политики:

- Подсеть;
- IP-диапазон;
- IP-хост;
- Хост Безопасности;
- Шлюз Безопасности;
- Группа;
- Пользователь;

– Расписание.

Ни один из вышеперечисленных Объектов не может одновременно принадлежать разным Доменам.

Принадлежность Объекта Политики домену описывается на вкладке *Общие* диалогового окна *Добавить/Изменить* Объекта Политики (см. Рисунок 70).

Доменная модель также позволяет описать принадлежность домену таких Объектов Политики, как:

– Правило;

– Группа Правил.

Ни один из вышеперечисленных Объектов не может одновременно принадлежать разным Доменам.

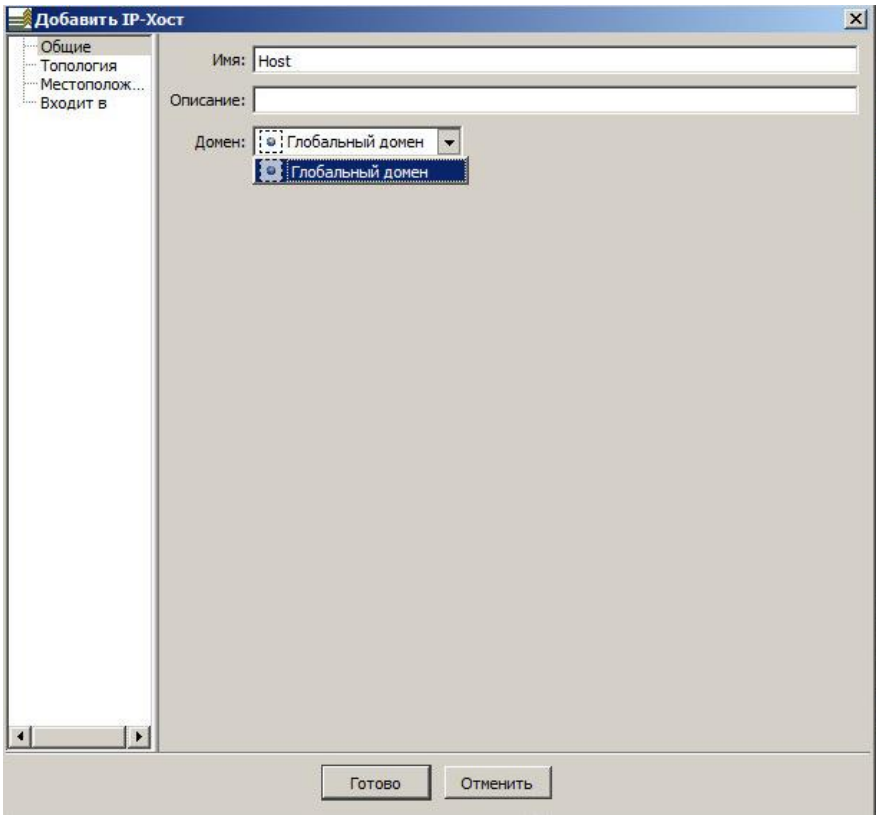

Рисунок 70 – Определение принадлежности Объекта Политики Домену

Принадлежность Объекта Политики «Правило» домену описывается на вкладке *Общие* диалогового окна *Добавить Правило* (см. Рисунок 71).

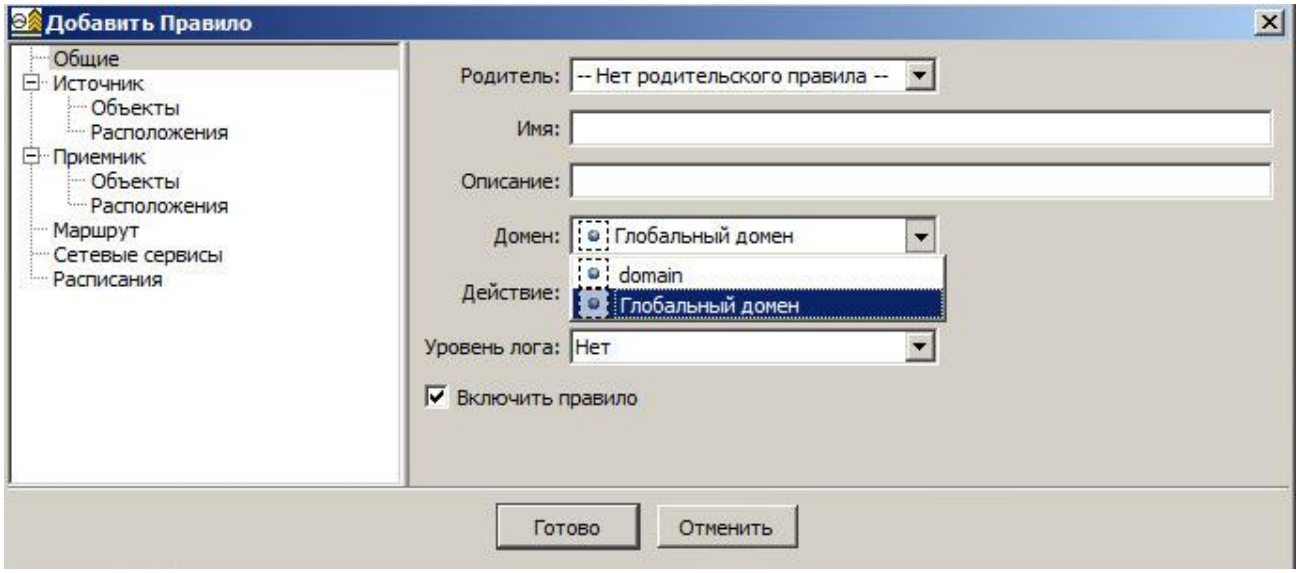

Рисунок 71 – Определение принадлежности Объекта Политики «Правило» домену

Принадлежность Объекта Политики **Группа Правил** домену определяется аналогичным образом.

Если Группа принадлежит домену, то в Группу могут входить Объекты Политики только из этого домена и доменов, для которых данный домен является Родительским.

Если Правило принадлежит домену, то Источником и Приемником в Правиле могут быть Объекты Политики только из этого домена и доменов, для которых данный домен является Родительским.

7.4.4. Учетные записи доменов

Управление учетными записями создаваемого/существующего домена осуществляется на вкладке *Логины* диалогового окна *Добавить Домен* (см. Рисунок 72).

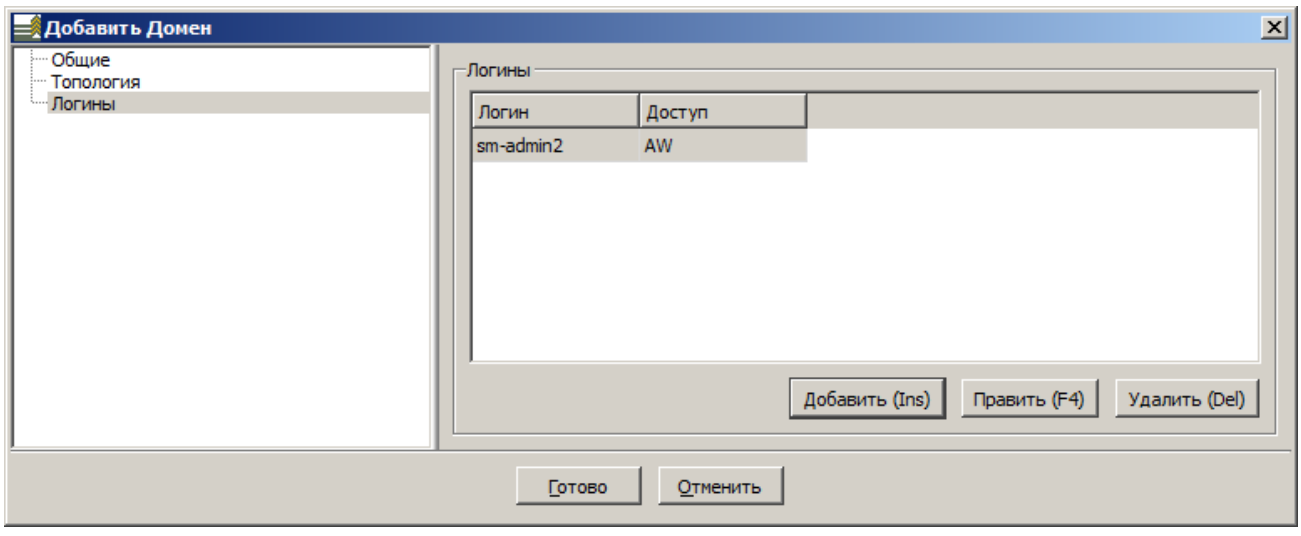

Рисунок 72 – Управление учетной записью Домена

Для создания учетной записи создаваемого/существующего домена нужно на вкладке *Логины* диалогового окна *Добавить Домен* нажать кнопку **Добавить** или клавишу <Insert> и в появившемся диалоговом окне *Добавить логин* ввести название учетной записи в поле **Имя пользователя.**

Для задания пароля для учетной записи нужно в диалоговом окне *Добавить Логин* нажать кнопку **Установить пароль…** и ввести пароль в полях **Пароль** и **Подтвердите пароль** появившегося диалогового окна *Введите пароль* (см. Рисунок 73). Для просмотра введенного пароля нужно воспользоваться флагом **Показать пароль**, который автоматически исчезает через три секунды. Ограничение на количество символов в пароле отсутствует.

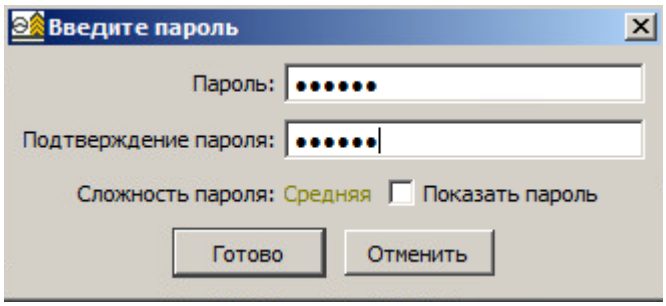

Рисунок 73 – Диалоговое окно *Введите пароль*

Для правки учетной записи создаваемого/существующего домена нужно на вкладке *Логины* диалогового окна *Добавить Домен* нажать кнопку **Править** или клавишу <F4>, для удаления учетной записи создаваемого/существующего домена нужно на вкладке *Логины* диалогового окна *Добавить Домен* нажать кнопку **Удалить** или клавишу <Delete>.

В группе **Доступ** диалогового окна *Добавить Логин* при помощи флагов можно задать следующие права доступа:

- *Активация (A)* – право активировать ГПБ на хостах, относящихся к текущему домену. Правом на глобальную активацию и активацию обновленных *Агентов* имеет право только Глобальная учетная запись. Правом на трансляцию также обладает только Глобальная учетная запись.
- *Запись (W)* – право удалять, создавать и модифицировать объекты, относящиеся к текущему домену, за исключением самих доменов, учетных записей, а также диапазонов IP-адресов из числа задающих топологию самого домена. Это право дает возможность выполнить трансляцию для объектов текущего домена и доменов вниз по иерархии.
- *Управление логинами (L)* – право удалять, создавать и модифицировать следующие объекты, относящиеся к текущему домену: сами домены, их подчинение другим доменам, учетные записи доменов, их имена, пароли, права, а также ограничения на

адреса в домене. Право на управление учетными записями автоматически дает права **Активации** и **Записи**.

7.5. Настройки IKE

Объекты *IKE-Предложение* – это набор параметров IKE, предлагаемых партнеру по связи для согласования защищенного соединения ISAKMP во время первой фазы IKE. Если есть несколько *IKE-Предложений*, то их параметры предлагаются последовательно, согласно с их положением в дереве (сверху вниз). Параметры *IKE-Предложения* инициатора защищенного соединения сравниваются с параметрами IKE предлагаемого партнера по связи. Если предлагаемые параметры сходятся, устанавливается сессия ISAKMP/IKE SA.

Чтобы перейти в окно *Настройки IKE* надо выбрать *Настройки IKE* в меню *Окно*. По умолчанию окно настроек IKE появится под секцией *Топологии*. Существует два уровня настройки параметров IKE. Они оба автоматически обнаруживаются еще до настройки конфигурации.

Параметры Объекта **Первая фаза** не зависят от того, какие алгоритмы шифрования доступны для управляемых *Агентов* (для *Агентов* это криптоплагины, устанавливаемые в модуле). Эти параметры являются глобальными и затрагивают все *Объекты ГПБ,* которые участвуют в Правилах.

IKE-Предложения связаны с алгоритмами аутентификации и шифрования. Они создаются пользователями; можно создать любое необходимое количество, в зависимости от того, какие алгоритмы шифрования доступны.

7.5.1. Объект первой фазы

7.5.1.1. Обмен сертификатами

Параметр **Обмен сертификатами** позволяет Вам выбрать один из трех вариантов, определяющих обмен сертификатами во время переговоров ISAKMP SA (см. Таблица 27). По умолчанию будет установлено значение **Всегда**.

Таблица 27 – Описание параметров обмена сертификатами

Параметр	Описание
Всегда	Обмен сертификатами между партнерами по связи будет производиться всегда, при переговорах в защищенном соединении.
Всегда по цепочке	При переговорах в защищенном соединении всегда будет производиться обмен сертификатами между партнером по связи и полной цепочкой аутентификации сертификатов, включая сертификаты УЦ. Эта функция особенно важна, когда сертификат одного из партнеров по связи принадлежит компании, которая использует более одного УЦ.
Никогда	При переговорах в защищенном соединении обмен сертификатами производиться не будет.

7.5.1.2. Режимы IKE

Выбрать режим соединения, который будет использоваться для защищенного обмена: **Основной режим, Агрессивный режим** или комбинация этих двух режимов (см. Таблица 28). **Основной режим** предоставляет полную защиту, однако, требует больше времени, включая минимум шесть обменов. **Агрессивный режим** не гарантирует полную защиту, однако, включает в себя менее шести обменов; он может быть использован при недостатке времени. Можно использовать комбинацию этих двух режимов.

Таблица 28 – Режимы IKE

Параметр	Характеристики
Основной режим	*Агенты* будут использовать только **Основной режим** для инициирования IKE защищенного соединения и будут отвечать только тем IKE защищенным соединениям, которые используют данный режим
Агрессивный режим	*Агенты* будут использовать только **Агрессивный режим** для инициирования IKE защищенных соединений и будут отвечать только тем IKE защищенным соединениям, которые используют данный режим
Основной режим, затем **Агрессивный**	Если данный *Агент* является инициатором IKE защищенного соединения, тогда для его установки будет использован **Основной режим**; если же *Агент* является приемником, то используемый режим будет зависеть от режима, применяемого инициатором (будет принят любой из двух)
Агрессивный режим, затем **Основной**	Если данный *Агент* является инициатором IKE защищенного соединения, тогда для его установки будет использован **Агрессивный режим**; если же *Агент* является приемником, то используемый режим будет зависеть от режима, применяемого инициатором (будет принят любой из двух)

Сделайте выбор, установив соответствующий переключатель.

7.5.1.3. Разрешение пуска

Если в поле **Разрешить автопропуск** стоит отметка**,** трафик протокола ISAKMP/IKE между двумя партнерами по связи будет пропускаться вне зависимости от индивидуальных настроек партеров по связи. Например, если настройки отдельно взятого Объекта хоста Безопасности, Шлюза Безопасности, пользователя не разрешают автопропуск трафика, это означает, что клиент желает закрыть порт UDP 500, используемый для передачи ISAKMP-трафика и значит невозможно создать IKE защищенное соединение с таким *Агентом*. Если Вы поставите отметку в поле **Разрешить автопропуск**, то порт UDP 500 будет принудительно открыт для пропуска ISAKMP-трафика, но только для тех партнеров по связи, которые участвуют в Правиле с этим *Агентом*.

Если Вы уберете отметку в поле **Разрешить автопропуск**, это будет означать, что пропуск ISAKMP/IKE-трафика между Объектами Политики запрещен. Таким образом, невозможно будет установить защищенное соединение IKE между Объектами Политики, управляемыми *ЦУП*! (Необходимо вручную создать Правила для пропуска IKE-трафика). В обычных условиях рекомендуется поставить отметку в этом поле.

7.5.2. Объекты IKE-Предложение

Параметры IKE, связанные с алгоритмами аутентификации и шифрования, должны быть установлены в *ЦУП-Консоль*. Можно как изменять настройки Объектов *IKE-Предложения* (предлагаемых наборов параметров) по умолчанию, так и создавать новые Объекты. Параметры, которые Вы выберете, будут зависеть от алгоритмов шифрования, поддерживаемых не только *ЦУП,* но и всеми остальными *Агентами*, включая устройства третьей стороны. (В *Агентах* поддерживаемые алгоритмы шифрования зависят от установленных криптоплагинов). Не выбирайте параметры, которые не поддерживаются алгоритмами шифрования, установленными в данный момент.

7.5.2.1. Создание и редактирование Объектов IKE-Предложение

Если будет использоваться только один набор IKE-параметров, тогда не обязательно создавать новый предлагаемый набор параметров. Если Вам необходимо изменить параметры, установленные по умолчанию, для уже существующего набора, можно просто отредактировать Объект *IKE-Предложение*, установленный по умолчанию. Для этого надо выбрать Объект *IKE-Предложение* и отредактировать его параметры в выпадающих списках и числовых полях, которые появятся в окне *Настройки IKE*.

Если участники Вашей Среды Безопасности будут использовать разные опции аутентификации и шифрования, тогда Вам потребуется более одного набора IKE-параметров. Если партнеры по связи в Вашей ГПБ будут использовать предварительно распределенные ключи, тогда Вам необходимо создать особое *IKE-Предложение*, в котором будет определяться порядок аутентификации предварительно распределенных ключей. Если существует более одного набора IKE-параметров надо указать порядок Объектов в дереве, с помощью выпадающего меню *Приоритет в Настройках IKE.* Высшая позиция в дереве обозначает самые предпочтительные параметры ГПБ. Объекты, занимающие нижние позиции, определяют менее предпочтительные параметры.

Чтобы создать новый Объект *IKE-Предложение* надо выбрать корневой узел *Первая фаза* или любой существующий узел *IKE-Предложения*, используя команду **Добавить IKE – Предложение** в главном или контекстном меню, откроется окно *Создания IKE-Предложения.* Затем выбрать и/или ввести нужные значения параметров *IKE-Предложения* (см. Таблица 29).

Таблица 29 – Атрибуты IKE Proposal

Параметр	Описание
Аутентификация	Алгоритм аутентификации IKE
Алгоритм шифрования	Алгоритм шифрования IKE

Параметр	Описание
Алгоритм хеширования	Алгоритм реализации хеш-функции IKE
Oakley группа	Определяет параметры, используемые для того, чтобы создать ключевой материал (keying material)
Время жизни SA по времени (сек)	Максимальная продолжительность ISAKMP защищенного соединения в секундах
Время жизни SA по трафику (Кбайт)	Максимальный размер трафика ISAKMP защищенного соединения в килобайтах
Уровень лога	Количество событий, записываемых в журнал регистрации *Агента*, при установлении IKE защищенного соединения с партнером по связи
Приоритет	Приоритет *IKE-Предложений* соответствует порядку, в котором они указаны в дереве - сверху вниз. Приоритет может быть от 1 до 4. Самые приоритетные (желаемые) *IKE-Предложения* должны находиться выше всех остальных в структуре.

Не обязательно указывать имя для *IKE-Предложения*. Они просто будут пронумерованы в том порядке, в котором они отображаются.

Если команда **Добавить IKE-Предложение** была запущена в то время, когда был выбран корневой узел **Первая фаза,** в окне *Добавить IKE-Предложение* значения для перечисленных выше параметров будут установлены по умолчанию. Если же команда была запущена в тот момент, когда было выбрано существующее *IKE-Предложение,* поля в этом окне будут содержать те же значения, что и поля выбранного Объекта.

Некоторые типы алгоритмов аутентификации и шифрования, представленные по умолчанию в *ЦУП,* действительны только для Российской Федерации - это алгоритмы аутентификации **GOST R 34 10-94 Signature** и **GOST R 34.10-2001 Signature** и алгоритмы шифрования и хеширования **GOST-TIK** и **GOST-CPRO.**

7.6. Действия

Действия определяют, как входящий/исходящий трафик, будет обрабатываться на данном устройстве защиты. Объект действия представляет комбинации опций аутентификации и шифрования, которые используются Правилами ГПБ для того, чтобы определять, как *Агенты* в данной Среде Безопасности будут обрабатывать различные типы трафика (установленные в сетевых сервисах). По умолчанию установлено Действие *Encrypt (CPRO),* которое зашифровывает трафик с помощью алгоритма ГОСТ, затем пропускает его.

Объекты действий могут создаваться и редактироваться в окне *Действия,* вызываемом из меню *Окно*, здесь представлены все существующие *Действия*. Чтобы добавить Действие, надо в контекстном меню этого окна выбрать команду **Добавить действие** (та же команда в меню *Править*). В этом окне создаются и редактируются только те Действия, которые используют шифрование. Действия **PASS** (пропустить) и **DROP** (блокировать) отредактировать нельзя.

Каждое Действие представлено вкладками *Действие* и *Предложение*, в каждой из которых есть набор параметров.

7.6.1. Создание Действий

Чтобы создать Действие необходимо:

1) В окне *Действия*, выбрать команду **Добавить Действие** из контекстного меню. Откроется окно *Добавить Действие* (см. Рисунок 74).
2) Ввести уникальное **Имя** для нового Действия.
3) При необходимости можно ввести текстовое описание Действия.
4) Если установить флаг **Использовать сервис для IPSec SA**, то, при использовании сервисов, создаются узкие правила с FW-процедурами с указанием порта и протокола, если флаг снят, то используются широкие Правила.

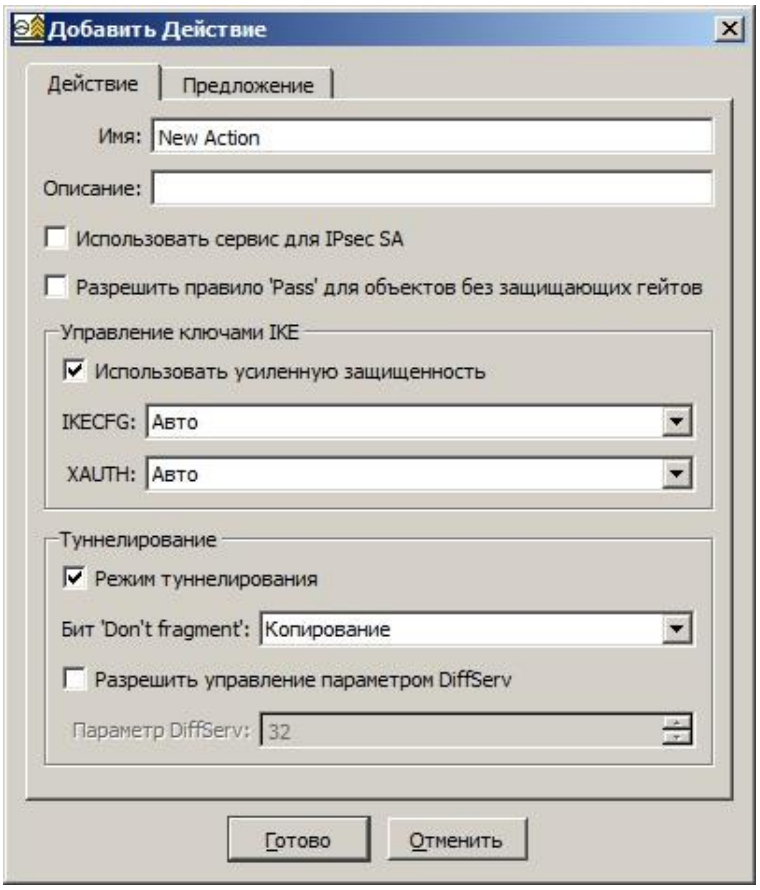

Рисунок 74 – Настройка параметров управления QoS

5) Если Вам необходимо создать правило для группы сетей, которые находятся за одним и тем же гейтом, необходимо поставить галочку в поле **Разрешить правило ‘Pass’ для объектов без защищающих гейтов** для того, чтобы между этими сетями не делать IPsec-туннель.
6) Если Вы хотите использовать **Использовать усиленную защищенность (**криптосистему, где шифрованный текст не дает никакой информации об открытом

тексте, возможно, за исключением его длины), которая будет создавать новую пару ключей для каждого сеанса защищенного соединения IPsec, надо поставить отметку в поле **Использовать усиленную защищенность**. Таким образом, каждый раз во время второй фазы IKE-переговоров защищенного соединения IPsec будет создаваться новый ключ. Иначе во второй фазе будет использоваться тот же ключ, что и в первой. Использование **Использовать усиленную защищенность** безопаснее, однако требует больше времени.

7) Выбрать одно из значений из выпадающего списка *IKE CFG,* чтобы настроить работу алгоритма трассировки топологии *ЦУП*. Этот алгоритм устанавливает, какой путь будет использоваться трафиком между источником и приемником Правила, которое применяет данное Действие:

   – **Вкл** - при поиске путей для данного Правила будут выбраны только те, которые проходят через Шлюз, на котором включен **IKE CFG**;
   – **Выкл** - при поиске путей для данного Правила будут выбраны только те, которые *не* проходят через Шлюз, на котором включен **IKE CFG**;
   – **Авто** - алгоритм трассировки топологии будет выбирать пути с или без **IKE CFG** в зависимости от настроек Объектов, которые должны вступить в соединение.

8) Значение, которое Вы выбираете в выпадающем списке *XAUTH,* также повлияет на алгоритм трассировки *ЦУП*. Значения те же, что и для **IKE CFG**.

9) Если Вы хотите, чтобы протоколы IPsec AH и ESP действовали в режиме туннелей, не убирайте отметку в поле **Режим туннелирования**. Если же Вы уберете эту отметку, протоколы будут работать в транспортном режиме.

10) Если Вы поставили отметку в поле **Режим туннелирования**, надо выбрать параметры для *Don*`t *fragment bit* из выпадающего списка. Этот параметр устанавливает тэг *Don`t fragment bit* в IP-пакетах для Правил, которые используют Действия по защите в туннельном режиме. Новый IP-заголовок будет добавлен ко всем IP-пакетам, а тэг *Don`t fragment bit* будет управлять процессом установки значения бита *"don`t fragment bit (бит не выполнения фрагментации)"* в новом внешнем IP-заголовке. Доступны следующие установки:

   – **Копирование -** копировать значение бита *"don`t fragment bit"* из исходного IP-пакета;
   – **Установка -** устанавливает значение бита *"don`t fragment bit"* на 1;

– **Очистка -** устанавливает значение бита *"don`t fragment bit"* на 0 *(по умолчанию).*

11) *Агенты* поддерживают управление QoS (качество обслуживания) путем модификации поля **Параметр DiffServ (0-63)** (точнее, DSCP: differentiated services codepoint) при туннелировании IP-пакетов. Данная функциональность полезна для протоколов, чувствительных к задержкам (VoIP и т.п.). Для включения данного режима надо отметить флажок **Разрешить управление параметром DiffServ** и установить нужное значение в поле **Параметр DiffServ (0-63)** (см. Рисунок 74). Более подробная информация о поле **Параметр DiffServ** и рекомендуемых значениях DSCP приведена в RFC2474, RFC2475, RFC2597 и RFC2598 (см. `www.ietf.org`). К примеру, для голосового трафика рекомендуемое значение DSCP – 46 (101110).

7.6.2. Создание IPsec-Предложения

Существует два способа создания нового IPsec-Предложения (предлагаемого набора параметров IPsec) внутри Объекта Действия: это можно сделать в процессе создания нового Объекта Действия, или же можно добавить Предложение к уже существующему Объекту Действия. В первом случае окно *Новое IPsec-Предложение* появится автоматически после создания Объекта Действия. Во втором случае, выбрать Объект Действия в соответствующем дереве и использовать в контекстном меню команду **Добавить IPsec-предложение.** Появится окно *Добавить IPsec-Предложение.*

1) Установить, будет ли использоваться протокол ESP (по умолчанию он будет использоваться). Если Вы оставите отметку в поле, нужно будет выбрать параметры протокола ESP.

2) Выбрать **Алгоритм шифрования**, который будет использоваться ESP.

3) Выбрать **Алгоритм Аутентификации**, который будет использоваться протоколом ESP.

4) Выбрать: будет ли использоваться протокол AH **(Применить AH протокол)**. Если Вы поставите отметку в соответствующем поле, необходимо будет выбрать **Алгоритм аутентификации**, который будет использоваться протоколом AH.

5) Выбрать: будет ли использоваться протокол IPComp (**Применить IPComp протокол**). Если Вы поставите отметку в соответствующем поле, необходимо будет выбрать **Алгоритм сжатия**, который будет использоваться протоколом IPComp.

6) Установить в поле *Время жизни SA* **Предельное время (сек)**.

7) Установить максимальное значение **Предельный трафик (Кбайт)**.

8) К действию будет добавлено новое IPsec-Предложение.

	Для параметров **Предельное время (сек)** и **Предельный трафик (Кбайт)**, значение ноль (0) подразумевает «неограниченно».
	Используйте только те алгоритмы шифрования, которые поддерживаются всеми *Агентами* в данном Правиле, которое применяет **Действие**, в том числе устройствами третьей стороны.
	Не рекомендуется использовать ограничение **Предельный трафик (Кб)**, когда ГПБ включает в себя Правила, распространяющиеся на пользователей.

7.6.3. Редактирование Действий и IPsec-Предложений

Чтобы изменить параметры любого Действия или вложенных в него IPsec-Предложений надо выбрать нужное Действие в дереве *Действий*. Параметры выбранного узла отображаются так же, как и в окне *Добавить действие* и/или *Добавить IPsec-Предложение*. Отредактировать параметры способом, описанным выше.

7.6.4. Удаление Объектов действий

Чтобы удалить Действие из списка в окне *Действий* надо выбрать этот нужное и использовать команду **Удалить из контекстного меню или Главного меню**. *ЦУП* проверит, участвует ли Действие, которое Вы собираетесь удалить в Правилах ГПБ. Если оно участвует - удалить его не удастся. Нельзя удалять Действия, которые находятся в списке участников Правил; перед удалением их необходимо исключить из всех Правил. В этом случае необходимо вернуться в главное окно и удалить данное Действие из всех Правил, в которых оно участвует; затем вернуться в окно *Действия правил* и удалить само Действие.

7.7. Сетевые сервисы

Объекты сетевых сервисов представляют протоколы сетевого обслуживания (или их группы), которые могут быть использованы, чтобы устанавливать, какие типы трафика будут обрабатываться данным Правилом (по умолчанию, Правила применяются ко всем типам IP-пакетов). Протоколы TCP, UDP и ICMP, группы этих протоколов, а также протоколы AH и ESP заранее установлены в *ЦУП*.

Можно указать номер порта для протоколов TCP/UDP. Можно также указать пользовательские IP-инкапсулированные протоколы, предоставив им соответствующие номера протоколов.

Объекты сетевых сервисов создаются и редактируются в окне *Сетевые Сервисы*. Чтобы перейти в это окно надо выбрать *Сетевые Сервисы* в меню *Окно*.

Когда Вам нужно указать диапазон номеров портов надо использовать две точки (..) между самым нижним и верхним номером порта в диапазоне. Также используйте звездочку (*), чтобы установить значение «любой» порт.

7.7.1. Иконки сетевых сервисов

Существует графическое представление сетевых сервисов (см. Таблица 30). Список предопределенных сетевых сервисов можно найти в приложении (см. ПРИЛОЖЕНИЕ 5. СЕТЕВЫЕ СЕРВИСЫ И ГРУППЫ СЕТЕВЫХ СЕРВИСОВ ПО УМОЛЧАНИЮ).

Таблица 30 – Графическое представление сетевых сервисов

Иконка	Описание	Иконка	Описание
	Все сервисы IP		Группа сетевых сервисов
	Сервисы ICMP		Сервисы TCP
	Сервисы UDP		

7.7.2. Создание сетевых сервисов TCP

Создание сетевых сервисов TCP происходит следующим образом:

1) Использовать команду **Добавить -> Сетевой Сервис** из меню *Править*. В выпадающем меню *Тип* выбрать **TCP**.
2) Ввести уникальное **Имя** для данного сетевого сервиса.
3) При необходимости ввести текстовое **Описание**.
4) Ввести один или несколько номеров портов, которые будут использоваться данными сервисами на компьютере-приемнике (сервере) **Порт(ы)**. Чтобы ввести диапазон номеров портов надо использовать форму <**нижний порт**>...<**верхний порт**> (например, **123...456**).
5) Ввести номер порта, который будет использоваться протоколом TCP на компьютере-источнике (клиенте) **Порт(ы) источника**. В большинстве случаев значение порта неизвестно, и в этом случае надо указать значение в виде звездочки (*). Чтобы ввести диапазон номеров портов надо использовать форму <**нижний порт**>..<**верхний порт**> (например, **123...456**).

6) Если Вы не хотите, чтобы компьютер, использующий данный сетевой сервис, принимал входящие TCP-соединения, надо выбрать кнопку **Отвергать входящие TCP соединения** во вкладке *Контроль трафика*. В противном случае надо установить кнопку **FW Процедура** и выбрать из выпадающего меню процедуру МЭ, которая будет применяться к данному сетевой сервису (можно выбрать значение **None**). Подробнее см. п. 7.7.7.

7.7.3. Создание Объектов сетевых сервисов UDP

Создание Объектов сетевых сервисов UDP происходит следующим образом:

1) Использовать команду **Добавить -> Сетевой Сервис** из меню *Править*. В выпадающем меню *Тип* выбрать **UDP.**

2) Ввести уникальное **Имя** для данного Объекта сетевого сервиса.

3) При необходимости ввести текстовое **Описание** Объекта.

4) Ввести один или несколько номеров портов, которые будут использоваться данными сервисами на компьютере-приемнике (сервере) **Порт(ы)**. Чтобы ввести диапазон номеров портов надо использовать форму <**нижний порт**>..<**верхний порт**> (например, **123...456**).

5) Ввести номер порта, который будет использоваться протоколом UDP на компьютере-источнике (клиенте) **Порт(ы) источника**. В большинстве случаев значение порта неизвестно и в этом случае надо указать значение в виде звездочки (*). Чтобы ввести диапазон номеров портов надо использовать форму <**нижний порт**>..<**верхний порт**> (например, **123...456**).

6) Выбрать из выпадающего списка процедуру МЭ **FW процедура**, которую Вы хотите применить к данному сетевому сервису. Подробнее см. п. 7.7.7.

7) Если Вы хотите, чтобы компьютер-источник (клиент) мог принимать ответы от компьютера-приемника (сервера), надо поставить отметку в поле **Принимать ответ**.

8) Если Вы хотите, чтобы компьютер-источник (клиент) мог принимать ответы от компьютера-приемника (сервера), вне зависимости от того, какой порт предназначен для того, чтобы принимать ответы, надо поставить отметку в поле **Принимать ответы с любого порта.**

7.7.4. Создание Объектов сетевых сервисов ICMP

Создание Объектов сетевых сервисов ICMP происходит следующим образом:

1) Использовать команду **Добавить -> Сетевой Сервис** из меню *Править*. В выпадающем меню *Тип* выбрать **ICMP**.
2) Ввести уникальное **Имя** для данного Объекта сетевого сервиса.
3) При необходимости ввести текстовое **Описание** Объекта.
4) Ввести **Тип** сообщения в заголовок ICMP. (подробнее о типах и кодах ICMP см. ПРИЛОЖЕНИЕ 7. ICMP-КОДЫ). Чтобы установить сообщения всех типов надо использовать звездочку (*).
5) Ввести **Код** сообщения. Чтобы установить все коды сообщений надо использовать звездочку (*).
6) Выбрать из выпадающего списка процедуру МЭ **FW Процедуры**, которую Вы хотите, чтобы применял данный сетевой сервис. Подробнее см. п. 7.7.7.

7.7.5. Создание групп сетевых сервисов

Создание групп сетевых сервисов происходит следующим образом:

1) Использовать команду **Добавить -> Сетевой Сервис** из меню *Править*. В выпадающем меню *Тип* выбрать **Группа.**
2) Ввести уникальное **Имя** для данной группы сетевых сервисов.
3) При необходимости ввести текстовое **Описание** Объекта.
4) Наполнить группу сетевыми сервисами. Для этого надо в поле **Элементы** переместить их из списка *Доступные Сервисы* в список *Выбранные Сервисы*.

7.7.6. Редактирование сетевых сервисов

Чтобы изменить параметры любого сетевого сервиса или Группы сервисов надо выбрать их в списке в Окне Сетевых Сервисов, которое по умолчанию располагается под Секцией Топологии. Двойное нажатие мышью ли команда **Изменить** из главного или контекстного меню откроет окно *Изменить Сетевой Сервис*, параметры которого идентичны окну *Добавить Сетевой Сервис*. Отредактировать параметры способом, описанным выше.

Порядок, в котором сетевые сервисы отображаются в окне, может быть изменен. По умолчанию, Объекты отсортированы в алфавитном порядке (по имени). Чтобы отсортировать Сервисы по необходимому параметру нужно нажать на соответствующий параметр вверху таблицы Сетевых Сервисов.

В контекстном меню окна *Сетевые Сервисы* существует команда **Найти правило**, которая позволяет выделять те Правила, в которых упоминается данный Сетевой Сервис.

7.7.7. Процедуры межсетевых экранов

Процедуры МЭ – это расширенные Правила фильтрации пакетов, применяемые *Агентами*. Процедуры МЭ отслеживают потоки сеансов соединений и пропускают только те IP-пакеты, которые соответствуют текущему статусу соединения. Для некоторых протоколов (например, FTP), назначаются динамические номера портов для вторичных соединений. В таких случаях невозможно использовать обычную фильтрацию пакетов и поэтому могут быть использованы только процедуры МЭ. Процедуры МЭ назначаются, как параметры Объектов сетевых сервисов.

По умолчанию, *ЦУП* содержит набор процедур МЭ, которые фильтруют трафик, используя несколько типов протоколов. Список этих протоколов приведен в таблице (см. Таблица 31). Можно выбрать одно из двух значений: **None** или **Auto** в **FW процедуре** в поле **Контроль трафика**. **None** означает, что данный сетевой сервис не будет использовать никаких процедур МЭ. Значение **Auto** подразумевает, что *ЦУП* автоматически включит процедуры, являющиеся стандартными для указанного протокола (только для TCP или UDP). Эта процедура МЭ будет принимать параметры напрямую из сетевых сервисов.

Таблица 31 – Процедуры МЭ

FW процедура	FW процедура	FW процедура
CUSEEME	LPD	RLOGIN
FTP*	NETSHOWTCP	RPC
H.323	NETSHOWUDP	RSH
H.323_RAS	PNA	RTSP
HTTP_STRICT	RCMD	VDOLIVE
Примечание. * - Для FTP-процедуры МЭ (в оттранслированной ЛПБ она называется "generic_ftp") есть специальный параметр flags, который определяет, какие режимы протокола FTP разрешаются (активный, пассивный или оба). По умолчанию у этого флага значение 3 (активный + пассивный режимы), однако, можно в тексте ЛПБ вручную их изменить на 1 (только активный режим) или 2 (только пассивный режим).		

Если ЛПБ содержит процедуру МЭ, которой нет на компьютере *Агента*, в файле регистрации событий *Агента* появится сообщение об ошибке и ЛПБ не будет загружена.

7.7.7.1. Файлы источников процедур МЭ

Каждой процедуре МЭ в *ЦУП* предписано «типовое» имя. При трансляции ЛПБ эти имена заменяются на «реальные», выбранные из файла источника. Эти файлы находятся в

инсталляционной директории *ЦУП* и имеют расширение FWT. Каждый файл источника уникален для каждого типа *Агента* (см. Таблица 32). Таким образом, процедуры МЭ могут быть транслированы на различные типы *Агентов* под одним типовым именем. Для того, чтобы обеспечить Правильность трансляции процедуры в соответствующем файле источнике должна содержаться запись о типовом имени процедуры.

Таблица 32 – Файлы источников процедур МЭ

Имя файла	**Типа *Агента***
`tws-fw.fwt`	*Trusted Agent* (*Агент*) (любая версия)

Также можно устанавливать типовые процедуры МЭ. Когда транслятор встречается с процедурой МЭ, не имеющей «типового» имени, сначала он проверяет описание процедуры МЭ в файле источнике для данного типа *Агента*. Если такой процедуры в файле нет, она будет проигнорирована.

Все нестандартные процедуры МЭ должны быть зарегистрированы в соответствующих файлах FWT для их правильного использования.

7.8. Определяемые пользователем ЛПБ

Объект определяемой пользователем ЛПБ – это часть ЛПБ (фрагмент ЛПБ) в текстовом формате. Такие фрагменты ЛПБ добавляются к ЛПБ и модифицируют ЛПБ, автоматически транслируемую из ГПБ, и могут быть созданы вручную. Когда Объекты определяемых пользователем ЛПБ включают в ЛПБ Объекта Политики, эти фрагменты помещаются либо в начало, либо в конец ЛПБ, автоматически сгенерированной при трансляции из ГПБ.

У Объектов Политики есть атрибут *Автоматически Созданная ЛПБ*, который представляет ЛПБ, автоматически оттранслированную из ГПБ. Определяемые пользователем Объекты ЛПБ могут быть добавлены к этому параметру на вложенной закладке *ЛПБ* закладки *Управление*, которая находится в окне *Свойства*, либо над атрибутом *Автоматически Созданная ЛПБ,* либо под ним. После трансляции ГПБ и создания ЛПБ для данного Объекта Политики, все фрагменты ЛПБ, представляемые Объектами определяемых пользователем ЛПБ будут добавлены к ЛПБ в порядке сверху вниз. Если в дереве определяемая пользователем ЛПБ находится выше атрибута *Автоматически Созданная ЛПБ,* ее фрагмент будет помещен в начало ЛПБ, если она располагается ниже, то фрагмент ЛПБ будет помещен в конец ЛПБ.

Определяемые пользователем ЛПБ создаются и редактируются в окне *Пользовательские ЛПБ*. Чтобы перейти в это окно надо выбрать *Пользовательские ЛПБ* в меню *Окно*.

7.8.1. Создание и редактирование Объектов определяемой пользователем ЛПБ

Чтобы создать Объект определяемой пользователем ЛПБ надо:

1) Воспользоваться командой **Добавить Пользовательскую ЛПБ** из меню *Править* или контекстного меню в окне Пользовательских ЛПБ.
2) Ввести новое имя **Пользовательской ЛПБ** для данного Объекта определяемой пользователем ЛПБ.
3) Перейти во вкладку *Текст ЛПБ*. Это окно представляет собой стандартный текстовый редактор. На данном этапе у Вас есть несколько вариантов:
   - Напечатать текст определяемой пользователем ЛПБ прямо с клавиатуры;
   - Скопировать текст из другой программы в это окно;
   - Выбрать **Править**, затем **Открыть** в меню *Файл* и импортировать фрагмент определяемой пользователем ЛПБ из файла.
4) После того, как Вы закончите, надо выбрать команду **Сохранить** в меню *Файл* и сохранить пользовательскую ЛПБ в виде текстового файла.

Чтобы отредактировать Объект определяемой пользователем ЛПБ надо выбрать его в списке, используя в контекстном меню команду **Изменить.**

7.9. Серверы

Окно *Серверы*, вызываемое из меню *Окно->Серверы* позволяет создавать и редактировать вспомогательные Объекты (серверы, службы), которые не являются в чистом виде Объектами Политики Безопасности, но, тем не менее, выполняют разнообразные важные функции, необходимые для работы защищенной сети. Все серверы разделены по разделам, представляющим собой вкладки (см. Таблица 33). В дальнейшем в данном подразделе будем называть такие вспомогательные Объекты Серверами.

Таблица 33 – Типы Серверов

Тип Сервера	Назначение объектов, содержащихся в папке
Microsoft Agent Policy Distribution Service*	Описания сервисов-прогрузчиков, которые используются для доставки и активации ЛПБ на Объекты с IPsec-*Агентами* Microsoft.
PMP Distribution Service*	Описания сервисов-прогрузчиков, которые используются для доставки и активации ЛПБ на Объекты с *Агентами* через протокол PMP.
SSH Protocol Policy Distribution Service*	Описания сервисов-прогрузчиков, которые используются для доставки и активации ЛПБ на Объекты с *Агентами* Cisco.
Telnet Protocol Policy Distribution Service*	Описания сервисов-прогрузчиков, которые используются для доставки и активации ЛПБ на Объекты с *Агентами* Cisco.
Web Management Service*	Описания сервисов-прогрузчиков, которые используются для доставки начальной конфигурации *Агентам*.
FTP Proxy Server	Описания proxy-серверов для протокола FTP, которые могут быть установлены на Объектах с *Агентами*

Тип Сервера	Назначение объектов, содержащихся в папке
HTTP Proxy Server	То же, но для протокола HTTP
SMTP Proxy Server	То же, но для протокола *SMTP*
SOCKS Proxy Server	То же, но для протокола SOCKS
LDAP Server	Описания LDAP-серверов, присутствующих в сети и содержащих каталоги с сертификатами/СОС. *Агенты* могут использовать эти серверы, чтобы получить требуемые сертификаты\СОС.
RADIUS Server*	Описания присутствующих в сети RADIUS-серверов, которые могут быть использованы для дополнительной аутентификации ВЧС-клиентов по протоколу XAUTH. Данный протокол поддерживается некоторыми типами ВЧС-Шлюзов и конфигурируется в их свойствах в закладке ВЧС->XAUTH Server.
SNMP-Server*	Описания присутствующих в сети SNMP-серверов, которые могут делать SNMP-запросы к Объектам Политики, а также принимать от этих Объектов Политики SNMP-трапы (т.е. сообщения о происходящих на Объекте событиях).
Syslog Server*	Описания присутствующих в сети Syslog-серверов, которые могут использоваться для сбора информации с управляемых *Агентов* по протоколу Syslog.
TACACS Server	Описания присутствующих в сети TACACS-серверов, которые (аналогично RADIUS-серверам) могут быть использованы для дополнительной аутентификации ВЧС-клиентов по протоколу XAUTH. Данный протокол поддерживается некоторыми типами ВЧС-Шлюзов и конфигурируется в их свойствах в закладке *ВЧС->XAUTH Server*.
TFTP Server*	Описания TFTP-серверов, которые используются для доставки ЛПБ на Объекты с *Агентами* Cisco IOS (и которые можно указывать для этих Объектов как Удаленные Серверы). Данный метод прогрузки используется в паре с протоколом Telnet.
Update Server	Описания веб-серверов, которые используются *Агентами* для проверки и скачивания автоматических обновлений.
Примечание. * Эти Серверы генерируются автоматически при создании БД *ЦУП* и представляют реальные сервисы или приложения, работающие на хосте *ЦУП-Сервер*. **Если во время установки *ЦУП* Вы зарегистрировали сертификаты для *ЗАСТАВА-Офис,* который защищает *ЦУП-Сервер*, то Объект СА, представляющий издателя локального сертификата *ЦУП*, будет создан автоматически.	

Большинство Серверов располагаются на реальных хостах в сетевой топологии (например, серверы управления, серверы аутентификации, сервисы-прогрузчики и т.п.), но есть и виртуальные сущности (например, Объекты СА, представляющие собой УЦ), которые напрямую не связаны с хостами в сети.

Для удобства пользователя многие Серверы создаются автоматически при создании БД *ЦУП* - обычно это приложения (системные сервисы), которые входят в состав *ЦУП* и взаимодействуют с внешними хостами.

Цель описания Серверов - дать возможность «привязывать» их к Объектам Политики Безопасности в роли «удаленных серверов», как описано в п. 7.1.1.2. Кроме того, некоторые

Серверы являются конфигурируемыми объектами и имеют свою собственную ЛПБ, которая создается транслятором *ЦУП* и передается на Серверы при активации ГПБ.

7.9.1. Общие принципы создания Объектов в окне *Серверы*

Ниже описаны основные параметры Серверов на примере **PMP Distribution Server** (см. Рисунок 75). Этот сервер представляет собой сервис-прогрузчик для *Агентов*, который передает ЛПБ на управляемые *Агенты* по протоколу PMP (Policy Management Protocol).

В таблице (см. Таблица 34) перечислены параметры, наиболее часто встречающиеся для всех типов Серверов.

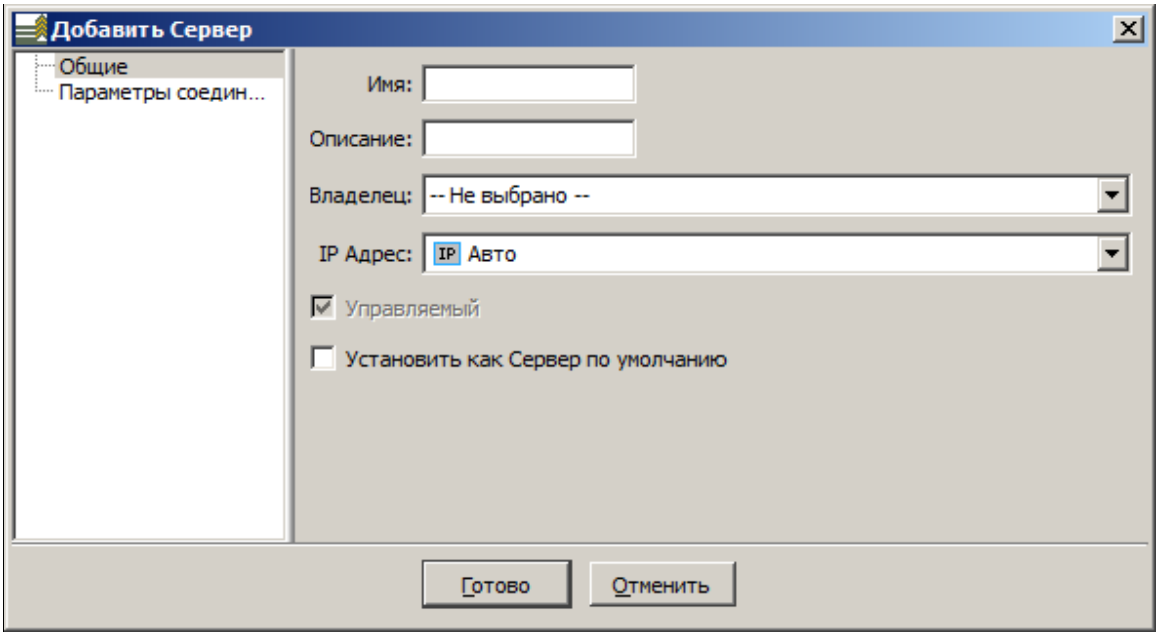

Рисунок 75 – Параметры PMP Distribution Service

Таблица 34 – Общие параметры серверов

Параметр	Значение
Имя	Название Сервера (произвольное). Данное название используется внутри *ЦУП* для идентификации этого Объекта.
Описание	Произвольный комментарий.
Владелец	Для большинства Серверов данный параметр обозначает хост в сети, на котором установлен описываемый сервер/сервис. Владелец выбирается через выпадающий список, который обычно содержит все существующие Объекты Политики. В некоторых случаях этот список сокращается из-за наличия ограничений, накладываемых типом Сервера.
IP-адрес	IP-адрес, который используется для работы с данным Сервером. Ввести этот адрес можно следующими способами: 1) выбрать один из интерфейсов хоста; 2) оставить значение Auto (рекомендуется). В последнем случае адрес будет вычисляться автоматически на основании информации о топологии сети (с учетом NAT-Правил, взаимного расположения Объектов и т.п.).

Параметр	Значение
Управляемый	Для управляемых Серверов этот флажок влияет на то, будет ли этот Сервер получать Политику Безопасности от данного экземпляра *ЦУП*. В большинстве случаев флажок должен быть установлен. Для неуправляемых Серверов этот флажок заблокирован.
Установить как Сервер по умолчанию	Если флажок установлен, то для вновь создаваемых Объектов Политики данный Сервер будет автоматически привязываться как удаленный Сервер.

Статус прогрузки управляемых серверов можно отслеживать в окне *Монитор*.

Как уже упоминалось выше, одна из целей привязки Серверов к Объектам Политики - создание технологических Правил для пропускания соответствующего трафика по защищаемой сети. Более подробная информация приведена в п. 7.1.1.2.

В таблице (см. Таблица 35) приведены основные параметры, которые используются для автоматического создания технологических Правил. Данные параметры присутствуют в свойствах большинства Серверов.

Таблица 35 – Параметры для автоматического создания технологических Правил

Параметр	Значение
Метод подключения	Протокол (или метод), который используется для связи между Сервером и Объектами Политики, к которым он привязан. В большинстве случаев в списке выбора доступен всего один протокол.
Сетевой сервис	Тип трафика, который будет указан в автоматически создаваемых технологических Правилах. Обычно значение данного параметра определяется протоколом связи, указанным в Методе подключения и изменять это значение не требуется.
Действия	Действие, которое будет указано в автоматически создаваемых технологических Правилах. Во многих случаях протокол связи (указанный в Методе подключения) сам по себе является защищенным и дополнительной защиты трафика при помощи IPsec не требуется; в таких ситуациях для данного параметра можно оставить значение по умолчанию (Pass).
Уровень протоколирования	Параметр, который задает уровень протоколирования событий.

Перед созданием Сервера в окне *Servers*, Вы должны создать Объект Политики, на котором будет установлен Сервер в секции *Топология* или секции *Объекты Политики*. Это не требуется только для тех Серверов, которые не связаны с хостами сети (например, серверы CA (Certificate Authority)).

7.9.2. Серверы-Прогрузчики

7.9.2.1. Объекты Microsoft Agent Policy Distribution Service

Для просмотра объектов Microsoft Agent Policy Distribution Service необходимо ввести команду **Окно->Серверы** выбрать соответствующий тип (см. Рисунок 76).

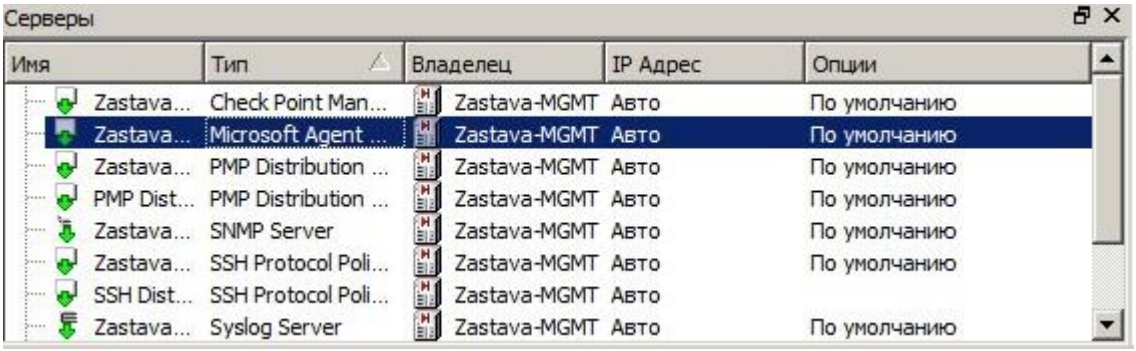

Рисунок 76 – Тип Microsoft Agent Policy Distribution Service

7.9.2.1.1. Основные сведения

Тип **Microsoft Agent Policy Distribution Service** содержит описания серверов-прогрузчиков, которые используются для доставки и активации ЛПБ на Объекты с IPsec-*Агентами* Microsoft (и которые можно указывать для этих Объектов как **Удаленные Серверы**).

В большинстве случаев в роли сервиса прогрузки выступает данный экземпляр *ЦУП* (а именно, сервер **TPNDistributor**); соответствующий Объект автоматически генерируется при создании БД и единственный параметр, который требуется указать - идентификатор сертификата.

7.9.2.1.2. Дополнительные сведения

Описание параметров:

Параметры, специфичные для **Microsoft Agent Policy Distribution Service**:

- **Метод подключения** - Протокол для связи между данным прогрузчиком и управляемыми Объектами. Единственное возможное значение - **SSL**.
- **Сетевой сервис** - Необходимый Сетевой Сервис.
- **Действие** – Выбор Действия: **Pass, Drop** или **Encrypt**.
- **Сертификат** - Идентификатор сертификата (в формате Distinguished Name), который будет использоваться для установления защищенных SSL-соединений при прогрузке управляемых Объектов. Данный сертификат должен быть зарегистрирован в стандартном хранилище сертификатов в ОС хоста, на котором установлен *ЦУП*.

7.9.2.2. Объекты PMP Distribution Service

Для просмотра объектов PMP Distribution Service необходимо ввести команду **Окно->Серверы** выбрать соответствующий тип (см. Рисунок 77).

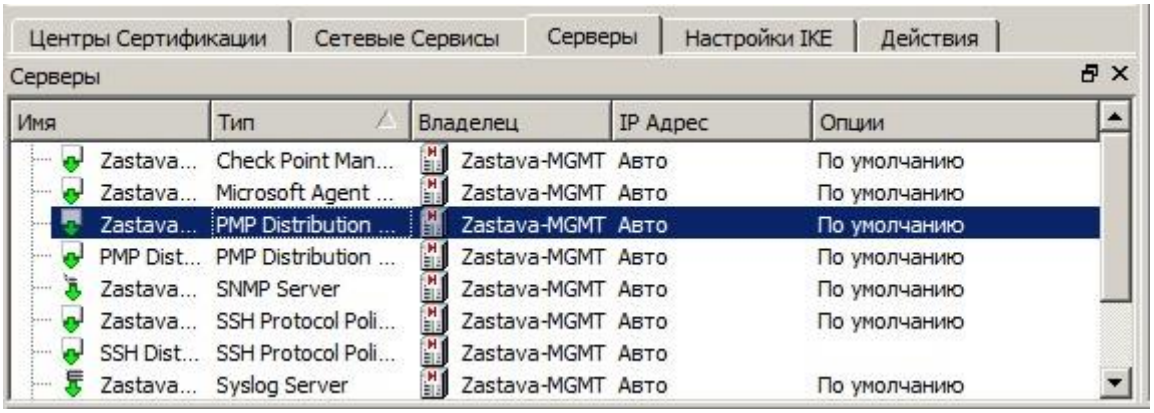

Рисунок 77 – Объекты PMP Distribution Service

7.9.2.2.1. Основные сведения

Тип **PMP Distribution Service** содержит описания сервисов-прогрузчиков, которые используются для доставки и активации ЛПБ на Объекты с *Агентами* (и которые можно указывать для этих Объектов как **Удаленные Серверы**).

Любой объект, с установленным *Агентом,* может быть использован как сервер-прогрузчик. В большинстве случаев в роли сервиса прогрузки выступает данный экземпляр *ЦУП* (а именно, сервер **TPNDistributor**); соответствующий Объект автоматически генерируется при создании БД.

Использование удаленных серверов-прогрузчиков позволяет разгрузить основной сервер-прогрузчик при большом количестве прогружаемых объектов.

7.9.2.2.2. Дополнительные сведения

Описание параметров:

Параметры, специфичные для **PMP Distribution Service**:

– **Владелец -** В качестве владельца должен использоваться хост в сети, на котором установлен описываемый сервис.

– **Метод подключения** - Протокол для связи между данным прогрузчиком и управляемыми Объектами. Единственное возможное значение – **PMPv2** (Policy Management Protocolv2).

– **Сетевой сервис -** В данном случае указано два протокола - IKE и IKE-NAT-Traversal.

– **Уровень протоколирования -** Задает уровень протоколирования событий. Возможны следующие значения, в порядке возрастания количества потенциальных протоколируемых сообщений:

- Заблокирован;
- События;

- Детальный;
- Отладочный;
- Из настроек IKE*.

Примечание. Уровень **Из настроек IKE** эквивалентен случаю, когда **Уровень протоколирования** будет взят из соответствующих настроек IKE Proposal.

Основные моменты при создании сервера-прогрузчика:

– Чтобы сервер-прогрузчик выполнял свои функции необходимо на *Агентах*, которые будут загружать с него Политику, правильно указать удаленный сервер на закладке *Параметры соединения*.
– На хосте, на котором реализован серевер-прогрузчик, в файле worker.properties в параметре worker.policy_worker.host указать адрес сервера *ЦУП*.
– Корректно указать параметры загрузки Политики на *Агентах*, которые будут загружать Политику с сервера-прогрузчика.

7.9.2.3. Объекты SSH Protocol Policy Distribution Service

Для просмотра объектов SSH Protocol Policy Distribution Service необходимо ввести команду **Окно->Серверы** и выбрать соответсвующий тип (см. Рисунок 78).

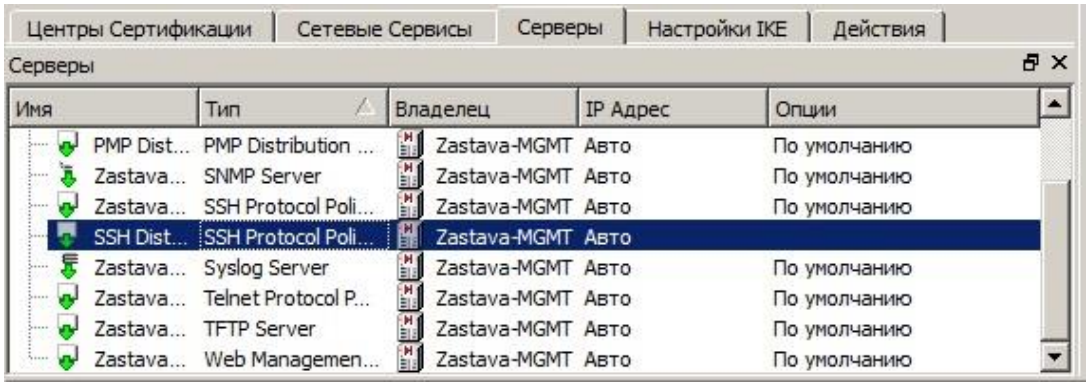

Рисунок 78 – Объекты SSH Protocol Policy Distribution Service

7.9.2.3.1. Основные сведения

Тип **SSH Protocol Policy Distribution Service** содержит описания сервисов-прогрузчиков, которые используются для доставки и активации ЛПБ на Объекты с *Агентами* Cisco (и которые можно указывать для этих Объектов как **Удаленные Серверы**).

В большинстве случаев в роли сервиса прогрузки выступает данный экземпляр *ЦУП* (а именно, сервер **TPNDistributor**); соответствующий Объект автоматически генерируется при создании БД и дополнительного конфигурирования не требуется.

7.9.2.3.2. Дополнительные сведения

Описание параметров:

– **Владелец -** В качестве владельца должен использоваться хост в сети, на котором установлен описываемый сервис;
– **Метод подключения** - Протокол для связи между данным прогрузчиком и управляемыми Объектами. Единственное возможное значение - **SSH**.

7.9.2.4. Объекты Telnet Protocol Policy Distribution Service

Для просмотра объектов Telnet Protocol Policy Distribution Service необходимо ввести команду **Окно->Серверы** и выбрать соответсвующий тип (см. Рисунок 79).

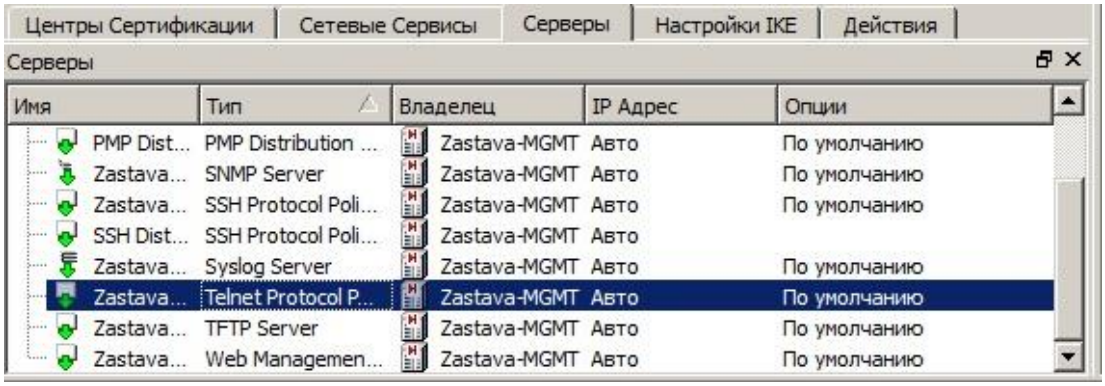

Рисунок 79 – Объекты Telnet Protocol Policy Distribution Service

7.9.2.4.1. Основные сведения

Тип **Telnet Protocol Policy Distribution Service** содержит описания сервисов-прогрузчиков, которые используются для доставки и активации ЛПБ на Объекты с *Агентами* Cisco (и которые можно указывать для этих Объектов как **Удаленные Серверы**).

В большинстве случаев, в роли сервиса прогрузки выступает данный экземпляр *ЦУП* (а именно, сервер **TPNDistributor**); соответствующий Объект автоматически генерируется при создании БД.

Необходимо обратить внимание на защиту Telnet-соединения при помощи IPsec-туннеля (см. описание параметра **Действие** в п. 7.9.2.4.2).

7.9.2.4.2. Дополнительные сведения

Описание параметров:

– **Владелец -** В качестве владельца должен использоваться хост в сети, на котором установлен описываемый сервис.

– **Метод подключения** - Протокол для связи между данным прогрузчиком и управляемыми Объектами. Единственное возможное значение – **Telnet**.
– **Действия** - Поскольку трафик по протоколу Telnet передается в открытом виде, необходимо включить защиту данного соединения при помощи протокола IPsec, т.е. поставить для параметра **Действие** значение **Encrypt**.

7.9.2.5. Объекты Web Management Service

Для просмотра объектов Web Management Service необходимо ввести команду **Окно->Серверы,** выбрать соответствующий тип (см. Рисунок 80).

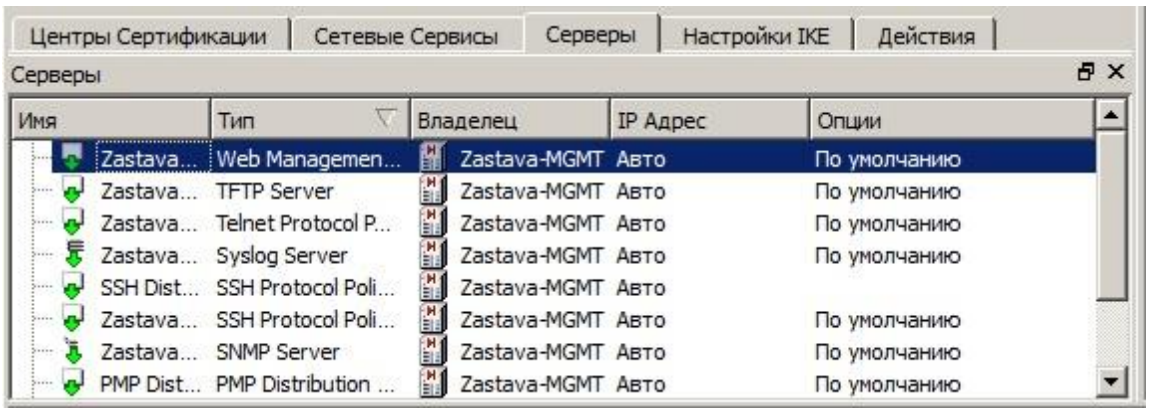

Рисунок 80 – Объекты Web Management Service

7.9.2.5.1. Основные сведения

Тип **Web Management Service** содержит описания сервисов-прогрузчиков, которые используются для доставки начальной конфигурации *Агентам*.

В большинстве случаев в роли сервиса прогрузки выступает данный экземпляр *ЦУП* (а именно, сервер **TPNDistributor**), соответствующий Объект автоматически генерируется при создании БД.

7.9.2.5.2. Дополнительные сведения

Описание параметров:

Параметры, специфичные для **Web Management Service**:

– **Владелец** - В качестве владельца должен использоваться хост в сети, на котором установлен описываемый сервис.
– **Метод подключения** - Протокол для связи между данным прогрузчиком и управляемыми Объектами. Единственное возможное значение – **Secure Hypertext Transfer Protocol**.

- **Сетевой сервис** – в данном случае https, значение можно выбрать из выпадающего списка.
- **Действия -** Поскольку трафик по протоколу **https** передается в закрытом виде, можно убрать защиту по протоколу IPsec, т.е. поставить для параметра **Действие** значение **Pass**. См. также п. 7.9.1.

7.9.3. Прокси-Серверы

Тип прокси-серверов содержит описания proxy-серверов для разных протоколов (HTTP, FTP и т.п.). Эти proxy-серверы входят в состав *ЗАСТАВА-Офис* и, при необходимости, могут использоваться для дополнительной интеллектуальной обработки трафика. Конфигурирование proxy-серверов производится централизованно – через *ЦУП*.

Для конфигурирования определенного proxy-сервера необходимо создать соответствующее описание в нужной папке и указать:

- информацию для *ЦУП* (Объект Политики, на котором установлен proxy-сервер, параметры служебного соединения между *ЦУП* и proxy-сервером: протокол, имя и пароль);
- параметры для конфигурирования самого proxy-сервера (используемый порт, время жизни сессии, аутентификация и т.п.).

7.9.3.1. Общие настройки для proxy-серверов

Тип **Прокси** содержит описания proxy-серверов для разных протоколов (HTTP, FTP и т.п.). Все протоколы имеют как общие параметры (см. Таблица 36), так и дополнительные параметры.

Таблица 36 – Общие настройки для proxy-серверов

Параметр	Значение
Имя	см. п. 7.9.1.
Владелец	см. п. 7.9.1. В качестве владельца должны использоваться только те Объекты Политики, на которых установлены *Агенты*, поддерживающие Proxy.
IP-адрес	см. п. 7.9.1.
Управляемый	см. п. 7.9.1.
Метод прогрузки, **Имя пользователя,** **Пароль пользователя**	Параметры для установления соединений между *ЦУП* и данным proxy-сервером при активации ГПБ. В качестве методов прогрузки можно выбирать **SSH** или **Telnet** (настройка данных методов подключения со стороны proxy-сервера должна быть выполнена штатными средствами ОС).
Время жизни сессии	При отсутствии активности со стороны клиента в течение данного времени текущая сессия с клиентом будет закрыта proxy-сервером (т.е. при

Параметр	Значение
	повторном обращении клиенту придется проходить повторную аутентификацию). Время задается в секундах.
Порт прокси	TCP/UDP-порт, на котором proxy-сервер будет обслуживать поступающие запросы клиентов. Данный параметр будет также использоваться *ЦУП* для создания нужных технологических правил (подробнее см. п. 7.1.1.2).
Система протоколирования (их может быть несколько или не быть вообще)	Proxy-сервер позволяет регистрировать происходящие [на нем] события с использованием следующих методов*: **Операционная система**: сообщения записываются в стандартный журнал протокола ОС компьютера, на котором запущен proxy-сервер (в случае ОС Windows это будет Application Log) **SNMP**: по каждому событию отсылается SNMP-трап на внешний SNMP-сервер **Консоль**: сообщения выводятся в окно консоли, из которой запущен данный proxy-сервер. Данный вариант возможен только при запуске proxy-сервера вручную в «консольном режиме» (с ключом `-d`). Примечание. * - Можно использовать *любую комбинацию* приведенных выше систем протоколирования, включая *отсутствие протоколирования вообще*. Допускается также указание *нескольких одинаковых* систем протоколирования (например, Вы хотите указать несколько SNMP-серверов, на которые нужно отправлять SNMP-трапы). Для добавления/удаления систем протоколирования надо выбрать соответствующие команды (**Добавить, Удалить**) из контекстного меню.
Уровень протоколирования (для конкретной системы протоколирования)	Задает уровень протоколирования событий. Возможны следующие значения, в порядке возрастания количества потенциальных протоколируемых сообщений: **Заблокирован*** **События** **Детальный** **Отладочный** Примечание. * - Уровень **Заблокирован** эквивалентен случаю, когда данная **Система протоколирования** вообще отсутствует в дереве параметров.
Кодировка сообщений (для конкретной системы протоколирования)	Задает кодировку русских букв, которая используется в протоколируемых сообщениях: KOI8-R ASCII (кодировка по умолчанию) **CP1251** (рекомендуется для proxy-серверов под ОС Windows) **CP866** (рекомендуется при запуске proxy-сервера под ОС Windows в консольном режиме)
Адрес SNMP-Сервера (только для системы протоколирования **SNMP**)	IP-адрес SNMP-сервера, на который будут отсылаться SNMP-трапы о протоколируемых событиях.
Пароль SNMP Сервера (только для системы протоколирования **SNMP**)	Community name (имя сообщества), которое будет указано в отсылаемых SNMP-трапах.
Аутентификация	Метод аутентификации клиентов, который будет использоваться proxy-

Параметр	Значение
	сервером. Возможные значения*: **Системная**: средствами ОС компьютера, на котором запущен данный proxy-сервер. Т.е., при обращении клиента к proxy-серверу присланная информация (логин/пароль) будет отправлена на проверку ОС. **Radius**: при помощи внешнего RADIUS-сервера. Т.е. при обращении клиента к proxy-серверу присланная информация (логин/пароль) будет отправлена на проверку RADIUS-серверу. **Локальная**: при помощи текстового файла (на компьютере proxy-сервера), содержащего пары вида «<логин>=<MD5-хеш пароля>».
RADIUS сервер (только для аутентификации **Radius**)	IP-адрес RADIUS-сервера (см. параметр **Аутентификация**).
Секретный ключ (только для аутентификации **Radius**)	Пароль для доступа к RADIUS-серверу (см. параметр **Аутентификация**). Proxy-сервер должен будет предъявлять этот пароль при каждом обращении к RADIUS-серверу.
Порт (только для аутентификации **Radius**)	Номер порта для доступа к RADIUS-серверу (см. параметр **Аутентификация**).
Имя файла (только для аутентификации **Локальная**)	Имя текстового файла с аутентификационной информацией о клиентах proxy-сервера в виде пар «<логин>=<MD5-хеш пароля>» (см. параметр **Аутентификация**). По умолчанию имя файла – "`passwd`". Примечание. MD5-хеш от строки можно вычислить, к примеру, при помощи утилиты `icv_writer`, входящей в состав *Агентов* версий 6.0 и выше.
Закладка *ЛПБ*	Данная закладка содержит локальную Политику Безопасности, оттранслированную для данного proxy-сервера. По функциональности эта закладка аналогична одноименной закладке в свойствах управляемых Объектов (**Управление->ЛПБ**).
Закладка *Удаленный сервер*	В таблице **Удаленные Серверы** при помощи кнопок добавляются и удаляются управляющие серверы (т.е. экземпляры *ЦУП*), с которых будет проводиться конфигурирование данного proxy-сервера. Особенности интерфейса данного окна описаны в п. 7.1.1.2.

7.9.3.2. Объекты FTP Proxy Server

Для просмотра Объектов FTP Proxy Server необходимо ввести команду **Окно->Серверы и** выбрать **соответствующий тип** (см. Рисунок 81).

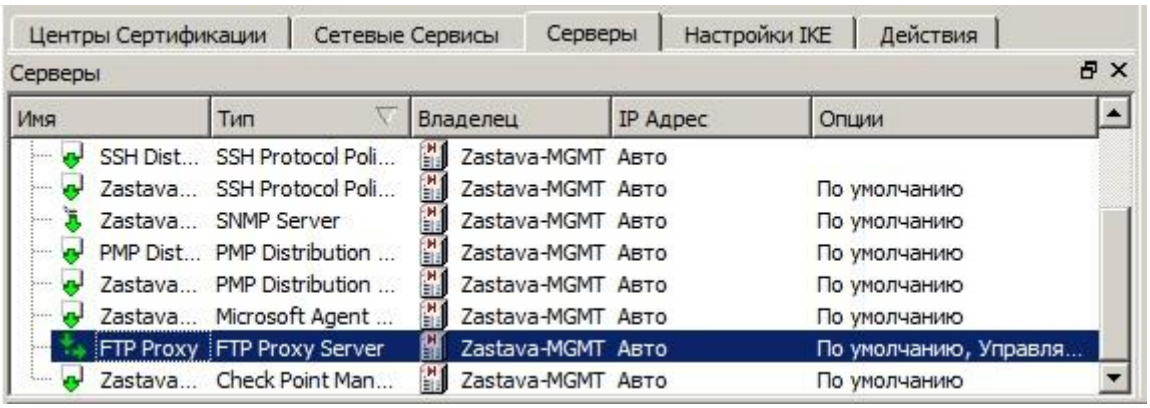

Рисунок 81 – Объекты FTP Proxy Server

7.9.3.2.1. Основные сведения

Тип **FTP Proxy Server** содержит описания proxy-серверов для протокола **FTP**, который является стандартным протоколом передачи файлов в сети Интернет. Ниже перечислены некоторые задачи, которые может выполнять FTP proxy-сервер:

- дополнительная аутентификация пользователей на основании следующих механизмов аутентификации: RADIUS, системная (средствами ОС компьютера), локальная (при помощи файла с хешами паролей);
- фильтрация запросов пользователей на основании IP-адреса или имени FTP-сервера, к которому идет обращение;
- фильтрация путем запрета определенных команд протокола FTP (например, запрет команды **upload**);
- удаление или замена произвольных полей в запросах к FTP-серверам.

7.9.3.2.2. Дополнительные сведения

Описания параметров, общих для всех proxy-серверов, приведены в п. 7.9.3.1.

Параметры, специфичные для FTP proxy-серверов, приведены ниже:

7.9.3.2.2.1. Закладка Ftp, поддерево Авторизация

Поддерево *Авторизация* содержит набор правил для авторизации клиентов proxy-сервера.

В таблице (см. Таблица 37) перечислены имена и значения ключей. Для ключей, допускающих разную множественность, она указана в квадратных скобках. Такие ключи создаются/удаляются при помощи команд **Добавить/Удалить** из контекстного меню.

Таблица 37 – Описание параметров Авторизации

Ключ	Описание
Правило [0..*]	Правило – это контейнер, содержащий фильтры, по которым проводится принятие решения об авторизации клиентов proxy-сервера. При необходимости, в колонке **Значение** можно ввести имя правила.
Имя логина	Логин, для которого будет срабатывать данное правило
Уровень протоколирования	Степень подробности сообщений, записываемых в лог proxy-сервера при срабатывании данного правила
Действие	Возможные значения: **Разрешить** – разрешить клиенту доступ к запрашиваемому ресурсу. **Сбросить** – запретить клиенту доступ и сбросить текущее состояние авторизации для данного клиента. **Отказать** – запретить клиенту доступ к запрашиваемому ресурсу
Фильтр [0..*]	Задает признаки, по которым будет срабатывать данное правило: **Фильтровать по** – поле в запросе клиента, по которому проводить фильтрацию: – **Имя хоста/IP-адрес** – к какому FTP-серверу идет обращение; – **Порт** – по какому порту идет обращение.

Ключ	Описание
	Тип выражения – формат, в котором будет вводиться строка фильтрации (можно использовать простые шаблоны/шаблоны чувствительные регистру или, при необходимости – регулярные выражения/ регулярные выражения чувствительные к регистру). **Выражение** – значение строки фильтрации

7.9.3.2.2.2. Закладка Ftp, поддерево Обработка

Поддерево *Обработка* содержит набор правил для обработки клиентских запросов, проходящих через proxy-сервер (подразумевается, что запрос уже прошел этап авторизации). Под «обработкой» понимается удаление и/или замена определенных полей в запросе.

В таблице (см. Таблица 38) перечислены имена и значения ключей. Для ключей, допускающих разную множественность, она указана в квадратных скобках. Такие ключи создаются/удаляются при помощи команд **Добавить/Удалить** из контекстного меню.

Если параметра **Обработка** нет в дереве, то его необходимо создать, поместив курсор на свободное место и используя команды **Добавить–> Обработка** из контекстного меню.

Таблица 38 – Описание параметров обработки клиентских запросов

Ключ	Описание
Правило удаления [0..*]	Контейнер, содержащий фильтры, по которым будет удаляться информация из запросов клиентов. При необходимости, в колонке **Значение** можно ввести имя правила.
Имя логина [0..1]	Логин, для которого будет срабатывать данное правило
Уровень протоколирования [0..1]	Степень подробности сообщений, записываемых в лог proxy-сервера при срабатывании данного правила
Фильтр [1..*] (для Правила удаления)	Задает элементы («опции») запроса, которые могут быть удалены. **Применить к** – тип удаляемого элемента (единственное значение – **Опции**) **Имя опции** – имя элемента, который может быть удален **Тип выражения** – формат, в котором будет вводиться строка поиска (можно использовать простые шаблоны или, при необходимости – регулярные выражения) **Выражение** – значение строки поиска. Если указанное выражение найдено в указанной опции, то данная опция будет удалена.
Правило замены [0..*]	Контейнер, содержащий фильтры, по которым будет проводиться замена информации в запросах клиентов. При необходимости, в колонке **Значение** можно ввести имя правила. Параметры **Имя логина** и **Уровень протоколирования** аналогичны одноименным параметрам из **Правил удаления**.
Имя логина [0..1]	Логин, для которого будет срабатывать данное правило
Уровень протоколирования [0..1]	Степень подробности сообщений, записываемых в лог proxy-сервера при срабатывании данного правила
Фильтр [1..*] (для Правила	Задает элементы («опции») запроса, в которых может быть проведена замена. **Применить к** – тип анализируемого элемента (единственное значение – **Опции**)

Ключ	Описание
замены)	**Имя опции** – имя элемента, в котором может быть проведена замена **Тип выражения** – формат, в котором будет вводиться строка поиска (можно использовать простые шаблоны или, при необходимости – регулярные выражения) **Из** – значение строки поиска **В** – значение, на которое будет заменен найденный блок текста

7.9.3.3. Объекты HTTP Proxy Server

Для просмотра Объектов HTTP Proxy Server необходимо ввести команду **Окно->Серверы** и выбрать соответствующий тип (см. Рисунок 82).

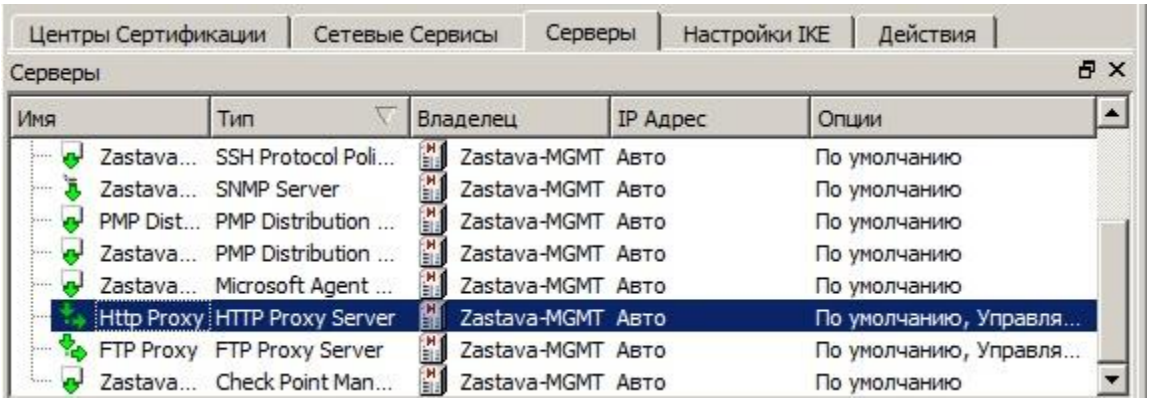

Рисунок 82 – Объекты HTTP Proxy Server

7.9.3.3.1. Основные сведения

Тип **HTTP Proxy Server** содержит описание proxy-серверов для протокола **HTTP**, который является стандартным протоколом передачи гипертекстовой информации в сети Интернет. Ниже перечислены некоторые задачи, которые может выполнять HTTP proxy-сервер:

- дополнительная аутентификация пользователей на основании следующих механизмов аутентификации: RADIUS, системная (средствами ОС компьютера), локальная (при помощи файла с хешами паролей);
- фильтрация запросов пользователей на основании URL, IP-адреса или имени HTTP-сервера, к которому идет обращение;
- удаление или замена произвольных полей в HTTP-пакетах;
- удаление или замена произвольных блоков текста в HTTP-пакетах.

7.9.3.3.2. Дополнительные сведения

Описания параметров, общих для всех proxy-серверов, приведены в п. 7.9.3.1.

Параметры, специфичные для HTTP proxy-серверов, приведены ниже.

7.9.3.3.2.1. Закладка Параметры соединения

Закладка *Параметры соединения* содержит параметр **Кодировка страниц по умолчанию,** определяющий кодировку символов, которые будут использоваться при поиске и фильтрации по тексту в получаемых клиентами HTTP-страницах. Возможные значения: **Windows-1251**, **KOI8-R**, **UTF-8**.

7.9.3.3.2.2. Закладка Http, поддерево Авторизация

Поддерево *Авторизация* содержит набор правил для авторизации клиентов proxy-сервера (см. п. 7.9.3.2.2.1).

Для ключей, допускающих разную множественность, она указана в квадратных скобках. Следует принять во внимание, что ключ **Фильтр** содержит дополнительные признаки, по которым будет срабатывать данное правило: **URL** (адрес ресурса, к которому идет обращение) и **Метод (**поле метода в HTTP-пакете).

Такие ключи создаются/удаляются при помощи команд **Добавить/Удалить** из контекстного меню.

7.9.3.3.2.3. Закладка Http, поддерево Обработка

Поддерево *Обработка* содержит набор правил для обработки клиентских запросов, проходящих через proxy-сервер (подразумевается, что запрос уже прошел этап авторизации). Под «обработкой» понимается удаление и/или замена определенных полей в запросе.

Параметры, специфичные для **HTTP Proxy Server**:

- **Фильтр [1..*]** (для **Правила удаления**) - Задает элементы («опции») запроса, которые могут быть удалены. **Применить к** – тип удаляемого элемента;
- **Опции** – поля в заголовке HTTP-пакета; **Имя опции** – имя элемента, который может быть удален (только для **Опций**);
- **Тип выражения** – формат, в котором будет вводиться строка поиска (можно использовать простые шаблоны или, при необходимости – регулярные выражения);
- **Выражение** – значение строки поиска.

Если указанное выражение найдено в указанном элементе, то блок текста с указанным выражением будет удален.

- **Правило замены [0..*] -** См. п. 7.9.3.2.2.1. Параметры **Имя логина** и **Уровень протоколирования** аналогичны одноименным параметрам из **Правил удаления**.
- **Фильтр [1..*]** (для **Правила замены**) - Задает элементы («опции») запроса, в которых может быть проведена замена.
- **Применить к** – тип анализируемого элемента:

- **Опции** – поля в заголовке HTTP-пакета;
- **Имя опции** – имя элемента, в котором может быть проведена замена (только для **Опций**);

– **Тип выражения** – формат, в котором будет вводиться строка поиска (можно использовать простые шаблоны или, при необходимости – регулярные выражения);

– **Из** – значение строки поиска;

– **В** – значение, на которое будет заменен найденный блок текста.

В некоторых случаях, когда HTTP-сервер посылает информацию в закодированном (упакованном) виде, операции удаления/замены могут не работать. Например, это будет наблюдаться тогда, когда в http-ответе (от сервера) присутствует поле: **/ Content-Encoding: gzip /**.

Эту проблему можно решить, добавив вручную в конфигурацию прокси-сервера (в секцию <process>) следующий фильтр:

```
<replace>
<option from="*" masktype="wild" name="Accept-Encoding" to=""/>
</replace>
```

Данный фильтр удалит опцию Accept-Encoding в http-запросе клиента, поэтому сервер пришлет страницу в незакодированном виде.

7.9.3.4. Объекты SMTP Proxy Server

Для просмотра Объектов SMTP Proxy Server необходимо ввести команду **Окно->Серверы** и выбрать соответствующий тип (см. Рисунок 83).

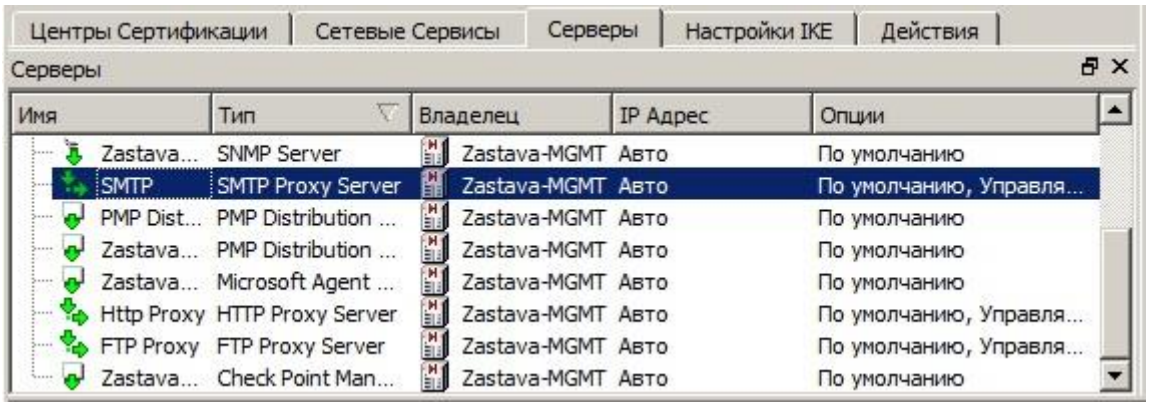

Рисунок 83 – Объекты SMTP Proxy Server

7.9.3.4.1. Основные сведения

Тип **SMTP Proxy Server** содержит описания proxy-серверов для протокола **SMTP**, который является стандартным протоколом передачи электронной почты в сети Интернет. Ниже перечислены некоторые задачи, которые может выполнять SMTP proxy-сервер:

- дополнительная аутентификация пользователей на основании следующих механизмов аутентификации: RADIUS, системная (средствами ОС компьютера), локальная (при помощи файла с хешами паролей);
- удаление или замена произвольных полей в заголовках писем;
- удаление или замена произвольных блоков текста в телах писем.

7.9.3.4.2. Дополнительные сведения

Описания параметров, общих для всех proxy-серверов, приведены в п. 7.9.3.1.

Параметры, специфичные для SMTP proxy-серверов, приведены ниже.

7.9.3.4.2.1. Закладка Smtp, поддерево Авторизация

Поддерево *Авторизация* содержит набор правил для авторизации клиентов proxy-сервера (см. п. 7.9.3.2.2.1).

7.9.3.4.2.2. Закладка Smtp, поддерево Обработка

Поддерево *Обработка* содержит набор правил для обработки клиентских запросов, проходящих через proxy-сервер (подразумевается, что запрос уже прошел этап авторизации) (см. п. 7.9.3.2.2.1). Под «обработкой» понимается удаление и/или замена определенных полей в запросе.

Параметры, специфичные для **SMTP Proxy Server**:

- **Фильтр [1..*]** (для **Правила удаления**) - Задает элементы (**Опции**) запроса, которые могут быть удалены:
- **Применить к** – тип удаляемого элемента:
  - **Опции** – поля в заголовке HTTP-пакета;
  - **Имя опции** – имя элемента, который может быть удален (только для **Опций**);
- **Тип выражения** – формат, в котором будет вводиться строка поиска (можно использовать простые шаблоны или, при необходимости – регулярные выражения);
- **Выражение** – значение строки поиска.

Если указанное выражение найдено в указанном элементе, то данный блок текста будет удален.

- **Правило замены [0..*]** - См. п. 7.9.3.2.2.1. Параметры **Имя логина** и **Уровень протоколирования** аналогичны одноименным параметрам из **Правил удаления**.
- **Фильтр [1..*]** (для **Правила замены**) - Задает элементы (**Опции**) запроса, в которых может быть проведена замена.

– **Применить к** – тип анализируемого элемента:
  – **Опции** – поля в заголовке HTTP-пакета;
  – **Имя опции** – имя элемента, в котором может быть проведена замена (только для **Опций**);
– **Тип выражения** – формат, в котором будет вводиться строка поиска (можно использовать простые шаблоны или, при необходимости – регулярные выражения);
– **Из** – значение строки поиска;
– **В** – значение, на которое будет заменен найденный блок текста.

7.9.3.4.3. Объекты SOCKS Proxy Server

Для просмотра Объектов SOCKS Proxy Server необходимо ввести команду **Окно->Серверы** и выбрать соответствующий тип (см. Рисунок 84).

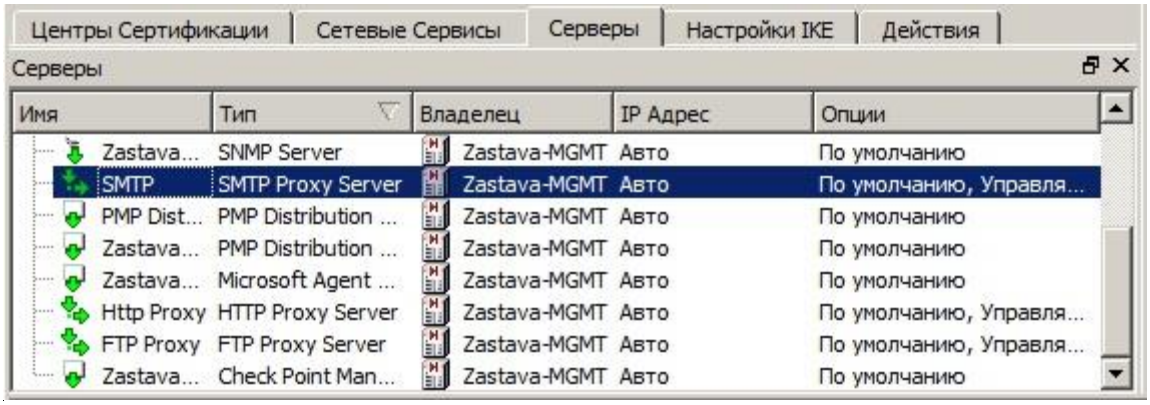

Рисунок 84 – Объекты SOCKS Proxy Server

7.9.3.4.4. Основные сведения

Тип **SOCKS Proxy Server** содержит описания proxy-серверов на основе протокола SOCKS версий 4 и 5. Ниже перечислены некоторые задачи, которые может выполнять SOCKS proxy-сервер:

— дополнительная аутентификация пользователей на основании следующих механизмов аутентификации: RADIUS, системная (средствами ОС компьютера), локальная (при помощи файла с хешами паролей);
— фильтрация запросов пользователей на основании IP-адреса или имени сервера, к которому идет обращение, а также номера порта.

7.9.3.4.5. Дополнительные сведения

Описания параметров, общих для всех proxy-серверов, приведены в п. 7.9.3.1.

Параметры, специфичные для SOCKS proxy-серверов, приведены ниже.

Закладка Socks, поддерево Авторизация

Поддерево *Авторизация* содержит набор правил для авторизации клиентов proxy-сервера (см п. 7.9.3.2.2.1).

Для ключей, допускающих разную множественность, она указана в квадратных скобках. Такие ключи создаются/удаляются при помощи команд **Добавить/Удалить** из контекстного меню.

7.9.4. Прочие Серверы

7.9.4.1. Объекты LDAP Server

Для просмотра Объектов LDAP Server необходимо ввести команду **Окно->Серверы и** выбрать соответствующий тип (см. Рисунок 85).

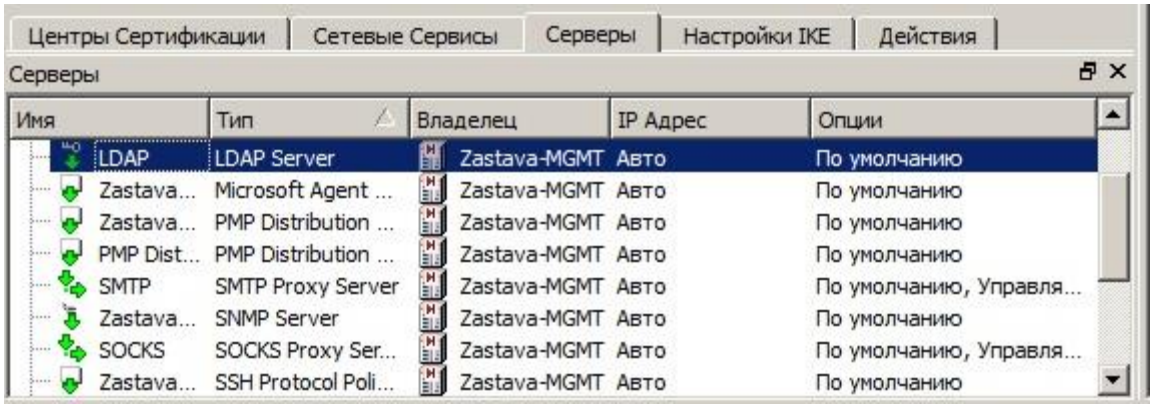

Рисунок 85 – Объекты LDAP Server

7.9.4.1.1. Основные сведения

Тип **LDAP Server** содержит описания LDAP-серверов, присутствующих в сети и содержащих каталоги с сертификатами/СОС. При создании Объекта Политики, представляющего управляемый ВЧС-*Агент*, в его свойствах, в закладке *ВЧС->Сертификаты* можно указать Объект LDAP-сервер как удаленный каталог, куда может обратиться *Агент* для получения сертификата партнера или свежего СОС. Флажок **LDAP autopass (обработка СОС)** всегда в состоянии **Disabled**, поскольку, данная функция поддерживается через привязку LDAP-сервера в закладке *ВЧС-> Сертификаты*.

7.9.4.1.2. Дополнительные сведения

Параметры, общие для **LDAP Server**, приведены в п. 7.8.1.

Параметры, специфичные для **LDAP Server**:

– **Метод подключения** - Разновидность протокола LDAP, который поддерживается данным LDAP-сервером. Возможные значения:

- LDAP;
- Защищенный LDAP.

См. также п. 7.8.1.

- **Пользовательский DN -** Идентификатор пользователя (логин) при обращении к LDAP-каталогу в формате Distinguished Name.
- **Пользовательский пароль -** Пароль доступа к каталогу для идентификатора пользователя, указанного в параметре **Login DN**. Для ввода и подтверждения пароля надо выделить эту ячейку и нажать кнопку, которая появится справа.
- **Ветки, Ветка -** Ветка каталога, с которой будет работать пользователь (в формате Distinguished Name).

7.9.4.2. Объекты RADIUS Server

Для просмотра Объектов RADIUS Server необходимо ввести команду **Окно->Серверы и** выбрать соответствующий тип (см. Рисунок 86).

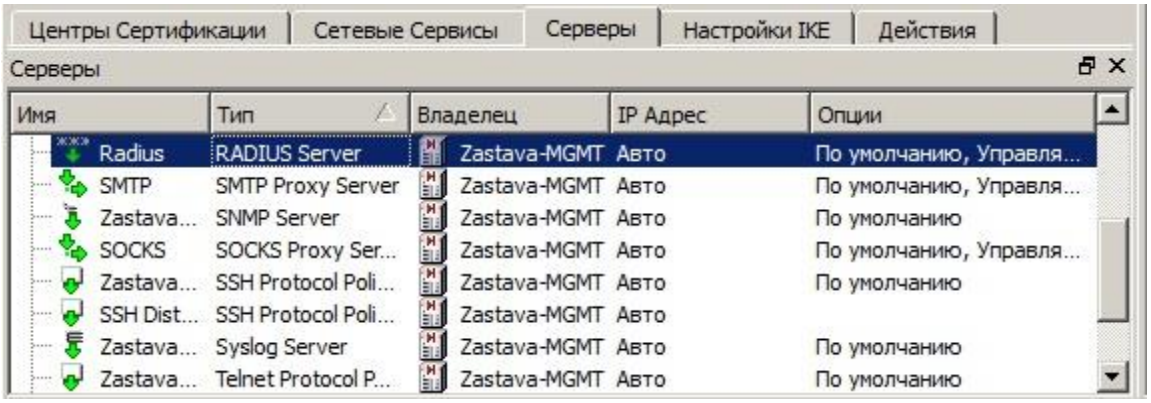

Рисунок 86 – Объекты RADIUS Server

7.9.4.2.1. Основные сведения

Тип **RADIUS Server** содержит описания присутствующих в сети RADIUS-серверов, которые могут быть использованы для дополнительной аутентификации ВЧС-клиентов по протоколу XAUTH. Данный протокол поддерживается некоторыми типами ВЧС-Шлюзов и конфигурируется в их свойствах в закладке *ВЧС->Расширенная аутентификация.*

В состав *ЦУП* входит собственный RADIUS-сервер (представленный сервером **FreeRadius Server**); описывающий его Объект автоматически генерируется при создании БД.

7.9.4.2.2. Дополнительные сведения

Параметры, общие для **RADIUS Server**, приведены в п. 7.8.1.

Параметры, специфичные для **RADIUS Server**:

- **Управляемый** - Данный флажок следует включать только для RADIUS-сервера, входящего в состав *ЦУП*; при описании внешних RADIUS-серверов флажок нужно сбросить, поскольку они не могут конфигурироваться при помощи *ЦУП*. См. также п. 7.8.1.
- **Секретный ключ** - Пароль для доступа к RADIUS-серверу. ВЧС-Шлюз должен будет предъявлять этот пароль при каждом обращении к RADIUS-серверу.
- **Закладка ЛПБ** - Данная закладка содержит ЛПБ, оттранслированную для данного RADIUS-сервера (актуально только для собственного RADIUS-сервера *ЦУП*). По функциональности эта закладка аналогична одноименной закладке в свойствах управляемых Объектов (*Управление->ЛПБ*).

7.9.4.3. Объекты SNMP Server

Для просмотра Объектов PMP Distribution Service необходимо ввести команду **Окно->Серверы** и выбрать соответствующий тип (см. Рисунок 87).

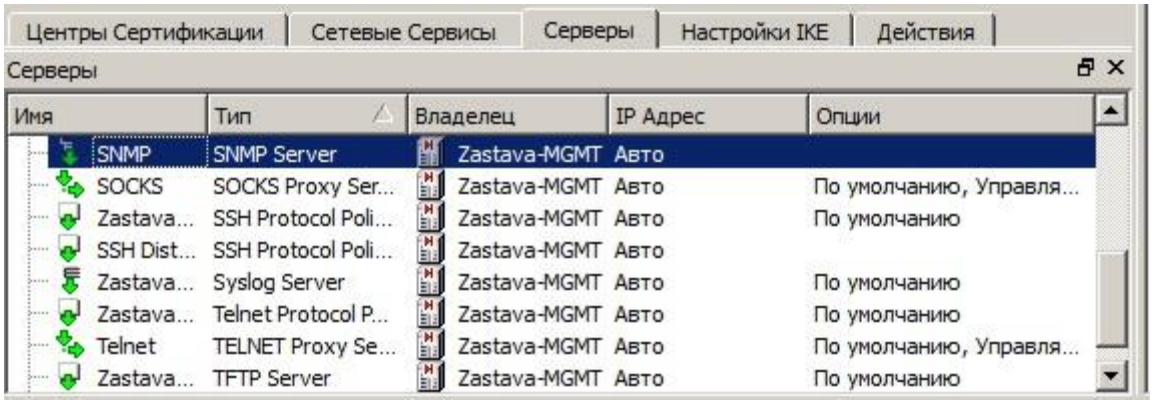

Рисунок 87 – Объект SNMP Server

7.9.4.3.1. Основные сведения

Тип **SNMP Server** содержит описания присутствующих в сети SNMP-серверов, которые могут делать SNMP-запросы к Объектам Политики, а также принимать от этих Объектов Политики SNMP-трапы (т.е. сообщения о происходящих на Объекте событиях).

К каждому Объекту Политики можно привязать один или несколько подобных SNMP-серверов.

В состав *ЦУП* входит собственный SNMP-сервер (представленный сервером **TPNSnmpServer**), описывающий его Объект автоматически генерируется при создании БД.

7.9.4.3.2. Дополнительные сведения

Параметры, общие для **SNMP Server**, приведены в п. 7.8.1.

Параметры, специфичные для **SNMP Server**:

– **Сетевой сервис** - см. п. 7.8.1. В данном случае создаваемое технологическое Правило отвечает только за отправку SNMP-трапов (от *Агентов* к SNMP-серверу), поэтому используется соответствующий Объект Network Service. Что же касается технологических Правил для SNMP-запросов (от SNMP-сервера к *Агентам*), то они настраиваются в свойствах самих *Агентов*, в закладке *SNMP*.
– **Community -** Идентификатор (своеобразный пароль), который можно использовать для выделения хостов, общающихся по SNMP, в отдельную группу. Стандартное значение данного идентификатора - **public**.

7.9.4.4. Объекты Syslog Server

Для просмотра Объектов PMP Distribution Service необходимо ввести команду **Окно->Серверы** и выбрать соответствующий тип (см. Рисунок 88).

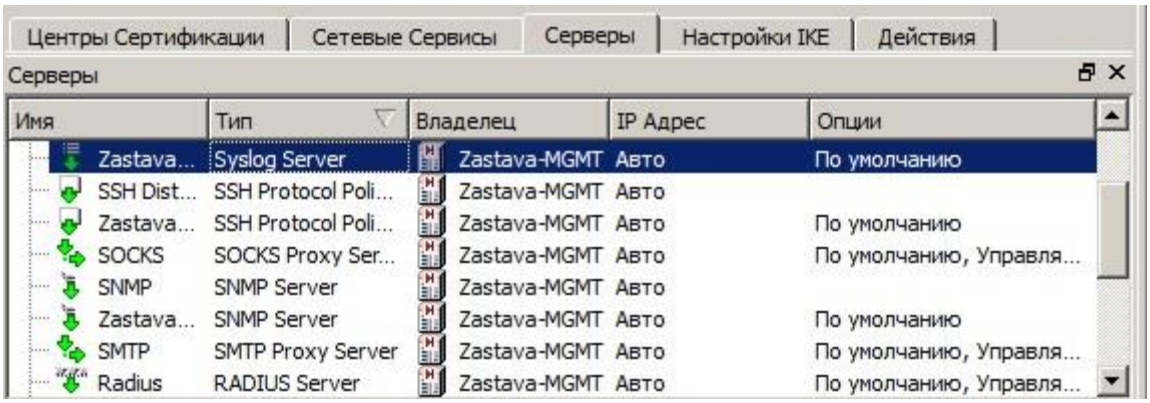

Рисунок 88 – Объекты Syslog Server

7.9.4.4.1. Основные сведения

Тип **Syslog Server** содержит описания присутствующих в сети Syslog-серверов, которые могут использоваться для сбора информации от управляемых *Агентов* по протоколу Syslog.

К каждому Объекту Политики, которые поддерживают этот протокол, можно привязать один или несколько подобных Syslog-серверов (на закладке *SysLog* в свойствах Объекта).

В состав *ЦУП* входит собственный Syslog-сервер (представленный сервером **TPNSyslog**), описывающий его Объект автоматически генерируется при создании БД и дополнительного конфигурирования в большинстве случаев не требуется.

7.9.4.4.2. Дополнительные сведения

Параметры, общие для **Syslog Server**, приведены в п. 7.8.1.

Параметры, специфичные для **Syslog Server**:

– **Уровень протоколирования** - Порог протоколирования событий. Данный параметр имеет смысл только для Syslog-сервера, входящего в состав *ЦУП (*собственный Syslog-сервер представленный сервером **TPNSyslog**).
– **Разрешить протоколирование** - Включение/отключение записи событий в журнал. Данный параметр имеет смысл только для Syslog-сервера, входящего в состав *ЦУП*.

7.9.4.5. Объекты TACACS Server

Для просмотра Объектов PMP Distribution Service необходимо ввести команду **Окно->Серверы** и выбрать соответствующий тип (см. Рисунок 89).

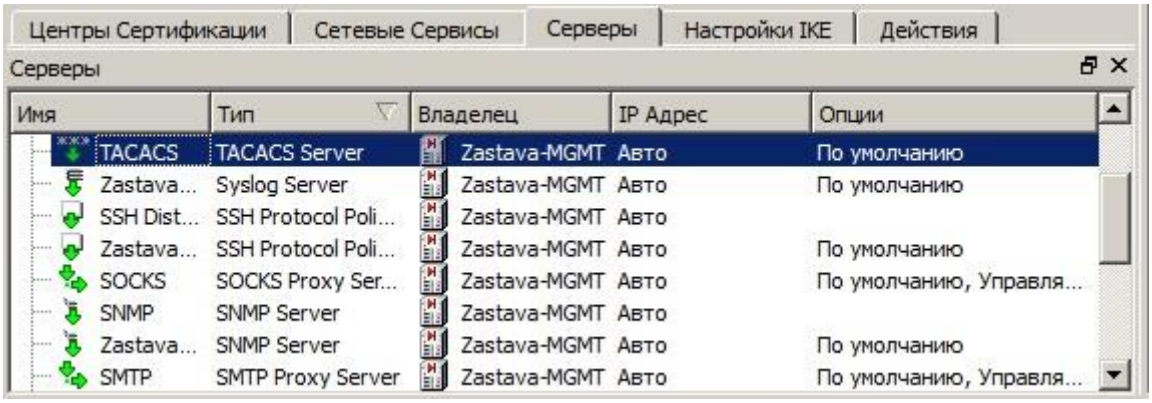

Рисунок 89 – Объекты TACACS Server

7.9.4.5.1. Основные сведения

Тип **TACACS Server** содержит описания присутствующих в сети TACACS-серверов, которые (аналогично RADIUS-серверам) могут быть использованы для дополнительной аутентификации ВЧС-клиентов по протоколу XAUTH. Данный протокол поддерживается некоторыми типами ВЧС-Шлюзов и конфигурируется в их свойствах в закладке *ВЧС->Расширенная аутентификация*.

7.9.4.5.2. Дополнительные сведения

Параметры, общие для **TACACS Server**, приведены в п. 7.8.1.

Параметры, специфичные для **TACACS Server**:

– **Сетевой сервис** - см. п. 7.8.1. При выборе необходимого метода подключения (TACACS/TACACS+) нужные сетевые сервисы выбираются автоматически.
– **Секретный ключ** - Пароль для доступа к TACACS-серверу. ВЧС-Шлюз должен будет предъявлять этот пароль при каждом обращении к TACACS-серверу.

7.9.4.6. Объекты TFTP Server

Для просмотра Объектов TFTP Server необходимо ввести команду **Окно->Серверы** и выбрать соответствующий тип (см. Рисунок 90).

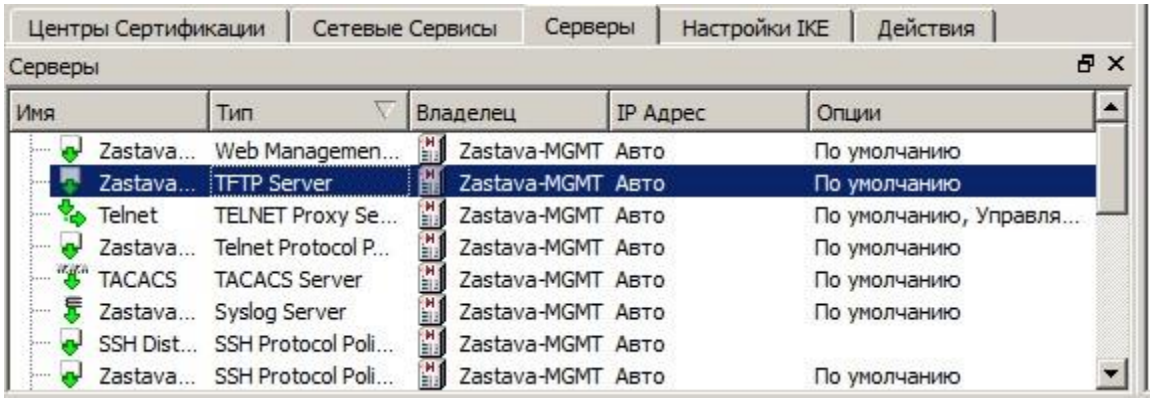

Рисунок 90 – Объекты TFTP Server

7.9.4.6.1. Основные сведения

Папка *TFTP Server* содержит описания TFTP-серверов, которые используются для доставки ЛПБ на Объекты с *Агентами* Cisco IOS (и которые можно указывать для этих Объектов как **Удаленные Серверы**). Данный метод прогрузки используется в паре с протоколом **Telnet**.

В большинстве случаев в роли TFTP-сервера выступает данный экземпляр *ЦУП* (а именно, приложение **Cisco TFTP Server**); соответствующий Объект автоматически генерируется при создании БД.

Необходимо обратить внимание на защиту TFTP-соединения при помощи IPsec-туннеля (см. описание параметра **Действие**, п. 7.9.4.6.2).

7.9.4.6.2. Дополнительные сведения

Параметры, общие для **TFTP Server**, приведены в п. 7.8.1.

Параметры, специфичные для **TFTP Server**:

- **Владелец** - см. п. 7.8.1. В качестве владельца должен использоваться хост в сети, на котором установлен описываемый сервис.
- **Сетевой сервис** - см. п. 7.8.1. При выборе необходимого метода подключения нужные сетевые сервисы выбираются автоматически.
- **Метод подключения** - Протокол для связи между управляемыми Объектами и данным TFTP-сервером. Единственное возможное значение - **TFTP Protocol.** См. п. 7.8.1.
- **Действие** - Поскольку трафик по протоколу TFTP передается в открытом виде, необходимо включить защиту данного соединения при помощи протокола IPsec, т.е. поставить для параметра **Действие** значение **Encrypt**. См. п. 7.8.1.

7.9.4.7. Объекты Update Server

Для просмотра Объектов Update Server необходимо ввести команду **Окно->Серверы** и выбрать соответствующий тип (см. Рисунок 91).

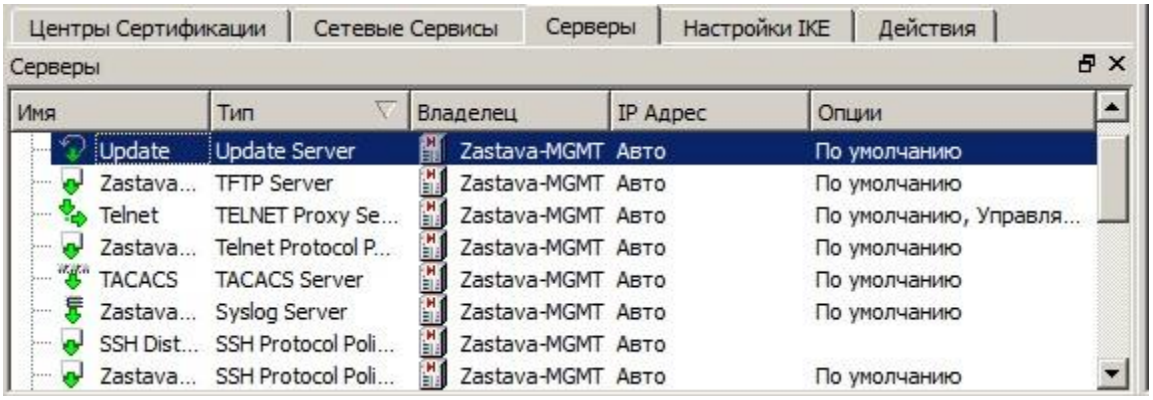

Рисунок 91 – Объекты Update Server

7.9.4.7.1. Основные сведения

Тип **Update Server** содержит описания Update-серверов, присутствующих в сети (или в сети Интернет) и содержащих обновления, которые позволяют скачивать и устанавливать свежие версии продукта.

Если на сервере выложена свежая версия продукта, то будет запущен процесс обновления (скачивание файла обновления, деинсталляция текущей версии и инсталляция новой, с сохранением всей информации о настройках, сертификатах и т.п.).

В зависимости от настроек в ЛПБ *Агента*, процессы скачивания и инсталляции обновлений могут выполняться либо полностью автоматически, либо по команде пользователя. Кроме того, поддерживается инсталляция обновлений по расписанию.

Обращение к серверу обновлений производится по открытому протоколу HTTP.

7.9.4.7.2. Дополнительные сведения

Параметры, общие для **Update Server**, приведены в п. 7.9.1.

Параметры, специфичные для **Update Server**:

– **URL Путь (URL Path) -** веб-адрес **Update** сервера, содержащим обновления, с которым будет периодически связываться *Агент* при проверке обновлений.

7.10. Объекты УЦ (Certificate Authority)

Для просмотра Объектов УЦ необходимо ввести команду **Окно->Центры Сертификации** (см. Рисунок 92).

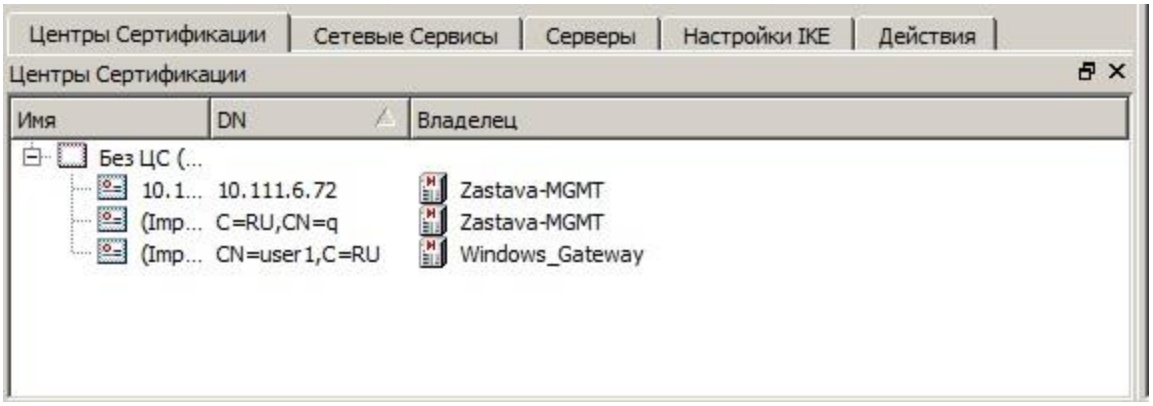

Рисунок 92 – Объекты УЦ

7.10.1. Основные сведения

Окно ЦС *Certificate Authority* содержит описания УЦ, которые издают сертификаты и СОС. По сути, описание УЦ представляет собой описание сертификата УЦ (CA certificate), принадлежащего данному УЦ.

Вводить эту информацию обязательно только в некоторых случаях, например, некоторые *Агенты* (в частности, маршрутизаторы Cisco IOS версий 12.2 и выше) требуют наличия в конфигурации информации о сертификате УЦ, которым подписан сертификат партнера по взаимодействию.

Для создания описания УЦ надо выбрать в контекстном меню пункт **Добавить ЦС** и заполнить все необходимые поля или выбрать в контекстном меню пункт **Импорт**, после чего указать файл с нужным сертификатом.

Возможен также ввод описания УЦ вручную (см. Таблица 39).

Таблица 39 – Описание параметров Certificate Authority

Параметр	Значение
Имя	Название Объекта. При импорте реального сертификата это значение выбирается из его поля **Subject**, из атрибута CN (Common Name).
Подписан	Вышестоящий сертификат УЦ, которым подписан данный сертификат. Если данный сертификат является корневым (Root) сертификатом УЦ, то указывается значение **Self-signed**. При импорте реального сертификата это значение выбирается из его поля **Issuer**.
Владелец (Subject)	Поле **Subject** сертификата (информация о владельце) в формате DN (Distinguished Name). Поскольку это сертификат УЦ, то владельцем сертификата является сам УЦ. При импорте реального сертификата это значение выбирается из его поля **Subject**.
Действителен с	Время действия сертификата в формате дата и время (дд.мм.гггг чч.мм.сс).
..по	Время действия сертификата в формате дата и время (дд.мм.гггг чч.мм.сс).

7.10.2. Дополнительные сведения

Объекты типа Certificate Authority могут создаваться через *Инструментальную панель->Добавить ЦС*, либо путем импорта собственно сертификата этого УЦ, или путем ручного ввода необходимых параметров. Кроме этого, возможно неявное автоматическое создание этих Объектов - например, если в окне свойств *Агента* импортировать локальный сертификат этого Объекта, то соответствующий сертификат УЦ, которым подписан этот локальный сертификат, будет автоматически добавлен в папку УЦ (если, конечно, такого Объекта там еще нет).

7.11. Мониторинг активации ГПБ

Окно *Монитор* остается пустым, до начала активации ГПБ.

Результаты активации ГПБ отображены в окне *Монитор*, выбрать **Монитор** из меню *Окно* (см. Рисунок 93).

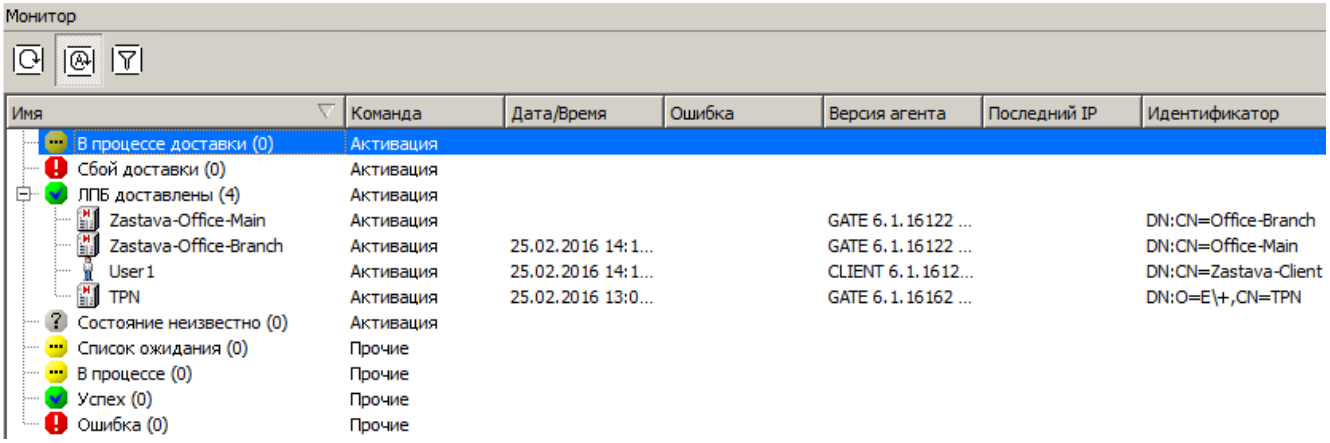

Рисунок 93 – Окно *Монитор*

Результаты активации ГПБ представлены в окне *Монитор* в отдельных списках:

- *Список ожидания* отображает имена Объектов, чьи ЛПБ ожидают распределения.
- Список ЛПБ *В процессе доставки* отображает имена Объектов, чьи ЛПБ находятся в процессе распределения.
- Список ЛПБ *Сбой доставки* отображает имена Объектов, чьи ЛПБ не доставлены по причине сбоя.
- Список *ЛПБ доставлены* отображает имена Объектов, чьи ЛПБ были успешно доставлены к их *Агентам*, с датой и временем, когда они были доставлены.
- Список ЛПБ *Состояние неизвестно* отображает имена Объектов, чье состояние ЛПБ неизвестно.

- Список *В процессе* отображает список Объектов, обновления для которых находятся в процессе установки.
- Список *Успех* отображает список обновленных Объектов.
- Список *Ошибка* отображает список Объектов, обновление которых невозможно по причине ошибки.

Список *Состояние обновления неизвестно* отображает список Объектов, состояние обновления которых неизвестно.

В столбце **Команда** окна *Монитор* расшифровано действие, которое происходит на *Агентах.*

В окне *Монитор* будут отображаться управляемые Объекты Политики, а также управляемые Серверы (у которых есть собственная ЛПБ).

7.11.1. Фильтрация в окне *Монитор*

При большом количестве Объектов мониторинг процесса прогрузки ЛПБ становится затруднительным. Для отфильтровывания необходимой информации служит строка ввода *Фильтр*. Действие фильтра распространяется на все таблицы *Монитора*. Фильтрация осуществляется по полям **Значение Id сертификата**, **IP-адрес**, **Версия *Агента***, **Имя**, ***ID в БД*** каждой таблицы. Фильтр применяется после нажатия кнопки **Готово**. Повторное нажатие кнопки **Фильтр** отменяет его действие.

7.11.2. Меню *Просмотр* в окне *Монитор*

В окне *Монитор* можно просмотреть ЛПБ любого Объекта Политики, просмотреть лог-файл, просмотреть лог активации, а также просмотреть и изменить свойства Объекта Политики. Для выполнения этих действий необходимо выбрать из любой таблицы *Монитора* интересующий вас Объект Политики, нажать на него правой кнопкой мыши, после чего выбрать в контекстном меню интересующие Вас действия.

7.11.3. Обновление статуса мониторинга

В окне *Монитор* доступны команды **Обновить статус монитора** и **Обновлять Монитор каждые 5 секунд**. Первая команда обновляет данные один раз, вторая позволяет непрерывно обновлять статус прогрузки Политики с интервалом в пять секунд.

7.12. Просмотр журналов регистрации Log и Syslog

Окно *Журнал* используется для просмотра зарегистрированных ошибок, предупреждений, событий и информационных сообщений, собранных в процессе работы с *ЦУП*, для этого надо выбрать **Журнал** в меню *Окно*.

Окно *Syslog-событий* используется для просмотра собранных Syslog-событий. Для просмотра событий надо выбрать **Syslog** в меню *Окно*.

7.12.1. Работа с журналами регистрации

Описанные ниже операции справедливы как для **Журнала событий**, так и для **Журнала Syslog-событий** (если не сказано иное).

Инструментальная линейка содержит следующие операции:

- *Очистить лог* – удаляет все зарегистрированные события из таблицы;
- *Обновить лог* – перезагружает и обновляет отображение информации журнала регистрации;
- *Автоматическое обновление журнала каждые 10 секунд* – это переключатель, который, при его активации, обновляет отображение в окне с интервалом в 10 секунд;
- *Показать только отфильтрованные сообщения* – команда вызова функции фильтрации записей в журнале событий;
- *Установить уровни лога* - выбор этой опции позволяет Вам установить уровень детализации журнала регистрации событий, конкретно Уровень лога Сервера, Уровень лога *Консоли* и Уровень лога *Прогрузчика*. Изменение настроек уровня журнала регистрации применимо только к событиям, встречающимся **после того**, как изменение было сделано. ВНИМАНИЕ: настройка уровня детализации доступна только для **Журнала событий**;
- *Индикаторы* – команда для вызова функции индикации событий. Позволяет задать индикаторы для выбранных типов событий, например: ошибка, предупреждение и т.д.;
- *Фильтры Syslog сервера* – команда для настройки отображения событий. Позволяет правила для отображений событий. ВНИМАНИЕ: настройка фильтров доступна только для Syslog журнала;
- *Псевдоним* - команда для настройки отображения источника событий. ВНИМАНИЕ: настройка псевдонима доступна только для Syslog-журнала.

7.12.2. Фильтрация результатов в журнале регистрации (Log)

Информацию журнала регистрации, отображенную в окне, можно фильтровать, используя выпадающие списки, в заголовке каждой колонки параметров лога.

Фильтрование невозможно, в лог-файле, который появляется в окне *Результаты трансляции, Результаты активации* и других диалоговых окнах.

Если фильтр по параметру применен, то кнопка фильтрации выделяется красным цветом, для снятия фильтра достаточно нажать на кнопку фильтра (если фильтр имеет несколько подфильтров, то необходимо выбрать используемый (ые)).

7.12.2.1. Выбор Фильтрации для модуля *ЦУП*

ЦУП состоит из трех модулей, которые могут создавать информацию для журнала регистрации: *Транслятор, Прогрузчик и Система*. Поставить отметку(и) рядом с модулем(ями), сообщения которого Вы желаете просмотреть. События журнала регистрации из модуля *Система* не фильтруются, и поэтому будут всегда отображаться.

7.12.2.2. Фильтрация по типу сообщений (только в окне Log Viewer)

ЦУП делит информацию журнала регистрации на четыре категории: **Ошибка**, **Предупреждение**, информационное **Сообщение** и отладочные события **Отладка**. Поставить отметку рядом с категориями информации, которые отобразятся в окне по Вашему желанию.

7.12.2.3. Фильтрация по дате и времени

Можно определить, что только зарегистрированная информация, сгенерированная в течение определенного периода времени, может быть отфильтрована и отображена **По дате и времени.** Чтобы использовать грубый фильтр надо в окне *Журнала* нажать кнопку в колонке **Дата/Время** выбрать тип фильтрации **За последние дни** и определить число дней, предшествующих текущей дате, после чего для применения фильтра нажать кнопку **Готово** Чтобы использовать более точный фильтр **За указанный период** надо установить период, заполнив поля **С...До** или **С**, и определить для временных интервалов дату и время, в которые была сгенерирована нужная Вам информация.

7.12.2.4. Фильтрация по тексту сообщения

Это – «заказной» фильтр. Можно искать зарегистрированную информацию, которая содержит задаваемую строку текста. Чтобы использовать грубый фильтр надо в окне *Журнала* нажать кнопку в колонке **Событие** и выбрать фильтр **По ключевому слову** и ввести эту строку в поле.

7.12.2.5. Фильтрация по *Агенту*/Объекту Политики

Это – «заказной» фильтр. Можно искать зарегистрированную информацию, которая включает *Агента*, представленного определенным Объектом Политики. Чтобы использовать грубый фильтр надо в окне *Журнала* нажать кнопку в колонке **Событие** и выбрать фильтр **По объекту политики** и выбрать нужный Объект Политики в выпадающем списке.

7.12.2.6. Фильтрация по *коду*

Можно искать зарегистрированную информацию, по коду сообщения. Для этого необходимо выбрать нужный код сообщения в выпадающем списке.

7.12.3. Фильтрация результатов в журнале Syslog

Информацию журнала регистрации, отображенную в окне, можно фильтровать, используя выпадающие списки, в заголовке каждой колонки параметров лога.

Если фильтр по параметру применен, то кнопка фильтрации выделяется красным цветом, для снятия фильтра достаточно нажать на кнопку фильтра (если фильтр имеет несколько подфильтров, то необходимо выбрать используемый (ые)).

7.12.3.1. Фильтрация по важности

ЦУП делит информацию журнала регистрации на категории: **Срочное, Тревога, Критическое, Ошибка, Предупреждение, Извещение, Информация, Отладочное**. Поставить отметку рядом с категориями информации, которые отобразятся в окне по Вашему желанию.

7.12.3.2. Фильтрация по дате и времени

Можно определить, что только зарегистрированная информация, сгенерированная в течение определенного периода времени, может быть отфильтрована и отображена **По дате и времени**. Чтобы использовать грубый фильтр надо в окне *Журнала* нажать кнопку в колонке **Дата/Время** выбрать тип фильтрации **За последние дни** и определить число дней, предшествующих текущей дате после чего для применения фильтра нажать кнопку **Готово** Чтобы использовать более точный фильтр **За указанный период** надо установить период, заполнив поля **С...До** или **С**, и определить для временных интервалов дату и время, в которые была сгенерирована нужная Вам информация.

7.12.3.3. Фильтрация по IP–адресу

Информацию можно фильтровать по IP-адресу объекта, для этого надо выбрать фильтр **По IP–адресу** и ввести IP-адрес в формате 0.0.0.0.

7.12.3.4. Фильтрация по подстроке

Это – «заказной» фильтр. Можно искать зарегистрированную информацию, которая содержит задаваемую строку текста. Для этого необходимо ввести эту строку в поле.

7.12.4. Правила фильтрации в журнале Syslog

Для настройки отображаемой информации можно задать правила фильтрации, используя команду **Фильтры Syslog сервера.** В появившемся окне *Отображение Syslog* (см. Рисунок 94) нужно нажать кнопку **Добавить** и задать необходимые фильтры.

После задания правил фильтрации сообщения в *Syslog* попадают согласно фильтрам по IP-адресам. Фильтры применяются в том порядке, как они указаны, т.е. сверху вниз. Более узкие фильтры надо ставить выше в таблице, для того чтобы они сработали.

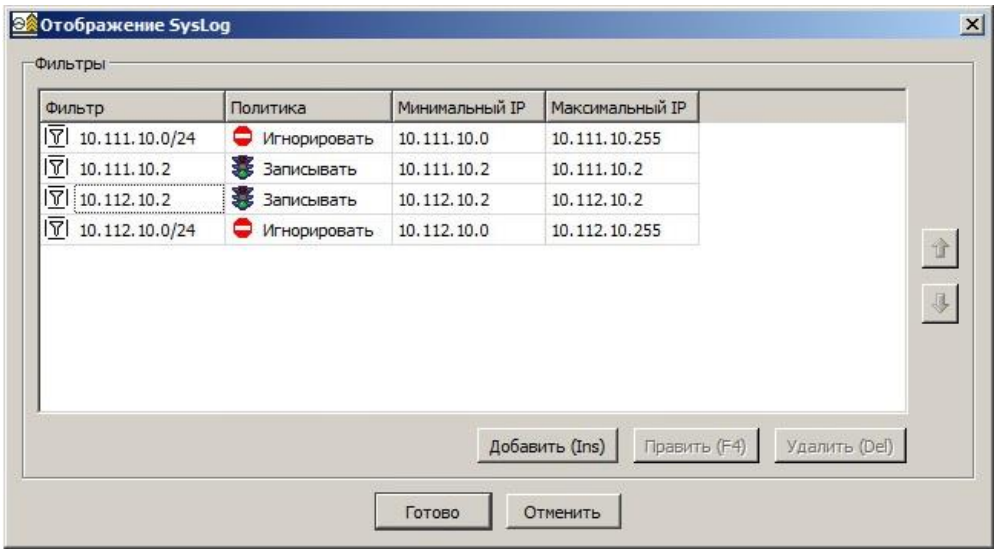

Рисунок 94 – Окно *Отображение Syslog*

7.12.5. Мониторинг сообщений в журнале событий

В *ЦУП-Консоль* имеется возможность отслеживания в автоматическом режиме определённых событий, возникающих как в **Журнале событий**, так и в **Журнале Syslog-событий.** При этом происходит визуальное и звуковое оповещение. Настройка мониторинга осуществляется отдельно для **Журнала событий** и **Журнала Syslog-событий** в меню *Индикаторы* соответствующего журнала.

Для каждого журнала независимо создаётся список *индикаторов*. Каждый *индикатор* описывает шаблон регистрируемого сообщения.

7.12.5.1. Настройка мониторинга для Журнала событий

Настройки мониторинга составляют следующую иерархию:

– Настройки;

– Индикатор;

– Условие.

Настройки содержат несколько индикаторов, каждый индикатор содержит несколько условий.

Диалог верхнего уровня содержит список индикаторов (см. Рисунок 95).

Можно удалить индикатор, добавить, изменить (в том числе при двойном нажатии на него в таблице), сохранить список индикаторов (кнопка **Готово**) или отменить изменения.

Все индикаторы работают по “ИЛИ” – то есть, при срабатывании хотя бы одного индикатора в статусной строке основного окна *ЦУП-Консоль* появляется мигающая иконка  .

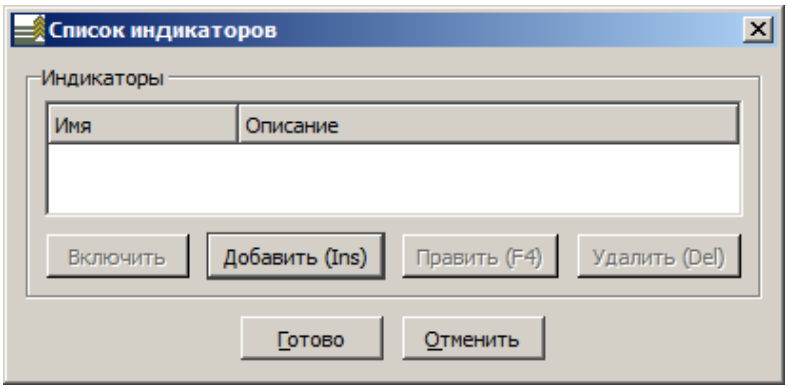

Рисунок 95 – Окно *Список индикаторов*

Добавление или правка индикатора запускает диалог следующего уровня (см. Рисунок 96).

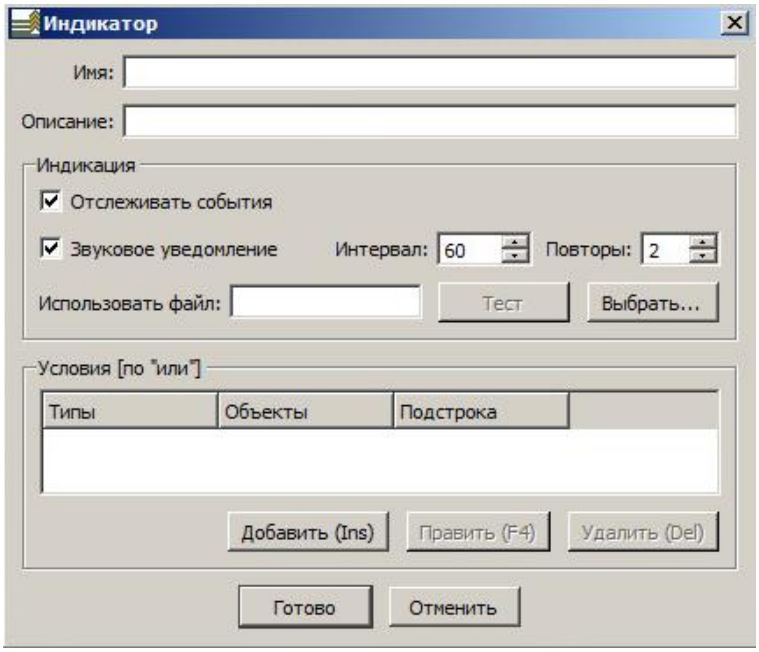

Рисунок 96 – Окно редактирования параметров индикаторов

Значение управляющих элементов показывается при наведении мыши на них во всплывающих подсказках.

Каждому индикатору можно назначить свой звуковой сигнал, для которого указать файл со звуком, период повторения сигнала и количество повторений. Кнопка **Тест** позволяет прослушать выбранный сигнал для проверки.

Если срабатывает несколько индикаторов, то сигналы могут звучать одновременно – каждый со своей заданной периодичностью.

Если поле **Использовать файл** пусто, будет срабатывать системный звуковой сигнал по умолчанию.

В качестве файла можно указать существующий, либо записать свой с микрофона. Для записи с микрофона надо использовать системную утилиту:

Start -> Programs -> Accessories ->Entertainment->Sound Recorder.

Установить галочку **Отслеживать** для тех индикаторов, которые в данный момент должны работать. Если хотя бы один индикатор отслеживает лог, в статусной строке основного окна *ЦУП-Консоль* появляется иконка  .

Индикатор должен содержать хотя бы одно условие срабатывания. Если указано несколько условий, то они объединяются по “ИЛИ” – то есть, для срабатывания индикатора достаточно срабатывания хотя бы одного из условий.

Добавление или правка условия запускает окно *Условия* для добавления параметров индикации (см. Рисунок 97).

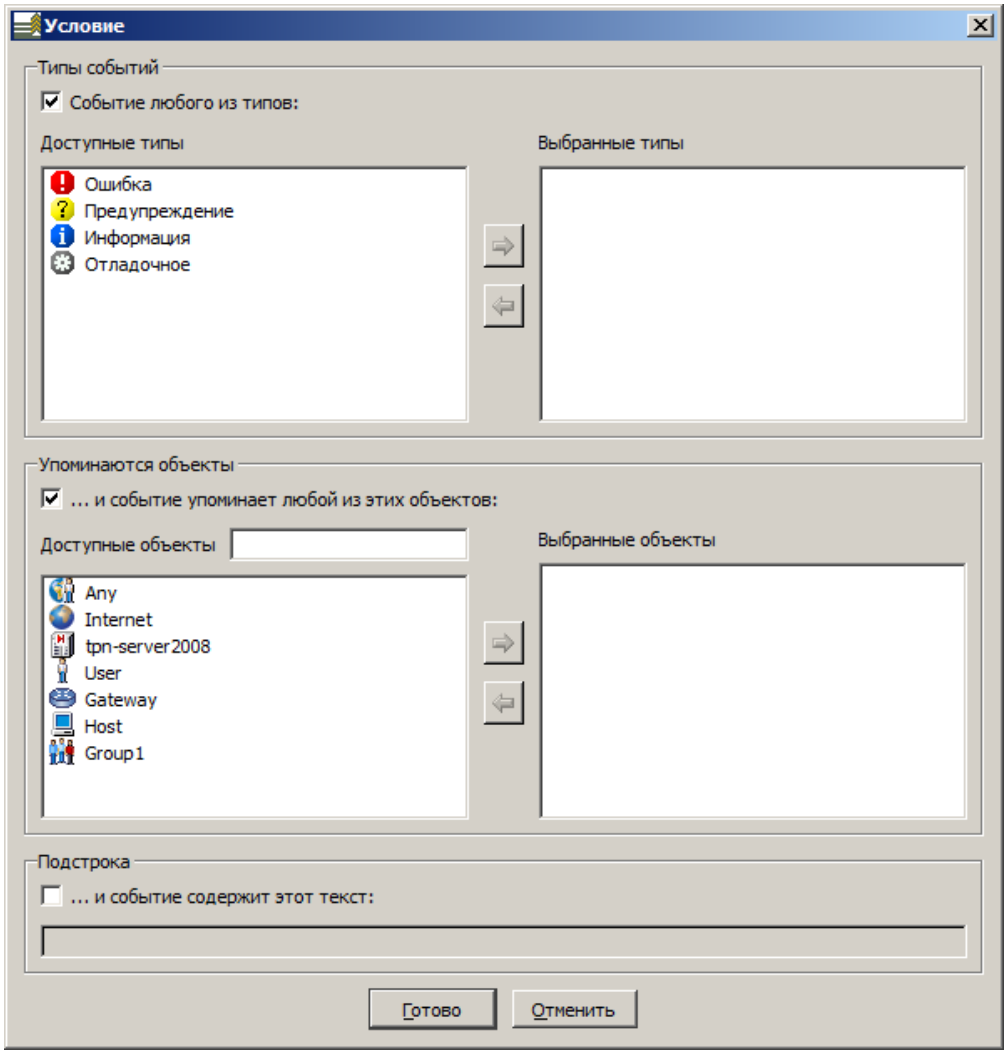

Рисунок 97 – Окно настройки условий срабатывания индикаторов

В каждом условии можно задать до трех вложенных условий, установив «галочку» около нужного вложенного условия. Все вложенные условия срабатывают по “И”, то есть, для срабатывания условия, должны сработать все вложенные условия. Если галочка не установлена, это вложенное условие не проверяется.

Первое подусловие реагирует на определенные типы событий (выбрать в списке справа те типы, которые должны вызывать срабатывание).

Второе подусловие реагирует на упоминание в логе определенного объекта политики (выбрать в списке справа те объекты, которые должны вызывать срабатывание).

Третье подусловие реагирует на появление в логе определенной динамической подстроки. Проверка аналогична проверке при фильтрации.

7.12.5.2. Настройка мониторинга для Журнала Syslog-событий

Процедура работы с индикаторами для журнала Syslog-событий аналогична работе с индикаторами для журнала событий.

Для настройки отображения событий Syslog можно выбрать соответствующий значок  или нажать правой кнопкой мыши в окне «Syslog» и в контекстном меню окна выбрать пункт **Задать псевдоним** (см. Рисунок 98). В этом окне можно выбрать кодировку, в которой *Агент* пересылает сообщения (затем эти сообщения перекодируются Syslog-сервером в формат UTF-8 и в таком виде записываются в БД). Для предоставления отчетов можно задать псевдоним для объекта с привязкой к его IP-адресу. Если псевдоним не указан, то отображение формируется, используя связь «IP-адрес – интерфейс».

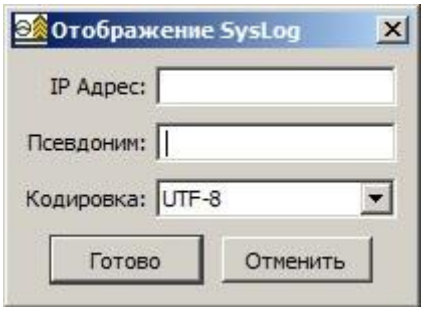

Рисунок 98 – Настройка Syslog-сервера для логирования

7.12.5.3. Срабатывание индикаторов

При срабатывании хотя бы одного индикатора (т.е. при возникновении в журнале события, подходящего под фильтр индикатора сообщения), иконка  в статусной строке основного окна *ЦУП-Консоль* начинает мигать. При нажатии на эту иконку появляется окно со списком сработавших индикаторов (см. Рисунок 99). В этом окне отображается следующая информация: название индикатора, описание индикатора, количество срабатываний индикатора с момента последнего просмотра журнала, тип журнала (Log или Syslog).

При выделении индикатора становится активной кнопка **Показать.** Нажатие на данную кнопку (или двойное нажатие по строке в таблице) активирует журнал (Log- или Syslog-событий, в зависимости от индикатора), в котором отфильтрованы соответствующие индикатору сообщения.

Список индикаторов периодически обновляется.

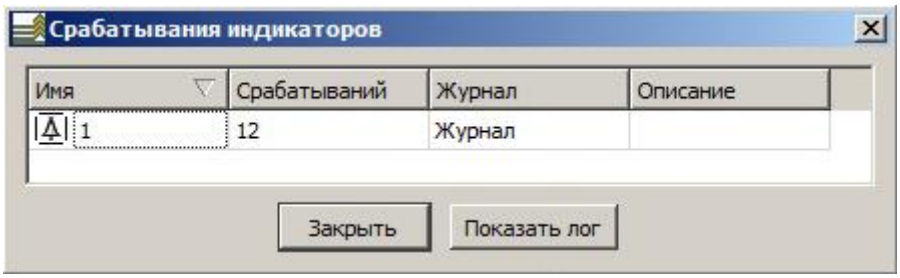

Рисунок 99 – Окно просмотра сообщений при срабатывании индикатора

7.12.6. Просроченные сертификаты

Окно *Валидность сертификатов* используется для того, чтобы отслеживать сертификаты с истёкшим сроком действия. Открыть это окно, используя команду **Валидность сертификатов** из меню *Окно*. Окно содержит список просроченных сертификатов, представленных в форме таблицы, с возможностью фильтрации по сроку истечения сертификата. Для фильтрации по сроку истечения сертификата необходимо отметить одно из полей в поле **Сертификаты.**

ЦУП-Консоль автоматически отслеживает сертификаты с истёкшим сроком действия. В случае обнаружения таких сертификатов в строке статуса основного окна *ЦУП-Консоль* появляется мигающая иконка . Нажатие на эту иконку открывает окно со списком сертификатов с истёкшим / истекающим сроком действия. Иконка мигает до тех пор, пока окно *Валидность сертификатов* не было открыто.

7.13. Дескрипторы Агентов

Окно *Дескрипторы Агентов* (см. Рисунок 51) используется для управления XML-файлами, которые содержат описания параметров для каждого типа Агента, производителя *Агента*, версии *Агента* (главной и второстепенной) и набор свойств. Эти XML-файлы переопределены в *ЦУП* и расположены в поддиректории `<ads>` инсталляционной директории *ЦУП* (см. подраздел 3.2).

Преобразовать устаревшие дескрипторы в поддерживаемые можно добавлением строки вида «SecureConnect Mobile Client,5.2,-,-,User->SecureConnect Mobile Client,5.3,-,-,User» с описанием замены в файл agent_replacements.txt в главной директории. После описания замены надо перезапустить GUI/CLI и повторите попытку импорта конфигурации.

7.13.1. Добавление дескриптора Агента

Чтобы добавить дескриптор Агента Вы должны иметь XML-файл с этим дескриптором. Нажать кнопку **Добавить** и выбрать файл в Вашей системе. При нажатии на кнопку **Open**, дескриптор загружается в *ЦУП* и появляется в таблице.

7.13.2. Удаление дескриптора Агента

Чтобы удалить дескриптор Агента надо выбрать его в таблице и нажать кнопку **Удалить**. После подтверждения удаления дескриптор будет удален из таблицы. Обратите внимание, что все записи таблицы, соответствующие данному файлу дескриптора, будут удалены из таблицы; таким образом, если дескриптор представлял больше чем один тип Объекта Политики, несколько записей таблицы будут удалены. Удалить дескриптор, который использован при описании объекта невозможно.

Удалить дескриптор, который использован при описании Объекта невозможно. При попытке удаления появится предупреждение о том, что дескриптор уже используется.

7.13.3. Просмотр дескриптора Агента

Чтобы просмотреть дескриптор Агента надо выбрать его в таблице, справа будет отображен дескриптор. В окне просмотра можно выбирать, копировать , а также искать строки текста в пределах дескриптора.

Очень осторожно изменяйте дескрипторы Агента. Дескрипторы влияют на то, как Объекты данного типа будут представлены в *ЦУП-Консоль* и как их параметры интерпретируются во время трансляции ГПБ. Настоятельно рекомендуем, чтобы Вы создали резервную копию полного набора дескрипторов перед внесением любых изменений.

7.14. Дескрипторы Серверов

Окно *Дескрипторы Серверов* используется для управления XML-файлами, которые содержат описания параметров для каждого типа Серверов и набор свойств.

Окно состоит из двух секций: в первой выводится список Серверов с указанием их имени и класса, во второй выводится сам дескриптор.

7.14.1. Добавление дескриптора Сервера

Чтобы добавить дескриптор Сервера Вы должны иметь XML-файл с этим дескриптором. Нажать кнопку **Добавить** и выбрать файл в Вашей системе. При нажатии на кнопку **Open**, дескриптор загружается в *ЦУП* и появляется в таблице.

7.14.2. Удаление дескриптора Сервера

Чтобы удалить дескриптор Сервера надо выбрать его в таблице и нажать кнопку **Удалить.** После подтверждения удаления дескриптор будет удален из таблицы. Обратите внимание, что все записи таблицы, соответствующие данному файлу дескриптора, будут удалены из таблицы.

Удалить дескриптор, который использован при описании Сервера невозможно. При попытке удаления появится предупреждение о том, что дескриптор уже используется.

7.14.3. Просмотр дескриптора Сервера

Чтобы просмотреть дескриптор Сервера надо выбрать его в таблице, справа будет отображен дескриптор. В окне просмотра можно выбирать, копировать, а также искать строки текста в пределах дескриптора.

8. Работа с Проектами и Глобальными Политиками Безопасности

Когда Вы определили все Объекты Политики, входящие в защищенную систему, и указали Правила, определяющие порядок взаимодействия этих Объектов, тем самым Вы создали ГПБ. ГПБ формально определяется как набор Правил, которые оперируют с набором Объектов Политики. Комбинация этих наборов Правил и Объектов Политики, с которыми они оперируют, называются Проектом.

ЦУП транслирует ГПБ в набор ЛПБ, по одной для каждого Управляемого *Агента*; полученные ЛПБ определяют, как определённый *Агент* может взаимодействовать с другими хостами внутри или снаружи защищенной системы. ЛПБ хранятся в БД *ЦУП* в текстовом формате. Любая ЛПБ может быть экспортирована в текстовый файл в файловой системе. Когда ГПБ активируется, все ЛПБ автоматически доставляются ко всем управляемым *Агентам* (кроме тех Пользователей, чьи IP-адреса *ЦУП* не знает - этим участникам защищённой системы должны сами обратиться к *ЦУП* для получения их последних ЛПБ).

В *ЦУП* можно применять Правило к индивидуальным Объектам Политики или сразу к Группе Объектов. Когда Объекты Политики организованы в Группы, для каждого устройства будут применены те же самые Правила, что и во всей Группе. Например, все компьютеры в Финансовом отделе могут иметь одинаковые Правила, применимые к входящему и выходящему трафику, в то время как компьютеры, принадлежащие к отделу Продаж или к отделу Маркетинга, могут использовать другие Правила.

ЦУП может посылать обновления ЛПБ всем устройствам Безопасности, когда изменится ГПБ. Части ЛПБ, которые не затрагивает обновление ГПБ, останутся неизменными, будет обновлены только части отражающие новые изменения. Процесс завершается ретрансляцией ГПБ (для всех Объектов) и ее реактивацией (для всех или некоторых Объектов).

8.1. Работа с проектами

Проекты (Правила и Объекты Политики) могут храниться в XML- и GSP-форматах и экспортироваться из *ЦУП* в файлы системы; подобным образом, Проекты, которые хранятся в XML-формате, могут быть импортированы в *ЦУП*. История ЛПБ для всех Объектов может быть очищена. В конце концов, единый Проект может быть перезагружен из БД.

8.1.1. Открытие проекта

Для перезагрузки БД *ЦУП Консоли* из XML-структуры необходимо:

– Выбрать *Проект->Открыть*.
– В окне *Импорт из файла* найти файл в XML-формате, который содержит ГПБ, нажать кнопку **Open**.

Если Вы хотите импортировать проект без его ЛПБ истории (то есть, ЛПБ со статусом **Архив** для всех Объектов Политики), то используйте команду **Открыть (без архива ЛПБ)**.

Когда команда **Open** выполнена, все текущие данные в БД *ЦУП-Консоль* будут стерты.

8.1.2. Сохранение проекта

Чтобы сохранить БД *ЦУП-Консоль* в GSP-структуру (файл с расширением .gsp) необходимо:

– После создания Проекта в *ЦУП-Консоль* выбрать в меню *Проект* команду **Сохранить**.
– В окне *Экспорт в файл* указать место, в котором Вы хотите сохранить проект, надо ввести имя и нажать кнопку **Save**. ГПБ сохраняется в указанном месте с расширением XML.

Если Вы хотите экспортировать проект без истории ЛПБ (то есть, ЛПБ со статусом **Архив** для всех Объектов Политики), тогда используйте команду **Сохранить (без архива ЛПБ)**. Обратите внимание на то, что выполнение экспорта наряду с историей ЛПБ может увеличить полный размер экспортируемого Проекта.

8.1.3. Перезагрузка проектов из базы данных

Для перезагрузки всех Объектов Политики, Правил и т.д. из БД и обновления отображения во всех квадратах окна программы надо выбрать *Проект-> Обновить из БД*.

8.2. Трансляция ГПБ в ЛПБ

Для трансляции ГПБ в ЛПБ выбрать команду **Транслировать** в меню *Проект* или нажать клавишу <F7>. Существуют три возможных результата трансляции ГПБ:

– Трансляция завершилась успешно.
– Обнаружены одна или более некритических проблем. Трансляция будет завершена и соответствующее сообщение записано в журнал регистрации сообщений.
– Обнаружена критическая ошибка. Процесс трансляции будет немедленно приостановлен и сообщение об этой ошибке записано в журнал регистрации сообщений.

8.2.1. Просмотр и редактирование ЛПБ

ЛПБ, созданные в процессе трансляции, сохраняются в буфере; во время активации они отправляются всем *Агентам* устройствам из буфера. Можно просматривать и редактировать ЛПБ тексты для определенного Объекта Безопасности в окне редактирования. Для этого надо:

- В секции *Топология* или *Объекты политики* выбрать Объект Политики, используя команду **Изменить**.
- Выбрать закладку *Управление* и затем вложенную закладку *ЛПБ*.
- Выбрать ЛПБ в таблице и нажать кнопку **Править**. Отредактировать ЛПБ в окне *Редактор ЛПБ*. После окончания надо нажать выбрать пункт **Сохранить** в меню *Файл*.

Также доступна функция сравнения ЛПБ. Для Объекта Политики Безопасности можно выбрать несколько политик и сравнить их, используя утилиту стороннего производителя. Утилиту необходимо заранее установить и указать путь к исполняемым файлам:

- Выбрать команду **Настройки программы сравнения** в меню *Просмотр*.
- В окне *Настройки программы сравнения* указать путь к утилите и аргументы: %1 – первая политика, %2 – вторая) (см. Рисунок 100).

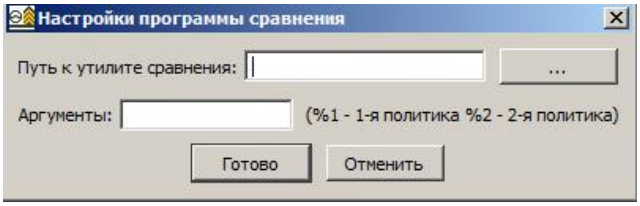

Рисунок 100 – Окно *Настройки программы сравнения*

Для того чтобы ЛПБ не была переписана еще раз для конкретного Объекта Политики надо установить отметку в переключателе «Не транслировать ЛПБ».

8.2.1.1. Прямое редактирование

Текст ЛПБ Хоста Безопасности, Шлюза Безопасности или Пользователя может непосредственно просматриваться и редактироваться в окне *Редактор ЛПБ*, которое появляется после нажатия кнопки **Править** в секции *Локальная Политика Безопасности* вложенной закладки *ЛПБ* закладки *Управление* в окне *Свойства* (когда такой Объект создается или редактируется). ЛПБ редактор – простой текстовой редактор, который позволяет Вам просматривать ЛПБ, делать любые желательные изменения в ее тексте и сохранять ЛПБ со статусом **Готова к активации**.

Пункты меню в окне *Редактор ЛПБ* очевидны и требуют только следующего разъяснения:

1) Выбор команды **Загрузка из файла** из меню *Файл* загружает ЛПБ для *Агента* из выбранного файла.
2) Выбор команды **Сохранить в файл** из меню *Файл* позволяет Вам сохранить ЛПБ, включая любые изменения, которые Вы сделали, во внешний файл. Можно сохранять ЛПБ в текстовом формате (файл *. txt).
3) Выбор команды **Сохранить в БД** из меню *Файл* сохраняет ЛПБ, включая любые изменения, которые Вы сделали, в буфер *ЦУП*. Эта ЛПБ будет сохранена в БД после нажатия кнопки **ОК**.
4) Выбор команды **Найти** из меню *Вид* позволяет запустить поиск необходимого текста в ЛПБ.
5) Выбор команды **Найти следующий** из меню *Вид* позволяет запустить поиск следующего результата команды **Найти.**
6) Выбор команды **Переход на строку** из меню *Вид* позволяет перейти на выбранную строку ЛПБ.

8.2.1.2. Редактирование структуры ЛПБ

Структура ЛПБ доступна для редактирования в поле **Структура ЛПБ** в закладке *Управление – ЛПБ*.

Редактирование структуры ЛПБ означает добавление/удаление определяемых пользователем фрагментов ЛПБ (см. п. 4.7.9) в или из ЛПБ, автоматически сгенерированной из ГПБ при помощи *ЦУП* для этого *Агента* или изменения положений таких определяемых пользователем ЛПБ фрагментов относительно автоматически сгенерированной конфигурации.

Фрагменты определяемых пользователем ЛПБ могут быть добавлены или удалены из автоматически сгенерированной конфигурации перемещением определяемой пользователем ЛПБ из *Списка доступных пользовательских ЛПБ* в список *Выбрать пользовательскую ЛПБ*. Просто выбрать одну или более определяемых пользователем ЛПБ в одном из окон, используя клавиши со стрелками <вправо>/<влево>, чтобы передвинуть их в другое окно.

После добавления в список *Структура ЛПБ* положение другого фрагмента ЛПБ относительно автоматически сгенерированной конфигурации может быть изменено, выбирая его в списке и используя клавиши <вверх>/<вниз>. Порядок ЛПБ сегментов, показанный в этом списке, будет фактическим порядком, в котором Правила ЛПБ помещены в ЛПБ, которая будет скомпилирована и доставлена *Агенту*. Таким образом, *Агент* обработает все фрагменты

определяемой пользователем ЛПБ, появляющиеся раньше автоматически сгенерированной конфигурации, а затем автоматически сгенерированную ЛПБ и любые фрагменты, появляющиеся позже ее.

Обратите внимание на то, что когда Хост Безопасности, Шлюз Безопасности или Объект пользователя создаются впервые, появляется запись – *Автоматически Созданная ЛПБ* – в списке *Структура ЛПБ.*

Можно просматривать содержание любого фрагмента ЛПБ, выбирая его в любом списке. Фрагмент ЛПБ появится внизу окна *Описание*.

8.3. Экспортирование ЛПБ

Обычно, ЛПБ экспортируются вручную. Начальные ЛПБ распределяются к *Агентам* так, чтобы они могли безопасно взаимодействовать с *ЦУП* для получения полной ЛПБ. Последующее распределение ЛПБ обычно происходит автоматически, используя команду **Активировать** в меню *Файл*. ЛПБ могут экспортироваться в текстовый файл.

8.3.1. Экспортирование полных ЛПБ для *Агента*

Чтобы экспортировать любую существующую полную ЛПБ для любого *Агента* надо сделать следующее:

- Открыть окно *Изменить* для *Агента,* выбрать закладку *Управление* и затем вложенную закладку *ЛПБ*.
- Выбрать ЛПБ в таблице *Локальная Политика Безопасности* и нажать кнопку **Править**.
- В окне *Редактор ЛПБ,* выбрать команду **Сохранить в файл** из меню *Файл.*
- Ввести имя для ЛПБ файла и экспортировать его как текстовый файл.

8.4. Активация ЛПБ на *Агентах*

Для активации ЛПБ для всех сконфигурированных *Агентов* надо использовать команду **Активировать** <F8> в меню *Проект*. Чтобы активировать ЛПБ для конкретного *Агента* надо выделить Объект Политики в секциях *Топология* или *Объекты политики*, используя команду **Активировать ЛПБ** из контекстного меню. В любом случае, когда *ЦУП* успешно обработал ЛПБ и готов активировать ЛПБ для *Агента*(ов), появится окно *Монитор* и укажет, что активация стартовала. Активация будет «завершена» только тогда, когда любой и все управляемые *Агенты* установили связь с *ЦУП* и получили и активировали их собственные ЛПБ. При попытке активации ЛПБ всех Объектов Политики с помощью команды **Активировать** <F8> в меню *Проект* появится окно, в нем необходимо подтвердить желание активировать ЛПБ для всех объектов (см. Рисунок 101) или отменить данную операцию, нажав кнопку **Нет**, если Вы хотите обновить ЛПБ только на одном Объекте Безопасности.

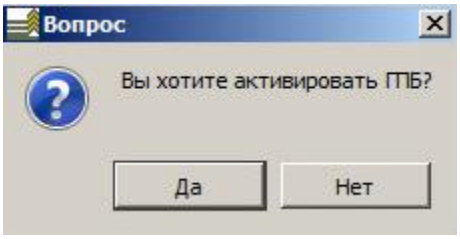

Рисунок 101 – Окно подтверждения активации ЛПБ для всех Объектов Политики

Файл `distributor.ini` содержит множество параметров для ошибок по превышению лимита времени, которые используются в течение GSP активации. См. раздел 14 для получения дополнительной информации о параметрах `distributor.ini`.

8.4.1. *Агенты*

Новая ЛПБ должна быть загружена и активирована на устройствах Безопасности со статусом **Управляемый**. Чтобы получать и активировать ЛПБ из *ЦУП, Агенты* должны иметь следующее:

1) Локальный сертификат (то есть свой собственный сертификат) и/или предварительно распределенный ключ, зарегистрированный в *Агенте* и в *ЗАСТАВА-Офис*.
2) Сертификат для верификации ЛПБ и соответствующий сертификат УЦ; он должен быть зарегистрирован как **Доверенный**.

8.4.2. Cisco и *Агенты* Microsoft

Для информации относительно формирования ЛПБ на Cisco и IPsec *Агентах* Microsoft надо обратиться к дополнительным документам, которые описывают использование этих продуктов с *ЦУП*.

8.4.3. Сценарии Активации

Существуют три различных сценария активации:

1) Для *ЗАСТАВА-Офис и ЗАСТАВА-Клиент,* установленных на компьютерах с постоянными IP-адресами и для Пользователей на *ЗАСТАВА-Клиент.* В этом случае, ЛПБ *Агента* может быть «доставлена в» или «получена от» *ЦУП* по умолчанию, как только ГПБ будет оттранслирована и подготовлена для определенного *Агента, ЦУП* свяжется с *Агентом* и «доставит» ЛПБ *Агенту*. В этом случае, нет необходимости в выполнении *Агентом* дальнейших действий. Если *Агент* «получит» ASK ЛПБ (по запросу от *ЦУП*), то ASK ЛПБ должна быть активирована в окне *Политика* Панели инструментов *Агента*, после чего полная ЛПБ будет запрошена от *ЦУП.*

2) Для Cisco маршрутизаторов и Cisco PIX Firewalls (которые служат, как Шлюзы Безопасности). Как только маршрутизатор будет сконфигурирован, чтобы использовать сертификаты и ключи и работать с *ЦУП*, *ЦУП* «доставит» ЛПБ к маршрутизатору.
3) Для хостов, использующих IPsec *Агента* ОС Microsoft Windows. Когда такой хост активирован, *ЦУП* создает SSL-туннель со специальным *Агентом*. Этот *Агент* должен быть установлен и сконфигурирован на хосте Microsoft. После получения ЛПБ этот *Агент* в свою очередь загрузит ее на IPsec *Агента* Microsoft.

8.4.4. Контроль статуса *Агента*

В главном окне *ЦУП* можно контролировать статус активации ЛПБ на *Агенте*, а также определять существуют ли какие-то проблемы с взаимодействием Cisco или ЛПБ IPsec *Агента* Microsoft, в режиме реального времени. Выбрать режим мониторинга; как только будет оттранслирована ГПБ и активирована ЛПБ, иконки статуса появятся в колонках **Имя** и **Активация** в секции *Объекты политики* и наверху иконок Объекта Политики в *Топологии.*

Когда режим мониторинга выбран из блока команд **Слежение** в меню *Просмотр:*

– Отслеживание состояния активации прослеживает изменение статуса активации ЛПБ *Агента* с помощью отображения иконок (см. Таблица 40).

Таблица 40 – Отображение статуса активации ЛПБ

Иконка	Описание
	Загрузка ЛПБ закончилась успешно
	Загрузка ЛПБ не удалась
	Состояние *Агента* неизвестно
	Загрузка ЛПБ в процессе

– Мониторинг Целостности ЛПБ (LSP Consistency Monitoring) прослеживает изменения ЛПБ устройства Cisco или IPsec *Агента* Microsoft, начиная с последней активации с помощью отображения иконок (см. Таблица 41).

Таблица 41 – Отображение изменения ЛПБ

Иконка	Описание
	На устройстве Cisco/Microsoft IPsec *Агенте* подлинная ЛПБ (согласно дате)
	ЛПБ на Cisco устройстве/Microsoft IPsec-*Агенте* была изменена, начиная с последней активизации от *ЦУП.* Для Cisco IOS маршрутизаторов этот статус будет также показан после начала сеанса администратора (даже если фактическая конфигурация устройства не была изменена).
	*ЦУП* не может соединяться с Cisco устройством/Microsoft IPsec-*Агентом* для проверки его

	взаимодействия с ЛПБ в настоящее время

9. Другие функции *ЦУП*

9.1. Работа с заказными криптоалгоритмами

По умолчанию, *ЦУП-Консоль* работает с набором криптоалгоритмов, включенных в *ЦУП*, которые позволяют Вам работать с большинством приложений. Однако, в некоторых (редких) случаях, Вам может понадобиться указывать в *ЦУП-Консоль* дополнительные криптоалгоритмы. Наиболее типичный сценарий - это когда *Агенты* в Вашей Среде Безопасности используют заказные криптоалгоритмы, зарегистрированные через интерфейс Synartra OpenCryptoAPI.

Если Вам нужно добавить новый криптоалгоритм в *ЦУП-Консоль,* необходимо выполнить следующее:

1) Создать копию XML-файла для требуемого дескриптора *Агента* (путь от главной директории *ЦУП*: `../ads/`).
2) Открыть скопированный XML-файл в текстовом редакторе, поддерживающем кодировку UTF-8, и добавить строки, описывающие новый криптоалгоритм к секции [Ph2SAParams]. Например,

```
<ESPCipherAlg Name= "Custom" ASTValue = "CUSTOM-K256-CBC"/>
```

3) Отредактировать в этом файле идентификатор дескриптора в тэге **Agent Name**, например,

```
< Agent Name= "SecureConnect Client CUSTOM"...
```

4) Используя текстовый редактор открыть файл `descriptorfiles.txt` (в главной директории *ЦУП*) и добавить в список новое имя файла.
5) Открыть *ЦУП-Консоль* и выбрать окно *Дескрипторы Агентов.*
6) Нажать кнопку **Добавить** и добавить новый XML-файл дескриптора в список.

Теперь можно создавать Объекты Политики с новым типом *Агента* и создавать **Действия**, используя новый криптоалгоритм `CUSTOM`.


Вы должны знать точный идентификатор нового криптоалгоритма в соответствии с тем, как он сконфигурирован в криптоплагине *Агента*; например, `"DES3-K168-CBC"`.


Заказные криптоалгоритмы не могут использоваться для цифровых подписей, т.к. Synartra Open CryptoAPI поддерживает только использование заказных криптоалгоритмов для симметрического шифрования и вычисления хеш-сумм.

9.2. Использование удаленной *ЦУП-Консоль*

Удаленная *ЦУП-Консоль* может быть установлена на компьютере с ОС Windows (см. подраздел 2.1). *ЗАСТАВА-Клиент* должен также быть установлен на этом компьютере.

Поскольку удаленная *ЦУП-Консоль* должна иметь защищенное соединение с *ЦУП-Сервер* / *ЦУП-Офис, Хостом Безопасности* и Объектом, соответствующем компьютеру, на котором удаленная *Консоль* будет установлена, должна присутствовать ГПБ, созданная на локальной *ЦУП-Консоль* (которая сначала должна быть установлена и сконфигурирована). ГПБ должна также содержать описание Политики (Правил) для работы с удаленной *Консолью*.

Чтобы правильно сконфигурировать удаленную *ЦУП*-Консоль локальная *Консоль* должна быть сконфигурирована для работы с удаленной *Консолью*. Тогда удаленная *Консоль* может быть установлена.

Следующие термины используются в этой секции - важно не путать их:

Локальная Консоль определяется, как экземпляр *ЦУП-Консоль*, которая устанавливается на компьютере, используемом как главный центральный пункт Администратора Безопасности компании. Это - обычно настольный компьютер, расположенный в корпоративных штаб-квартирах с установленным IP-адресом и внутренним периметром Безопасности компании. *ЦУП-Сервер* и *ЦУП-Офис* (и его БД) должны также быть установлены на этом компьютере, и БД SQL-сервера должна быть установлена на компьютере внутри периметра Безопасности (идеально, на том же самом компьютере, что и локальная *Консоль*).

Удаленная Консоль определена как экземпляр *ЦУП-Консоль*, установленной на компьютере, который используется, как вспомогательный пункт управления Политикой Безопасности. Это - обычно портативный компьютер Администратора Безопасности, и используемый Администратором Безопасности в различных местах и с различных IP-адресов. Этот экземпляр *ЦУП-Консоль* получит доступ к *ЦУП-Сервер* и БД *ЦУП* SQL из удаленного местоположения вне периметра Безопасности компании.

9.2.1. Конфигурирование локальной *ЦУП-Консоль*

Для конфигурирования локальной *Консоли* необходимо выполнить следующие правила:

1) Если Вы используете полную версию MS SQL-сервера, чтобы хранить *БД ЦУП*, надо удостовериться в том, что Ваш SQL-сервер поддерживает TCP/IP-советы. Если Вы не изменяли никакие настройки во время установки SQL, TCP/IP-советы поддерживаются автоматически.

2) Создать Хост Безопасности или Объект Пользователя в локальной *ЦУП-Консоль*, чтобы представить удаленную *Консоль*. Если удаленная *Консоль* будет иметь фиксированный IP-адрес, надо создать Объект хоста Безопасности; если удаленная

Консоль будет иметь динамически назначенный IP-адрес, надо создать Объект пользователя. Убедиться в том, что описание сертификата, созданного Объекта Пользователя/хоста (так же, как IP-адрес в случае Объекта хоста Безопасности), соответствует фактическому локальному сертификату, который будет зарегистрирован в *ЗАСТАВА-Клиент*, который защищает хост и на котором будет установлена удаленная *Консоль*.

3) Создать Правило Безопасности в ГПБ для управления взаимодействием между удаленной *Консолью* и *ЦУП-Сервер* / *ЦУП-Офис*. Это должно быть Правило, содержащее протоколы IPsec-трафика. Вам, вероятно, придется создавать Объекты Действия и IKE-Предложения (наборы параметров), чтобы использовать это Правило, если Вы еще не создали их.

ЦУП не запрещает Вам создавать Правило для этого взаимодействия по незащищённому соединению. Однако создание этого Правила в этой ситуации не обеспечит уровень Безопасности, необходимый для этой важной связи, и поэтому настоятельно рекомендуем его не создавать.

4) Если Объект пользователя был создан, чтобы представить удаленную *Консоль*, надо удостовериться в том, что параметр **Политика по умолчанию** (В закладке (*Управление* −> *Общие* окна *Свойства*)) для Объекта хоста Безопасности, который представляет собой локальную *Консоль*, установлен с параметром **Запретить всех**.

5) Оттранслировать ГПБ, выбрав команду **Транслировать** из меню *Проект* или нажав клавишу <F7>.

6) Активировать ГПБ, выбрав команду **Активировать** из меню *Проект* или нажав клавишу <F8>. В появившемся окне подтвердить желание активировать Политику для всех Объектов Политики.

Если *Агент* еще не был установлен (или должным образом конфигурирован) на хосте удаленной *Консоли*, активизация этого хоста не состоится. Это - не ошибка, не смотря на это хост удаленной *Консоли* правильно загрузит ее ЛПБ после активации Начальной ЛПБ (см. п. 9.2.2).

9.2.2. Конфигурирование хоста удаленной *Консоли*

Для конфигурирования удаленной *Консоли* необходимо выполнить следующие правила:

1) Необходимо установить *ЗАСТАВА-Клиент* на компьютер, на котором будет находиться хост удаленной *Консоли*. Не изменяя настройки по умолчанию в течение установки.

2) Определить максимальное число повторений (попыток восстанавливать взаимодействие), когда TCP/IP-взаимодействие прерывается:

– Запустить Редактор Реестра ОС Windows: выбрать команду **Run** из меню *Start*, ввести **regedit** и нажать кнопку **OK**.
– Найти HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\ Parameters key в левой части окна и выбрать его.
– Поместить мышь в правом окне. Нажать правой кнопкой мыши и выбрать команды **New −>DWORD Value** из контекстного меню. Ввести имя нового параметра.
– Переименовать параметр **TcpMaxDataRetransmissions**.
– Нажать правой кнопкой на новом имени параметра и выбрать команду **Modify** из контекстного меню.
– В диалоговом окне ввести **100** в поле **Value Data**. Удостовериться в том, что переключатель в диалоговом окне установлен в **Hexadecimal**.

Оптимальное значение для поля **TcpMaxDataRetransmissions** может быть установлено, экспериментируя с различными значениями параметра. Если у Вас возникли трудности, устанавливая **Security Association** (SA - защищённое соединение), можно увеличить значение.

3) Выйти из **Редактора Реестра** и перезагрузить компьютер.

4) Запустить *ЗАСТАВА-Клиент*. Сконфигурировать *ЗАСТАВА-Клиент* и установить необходимые сертификаты (по крайней мере, сертификат локального *Клиента* и его закрытый ключ, *ЦУП* сертификат, и соответствующие сертификаты УЦ). Загрузить и активировать **Начальную ЛПБ** (из ранее созданного файла). Это создаст туннель для удаленной *Консоли*, чтобы взаимодействовать с *ЦУП-Сервер*.

5) Проверить то, что защищенное соединение IPsec было установлено между хостом удаленной *Консоли* и *ЦУП-Сервер*. Это может быть сделано, используя команду **Ping** для компьютера *ЦУП-Сервер*. Можно также проверить окно *Monitor ЗАСТАВА-Клиент* или *ЗАСТАВА-Офис*, защищающих компьютер *ЦУП-Сервер*; оно должно показать IPsec-соединение между локальной и удаленной *Консолями*.

6) Установить *ЦУП-Консоль*. За подробной информацией надо обратиться к подразделу 2.3:

– Запустить программу *ЦУП* `\setup.exe` из дистрибутивного диска *ЦУП*. Запускается мастер установки. Перейти к окну лицензионного соглашения.
– Подтвердить Ваше принятие лицензионного соглашения.
– Выбрать местоположение для установки *ЦУП* файлов.

– Выбрать только *ЦУП-Консоль* и Справочную систему для установки.
– Закончить установку *ЦУП* и перезагрузить компьютер, на который производилась установка.

7) Запустить *ЦУП-Консоль*. В окне *ЦУП Login* нажать кнопку **Еще**:

– Нажать кнопку **Настроить**.
– В окне *ODBC Data Source Administrator* выбрать закладку *System DSN*.
– Выбрать источник системных данных, который использует *ЦУП* (по умолчанию - «*ЦУП* MSSQL База данных») и нажать кнопку **Configure**.
– Ввести IP-адрес хоста SQL-сервера в поле **Server**. Нажать кнопку **Finish** и затем нажать кнопку **OK** в следующих окнах, чтобы вернуться к окну *ЦУП Login*.
- В поле **Имя БД** ввести имя *БД ЦУП* так, как оно было введено во время установки *ЦУП-Сервер*.
– В поле **ЦУП** ввести IP-адрес *ЦУП-Сервер*.

Теперь, можно запустить удаленную *Консоль* (локальная *Консоль* должна быть закрыта) и использовать ее для доступа к *ЦУП-Сервер* и работы с ГПБ.

Когда ЛПБ хоста удаленной *Консоли* обновлена (см. шаг 8)), IPsec-соединение с *ЦУП-Сервер* потеряно и восстановлено вновь, как часть обычного процесса обновления защищенного соединения IPsec. Соединение автоматически восстановлено после окончания переговоров о новом защищенном соединении. Если удаленная *Консоль* GUI внезапно закрывается, это происходит потому, что она превысила максимальное число попыток повторения при восстановлении соединения. Если это случается, и Вы имеете проблемы с созданием защищенного соединения, просто нужно увеличить значение **TcpMaxDataRetranissions** параметра, который Вы создавали на шаге 3). **IP-адрес может находиться только в одной Зоне.**

9.2.3. Запуск удаленной *Консоли*

После начальной установки и конфигурации, описанной выше, в последующих случаях необходимы следующие шаги для запуска удаленной *Консоли*, получения доступа к БД *ЦУП* и работы с ГПБ:

1) Удостовериться в том, что никакие другие экземпляры *ЦУП-Консоль* в данное время не запускаются. Возможно, только запускать один экземпляр *ЦУП-Консоль* одновременно. Если Вы пытаетесь запускать удаленную *Консоль*, в то время как локальная *Консоль* все еще запускается, может быть конфликт с данными в БД *ЦУП*.
2) Удостовериться в том, что *ЗАСТАВА-Клиент* запущен.
3) Соединиться с сетью Интернет.

4) Запустить удаленную *Консоль*.

5) Активировать ЛПБ в *ЗАСТАВА-Клиент*.

9.2.4. Настройка других параметров системы

Если соединение между удаленной *ЦУП-Консолью* и SQL-сервером медленное, может быть необходимо изменить значение для **DBRetryTimeout** и **DBRetryCount** параметров в файле `TPNServer.ini`, расположенном в главной директории *ЦУП*. Значение по умолчанию для обоих параметров - 10; в некоторых случаях, оно должно быть увеличено до 40 или 50.

10. РАБОТА СО СРЕДСТВОМ КОНФИГУРИРОВАНИЯ *ЦУП*

Утилита конфигурирования ЦУП (SecureManage Configuration Tool) разработана для установления соединений между *ЦУП* модулями (*Консоль, Сервер, Distributor*) и БД *ЦУП*. Это отдельное приложение, и оно должно быть запущено из меню *Пуск*.

Окно *Утилита Конфигурирования ZASTAVA Management* имеет две закладки:

- *База данных* - для конфигурирования параметров доступа к БД. В этой закладке можно создавать новую БД, удалять существующую БД или конфигурировать соединение *ЦУП* с существующей БД.
- *Лицензия* - для управления файлами с лицензиями.

10.1. Управление базой данных

10.1.1. Создание новой базы данных

Чтобы создавать новую БД необходимо нажать кнопку **Создать БД** и следовать инструкциям Мастера:

- Определить источник данных, который нужно использовать для БД, выбирая его из выпадающего списка или напечатав имя в поле **Data Source Name**. Если Вам нужно сконфигурировать источник данных надо нажать кнопку **ODBC**, чтобы перейти к ODBC Data Source Administrator.
- Ввести имя пользователя и пароль, чтобы получить доступ администратора к серверу базы данных.
- Ввести IP-адрес хоста БД (или ввести **Local**, если БД будет на локальном компьютере).
- Ввести имя для новой БД.
- Определить имя пользователя и пароль для новой учетной записи *ЦУП-Сервер.*
- Определить имя пользователя и пароль для новой учетной записи *ЦУП Console*. После этого необходимо нажать кнопку **Завершить**, запустится Мастер конфигурации *ЗАСТАВА-Офис*.

10.1.2. Удаление базы данных

Чтобы удалять БД, показанную в окне *SecureManage Configuration Tool*, необходимо нажать кнопку **Удалить БД**, ввести имя пользователя и пароль для доступа администратора к серверу базы данных.

10.1.3. Соединение с базой данных

Чтобы соединяться с другой БД, а не с той, которая показана в окне *Утилита конфигурирования ЦУП,* необходимо нажать кнопку **Подключиться к БД** и ввести параметры БД, с которой Вы желаете соединиться:

1) Определить источник данных, который нужно использовать для БД, выбирая его из выпадающего списка или печатая имя в поле **Data Source Name**. Если Вам нужно сконфигурировать источник данных необходимо нажать кнопку **ODBC**, чтобы перейти к ODBC *Data Source Administrator*.
2) Ввести IP-адрес хоста БД.
3) Ввести имя БД.
4) Ввести имя пользователя и пароль существующей учетной записи *ЦУП-Сервер*.

10.2. Управление Лицензией

Чтобы активировать ГПБ в *ЦУП* Вы должны иметь действительный файл лицензии. Если Вы еще не зарегистрировали *ЦУП*, можно сделать это в закладке *Лицензия*. Если Ваша лицензия истекла, можно здесь регистрировать новую лицензию.

ЦУП лицензии основаны на уникальном ID хоста, который идентифицирует Ваш компьютер (доступен по команде **Получить ID Хоста**). Таким образом, лицензия *ЦУП* имеет силу только для одного компьютера. Таблица показывает параметры зарегистрированной лицензии, включая срок годности. *ЦУП* лицензии могут также ограничивать число *Агентов,* которыми может управлять *ЦУП.*

Чтобы зарегистрировать лицензию необходимо нажать кнопку **Загрузить,** переместиться к файлу лицензии и нажать кнопку **Открыть**. Если лицензия действительная, ее параметры будут показаны в таблице.

11. Приложение 1. Меры безопасности при использовании *ЦУП*

11.1. Краткий обзор проблем безопасности в *ЦУП*

Безопасность *ЦУП* включает следующие компоненты:

- Безопасность БД (включая Безопасность регистрации БД);
- Безопасность сертификатов и ключей;
- Безопасность управления соединениями;
- Безопасность управления структурами данных (Безопасность ЛПБ).

11.1.1. Безопасность базы данных *ЦУП*

Главный инструмент для предотвращения несанкционированного доступа к БД *ЦУП* – администрирование сервера базы данных (MS SQL или MSDE). В свою очередь, Безопасность сервера баз данных основана на использовании средств защиты сервера баз данных. Администратор сервера баз данных (имя учетной записи «**sa**») имеет право копировать, удалять и изменить любые данные в БД.

Примечание. Выполнение этого может привести к отказу работы системы *ЦУП*.

В общем, безопасность сервера баз данных состоит из двух частей. Первое – это надежное хранение пароля пользователя «**sa**». Второе – это защищенность сетевого трафика между сервером баз данных и MS SQL *Клиентом*, основанного на механизме «**named pipe**» ОС. Чтобы избегать дополнительных проблем, рекомендуется, чтобы Серверы баз данных и *ЦУП* были установлены на одном компьютере.

Как отмечено в подразделе 2.3, есть два способа первоначального управления MS SQL. Первый представляет собой предопределенную процедуру установки, которая используется, когда команда **Создать новую базу данных** отобрана в течение *ЦУП* установки.

Второй способ подразумевает подключение к уже созданной ранее БД. Используется команда **Подсоединиться к БД**.

Настоятельно рекомендуем, чтобы Вы установили все необходимые пакеты обслуживания MS SQL Server сразу после установки SQL-Сервера.

11.1.2. Безопасность Сертификатов и ключей

Сертификаты и ключи для подтверждения подлинности ЛПБ и для защиты ВЧС-соединений могут храниться как PKCS#11 токены на сменных носителях данных. Обратите внимание на то, что этот метод защиты не обязателен, если выделенная и управляемая должным образом платформа используется для *ЦУП*.

11.1.3. Безопасность управления сетевыми соединениями

Все *ЦУП*-соединения, особенно соединения между распределенными частями *ЦУП*, защищены службой ВЧС. *ЦУП* использует управление защищёнными соединениями, основанное на IKE-протоколе, чтобы загружать ЛПБ на Хосты Безопасности и Шлюзы Безопасности.

11.1.4. Защита данных ЛПБ

ЦУП использует цифровую подпись, чтобы защитить ЛПБ, которая может пройти через потенциально непроверенные каналы доставки. Эта мера обеспечивает подлинность и целостность ЛПБ. Обратите внимание, что ЛПБ обычно не содержит высокочувствительных данных; однако большинство каналов доставки ЛПБ защищено.

11.2. Рекомендации по Политике Безопасности *ЦУП*

11.2.1. Общие замечания

Значимость и уязвимость *ЦУП* Вашего решения защиты корпоративной сети настолько важны, что стоит предпринять специальные меры Безопасности. Наиболее важная и чувствительная информация в *ЦУП* и наиболее уязвимые точки (в порядке уменьшения уязвимости) следующие:

- Права Доступа на систему управления;
- Ключ для подписи ЛПБ;
- ВЧС ключи;
- Спецификации Политики Безопасности[2]..

Основная мера, которая должна быть осуществлена, чтобы защитить управляющую платформу, это использование предназначенной платформы только для одного приложения

[2] Вообще говоря, информация, содержащаяся в Спецификации Политики Безопасности не является конфиденциальной. Однако следует учитывать, что данные, о Политики, собранные нарушителем информационной информации (взломщиком), могут быть полезны для него.

(*ЦУП*) и настройка Безопасности этой платформы, средствами администрирования и сетевой Безопасности.

11.2.2. Рекомендации для обеспечения безопасности *ЦУП* платформы

Для обеспечения безопасности *ЦУП* платформы рекомендуется выполнять следующие действия:

1) Установить MS SQL-сервер и *ЦУП* на одном компьютере.

2) Использовать единую учетную запись на этом компьютере, чтобы ограничить доступ к *ЦУП* данными. После установки ОС Windows 2003, создаются некоторые учетные данные по умолчанию (типа «**guest**»). Вы должны удалить их.

3) Доступ к паролю администратора MS SQL-Сервера («**sa**») должен быть ограничен. Пароль предопределен как пустая строка после установки MS SQL-Сервера (при использовании MSDE пароль по умолчанию «**manager**»). Его следует изменить перед установкой *ЦУП*. Если MSExpress Edition используется вместо полного MS SQL-Сервера, пароль пользователя «**sa**» может быть изменен, используя удаленно приложение SQL Enterprise Manager, см. п. 2.3.3.

4) Доступ к компьютеру с *ЦУП* должен быть физически ограничен (например, в предназначенной специально безопасной комнате).

5) Использовать *ЦУП*, в качестве единственного приложения на предназначенной платформе. Установить только MS SQL-Сервер и *ЦУП* на данном компьютере. Никакие другие сетевые программные продукты не должны быть установлены на этом компьютере.

6) Все коммуникационные протоколы, кроме TCP/IP, должны быть удалены.

7) Всегда используйте разбиение диска NTFS вместо FAT. NTFS предлагает возможности обеспечения Безопасности, в то время как FAT - нет.

8) Учетная запись администратора по умолчанию – это цель для большинства злоумышленников. Создавая новую учетную запись Администратора надо удалить все разрешения из существующей учетной записи Администратора. Делайте это, создавая нового Пользователя, добавляя его к группе Администраторов и дублируя все Политики учетной записи и разрешения, предоставленные по умолчанию учетной записью Администратора. Как только Вы закончили, возвратитесь и удалите все права и разрешения из учетной записи Администратора. Однако, надо

оставить учетную запись по умолчанию разрешённой; таким образом, злоумышленники не будут знать, что она изменена, когда они попытаются взломать учетную запись.

9) Включение аудита на всех системах ОС Windows:

   – Открыть **Administrative Tools** в Управляющей панели ОС Windows.
   – Открыть **Local Security Settings** или **Local Security Policy.**
   – Открыть дерево атрибутов *Local policies* и затем выбрать **Audit Policy**; здесь можно находить события, связанные с учетной записью, которые могут быть проверены.

10) Отменить **NetBIOS** поверх TCP/IP везде, где можно – особенно на Ваших NIC-ах, ведущих к сети Интернет, если это возможно.

11) Настоятельно рекомендуется использовать только безопасные Правила (т.е., с IPsec) для любых взаимодействий между *ЦУП* и другими хостами.

12) Блокировать все TCP и UDP-порты, исключая UDP 500 порт (по умолчанию для защищенного соединения ISAKMP-трафика):

   – Открыть **Network and Dial-up Connections** в Управляющей панеле ОС Windows.
   – Открыть **Local Area Connection**.
   – В диалоговом окне нажать кнопку **Properties**.
   – Выбрать **Internet Protocol(TCP/IP)** и затем нажать кнопку **Properties**.
   – Нажать кнопку **Advanced**.
   – Выбрать закладку *Options*.
   – Выбрать **TCP/IP filtering** и нажать кнопку **Properties**.

   Примечание. Порт UDP 500 достаточен для всех взаимодействий управления. Если будет необходимо взаимодействовать с LDAP-сервером, порт TCP 389 должен также быть открыт.

ЗАСТАВА-Офис на хосте *ЦУП* также исполняют фильтрование трафика; однако, меры, описанные выше, обеспечивают дополнительную Безопасность.

Некоторые функции *ЦУП* (SNMP-контроль, SNMP-сообщения, RADIUS-аутентификация, использование LDAP-серверов или протокол NAT и т.д.) могут требовать, чтобы дополнительные TCP/UDP-порты были открытыми. Эти номера портов можно просмотреть в ЛПБ для *ЗАСТАВА-Офис*, который защищает *ЦУП* после передачи ГПБ.

13) Выключить простые TCP/IP-сервисы (если они включены), используя **Control Panel|Administrative Tools |Services**. Это останавливает сервисы: `chargen, acho, daytime, discard и quote-of-the-day (qotd)`, каждый из которых может быть использован для организации атак отказа в обслуживании. Ни один из этих сервисов не требуется для собственной работы сети, хотя Вы должны знать, что несколько типов сетевых мониторов иногда проверяют порт эха, когда они не могут получить ответ, используя `ping`.

14) Все меры предосторожности, описанные компанией Microsoft, должны быть выполнены. Все доступные пакетные сервисы должны быть установлены. Настоятельно рекомендуется, чтобы Вы не устанавливали IIS (Microsoft Internet Information Server).

15) Настоятельно рекомендуется установить опции BIOS для загрузки только с жесткого диска. Установить пароль для доступа опции BIOS и ограничить доступ этим паролем.

16) Используйте файл `hosts` для разрешения DNS имен.

12. Приложение 2. Настройка сервера обновлений

12.1. Создание сервера обновлений

12.1.1. Настройка встроенного сервера обновления

Данная процедура доступна только для *Агентов*, работающих под ОС Windows, ALT Linux 6, ALT Linux 4. Обновление *Агентов* осуществляется по протоколу http.

Использование незащищенного с помощью *ПК «VPN/FW «ЗАСТАВА»* канала обновления ЗАПРЕЩЕНО!!!!

Для настройки сервера обновлений необходимо:

- В главной директории *ЦУП ЗАСТАВА-Управление*: C:\Programs Files\ELVIS+\ZASTAVA Management в каталоге C:\Program Files\ELVIS+\ZASTAVA Management\web\webapps\ создать каталог с именем, например, agentupdate.
- В каталоге agentupdate создать файл update.ini, который должен содержать набор секций, соответствующих типу обновляемого *Агента*, а также архитектуре процессора и названию ОС. В каждой секции описывается версия доступного обновления, файлы для скачивания, исполняемая системная команда для осуществления обновления. Эти параметры - редактируемы; можно изменять значения параметра, редактируя файл в любом текстовом редакторе:
- Секции имеют следующий формат: [<тип *Агента*>.<ОС>.<процессор>.<вендор>], где:
  - <тип *Агента*> - GATE или CLIENT;
  - <ОС> - WINXX или ALT-LINUX6 или ALT-LINUX4;
  - <процессор> - i386 или amd64;
  - <вендор> - zastava.

  Пример: [CLIENT.WINXX.i386.zastava] или [GATE.ALT-LINUX6.amd64.zastava]
- [CLIENT.WINXX.i386.zastava] – начало секции для конфигурирования обновления программного компонента *ЗАСТАВА-Клиент*;
- [GATE.WINXX.i386.zastava] – начало секции для конфигурирования обновления программного компонента *ЗАСТАВА-Офис*;
- version=X.X.XXXXX - версия дистрибутива, в формате как она указана в файле version.txt дистрибутива компонента *ПК «VPN/FW «ЗАСТАВА»*, например, 6.0.13690. Версия доступного обновления сравнивается с текущей версией *Агента*, если

значение версии обновления больше, то загружаются файлы обновления и выполняется команда;

- file=zastavaclient.exe – список имен файлов, разделенный запятыми, которые нужно загрузить;
- hash=#GOST3411_256_2012:<значение> - контрольная сумма загружаемых файлов, предназначена для проверки целостности при загрузке. Контрольных сумм должно быть столько же, сколько и файлов. Если параметр не указан, то проверка целостности не производится.
- exec – исполняемая команда. Для указания путей можно использовать встроенные переменные: $download_path - путь к папке, в которую были загружены файлы; $agent_bin - путь к папке с исполняемыми файлами *Агента* (в ОС Linux запускается из под vpndmn, в ОС WINXX из под vpnagent) Дополнительные исполняемые команды:
  - exec_sys - исполняемая команда. exec_sys = "$download_path\zastavaoffice64.exe" если есть, игнорируется поле exec для ОС UNIX, значение - команда, запускаемая из под vpndmn;
  - exec_user - исполняемая команда. exec_user = "$download_path\zastavaoffice64.exe" если есть, игнорируется поле exec для ОС WINXX, значение - команда, запускаемая из под vpnagent;
  - exec_sys_wait = 1 (по умолчанию = 0) если = 1, запустить команду exec_sys и дождаться ее завершения, иначе запустить в фоновом режиме;
  - exec_user_wait = 1 (по умолчанию = 0) если = 1, запустить команду exec_user и дождаться ее завершения, иначе запустить в фоновом режиме;
  - exec = "$download_path\zastavaoffice64.exe" /l*v c:\zastava_setup.log Положить в каталог *agentupdate* дистрибутивы, выпущенные в установленном порядке, которые должны быть установлены на компоненты *ПК «VPN/FW «ЗАСТАВА»*.
- silent – параметр характеризующий оповещение пользователей (0|1 по умолчанию 0 - показывать сообщение пользователю);
- timeout – параметр характеризующий время ожидания действий на появившееся сообщение пользователю (нет параметра или 0 - без таймаута закрытия, timeout= N - ожидать N секунд, если пользователь не нажмет кнопку «Отмена», то запустится установка обновления).

- message = some text – сообщение, которое будет показано пользователю перед выполнением команды;

  Пример: exec = cmd /C echo off & "$download_path\zastavaoffice32.exe" /l*v c:\zastava_setup.log && "$agent_bin\vpnconfig.exe" -add cert "$download_path\ca.cer" ca trusted.

- Переменные, которые можно использовать в командах:
  - $download_path - папка, куда скачиваются файлы, TEMP папка для системного пользователя (WINXX: C:\Windows\temp)
  - $agent_bin – папка, в которой находятся запускаемые файлы *Агента* (WINXX: C:\Programm Files\ZASTAVA office, UNIX: /opt/ZASTAVAoffice/bin)
  - $agent_lib - папка, в которой находятся подгружаемые библиотеки *Агента* (WINXX: C:\Programm Files\ZASTAVA office, UNIX: /opt/ZASTAVAoffice/lib)
  - $agent_etc - папка, в которой находятся конфигурационные файлы (WINXX: C:\Programm Files\ZASTAVA office, UNIX: /opt/ZASTAVAoffice/etc)
  - $system_etc - папка, в которой находятся конфигурационные файлы (WINXX: C:\Programm Files\ZASTAVA office, UNIX: /etc/vpnagent)
  - $system_log - папка, в которой находятся файлы логирования системы (WINXX: C:\Programm Files\ZASTAVA office\log, UNIX: /var/vpnagent/log)
  - $system_var – папка, в которой находится файл с локальными настройками localsettings.ini (WINXX: c:\Programm Files\ZASTAVA office, UNIX: /var/vpnagent)
  - $system_var_etc - папка, в которой находится файл с настройками (WINXX: c:\Programm Files\ZASTAVA office, UNIX: /var/vpnagent/etc)
  - $system_tmp - папка, в которой находятся временные файлы (WINXX: C:\Windows\Temp, UNIX: /tmp)
  - $agent_version - текущая версия *Агента*.

    Пример:

    [GATE.WINXX.amd64.zastava]

    version = 6.0.13690

    file = zastavaoffice64.exe

    exec = "$download_path\zastavaoffice64.exe" /l*v c:\zastava_setup.log

    [GATE.WINXX.i386.zastava]

    version = 6.0.13690

    file = zastavaoffice32.exe

- После выполненных действий необходимо перезапустить службу *SecureManage Application Server*.
- При использовании встроенного сервера обновления в *ПК «VPN/FW «ЗАСТАВА»* необходимо добавить сетевой сервис TCP с портом 8080 (см. п. 7.7.2). После создания сетевого сервиса надо создать сервер обновления с методом подключения http. Для этого надо выбрать созданный сервис и указать URL, например, http://10.111.10.231:8080/agentupdate. На Объектах Политики безопасности открыть *Управление – Автоматическое обновление – Обновлять* согласно ЛПБ.
- Существует возможность обновления *Агентов* с помощью команд с сервера обновлений. Необходимо в настройках Объекта Политики выбрать закладку *Управление->Автоматические обновления* в поле **Тип обновления** выбрать параметр *Обновлять по командам с сервера обновления* и в поле **Серверы обновления** добавить сервер обновления. Для выбора команд по обновлению необходимо выбрать пункт из выпадающего списка меню *Проект* (**Обновить версию агентов** или **Загрузить версию обновлений для агентов**) или воспользоваться аналогичными командами контекстного меню для конкретного *Объекта Политики*. При обновлении кластера с версией дескриптора *Агента* выше 6.1 существует возможность обновить отдельно каждый узел кластера, для этого с помощью маркера надо выбрать номер узла для загрузки обновлений или непосредственно обновления *Агента*. Если оставить маркер в значении «0», то действие будет выполнено для всех узлов кластера.

Для выполнения команд из update.ini в ОС LINUX используется системный вызов system. Данный вызов дублирует все открытые файловые дескрипторы текущего процесса (в данном случае vpndmn). В результате может не выгрузиться драйвер vpnpcap. Чтобы это избежать, можно воспользоваться командами at или batch, которые добавляют заданные команды в системную очередь. После чего система сама выполняет команды из этой очереди в заданное при добавлении время.

Пример описания команды в update.ini:

- exec = echo "rpm -U $download_path/ZASTAVAoffice-6.1.16122-alt27.i386.rpm > /tmp/vpnupdate.log 2> &1" | batch;
  или
- exec = echo "rpm -U $download_path/ZASTAVAoffice-6.1.16122-alt27.i386.rpm > /tmp/vpnupdate.log 2> &1" | at now.

Для того чтобы обойти USER ACCOUTN CONTROL в ОС Windows можно выполнить следующее:

- использовать параметр exec_sys вместо exec в файле update.ini. Это приведет к запуску команды из vpndmn т.е. с системными правами. Недостаток: нет доступа к оконному пользовательскому интерфейсу;
- в параметр exec или exec_user в самое начало добавить cmd /C. В результате, если требуется, система выдаст запрос на запуск приложения с правами администратора;
- в параметр exec или exec_user в самое начало добавить runas. Система должна выдать запрос на запуск приложения с правами администратора.

12.1.2. Настройка автоматического обновления *Агентов* в *ЦУП-Консоль*

Параметры настройки автоматического обновления см. в п. 7.1.1.4.

12.1.3. Настройка обновления на *Агент*

Для централизованного управления настройками автообновлений (через *ЦУП*) необходимо на самом *Агенте* включить режим **Local Security Policy (Локальная политика безопасности)** (в окне *Настройки -> Настройки Обновления*). В противном случае информация о настройках обновлений в ЛПБ будет игнорироваться *Агентом*.

Для автоматического обновления *Агентов* на ОС Windows XP необходимо выполнить дополнительные настройки опций защиты системных файлов на машине с установленным *Агентом*: поставить маркер в поле System Properties ->Driver Signing Options ()->Ignore - Install the software anyway and don't ask for my approval.

Для дальнейшей настройки автоматического обновления, в зависимости от выбранных компонентов продукта *ЗАСТАВА*, надо обратиться к документам:

- МКЕЮ.00434-01 32 01 Компонент «ЗАСТАВА-Офис», версия 6. Руководство системного программиста;
- МКЕЮ.00435-01 32 01 Компонент «ЗАСТАВА–Клиент» версия 6. Руководство системного программиста.

13. Приложение 3. Пример конфигурирования *ЦУП*

13.1. *ЦУП* и два *ЗАСТАВА-Клиент*

13.1.1. Цель

Это - детальная процедура, которая поможет Вам устанавливать, конфигурировать и создавать безопасное взаимодействие между двумя *ЗАСТАВА-Клиент*, использующими *ЦУП* как станцию управления. Это - основной пример того, как работать с продуктами *ЗАСТАВА*. Логика процесса конфигурации представлена наряду с определенными и детальными шагами, необходимыми, чтобы создать конфигурацию.

13.1.1.1. Необходимое программное и техническое обеспечение

Одна ОС Windows 2008 R2 Standart Edition рабочая станция для *ЦУП* с дисководом.

Две ОС Windows XP/7/8 рабочие станции для *ЗАСТАВА-Клиент*, каждый с устройством для дискет или портом для съемного USB-носителя.

Набор сертификатов и соответствующих закрытых ключей, хранимых в PKCS#12 пакетах (например, набор тестовых сертификатов, названных следующим образом: `gate.pfx, client1.pfx и client2.pfx`; сгенерировать сертификаты самостоятельно или войти в контакт с поставщиком для получения копий тестовых сертификатов).

Действительный файл лицензии для *ЦУП*.

Следующее ПО: *ЗАСТАВА-Клиент* для ОС Windows XP/7/8 и *ЦУП*. Вы должны иметь привилегии администратора (пароли) для ОС Windows XP/7/8 и MS SQL-сервера (если он уже установлен).

13.1.2. Описание сертификатов

Этот пример предполагает, что Вы будете использовать следующие файлы с сертификатами для этой конфигурации теста (см. Таблица 42).

Таблица 42 – Описание файлов с сертификатами

Имя файла	Назначение Сертификата
`gate.pfx`	PKCS#12 файл, содержащий: Сертификат УЦ (тип идентификатора DN, значение идентификатора **CN=MainCA**); Локальный сертификат и закрытый ключ для *ЦУП* (тип идентификатора MAIL, значение идентификатора **test0@test.com**).
`client1.pfx`	PKCS#12 файл, содержащий: Сертификат УЦ (тип идентификатора DN, значение идентификатора

Имя файла	Назначение Сертификата
	CN=MainCA); Локальный сертификат и закрытый ключ для *ЗАСТАВА-Клиент#* 1 (тип идентификатора MAIL, значение идентификатора **test1@test.com**).
`client2.pfx`	PKCS#12 файл, содержащий: Сертификат УЦ (тип идентификатора DN, значение идентификатора **CN=MainCA**); Локальный сертификат и закрытый ключ для *ЗАСТАВА-Клиент#* 2 (тип идентификатора MAIL, значение идентификатора **test2@test.com**).

13.1.3. Подготовка к установке

Перед началом процесса установки удостовериться в том, что все три рабочие станции связаны друг с другом, используя TCP/IP-соединения. Убедиться в том, что Вы знаете все три IP-адреса. Позже в этой процедуре, появится пример, который предполагает, что:

- *ЦУП* будет использовать рабочую станцию ОС Windows 2008 Server R2 Standart Edition с IP-адресом 10.0.0.10.
- *ЗАСТАВА-Клиент* 1 (Клиент 1) будет использовать рабочую станцию ОС Windows 7 с IP-адресом 10.0.0.1.
- *ЗАСТАВА-Клиент* 2 (Клиент 2) будет использовать рабочую станцию ОС Windows 7 с IP-адресом 10.0.0.2.

Эти IP-адреса даются только, как пример. Могут использоваться любые другие IP-адреса. Не обязательно использовать установленные IP-адреса; например, один из Ваших *ЗАСТАВА-Клиент* может быть мобильным пользователем без установленного IP-адреса. Однако в этом примере Вы должны использовать три фактических компьютера с реальными IP-адресами. Не удастся активировать ГПБ, если *ЦУП* не может найти IP-адрес, на котором она установлена; точно также активизация не удастся, если *ЦУП* не может установить контакт с компьютерами, на которых установлен *ЗАСТАВА-Клиент*.

Если Вы используете DHCP-сервер, чтобы получать IP-адреса автоматически, Вы будете должны определить этот сервер в ГПБ. Таким образом, в этом примере рекомендуется использовать постоянные IP-адреса.

13.1.4. Установка пакета программ *ЦУП*

Запустить программу *ЦУП*`\setup.exe` с дистрибутивного диска. В течение процедуры установки, сделать следующее:

- В окне, в котором Вас спросят **Выбрать компоненты программы для установки**, убедиться в том, что выбраны и *ЦУП-Консоль,* и *ЦУП Server*;

- Когда спросят: **Сервер базы данных** *Выбрать расположение SQL Server*, выбрать **Встроенный сервер БД.** Будет установлен сервер базы данных (MS SQL 2008 R2 Express Edition) и компоненты для доступа к нему;
- В процессе установки MS SQL Server 2008 R2 на этапе конфигурирования пароля для аутентификации под учетной записью администратора необходимо сгенерировать пароль, отвечающий следующим требованиям:
  - Не содержит всю или часть имени учетной записи пользователя;
  - Длиной более восьми знаков;
  - Содержит символы, по крайней мере, трёх следующих категорий:
    - Заглавные буквы английского алфавита (от A до Z);
    - Строчные буквы английского алфавита (от a до z);
    - Основные 10 цифр (0-9);
    - Небуквенные символы (например: !,#,%);
- *ЗАСТАВА-Офис* будет установлен дополнительно;
- Когда спросят выбрать тип БД **Вы хотите создать новую БД *ЦУП*?**, надо нажать кнопку **Yes**;
- В появившемся окне необходимо нажать кнопку **ODBC**;
- Выбрать вкладку *System DNS* и указать ресурс БД;
- Появится окно с предложением ввода названия, описания и адреса сервера базы данных. В последнем пункте ввести 127.0.0.1 или **(local)**;
- В поле **Название БД** ввести (или оставить по умолчанию) новое имя **TPNDB** для создаваемой БД;
- Нажать кнопку **Client Configuration**, слева выбрать **TCP/IP**, в появившемся окне снять отметку возле **Dynamically determine port** и указать порт **1433**, нажать кнопку **OK**;
- Можно завершать процесс конфигурирования БД. После нажатия кнопки **Finish** появится окно с параметрами создаваемого программного интерфейса доступа к БД, необходимо выполнить тестирование соединения, который, если всё было выполнено правильно, закончится успешно;
- Ввести логин и пароль администратора сервера базы данных, которые были заданы на этапе установки MS SQL 2008. Нажать кнопку **ОК** (данная информация будет проверена на следующем этапе, при попытке создания БД);
- Ввести имя пользователя **tpn-server** и пароль **server-pwd** для *ЦУП-Сервер*;
- Ввести имя пользователя **tpn-admin** и пароль **admin-pwd** для *ЦУП-Консоль*.

Теперь установка *ЦУП* завершена. Перезагрузить ОС, когда установка завершена. Как только Вы перезагрузили компьютер появится Мастер конфигурирования *ЗАСТАВА-Офис*. Указать то, что Вы будете конфигурировать *ЗАСТАВА-Офис* вручную.

13.1.5. Установка *ЗАСТАВА-Клиент*

Установить *ЗАСТАВА-Клиент* на каждом компьютере ОС Windows 7. В течение установки не менять никаких настроек – оставить все установки по умолчанию без изменений.

13.1.6. Конфигурирование *ЗАСТАВА-Офис*

Первый шаг состоит в добавлении *ЦУП* сертификатов в *ЗАСТАВА-Офис*.

1) Запустить *ЗАСТАВА-Офис* из меню *Start* (`Start|Programs| Zastava Office |VPN Agent)`.
2) Нажать кнопку **Сертификаты**. Появится окно *Сертификаты и ключи.*
3) Нажать кнопку 

Импорт или **Импорт сертификата** из меню *Сертификат*. Запустится программный Мастер.
4) Чтобы зарегистрировать новый сертификат (Доверенные) в *ЗАСТАВА-Офис* необходимо сделать следующее:
   - В появившемся окне выбрать необходимый для установки сертификат gate.pfx и нажать кнопку **Открыть**.
   - Ввести PIN-код токена, на котором хранится контейнер с сертификатом(ами), чтобы получить доступ к PKCS#12 пакету. Мастер теперь показывает сертификат, который Вы собираетесь зарегистрировать.
   - В поле **Режим импорта** должны быть установлены следующие настройки:
     - В поле **Режим импорта** переключатель слева от строки CN=MainCA выбираем **Доверенный** для импорта сертификата УЦ;
     - В поле **Режим импорта** переключатель слева от строки с локальным сертификатом выбираем **С ключом**;
     - Необходимо ввести PIN-код токена, в котором будет содержаться сертификат. После ввода PIN-кода нужно нажать кнопку **Готово**.

5) Чтобы зарегистрировать новый сертификат (Персональный) в *ЗАСТАВА-Офис* необходимо сделать следующее:

   – В появившемся окне выбрать необходимый для установки сертификат `gate.cer` и нажать кнопку **Открыть**.
   – Вы регистрируете сертификат УЦ, нужно в поле **Режим импорта** назначить этому сертификату соответствующий статус - **Импортировать**. После чего нажать кнопку **Далее**.

6) При успешном импортировании появится индикатор  . Теперь Мастер сертификатов показывает импортированный сертификат, нажать кнопку **Готово**.

7) Зарегистрированный сертификат теперь включен в таблицу вкладки *Персональные* окна *Сертификаты и Ключи*.

Сертификат УЦ будет использоваться, чтобы проверить подписи всех сертификатов теста. Все сертификаты были подписаны этим сертификатом УЦ. Сертификаты УЦ не нуждаются в закрытых ключах.

Локальный сертификат будет использоваться, чтобы идентифицировать *ЦУП* всеми другими участникам Среды Безопасности. Закрытый ключ позволяет осуществлять двустороннюю криптографическую аутентификацию при установлении соединений с другими хостами защищенной корпоративной сети на базе протоколов IKEv1 и IKEv2.

13.1.7. Создание ГПБ в *ЦУП-Консоль*

Запустить *ЦУП-Консоль* из меню *Start* (см. подраздел 3.2) или нажать два раза левой кнопкой мыши на иконку рабочего стола. Ввести пароль *ЦУП-Консоль (admin-pwd).*

13.1.7.1. Создание Объектов Политики

Следующий шаг должен создать и сконфигурировать Объекты Политики:

1) В секции *Объекты политики* выбрать вкладку *Сетевые Объекты*.

2) Чтобы добавить Объект Политики *Клиент 1*, надо нажать кнопку **Добавить Хост Безопасности** на Панели инструментов или использовать команды **Добавить Хост Безопасности** из контекстного меню и сделать следующее:

   – В окне *Выбор Дескриптора Агента* выбрать **SecureConnect Clients** последней версии в качестве типа *Агента*. Нажать кнопку **OK**. В закладке *Общее*:
      – Ввести **Client1** в поле **Имя.**
      – Выбрать домен, в который будет входить данный объект.
   – В закладке *Топология* нажать кнопку **Добавить**:

- Ввести любой идентификатор логического имени и IP-адрес 10.0.0.1. Выбрать из списка *Привязка к зоне:* параметр **Зона Интернет**. Нажать кнопку **OK**.

– В закладке *ВЧС* выбрать вложенную закладку *Сертификаты*:
  - В окне *Сертификаты* нажать кнопку **Импорт**.
  - В окне *Импорт сертификатов* выбрать нужный сертификат и нажать кнопку **Open**.
– Нажать кнопку **OK**. Объект Политики *Клиент 1* с именем *Client1* теперь появляется в секции *Топология ВЧС* и в папке *Сетевые Объекты* в секции *Объекты политики*.

3) Чтобы добавить Объект Политики *Клиент 2* надо нажать кнопку **Добавить Хост Безопасности** на Панели инструментов или использовать команды **Добавить Хост Безопасности** из контекстного меню и сделать следующее:

– В окне *Выбор Дескриптора Агента* выбрать **SecureConnect Clients** последней версии в качестве типа *Агента*. Нажать кнопку **OK**.
– В закладке *Общее*:
  - Ввести **Client2** в поле **Имя**.
  - Выбрать домен, в который будет входить данный объект.
– В закладке *Топология* нажать кнопку **Добавить**. Ввести любой идентификатор логического имени и IP-адрес 10.0.0.2. Выбрать из списка *Привязка к зоне:* параметр **Зона Интернет**. Нажать кнопку **OK**.
– В закладке *Местоположение* определить местоположение **Client2**, вводя в поля **Широта** и **Долгота** его координаты.
– В закладке *ВЧС* выбрать вложенную закладку *Сертификаты*:
  - В окне *Сертификаты* нажать кнопку **Импорт**.
  - В окне *Импорт сертификатов* выбрать нужный сертификат и нажать кнопку **Open**.
  - Выбрать DN из выпадающего списка *Тип идентификатора*.
  - В поле **Значение идентификатора** появится его значение. Нажать кнопку **OK**.
– Нажать кнопку **OK**. Объект Политики *Клиент 2* с именем *Client2* теперь появляется в секции *Топология ВЧС* и в папке *Сетевые Объекты* в секции *Объекты политики*.

4) Изменить настройки *Объекта Политики* хоста, на котором расположен *ЦУП-Сервер*:

   – Выбрать Объ*ект Политики*, на котором расположен *ЦУП-Сервер* (данный объект создается автоматически при создании БД *ЦУП*), используя **Изменить** из контекстного меню.
   – В закладке *Общее* изменить имя *Объекта Политики* на **TPN_Gate**.
   – Удостовериться в том, что IP-адрес в поле **Адрес Агента** верен (например, 10.0.0.10). Если нет - ввести Правильный IP-адрес в соответствующее поле.
   – Выбрать домен, в который будет входить данный объект.
   – Выбрать закладку *Топология*. Убедиться в том, что в таблице указана правильная информация об интерфейсах хоста (в зависимости от сценария использования, у хоста *ЦУП* может быть один или более интерфейсов).
   – В закладке *Местоположение* определить местоположение **TPN_Gate**, вводя в поля **Широта** и **Долгота** его координаты.
   – Выбрать закладку *ВЧС* и затем вложенную закладку *Сертификаты*.
   – Нажать кнопку **Импорт**.
   – В окне *Импорт сертификатов* указать путь к файлу с локальным сертификатом без ключа gate.cer и нажать кнопку **Open**.
   – В поле **Значение идентификатора** появится его значение. Нажать кнопку **OK**.
   – Нажать кнопку **OK**, чтобы выйти из окна *Свойства*.

9) Изменить настройки *ЦУП Server*:

   – Выбрать **Серверы** из меню *Окно*.
   – Выбрать *Объект* **PMP Distribution Service**.
   – Удостовериться в том, что IP-адрес установлен в значение **Auto** и что **RSA DN = 'CN=MainCA'** появился в поле **Сертификаты**.

Когда Вы закончили, появится изображение в *Графе топологии* (см. Рисунок 102).

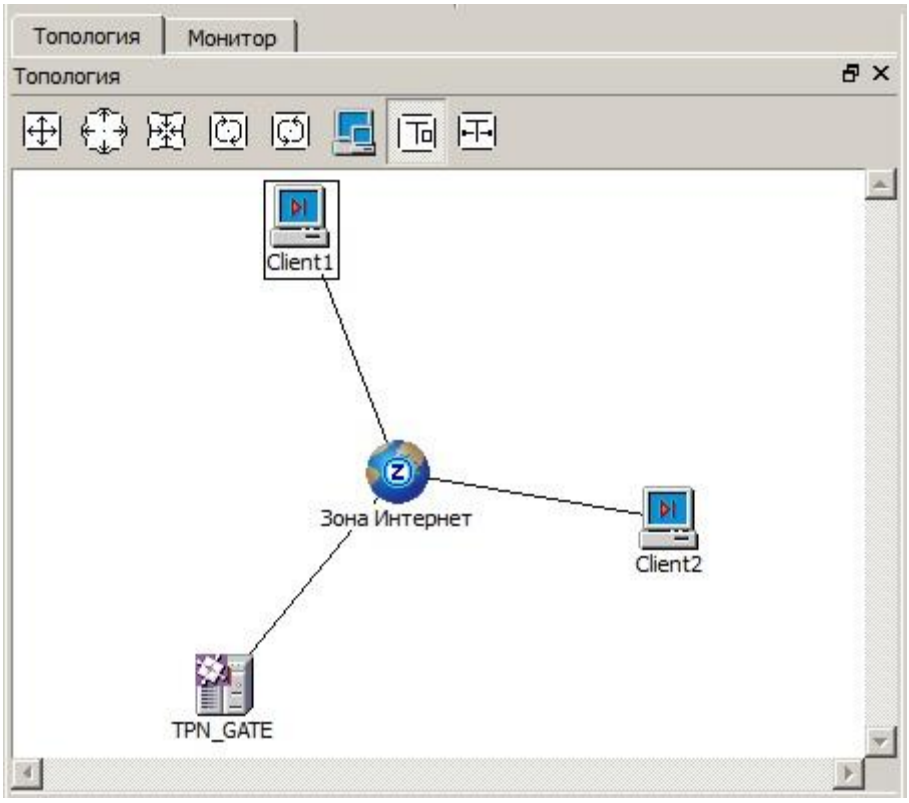

Рисунок 102 – Созданный *Граф топологии*

13.1.7.2. Создание Действий

Следующий шаг в процессе – это определение действий для обработки трафика. Эти Действия будут использоваться Правилами, которые Вы создадите на следующем шаге. Есть два шифрования Действия, предопределенные в *ЦУП* для практических целей, однако, необходимо создать Ваше собственное Действие (см. Рисунок 103) следующим образом:

1) Перейти к окну *Действия*, выбирая команду **Действия** из меню *Окно*.

2) Добавить **Действие**:

   – Поместить курсор в открывшееся окно и нажать правой кнопкой мыши. Выбрать команду **Добавить Действие**.
   – Ввести **My_first_action** в поле **Имя.**
   – Оставить другие параметры по умолчанию. Нажать кнопку **OK.**

3) Добавить **Новое IPsec-Предложение**:

   – Поместить курсор на действие **My_first_action** и нажать правой кнопкой мыши. Выбрать команду **Добавить IPsec-Предложение**.
   – Определить нужные опции ESP-протокола или оставить настройки по умолчанию.

– Определить нужные опции АН протокола или оставить настройки по умолчанию.
– Определить настройки, продолжительность существования защищенного соединения в поле **Время жизни SA,** или оставить настройки по умолчанию.

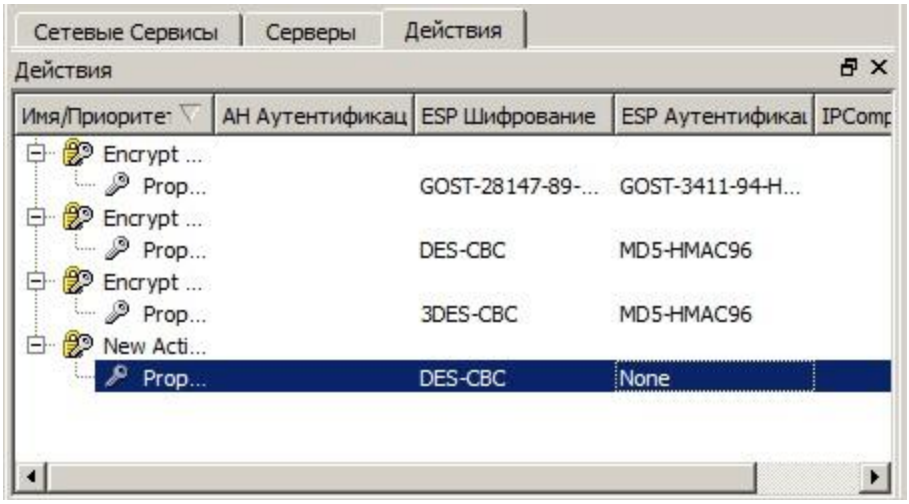

Рисунок 103 – Окно *Действия* с созданным новым правилом

13.1.7.3. Проверка ГПБ

Теперь Вы должны проверить, были ли сделаны ошибки в ГПБ. Перейти к меню *Проект* и выбрать команду **Транслировать**. Появится окно *Результаты трансляции* с результатами трансляции (ошибки, предупреждения и информационные сообщения).

В течение процесса трансляции *ЦУП* создает ЛПБ для всех *Агентов* и проверяет созданную ГПБ на согласованность. Это также означает то, что, как только Вы сделали любые изменения в ГПБ и хотите применить их к Среде Безопасности, Вы должны транслировать ГПБ снова. ГПБ должна быть успешно оттранслирована до ее активизации.

13.1.7.4. Создание Правил

В этом примере необходимо только создать одно Правило для взаимодействия между *Клиентом 1* и *Клиентом 2*:

1) Перейти в секцию *Таблица Правил* (см. Рисунок 104), используя команду **Добавить Правило** из контекстного меню:
   – Ввести **My_first_rule** в поле **Имя.**
   – Добавить **Client1** в качестве источника Правила:
     – Выбрать вкладку *Объекты* поля **Источник.**

– Выбрать Хост Безопасности **Client1** и нажать кнопку с изображением правой стрелки.

2) Добавить **Client2** в качестве Приемника Правила:

– Выбрать вкладку *Объекты* поля **Приемник.**

– Выбрать Хост Безопасности **Client2** и нажать кнопку с изображением правой стрелки.

3) Выбрать **My_first_action** из выпадающего списка *Действие*.

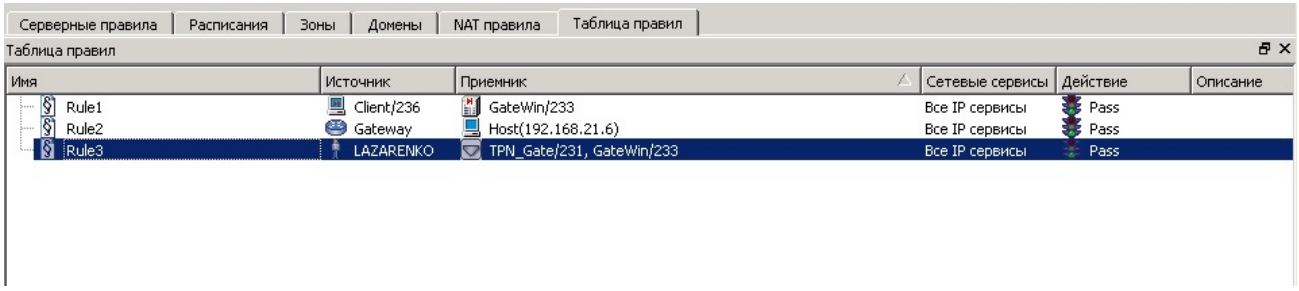

Рисунок 104 – Окно Правил

Теперь *ЦУП* полностью сконфигурирован. Последнее, что Вы должны сделать, это передать эту конечную ГПБ (выбрать **Транслировать** из меню *Проект*). После того, как *ЦУП* укажет, что трансляция была выполнена успешно, можно перейти к следующей секции и сконфигурировать *ЗАСТАВА-Клиент*.

13.1.8. Конфигурирование *ЗАСТАВА-Клиент*

Для того чтобы использовать *ЦУП* для управления *ЗАСТАВА-Клиент* и создавать безопасные соединения между двумя *ЗАСТАВА-Клиент* необходимо добавить следующие сертификаты для *ЗАСТАВА-Клиент 1 (Client1)* и *ЗАСТАВА-Клиент 2 (Client2)*:

– Пакет сертификата для *ЗАСТАВА-Клиент 1* (`client1.pfx`), содержащий сертификат УЦ и локальный сертификат с соответствующим закрытым ключом, должен быть добавлен к **Client1**.

– Пакет сертификата для *ЗАСТАВА-Клиент 2* (`client2.pfx`), содержащий сертификат УЦ и локальный сертификат с соответствующим закрытым ключом, должен быть добавлен к **Client2**.

13.1.8.1. Регистрация Сертификатов

Теперь надо зарегистрировать сертификаты в *Клиенте 1*:

1) На компьютере, который управляет **Client1**, запустить *ЗАСТАВА-Клиент* из меню *Start* (`Start\Programs\ELVIS+\VPN Agent`).

2) Нажать кнопку **Сертификаты** на Панели инструментов. Появится окно *Сертификаты и Ключи*.

3) Добавить сертификат УЦ и сертификат **Client1** с его соответствующим закрытым ключом:

   – Нажать кнопку **Импорт**, чтобы перейти к мастеру регистрации сертификата.
   – Нажать на кнопку **Обзор** и найти файл client1.pfx. Выбрать этот файл и нажать кнопку **Открыть**, чтобы возвратиться к мастеру. Нажать кнопку **Далее**.
   – Ввести пароль, чтобы получить доступ к PKCS#12 пакету. Нажать кнопку **ОК**.
   – Установить значения для двух переключателей в поле **Тип импорта**. Их значение следующие:
      – переключатель слева от строки **CN=MainCA** выбирает для импорта сертификат УЦ – **Доверенный**;
      – переключатель слева от строки test1@test.com выбирает для импорта локальный сертификат *ЗАСТАВА-Офис* - **Секретный ключ**;

5) Закрыть все окна *ЗАСТАВА-Клиент* и выйти из программы.

Теперь надо зарегистрировать сертификаты в *Клиенте 2*. Повторить шаги 1) – 5), на компьютере, который управляет *ЗАСТАВА-Клиент 2*. Используйте файл `client2.pfx` для сертификата УЦ и локального сертификата/закрытого ключа.

13.1.8.2. Загрузка начальной ЛПБ

Теперь, когда все сертификаты зарегистрированы, начальная ЛПБ должна быть загружена на *ЗАСТАВА-Клиент*:

1) Запустить *Клиент 1*, нажать кнопку **Политика**. Появляется окно *Управление политиками*.

2) Выбрать закладку *Системная*.

3) Выбрать один из способов добавления ЛПБ в окне *Добавить политику*:

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

– Для загрузки ЛПБ с сервера необходимо выполнить следующие действия: ввести адрес сервера, с которого будет получена политика, заполнить поля **Сертификат** и **Уровень лога**.

4) Нажать кнопку **Готово**.

5) Подтвердить активацию измененной Политики.

6) Вернуться к компьютеру *Клиент 2* и повторить шаги 1) – 5) с использованием для него файла `client2.txt`.

13.1.9. Активизация ГПБ

Теперь Вы готовы управлять *Клиент 1* и *Клиент 2* из *ЦУП*. Запустить *ЦУП-Консоль* и запустить *Активировать* из меню *Файл*. В появившемся окне подтвердить желание активировать Политику для всех Объектов Политики. Откроется автоматически окно *Монитор* так, чтобы Вы смогли наблюдать за ходом активизации. После нескольких секунд все хосты должны появиться в папке *ЛПБ доставлены* (см. Рисунок 105).

Состо...	Активация	Имя	Тип	Тип Агента	Запрети...	IP адрес	Сертифик...	Участник	Описани
	Успех	TPN_Gate	Шлюз без...	Synartra T...		212.114.5.32	RSA ID_DE...		
	Успех	Client1	Хост без...	Synartra T...		212.114.5.248	RSA ID_US...		
	Успех	Client2	Хост без...	Synartra T...		212.114.5.82	RSA ID_US...		

Рисунок 105 – Таблица ГПБ индикация активации ЛПБ

Теперь, когда система была Правильно конфигурирована, *Клиент 1* и *Клиент 2* могут безопасно взаимодействовать, используя настройки, которые применялись в *ЦУП*.

14. Приложение 4. *ЦУП* файлы инициализации

14.1. Файл TPNServer.ini

Файл `TPNServer.ini`, представленный в *ЦУП* директории по умолчанию после установки, определяет некоторые соединения, и параметры по превышению лимитов времени (timeout), которые управляют различными аспектами действий *ЦУП*. Эти параметры – редактируемы. Можно изменять величины превышения лимитов времени, редактируя `TPNserver.ini` файл в любом текстовом редакторе.

14.1.1. Опции транслятора

Для редактирования файла инициализации `TPNserver.ini` необходимо изменить параметры файла в любом текстовом редакторе (см. Таблица 43).

Таблица 43 – Описание транслятора

Параметр	Значение по умолчанию	Значение
LogfileName	server.log	Имя файла системного журнала *ЦУП-Сервер*
LogLevel	1	Определяет значение по умолчанию, которое используется системой, пока фактический уровень журнала регистрации не будет прочитан из БД *ЦУП*
EDServerPort	3118	Номер удаленного порта для модуля Event Dispatcher Service, который посылает и получает пакеты для обмена между *ЦУП*-компонентами
EDServerhostName	127.0.0.1	Имя хоста для модуля Event Dispatcher Service
DBRetryTimeout	10	Время, которое *ЦУП* будет ожидать, чтобы соединиться с БД до выдачи ошибки о превышении времени ожидания (для одной попытки соединения)
DBRetryCount	10	Количество раз, которое *ЦУП* будет пытаться соединиться с БД перед возвращением сообщения об ошибке
IntegrityChecking Interval	5	Время, в течение которого *ЦУП* проверяет целостность
LogLevelMonitor CheckingInterval	1	Время, в течение которого *ЦУП* проверяет изменения в уровне лога
LoginAttemptsPerAddressUntilBlock	5	Колическтво неудачных попыток входа пользователя до блокировки
LoginBlockPeriod	60	Время, на которое будет заблокирована учетная запись
MaxAllowedTraces	1024	Максимально разрешенное число трасс между Зонами
MaxLoggedMessagess	1000	Максимальное число записей о событиях с одинаковым ID

14.1.2. Опции Cisco IOS

Для редактирования файла инициализации `TPNserver.ini` для Cisco IOS необходимо изменить параметры файла в любом текстовом редакторе (см. Таблица 44).

Таблица 44 – Опции Cisco IOS

Параметр	Значение по умолчанию	Значение
CISCOACL Base	100	Списки контроля доступа, используемые в ЛПБ, произведенные транслятором для Cisco, будут пронумерованы, начиная с этого номера.
CISCOCom mentLevel	0xFF (255)	Уровень детализации комментария, появляющегося в файле конфигурации при трансляции Политики для Cisco IOS Шлюза. Возможные значения: 0x01 Добавить имя к списку фильтрованного доступа 0x02 Добавить имя к статическому шифратору ACL 0x04 Добавить имя к динамическому шифратору ACL 0x08 Добавить имя к autopass crypto ACL 0x10 Добавить имя к autopass filter ACL 0x20 Отражает имя секции в конфигурации 0x40 Другой комментарий 0x80 Показывает начало и конец конфигурирования 0xFF Добавить все комментарии Эти значения могут быть объединены, используя битовую операцию OR.
CISCORule LogLevelOn	Details	Определяет уровень регистрации Правила в системном журнале *ЦУП*, для данного Правила, переключённого для Cisco IOS Шлюза
CiscoDelete LocalUsers	2	Определяет, могут ли локальные пользователи Cisco маршрутизатора, уже существующие в конфигурации Cisco маршрутизатора, быть удалены из маршрутизатора, используя соответствующие команды в ЛПБ, сгенерированной *ЦУП*. Возможные значения: Все пользователи в ГПБ должны быть удалены из маршрутизатора; Все пользователи в ГПБ должны быть удалены из маршрутизатора только если есть отметки **Включить XAUTH** и **Включить IKE/IPsec-обработку** в свойствах *Объекта Политики*, представляющего данный маршрутизатор. Обновить части пользователя на маршрутизаторе только для тех пользователей, которые имеют соответствующие с маршрутизатором Правила **Encrypt** и **XAUTH**

14.1.3. Опции Cisco PIX

Для редактирования файла инициализации `TPNserver.ini` для Cisco PIX необходимо изменить параметры файла в любом текстовом редакторе (см. Таблица 45).

Таблица 45 – Опции Cisco PIX

Параметр	Значение по умолчанию	Значение
PIXDeleteL ocal Users	2	Определяет, могут ли локальные пользователи, уже существующие в конфигурации PIX Firewall, быть удалены из МЭ, используя соответствующие команды в ЛПБ, сгенерированной *ЦУП*. Возможные значения:

Параметр	Значение по умолчанию	Значение
		Удалить всех пользователей из PIX Firewall; Все пользователи в ГПБ должны быть удалены из МЭ; Все пользователи в ГПБ должны быть удалены из МЭ только, если установлены переключатели **Включить XAUTH** и **Включить IKE/IPsec-обработку** в свойствах *Объекта Политики*, представляющих МЭ в запросе. Обновить части Пользователя на МЭ только для тех Пользователей, которые имеют соответствующие с МЭ **Encrypt** и **XAUTH** Правила

14.1.4. Другие параметры

Для редактирования файла инициализации `TPNserver.ini` и изменения общих параметров для всех устройств необходимо изменить параметры файла в любом текстовом редакторе (см. Таблица 46).

Таблица 46 – Опции других параметров фала `TPNServer.ini`

Параметр	Значение по умолчанию	Значение
ErrorBadFWname	1	Этот параметр определяет, как отреагирует *ЦУП*, если имя Процедуры МЭ не может быть найдена в списке шаблона. Возможные значения: 0, 1. Если установлено 0, «ошибка» будет игнорироваться, и сообщение не появится. Если установлено 1, сообщение об ошибке появится с именем типа *Агента*, на котором произошла ошибка.
NomadicPeerLocationMask	255.255.255.0	Этот параметр определяет максимальный размер маски пользовательской ЛПБ, который позволяет разделение на отдельные адреса
UseLocalAddress	1	Этот параметр определяет тип трансляции IP-адресов в локальной сети, значение 1 определяет трансляцию IP-адресов согласно IP-интерфейсам, значение 0 создает пустой адресный лист.
CheckCollisions	1	Этот параметр используется Транслятором и определяет, есть ли противоречия между Правилами PASS/ENCRYPT для Объектов Интернет/Пользователи. Возможные значения: 0 (проверка выключена), 1 (проверка включена).
ShouldCreatePassRuleForNomadics	True	Этот параметр определяет, следует ли Транслятору создавать разрешающие правила для пользователя внутри защищаемого периметра.
ShouldSplitSubnetForNomadicRules	False	Если пользователь взаимодействует с пересекающимися объектами, то, при значении **False** данного параметра, указанные объекты при трансляции не разбиваются, при значении **True** – разбиваются.
DomainPasswordExpirePeriod	30	Этот параметр определяет время действия доменного пароля в днях.

14.1.5. Параметры сервера приложений секция [Appsrv]

Для редактирования файла инициализации `TPNserver.ini` и изменения общих параметров для всех устройств необходимо изменить параметры файла в любом текстовом редакторе (см. Таблица 47).

Таблица 47 – Опции других параметров фала `TPNServer.ini`

Параметр	Значение по умолчанию	Значение
DomainPasswordExpirePeriod	90	Этот параметр определяет, время до истечения срока действия доменного пароля в днях. Значение параметра 0 = не проверять
InactiveUserSessionExpirePeriod	600	Этот параметр определяет, таймаут отсоединения консоли, если пользователь ничего не делает. Для продолжения работы необходимо войти в систему. Значение параметра 0 = не проверять
IgnoreAuthPassword	false	Этот параметр определяет, проверяется пользовательский пароль или нет. Если установлено true, то пароль не проверяется
PingAliveExpirePeriod	30	Этот параметр определяет время, в течение которого от консоли может не быть ответа (даже если нет никакой длительной задачи). Если консоль молчит дольше, считается, что консоль по каким-то причинам «умерла», и соединение закрывается (если клиент вдруг опять начнет запрашивать информацию, то потребуется ввести идентификационные данные заново)
TaskDesyncExpirePeriod	10	Этот параметр определяет время, в течение которого возможны ожидания между сервером и консолью во время выполнения длительных задач с «прогресс баром» как импорт и трансляция. Если это время превышено, консоль и сервер думают друг о друге «плохое» (завис, упал) и принимают меры: сервер пытается прекратить эту операцию, чтобы не занимать ресурсы вечно, а консоль сообщает пользователю, что операция завершена с ошибкой
CommandReplyExpirePeriod	6	Этот параметр определяет время, в течение которого сервер может не отвечать на команду, которая требует немедленного ответа. Эта команда, в отличие от TaskDesyncExpirePeriod, относится к коротким командам, которые не требуют прогресс-бара и в нормальном состояние должны выполняться очень быстро. Если TaskDesyncExpirePeriod превышен, предполагается, что в сети такие большие задержки, что комфортная работа человека невозможна в принципе - GUI будет постоянно «подвисать»

14.2. Файл distributor.ini

Файл `distributor.ini` присутствует в *ЦУП* директории по умолчанию. Этот файл содержит несколько параметров, которые управляют различными аспектами взаимодействия *ЦУП* с Cisco. Эти параметры - редактируемы; можно изменять значения параметра, редактируя файл в любом текстовом редакторе.

14.2.1. Секция [GlobalSettings]

Эта секция содержит параметры настроек (см. Таблица 48), общие для всех устройств.

Таблица 48 – Параметры секции GlobalSettings

Параметр	Значение по умолчанию	Значение
LogFileName	distributor.log	Имя файла журнала регистрации *ЦУП* Distributor
LogLevel	1	Определяет значение по умолчанию, которое используется системой журнализации, пока действительный уровень журнала регистрации не прочитан из БД *ЦУП*
MaxLoadRequest	10	Максимальное число одновременных запросов, которые могут быть обработаны. Все дополнительные запросы будут находиться в очереди
SessionTimeout	60	Время в секундах, которое система будет ожидать установления сетевого соединения
ConnectionRetry	3	Максимальное число попыток, которое будет делать LSP Loader (Загрузчик), чтобы установить взаимодействие сети с конфигурируемым устройством
ConnectionRetryTimeout	30	Время в секундах, которое система будет ждать между попытками установить сетевое соединение
SimultaneousCheckSize	1	Максимальное число проверочных задач, выполняющихся совместно
CheckWaitTime	300	Время ожидания между попытками реализации проверок. Когда LSP Loader запустится, проверочная программа извлекает список хостов, которые будут проверены и начинает выполнение задач проверки пока, список проверок не будет исчерпан. Следующая попытка загрузить список проверок произойдет после того, как значение этого параметра будет превышено, или после того, как все задачи будут завершены
TimetableCheckTime	10	Является временем ожидания между проверкой на предмет изменений в текущей политики

14.2.2. Секция [ConfFiles]

Эта секция содержит параметры загрузки конфигурационных файлов (см. Таблица 49).

Таблица 49 – Параметры секции ConfFiles

Параметр	Значение по умолчанию	Значение
Entries	5	Число конфигурационных файлов, которое загрузит LSP Loader. LSP Loader будет просматривать имена файлов, заданные как значения параметра
Entry0	ios.xml	Файл конфигурации для Cisco IOS
Entry1	pix.xml	Файл конфигурации для Cisco PIX
Entry2	ckp.xml	Файл конфигурации для Check Point
Entry3	radius.xml	Файл конфигурации для RADIUS-сервера
Entry4	win.xml	Файл конфигурации для IPsec *Агентов* Microsoft

15. Приложение 5. Сетевые сервисы и Группы сетевых сервисов по умолчанию

15.1. Сетевые сервисы

В *ЦУП* существуют предопределенные сетевые сервисы (см. Таблица 50).

Таблица 50 – Сетевые сервисы в составе *ЦУП*

Имя сервиса	Номер протокола по умолчанию	Номер(а) порта по умолчанию	ICMP тип	TCP сервис?	*UDP сервис?*	ICMP сервис?
AH	51					
all-icmp						✓
all-tcp				✓		
all-udp					✓	
biff		512			✓	
bootp		67, 68*			✓	
CPD		18191		✓		
CPD_amon		18192		✓		
CPMI		18190		✓		
CP_Exnet_PK		18262		✓		
CP_Exnet_resolve		18263		✓		
CP_redundant		18221		✓		
CP_reporting		18205		✓		
CP_rtm		18202		✓		
cuseeme		7648			✓	
daytime-tcp		13		✓		
daytime-udp		13			✓	
dhcp		67, 68*			✓	
discard-tcp		9		✓		
discard-udp		9			✓	
dns-tcp		53		✓		
dns-udp		53			✓	
dst_unreachable			3			✓
echo-tcp		7		✓		
echo-udp		7			✓	
echo_reply			0			✓
echo_request			8			✓
ESP	50					
exec		512		✓		
finger		79		✓		
ftp**		21		✓		

Имя сервиса	Номер протокола по умолчанию	Номер(а) порта по умолчанию	ICMP тип	TCP сервис?	*UDP сервис?*	ICMP сервис?
gopher		70		✓		
h323		1720		✓		
h323_ras		1719			✓	
http		80		✓		
https		443		✓		
ike		500			✓	
ike-nat-t		4500			✓	
ike-nat-t-cp		2746			✓	
imap		143		✓		
info_reply			16			✓
info_request			15			✓
kerberos-tcp		750		✓		
kerberos-udp		750			✓	
l2tp		1701			✓	
ldap		389		✓		
ldap-ssl		636		✓		
login		513		✓		
mask_reply			18			✓
mask_request			17			✓
mngmt-agent		3440		✓		
mngmt-event		3118		✓		
name-tcp		42		✓		
name-udp		42			✓	
netbios-datagram		138			✓	
netbios-name		137			✓	
netbios-session		139		✓		
netshow-tcp		1755		✓		
netshow-udp		1755			✓	
netstat		15		✓		
nfs-tcp		2049		✓		
nfs-udp		2049			✓	
nntp		119		✓		
ntp-tcp		123		✓		
ntp-udp		123			✓	
param_problem			12			✓
pop2		109		✓		
pop3		110		✓		
pptp		1723		✓		
printer		515		✓		

Имя сервиса	Номер протокола по умолчанию	Номер(а) порта по умолчанию	ICMP тип	TCP сервис?	*UDP сервис?*	ICMP сервис?
radius		1645			✓	
radius-acc		1646			✓	
realaudio		7070		✓		
redirect		5				✓
rip		520			✓	
rtsp		554		✓		
shell		514		✓		
*sm*b		445		✓		
SMTP		25		✓		
snmp		161			✓	
snmp-trap		162			✓	
source_quench		4				✓
sqlnet-v1		1521		✓		
ssh		22		✓		
streamworks		1558			✓	
syslog		514			✓	
tacacs-tcp		49		✓		
tacacs-udp		49			✓	
telnet		23		✓		
tftp		69			✓	
time-tcp		37		✓		
time-udp		37			✓	
timestamp		13				✓
timestamp_reply		14				✓
time_exceeded		11				✓
vdolive		7000		✓		

Примечание.
* Обозначает исходный порт.
** Сетевой сервис FTP использует соответствующую процедуру МЭ («generic_ftp»), которая автоматически управляет вторичными соединениями для передачи данных (см. п. 7.7.7). Например, в случае «активного» варианта FTP, TCP-порт 20 будет открыт автоматически.

15.2. Группы сетевых сервисов

Некоторые сетевые сервисы, предопределенные в *ЦУП,* были собраны в Группы сервисов для удобства. По умолчанию, те сетевые сервисы, в которых присутствуют и как TCP-сервисы и как UDP-сервисы, представлены Группой сервисов, которая содержит TCP-сервисы и UDP-сервисы.

16. Приложение 6. Глоссарий Протоколов

AH

Заголовок аутентификации. AH обеспечивает целостность данных, аутентификацию источника данных и защиту от атак типа «повторная передача» (anti-replay). AH - один из трех составляющих блоков IPsec, наряду с ESP и IKE.

ARP

Протокол разрешения адресов. ARP - это TCP/IP-протокол, который динамически передает IP-адрес высокого уровня в физический адрес низкого уровня аппаратных средств узла (сетевая интерфейсная карта).

BIFF

BIFF – это служба уведомления прибытия почты, которая сообщает серверу о получателе и смещении файла почтового ящика, который затем извлекает информацию сообщения и уведомляет пользователя, что он или она получил новую почту.

BOOTP

Протокол, определяющий процедуры взаимодействия с узлами, не имеющими жестких дисков. BOOTP – Интернет-протокол, который позволяет бездисковой рабочей станции обнаружить ее собственный IP-адрес, адрес IP BOOTP сервера в сети и файл, который будет загружен в память для загрузки компьютера, таким образом, позволяя рабочей станции производить загрузку без дисковода жесткого диска или гибкого диска.

CU-SeeMe

CU-SeeMe – программа видеоконференции, которая передает звуковые и видео сигналы по сети Интернет. Этот протокол может использоваться для типа «точка–точка» так же, как многоточечных видеоконференций.

Daytime

Протокол daytime извлекает официальную дату и время от NIST-сервера времени и обновляет системное время на компьютере.

Destination Unreachable (ICMP)

Если, согласно информации в таблицах маршрутов Шлюза Безопасности, сеть, указанная в поле **Internet Destination** дейтаграмма, недостижима, Шлюз может посылать ICMP сообщение «Destination unreachable» хосту источнику Интернет-дейтаграммы.

DHCP

Протокол динамической конфигурации хоста. Этот протокол назначает динамические IP-адреса устройствам сети. Устройство может иметь различный IP-адрес, каждый раз как оно соединяется с сетью, в некоторых случаях, в то время как он все еще соединяется.

discard

Сервис Discard просто отбрасывает любые данные, которые он получает, как только было установлено соединение, и продолжается до тех пор, пока создатель соединения не закончит его.

DNS

Сервис имен доменов. DNS - распределенная база данных, используемая для просмотра информации о сетевых адресах. Определенно, DNS позволяет пользователям ссылаться на имя компьютера, а не использовать числовой адрес, используя сервер доменного имени, чтобы транслировать доменные имена в соответствующие числовые IP-адреса (и наоборот).

Echo (ICMP)

Эхо, которое работает поверх ICMP, более обычно известно как "ping". Пакет отправляется удаленному хосту (пакет «echo request»), который затем возвращает этот же пакет (пакет «echo reply»).

ESP

Encapsulating Security Payload. ESP обеспечивает конфиденциальность данных и ограниченную конфиденциальность потока трафика. Он может также обеспечивать целостность данных, аутентификацию происхождения данных и защиту от атак типа «повторная передача» (anti-replay). ESP - один из трех составляющих блоков IPsec, наряду с AH и IKE.

Exec

Сервис выполнения удаленного процесса, используемый почтовыми системами, чтобы уведомить пользователей, что была получена новая почта.

FTP

Протокол передачи файлов. FTP – это TCP/IP-протокол, который позволяет пользователю на одном хосте сети надежно передавать файлы другому хосту сети и принимать от него.

Generic Sun RPC

RPC – это простая система понятий (принцип), для реализации сетевой модели клиент/сервер. RPC, позволяющий пользователю выполнять команду или процедуру на любой удаленной системе и получать результат на собственном терминале пользователя. Generic Sun RPC – это RPC, используемый Sun Microsystems, Inc.

gopher

Система (существовавшая до появления WWW) для организации и показа файлов на Интернет-серверах в виде иерархически структурированного списка файлов.

H.323

H.323 – это стандарт, определяющий как аудиовизуальные данные для телеконференции передаются по сети. Это позволяет пользователям, использующим различные приложения видеоконференций, участвовать в одной конференции.

Host Name Service

Простой метод для преобразования строк имени хоста в IP-адрес.

HTTP

Протокол передачи гипертекста. HTTP – это протокол, используемый WWW для передачи по сети файлов, закодированных в HTML (Язык Гипертекстовой Разметки).

HTTPS

Протокол защищённой передачи гипертекста. HTTPS – это расширение HTTP протокола для безопасной посылки данных (и индивидуальных сообщений) по WWW.

Hybrid IKE

Hybrid IKE является расширением IKE, который позволяет организациям использовать широко применяемые методы аутентификации, такие как токены, RADIUS или TACACS + в пределах IPsec ВЧС. Это расширяет опции IKE-аутентификации за пределы текущих методов разделенных ключей и цифровых сертификатов. Режим Hybrid IKE – это в настоящее время является проект IETF.

ICMP

Протокол управления сообщениями в сети Интернет. ICMP – это протокол (фактически, расширение IP), который сообщает относительно пригодности компьютера сети и любых трудностях в передаче датаграммы. Он учитывает сообщение об ошибке, пакеты проверки и информационные сообщения, связанные с IP.

IKE

Internet Key Exchange IKE – это часть текущего IPsec-стандарта для Правил переговоров защищенных соединением, управления ключом и обмена ключами. IKE – это протокол, определенный IPsec, чтобы обеспечить безопасное и своевременное распределение ключей и связанного с ключом материала между участвующими IPsec-хостами. IKE – это один из трех составляющих блоков IPsec, наряду с AH и ESP.

IKE CFG

IKE CFG – это расширение (известное как Режим Конфигурации) протокола IKE, первоначально развитого Cisco Systems. Этот протокол вставляет дополнительные двусторонние IKE транзакции в середину процесса установки IPsec-туннеля. Таким образом,

IKE CFG позволяет IPsec Шлюзу Безопасности снабжать удаленного клиента IPv4 и IPv6 назначениями адресов, сетевыми масками и адресами DNS/DHCP-сервера.

IMAP

Протокол доступа к сообщениям в сети Интернет. IMAP – это клиент-серверный протокол, который позволяет пользователю динамически получать доступ к почтовым средствам на хосте сервера. Он также определяет, как Сервер Интернет-пользователя обрабатывает его/ее электронную почту, позволяя пользователю более сложные возможности выбора, чем с POP по обработке электронной почты.

Information request/reply (ICMP)

Запрос/ответ информации поддерживается системами с автоматическим (ре)конфигурированием, такими как бездисковые рабочие станции, чтобы позволять им обнаруживать их IP network prefixes во время загрузки.

IP

Интернет-Протокол. IP – это основной протокол коммуникации пакетов, который маршрутизирует и доставляет TCP и UDP-пакеты по сети без необходимости прямого соединения между двумя компьютерами (непрерывное отправление данных). IP отвечает только за доставку пакетов к месту их назначения.

IPsec

Internet Protocol security. IPsec – это набор протоколов для обмена пакетов в IP-слое. IPsec имеет два режима шифрования: транспортный и туннель. Транспортный режим шифрует только данные пакета, в то время как туннельный режим, который является более безопасным, шифрует и заголовок пакета и данные пакета. Устройства, посылающие и получающие эти пакеты, должны совместно используемый открытый ключ.

Kerberos

Kerberos – это система аутентификации, которая позволяет двум сторонам обмениваться секретной информацией по открытой сети, назначая уникальный ключ каждому пользователю, который входит в сеть и использовать этот ключ для идентификации источника сообщения.

L2TP

Layer 2 Tunnelling Protocol. L2TP – это расширение PPP протокола, которое позволяет ISPs использовать Виртуальные Частные Сети.

LDAP

Lightweight Directory Access Protocol (Протокол доступа к каталогу). LDAP – это протокол, используемый для извлечения информации из совместимой с X.500 директории.

Клиент, использующий LDAP, может восстановить списки информации такие, как имена, адреса электронной почты, местоположения и открытые ключи.

Login

Удаленный сервис регистрации, который обслуживает базы данных тех, кто зарегистрировался в локальной сети и среднюю загрузку компьютера.

LPD

Line Printer Daemon. LPD – это программа управления принтером, которая выполняется на хосте сети сервере или клиенте.

Mask request/reply (ICMP)

Маска адреса запроса/ответа используется, чтобы определить поле маски адреса Шлюза подсети, с которой был получен запрос.

NAT

Network Address Translation (Трансляция сетевых адресов) – это трансляция IP-адресов, используемых в пределах одной сети в IP-адреса, используемые в пределах другой сети. Одна сеть - внутренняя сеть, и другая - внешняя. Компания может устанавливать свои собственные «внутренние локальные» адреса одному или более «внешним глобальным» IP-адресам и преобразовывать глобальных IP-адресов из входящих пакетов в локальные IP-адреса. NAT помогает обеспечивать Безопасность и сохраняет необходимое число глобальных IP-адресов; компания может таким образом, использовать единый IP-адрес, чтобы связаться по сети Интернет. NAT используется, как часть маршрутизатора и часто, как часть корпоративного межсетевого экрана. NAT может быть определен для статической или динамической трансляции в/из пул(а) IP-адресов.

NetBIOS

Network Basic I/O System. NetBIOS (Сетевая базовая система ввода-вывода). NetBIOS – это сервис сеансового уровня соединения, используемый клиентом и приложениями сервера в TokenRing и LAN сетях. Это обеспечивает приложения с программируемым интерфейсом для совместного использования сервисами и информацией в разнообразных сетевых протоколах низшего уровня, включая IP. Дейтаграмма, имя и сервисы сессии доступны через NetBIOS.

NetShow

Протокол, разработанный компанией Microsoft для потоковой передачи содержимого мультимедиа по WWW.

Netstat

Сервис, который показывает сетевые статистические данные текущего хоста.

NFS

Network File System (Сетевая файловая система). Приложение для клиента/сервера, разработанное Sun Microsystems, которые позволяет всем пользователям сети получать доступ к коллективным файлам, хранящимся на компьютерах различных типов. NFS выполняется над TCP/IP. Компьютеры сети с NFS будут действовать как клиенты при доступе к удаленным файлам и как серверы при обеспечении удаленного доступа пользователей к локальным коллективным файлам.

NNTP

Network News Transfer Protocol (Сетевой протокол передачи новостей). NNTP – это TCP/IP протокол для отправления, распределения, запроса и исправления статей новостей. Он обеспечивает центральное хранение базы данных статей новостей и позволяет подписчику выбирать и извлекать только определенный набор сообщений. Также обеспечивается индексация, перекрестные ссылки и удаление старых сообщений.

NTP

Network Time Protocol. (сетевой протокол времени). NTP – это протокол, который гарантирует, что часы локального компьютера работают точно относительно радио и атомных часов (серверов времени), расположенных в сети Интернет. NTP позволяет всем коммуникационным сетям иметь точное время.

Parameter problem (ICMP)

Сообщение «о проблеме с параметром» создаётся, как ответ на любую ошибку обработки дейтограммы, не покрывающую другим ICMP-сообщением.

POP2

Post Office Protocol (Почтовый протокол), версия 2. POP2 позволяет пользователю динамически получать доступ к почте на хосте сервера. Это позволяет меньшему узлу извлекать почту из хоста сервера по требованию без совместного выполнения *SMTP*-сервера.

POP3

Post Office Protocol (Почтовый протокол), версия 3. POP3 позволяет пользователю динамически получать доступ к почте на хосте сервера. Это позволяет меньшему узлу извлекать почту из хоста сервера по требованию без совместного выполнения *SMTP*-сервера.

PPTP

Point-to-Point Tunnelling Protocol (Протокол туннелирования «точка-точка»). PPTP – это технология для создания Виртуальных Частных Сетей как альтернативы IPsec проколу. PPTP гарантирует Безопасность, сообщений, переданные от одного ВЧС узла к другому.

RADIUS

Remote Authentication Dial-In User Service (Сервис удаленной аутентификации пользователей по телефонным линиям). Сервер RADIUS позволяет серверу удаленного доступа связываться с центральным сервером, чтобы подтвердить аутентификацию dial-up (коммутируемых) соединений и авторизовать этих пользователей для получения доступа к данной системе или сервису. Профили пользователей могут храниться в центральной базы данных, совместно используемой всеми удаленными серверами, также возможно установить Политику, которая может применяться для взятой в отдельности точки в сети. Серверы RADIUS используют UDP протокол, и содержат аутентификацию и авторизацию в единственном профиле пользователя.

RealAudio

Стандарт, разработанный RealNetworks для передачи потоковых аудио данных по WWW.

Redirect (ICMP)

Сервис ICMP Redirect – это механизм для маршрутизаторов, чтобы передать информацию маршрутизации к хостам так, чтобы хост мог посылать пакеты к ближайшим Шлюзам.

RIP

Routing Information Protocol (Протокол маршрутной информации). Rip – это Протокол внутреннего Шлюза (IGP), который используется, чтобы определить самый короткий и/или самый быстрый путь для передачи данных по сети.

RTSP

Real-Time Streaming Protocol. RTSP – это стандарт для управления потоком данными в сети Интернет. RTSP использует RTP (Real-Time Transport Protocol), чтобы форматировать пакеты мультимедиа. RTSP, главным образом, предназначен для широковещания аудиовизуальных данных.

Shell

Удаленный протокол пользовательского интерфейса (оболочки), характерный для UNIX-систем, предназначенный для выполнения команд оболочки на удаленном хосте UNIX без выполнения полной регистрации.

SMTP

Simple Mail Transfer Protocol (Простой протокол передачи электронной почты). SMTP – это TCP/IP-протокол для надежного обмена электронными сообщениями почты по сети. Все сообщения, посланные через *SMTP*, должны представлять собой простой текст.

SNMP

Simple Network Management Protocol (Простой протокол сетевого управления). SNMP – это протокол уровня приложения для управления TCP/IP сети. SNMP выполняется поверх UDP, который в свою очередь выполняется поверх IP. SNMP сформирован в терминах станций управления сети (NMS), которые выбирают устройства сети (SNMP-*Агенты*). По требованию NMS, SNMP-*Агент* получает доступ к базе информации управления (MIB) и посылает информацию к NMS. MIB обеспечивает стандартное представление информации о SNMP-*Агенте* и о месте ее хранения.

Source quench (ICMP)

Source quench message – это запрос на уменьшение скорости передачи данных сообщений, посланных приемником в сети Интернет.

SQLNet v1

Oracle Structured Query Language Network, версия 1. Этот протокол обеспечивает прозрачные соединения от клиентских инструментальных средств Oracle к БД Oracle или между двумя базами данных.

SSH

Secure Shell Protocol. SSH позволяет защищать удаленный вход в сеть, передачу файлов и перенаправление TCP/IP- и X11-соединений. Протокол шифрует, аутентифицирует и сжимает передаваемые данные.

StreamWorks

StreamWorks – это протокол аудио/видео потоковой передачи, разработанный Real Networks, чтобы рассылать аудиовизуальные данные как поток UDP-пакетов по TCP/IP-сетям.

Syslog

Syslog – это UNIX-утилита, которая позволяет администраторам системы контролировать, регистрировать и управлять сообщениями об ошибке, сгенерированными сетевой системой, обеспечивать централизацию и распределение по категориям сетевых журналов. Также указывать формат сетевых журналов, который может использоваться для централизованного управления сообщений регистрации.

TACACS +

Terminal Access Controller Access Control System. TACACS + - это протокол аутентификации, который позволяет удаленному серверу доступа отправлять пароль пользователя серверу аутентификации, чтобы определить, можно ли предоставить доступ этому пользователю. Он использует TCP-протокол, и разделяет процессы аутентификации и авторизации.

TCP

Transmission Control Protocol.(Протокол управления передачей). TCP – это универсальный протокол транспортного уровня, который обеспечивает надежную двухточечную связь, используя дейтораммы (пакеты), посылаемые поверх IP. TCP ориентирован как на соединения, так и на поток. Он разбивает длинные потоки данных на отдельные части (пакеты) на источнике и гарантирует их точную и надежную повторную сборку на устройстве приемника, по существу создавая временный выделенный канал между двумя узлами.

Telnet

Telnet – это стандартный Интернет-протокол для соединения удаленных терминалов. Telnet позволяет пользователю входить в систему и непосредственно использовать ее на удаленном компьютере.

TFTP

Trivial File Transfer Protocol (Простой протокол передачи данных) TFTP – это TCP/IP-протокол, используемый для обмена файлами между сетевыми станциями с меньшими системными издержками, чем FTP потому что TFTP не требует действительных имени пользователя и пароля. Он реализован UDP (Протокол Дейтограмм Пользователя).

Time

Time Server Protocol (Протокол сервера времени) используется, чтобы подтверждать или исправить настройки времени компьютера, опрашивая независимые сайты в сети.

Timestamp request/reply (ICMP)

Временная метка запроса/ответа используется, чтобы проследить время, которое занимает удаленное устройство, чтобы получать и повторно отправлять пакеты.

UDP

User Datagram Protocol (Пользовательский протокол дейтограмм). UDP – это универсальный протокол транспортного уровня, который передает дейтограммы (пакеты) поверх IP в ситуациях, где не требуется надежная, последовательная доставка. Клиенты сети используют UDP, прежде всего, чтобы связаться с серверами доменных имен, чтобы определить сетевые адреса.

VDOLive

VDOLive – это аудио/видео потоковый протокол, который использует сжатие в реальном времени, чтобы осуществлять аудиовизуальное широковещание режиме реального времени.

XAUTH

XAUTH – это расширение протокола IKE. XAUTH вставляет новую транзакцию обмена IKE в середину IKE, после того, как стадия 1 (аутентификация уровня устройства) была осуществлена. Используя XAUTH, IPsec Шлюз Безопасности может побудить клиента к расширенным мандатам аутентификации и затем проверить их на указанном RADIUS или TACACS + сервере. Стадия 2 IKE (установка туннеля) будет пройдена, только если клиент произвел удовлетворительные мандаты.

X11

X11 – это наиболее широко применяемая версия системы X-Windows, которая является TCP/IP-системой сетевого графического интерфейса пользователя (GUI) и позволяет программе использовать дисплей на другом компьютере. Протокол X11 использует TCP в качестве транспортного протокола.

17. ПРИЛОЖЕНИЕ 7. ICMP-КОДЫ

Протокол управления сообщениями в сети Интернет (ICMP) предоставляет информацию о сетевом трафике. Например, узел (источник) послал пакет и установил опцию, что во время пути он не должен делиться на фрагменты; Ваш сервер или маршрутизатор не смогли получить пакет, потому что его размер был слишком велик согласно установленным настройкам; пакет не был доставлен. ICMP – это сервис, который создаёт сообщения о таких транзакциях трафика. ICMP-серверы разделены на типы, и есть несколько кодов, которые определяют транзакцию. Например, если пакет был возвращен источнику, потому что необходимый порт на хосте конечного устройства был заблокирован или был не досягаемый, то это соответствует типу сервиса ICMP равным «3» и коду ICMP равным «3».

ICMP-сервисы не работают с IKE/IPsec когда ICMP-типы или коды определены наряду с действиями пользователя, например, шифрованием. Например, Вы хотите определить ICMP-пакеты как Сервис и использовать это в Правилах. В этом случае, можно только включать ICMP-сервисы в Правило. Включение определяемого пользователем шифрования приводит к шифрованию ICMP-пакетов независимо от типа или кода. Любое сообщение, инкапсулированное в IPsec, длиннее, чем первоначальное, и, следовательно, образовавшийся пакет неправилен. При определении конкретных типов/кодов (см. Таблица 51), можно использовать только Pass/Drop действия без шифрования.

Таблица 51 – ICMP-коды

Тип	Код	Описание
		Echo request and echo reply messages
		(Эхо сообщения ответа и запроса):
0	0	Эхо сообщение ответа
8	0	Эхо сообщения запроса
		Destination unreachable messages Сообщение о недостижимости получателя:
3	0	Сеть недостижима
3	1	Хост не достижим
3	2	Протокол не доступен
3	3	Порт не доступен
3	4	Необходима фрагментация сообщения и DF набор
3	5	Сеть места назначения неизвестна
3	6	Конечное устройство сети неизвестно
3	7	Хост конечного устройства неизвестен
		Source quench message(Исходное сообщение блокировано):
4	0	Отключение источника при переполнении очереди
		Redirect messages (Переадресовать (изменить маршрут):
5	0	Переадресовать дейтограмму в сеть (устарело)
5	1	Переадресовать дейтограмму для хоста

Тип	Код	Описание
5	2	Переадресовать дейтограмму для типа сервиса и сети
5	3	Переадресовать дейтограмму для типа сервиса и хоста
		Time exceeded messages (Сообщения об истечении времени жизни):
11	0	Время существования дейтограммы превышено при прохождении
11	1	Время сборки фрагмента превышено
		Parameter problem message (Сообщение о проблеме с параметрами дейтограммы):
12	0	Ошибка в IP-заголовке
		Timestamp request and timestamp reply messages (Сообщения запроса и отклика временной метки):
13	0	Запрос временной метки
14	0	Отклик временной метка
		Information request and information reply messages:
15	0	Сообщение - запрос информации
16	0	Сообщение - информационный отклик

18. Приложение 8. Утилит командной строки TPNCLI

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

Утилита командной строки позволяет выполнить действия с объектами политики, ЛПБ, ГПБ, а также настройками БД в системе и её состоянием.

Синтаксис командной утилиты выглядит следующим образом:

`TPNCLI <common options> <command> [<command options>],`

где: «`common options`» - общие параметры команды (см. Таблица 52),

«`command`» - исполняемые команды (см. Таблица 53).

Таблица 52 – Общие параметры команды

Параметр	Описание
u <user name>	Доменное имя пользователя, по умолчанию «sm-admin»
p <password>	Пароль пользователя в домене, по умолчанию пустой
np <password>	Новый пароль при необходимости смены
s <ip>[:<port>]	Адрес сервера базы данных, по умолчанию 127.0.0.1:3118
l <language>	Язык интерфейса
sp+	Параметр сохранения введённых паролей
sp-	Параметр отмены сохранения введенного пароля
tc+	Обрезать колонки в таблице (по умолчанию)
tc-	Параметр позволяет не обрезать колонки (эффект сохраняется до выхода из-под учетной записи)
ac+	Выровнять столбцы при выводе таблицы (действует по умолчанию)
ac-	Не выравнивать столбцы (действует до выхода из системы)

Команды утилиты командной строки tpncli загружают в проект новые правила.

Для создания правила с помощью утилиты необходимо создать описание правила в текстовом редакторе и сохранить его в формате xml. Для просмотра id объекта политики необходимо выбрать объект и выполнить комбинацию клавиш <Cntrl>+<Alt>+<Shift>+<i>.

Таблица 53 – Команды `tpncli`

Параметр	Описание	Синтаксис и параметры команд
get	Показать содержимое таблицы или одного элемента	**`TPNCLI <общие опции> -get all`** **`TPNCLI <общие опции> -get <фильтр>*`** - показать идентификаторы, имена, типы и владельцев элементов таблицы. **`TPNCLI <общие опции> -get <фильтр> <xml-файл>`** - записать содержимое элементов таблицы в xml-файл

Параметр	Описание	Синтаксис и параметры команд
set	Изменить содержимое отдельного элемента в таблице	**TPNCLI <общие опции> -set <xml-файл>** - читает из XML содержимое элемента и изменяет его
let	Присвоить значение параметров элемента или элементов	**TPNCLI <общие опции> -[let] <фильтр>** - незавершенная команда let работает как get, т.е. получает текущее содержимое соответствующего элемента ГПБ. **TPNCLI <общие опции> -let <фильтр> = <фильтр2>** - замена текущих связей на связь с <фильтром2>. Например, установить действие 'Pass' в качестве действия для правила 'r1': **TPNCLI - rule['r1'].to_assoc = assoc['pass']** Например, установить действие 'Pass' в качестве действия для всех правил: **TPNCLI - rule.to_assoc = assoc['pass']** Например, для правила 'r1' установить то же действие, что и в правиле 'r2': **TPNCLI - rule['r1'].to_assoc = rule['r2'].to_assoc** В случае, если <фильтр2> равен нулю, все связи заданного типа убираются. Например, очистить колонку 'Source' для правила 'r1': **TPNCLI - rule['r1'].to_host_src = 0** *Команда добавления связей.* **TPNCLI <общие опции> -let <фильтр> + <фильтр2>** - добавление связи с <фильтром2> к уже имеющимся связям. Например, добавить в колонку 'Source' правила 'r1' хост 'any': **TPNCLI - rule['r1'].to_host_src + host['any']** *Команда удаления связей* **TPNCLI <общие опции> -let <фильтр> - <фильтр2>** - удаление связи с <фильтром2> из имеющихся. Например, удалить хост 'any' из колонки 'Source' во всех правилах, где он есть в этой колонке: **TPNCLI - rule.to_host_src - host['any']** Во всех командах изменения связей название таблицы и квадратные скобки можно опускать, например, **TPNCLI - rule.to_host_src - 'any'** Чтобы посмотреть синтаксис <фильтра> надо ввести: **TPNCLI -help filter**
new/ create	Создать элемент в таблице	**TPNCLI <общие опции> -new [-soft] <xml-файл>** - читает из XML содержимое элемента и создает его опция -soft заставляет по возможности игнорировать ошибки. **TPNCLI <общие опции> -new [<фильтр>] [-pass**

Параметр	Описание	Синтаксис и параметры команд
		<пароль>] <файл сертификата> [<файл ключа>] - создает сертификаты, импортируя их из файла (если он не .xml) <фильтр> - чтобы указать хост для сертификата безопасности <пароль> - указывает пароль для контейнера PKCS#12
del/ remove	Удалить элемент из таблицы	**TPNCLI <общие опции> -del <фильтр>**
erase	Сброс БД	**TPNCLI <общие опции> -erase**
import	Импортировать файл в БД (.zip, .xml, .gsp)	**TPNCLI <общие опции> -import [-archive] [-timestamp] <файл>** - <файл> может быть .zip, .gsp или .xml Опция -archive импортирует также архивные ЛПБ. Опция -timestamp записывет в XML дату экспорта.
export	Экспортировать файл в БД (.zip, .xml, .gsp)	**TPNCLI <общие опции> -export [-archive] <файл>** – <файл> может быть только .gsp Опция -archive экспортирует также архивные ЛПБ
activate	Активировать выбранные объекты или всю ГПБ	**TPNCLI <общие опции> -activate [-updated] -all** - активировать всё (опция '-updated' фильтрует по измененным). **TPNCLI <общие опции> -activate [-updated] <фильтр>** - активировать указанные элементы политики (хосты, сервера, домены).
translate	Транслировать выбранные объекты или всю ГПБ	**TPNCLI <общие опции> -translate -all** - транслировать ГПБ **TPNCLI <общие опции> -translate <фильтр>** - транслировать указанные элементы политики (хосты, домены)
merge	Скачать ЛПБ для слияния	**TPNCLI <общие опции> -merge <gfgrf> [gates] [users] [hosts]** - получить активные и готовые к активации ЛПБ в указанную <папку> для последующего сопоставления. gates, users, hosts - фильтры с указанием, для каких объектов ЛПБ (по умолчанию только для gates)
update	Обновить *Агентов*	**TPNCLI <общие опции> -update -all** - обновить все *Агенты* **TPNCLI <общие опции> -update <фильтр>** - обновить указанные элементы политики (хосты, домены)
upload	Загрузить *Агентов*	**TPNCLI <общие опции> -upload -all** - загрузить все *Агенты* **TPNCLI <общие опции> -upload <фильтр>** - загрузить *Агенты* для указанных элементов политики (хостов, доменов)
login	Загрузится в БД и внести изменения	**TPNCLI <общие опции> -login**
logout	Выйти из БД и	**TPNCLI <общие опции> -logout**

Параметр	Описание	Синтаксис и параметры команд
	закрыть клиент	
state/ monitor	Просмотреть состояние	**TPNCLI <общие опции> -state all** - получить состояние всех (прогружаемых) объектов политики и серверов **TPNCLI <общие опции> -state defined** - получить состояние объектов политики и серверов, кроме «неопределенного» **TPNCLI <общие опции> -state <filter>** - получить состояние объектов политики или серверов
Примечание. * Чтобы посмотреть синтаксис <фильтра>, введите: **TPNCLI -help filter**		

Параметры команд tpncli можно посмотреть в справке к необходимой команде, для этого необходимо воспользоваться ключом –h.

19. Устранение неисправностей

п/н	Описание неисправностей	Решение
1	Конфигурирование «КриптоПро CSP» версии 3.6.1 Смена исполнения провадера - KC1, KC2.	*/opt/cprocsp/sbin/<arch>/cpconfig -defprov -view -provtype 75 :* показать список установленных провайдеров СКЗИ «КриптоПро CSP» типа 75 (ГОСТ Р 34.10-2001) */opt/cprocsp/sbin/<arch>/cpconfig -ini '\cryptography\Defaults\Provider Types\Type 075\Name' -view:* показать провайдер по умолчанию типа 75 */opt/cprocsp/sbin/<arch>/cpconfig -defprov -setdef -provtype 75 -provname 'Crypto-Pro GOST R 34.10-2001 KC2 CSP':* установить провайдер по умолчанию типа Crypto-Pro GOST R 34.10-2001 KC2 CSP */opt/cprocsp/sbin/<arch>/cpconfig -license -set <license> :* Установить лицензию КриптоПро CSP */opt/cprocsp/bin/<arch>/csptest -keys -verifycontext :* показать версию КриптоПро CSP */opt/cprocsp/sbin/amd64/cpconfig -hardware reader -del FLASH :* Удалить аппаратный считыватель "FLASH"
2	Невозможно сделать автоматическое обновление, если сертификат, которым подписан агент, просрочен.	При автоматическом обновлении с параметром silent=0 см. п. 12.1.1 появляется окно, с запросом о том, что АО «ЭЛВИС-ПЛЮС» - доверенный производитель. При автоматическом обновлении с параметром silent=1 запросов не возникает. Примеры update.ini: – если путь к утилите содержит пробел: [CLIENT.WINXX.amd64.zastava] version = 6.1.15455 file = zastavaclient64-exp.exe, cert.cer exec = cmd /C echo off & "C:\WINDOWS\system32\certutil.exe" -addstore trustedpublisher "$download_path\cert.cer" && "$download_path\zastavaclient64-exp.exe" /l*v c:\distr\zastava1-setup.txt silent = 1 – если путь к утилите не содержит пробел: [CLIENT.WINXX.amd64.zastava] version = 6.1.15455 file = zastavaclient64-exp.exe, cert.cer exec = cmd /C certutil.exe -addstore trustedpublisher "$download_path\cert.cer" && "$download_path\zastavaclient64-exp.exe" /l*v c:\distr\zastava1-setup.txt silent = 1

3	Неверно отображается статус активации узлов кластера.	Вручную выставить соответствующие номера узлов кластера для каждого локального сертификата на вкладке *ВЧС/сертификаты*.

20. Перечень сокращений

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

БД – база данных

ВЧС - виртуальная частная сеть

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

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

ЗРС - Запрос Регистрации Сертификата

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

МСЭ – межсетевое экранирование

МЭ – межсетевой экран

ОС - операционная система

ПК - программный комплекс

ПО - программное обеспечение

СКЗИ - средство криптографической защиты информации

СОС - список отозванных сертификатов

СУБД – система управления базами данных

УЦ – Удостоверяющий Центр

ЦС - Центр Сертификации

ЦУП - центр управления политиками безопасности *ЗАСТАВА-Управление*

AH (Authentication Header) - протокол из группы IPsec

ASK LSP - начальная ЛПБ, после активации которой *Агент* соединяется с *ЦУП* и получает от него текущую полную ЛПБ

CA (Certification Authority) - см. ЦС

CER (Certificate Enrollment Request) - см. ЗРС

CLI (Command Line Interface) - интерфейс командной строки

CRL (Certificate Revocation List) - см. СОС

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

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

ESP (Encapsulated Security Payload) - протокол из группы IPsec

FQDN (Fully Qualified Domain Name) – полное доменное имя хоста

GMT - время по Гринвичу

GSP (Global Security Policy) - см. ГПБ

GUI (Graphical User Interface) - графический интерфейс пользователя

IKE (Internet Key Exchange) - протокол обмена ключевой информацией; используется совместно с протоколами IPsec для организации первичного защищенного канала ISAKMP SA

IP (Internet Protocol) - протокол сетевого уровня, являющийся базовым протоколом IP-сетей

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

LDAP (Lightweight Directory Access Protocol) – группа стандартных протоколов для доступа к каталогам («Directories»)

Log - журнал регистрации

Log level - уровень детализации при регистрации событий

LSP (Local Security Policy) - см. ЛПБ

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

MSDE (Microsoft SQL Server Desktop Engine) – сервер базы данных

NAT (Network Address Translation) - трансляция сетевых адресов

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

Nomadic Client (мобильный пользователь) – устаревшее название для объекта User (в контексте ПК «VPN/FW «ЗАСТАВА»)

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

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

PPP (Point-to-Point Protocol) - протокол соединений «точка-точка» в IP-сетях

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

SMB - протокол доступа к ресурсам сети

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

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

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

VPN (Virtual Private Network) - см. ВЧС

Перечень ссылочных документов

[1] МКЕЮ.00434 01 32 01 «Программный комплекс защиты корпоративных вычислительных ресурсов на сетевом уровне с использованием технологий VPN и распределенного межсетевого экранирования на основе интернет-протоколов семейства IPsec/IKE «VPN/FW «ЗАСТАВА», версия 6» («ПК «VPN/FW «ЗАСТАВА», версия 6»). Компонент «ЗАСТАВА-Офис», версия 6. Руководство системного программиста».

[2] МКЕЮ.00435-01 32 01 «Программный комплекс защиты корпоративных вычислительных ресурсов на сетевом уровне с использованием технологий VPN и распределенного межсетевого экранирования на основе интернет-протоколов семейства IPsec/IKE «VPN/FW «ЗАСТАВА», версия 6» («ПК «VPN/FW «ЗАСТАВА», версия 6»).. Компонент «ЗАСТАВА–Клиент», версия 6. Руководство системного программиста».

[3] МКЕЮ.00433-01 91 01 «Программный комплекс защиты корпоративных вычислительных ресурсов на сетевом уровне с использованием технологий VPN и распределенного межсетевого экранирования на основе интернет-протоколов семейства IPsec/IKE «VPN/FW «ЗАСТАВА», версия 6» («ПК «VPN/FW «ЗАСТАВА», версия 6»). Правила пользования».

ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ

Изм.	Номера листов (страниц)				Всего листов (страниц) в документе	Номер документа	Входящий номер сопроводительного документа и дата	Подпись	Дата
	изме–ненных	заме–ненных	новых	изъя–тых					
1	-	все	-	-	284	МКЕЮ.042	-	Власов П.Ю.	15.02. 2016 г.